


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

April 28, 2009

Document Control Desk
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

Attention: Mr. Jeffrey A. Ciocco

Docket No. 52-021
MHI Ref: UAP-HF-09196

Subject: MHI's Responses to US-APWR DCD RAI No.229-2022, No.226-2018, No.230-2028, No.227-2020, No.238-2030, No.239-2033, No.240-2035, No.228-2021, and No.231-2037, Revision 0

- Reference:**
- 1) "Request for Additional Information 229-2022 Revision 0, SRP Section: 07.01 – Instrumentation and Controls - Introduction, Application Section: 07.01, dated 2/26/2009
 - 2) "Request for Additional Information 226-2018 Revision 0, SRP Section: 07.02 – Reactor Trip System, Application Section: 07.02, dated 2/26/2009
 - 3) "Request for Additional Information 230-2028 Revision 0, SRP Section: 07.03 – Engineered Safety Features Systems, Application Section: 07.03, dated 2/26/2009
 - 4) "Request for Additional Information 227-2020 Revision 0, SRP Section: 07.04 – Safe Shutdown Systems, Application Section: 07.04, dated 2/26/2009
 - 5) "Request for Additional Information 238-2030 Revision 0, SRP Section: 07.05 – Information Systems Important to Safety, Application Section: 07.05, dated 2/26/2009
 - 6) "Request for Additional Information 239-2033 Revision 0, SRP Section: 07.06 – Interlock Systems Important to Safety, Application Section: 07.06, dated 3/2/2009
 - 7) "Request for Additional Information 240-2035 Revision 0, SRP Section: 07.07 – Control Systems, Application Section: 07.07, dated 3/2/2009
 - 8) "Request for Additional Information 228-2021 Revision 0, SRP Section: 07.08 – Diverse Instrumentation and Control Systems, Application Section: 07.08, dated 2/26/2009
 - 9) "Request for Additional Information 231-2037 Revision 0, SRP Section: 07.09 – Data Communication Systems, Application Section: 07.09, dated 2/26/2009

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

Enclosed are the responses to RAIs contained within References 1 through 9.

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

MHI 2/26/2009

DO81

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

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

Sincerely,



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

Enclosure:

1. Affidavit of Yoshiki Ogata
2. Responses to Request for Additional Information No. 229-2022, 226-2018, 230-2028, 227-2020, 238-2030, 239-2033, 240-2035, 228-2021, and 231-2037 Revision 0 (proprietary version)
3. Responses to Request for Additional Information No. 229-2022, 226-2018, 230-2028, 227-2020, 238-2030, 239-2033, 240-2035, 228-2021, and 231-2037 Revision 0 (non-proprietary version)

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-09196

MITSUBISHI HEAVY INDUSTRIES, LTD.

AFFIDAVIT

I, Yoshiki Ogata, state as follows:

1. I am General Manager, APWR Promoting Department, of Mitsubishi Heavy Industries, LTD ("MHI"), and have been delegated the function of reviewing MHI's US-APWR documentation to determine whether it contains information that should be withheld from public disclosure pursuant to 10 C.F.R. § 2.390 (a)(4) as trade secrets and commercial or financial information which is privileged or confidential.
2. In accordance with my responsibilities, I have reviewed the enclosed document entitled Responses to Request for Additional Information No. 229-2022, 226-2018, 230-2028, 227-2020, 238-2030, 239-2033, 240-2035, 228-2021, and 231-2037 Revision 0 dated April 2009, and have determined that portions of the document contain proprietary information that should be withheld from public disclosure. Those pages containing proprietary information are identified with the label "Proprietary" on the top of the page and the proprietary information has been bracketed with an open and closed bracket as shown here "[]". The first page of the document indicates that all information identified as "Proprietary" should be withheld from public disclosure pursuant to 10 C.F.R. § 2.390 (a)(4).
3. The information identified as proprietary in the enclosed document has in the past been, and will continue to be, held in confidence by MHI and its disclosure outside the company is limited to regulatory bodies, customers and potential customers, and their agents, suppliers, and licensees, and others with a legitimate need for the information, and is always subject to suitable measures to protect it from unauthorized use or disclosure.
4. The basis for holding the referenced information confidential is that it describes the unique design and methodology developed by MHI for performing the design of the US-APWR reactor.
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 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 I&C system. Providing public access to such information permits competitors to duplicate or mimic the 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 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, 2009.

A handwritten signature in black ink, appearing to read "Y. Ogata". The signature is written in a cursive, somewhat stylized font.

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

Enclosure 3

UAP-HF-09196
Docket No. 52-021

Responses to Request for Additional Information No. 229-2022,
226-2018, 230-2028, 227-2020, 238-2030, 239-2033, 240-2035,
228-2021, and 231-2037 Revision 0

April 2009
(Non-Proprietary)

**Responses to Request for Additional Information No.229-2022
Revision 0**

**SPR Section 7.1
Instrumentation and Controls - Introduction**

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 229-2022 REVISION 0
SRP SECTION: 07.01 – INSTRUMENTATION AND CONTROLS - INTRODUCTION
APPLICATION SECTION: 07.01
DATE OF RAI ISSUE: 2/26/2009

QUESTION NO.: 07.01-1

The staff requests MHI to provide a Table, or revise Table 7.1-2 accordingly, which specifically locates the paragraph or section within the DC-FSAR, or another US-APWR document, that demonstrates, or states, that a particular system(s) or feature(s) of the US-APWR conforms to each Criteria of IEEE-603. The staff will use this as a roadmap for evaluation of IEEE Std 603 specific criteria compliance. (See attached Table "Attachment to RAI 7.1-01: Roadmap of US-APWR I&C Systems Conformance to IEEE Std. 603")

Compliance with IEEE Std 603 is required under 10 CFR 50.55a(h).

ANSWER:

Topical Report, "Safety I&C System Description and Design Process" (Safety I&C TR), MUAP-07004, Appendix A describes conformance to IEEE Std. 603-1991. DCD Subsection 7.1.2 already refers MUAP-07004 Appendix A as follows.

Additionally, compliance with Appendices C.I.7.1-B, "Conformance with Institute of Electrical and Electronics Engineers (IEEE) Std 603", and C.I.7.1-C, "Conformance with IEEE Std 7-4.3.2", are discussed in TR MUAP- 07004 Appendices A and B respectively.

For some sections of IEEE Std 603-1991, complete compliance requires plant specific descriptions. For these areas the Safety I&C TR refers to "plant licensing documentation". For the US-APWR these plant specific items are addressed in the table below. The table provides a roadmap for evaluation of each clause of IEEE Std 603-1991, where "plant licensing documentation" is referenced in the Safety I&C TR, with the corresponding DCD sections, which describe the plant specific information.

The road map of the US-APWR I&C system conformance to IEEE Std. 603-1991 will be added in Chapter 7. It is noted that the table references new DCD Subsection 7.1.3.19 which addresses the color coding for labels and name tags required from criteria 5.11 of IEEE Std 603-1991.

Impact on DCD

The third paragraph in Subsection 7.1.2 will be revised as follows.

Compliance to the corresponding sections of Appendix C.I.7.1-A in RG 1.206 (Reference 7.1-7), "Digital Instrumentation and Control Systems Application Guidance", are discussed in

Subsection 7.1.3. Additionally, compliance with Appendices C.I.7.1-B, "Conformance with Institute of Electrical and Electronics Engineers (IEEE) Std 603", and C.I.7.1-C, "Conformance with IEEE Std 7-4.3.2", are discussed in Topical Report MUAP-07004 Appendices A and B respectively. Additionally, compliance with Appendices C.I.7.1-B, "Conformance with Institute of Electrical and Electronics Engineers (IEEE) Std 603", and C.I.7.1-C, "Conformance with IEEE Std 7-4.3.2", are discussed in TR MUAP- 07004 Appendices A and B respectively. For some sections of IEEE Std 603-1991, complete compliance requires plant specific descriptions. For these areas the Topical Report MUAP-07004 refers to "plant licensing documentation". For the US-APWR these plant specific items are addressed in the DCD. Table 7.1-3 provides a roadmap for evaluation of each clause of IEEE Std 603-1991, where "plant licensing documentation" is referenced in TR MUAP-07004, with the corresponding DCD sections, which describe the plant specific information.

Table 7.1-3 will be added as follows.

Table 7.1-3 Road Map of US-APWR I&C System Conformance to IEEE Std. 603-1991

IEEE Std 603-1991 Criteria*		Plant Licensing Documentation (PLD) Referenced in MUAP-07004	Resolution of PLD in DCD
4	Safety System Designation	-	-
4.1	Design Basis Events	Plant safety analyses (not I&C specific)	Chapter 15
4.2	Safety Functions and Corresponding Protective Actions	Plant safety analyses (not I&C specific)	Chapter 15
4.3	Permissive Conditions for Each Operating Bypass Capability		
4.4	Variables Required to be Monitored for Protective Action	Specific reactor trip functions Specific protection system functions	Section 7.2, 7.3
4.5	The Minimum Criteria for Each Action Controlled by Manual Means		-
4.5.1	Allowed Time and Plant Condition	Credit for manual actions and associated HSI	Subsection 7.5.1.5
4.5.2	Justification of Permitting Initiation or Control Subsequent to Initiation	-	-
4.5.3	Control Room Habitability	-	-
4.5.4	Display of Variable	Credit for manual actions and associated HSI HSI for discretionary manual actions	Subsection 7.5.1.5, Section 7.5
4.6	Spatially Dependent Variables	Number, locations and processing method for spatially dependent variables	Section 7.2
4.7	Range of Conditions for Safety System Performance	-	-
4.8	Functional Degradation of Safety Functions	-	-
4.9	Reliability	-	-
4.10	The Critical Points in Time or the Plant Conditions	-	-
4.11	Equipment Protective Provisions	Equipment protective provisions	Section 8.3.1
4.12	Other Special Design Basis	-	-
5	Safety System Criteria	-	-
5.1	Single Failure Criterion	-	-
5.2	Completion of Protective Action	-	-
5.3	Quality	-	-
5.4	Equipment Qualification	-	-
5.5	System Integrity	-	-
5.6	Independence	-	-

5.6.1	Between Redundant Portions of a Safety System	-	-
5.6.2	Between Safety Systems and Effects of a Design Basis Event	-	-
5.6.3	Between Safety Systems and Other Systems	-	-
5.6.3.1	Interconnected Equipment	-	-
5.6.3.2	Equipment in Proximity	-	-
5.6.3.3	The Effects of a Single Random Failure	-	-
5.6.4	Detailed Independence Criteria	-	-
5.7	Capability for Test and Calibration	Test frequency for the plant process components	Subsection 7.1.3.14
5.8	Information Displays	-	-
5.8.1	Displays for Manually Controlled Actions	Credit for manual actions and associated HSI	Subsection 7.5.1.5
5.8.2	System Status Indication	-	-
5.8.3	Indication of Bypasses	-	-
5.8.4	Location of Displays	-	-
5.9	Control of Access	Security system for access control in the plant	Section 13.6
5.10	Repair	-	-
5.11	Identification	Color coding for labels and name tags	Subsection 7.1.3.19
5.12	Auxiliary Features	Description of auxiliary features (e.g. electrical power sources, building HVAC)	Subsection 7.1.1.10, Chapter 8; Chapter 9
5.13	Multi-Unit Stations	Sharing of this equipment between multiple units, as needed	Not Applicable for I&C
5.14	Human Factors	-	-
5.15	Reliability	Reliability analysis for specific plant applications	Chapter 19 MUAP-07030
5.16	Common Cause Failure (IEEE 603-1998)	-	-
6	Sense and Command Features - Functional and Design Requirements	-	-
6.1	Automatic Control	Credit for manual actions and associated HSI	Subsection 7.5.1.5
6.2	Manual Control	-	-
6.3	Interaction between the Sense and Command features and other Systems	-	-
6.4	Derivation of System Inputs	Direct process measurements and algorithms for calculated functions	Subsection 7.2.1
6.5	Capability for Testing and Calibration	-	-
6.6	Operating Bypasses	Automatically initiated operating bypasses	Subsection 7.1.3.11
6.7	Maintenance Bypass	-	-
6.8	Setpoint	-	-
6.8.1	Setpoint Uncertainties	-	-
6.8.2	Multiple Setpoints	Parameters with multiple setpoints that are automatically or manually disabled	Subsection 7.2.1.6.1, 7.2.1.6.2, 7.3.1.6.2, 7.2.1.6.3
7	Executive Features - Functional and Design Requirements	-	-

7.1	Automatic Control	-	-
7.2	Manual Control	Plant components with execute feature manual controls	Section 7.1, Table 7.1-1
7.3	Completion of Protective Action	-	-
7.4	Operating Bypass	-	-
7.5	Maintenance Bypass	-	-
8	Power Source Requirements	Electric power sources for this equipment	Subsection 7.1.1.10, Chapter 8

*The conformance to IEEE 603-1991 except for plant specific items is described in Appendix A of MUAP-07004.

Subsection 7.1.3.19 will be added as follows.

7.1.3.19 Identification

I&C equipments identification follows the guidance of RG 1.75, which endorses IEEE Std 384. The following color coding is provided on tags used for the identification of I&C system cabinets and for stand alone components, such as field instruments.

- Train A: Red with white lettering
- Train B: Green with white lettering
- Train C: Blue with white lettering
- Train D: Yellow with Black lettering
- Non-safety train: White with Black lettering

This color coding is consistent with the color coding defined in Subsection 8.3.1.1.8 identification of class 1E electrical equipment and cables.

For computer-based systems, the configuration management plan describes the identification process for software. To ensure that the required computer system hardware and software are installed in the appropriate system configuration, the system meets the following identification criteria specific to software systems:

- Firmware and software identification ensures that the correct software is installed in the correct hardware component.
- The software has a means to retrieve identification from the firmware by using software maintenance tools.
- Physical identification requirements of the digital computer system hardware are in accordance with the identification requirements in IEEE Std 603-1991.

The configuration identification management is addressed in Technical Report MUAP-07017.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 229-2022 REVISION 0
SRP SECTION: 07.01 – INSTRUMENTATION AND CONTROLS - INTRODUCTION
APPLICATION SECTION: 07.01
DATE OF RAI ISSUE: 2/26/2009

QUESTION NO.: 07.01-2

MHI is requested to provide a commitment to industry standards in the DC-FSAR similar to that provided in the topical reports.

10 CFR 50.55a(a)(1) and 10 CFR Part 50 Appendix A, General Design Criteria 1, require, in part, that structures, systems and components be designed, fabricated, erected, constructed, tested, and inspected to quality standards commensurate with the importance of the safety function to be performed. Chapter 7 of NUREG-0800, Standard Review Plan for Light-Water Reactors, identifies various regulatory guidance and industry standards for design of instrumentation and control systems (I&C). Chapter 7 of the US-APWR design certification final safety analysis report (DC-FSAR), does not reference or cite many industry standards or regulatory guides for the design or testing of I&C systems. Where applicable, an explicit commitment to industry standards is needed for the staff to arrive at a conclusion that the design and testing of the US-APWR I&C systems will be performed in a quality manner.

ANSWER:

MHI's I&C Topical Reports describes the applicable industry standards. MHI will add the references of TRs in DCD.

Impact on DCD

The second paragraph in Subsection 7.1.2 will be revised as follows.

Section 3 of each MHI Topical Report describes applicable code, regulatory, and industry standard compliance. The code, regulatory, and industry standards in the Section 3 of each Topical Report are also applicable to the US-APWR I&C design.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 229-2022 REVISION 0
SRP SECTION: 07.01 – INSTRUMENTATION AND CONTROLS - INTRODUCTION
APPLICATION SECTION: 07.01
DATE OF RAI ISSUE: 2/26/2009

QUESTION NO.: 07.01-3

MHI is requested to update Table 7.1 of the DC-FSAR to resolve inconsistencies, provide a list of regulations & guidance for each of the subsections in Chapter 7 and preferably use section numbers as column headings rather than systems.

DC-FSAR Table 7.1-2 provides a matrix of compliance based on system rather than by SRP section, as is done in SRP Chapter 7 of NUREG-0800, Standard Review Plan for Light-Water Reactors, Table 7.1. Inconsistencies in Table 7.1-2 coupled with the column headings not matching those in SRP Table 7.1 (Table 7.1-2 headings are by system) prevents a complete review of what regulatory criteria is applicable to the US-APWR. For example, Table 7.1-2 shows that §50.34(f)(2)(v) is applicable to the RPS, ESFAS, SLS, and Safety HSI, which are covered in Sections 7.2, 7.3, and 7.5. The column titled "Related Section in US-APWR DC-FSAR" in Table 7.1-2 indicates that this requirement is applicable to only Section 7.5. Additional examples; Table 7.1-2, Regulatory Requirements Applicability Matrix, does not identify GDC 1 or 50.55a(a)(1) as applicable to the PCMS and the DAS. 50.55a(a)(1) and this GDC are applicable to all SAR Sections of Chapter 7 as GDC 1 specifies "quality standards commensurate with the importance of the safety functions to be performed."

ANSWER:

Current Table 7.1-2 provides more clarity, because MHI systems do not map directly to single SRP sections. For example the safety logic system (SLS) in PSMS is applicable to 7.3, 7.4, 7.5, 7.6, and 7.9. The PCMS is applicable to 7.5, 7.7 and 7.9. If MHI change the columns to SRP sections the table will end up with an X in almost every box, due to this system overlap. Therefore, no update will be made for Table 7.1-2 from this RAI.

Impact on DCD

There is no impact on the DCD.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 229-2022 REVISION 0
SRP SECTION: 07.01 – INSTRUMENTATION AND CONTROLS - INTRODUCTION
APPLICATION SECTION: 07.01
DATE OF RAI ISSUE: 2/26/2009

QUESTION NO.: 07.01-4

MHI is requested to incorporate some of the details that are provided in the TRs in the appropriate DC-FSAR subsections or with references to specific TR sections for additional details in the DC-FSAR.

Example 1; DC-FSAR Sections 1.9 and 7.1.3 and Table 7.1-2 address compliance with regulatory requirements/guidance in keeping with Sections C.I.1.9.1—C.I.1.9.5 of RG 1.206 and Section 1.9 of the SRP. That is, conformance with these criteria is noted in the DC-FSAR in the following sections:

- Sections 1.9, Tier 1—RGs and BTPs;
- Section 3.1, Tier 2—GDCs;
- Section 7.5.2, Tier 2—TMI Action Plan Items, §50.34(f)(2))

From the list of requirements/guidance listed above, missing is an evaluation of compliance with §50.55a(h), and thus IEEE Std 603-1991.

Example 2; See RAI question 7.9-11 on determining if the guidelines of BTP 7-21 are met.

ANSWER:

See response to RAI 7.1-01 about the conformance to IEEE Std 603-1991. The conformance of BTP 7-21 is responded in RAI response 7.9-11.

Impact on DCD

There is no impact on the DCD.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No. 52-021

RAI NO.: NO. 229-2022 REVISION 0
SRP SECTION: 07.01 – INSTRUMENTATION AND CONTROLS - INTRODUCTION
APPLICATION SECTION: 07.01
DATE OF RAI ISSUE: 2/26/2009

QUESTION NO.: 07.01-5

MHI is requested to correct the DC-FSAR to match the TR or vice versa. If three levels of defense are correct, provide a discussion of this deviation from BTP 7-19 and ISG-02.

Section 7.1.3.1 indicates that the Diversity and Defense-in-Depth concept relies on the following four echelons of defense: control system, reactor trip system, ESFAS, and monitoring and indicators. TR MUAP-07006-P has the RPS/ESFAS combined into a single level of defense because of the reliance of the ESFAS on the RPS. Thus, the DC-FSAR shows three echelons of defense.

ANSWER:

There is no discrepancy between the DCD and TR "Defense in Depth and Diversity" (D3 TR), MUAP-07006 about the D3 concept. Both define four functional echelons (Reactor Trip System, Engineered Safety Features Actuation System, Control Systems, Monitoring and Indicators). Table 4.1-1 of the D3 TR shows the relationship between the functional echelons and the actual I&C hardware architecture. The design conforms to BTP 7-19 and ISG-02.

Impact on DCD

There is no impact on the DCD.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 229-2022 REVISION 0
SRP SECTION: 07.01 – INSTRUMENTATION AND CONTROLS - INTRODUCTION
APPLICATION SECTION: 07.01
DATE OF RAI ISSUE: 2/26/2009

QUESTION NO.: 07.01-6

The staff is requesting a complete clarification of the applicability of ALL documents that have been submitted for MELTAC and US-APWR. Particularly, 1) Which documents are applicable to the Basic software, the Application software, or both. 2) How the documents should be grouped with the topical reports and the design certification.

ANSWER:

Followings are relationship of the MHI I&C documents.

Table 07.01-6.1 MHI I&C Documents with Applicability to the Basic/Application Software

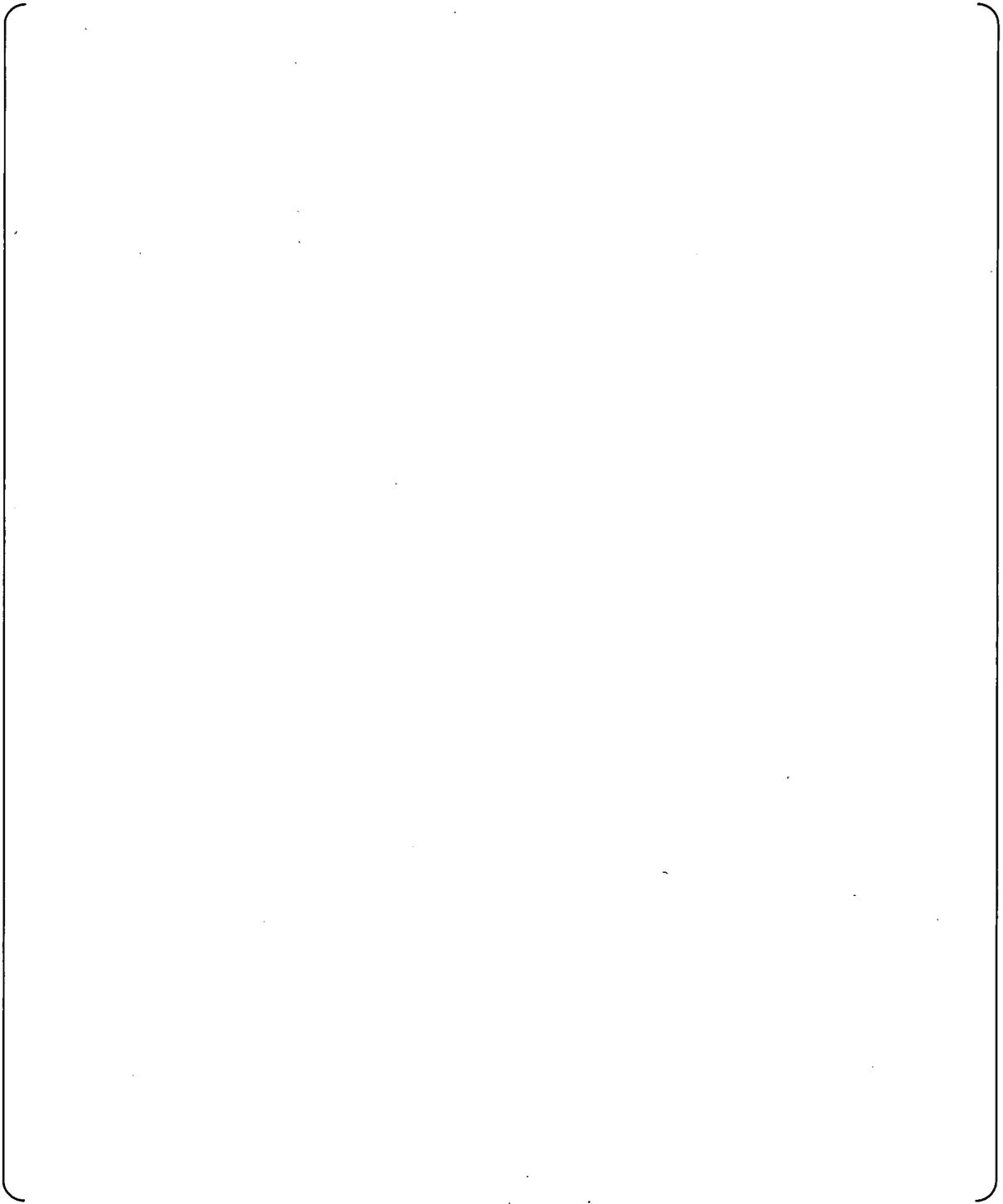




Table 07.01-6.2 MHI I&C Documents with Document Group of Topical Report and DCD

Impact on DCD

There is no impact on the DCD.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No. 52-021

RAI NO.: NO. 229-2022 REVISION 0
SRP SECTION: 07.01 – INSTRUMENTATION AND CONTROLS - INTRODUCTION
APPLICATION SECTION: 07.01
DATE OF RAI ISSUE: 2/26/2009

QUESTION NO.: 07.01-7

MHI is requested to discuss any anticipatory trips in the DC-FSAR including if any nonsafety grade equipment has been introduced into safety systems through the use of anticipatory trips.

Table 7.1-2 in the DC-FSAR cites conformance with SRP BTP 7-9, Guidance on Requirements for Reactor Protection System Anticipatory Trips. For the US-APWR, it is unknown if anticipatory functions were designed to the requirements of IEEE Std 6031991, and therefore introduced non-safety-grade equipment into the RPS. The concern is that the addition of anticipatory trips can degrade the RPS.

ANSWER:

DCD Subsection 7.2.1.4.8 already describes reactor trip (RT) on turbine trip (TT) as an anticipatory trip. RT on TT is common in most operating plants. Trip circuit is an associated circuit. Since the signals can only cause a reactor trip, not prevent a trip there can be no degradation to the RPS. The RT on TT conforms to BTP 7-9.

Impact on DCD

Following sentences will be added after the first paragraph in Subsection 7.2.1.4.8.

The high reliable design meets the guidance of BTP 7-9. The RPS and RTB which meet Class 1E criteria with Seismic Category I are applied as the signal processor and final actuation devices for RT on TT. The sensors for RT on TT also meet the requirements of IEEE Std 603-1991. The sensors are located in non-seismic areas (Turbine Building). The installation (including circuit routing) and design of the sensors is such that the effects of credible faults (i.e., grounding, shorting, application of high voltage, or electromagnetic interference) or failures in these areas could not be propagated back to the reactor protection system and degrade the reactor protection system performance or reliability. Thus the sensors in non-seismic areas are qualified to operate in a seismic event. (i.e., not fail to initiate a trip for conditions which would require a trip.)

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 229-2022 REVISION 0
SRP SECTION: 07.01 – INSTRUMENTATION AND CONTROLS - INTRODUCTION
APPLICATION SECTION: 07.01
DATE OF RAI ISSUE: 2/26/2009

QUESTION NO.: 07.01-8

MHI is requested to address conformance with IEEE Std 308-1980 for the systems required to achieve and maintain safe shutdown.

Table 7.1-2 cites conformance with RG 1.75. DC-FSAR Subsection 7.2.1.2 indicates that the isolation between train A and B and between train C and D of the RPS is based on IEEE Std 384-1992 including minimum distance and barriers. DC-FSAR Subsection 7.9.2.7 indicates that all PSMS DCS cables, with the exception of its maintenance networks, are routed in accordance with IEEE Std 384-1992 to ensure physical independence of each division. The DC-FSAR does not address conformance anywhere with IEEE Std 308-1980, "IEEE Std for Class 1E Power Systems".

ANSWER:

The Class 1E ac/dc power system is designed as safety-related equipment, fully conformed to the requirements of IEEE Std 308 with an exception that pertains to sharing of power systems at multi-unit nuclear power plants since the US-APWR is a single unit plant. MHI will add the conformance with IEEE Std 308-1980.

Impact on DCD

The third paragraph of Subsection 7.1.1.10 will be revised as follows:

The PSMS is powered from two Class 1E Power Sources. These sources are uninterruptible power supplies (UPSs) backed-up by Class 1E station batteries and by the Class 1E gas turbine generators (GTGs). Power sources for the PSMS are shown in Figures 7.1-4 and 7.1-5. A description of the power distribution to PSMS equipment is described in Subsection 8.3.1. The Class 1E ac/dc power system is designed as safety-related equipment, fully conformed to the requirements of IEEE Std 308-2001 with an exception that pertains to sharing of power systems at multi-unit nuclear power plants since the US-APWR is a single unit plant. More detail descriptions for this conformance are described in Section 8.3.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 229-2022 REVISION 0
SRP SECTION: 07.01 – INSTRUMENTATION AND CONTROLS - INTRODUCTION
APPLICATION SECTION: 07.01
DATE OF RAI ISSUE: 2/26/2009

QUESTION NO.: 07.01-9

MHI is requested to address isolation from a design basis events in Section 7.1.3.5, Isolation. Further elaborate the independence of, and physical separation from, the effects of design basis events of safety systems and those used to achieve and maintain safe shutdown conditions.

Per 5.6.2 of IEEE Std. 603-1991: "Safety system equipment required to mitigate the consequences of a specific design basis event shall be independent of, and physically separated from, the effects of the design basis event."

ANSWER:

The PSMS digital components are located in a mild environment that is not impacted by any design basis event. Fire or HVAC failures are isolated to a single division. PSMS instrumentation is qualified for the design basis event environment. This is addressed in Subsection 7.1.3.7. MHI will add the reference.

Impact on DCD

Following sentence will be added after the third paragraph in Subsection 7.1.3.5. The revision also includes the RAI response to 07.01-10.

The electrical, physical and functional isolation is also discussed in Subsection 7.1.3.4. The isolation from a design basis event of safety system based on the equipment qualification is discussed in Subsection 7.1.3.7. The PSMS digital components are located in a mild environment that is not impacted by any design basis event.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 229-2022 REVISION 0
SRP SECTION: 07.01 – INSTRUMENTATION AND CONTROLS - INTRODUCTION
APPLICATION SECTION: 07.01
DATE OF RAI ISSUE: 2/26/2009

QUESTION NO.: 07.01-10

MHI is requested to address in Section 7.1.3.5, Isolation, those conditions that have the potential for functional degradation of safe shutdown system performance. This section does not document those provisions incorporated to retain the capability for performing the safety function.

The safety system design shall be such that credible failures in and consequential actions by other systems shall not prevent the safety systems from meeting the requirements of IEEE Std 603-1991. That is, IEEE Std 603-1991, Criterion 4.8, requires that the design basis shall document the conditions having the potential for functional degradation of safety system performance and for which provisions shall be incorporated to retain the capability for performing the safety functions (for example, missiles, pipe breaks, fires, loss of ventilation, spurious operation of fire suppression systems, operator error, failure in non-safety-related systems).

ANSWER:

Each train of the PSMS is independent from each other such that the function of one train is not degraded by failures outside of its train. Electrical, physical and functional independence are provided. This is addressed in Subsection 7.1.3.4. MHI will add the reference.

The impact on DCD from this RAI response is added within the RAI response to 07.01-09.

Impact on DCD

There is no impact on the DCD.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No. 52-021

RAI NO.: NO. 229-2022 REVISION 0
SRP SECTION: 07.01 – INSTRUMENTATION AND CONTROLS - INTRODUCTION
APPLICATION SECTION: 07.01
DATE OF RAI ISSUE: 2/26/2009

QUESTION NO.: 07.01-11

MHI is requested to address in Section 7.1.3.4, Independence, conformance with Clause 6.3 of SRP Appendix 7.1-C and IEEE 603-1991 for those systems used to achieve and maintain safe shutdown.

Clause 6.3 of SRP Appendix 7.1-C and IEEE 603-1991 address the interaction between the sense and command features and other systems. The objective of this review is to ensure that non-safety system interactions with safety systems are limited such that the requirements of 10 CFR 50 Appendix A, GDC 24 are met. The event of concern is simple failure of a sensing channel shared between control and protection functions. Provisions shall be included so that these requirements can be met in conjunction with the requirements of a safety system still being able to accomplish its safety function while sense and command features equipment is in maintenance bypass. During such operation, the sense and command features shall continue to meet the requirements of the single failure criteria and one of the two sense and command requirements listed above. These provisions include reducing the required coincidence, defeating the non-safety system signals taken from the redundant channels, or initiating a protective action from the bypassed channel.

ANSWER:

Conformance to Clause 6.3 of IEEE 603-1991, interaction between the sense and command features and other systems, for sensors shared between the PSMS and PCMS are addressed in Subsection 7.1.3.16. MHI will add the reference.

Impact on DCD

Following sentence will be added after the fifth paragraph in Subsection 7.1.3.4.

The independence between the PSMS and PCMS for shared sensors is discussed in Subsection 7.1.3.16.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 229-2022 REVISION 0
SRP SECTION: 07.01 – INSTRUMENTATION AND CONTROLS - INTRODUCTION
APPLICATION SECTION: 07.01
DATE OF RAI ISSUE: 2/26/2009

QUESTION NO.: 07.01-12

MHI is requested to identify in the Section 7.3.3.9 of the DC-FSAR:

- a) The 2 sources of AC power. Topical Report, MUAP-07005-P(R2), Section 4.1.2.10, Power Supply Configuration, states the source of AC power is described in system application documentation.
- b) The maintenance bypass of power sources and the reliability of electric power for the systems required to achieve and maintain safe shutdown. Section 4.1.2.10 of Topical Report, MUAP-07005-P(R2) says the "DC power from both sources is diode auctioneered, then distributed to each component in the cabinet." Include in the DCFSAR if a capacitor is used during switchover from one source to another or if the supplies are simply run in parallel.

IEEE 603-1991, Clause 8.3 requires that the capability of the safety systems to accomplish their safety functions shall be retained while power sources are in maintenance bypass. Portions of the power sources with a degree of redundancy of one shall be designed such that when a portion is placed in maintenance bypass (that is, reducing temporarily its degree of redundancy to zero), the remaining portions provide acceptable reliability.

ANSWER:

- a) The power supply configuration of the US-APWR I&C system is described in Subsection 7.1.1.10 and Figures 7.1-4 to 7.1-7.
- b) Each PSMS division is powered from two different ac vital buses as shown in Subsection 7.1.1.10 and Figures 7.1-4 and 7.1-5 of the DCD. The technical specifications control bypass of the power source (inverter), and bypass of the four (4) ac vital buses in operating modes. An LCO is defined for any condition that results in the PSMS operability to be reduced beyond the required number of operable divisions. Diode auctioneering is a parallel configuration, no capacitors.

Impact on DCD

There is no impact on the DCD.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 229-2022 REVISION 0
SRP SECTION: 07.01 – INSTRUMENTATION AND CONTROLS - INTRODUCTION
APPLICATION SECTION: 07.01
DATE OF RAI ISSUE: 2/26/2009

QUESTION NO.: 07.01-13

MHI is requested to identify in the DC-FSAR any exceptions to testing and calibration during power operation for the systems required to achieve and maintain safe shutdown.

Section 7.1.3.14, System Calibration, Testing and Surveillance, states "Most remaining manual tests may be performed with the plant at full power." Per IEEE Std. 603, Criterion 5.7, "Exceptions to testing and calibration during power operation are allowed where this capability cannot be provided without adversely affecting the safety or operability of the generating station. In this case:

1. appropriate justification shall be provided (for example, demonstration that no practical design exists),
 2. acceptable reliability of equipment operation shall be otherwise demonstrated, and the capability shall be provided while the generating station is shut down."
-

ANSWER:

There are no exceptions for testing at power in the PSMS. All limitations are based on plant mechanical components (e.g., main steam isolation valves).

Impact on DCD

The first paragraph of Subsection 7.1.3.14 will be revised as follows:

Testing from the sensor inputs of the PSMS through to the actuated equipment and HSI is accomplished in a series of overlapping sequential tests and calibrations. The majority of the tests are conducted automatically, through self-diagnostics. Most remaining manual tests may be performed with the plant at full power. There are no exceptions for testing at power in PSMS.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 229-2022 REVISION 0
SRP SECTION: 07.01 – INSTRUMENTATION AND CONTROLS - INTRODUCTION
APPLICATION SECTION: 07.01
DATE OF RAI ISSUE: 2/26/2009

QUESTION NO.: 07.01-14

MHI is requested to add conformance to the requirements of IEEE 338-1987 is met. Section 7.1.3.14, System Calibration, Testing and Surveillance, does not discuss conformance to IEEE 338-1987 whereas sections 7.2.3.3 and 7.3.3.3 state "the requirements of IEEE 338-1987 are met as discussed in Subsection 7.1.3.14." MHI is also requested to discuss, in the DC-FSAR, the test procedure for meeting IEEE 3381987 Subsection 6.4 as it relates to safety systems including the safe shutdown systems. Section 7.1.3.14 should also include the development of the test procedures that will be written and the guidance used to write those procedures for the systems used to achieve and maintain safe shutdown

Subsection 6.4 of IEEE 338-1987, requires that a "specific test procedure meeting the requirements of this standard and utilizing the applicable methods set forth in this section shall be developed for each system." Also, Subsection 6.6 of IEEE 338-1987, requires that "Testing shall be performed to written approved test procedures. The test procedures shall be developed in accordance with Section 5.3 of ANSI/ANS 3.2-1982, or the equivalent."

ANSWER:

Subsection 7.1.3.14 and the Safety I&C TR, MUAP-07004, clearly describe periodic testing. The conformance to IEEE Std 338 is described in the Safety I&C TR. MHI will add the description.

Impact on DCD

The fifth paragraph in Subsection 7.1.3.14 will be revised as follows.

The PSMS meets the periodic testing requirements of IEEE Std 338-1987 which is endorsed by RG 1.22. The test intervals are specified in the technical specifications, Chapter 16. All periodic testing is conducted to written procedures. For more detailed discussion on this topic, refer to Topical Report MUAP-07004 Sections 4.3 through 4.5, Appendix A.5.7, A.5.9, A.5.10, A.6.5 through A.6.7, and A.7.5.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 229-2022 REVISION 0
SRP SECTION: 07.01 – INSTRUMENTATION AND CONTROLS - INTRODUCTION
APPLICATION SECTION: 07.01
DATE OF RAI ISSUE: 2/26/2009

QUESTION NO.: 07.01-15

MHI is requested to identify in Subsection 7.1.3.10, the types of manual testing and manual calibration verification for functions with self-diagnostics of the systems used to achieve and maintain safe shutdown. Also discuss in the broader sense the implication from Sections 7.1.3.10 and 7.1.3.11 that manual testing and manual calibration verification are not provided for functions with self-diagnostics.

Per BTP 7-17, digital computer-based I&C systems should include self-test features to confirm computer system operation on system initialization. DC-FSAR Subsection 7.1.3.10 states that "The integrity of digital I&C components is continuously checked by their self-diagnosis features. These self-diagnostic features result in early detection of failures, and allow on-line repair that improves system availability. Information about detected failures is gathered through networks and provided to maintenance staff in a comprehensive manner. In addition, the self-diagnostic features control redundant controller configuration, to maintain all system functions, even in the presence of failures. Continuous self-diagnostic features allow elimination of most of the manual surveillance testing required for technical specification conformance. Manual testing and manual calibration verification are only provided for functions with no self-diagnostics." DC-FSAR Subsection 7.1.3.11 states that "Manual test features are provided to allow periodic testing of all functions that are not automatically tested through self-diagnostics."

ANSWER:

Safe shutdown functions will be tested just like any other function. All testing is discussed in detail in the Platform TR, MUAP-07005 and the Safety I&C TR, MUAP-07004. Coverage of self-diagnosis and manual test is described in the Safety I&C TR sections 4.3 and 4.4. MHI will add the references. DCD Subsections 7.1.3.10 and 7.1.3.11 will be clarified regarding the manual confirmation of self-diagnostics.

Impact on DCD

Subsection 7.1.3.10 will be revised as follows. The revision also includes the RAI responses to RAI 07.01-16, RAI 07.01-17 and RAI 07.01-18.

7.1.3.10 Self-Diagnosis Function

The integrity of digital I&C components is continuously checked by their self-diagnosis features. These self-diagnostic features result in early detection of failures, and allow on-line repair that

improves system availability. Information about detected failures is gathered through networks and provided to maintenance staff in a comprehensive manner. In addition, the self-diagnostic features control redundant controller configuration, to maintain all system functions, even in the presence of failures. The self-diagnosis is always working in the digital control system but does not affect system operation.

Continuous self-diagnostic features allow elimination of most of the manual surveillance testing required for technical specification compliance. Manual testing and manual calibration verification are ~~only~~ specifically provided for functions with no self-diagnostics. The integrity of the self-diagnosis is confirmed by a periodic manually initiated software memory check, which includes the software memory which is used for self-diagnosis. 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 Topical Report MUAP-07004 Sections 4.3 and 4.4. Topical Report MUAP-07005 Section 4.1.5.1 describes self-diagnosis. The self-testing is provided for MELTAC components of PSMS, with the exception of the conventional circuits within the I/O and PIF modules, and the touch screens of the safety VDU.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 229-2022 REVISION 0
SRP SECTION: 07.01 – INSTRUMENTATION AND CONTROLS - INTRODUCTION
APPLICATION SECTION: 07.01
DATE OF RAI ISSUE: 2/26/2009

QUESTION NO.: 07.01-16

MHI is requested to identify in the DC-FSAR the MELTAC components containing self checking software, or hardware, by identification of those components at the circuit board or modular level. Section 7.1.3.10, Self-Diagnosis Function, states "The integrity of digital I&C components is continuously checked by their self-diagnosis features."

However, as BTP 7-17 states "Some small, stand-alone, embedded digital computers may not need self-testing." MHI is requested to identify digital, software based, stand alone components categorized, or briefly discussed, in other chapters of the DC-FSAR, and if they need self-testing or not. This may include electrical components such as breakers, or radiation monitoring equipment including processors or sensors.

ANSWER:

The Platform TR, MUAP-07005 Sections 4.1.5 and 4.2.3 describe self-diagnosis. Self-testing is provided for all MELTAC components of the PSMS, with the exception of the conventional circuits within the I/O and PIF modules, and the touch screens of the safety VDU. These components are manually tested as described in the Safety I&C TR, MUAP-07004 Section 4.4.1 Manual Testing. MHI will add the references.

The impact on DCD from this RAI response is added within the RAI response to 07.01-15.

Impact on DCD

There is no impact on the DCD.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 229-2022 REVISION 0
SRP SECTION: 07.01 – INSTRUMENTATION AND CONTROLS - INTRODUCTION
APPLICATION SECTION: 07.01
DATE OF RAI ISSUE: 2/26/2009

QUESTION NO.: 07.01-17

MHI is requested to address in Section 7.1.3.10, self tests and diagnostics occurring in more than one division simultaneously; how this affects operation and how this situation is presented to the operator.

In Section 7.1.3.10, Self-Diagnosis Function, discusses the automatic self-test features and its ability to maintain channel independence, system integrity, and meet the single-failure criterion during testing for the systems required to achieve and maintain safe shutdown.

ANSWER:

Self-diagnosis is always working but does not affect system operation. Operators are notified of errors detected by the self-diagnostics through a system level group alarm on the Large Display Panel (LDP). The specific error is presented on the MELTAC Engineering Tool which is located in each I&C room and plant maintenance facilities near MCR. The self-diagnosis is described in TRs MUAP-07004 Section 4.3 PSMS Self-diagnostics Features and MUAP-07005 Sections 4.1.5 and 4.2.3. MHI will add the explanation.

The impact on DCD from this RAI response is added within the RAI response to 07.01-15.

Impact on DCD

There is no impact on the DCD.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 229-2022 REVISION 0
SRP SECTION: 07.01 – INSTRUMENTATION AND CONTROLS - INTRODUCTION
APPLICATION SECTION: 07.01
DATE OF RAI ISSUE: 2/26/2009

QUESTION NO.: 07.01-18

MHI is requested to address in Section 7.1.3.10 the periodic functional or surveillance tests that are used to verify the self-test functions for the systems required to achieve and maintain safe shutdown. Section 7.1.3.10 does state that "Manual testing and manual calibration verification are only provided for functions with no self-diagnostics." Per BTP 7-17, self-test functions should be verified during periodic functional tests.

ANSWER:

Software memory, including the memory used for self-diagnosis is periodically checked by the Software Memory Integrity test which is described in the Safety I&C TR, MUAP-07004 Section 4.4.1 and Platform TR, MUAP-07005 Section 4.1.4.1(c). This Software Memory Integrity test is manually initiated and monitored. Also when input/output (I/O) is manually checked by 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. MHI will add the explanation.

The impact on DCD from this RAI response is added within the RAI response to 07.01-15.

Impact on DCD

There is no impact on the DCD.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 229-2022 REVISION 0
SRP SECTION: 07.01 – INSTRUMENTATION AND CONTROLS - INTRODUCTION
APPLICATION SECTION: 07.01
DATE OF RAI ISSUE: 2/26/2009

QUESTION NO.: 07.01-19

MHI is requested to address BTP 7-17 in Section 7.1.3.11, Manual Testing, Bypasses, Overrides and Resets, with regards to compensatory actions and operator notification of detected failures.

BTP 7-17 discusses the design having either the automatic or manual capability to take compensatory action on detection of any failed or inoperable component; plant procedures specifying manual compensatory actions and mechanisms for recovery from automatic compensatory actions; and mechanisms for operator notification of detected failures complying with the system status indication provisions of IEEE Std 603-1991 and being consistent with, and support, plant technical specifications, operating procedures, and maintenance procedures.

ANSWER:

When failures occur in one safety division, the other division(s) is/are credited for the safety function. There are no credited compensatory actions in the failed division, for repair or alternate success paths. Failures that are detected are alarmed on the LDP. For failures detected through process inputs (e.g., sensor deviations) alarms are diagnosed through PCMS displays. For failures detected through self-diagnostics, the MELTAC Engineering Tool provides the details of the error condition. Operators respond to failure alarms and diagnostic displays by initiating appropriate maintenance actions and entering Technical Specification Actions, where failures result in the inoperability of required safety functions. Division level displays are provided on the LDP to continuously indicate a bypassed or inoperable safety function. These displays are automatically initiated for failures that are automatically detected. The displays can be manually initiated for failures that are not automatically detected. The PCMS provides more detailed displays that allow drill down for component level bypassed or inoperable conditions.

Impact on DCD

There is no impact on the DCD.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 229-2022 REVISION 0
SRP SECTION: 07.01 – INSTRUMENTATION AND CONTROLS - INTRODUCTION
APPLICATION SECTION: 07.01
DATE OF RAI ISSUE: 2/26/2009

QUESTION NO.: 07.01-20

MHI is requested to address in the DC-FSAR Section 7.1.3.14, System Calibration, Testing and Surveillance discuss any conditions that may arise when only two channels of readout are provided, what operator action will be, and the basis used to ensure that an operator will not take incorrect action when the two channel readouts differ for the systems required to achieve and maintain safe shutdown.

Per IEEE 338, consideration shall be given to common mode failures when selecting channels for comparison.

ANSWER:

The situation of needing validation with only two parameters is not unique to the US-APWR. All operating plants have parameters with only two channels. Operators are trained to check related process parameters. This same training will apply to operators for the US-APWR. For the US-APWR, operators may also check the diverse HSI panel (DHP) for third indication, when there is an available parameter on the DHP.

This situation is not related to System Calibration, Testing and Surveillance so MHI does not believe this should be addressed in Subsection 7.1.3.14. Continuous automatic cross channel comparison is described in the Safety I&C TR, MUAP-07004 Section 4.3 PSMS Self-diagnostics Features.

Impact on DCD

There is no impact on the DCD.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No. 52-021

RAI NO.: NO. 229-2022 REVISION 0
SRP SECTION: 07.01 – INSTRUMENTATION AND CONTROLS - INTRODUCTION
APPLICATION SECTION: 07.01
DATE OF RAI ISSUE: 2/26/2009

QUESTION NO.: 07.01-21

MHI is requested to address in Table 7.1-2 conformance with RG 1.204 with respect to I&C systems

Table 1.9.1-1 cites compliance with RG 1.204 with no exceptions identified. Conformance is addressed in Section 8.1.5.3. However, lightning strikes can have a big impact on I&C.

ANSWER:

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

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

Therefore, MHI will add the detail reference for conformance to RG 1.204 in Table 7.1-2.

Impact on DCD

Item v. in Table 7.1-2 (Sheet 5 of 8) will be revised as Attachment 1.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No. 52-021

RAI NO.: NO. 229-2022 REVISION 0
SRP SECTION: 07.01 – INSTRUMENTATION AND CONTROLS - INTRODUCTION
APPLICATION SECTION: 07.01
DATE OF RAI ISSUE: 2/26/2009

QUESTION NO.: 07.01-22

MHI is requested to address in Section 7.1.3.11, Manual Testing, Bypasses, Overrides and Resets, the following issues:

- 1) The reliability of the digital I&C equipment is significantly higher than the reliability of the plant components. Or provide a reference to where this is demonstrated.
- 2) What is meant by "periodic test frequency";
- 3) What type of testing this applies to; surveillances, calibrations etc.
- 4) The guidelines of IEEE 7-4.3.2 with regards to the reliability requirements identifying the need for self diagnostics.

Section 7.1.3.11, Manual Testing, Bypasses, Overrides and Resets, states "Since the reliability of the digital I&C equipment is significantly higher than the reliability of the plant components, the periodic test frequency is determined by the reliability of the plant components, not the reliability of the digital I&C equipment."

Per IEEE 7-4.3.2, "The reliability requirements of the safety system shall be used to establish the need for self-diagnostics. Self diagnostics are not required for systems in which failures can be detected by alternate means in a timely manner." This standard goes on to state "If reliability requirements warrant self-diagnostics, then computer programs shall incorporate functions to detect and report computer system faults and failures in a timely manner."

ANSWER:

1) The surveillance frequency of digital I&C equipment is provided in DCD Chapter 16 Section 3.3 and is consistent with the reliability data in the PRA. The surveillance of PSMS output modules is conducted with plant components (e.g., pump or valve). Since the PSMS uses solid-state output modules, these modules have higher reliability than the plant components they control. Therefore, the surveillance frequency is determined by the reliability of the plant component. Comparison of the reliability of the output module and plant component is shown below. This comparison is based on actual operating experience as NUREG reliability data used in PRA is based on operating experience.



2) "Periodic test frequency" means surveillance frequency.

3) The actuation test of output module and plant component is applied with simultaneously conducted surveillance tests.

4) Self-diagnostics are provided primarily to (1) reduce the potential for spurious plant transients due to errors in manual testing and (2) to reduce the labor burden associated with manual testing. Therefore, MHI has not determined if the reliability of the PSMS without self-diagnostics would warrant self-diagnostics. Similarly, MHI has not determined if failures that are detected by self-diagnostics can be manually detected in a timely manner. IEEE 7-4.3.2 would require these evaluations only if self-diagnostics were not included in the PSMS.

Impact on DCD

There is no impact on the DCD.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 229-2022 REVISION 0
SRP SECTION: 07.01 – INSTRUMENTATION AND CONTROLS - INTRODUCTION
APPLICATION SECTION: 07.01
DATE OF RAI ISSUE: 2/26/2009

QUESTION NO.: 07.01-23

MHI is requested to provide information in the DC-FSAR that will enable the staff to determine how functional systems are separated within the processing electronics and the connections between them.

One possible presentation of this information is to identify the cabinet separations or cabinet designations on the functional logic diagrams. The staff's concern is the independence and separation of each safety function as identified in IEEE Std 603 criterion 5.6.1.

ANSWER:

IEEE Std 603-1991 criterion 5.6.1 requires independence between redundant divisions which provide the same safety function, not between different safety functions in the same division. Isolation and independence between divisions is clearly described in Subsections 7.1.3.4 and 7.1.3.5.

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.

**Responses to Request for Additional Information No.226-2018
Revision 0**

**SRP Section 7.2
Reactor Trip System**

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No. 52-021

RAI NO.: NO. 226-2018 REVISION 0
SRP SECTION: 07.02 – REACTOR TRIP SYSTEM
APPLICATION SECTION: 07.02
DATE OF RAI ISSUE: 2/26/2009

QUESTION NO.: 07.02-1

DCD Sect. 7.2.3.1 cites compliance with IEEE Std 379-2000 for its methodology for performing a failure modes and effects analysis (FMEA). Based on IEEE Std 603-1991 and Std 7-4.3.2-2003, IEEE Std 352 is the standard that provides the guidance for performing a FMEA. Conformance with the requirements of IEEE Std 379-2000, provides methods acceptable to the NRC staff for satisfying the NRC's regulations with respect to the application of the single-failure criterion. IEEE Std 352 states that a FMEA "is conducted to determine the effects of each component failure mode on the overall system performance. In this process, the component failure modes that could contribute to unsafe system failure are identified, and necessary action can be taken at this point in the procedure." Address the applicability of IEEE Std 352 in performing a FMEA analysis for the APWR I&C systems.

ANSWER:

The FMEA of the I&C system also follows the guidance of IEEE Std 352-1987, "IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Safety Systems". MHI will add the reference of IEEE Std 352-1987.

Impact on DCD

The first paragraph in Subsection 7.2.3.1 will be revised as follows.

The methodology for the FMEA is provided in the Topical Report MUAP-07004 Section 6.5.1. The FMEA follows the guidance of IEEE Std 352-1987 which is referred from IEEE Std 603-1991 and IEEE Std 7-4.3.2-2003, and IEEE Std 379-2000 (Reference 7.2-8), which is endorsed by RG 1.53 (Reference 7.2-9).

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 226-2018 REVISION 0
SRP SECTION: 07.02 – REACTOR TRIP SYSTEM
APPLICATION SECTION: 07.02
DATE OF RAI ISSUE: 2/26/2009

QUESTION NO.: 07.02-2

MHI is requested to provide additional information to be docketed with regards to the application of the MELTAC platform for the US-APWR. NUREG-0800, Standard Review Plan, Branch Technical Position 7-14.

"Guidance on Software Reviews for Digital Computer-based Instrumentation and Control Systems." (BTP-14) identifies guidelines for evaluating software life-cycle processes for digital computer-based instrumentation and control (I&C) systems. Table 1.9.2-7, of the DC-FSAR, "US-APWR Conformance with Standard Review Plan Chapter 7 Instrumentation and Controls" identifies conformance to BTP-14 with no exceptions. The staff requests MHI to address the guidelines of BTP-14, Section B.2.1, Software Life Cycle Process Planning and specific plans for the application software. Section 6.3 provides a high level summary of the plans for the application software. MUAP-07017, "US-APWR Technical Report; Software Program Manual" provides further detail of individual plans for the application software for the US-APWR. MHI is requested to docket the plant specific project plans, as part of the US-APWR design certification, so that a review can be done to ensure compliance with the SPM and 10 CFR. If the above information is not available, MHI should expand ITAAC beyond the single ITAAC on the life cycle process for the Class IE safety systems, Design Commitment No. 24 of Table 2.5.1-5. The additional ITAACs would be identified as Design Acceptance Criteria (DAC) and would typically specify the applicable portions of the High Quality Design Process delineated in Section C of Appendix A to RG 1.206, "Combined License Applications For Nuclear Power Plants (LWR Edition)."

MHI is requested to identify at the document level as a minimum, or section of information, what is applicable to the basic software, application software or both.

ANSWER:

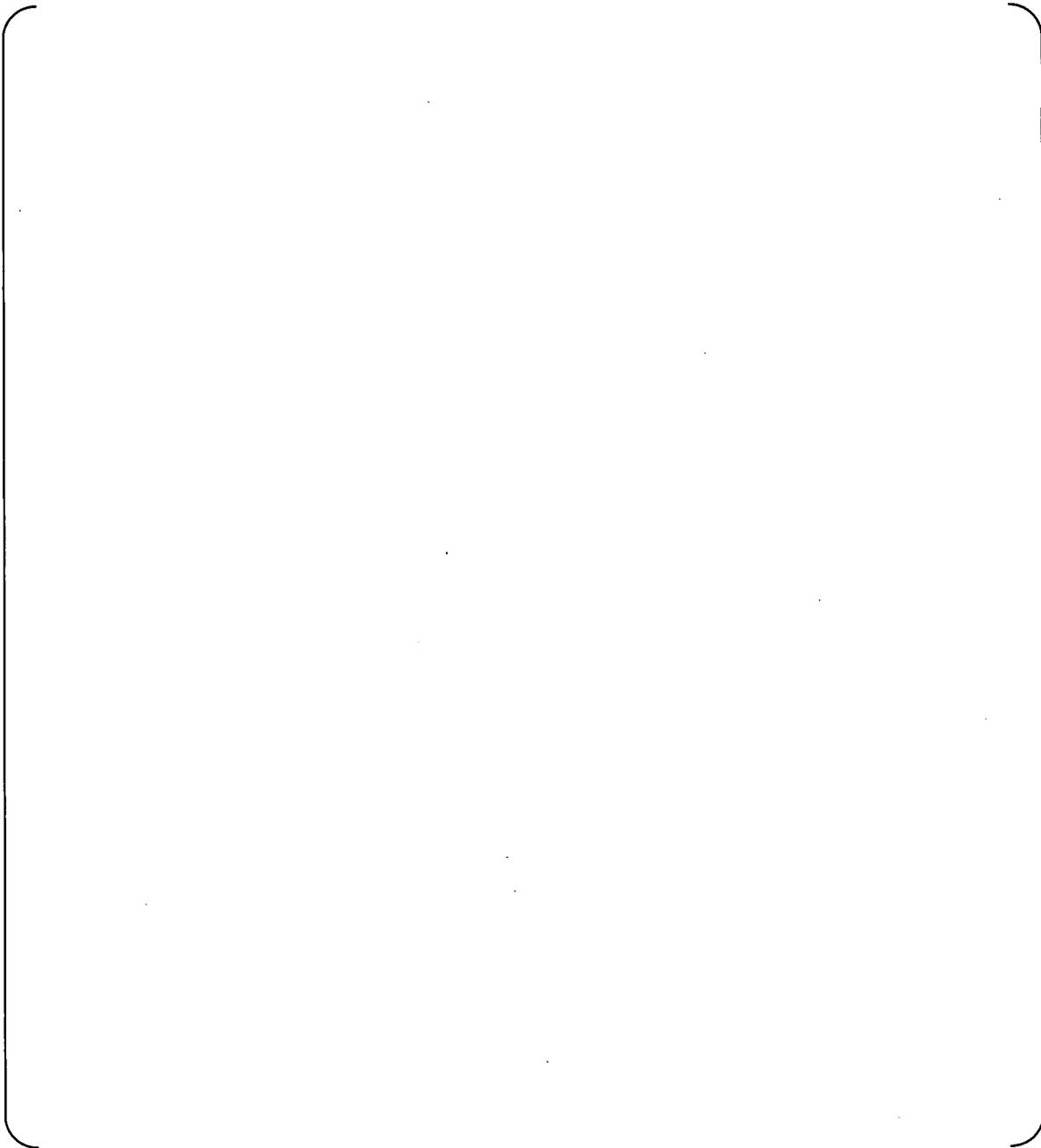
For the MELTAC platform Basic Software, compliance to BTP 7-14 is addressed by the design process and documentation described in the MELTAC Platform TR, MUAP-07005 Section 6 Life Cycle. Additional documentation has been submitted and audited in response to RAIs relating to that topical report.

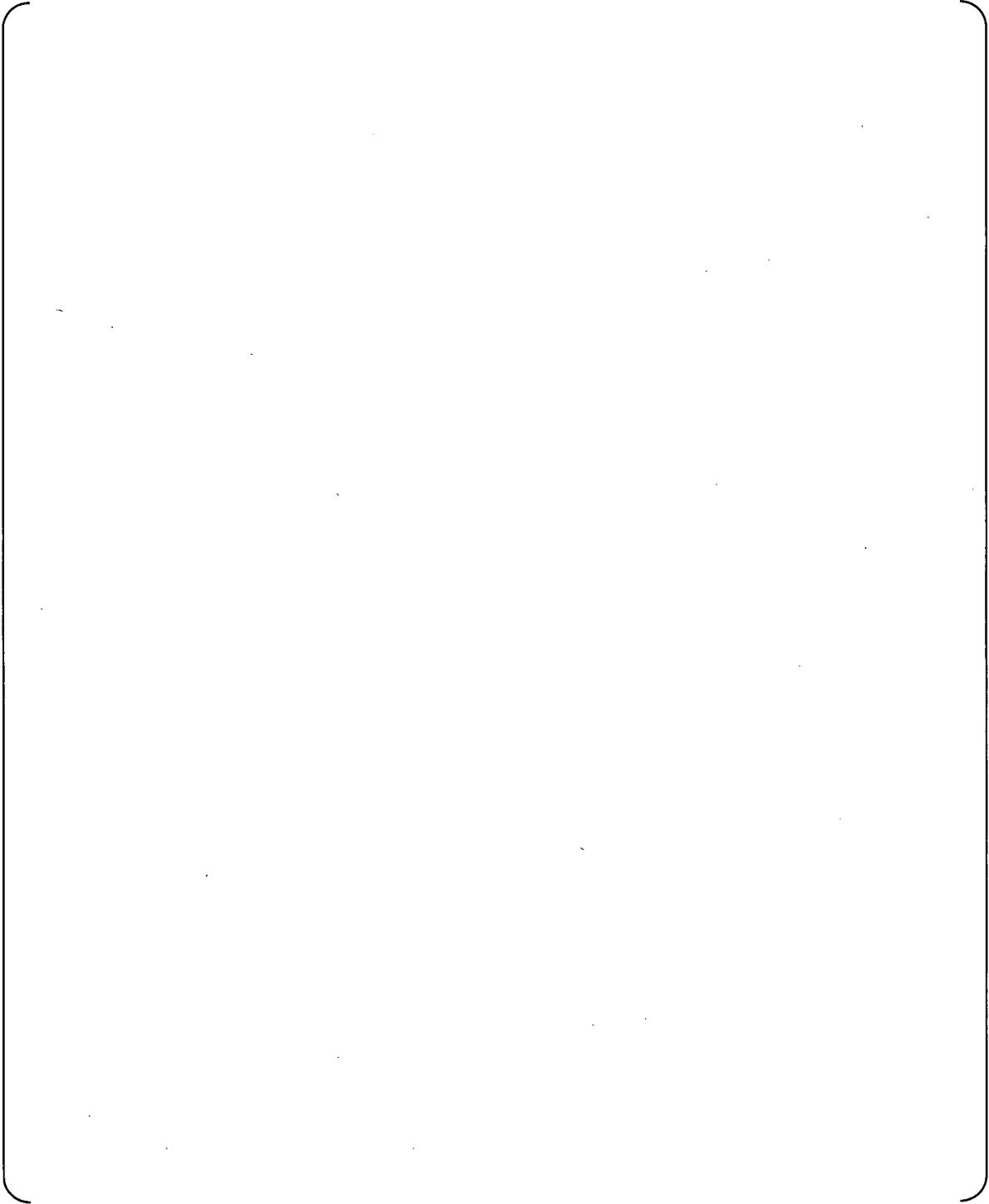
For PSMS Application Software, Software Program Manual (SPM), MUAP-07017 describes the individual life cycle plans that apply to all US-APWR plants. All design and associated V&V activities are generically applicable to all plants, and will therefore be conducted one time. Every plant will have its own factory acceptance testing and site installation testing, but most of this will be generic and therefore covered by the generic SPM plan and generic procedures. Therefore,

MHI does not intend to generate project specific plans for each section of the SPM, since the entire SPM is generically applicable to all US-APWR projects. As stated in Section 1.2, where the SPM requires additional project specific information, that additional information will be included in the US-APWR Project Plan.

The generic US-APWR PSMS design schedule of the Project Plan is provided in this RAI response. The design schedule of Project Plan for the generic US-APWR PSMS are shown as the following table. This schedule encompasses all activities that are generically applicable to all US-APWR plants.

Table 07.02-2 US-APWR Standard Electrical and I&C System Basic Design Schedule





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.

Responses to Request for Additional Information No.230-2028
Revision 0

SRP Section 7.3
Engineered Safety Features Systems

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 230-2028 REVISION 0
SRP SECTION: 07.03 – ENGINEERED SAFETY FEATURES SYSTEMS
APPLICATION SECTION: 07.03
DATE OF RAI ISSUE: 2/26/2009

QUESTION NO.: 07.03-1

MHI is requested to address GDCs 10, 15 and 16 in Chapter 7 of the DC-FSAR with regards to the ESF system. The DC-FSAR does not address compliance with GDCs 10, 15 and 16 in Section 7.3 or Table 7.1-2, and refers to Chapters 4, 5, and 6, respectively. These GDCs ensure that certain design conditions are not exceeded for AOOs or PAs. Chapter 3.1 addresses compliance with these GDCs but does not address the function of the ESFAS and ESF control systems. Address the occurrence of AOOs and PAs with respect to GDCs 10, 15, and 16 and the ESFAS and ESF control systems function and I&C capability to actuate these systems. Address compliance with GDCs 10, 15, and 16 with respect to the ESFAS and ESF control systems in Chapter 3.1, Chapter 7.3, and Table 7.1-2.

ANSWER:

Reference to GDC10, 15 and 16 will be added in Table 7.1-2. Compliance to GDC 10, 15, 16 is demonstrated primarily through the Chapter 15, safety analysis. The setpoint methodology and response time methodology ensure adequate margin to the safety limits.

Impact on DCD

Item d., f., and g. in Table 7.1-2 Section 2 GDC 10 CFR 50 Appendix A (Sheet 2 of 8) will be revised as Attachment 1.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 230-2028 REVISION 0
SRP SECTION: 07.03 – ENGINEERED SAFETY FEATURES SYSTEMS
APPLICATION SECTION: 07.03
DATE OF RAI ISSUE: 2/26/2009

QUESTION NO.: 07.03-2

MHI is requested to address GDCs 34, 35, 38 and 41 in Chapter 7 of the DC-FSAR with regards to the ESF system. The DC-FSAR does not address compliance with GDCs 34, 35, 38 and 41 in Section 7.3 or Table 7.1-2, and refers to Chapters 5 and 6. Chapter 3.1 addresses compliance with these GDCs but does not address the function of the ESFAS and ESF control systems. To complete a review of the ESF control systems for conformance to the requirements for testability, operability with onsite and offsite electrical power, and single failures, the DC-FSAR needs to address compliance with these GDCs. Address compliance with GDCs 34, 35, 38, and 41 with respect to the ESFAS and ESF control systems in Chapter 3.1, Chapter 7.3, and Table 7.1-2.

ANSWER:

Reference to GDC 34, 35, 38 and 41 will be added in Table 7.1-2. Compliance to GDC 34, 35, 38 and 41 is demonstrated primarily through the Chapter 5, and 6.

Impact on DCD

Item r, s, t, and u. in Table 7.1-2 Section 2 GDC 10 CFR 50 Appendix A (Sheet 3 of 8) will be revised as Attachment 1.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 230-2028 REVISION 0
SRP SECTION: 07.03 – ENGINEERED SAFETY FEATURES SYSTEMS
APPLICATION SECTION: 07.03
DATE OF RAI ISSUE: 2/26/2009

QUESTION NO.: 07.03-3

The DC-FSAR does not address compliance with GDCs 33 and 44 in Section 7.3 or Table 7.1-2, and refers to Chapter 9. Chapter 3.1 addresses compliance with these GDCs but does not address the function of the ESFAS and ESF control systems. To complete the review of the applicant's proposed design criteria, design bases, and safety classification for the cooling systems, and the requirements for system performance of necessary functions during normal, abnormal, and accident conditions, assuming loss of offsite power and a single failure, and that system portions can be isolated so the safety function of the system is not compromised, the staff needs to ensure compliance with GDCs 33 and 44. Address compliance with GDCs 33 and 34 with respect to the ESFAS and ESF control systems in Chapter 3.1, Chapter 7.3, and Table 7.1-2.

ANSWER:

Reference to GDC 33 and 44 will be added in Table 7.1-2. Compliance to GDC 33 and 44 is demonstrated primarily through the Chapter 9.

Impact on DCD

Item q. and v. in Table 7.1-2 Section 2 GDC 10 CFR 50 Appendix A (Sheet 2 of 8) will be revised as Attachment 1.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 230-2028 REVISION 0
SRP SECTION: 07.03 – ENGINEERED SAFETY FEATURES SYSTEMS
APPLICATION SECTION: 07.03
DATE OF RAI ISSUE: 2/26/2009

QUESTION NO.: 07.03-4

MHI is requested to address applicability of RG 1.151 with regards to the ESF system in the DC-FSAR. The DC-FSAR does not cite compliance with RG 1.151 for the ESFAS or ESF control systems in Table 7.1-2. However, DC-FSAR Table 1.9.1-1 (Tier 2) and MUAP-07004-P cite compliance with RG 1.151 but not specifically with respect to ESFAS or ESF control systems. MHI is requested to address conformance with RG 1.151 in DC-FSAR Table 7.1-2.

ANSWER:

Compliance with RG 1.151 is stated in Subsection 7.1.3.7 and Table 7.1-2 for Section 7.2 to 7.6. RPS compliance is sufficient, since sensors for ESF actuation interface via the RPS. Section 7.2 to 7.6 is also described as the related section in US-APWR DCD in Table 7.1-2. Thus the ESF function is also covered in the scope of RG1.151 applicability.

The applicable mark "x" is also cited for DAS in item i. of Table 7.1-2 (Sheet 4 of 8). The sensor signals for DAS also come from the RPS through analog isolation modules. Therefore RG 1.151 is not applicable to DAS. This will be corrected.

Impact on DCD

Item i. in Table 7.1-2 (Sheet 4 of 8) will be revised as Attachment 1.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 230-2028 REVISION 0
SRP SECTION: 07.03 – ENGINEERED SAFETY FEATURES SYSTEMS
APPLICATION SECTION: 07.03
DATE OF RAI ISSUE: 2/26/2009

QUESTION NO.: 07.03-5

MHI is requested to address compliance with BTP 7-13 with respect to the ESFAS and ESF control systems in DC-FSAR. DC-FSAR Table 7.1-2 does not cite compliance with BTP 7-13 for ESFAS; however, MUAP-07004-P cites compliance with BTP 7-13 will be in the plant licensing documentation, as does Table 1.9.2-7 (Tier 2).

ANSWER:

Compliance with BTP 7-13 is committed in the Safety I&C TR, MUAP-07004. Compliance with BTP7-13 is also identified in Table 7.1-2 for Sections 7.2 and 7.3. Safety related RTDs are applied for the RT and ESF function. Thus Table 7.1-2 identifies the applicability to Sections 7.2 and 7.3 for BTP 7-13. In Table 7.1-2, RPS compliance is sufficient for BTP 7-13, since safety related RTDs for ESF actuation interface via the RPS.

Impact on DCD

The following will be added to Subsection 7.1.3.14:

Installed RTDs will be calibrated using the method defined in BTP 7-13. The following accuracy calibration is applicable to all safety related RTDs:

- A reference RTD is checked for acceptable accuracy and response time in controlled laboratory conditions.
- The reference RTD is installed. Loop current step response (LCRS) is checked to confirm applicability of laboratory test data.
- Measurements from installed RTDs are cross correlated to the reference RTD under known and sufficiently similar temperature and flow conditions (i.e., isothermal conditions of all RCS hot and cold legs to the extent practical).
- Calibration readout will be on digital displays, as discussed above, to ensure correct signal propagation and accuracy through the digital systems.

In addition, the LCRS is checked for installed RTDs used in the RPS or ESFAS, where response times are credited in the safety analysis. To detect response time degradation, the LCRS data is compared to the installed RTD's own historical data and to the LCRS for the reference RTD.

The accuracy and response time acceptance criteria account for expected instrument

uncertainties and expected temperature and flow deviations. "As found" and "As-left" data is recorded and maintained.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 230-2028 REVISION 0
SRP SECTION: 07.03 – ENGINEERED SAFETY FEATURES SYSTEMS
APPLICATION SECTION: 07.03
DATE OF RAI ISSUE: 2/26/2009

QUESTION NO.: 07.03-6

MHI is requested to explain how independence between the RPS and the ESF is achieved, whether sensors are shared between the reactor trip system and the engineered safety system, how this relates to the defense-in-depth (D3) approach used in the US-APWR, and what subsystems are used to achieve D3 in the US-APWR. This should be adequately explained in the DC-FSAR/

The description of how the ESF system is actuated by signals from the RPS suggest that the ESF is not independent of the RPS and cannot function without the RPS. Current guidelines for D3 (e.g., BTP 7-19) indicate independence among control, trip, engineered safety features, and post accident monitoring systems as an appropriate defense-in-depth approach. If an alternative D3 approach is used, the difference between the US-APWR and conventional approaches needs to be briefly explained and the document where this approach is described needs to be referenced.

ANSWER:

The RPS bistable and voting logic is common to the RTS and ESF systems. Therefore, the ESF system cannot automatically actuate without the RPS, while manual actuation can be achieved only by ESFAS and SLS. This integrated design complies with ISG-02 Problem statement 6 (ECHELONS OF DEFENSE) which states that separation of RPS and ESFAS is not required. The basis of this for the US-APWR is that the RPS and ESFAS are not independently credited in the Chapter 15 accident analysis. The complete approach to defense-in-depth and diversity, including the independence between echelons of defense, is described in D3 TR, MUAP-07006 and the response to RAI-03 in "Response to NRC's RAIs on Topical Report" (UAP-HF-08070).

Impact on DCD

There is no impact on the DCD.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 230-2028 REVISION 0
SRP SECTION: 07.03 – ENGINEERED SAFETY FEATURES SYSTEMS
APPLICATION SECTION: 07.03
DATE OF RAI ISSUE: 2/26/2009

QUESTION NO.: 07.03-7

MHI is requested to explain how a failure of one of the subsystems of an ESF train is detected, and how such a failure affects the response of the corresponding SLS train. This should be adequately explained in the DC-FSAR.

Figure 7.3-1 of the DC-FSAR shows that each ESF train has two redundant subsystems (CPU 1A1 and CPU 1A2). The diagram also suggests that each of these subsystems processes the same set of trip/no trip information from all four protection system trains, and actuate the necessary ESF systems and/or components to mitigate abnormal and/or accident condition(s). Each of the ESF subsystems (of a single train) communicates its information to redundant SLS subsystems (of a single train) via the safety system bus. It is not clear whether the communication protocol is such that a failure of an ESF subsystem is detected by the corresponding ESF train, by the corresponding SLS subsystem, or by any of the SLS subsystems.

ANSWER:

The Safety I&C TR, MUAP-07004 describes the ESFAS and SLS redundancy configuration and signal processing in Sections 4.2.2 ESF Actuation System (ESFAS) and 4.2.3 Safety Logic System. In summary redundant duplex controllers in the ESFAS actuate the corresponding redundant duplex controllers in the SLS. Therefore, if a failure occurs in one ESFAS controller, the corresponding SLS controllers, will not automatically actuate. However, since all SLS controllers are redundant, there will be no adverse effect on the safety function of that division. A failure of one ESFAS controller results in loss of data communication to all corresponding SLS controllers via the Safety Bus, and loss of data communication to the Engineering Tool via the Maintenance Network. The SLS controllers and Engineering Tool generate self-diagnostic error alarms for this condition. A grouped PSMS trouble alarm is displayed on the LDP; the Engineering Tool displays the error details.

Impact on DCD

There is no impact on the DCD.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 230-2028 REVISION 0
SRP SECTION: 07.03 – ENGINEERED SAFETY FEATURES SYSTEMS
APPLICATION SECTION: 07.03
DATE OF RAI ISSUE: 2/26/2009

QUESTION NO.: 07.03-8

Identify the FMEA section, table, or report that describes which process or processes were assigned to which controller, and how the failure analyses was performed to reach such decisions. This should be adequately addressed in the DC-FSAR.

The DC-FSAR states that plant process systems are assigned to controllers based on consideration of maintenance, potential SLS equipment failures, and optimization of controller performance. Multiple process systems are assigned to the same controller or a single process system is assigned to multiple controllers only if the plant effects of controller failure and maintenance are demonstrated to be acceptable, based on the FMEA. The staff needs to review the FMEA analysis for adequate assurance that the design complies with the single failure criterion.

ANSWER:

Compliance to the single failure criterion is achieved through the independence of the four redundant PSMS divisions. Each PSMS division controls only the plant components in the corresponding mechanical division. There is no credit for independence within a single PSMS or mechanical division for compliance with the single failure criterion. Therefore, the FMEA shown in Table 7.3-7 is sufficient to demonstrate compliance to the single failure criterion. However, the errors will be corrected in section 7.3.1.2.4 and the SLS output section of Table 7.3-7, and will be deleted Table 7.3-8.

FMEA report will be submitted by September 2009 including overall system required from RAI of 7.9.

Impact on DCD

Section 7.3.1.2.4 will be revised as follows;

7.3.1.2.4 Functional Allocation in SLS Controllers

Failure Mode of communication part and processing part is no data output as shown in the Table 7.3-7. Therefore the functional allocation in SLS Controllers is decided by load balance for the CPU.

~~Some ESF component control functions should be allocated to separate SLS controllers as shown in Table 7.3-8, to ensure SLS failures, which result in spurious output state changes, do not cause plant conditions that have not been considered in the plant safety analysis. As defined in Subsection 7.3.1.2, an SLS controller consists of a duplex architecture using redundant CPUs operating in a redundant parallel configuration. Controller outputs for a specific component are configured so that either redundant controller can position the plant component to its predetermined preferred safe state. In addition to component to controller assignment for consistency with the safety analysis, the following component logic is allocated to two separate controllers which are configured in a 2-out-of-2 logic scheme (external outputs wired in series to achieve AND logic). This 2-out-of-2 configuration ensures output state changes, that result from a single controller failure, do not cause a spurious reactor trip.~~

- ~~• Close logic for main steam isolation valve.~~
- ~~• Close logic for main feedwater isolation valve.~~
- ~~• Close logic for main feedwater control valve.~~
- ~~• Trip logic for RCP.~~

Table 7.3-7 will be revised as follows;

**Table 7.3-7 FMEA for ESF Actuation in PSMS (for Figure 7.3-5)
(Sheet 3 of 3)**

Component (one train)*1	Failure Mode	Method of Failure Detection	Local Failure Effect	Effect on Protective Function
SLS Output part (to Component)	Spurious change status	Manual periodic test <u>or plant system disturbance.</u>	One train of ESF can change their status. (If the change of their status affects plant disturbances, appropriate design such as duplicated output module are adopted.)	<u>One train of ESF can be actuated due to the output failure. All trains can still provide ESF actuation.</u> <u>The periodic test is administrated to detect the failure for components whose spurious actuation does not cause a plant disturbance.</u> <u>Three trains of ESF can be actuated due to the output failure. Remaining three trains provide ESF actuation.</u> <u>If another train is being tested, two trains provide ESF actuation. The periodic test is administrated to minimize the effect of failure.</u>
	Fail as is	Manual periodic test.	One train ESF does not actuate when process reaches actuation level.	<u>One train of ESF can fail due to the output failure. The remaining one or three trains provide ESF actuation, depending on the two or four train mechanical system configuration.</u> <u>For four train mechanical systems, if another train is being tested, two trains provide ESF actuation. The periodic test is administrated to detect the failure.</u> <u>One Three trains of ESF can fail be actuated due to the output failure.</u>

			<p>Remaining three trains provide ESF actuation. If another train is being tested, two trains provide ESF actuation. The periodic test is administered to minimize the effect of failure.</p>
--	--	--	--

Table 7.3-8 will be deleted as follows;

~~Table 7.3-8 Functional Allocation in SLS Controllers~~

Group-1	Group-2	Group-3
Main steam relief valve	Safety Injection pump	Letdown isolation valve
Main steam depressurization valve	Emergency feedwater actuation components	Safety depressurization valve

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 230-2028 REVISION 0
SRP SECTION: 07.03 – ENGINEERED SAFETY FEATURES SYSTEMS
APPLICATION SECTION: 07.03
DATE OF RAI ISSUE: 2/26/2009

QUESTION NO.: 07.03-9

MHI is requested to explain in detail and with figures, the priority logic portions of the SLS, showing all inputs to the priority logic, which actuators use such priority logic, and how the diverse actuation requirements are met.

The SLS has portions with priority logic “to accommodate signals from the diverse actuation system.” Position 2 of Section 2, “Command Prioritization,” of Interim Staff Guidance DI&C-ISG-04, states that “priority modules used for diverse actuation signals should be independent of the remainder of the digital system, and should function properly regardless of the state or condition of the digital system. If these recommendations are not satisfied, the applicant should show how the diverse actuation requirements are met. The staff needs further clarification to make a determination as to whether the design of the SLS satisfies this guidance.

ANSWER:

To clarify the priority logic, the following description will be added to the next revision of the Safety I&C TR, MUAP-07004:

Safety related plant components are mainly controlled by manual control from the Safety VDU and manual control from the PCMS Operational VDU, safety automatic demand, non-safety automatic demand from the PCMS, and DAS demand. The priority logic which combines all signals, except the DAS demand, is implemented within the PSMS software. The priority logic which combines the SLS output with the DAS demand is implemented within the conventional solid state interposing logic (IPL) of the PIF module.





Impact on DCD

There is no impact on the DCD.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 230-2028 REVISION 0
SRP SECTION: 07.03 – ENGINEERED SAFETY FEATURES SYSTEMS
APPLICATION SECTION: 07.03
DATE OF RAI ISSUE: 2/26/2009

QUESTION NO.: 07.03-10

MHI is requested to identify if the priority module identified in Section 7.3.1.5.8.2 contain any software? If so describe the processes used to assure the quality of the software. If the priority module does not include any software, describe the process for accepting any software tools used to assure the quality of the design of the priority module.

Clause 5.3, "Quality," of IEEE Std 603-1998, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," requires safety system equipment to be designed, manufactured, inspected, installed, tested, operated, and maintained in accordance with a prescribed quality assurance program. Guidance on the application of this criterion for safety system equipment employing digital computers and programs or firmware is found in IEEE Std 7-4.3.2-1993. Priority modules are safety-related systems, and the staff requires assurance that any software that is part of the priority module has undergone the same V&V as the rest of the safety system. If the priority module does not contain any software, then Position 6 of Section 2, "Command Prioritization," of DI&C-ISG-04 requires software used in the design, testing, Maintenance, etc. of a priority module to be subject to all of the applicable guidance in Regulatory Guide 1.152, which endorses IEEE Std 7-4.3.2-2003 (with comments). This includes software applicable to any programmable device used in support of the safety function of a prioritization module, such as programmable logic. Position 6 of Section 2 of DI&C-ISG-04 also states that validation of design tools used for programming a priority module or a component of a priority module is not necessary if the device directly affected by those tools is 100% tested before being released for service. The staff needs to know the design details and the process of accepting the software tools to make an assessment of the adequacy of the quality of the priority module.

ANSWER:

There is no priority function described in Subsection 7.3.1.5.8.2.

Priority functions 1 and 2, described in the response to RAI 07.03-09, are implemented within the software of the PSMS controllers. All PSMS controller software is implemented in accordance with all regulatory requirements for Class 1E software.

Priority function 3, described in the response to RAI 07.03-09, is implemented within the conventional solid state logic of the PIF module. This hardware is implemented in accordance with all requirements for hardware based Class 1E systems.

Impact on DCD

There is no impact on the DCD.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 230-2028 REVISION 0
SRP SECTION: 07.03 – ENGINEERED SAFETY FEATURES SYSTEMS
APPLICATION SECTION: 07.03
DATE OF RAI ISSUE: 2/26/2009

QUESTION NO.: 07.03-11

MHI is requested to identify if the priority module identified in Section 7.3.1.5.8.2 of the SLS train control one component, or does it control more than one component? If a priority module controls more than one component, show how the independence requirement above is met.

Position 4 of Section 2, "Command Prioritization," of Interim Staff Guidance DI&C-ISG-04, states that a priority module may control one or more components, but that if a priority module controls more than one component, then all of the recommendations stated in the ISG also apply to each of the actuated components.

ANSWER:

Priority function 1, described in the response to RAI 07.03-09, is implemented separately for each safety division; the priority function effects all components of that division. Priority function 2 is implemented separately for each component; multiple components are controlled by the same controller. Priority function 3 is implemented separately for each PIF module; a PIF module can control multiple components but only if the exact same logic is applicable to those components and they can be controlled simultaneously.

Impact on DCD

There is no impact on the DCD.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 230-2028 REVISION 0
SRP SECTION: 07.03 – ENGINEERED SAFETY FEATURES SYSTEMS
APPLICATION SECTION: 07.03
DATE OF RAI ISSUE: 2/26/2009

QUESTION NO.: 07.03-12

MHI is requested to provide in Sections 7.3.2.8, and 7.2.2.8, "Equipment Qualification," of Chapter 7 of US-APWR DC-FSAR, a concise but sufficient information of the environmental qualification results, to enable adequate review without having to refer to (several) other reports. A reference to another report providing further details may be contained in the DC-FSAR. However, the reviewer should only have to resort to this if there are questions regarding the results or if further details of the testing methodology are required.

Sections 7.3.2.8 and 7.2.2.8, "Equipment Qualification," of the DC-FSAR refers to Subsection 7.1.3.7 for details of the qualification of the safety systems. This section states that the PSMS is qualified for worst-case environmental and seismic requirements for the place of its installation. However, it does not provide details of the tests, nor does it point to any report(s) that document the test procedure and results. The DC-FSAR states that details of PSMS qualification testing may be found in TR MUAP-07004-P, Sections 5.2.1 through 5.2.5. However, these sections only describe environmental design features and service conditions. They do not provide environmental, seismic, and EMI/RFI test results, nor do they reference any test reports. Section 5.2.1 of TR MUAP-07004-P states that the PSMS is located in the main control room, remote shutdown room and I&C equipment rooms so that it is not influenced by external effects such as tornadoes, hurricanes and floods. It also states that the PSMS is located in areas where the radiation influence is negligible (i.e. up to 103 rads (10 Gy)). Section 5.2.2 of the same reference further states that the PSMS, including the Safety VDU, is classified as Class 1E Seismic Category 1, and that the system is qualified to maintain physical integrity and all functionality during and after an Operating Basis Earthquake and a Safe Shutdown Earthquake. The DC-FSAR refers to TR MUAP-07005-P for further details regarding the seismic testing.

ANSWER:

The Platform TR, MUAP-07005 describes generic equipment qualification test methods and test results for the MELTAC. Detailed test procedures and test reports were provided at the MELTAC platform audits in Arlington and Kobe. The environmental conditions of the US-APWR are described in "US-APWR Equipment Environmental Qualification Program" MUAP-08015(R3). The Class 1E I&C room and Class 1E electrical room in which safety-related MELTAC is located is mild environmental area during design basis event.

Impact on DCD

The first paragraph of Subsection 7.1.3.7 will be revised as follows;

7.1.3.7 Qualification and Equipment Protection

The PSMS is qualified for worst-case environmental and seismic requirement for the place of its installation. The PSMS qualification envelopes the seismic and environmental boundary conditions for these locations are described in Sections 3.10 and 3.11. The Topical Report MUAP-07005 describes equipment qualification testing for the MELTAC platform. The environmental condition of the US-APWR is described in "US-APWR Equipment Environmental Qualification Program" MUAP-08015.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 230-2028 REVISION 0
SRP SECTION: 07.03 – ENGINEERED SAFETY FEATURES SYSTEMS
APPLICATION SECTION: 07.03
DATE OF RAI ISSUE: 2/26/2009

QUESTION NO.: 07.03-13

MHI requested to provide sufficient information to show that, for the cases in which manual ESF actuation is used as the second and only means of providing signal diversity, the response time requirement for the safety function is met.

The US-APWR DC-FSAR does not contain sufficient information for assessing the adequacy of providing manual ESF actuation as the only means for achieving signal diversity. Part F of Section II, "Review Procedures," of Chapter 7.3, "Engineered Safety Features Systems," of the SRP allows manual activation to be used as the alternate, diverse means, of ESF actuation if it is consistent with the response time requirements of the function (i.e., for the mitigation of the accident scenario).

ANSWER:

Manual ESF actuation is not credited in Chapter 15 safety analysis for any event. Therefore, there is no description of response time requirements for manual ESF actuation.

Signals diversity within the PSMS is not credited for coping with CCF, since complete failure of the digital part of PSMS is assumed in the CCF coping analysis. However, signal diversity within the PSMS is described in Section 7.2 and shown in Table 7.2-5.

Impact on DCD

There is no impact on the DCD.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 230-2028 REVISION 0
SRP SECTION: 07.03 – ENGINEERED SAFETY FEATURES SYSTEMS
APPLICATION SECTION: 07.03
DATE OF RAI ISSUE: 2/26/2009

QUESTION NO.: 07.03-14

MHI is requested to provide equipment location drawings for the ESF per RG 1.206, Section C.I.7.3.1.2. Section 7.3.1.2, with regards to the SLS controllers, states that "I/O for each train in the US-APWR is remotely distributed throughout the plant." At this discussion reference should be made to the equipment location drawings. Also, is the remote I/O located in harsh environment areas or areas which would require qualification beyond normal mild environment criteria?

ANSWER:

All SLS I/O will be located within the Class 1E I&C equipment rooms and Class 1E electrical rooms. These rooms are maintained in a mild environment condition by the safety ventilation system at all times.

Impact on DCD

The following sentence in Subsection 7.3.1.2 will be deleted:

~~To minimize field cabling, the I/O for each train in the US-APWR is remotely distributed throughout the plant in close proximity to safety equipment.~~

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 230-2028 REVISION 0
SRP SECTION: 07.03 – ENGINEERED SAFETY FEATURES SYSTEMS
APPLICATION SECTION: 07.03
DATE OF RAI ISSUE: 2/26/2009

QUESTION NO.: 07.03-15

MHI is requested to identify how Clause 6.2.1 of IEEE Std 603-1991 is met for the ESF System. Clause 6.2.1 of IEEE Std. 603-1991 states that "means shall be provided in the control room to implement manual initiation at the division level of the automatically initiated protective actions. The means provided shall minimize the number of discrete operator manipulations and shall depend on the operation of a minimum of equipment." Regulatory Guide 1.62 states in Regulatory Position C.4 the staff position for what constitutes "operation of a minimum of equipment." The ESF manual system level initiation path, presented in Figure 7.3-1, does apparently use common digital components with the automatic protection line. MHI is requested to thoroughly explain by text and confirmation via figures, how Clause 6.2.1 of IEEE Std. 603-1991 and RG 1.62 is met by the US-APWR for ESF manual actuations.

ANSWER:

Compliance to RG 1.62 and IEEE std 603 Section 6.2 is described in the Safety I&C TR MUAP-07004 Sections 3.3(5) and A6.2, respectively. The design is described in Section 4.2.2 and shown in detail in Figure 4.4-2.

Manual initiation depends on a "minimum of equipment" by bypassing the automatic initiation section in the RPS, which bypasses the bistable comparators and the parameter coincidence voting. The ESFAS controller must be used for manual initiation to allow the ESFAS signals to be properly sequenced and to allow the signals to be distributed to SLS controllers using the safety bus. Proper sequencing is critical to avoid electrical bus overload. Signal distribution via the safety bus is more reliable than discrete I/O connections, since digital data communications is continuously self-tested. For four train systems final voting must be common to manual and automatic actuation to allow all four train systems to be actuated while "minimizing the number of discrete operator manipulations" (i.e., two is the minimum number to prevent spurious actuation of all divisions due to a single failure).

MHI will add the description of manual ESF actuation logic to the Safety I&C TR MUAP-07004 Section 4.2.2.

Manual initiation bypasses the automatic initiation section in the RPS. All trains are separately initiated from train specific manual actuation switches. In addition, for four train systems each train is actuated by 2-out-of-3 manual initiation signals received from the other 3 trains.

Therefore, for all safety functions (two train or four train) all trains are manually initiated by actuating two manual initiation switches.

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.

**Responses to Request for Additional Information No.227-2020
Revision 0**

**SRP Section 7.4
Safe Shutdown Systems**

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 227-2020 REVISION 0
SRP SECTION: 07.04 – SAFE SHUTDOWN SYSTEMS
APPLICATION SECTION: 07.04
DATE OF RAI ISSUE: 2/26/2009

QUESTION NO.: 07.04-1

MHI should address the CFR subsections applicable to safe shutdown in Section 7.4 and in Table 7.1-2.

Table 7.1-2 in the Design Control Document (DCD) does not provide a column in its list of systems for safe shutdown systems, 7.4. Because safe shutdown functions are achieved by the PSMS, five columns in Table 7.1-2 of the DCD were checked in this review: RPS, ESFAS, SLS and safety HSI, and the column titled "Related Section in USAPWR DCD." Table 7.1-2 in the DCD cites compliance with all the CFR sections listed in SRP Table 7-1 for systems that provide safe shutdown functions.

ANSWER:

As for Table 7.1-2, Section 7.4 "Safe Shutdown Systems" have already been indicated in the column of "Related Section in the US-APWR DCD". According to NUREG 0800; SRP 7.4, applicable CFR will be added in the Subsection 7.4.2.

Impact on DCD

Following sentence will be added at after the first paragraph of subsection 7.4.2;

In addition, the design of the safe shutdown systems including the design of the RSR is based on the following CFR:

1. 10 CFR 50.55a(a)(1), "Quality Standards."
2. 10 CFR 50.55a(h), "Protection Systems and Safety Systems"
3. 10 CFR 50.34(f)(2)(xx), "Power for Pressurizer Level Indication and Controls for Pressurizer Relief and Block Valves"
4. 10 CFR 50, Appendix A, GDC 1, "Quality Standards and Records."
5. GDC 2, "Design Bases for Protection against Natural Phenomena."
6. GDC 4, "Environmental and Missile Design Bases."
7. GDC 13, "Instrumentation and Control."
8. GDC 24, "Separation of Protection and Control Systems."
9. GDC 34, "Residual Heat Removal."
10. GDC 35, "Emergency Core Cooling."
11. GDC 38, "Containment Heat Removal."

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 227-2020 REVISION 0
SRP SECTION: 07.04 – SAFE SHUTDOWN SYSTEMS
APPLICATION SECTION: 07.04
DATE OF RAI ISSUE: 2/26/2009

QUESTION NO.: 07.04-2

MHI is requested to discuss compliance with GDCs 34, 35, and 38 in relation to the safe shutdown systems, any potential common-mode failures, and the propagation of erroneous data. Update Table 7.1-2 if necessary.

Table 7.1-2 in the DCD indicates compliance with the GDC listed in Table 7-1 of the SRP as applicable to Section 7.4, Safe Shutdown Systems, with the exception of GDCs 34, 35 and 38. DCD Table 7.1-2 cites Chapter 5 "Reactor Coolant System and Connected Systems" for conformance to GDC 34, and Chapter 6 "Engineered Safety Features" for conformance to GDCs 35 and 38. The staff conducted a review of the RCS and ESF systems, and concluded that ESF control systems are testable and are operable using either onsite or offsite power (assuming only one source is available). Additionally, controls associated with redundant ESF systems are independent and satisfy the single failure criterion. Therefore, the RHR, emergency core cooling system, and containment heat removal systems satisfy the criteria set forth by GDCs 34, 35 and 38, respectively. Detailed compliance with the GDCs is described in TR MUAP-07004-P(R1). SRP Table 7-1 indicates that GDCs 34, 35, and 38 are required for compliance for safe shutdown systems.

ANSWER:

GDC 34, 35 and 38 are related to Section 7.4.

Impact on DCD

Section "7.4" will be added in item r., s., and t. of Table 7.1-2 as Attachment 1.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 227-2020 REVISION 0
SRP SECTION: 07.04 – SAFE SHUTDOWN SYSTEMS
APPLICATION SECTION: 07.04
DATE OF RAI ISSUE: 2/26/2009

QUESTION NO.: 07.04-3

Discuss conformance with RG 1.204 in relation to the safe shutdown systems, and assurance that electrical transients resulting from lightning phenomena do not render safety-related systems inoperable or cause spurious operation of such systems. Update Table 7.1-2 if necessary.

RG 1.204 provides guidance for the design and implementation of lightning protection systems (LPSs) to ensure that electrical transients resulting from lightning phenomena do not render safety-related systems inoperable or cause spurious operation of such systems. Table 7.1-2 in the DCD does not cite conformance with RG 1.204, and references Chapter 8, "Electric Power." The staff conducted a review of the grounding and the LPS in Chapter 8 of the DCD, and concluded that the design of the system is in accordance with the IEEE Std 665, 666, 1050 and C62.23, as endorsed by RG 1.204.

ANSWER:

RG 1.204 is a requirement for the electrical system. Conformance with RG 1.180, which is the corresponding requirement for the I&C system has already been described in Table 7.1-2. See response to RAI 07.01-21.

Impact on DCD

There is no impact on the DCD.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 227-2020 REVISION 0
SRP SECTION: 07.04 – SAFE SHUTDOWN SYSTEMS
APPLICATION SECTION: 07.04
DATE OF RAI ISSUE: 2/26/2009

QUESTION NO.: 07.04-4

Discuss conformance with RG 1.151 in relation to the safe shutdown systems, and the design and installation of safety-related instrument sensing lines. Update Table 7.1-2 if necessary.

RG 1.151 describes a method acceptable to the staff with regard to the design and installation of safety-related instrument sensing lines in nuclear power plants. Table 7.1-2 in the DCD cites compliance with RG 1.151 only for the RPS yet the column titled "Related Section in US-APWR DCD" cites applicability to DCD Sections 7.2–7.6 (RPS, ESFAS, safe shutdown, information systems important to safety, and interlock systems important to safety, respectively). In the US-APWR, all safety-related instrument sensing lines are connected to the RPS, and the signals are redistributed from this system. Because the RPS satisfies all the criteria set forth by RG 1.151, the criteria are met for the overall system to provide safe shutdown functions. However, the column titled "Related Section in US-APWR DCD" indicates that RG 1.151 is applicable to Section 7.4—the section for safe shutdown systems.

ANSWER:

In Table 7.1-2 the "I&C System" columns identify the specific US-APWR I&C system(s) that are credited in conforming to the requirement, and therefore the specific US-APWR systems to which the requirement applies. The column, "Related Section in US-APWR DCD", in Table 7.1-2 indicates the sections of the DCD to which the requirement applies. Since Safe shutdown is achieved using instrumentation which interfaces via the RPS, Table 7.1-2 appropriately identifies conformance with RG 1.151 for the RPS, and the related DCD section for Safe Shutdown functions is Section 7.4.

Impact on DCD

There is no impact on the DCD.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 227-2020 REVISION 0
SRP SECTION: 07.04 – SAFE SHUTDOWN SYSTEMS
APPLICATION SECTION: 07.04
DATE OF RAI ISSUE: 2/26/2009

QUESTION NO.: 07.04-5

Discuss conformance with BTP 7-13 in relation to the safe shutdown systems. Update Table 7.1-2 if necessary.

Only I&C system column "RPS" cites conformance with the BTP 7-13 in Table 7.1-2 in the DCD. This is acceptable because, as explained above for RG 1.151, all safety-related instrument sensing lines go through the RPS before distributed to other systems. Therefore, if RPS complies with BTP 7-13, the overall system for safe shutdown meets the criteria of the staff position. However, the column titled "Related Section in USAPWR DCD" does not indicate that BTP 7-13 is applicable to safe shutdown systems (Section 7.4); SRP Table 7-1 indicates that BTP 7-13 is applicable to safe shutdown systems.

ANSWER:

BTP 7-13 is also applicable to safety related RTDs for Section 7.4 of safe shutdown and Section 7.5 of PAM. However, as explained in the response to RAI 7.03-5, the response time testing in BTP 7-13 is only required for fast response RTDs used within the RT or ESF functions. The fast response RTDs are not used for the RTDs of wide range RCS temperature for safe shutdown and PAM. Thus the response time testing in BTP 7-13 is not applicable to the RTDs in section 7.4 and 7.5. In Table 7.1-2, RPS compliance is sufficient for BTP 7-13, since safety related RTDs for safe shutdown interface via the RPS. Therefore, no update will be made for Table 7.1-2.

Impact on DCD

There is no impact on the DCD.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 227-2020 REVISION 0
SRP SECTION: 07.04 – SAFE SHUTDOWN SYSTEMS
APPLICATION SECTION: 07.04
DATE OF RAI ISSUE: 2/26/2009

QUESTION NO.: 07.04-6

Discuss any features of the ESF systems that are unique to safe shutdown and not directly related to accident mitigation.

The review of DCD Section 7.4 evaluates those I&C systems used to achieve and maintain a safe shutdown condition of the plant as required by 10 CFR 50 Appendix A, GDCs 13 and 19. To the extent that the ESF systems are used to achieve and maintain safe shutdown, the review of these systems in this section is limited to those features that are unique to safe shutdown and not directly related to accident mitigation. The features within the scope of SRP Section 7.4 may involve individual component control for safe shutdown versus system-level actuation for accident mitigation, or system-level controls used to achieve and maintain safe shutdown but not used for accident mitigation.

ANSWER:

ESF systems which are unique to safe shutdown and not used for accident mitigation are the emergency letdown system and the accumulator nitrogen discharge system.

The emergency letdown system, which is described in Subsection 6.3.2.1.3, and identified in Table 7.4-1, is used for safety grade cold shutdown by providing a means for feed and bleed for boration, and make up water for compensation of shrinkage. This system is not used for accident mitigation.

The accumulator nitrogen discharge system which is described in Subsection 6.3.2.2.6.9 and identified in Table 7.4-1 is not used for accident mitigation. If an accumulator discharge valve is not closed due to a single failure, for safe shutdown the accumulator nitrogen discharge valve can be manually opened by operator action from the MCR and RSC, depressurizing the accumulator to prevent the accumulator from inadvertently discharging nitrogen gas into the RCS.

Safe shutdown functions are performed only by individual component controls; there are no system-level controls for safe shutdown. Component level controls used for safe shutdown are also used for accident mitigation for components that are used for both functions. System level controls are only used for accident mitigation.

Impact on DCD

There is no impact on the DCD.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 227-2020 REVISION 0
SRP SECTION: 07.04 – SAFE SHUTDOWN SYSTEMS
APPLICATION SECTION: 07.04
DATE OF RAI ISSUE: 2/26/2009

QUESTION NO.: 07.04-7

Discuss the applicability of Mode 4—hot shutdown using safety-related plant equipment and what circumstances would this apply? What are the primary functions and related process systems required to achieve and maintain hot shutdown using only safety-related equipment?

The technical specifications for the US-APWR define the modes as any one inclusive combination of core reactivity condition, power level, average reactor coolant temperature, and reactor vessel head closure bolt tensioning with fuel in the reactor vessel. Shutdown functions consist of normal shutdown operation, and safe shutdown operation (i.e., safe shutdown using only safety-related plant equipment). During safe shutdown, reactivity control systems must maintain a subcritical condition of the core, and residual heat removal systems must operate to maintain adequate cooling of the core. Section 7.4.1.6 and its subsections indicates that the US-APWR can achieve hot standby (Mode 3) and cold shutdown (Mode 5) with either the normal or safe shutdown systems.

ANSWER:

The functions defined to achieve and maintain Cold Shutdown from Hot Standby, include the functions to achieve and maintain Hot Shutdown. The first paragraph of subsection 7.4.1.6.1.2 will be revised to incorporate the explanation above.

The period to maintain Hot Shutdown using only safety related equipment is limited by the capacity of EFW pit, as described in DCD Subsection 10.4.9.

Impact on DCD

Subsection of 7.4.1.6.1.2 will be revised as follows

7.4.1.6.1.2 Hot and Cold Shutdown

The primary functions and related process systems (shown in parenthesis) required to achieve and maintain cold shutdown are as follows. This describes functions to achieve and maintain cold shutdown from hot standby, therefore this includes functions to achieve and maintain hot shutdown. The capabilities and limitations of these systems are defined in the sections of this document that describe the respective process systems.

Also, Subsection of 7.4.1.6.1.2 will be revised as follows;

7.4.1.6.2.2 Hot and Cold Shutdown

The primary functions and related process systems (shown in parenthesis) required to achieve and maintain cold shutdown using only safety-related equipment are as follows. This describes functions to achieve and maintain cold shutdown from hot standby, therefore this includes functions to achieve and maintain hot shutdown. The capabilities and limitations of these systems are defined in the sections of this document that describe the respective process systems.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 227-2020 REVISION 0
SRP SECTION: 07.04 – SAFE SHUTDOWN SYSTEMS
APPLICATION SECTION: 07.04
DATE OF RAI ISSUE: 2/26/2009

QUESTION NO.: 07.04-8

Identify and discuss any single detectable failure within the safe shutdown systems concurrent with all identifiable but nondetectable failures that were evaluated in the presence of a design basis event.

Section 5.1 of IEEE Std 603-1991 states that the safety system must perform all safety functions required for a design basis event in the presence of (a) any single detectable failure within the safety systems concurrent with all identifiable but nondetectable failures, (b) all failures caused by the single failure, and (c) all failures and spurious system actions that cause or are caused by the design basis event requiring the safety functions. The single failure could occur prior to, or at any time during, the design basis event for which the safety system is required to function. DCD Section 7.4.2.2 states that "all functions . . . including those used to achieve safe shutdown meet the single failure criterion." Insufficient information is provided to address DBEs, seismic events, and accident conditions.

ANSWER:

The test method for all I&C equipment within the PSMS, including equipment used for safe shutdown, is the same. Self-diagnosis with overlapping manual tests that encompass PSMS I/O and interfacing plant process components, such as sensors, pumps and valves, ensure there are no undetectable failures. There are at least two fully redundant and independent trains for all safety shutdown components to satisfy the single failure criterion. Columns will be added to Table 7-4.1 to show that there is redundancy for each component credited for safe shutdown.

Impact on DCD

Table 7.4-1 will be revised as follows.

**Table 7.4-1 Component Controls for Shutdown
(Sheet 1 of 3)**

Systems	Components	Normal Shutdown	Safe Shutdown	Train number for Safe Shutdown		Remarks
				Required Number	Actual Number	
RT System	RTB	No	Yes	<u>2</u>	<u>4</u>	
RCS	RCP	Yes	No	=	=	Available with off-site power.
	Safety Depressurization Valve	No	Yes	<u>1</u>	<u>2</u>	<u>Note 1</u>
	Safety Depressurization Valve Block Valve	No	Yes	<u>1</u>	<u>2</u>	<u>Note 1</u>
	Pressurizer Heater Backup Group	No	Yes	<u>2</u>	<u>4</u>	
	Pressurizer Spray Valve	Yes	No	=	=	
	Reactor Vessel (RV) Vent Valve	No	Yes	<u>1</u>	<u>2</u>	These valves could be used only if the venting becomes necessary in LOOP and Reactor Vessel is required.
CVCS	Charging Pump	Yes	No	=	=	Automatic start in LOOP.
	Charging Flow Control Valve	Yes	No	=	=	
	Letdown Line 1st (2nd) Stop Valve	Yes	No	=	=	
	Letdown Line inside C/V Isolation Valve	Yes	No	=	=	
	CHP Inlet Line VCT Side 1st, 2nd Isolation Valve	Yes	No	=	=	
	CHP Inlet Line BAT Side Isolation Valve	Yes	No	=	=	
	CHP Inlet Line RWSAT Side Isolation Valve	No	No	=	=	These valves are automatically opened on Low Volume Control Tank Water Level.
	Pressurizer Auxiliary Spray Valve	Yes	No	=	=	
	RHR Letdown Line Flow Control Valve	Yes	No	=	=	
	Seal Water Return Line 1st, 2nd Isolation Valve	Yes	Yes	<u>1</u>	<u>2</u>	These valves are used to holdup seal water inside containment in Safe Shutdown.
SIS	Safety Injection Pump (SIP)	No	Yes	<u>2</u>	<u>4</u>	<u>Table 6.3-6</u>
	SIPs Suction	No	Yes	<u>2</u>	<u>4</u>	<u>Table 6.3-6</u>

Isolation Valve						
SIPs Discharge Containment Isolation Valve	No	Yes	<u>2</u>	<u>4</u>	<u>Table 6.3-6</u>	
Direct Vessel Safety Injection Line Valve	No	Yes	<u>2</u>	<u>4</u>	<u>Table 6.3-6</u>	
Emergency Letdown Line 1st, 2nd Isolation Valve	No	Yes	<u>1</u>	<u>2</u>	<u>Table 6.3-6</u>	
Accumulator Discharge Valve	Yes	Yes	<u>4</u>	<u>4</u>	<u>Table 6.3-6</u>	
ACC Nitrogen Supply Line Isolation Valve	No	Yes	<u>4</u>	<u>4</u>	These valves are used in case of ACC discharge valve failure to close. <u>Table 6.3-6</u>	
ACC Nitrogen Discharge Valve	No	Yes	<u>1</u>	<u>2</u>		

Note1: The configuration of the Safety Depressurization Valves and Safety Depressurization Valve – Block Valves meets the single failure criteria (for both electrical and mechanical failures), to ensure the capability for depressurization when required and to prevent spurious depressurization. There are two depressurization lines, each with one Safety Depressurization Valve (normally closed) and one Safety Depressurization Valve – Block Valve (normally open), each assigned to different trains. Four trains are used, such that the four valves in the two depressurization lines do not share any common train assignments. Should a Safety Depressurization valve fail to open when required, depressurization can be achieved through the other line. Should a Safety Depressurization valve spuriously open, the series block valve can be closed.

**Table 7.4-1 Component Controls for Shutdown
(Sheet 2 of 3)**

Systems	Components	Normal Shutdown	Safe Shutdown	Train number for Safe Shutdown		Remarks
				Required Number	Actual Number	
RHRS	CS/RHR Pump	Yes	Yes	<u>2</u>	<u>4</u>	<u>Table 5.4.7-1</u>
	1st/2nd CS/RHR Pump Hot Leg Isolation Valve	Yes	Yes	<u>2</u>	<u>4</u>	<u>Table 5.4.7-1</u>
	CS/RHR Hx Outlet Flow Control Valve	Yes	No	=	=	
	CS/RHR Hx Bypass Flow Control Valve	Yes	No	=	=	
	CS/RHR Pumps RWSP Suction Isolation Valve	Yes	Yes	<u>2</u>	<u>4</u>	<u>CSS Valves Table 6.2.2-3</u>
	RHR Discharge Line Containment Isolation Valve	Yes	Yes	<u>2</u>	<u>4</u>	<u>Table 5.4.7-1</u>
	RHR Flow Control Valve	Yes	Yes	<u>2</u>	<u>4</u>	<u>Table 5.4.7-1</u>
	CS/RHR Pump Full-Flow Test Line Stop Valve	No	Yes	<u>2</u>	<u>4</u>	<u>Table 5.4.7-1</u>
EFWS	EFW Pump (Motor-Driven or Turbine Driven)	No	Yes	<u>2</u>	<u>4</u>	<u>Table 10.4.9-3</u>
	EFW Isolation Valve	No	Yes	<u>2 per 2 SG</u>	<u>4 per 4 SG</u>	<u>2 electrical train assigned per SG Table 10.4.9-3</u>
	T/D-EFW Pump MS Line Steam Isolation Valve	No	Yes	<u>1 per pump</u>	<u>2 per pump</u>	<u>Table 10.4.9-3</u>
	T/D-EFW Pump Actuation Valve	No	Yes	<u>1</u>	<u>2</u>	<u>Table 10.4.9-3</u>
MSS	Main Steam Depressurization Valve	No	Yes	<u>2</u>	<u>4</u>	<u>Table 10.3.3-1</u>
	Main Steam Relief Valve	Yes	No	=	=	
	Main Steam Relief Valve Block Valve	No	Yes	<u>2</u>	<u>4</u>	<u>Table 10.3.3-1</u>
	Main Steam Isolation Valve	Yes	Yes	<u>4</u>	<u>4</u>	<u>Table 10.3.3-1</u>
	Main Steam Bypass Isolation Valve	Yes	Yes	<u>4</u>	<u>4</u>	<u>Table 10.3.3-1</u>
	Turbine Bypass Valve	Yes	No	=	=	
CFS	MFW Bypass Regulation valve	Yes	No	=	=	
	SG Water Filling Control Valve	Yes	No	=	=	
CCWS	CCW Pump	Yes	Yes	<u>2</u>	<u>4</u>	Automatic start in LOOP. <u>Table 9.2.2-3</u>
	CS/RHR Hx CCW Outlet Valve	Yes	Yes	<u>2</u>	<u>4</u>	<u>Table 9.2.2-3</u>

ESWS	ESW Pump	Yes	Yes	<u>2</u>	<u>4</u>	Automatic start in LOOP. <u>Table 9.2.1-2</u>
	ESW Pump Discharge Valve	Yes	Yes	<u>2</u>	<u>4</u>	<u>Table 9.2.1-2</u>
IAS	Instrument Air Compressor	Yes	No	=	=	Automatic start in LOOP.
PSS	Letdown Demineralizer Inlet Sampling Valve	Yes	No	=	=	Local Manual Valve
	RHR Loop Sampling Stop Valve	Yes	No	=	=	Installed inside sampling rack.
	Inside Sampling Hood Isolation Valve	Yes	No	=	=	Installed inside sampling rack.
	Loop Sampling Line In and out side C/V Isolation Valve	Yes	No	=	=	
SGBDS	SGBD Line Containment Isolation Valve	No	Yes	<u>4</u>	<u>4</u>	Close on EFW Pump Start Signal. in <u>Table 10.3.3-1</u>
	SGBD Line Isolation Valve	No	Yes	<u>4</u>	<u>4</u>	Close on EFW Pump Start Signal. <u>Table 10.3.3-1</u>
	SGBD Sampling Line Containment Isolation Valve	No	Yes	<u>4</u>	<u>4</u>	Close on EFW Pump Start Signal. <u>Table 10.3.3-1</u>

**Table 7.4-1 Component Controls for Shutdown
(Sheet 3 of 3)**

Systems	Components	Normal Shutdown	Safe Shutdown	Train number for Safe Shutdown		Remarks
				Required Number	Actual Number	
Other	ECCS Actuation Signal Block	Yes	Yes	<u>4</u>	<u>4</u>	
	Main Steam Line Pressure Signal Block	Yes	Yes	<u>4</u>	<u>4</u>	
	Emergency Power Generator	No	Yes	<u>2</u>	<u>4</u>	Automatic start in LOOP.
HVAC	MCR Air Handling Unit & Damper	Yes	Yes	<u>2</u>	<u>4</u>	Automatic start in LOOP.
	Class 1E Electrical Room Air Handling Unit & Damper	Yes	Yes	<u>2</u>	<u>4</u>	Automatic start in LOOP.
	Class 1E Electrical Room Return Air Fan	Yes	Yes	<u>2</u>	<u>4</u>	Automatic start in LOOP.
	Class 1E Battery Room Exhaust Fan & Damper	Yes	Yes	<u>2</u>	<u>4</u>	Automatic start in LOOP.
	Safeguard Component Area Air Handling Unit & Damper	No	Yes	<u>2</u>	<u>4</u>	
	CCW Pump Area Air Handling Unit	No	Yes	<u>2</u>	<u>4</u>	
	Essential Chiller Unit Area Air Handling Unit	No	Yes	<u>2</u>	<u>4</u>	
	EFW Pump Area Air Handling Unit	No	Yes	<u>2</u>	<u>4</u>	
	Essential Chiller Unit	Yes	Yes	<u>2</u>	<u>4</u>	
	Essential Chilled Water Pump & Valves	Yes	Yes	<u>2</u>	<u>4</u>	
	Containment Fan Cooler Unit	Yes	No	=	=	Automatic start in LOOP.
	Reactor Cavity Cooling Fan	Yes	No	=	=	Automatic start in LOOP.
	CRDM Cooling Fans & Unit	Yes	No	=	=	Automatic start in LOOP.
	Non-Class 1E Electrical Room Air Handling Unit & Damper	Yes	No	=	=	Automatic start in LOOP.
	Non-Class 1E Electrical Room Return Air Fan	Yes	No	=	=	
	Non-Class 1E Battery Room Exhaust Fan & Damper	Yes	No	=	=	Automatic start in LOOP.
Auxiliary Building	Yes	No	=	=		

Air Handling Unit & Damper						
MS/FW Piping Area Air Handling Unit & Damper	Yes	No	=	=		
Non- Essential Chiller Unit	Yes	No	=	=		Automatic start in LOOP.
Non- Essential Chilled Water Pump & Valves	Yes	No	=	=		Automatic start in LOOP.
Non-Essential Chiller Condenser Water Pump & Valves	Yes	No	=	=		Automatic start in LOOP.
Non-Essential Chilled Water System Cooling Tower Fan	Yes	No	=	=		Automatic start in LOOP.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 227-2020 REVISION 0
SRP SECTION: 07.04 – SAFE SHUTDOWN SYSTEMS
APPLICATION SECTION: 07.04
DATE OF RAI ISSUE: 2/26/2009

QUESTION NO.: 07.04-9

Discuss the conditions and events analyzed where components and systems are assumed to function if functioning adversely affects safety system performance. In addition, discuss the analyses where after assuming the failures of non-safety-grade, non-qualified equipment and those failures caused by a specific event, a random single failure is arbitrarily assumed. With these failures assumed, the safe shutdown system must be capable of performing the protective functions required to mitigate the consequences of the specific event.

SRP Appendix 7.1-C, Subsection 5.1 addresses components and systems not qualified for seismic events or accident environments; non-safety-grade components and systems are assumed to fail to function if failure adversely affects safety system performance. Nonsafety-related components and systems are assumed to function if functioning adversely affects safety system performance. After assuming the failures of non-safety-grade, non-qualified equipment and those failures caused by a specific event, a random single failure is arbitrarily assumed. With these failures assumed, the safety system must be capable of performing the protective functions required to mitigate the consequences of the specific event. DCD Section 7.4.2.2 states that "all functions . . . including those used to achieve safe shutdown meet the single failure criterion." Insufficient information is provided to address DBEs, seismic events, and accident conditions.

ANSWER:

The PSMS is the only I&C system credited for safe shutdown. The PSMS meets the single failure criteria through multiple redundant and independence trains, which control multiple redundant and independent mechanical trains, as described in the Safety I&C TR, MUAP-07004 Section 4.1(b). The PSMS is completely isolated from all non-safety I&C systems, such that there are no failures in non-safety I&C systems that can adversely affect the PSMS, as described in the Safety I&C TR, MUAP-07004 Section 3.3(6). The redundancy of the mechanical systems credited for safe shutdown and the independence of these mechanical systems from the adverse affects of non-safety mechanical equipment will be described in Table 7.4-1, which will be revised according to RAI 07.04-8.

Impact on DCD

There is no impact on the DCD.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 227-2020 REVISION 0
SRP SECTION: 07.04 – SAFE SHUTDOWN SYSTEMS
APPLICATION SECTION: 07.04
DATE OF RAI ISSUE: 2/26/2009

QUESTION NO.: 07.04-10

Does the design and use of the systems for safe shutdown preclude the use of components that are common to redundant portions of the systems, such as common switches for actuation, reset, mode, or test; common sensing lines; or any other features which could compromise the independence of redundant portions of the safety systems?

Redundant portions of a safety system provided for a safety function shall be independent of and physically separated from each other to the degree necessary to retain the capability to accomplish the safety function during and following any design basis event requiring that safety function. DCD Subsection 7.4.2.4, Independence, states that

Redundant divisions of the RPS, ESFAS, SLS, and safety grade HSI, including those used to achieve safe shutdown, are independent from each other and from the nonsafety division. This independence is also applicable to redundant divisions of safety-related plant instrumentation and component controls for all safe shutdown functions.

This statement indicates physical, electrical, and communications independence within and between channels but does not provide any evidence to substantiate this claim. For example, does the safety system design preclude the use of components that are common to redundant portions of the safe shutdown system, such as common switches for actuation, reset, mode, or test; common sensing lines; or any other features which could compromise the independence of redundant portions of the systems used to achieve and maintain safe shutdown.

ANSWER:

Within the PSMS, which is the only I&C system credited for safe shutdown, there are no components that are common to redundant trains, such as common switches for actuation, reset, mode, or test, or any other features which could compromise the independence of the redundant trains.

Within the mechanical systems credited for safe shutdown, the main steam isolation valves and main feed water isolation valves are common to both redundant safe shutdown trains. Each valve has two separate and redundant solenoid operators which are assigned to separate trains.

Impact on DCD

There is no impact on the DCD.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 227-2020 REVISION 0
SRP SECTION: 07.04 – SAFE SHUTDOWN SYSTEMS
APPLICATION SECTION: 07.04
DATE OF RAI ISSUE: 2/26/2009

QUESTION NO.: 07.04-11

Is safety system equipment used to achieve safe shutdown functions qualified by type test, previous operating experience, or analysis, or any combination of these three methods? Discuss how these methods will substantiate will be capable of meeting, on a continuing basis, the performance requirements as specified in the design basis. Confirm that the qualification of Class 1E equipment is in accordance with the requirements of IEEE Std 323-1983 and IEEE Std 627-1980.

DCD Subsection 7.4.2.3, Quality of Components and Modules, states that

All functions of the RPS, ESFAS, SLS, and safety grade HSIS, including those used to achieve safe shutdown, are Class 1E, and meet all appropriate quality requirements. Class 1E plant instrumentation and component controls are provided for all safe shutdown functions.

IEEE Std 603-1991 requires that components and modules shall be of a quality that is consistent with minimum maintenance requirements and low failure rates. Safety system equipment shall be designed, manufactured, inspected, installed, tested, operated, and maintained in accordance with a prescribed quality assurance program (ANS/ASME NQA 1-1989). IEEE Std 603-1991 also requires that safety system equipment be qualified by type test, previous operating experience, or analysis, or any combination of these three methods, to substantiate that it will be capable of meeting, on a continuing basis, the performance requirements as specified in the design basis. It further requires that the qualification of Class 1E equipment shall be in accordance with the requirements of IEEE Std 323-1983 and IEEE Std 627-1980.

ANSWER:

The PSMS and other safety related plant components are credited to achieve safe shutdown. The Class 1E qualification of this equipment is described in DCD subsection 7.1.3.7, including conformance to IEEE 323-2003.

Impact on DCD

There is no impact on the DCD.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 227-2020 REVISION 0
SRP SECTION: 07.04 – SAFE SHUTDOWN SYSTEMS
APPLICATION SECTION: 07.04
DATE OF RAI ISSUE: 2/26/2009

QUESTION NO.: 07.04-12

Is the separation of Class 1E equipment used for safe shutdown in accordance with the requirements of IEEE Std 384-1981? Discuss the physical independence of the equipment used to achieve safe shutdown.

Physical independence is attained by physical separation and physical barriers. Equipment in other systems that is in physical proximity to safety system equipment, but that is neither an associated circuit nor another Class 1E circuit, shall be physically separated from the safety system equipment to the degree necessary to retain the safety systems' capability to accomplish their safety functions in the event of the failure of non-safety equipment. The separation of Class 1E equipment is typically in accordance with the requirements of IEEE Std 384-1981.

ANSWER:

All Class 1E classified equipment, including the redundant divisions of the PSMS which are credited for safe shutdown, are separated in accordance with IEEE 384-1992. The description of the conformance with IEEE Std 384-1992 will be added to Subsection 7.1.3.4.

Impact on DCD

The first paragraph of the Subsection 7.1.3.4 will be revised as follows;

Each train of the PSMS is independent from each other and from non-safety systems, including the PCMS. The physical independence is designed based on the RG 1.75 which endorses IEEE Std 384-1992. Electrical independence is maintained through qualified isolation devices, including fiber optic data communications cables. Functional independence between controllers is maintained through communication processors that are separate from function processors, and through logic that (1) ensures prioritization of safety functions over non-safety functions and (2) does not rely on signals from outside its own train to perform the safety function within the train.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 227-2020 REVISION 0
SRP SECTION: 07.04 – SAFE SHUTDOWN SYSTEMS
APPLICATION SECTION: 07.04
DATE OF RAI ISSUE: 2/26/2009

QUESTION NO.: 07.04-13

Confirm that the routing of signals related to achieving safe shutdown maintains (1) proper channeling through the communication systems, and (2) proper data isolation between redundant channels or alternatively, some form of data communication such that data from one channel cannot adversely affect the operation of another channel.

SRP Appendix 7.1-C addresses the transmission of signals between independent channels being through isolation devices. SRP BTP 7-11 addresses the application and qualification of isolation devices. SRP Appendix 7.0-A and SRP Section 7.9 addresses communications independence.

ANSWER:

Redundant divisions of the PSMS and redundant plant components are independent from each other and independent from non-safety divisions, including all data communications.

Impact on DCD

The first paragraph of Subsection 7.4.2.4 will be revised as follows;

Redundant divisions of the RPS, ESFAS, SLS, and safety grade HSI, including those used to achieve safe shutdown, are independent from each other and from the non-safety division. This independence is also applicable to redundant divisions of safety-related plant instrumentation and component controls for all safe shutdown functions as described in Subsections 7.1.3.4 and 7.1.3.5.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 227-2020 REVISION 0
SRP SECTION: 07.04 – SAFE SHUTDOWN SYSTEMS
APPLICATION SECTION: 07.04
DATE OF RAI ISSUE: 2/26/2009

QUESTION NO.: 07.04-14

Table 7.4-1, Component Controls for Shutdown, identifies components used for normal and/or safe shutdown. It is assumed then Safe Shutdown components are safety related and Normal Shutdown components may or may not be. Confirm that a logical or software malfunction of the non-safety system cannot affect the functions of the systems used to achieve a safe shutdown.

Where data communication exists between different portions of the safety system used for safe shutdown, a logical or software malfunction in one portion cannot affect the safety functions of the redundant portion(s). In addition, the SLS, RPS, and ESFAS are digital systems that have a communications link with the non-safety PCMS and DAS. Confirm that a logical or software malfunction of the non-safety system cannot affect the functions of the systems used to achieve a safe shutdown.

ANSWER:

The PSMS is physically separated and electrically isolated from all non-safety systems. Refer to DCD Subsection 7.1.3.4 and 7.1.3.5.

The data communication between the PSMS and non-safety systems meets the inter-division communication independence requirements of ISG-04. Safety control signals related to safe shutdown have higher priority than non-safety control signals. Refer to response to RAI 07.03-9.

As for affect of non-safety component malfunction, see the response to RAI 07.04-9.

Impact on DCD

There is no impact on the DCD.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 227-2020 REVISION 0
SRP SECTION: 07.04 – SAFE SHUTDOWN SYSTEMS
APPLICATION SECTION: 07.04
DATE OF RAI ISSUE: 2/26/2009

QUESTION NO.: 07.04-15

Table 7.4-1, Component Controls for Shutdown, identifies components used for normal and/or safe shutdown. It is assumed then Safe Shutdown components are safety related and Normal Shutdown components may or may not be safety related. MHI is requested to address the effects of a single random failure in a nonsafety system that can (1) result in a design basis event, and (2) also prevent proper action of a portion of the safe shutdown system designed to protect against that event, and the ability of the remaining portions of the safe shutdown system being capable of providing the safety function even when degraded by any separate single failure.

The safety system design shall be such that credible failures in and consequential actions by other systems shall not prevent the safety systems from meeting the requirements of IEEE Std 603-1991. That is, to address the effects of a single random failure, IEEE Std 603-1991 requires that where a single random failure in a nonsafety system can (1) result in a design basis event, and (2) also prevent proper action of a portion of the safety system designed to protect against that event, the remaining portions of the safety system shall be capable of providing the safety function even when degraded by any separate single failure. See IEEE Std 379-1988 for the application of this requirement.

ANSWER:

See the response to RAI 07.04-9. There are no non-safety components that can degrade the performance of the safe shutdown systems. Even though there are sensors shared between safety and non-safety systems, the Signal Selection Algorithm in the PCMS ensures a failed sensor does not result in a transient or accident condition.

Impact on DCD

There is no impact on the DCD.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 227-2020 REVISION 0
SRP SECTION: 07.04 – SAFE SHUTDOWN SYSTEMS
APPLICATION SECTION: 07.04
DATE OF RAI ISSUE: 2/26/2009

QUESTION NO.: 07.04-16

Address how the operational availability of each sensor will be tested and verified for the systems required to achieve and maintain safe shutdown.

DCD Subsection 7.4.2.5 states that "All functions of the RPS, ESFAS, SLS, and safety grade HSI, including those used to achieve safe shutdown, are periodically tested, as described in Subsection 7.1.3.14." DCD Subsection 7.1.3.14 however, only addresses testing or calibration from the sensor inputs to the actuated equipment or from the sensor to the analog to digital converter. The means for checking the operational availability of each sensor is not addressed.

SRP Appendix 7.1-C and IEEE Std 603-1991 require that means be provided for checking the operational availability of each sensor required for a safety function. For assuring the operational availability of each sense and command feature required during the post-accident period, one means could be checking the operational availability of sensors by use of the methods described in IEEE 603-1991, or by specifying equipment that is stable and retains its calibration during the post-accident time period

Also, the applicant/licensee should state the method to be used for checking the operational availability of non-indicating sensors. Tables 7.2-8 and 7.3-7 analyze sensor failures for Reactor Trip and ESFAS in the PSMS, its' effect, and method of failure detection. DCD Subsection 7.8.2.5 addresses failed sensors for the DAS.

ANSWER:

Safety related indications including sensors listed in Table 7.4-2 are applied to achieve and maintain safe shutdown. The detail description for checking the operational availability of all safety related functions of the PSMS are described in Sections 4.3, 4.4, and 4.5 of the Safety I&C TR, MUAP-07004. These overlapping tests confirm complete operability including the sensor, the HSI and the control functions.

Impact on DCD

The first paragraph of Subsection 7.1.3.14 will be revised as follows:

Testing from and including the sensors ~~inputs~~ of the PSMS through to and including the actuated equipment and HSI is accomplished in a series of overlapping sequential tests and calibrations.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 227-2020 REVISION 0
SRP SECTION: 07.04 – SAFE SHUTDOWN SYSTEMS
APPLICATION SECTION: 07.04
DATE OF RAI ISSUE: 2/26/2009

QUESTION NO.: 07.04-17

Address the capability of the RSR being able to accommodate a safety injection initiation during cooldown.

SRP Section 7.4 provides guidance for control in locations removed from the MCR that may be used for manual control and alignment of safe shutdown system equipment needed to achieve and maintain hot and cold shutdown. One item is that the remote shutdown capability should be capable of accommodating expected plant response following a reactor trip, including protective system actions that could occur as a result of plant cooldown. For example, in the cooldown of a PWR, reactor cooling system pressure will eventually drop below the safety-injection initiation setpoint. Because the MCR is not available, it may be impossible to block this trip. Therefore, the remote shutdown capability must be able to accommodate this condition.

ANSWER:

The RSR is equipped with the control of all equipment required for safe shutdown. The operating bypass of ECCS is listed on Table 7.4-1(sheet 3/3) as "ECCS Actuation Signal Block". All functions required for safe shutdown, including the operating bypass of ECCS, are performed by the PSMS and safety-related plant components. All PSMS controllers are located in Class 1E I&C rooms, which are electrically and physically isolated from both the MCR and RSR. Therefore, these functions are independent from the MCR, and can be controlled from the RSR. Therefore, if safety injection is required it can be manually actuated from the RSR. If safety injection actuates inadvertently, it can be controlled or terminated from the RSR.

Impact on DCD

The following will be added to the end of 7.4.1.5:

All safety functions are controlled by the PSMS. All PSMS controllers are located in Class 1E I&C rooms, which are electrically and physically isolated from both the MCR and RSR. Therefore, all functions of the PSMS, including safe shutdown functions, are independent from the MCR, and can be controlled from VDUs in the RSR. Therefore, if any PSMS function is required, including ESF, it can be manually actuated from the RSR. If any ESF function actuates inadvertently, it can be controlled or terminated from the RSR.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 227-2020 REVISION 0
SRP SECTION: 07.04 – SAFE SHUTDOWN SYSTEMS
APPLICATION SECTION: 07.04
DATE OF RAI ISSUE: 2/26/2009

QUESTION NO.: 07.04-18

Discuss the analog plant instrumentation and conventional component controls that are relied on for safe shutdown functions.

DCD Section 7.4.2.6 states that "All functions of the PCMS, used to achieve normal shutdown, and all functions of the RPS, ESFAS, SLS, and safety grade HSI, including those used to achieve safe shutdown, rely on digital systems, as described in Subsections 7.1.3.8 and 7.1.3.17. Analog plant instrumentation and conventional component controls are relied on for normal and safe shutdown functions."

ANSWER:

Only the sensor and output part of the PSMS are conventional analog equipment. All digital functions are continuously checked by channel check and self-testing. Sensors are manually checked through channel calibration and the output part is manually checked through the component actuation test. Manual tests and the Actuation Logic Test confirm the operability of all self-test functions.

Impact on DCD

There is no impact on the DCD.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 227-2020 REVISION 0
SRP SECTION: 07.04 – SAFE SHUTDOWN SYSTEMS
APPLICATION SECTION: 07.04
DATE OF RAI ISSUE: 2/26/2009

QUESTION NO.: 07.04-19

Address the relationship between DCD Section 7.4.1.6.2 and Table 7.4-1 for LOOP events.

All of the required functions for safe shutdown as shown in DCD Section 7.4.1.6.2 do not have automatic starts based on Table 7.4-1. For example, in a LOOP condition, the CCW and ESW pumps automatically start, as does the IAS instrument air compressor and the emergency power generator. Table 7.4-1, Component Controls for Shutdown, shows that the RHR pumps are used for safe shutdown but does not indicate an automatic start for LOOP conditions. Safety plant components are manually loaded on the non-safety alternate ac power source from the SLS during station blackout (which includes a loss of the Class 1E GTG Power Source).

ANSWER:

Automatic start function due to LOOP is described in Subsection 8.3.1. Manual loading in station blackout, refer to Section 8.4.

Section 7.4 describes the required function for safe shutdown after LOOP sequence. Safe shutdown is realized by manual action. In LOOP condition, necessary actions at first are automatically initiated, after that other actions are actuated manually.

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.

**Responses to Request for Additional Information No.238-2030
Revision 0**

**SRP Section 7.5
Information Systems Important to Safety**

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 238-2030 REVISION 0
SRP SECTION: 07.05 – INFORMATION SYSTEMS IMPORTANT TO SAFETY
APPLICATION SECTION: 07.05
DATE OF RAI ISSUE: 2/26/2009

QUESTION NO.: 07.05-1

MHI should state specifically if the design of the information systems important to safety are only "based on" and not in full compliance/conformance with cited requirements and guidance, the areas of exception need to be explicitly called out and justified. If compliance/conformance is intended, this should be stated.

The following sections begin with the indication that the design for the US-APWR is "based on" the requirements of codes, standards, and RGs rather than in compliance with those requirements and guidelines:

- 7.5.2.1 Post Accident Monitoring
- 7.5.2.2 Bypassed and Inoperable Status Indication
- 7.5.2.3 Plant Annunciators
- 7.5.2.4 Safety Parameter Displays System
- 7.5.2.5 [Emergency] Facilities

In addition, the specific PAM variables selected for the US-APWR are only described as being selected "based on" IEEE Std 497-2002 (as opposed to in compliance with). The areas of exception from IEEE Std 497-2002 need to be explicitly called out and justified.

ANSWER:

MHI will change "is based on" to "complies with". There is no exception to any applicable regulatory guides or industry standards.

Impact on DCD

The second paragraph in Subsection 7.5.1.1 will be revised as follows.

Safety-related PAM parameters are displayed on the safety VDUs, operational VDUs, and on the LDP. Non safety-related PAM parameters are displayed on operational VDUs. The parameters selected are ~~based on~~ comply with the guidelines of RG 1.97 (Reference 7.5-1). Display of at least two trains of each safety-related parameter is available.

The first sentence in Subsection 7.5.2.1 will be revised as follows.

The PAM design for the US-APWR ~~is based on~~ complies with the requirements of the following

codes, standards, and RGs:

The second sentence in Subsection 7.5.2.1 will be revised as follows.

IEEE Std 497-2002 contains functional and design requirements for accident monitoring instrumentation for nuclear plant. RG 1.97 endorses IEEE Std 497-2002. For the US-APWR, specific PAM variables ~~are selected based on~~ comply with the selection criteria described in IEEE Std 497-2002.

The first sentence in Subsection 7.5.2.2 will be revised as follows.

The BISI design for the US-APWR ~~is based on~~ complies with the requirements of the following Codes, Standards and RGs:

The first sentence in Subsection 7.5.2.3 will be revised as follows.

The Plant Annunciators design for the US-APWR ~~is based on~~ complies with the following regulatory guidance:

The first sentence in Subsection 7.5.2.4 will be revised as follows.

The SPDS design for the US-APWR ~~is based on~~ complies with the requirements of the following codes, standards, and RGs:

The first sentence in Subsection 7.5.2.5 will be revised as follows.

The emergency response facility design for the US-APWR ~~is based on~~ complies with the requirements of the following codes, standards, and RGs:

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 238-2030 REVISION 0
SRP SECTION: 07.05 – INFORMATION SYSTEMS IMPORTANT TO SAFETY
APPLICATION SECTION: 07.05
DATE OF RAI ISSUE: 2/26/2009

QUESTION NO.: 07.05-2

Address conformance with BTP 7-13 as it relates to information systems important to safety.

DC-FSAR Table 7.1-2 does not cite conformance with BTP 7-13 for DC-FSAR Section 7.5; TRs MUAP-07004-P and MUAP-07005-P indicate that the methods used for periodically verifying the accuracy and response time of RTDs complies with this standard.

ANSWER:

See response to RAI 07.04-5.

Impact on DCD

There is no impact on the DCD.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No. 52-021

RAI NO.: NO: 238-2030 REVISION 0
SRP SECTION: 07.05 – INFORMATION SYSTEMS IMPORTANT TO SAFETY
APPLICATION SECTION: 07.05
DATE OF RAI ISSUE: 2/26/2009

QUESTION NO.: 07.05-3

Will the design of the US-APWR adhere to the variable definitions of IEEE Std 497-2002?

While Section 7.5.1.1 Post-Accident Monitoring indicates that IEEE Std 497-2002 provides principles relating to PAM variables, it does not explicitly indicate that the USAPWR will adhere to the variable definitions of IEEE Std 497-2002.

ANSWER:

MHI will add a clear statement about compliance with IEEE Std 497-2002. See also response to RAI 07.05-1.

Impact on DCD

There is no impact on the DCD.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 238-2030 REVISION 0
SRP SECTION: 07.05 – INFORMATION SYSTEMS IMPORTANT TO SAFETY
APPLICATION SECTION: 07.05
DATE OF RAI ISSUE: 2/26/2009

QUESTION NO.: 07.05-4

Are there any other functions that an operator can manually initiate from the operational VDU that are not addressed in Section 7.5.1.2.1? Is the list provided in Section 7.5.1.2.1 inclusive of all inoperable conditions?

Section 7.5.1.2.1 Design of Bypassed and Inoperable Status Indication, states that "Especially, with regard to certain items performed at least once per fuel cycle (i.e., 24 months while RG 1.47 recommends 'per one year'), the system level BISI is automatically initiated by a signal from the PSMS and is not removed by any method until the initiating signal is reset from the PSMS." RG 1.47 instead requires that all "inoperable condition can reasonably be expected to occur more frequently than once per year". The word "Especially" is not inclusive.

ANSWER:

MHI listed the planned inoperable conditions that automatically initiate BISI in Subsection 7.5.1.2.1. Manual initiation capability is also provided for conditions that do not automatically initiate BISI. As written, subsection 7.5.1.2.1 implies the list is only for the functions for which BISI is not automatically initiated. This subsection of the DCD will be revised to make these points clear.

Regarding frequency of planned bypass or deliberately induced inoperable conditions, RG 1.47 (May 1973) does not state that a frequency of once per year can be reasonably expected. Rather, RG 1.47 Clause C.3 says that if the frequency of each bypass or deliberately induced inoperable status is expected to occur more frequently than once per year, then automatic indication should be provided in the control room in accordance with Clauses C.1 and C.2. As stated in DCD Section 7.5.1.2.1, the BISI design accommodates indications for conditions that are expected at least once per fuel cycle (24 months), thus exceeding the requirements of RG 1.47.

Impact on DCD

The second paragraph of DCD Subsection 7.5.1.2.1 will be revised as follows:

~~Especially, w~~ With regard to certain items performed at least once per fuel cycle (i.e., 24 months while RG 1.47 recommends "per one year"), the system level BISI is automatically initiated by a signal from the PSMS and is not removed by any method until the initiating signal is reset from the PSMS. In addition to the automatic initiation conditions listed below, the operator can manually initiate the system level BISI ~~of related functions~~ from the operational VDU.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 238-2030 REVISION 0
SRP SECTION: 07.05 – INFORMATION SYSTEMS IMPORTANT TO SAFETY
APPLICATION SECTION: 07.05
DATE OF RAI ISSUE: 2/26/2009

QUESTION NO.: 07.05-5

MHI should address how CCF concerns are addressed in the PAM design for Type A, B, and C variables in Section 7.5.1.1.1.

Section 7.5.1.1.1 of the DC-FSAR states that “the process measurement channels are interfaced to redundant trains of the RPS. Component status signals are interfaced to redundant trains of the SLS. PAM information is then interfaced to redundant safety grade HSI and nonsafety HSI for display.” This section in the DC-FSAR further indicates that the PAM design ensures that at least one measurement is available after all credible single failures. However, the DC-FSAR does not discuss how common cause failure is addressed. Section 6.2, “Common Cause Failure,” of IEEE 497-2002 requires microprocessor-based sensors, data acquisition, or display equipment for Type A, B, and C variables to address CCF concerns, and also provides guidelines for addressing CCF. The measurement channels are interfaced to the RPS as well as display systems which may be microprocessor-based. This makes CCF concerns an issue.

ANSWER:

The US-APWR does not use microprocessor based sensors for any safety related application. Microprocessors are only used for control and HSI functions. CCF concerns are addressed in detail in Section 7.8 of the D3 TR, MUAP-07006, and in the D3 Analysis Technical Report (MUAP-07014). If a postulated CCF were to occur, all PAM indications associated with the PCMS and PSMS systems would be disabled. To cope with this failure mode, the Diverse Actuation System (DAS) includes a Diverse HSI Panel (DHP) that provides the diverse indications determined by the best estimate D3 analysis. The US-APWR complies with BTP 7-19 for coping with CCF. For this compliance the DHP provides diverse indications for variables needed to prompt credited manual operator actions (Type A variables) and variables to monitor critical safety functions (Type B variables). BTP 7-19 does not require diverse indications for monitoring fission product barriers (Type C variables).

Impact on DCD

Following sentences will be added after the last sentence in Subsection 7.5.1.1.1.

PAM parameters are displayed on the VDUs and LDP, supported by the PCMS and PSMS. If a software common cause failure (CCF) in the PCMS and PSMS were occur, they will be disabled including PAM indications on the VDUs and LDP. The diverse actuation system (DAS) provides the diverse actuation and indications to cope with this failure mode. Diverse

indications are provided on the diverse HSI panel (DHP). The variables indicated on the DHP are determined from the best estimate D3 analysis. The US-APWR complies with BTP 7-19 for coping with CCF. For this compliance the DHP provides diverse indications for variables needed to prompt credited manual operator actions (Type A variables) and variables to monitor critical safety functions (Type B variables). BTP 7-19 does not require diverse indications for monitoring fission product barriers (Type C variables). More detailed discussions are provided in Section 7.8, Topical Report MUAP-07006, and Technical Report MUAP-07014. Therefore, the indication for CCF is out of scope of the PAM design criteria. The DHP demonstrates that defense-in-depth exists against the consequences of a software CCF in the PCMS and PSMS systems that would disable PAM indications.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 238-2030 REVISION 0
SRP SECTION: 07.05 – INFORMATION SYSTEMS IMPORTANT TO SAFETY
APPLICATION SECTION: 07.05
DATE OF RAI ISSUE: 2/26/2009

QUESTION NO.: 07.05-6

MHI is requested to further describe in Section 7.5.1.1.1 or specific referenced section in the DC-FSAR, how the PAM system design meets the requirements of DI&C-ISG-04.

Clause 6.3, "Independence and Separation," of IEEE Std 497-2002 requires accident monitoring instrumentation channels for types A, B, and C variables to be independent and physically separated. Item (6) of Section 7.5.1.1.1 of the US-APWR DC-FSAR simply states that "electrical independence and physical separation are provided for all redundant trains." This information is inadequate to assess how the PAM design meets the independence requirement. For example, PAM information is interfaced to redundant safety grade HSI and nonsafety HSI for display. These HSI systems are computer-based, which is unlike a conventional control panel, where individual functions are separated. The Interim Staff Guidance DI&C-ISG-04, "Highly-Integrated Control Rooms—Communications Issues (HICRc)," provides guidance for addressing issues related to interactions among safety divisions and between safety-related equipment and equipment that is not safety-related. The DC-FSAR should provide more details regarding how the PAM system design meets the requirements of DI&C-ISG-04.

ANSWER:

There is not a unique PAM system and therefore not a unique communication method for PAM signals. The PAM functions are an integral part of the PSMS and PCMS, and therefore, the unit bus is applied for inter-divisional data communication. Safety-related PAM variables are interfaced between the safety and non-safety systems via the unit bus as illustrated in DCD Figure 7.5-1. The unit bus communication is fully described in the Safety I&C TR, MUAP-07004 and Platform TR, MUAP-07005 and in DCD Section 7.9. This design meets the requirements of DI&C-ISG-04.

Impact on DCD

Item (6) in Subsection 7.5.1.1.1 will be revised as follows.

(6) Independence and Separation: Electrical Independence and physical separation are provided for all redundant trains between redundant safety systems and between the safety and non-safety systems. Safety-related PAM variables are interfaced between safety system and non-safety system via the unit bus as illustrated in Figure 7.5-1. This design meets the requirements of DI&C-ISG-04. More detail for the unit bus is described in Subsection 7.9.1.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 238-2030 REVISION 0
SRP SECTION: 07.05 – INFORMATION SYSTEMS IMPORTANT TO SAFETY
APPLICATION SECTION: 07.05
DATE OF RAI ISSUE: 2/26/2009

QUESTION NO.: 07.05-7

Provide a summary of the analysis performed to demonstrate that the qualification of PAM equipment by the instrument OEM bounds the environmental conditions for the specific instrument location and required qualification duration. Also, provide a reference for the full report, if any.

Clause 7, "Qualification Criteria," of IEEE Std 497-2002 requires equipment qualification of accident monitoring instruments to be consistent with the assigned function of that variable during and following a design basis event or following a seismic event. Item (3), "Environmental Qualification," of Section 7.5.1.1.1 of the DC-FSAR states, in part, that PAM measurement channels are generically qualified by the instrument OEM, and that specific analysis by MHI for the US-APWR demonstrates that this qualification bounds the environmental conditions for the specific instrument location and required qualification duration. For Equipment Qualification issues, the staff needs the following details of this analysis to confirm the conclusions arrived at by MHI:

- Minimum levels of survivability
- Test method to be used
- Test Confirmation

ANSWER:

The qualification of instruments including PAM equipment is within the scope of DCD Section 3.11 and Technical Report MUAP-08015, "US-APWR Equipment Environmental Qualification Program". This reference will be added to DCD Subsection 7.5.1.1.1. Since PAM instruments are located in harsh environments, demonstrating qualification is covered in ITAAC of DCD Tier1.

Impact on DCD

The following sentence will be added after the last sentence of item (3) in Subsection 7.5.1.1.1.

The qualification of PAM equipment is the scope of Section 3.11 and Technical Report MUAP-08015, "US-APWR Equipment Environmental Qualification Program".

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 238-2030 REVISION 0
SRP SECTION: 07.05 – INFORMATION SYSTEMS IMPORTANT TO SAFETY
APPLICATION SECTION: 07.05
DATE OF RAI ISSUE: 2/26/2009

QUESTION NO.: 07.05-8

Provide an explicit explanation of the reasoning for the PAMs selections following DBAs, uncertainties associated with the sensors used, and show that given these uncertainties, the equipment will still perform its safety function following a DBA.

SRP Chapter 7, Section 7.5, Item D, requires that the accident monitoring instrumentation should be demonstrated to perform their intended function for severe accident protection. They need not be subject to additional 10 CFR 50.49 environmental qualification requirements; however, they should be designed so there is reasonable assurance that they will operate in the severe accident environment for which they are intended and over the time span for which they are needed.

To follow the guidance of Item D, the applicant needs to provide an explicit explanation of the reasoning for the PAM following DBAs, uncertainties associated with the sensors used, and show that based on these uncertainties, the PAM system will function as intended during and following a DBA. These discussions are not included in the DCFSAR, so the staff cannot verify that there is reasonable assurance that the PAM will continue to operate during a severe accident. The last sentence of Section 7.5.1.1, Post Accident Monitoring, of the DC-FSAR states that "Instrumentation for monitoring severe accidents is described in Section 19.2." As a minimum, a summary of how the PAM system design complies with Item D should be provided in this section of the DC-FSAR (i.e., Section 7.7), even if details are provided elsewhere.

**ANSWER:
Instrumentation for Severe Accidents**

Per DCD Subsection 7.5.1.1, instrumentation for monitoring severe accidents (SAs) is described in DCD Section 19.2. However, a more detailed description of the instruments required for SA monitoring is provided in Chapter 15 of PRA Technical Report, MUAP-07030.

Chapter 15 of the PRA Technical Report, MUAP-07030 identifies indications necessary to be available for severe accident conditions beyond DBA conditions (inside containment, after core damage).

The instrument channels that perform these indication functions will be designed to provide a reasonable level of confidence that they will operate in the severe accident conditions beyond DBA conditions. Instrument specifications will envelope the severe accident conditions described in

PAM Selection Basis for Design Basis Accident

The selection basis for the PAM variables is provided in this RAI response. The US-APWR PAM variables are selected based on Clause 4 of IEEE Std 497-2002. Each PAM variable is based on the required monitoring parameter for its associated accident condition function as described within the listed source documents as described in DCD Subsection 7.5.1.1 and Table 7.5-1. MHI is currently developing an Emergency Response Guidelines (ERG) document for the US-APWR for the purpose of supporting plant-specific Emergency Operating Procedures (EOPs) and Abnormal Operating Procedures (AOPs). The ERG document will identify the instrumentation used to support event- and function-based steps to support the development of plant-specific operating procedures. When these procedures are complete, they will be used to verify that the PAM list is complete. To further clarify the US-APWR PAM variable selection basis, Tables 07.05-8.1 through 07.05-8.5 show specific PAM variables and their required functions.

DCD Table 7.5-2 shows that the US-APWR PAM variable Types A, B, C, and D will be environmentally qualified to assure that the equipment performs its intended function under DBA induced environmental conditions. Sensors with uncertainties acceptable for operator manual action are used. A more detailed discussion of PAM instrument uncertainty is provided in the response to RAI Question 07.05-9.

Table 07.05-8.1 Function of Type A PAM Variables

Variable	Monitored Function or System	Required Function
Reactor Coolant Hot Leg Temperature (Wide Range)	Core Cooling	-SGTR Safety Analysis -RCS Depressurization based on EOPs in SGTR event
Reactor Coolant Cold Leg Temperature (Wide Range)	Core Cooling	
Reactor Coolant Pressure	-Core Cooling -Maintaining RCS Integrity	
Degrees of Subcooling	Core Cooling	
Pressurizer Water Level	Primary Coolant System	
Main Steam Line Pressure	Secondary System (SG)	
SG Water Level (Narrow Range)	Secondary System (SG)	-SGTR Safety Analysis -Manual action based on EOPs such as Safety injection termination in SGTR event
EFW Flow	Emergency Feedwater System	

Table 07.05-8.2 Function of Type B PAM Variables

Variable	Monitored Function or System	Required Function
Reactor Coolant Hot Leg Temperature (Wide Range)	Core Cooling	Assess process of accomplishing manual RCS cooling
Reactor Coolant Cold Leg Temperature (Wide Range)	Core Cooling	
Degrees of Subcooling	Core Cooling	
Pressurizer Water Level	Primary Coolant System	
Main Steam Line Pressure	Secondary System (SG)	
Reactor Coolant Pressure	-Core Cooling -Maintaining RCS Integrity	Assess process of manual RCS depressurization
SG Water Level (Wide Range)	Secondary System (SG)	Assess maintaining SG Heat Removal Function
SG Water Level (Narrow Range)	Secondary System (SG)	
EFW Flow	Emergency Feedwater System	
Wide Range Neutron Flux	Reactivity Control	-Assess maintaining sub-critical state -Monitoring neutron flux decreasing

		after reactor trip
Core Exit Temperature	-Core Cooling -Fuel Cladding	Assess maintaining Core Cooling
RV Water Level	Core Cooling	
Containment Pressure	-Maintaining RCS Integrity -Maintaining Containment Integrity	-Assess maintaining CV Integrity -Monitoring CV pressure response
Containment Isolation Valve Position (Excluding Check Valves)	Maintaining Containment Integrity	Assess the process of accomplishing or maintaining CV Isolation
Reactor Coolant Soluble Boron Concentration	Reactivity Control	Indicate boron concentration (sampling)
Refueling Water Storage Pit Water Level (Wide Range)	Safety Injection System	Verifying safety injection source
Refueling Water Storage Pit Water Level (Narrow Range)	Safety Injection System	
EFW Pit Water Level	Emergency Feedwater System	Verifying EFW source

Table 07.05-8.3 Function of Type C PAM Variables

Variable	Monitored Function or System	Required Function
Core Exit Temperature	-Core Cooling -Fuel Cladding	-Indicate potential for a breach of fission product barriers - Indicate an actual breach of fission product barriers
Radioactivity Concentration or Radiation Level in Circulating Primary Coolant	Fuel Cladding	Indicate an actual breach of fission product barriers
Containment High Range Area Radiation	Containment Radiation	

Table 07.05-8.4 Function of Type D PAM Variables

Variable	Monitored Function or System	Required Function
Reactor Coolant Hot Leg Temperature (Wide Range)	Core Cooling	Monitoring Long Term Core Cooling
Reactor Coolant Cold Leg Temperature (Wide Range)	Core Cooling	
Reactor Coolant Pressure	-Core Cooling -Maintaining RCS Integrity	
Degrees of Subcooling	Core Cooling	
Pressurizer Water Level	Primary Coolant System	
Main Steam Line Pressure	Secondary System (SG)	
RV Water Level	Core Cooling	
SG Water Level (Wide Range)	Secondary System (SG)	Monitoring Long Term SG Heat Removal
SG Water Level (Narrow Range)	Secondary System (SG)	
EFW Flow	Emergency Feedwater System	
EFW Pit Water Level	Emergency Feedwater System	
Wide Range Neutron Flux	Reactivity Control	Monitoring Long Term Reactor Shutdown State
Containment Pressure	-Maintaining RCS Integrity -Maintaining Containment Integrity	Monitoring CV Integrity
Containment Temperature	Containment Cooling Systems	
Containment Isolation Valve Position (Excluding Check Valves)	Maintaining Containment Integrity	Monitoring CV Isolation

CS/RHR Pump Discharge Flow	RHR or Decay Heat Removal System	Indicate performance of CV spray system
CS/RHR Pump Minimum Flow	RHR or Decay Heat Removal System	
Accumulator Pressure	Safety Injection System	Indicate performance of Accumulator
Accumulator Water Level	Safety Injection System	
Safety Injection Pump Discharge Flow	Safety Injection System	Indicate performance of Safety Injection system
Safety Injection Pump Minimum Flow	Safety Injection System	
Refueling Water Storage Pit Water Level (Wide Range)	Safety Injection System	
Refueling Water Storage Pit Water Level (Narrow Range)	Safety Injection System	
CCW Header Pressure	Cooling Water System	
ESW Header Pressure	Cooling Water System	Indicate performance of ESW system
Status of Standby Power and Other Energy Sources Important to Safety Class 1E ac Bus Voltage Class 1E dc Bus Voltage	Power Supplies	Verifying Energy Sources

Table 07.05-8.5 Function of Type E PAM Variables

Variable	Monitored Function or System	Required Function
MCR Area Radiation	Area Radiation	Monitor radiation and radioactivity levels in the control room and selected plant areas where access may be required for plant recovery
TSC Area Radiation	Area Radiation	
MCR Outside Air Intake Radiation	Airborne Radioactive Materials taken into MCR	
TSC Outside Air Intake Radiation	Airborne Radioactive Materials taken into TSC	
Plant Vent Radiation Gas Radiation (Including High Range)	Airborne Radioactive Materials Released from Plant	Monitor the magnitude of releases of radioactive materials through identified pathways
Main Steam Line Radiation	Airborne Radioactive Materials Released from Plant	
GSS Exhaust Fan Discharge Line Radiation (Including High Range)	Airborne Radioactive Materials Released from Plant	
Condenser Vacuum Pump Exhaust Line Radiation (Including High Range)	Airborne Radioactive Materials Released from Plant	
Plant Air Vent High Concentration Sampling System	Airborne Radioactive Materials Released from Plant Particulates and Halogens	
Airborne Radio Halogens and Particulates (Portable Sampling with Onsite Analysis Capability)	Enviorns Radiation and Radioactivity	Monitor radiation levels and radioactivity in the plant enviorns
Plant and Enviorns Radiation (Portable Instrumentation)	Enviorns Radiation and Radioactivity	
Plant and Enviorns Radioactivity (Portable Instrumentation)	Enviorns Radiation and Radioactivity	
Meteorological Parameters (Wind Direction, Wind Speed, Estimation of Atmospheric Stability)	Meteorology	Monitor the environmental conditions used to determine the impact of releases of radioactive materials through identified pathways

Impact on DCD

DCD will be revised to incorporate this RAI response.

DCD Subsection 7.5.1.1 will be revised as follows:

Instrumentation for monitoring severe accidents is ~~described~~ 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 reference to the PRA Technical Report MUAP-07030 will be added to DCD Subsection 7.5.5 as follows:

7.5-15 US-APWR Probabilistic Risk Assessment, MUAP-07030 (Proprietary) Revision 1, August 2008.

Also, the PAM selection basis and the tables for PAM type A, B, C, D, and E explained above will be added in DCD Subsection 7.5.1.1.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 238-2030 REVISION 0
SRP SECTION: 07.05 – INFORMATION SYSTEMS IMPORTANT TO SAFETY
APPLICATION SECTION: 07.05
DATE OF RAI ISSUE: 2/26/2009

QUESTION NO.: 07.05-9

MHI is requested to address the specific topics used in the assessment of the performance criteria for each of the PAMs variables in Section 7.5.

SRP 7.5, Item E identifies that, for systems developed in accordance with guidance of RG 1.97, Rev. 4, the review should confirm that the performance assessment fulfils the goals outlined in Clause 5.6, "Performance Assessment Documentation," of IEEE Std 497-2002. Clause 5.6 of IEEE Std 497-2002 recommends an assessment of the performance criteria for each of the PAM variables. While the DC-FSAR indicates that the PAM design for the US-APWR is based on the requirements of this standard, the Section 7.5 does not address the topics (calibration uncertainties, loop errors, and drift caused by environmental or seismic conditions during and after the postulated event) of Clause 5.6.

ANSWER:

The following assessment of performance criteria, as described in IEEE 497-2002, is provided:

(1) IEEE Std 497-2002, Clause 5.1, Range

The range of each PAM channel described in Table 7.5-3 of DCD Chapter 7 was established to ensure that it covers the anticipated operational occurrences (AOOs) and postulated accidents (PAs). Instrument ranges were developed per the US-APWR system design and safety analysis, and have been confirmed to be consistent with similar instruments in operating plants. Instrument ranges are confirmed again during development of the Emergency Response Guidelines (ERGs). Validation of the complete HSI, including instrument indicators and Emergency Operating Procedures (EOPs) will be conducted during Phase 2b of the HFE program.

(2) IEEE Std 497-2002, Clause 5.2, Accuracy

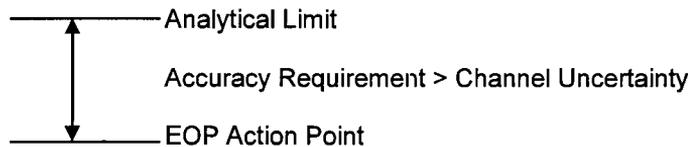
The required accuracy of each PAM channel is established according to how the indication is to be used by control room personnel and is established in accordance with Annex A of IEEE 497-2002, which divides accuracy requirements into two groups.

The first group consists of those variables, that support credited manual actions and where the corresponding channel accuracy is specified in the accident analysis or licensing basis. These are the Type A PAM variables listed in Table 7.5-3.

Table 07.05-9, attached, describes the analytical limits for manual actions based on PAM Type A

instrumentation, assumed in the Chapter 15 the Steam Generator Tube Rupture (SGTR) safety analysis. For safety analysis, the SGTR is the only event that assumes Type A variables listed in Table 7.5-3. Operator actions required for other events are initiated by an alarm or they are based on a time limit. MHI is currently developing an ERG document for the US-APWR for the purpose of supporting plant-specific EOPs and Abnormal Operating Procedures (AOPs). The EOP action point and the accuracies will be determined during the development of the ERGs. The function and action are defined as important safety function, thus the setpoint methodology conforms to RG1.105 as same as other safety-related function.

The following figure graphically depicts the relationship between the analytical limit, the EOP Action Point, and channel uncertainty.



The second group consists of those variables that provide trend or plant stability information. In this case, it is of primary importance to know whether the variable is increasing, decreasing, or constant, and the exact value of the variable is only of secondary importance. All PAM variables, except for Type A variables, are categorized in this group. For linearly derived display instruments, the typical required accuracy is ± 20 percent or more. For logarithmic scale instruments, the typical required accuracy is ± 50 percent of the reading or alternatively plus/minus a half decade. Trend information for these variables is displayed on the operational VDUs as described in DCD Subsection 7.5.1.1.1 and Figures 7.5-1 and 7.5-2.

(3) IEEE Std 497-2002, 5.3 Response Time

A PAM channel is designed to provide real time and timely information. PAM signals are transmitted from the sensors to the VDUs through a digital control system. The response time between detection and indication is approximately one to three seconds. The update frequency is less than one second. Thus, the PAM channel has sufficient capability to provide real time and timely information.

(4) IEEE Std 497-2002, 5.4 Required Instrumentation Duration

The operating time for each variable required for DBA conditions is addressed in the development of the qualification program, per Section 3.11 and Technical Report MUAP-08015. The design basis accident analyses provide the basis for the required durations.

- a) The duration for Type A variables is determined from required operator action by the accident analysis and emergency procedure which duration is less than 4 months. All Type A variables are also other type. Therefore, the duration for Type A variables is required to be 4 months consistent with the duration for other type.
- b) The duration for Type B variables is at least the duration associated with the longest-duration design basis event for that variable; 4 months is required by the accident analyses and emergency procedure of the US-APWR.
- c) The duration for Type C variables is at least 100 days for instrument channels monitoring the fission product barriers; 4 months is required by the accident analyses and emergency procedure of US-APWR.
- d) The duration for Type D and E is 4 months as required by the accident analyses and emergency procedure.

A shorter duration may be acceptable if equipment replacement or repair can be accomplished within an acceptable out-of-service time, taking into consideration the location and accessibility of the equipment. When PAM instrumentation is located inside containment, is inaccessible, or cannot be repaired, replaced, recalibrated or equivalent indication cannot be obtained, the

required duration is 1 year.

(5) IEEE Std 497-2002, 5.5 Reliability

DCD Subsection 19.1.4.1.1, "Description of the Level 1 PRA for Operations at Power," states that for each component type and failure mode, the failure rates are extracted from available generic data sources. This section also makes two key assumptions related to component reliability:

- US generic data are applied for component reliability data
- US generic data are applied to component unavailability due to test and unplanned maintenance

The US-APWR PRA directly models instrument reliability using generic data, and the PRA is used to analyze the plant design to confirm that system reliability goals, such as those set for the maintenance rule, are acceptable. PAM instruments will be procured with sufficient reliability to be consistent with the generic reliability data used in the PRA, Chapter 7 of MUAP-07030. Therefore, assuring that system reliability goals are met.

Table 07.05-9 Analytical Limit for Operator Actions in SGTR Safety Analysis



Impact on DCD

Subsection 7.5.1.1.4 "Performance Design" will be added to incorporate this answer.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 238-2030 REVISION 0
SRP SECTION: 07.05 – INFORMATION SYSTEMS IMPORTANT TO SAFETY
APPLICATION SECTION: 07.05
DATE OF RAI ISSUE: 2/26/2009

QUESTION NO.: 07.05-10

MHI is requested to address the electrical independence and physical separation provided for all redundant trains and evaluates the potential for interaction between the BISI and other systems, preferably in Section 7.5.1.1.1.

In Item (6) of Section 7.5.1.1.1 of the DC-FSAR, only a single statement "Electrical independence and physical separation are provided for all redundant trains" is provided. The ability to assess the potential for interaction between the BISI and other systems cannot be made based on this sentence alone. Further details are needed in order to assess whether the Independence criterion is met. Also, Part one of D&IC-ISG-04, "Highly Integrated Control Rooms - Communication Issues," provides guidance on issues related to interactions among safety divisions and between safety-related equipment and equipment that is not safety-related.

ANSWER:

Criteria in Subection 7.5.1.1.1 are provided for the PAM function, not BISI. BISI functions are described in Subsection 7.5.1.2. BISI functions are provided from the status of PCMS and PSMS systems. BISI is a non-safety function implemented within the PCMS. The interface of BISI data signals from safety to non-safety systems uses the unit bus and therefore meets ISG-04 in the same manner as all other safety to non-safety data communications. Independence and physical separation are provided between redundant safety systems and between the safety and non-safety systems as described in Appendix A.5.6 and Appendix B.5.6 of the Safety I&C TR, MUAP-07004 and DCD Subsections 7.1.3.4 and 7.1.3.5.

Impact on DCD

A sentence will be added to Subsection 7.5.1.2.1 as follows.

BISI functions are provided from the status of PCMS and PSMS systems. BISI is a non-safety function implemented within the PCMS. The interface of BISI data signals from safety to non-safety systems uses the Unit Bus and therefore meets ISG-04 in the same manner as other safety to non-safety data communications. Independence and physical separation are provided between redundant safety systems and between the safety and non-safety systems.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 238-2030 REVISION 0
SRP SECTION: 07.05 – INFORMATION SYSTEMS IMPORTANT TO SAFETY
APPLICATION SECTION: 07.05
DATE OF RAI ISSUE: 2/26/2009

QUESTION NO.: 07.05-11

MHI should justify that the degree of redundancy, diversity, testability, and quality provided in annunciator systems is adequate to support normal and emergency operations.

SRP Section 7.5 states that "The applicant/licensee should justify that the degree of redundancy, diversity, testability, and quality provided in annunciator systems is adequate to support normal and emergency operations." DC-FSAR Section 7.5 does not address these issues for annunciator systems.

ANSWER:

The PCMS provides a highly reliable annunciator system for all alarms, including alarms to prompt manual operator actions that are credited in the Chapter 15 safety analysis. A more detailed description of the alarm system will be added to the DCD as shown below.

Impact on DCD

Subsection 7.5.1.5.1 will be added as follows.

7.5.1.5.1 Quality of Alarms

The reliability of all PSMS alarms is ensured based on the following design aspects:

- Redundancy is provided for all alarm HSI components including audible and visual devices to ensure no adverse affects by credible malfunctions.
- Separation between redundant segments is provided so that a failure in one segment does not result in the failure of both redundant segments.
- Testability is provided from self-diagnosis of MELTAC and HSI computers.
- An augmented qualification program is provided for alarms for credited related to SPDS.
- Similar environmental, seismic, and EMI/RFI specifications are provided as for the PSMS. Conformance testing differs with respect to the QA level and documentation.

The PCMS provides a highly reliable design for all audible and visual alarms. The reliability of alarms credited for manual action in the safety analysis is further ensured from the following additional design aspects.

- Prompts for credited manual operator actions are provided on PCMS non-safety VDUs and PSMS safety VDUs.

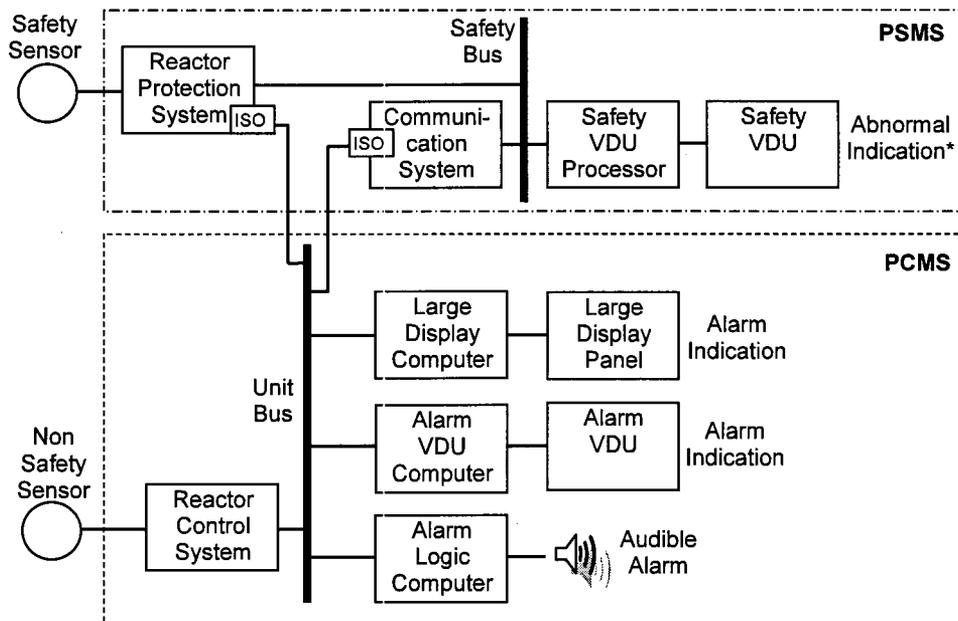
- The PCMS alarms for credited manual operator actions are developed through an augmented quality program, which includes software V&V.
- Diverse alarms from DHP address CCF in PSMS and/or PCMS.
- The parameters for credited manual operator actions are indicated on the safety VDU to accommodate degraded HSI conditions (i.e., loss of PCMS VDUs), since restricted, continued operation with complete loss of PCMS VDUs is within the US-APWR HSI design basis. Indications on the safety VDU are spatially dedicated and continuously visible (SDCV) and include alarm color coding. The safety VDUs provide notification of the plant accident condition to the operator in case of malfunction of the PCMS VDUs.

SECY-93-087 requires the annunciator to meet “applicable” requirements of Class 1E equipment, not all requirements. The intent is to ensure high reliability. Complete IEEE 603 conformance is not appropriate, since most aspects of IEEE Std 603-1991 pertain to the sense, command and execute features of the RPS and ESFAS. PCMS indications and alarms, together with safety VDU indications, provide a highly reliable HSI system to prompt credited manual operator actions.

The alarm system configuration including alarms credited for manual actions in safety analysis with safety sensors and non-safety sensors are shown in Figures 7.5-4. In addition to the sufficient reliable PCMS alarm, the parameters for credited manual operator actions are indicated on safety VDU to accommodate degraded HSI conditions (i.e., loss of PCMS VDUs). Restricted, continued operation with complete loss of PCMS VDUs is within the US-APWR HSI design basis. Indications on the safety VDU are spatially dedicated and continuously visible (SDCV), which enables notification of the plant accident condition to the operator in case of malfunction of PCMS VDUs.

PCMS indications and alarms, together with safety VDU indications, provide a highly reliable HSI system to prompt credited manual operator actions.

Figure 7.5-4 will be added as follows.



*1 Alarms to prompt credited manual actions in safety analysis are indicated on the safety VDU as abnormal indications.

Figure 7.5-4 Alarm System Configuration

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 238-2030 REVISION 0
SRP SECTION: 07.05 – INFORMATION SYSTEMS IMPORTANT TO SAFETY
APPLICATION SECTION: 07.05
DATE OF RAI ISSUE: 2/26/2009

QUESTION NO.: 07.05-12

The issues of diversity, common cause failures, software quality, etc. of digital systems for BISI and annunciators should be addressed by MHI in the DC-FSAR.

The issues of diversity, common cause failures, software quality, etc. for the digital aspects of the BISI and annunciator usage have not been addressed in the DC-FSAR. Additional information on the digital aspects of the BISI is required to assess this aspect.

ANSWER:

The BISI function and other alarms are implemented within the PCMS based on BISI signals and other alarm signals generated by the PSMS, PCMS or DAS. There is no diversity credited for the BISI functions or other alarm, except for alarms credited in the D3 coping analysis. There is no diversity requirement or requirement to address CCF for BISI or alarms, except for alarms credited in the D3 coping analysis. Diversity for the alarms used to prompt operator actions credited in the D3 coping analysis for coping with accidents and concurrent CCF is discussed in RAI 07.05-11 and the D3 TR, MUAP-07006. The software quality for BISI alarms is the same as for all PCMS functions; there are no special software quality requirements for BISI alarms.

Impact on DCD

There is no impact on the DCD.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 238-2030 REVISION 0
SRP SECTION: 07.05 – INFORMATION SYSTEMS IMPORTANT TO SAFETY
APPLICATION SECTION: 07.05
DATE OF RAI ISSUE: 2/26/2009

QUESTION NO.: 07.05-13

The mechanisms for achieving the isolation between the PSMS and the alarm systems and their independence should be address by MHI.

The DC-FSAR indicates that the data interface to the PSMS is physically and functionally isolated from the alarm system. However, the mechanisms for achieving this isolation are not described. Additional information is required to assess annunciator independence.

ANSWER:

See also the response to RAI 07.05-6.

The alarm systems are part of the PCMS or DAS. Subsection 7.1.3.4 of DCD describes the independence between PSMS and PCMS. Subsection 7.1.3.5 of DCD describes the isolation between PSMS and PCMS. Isolation between the PSMS and DAS is described in Subsection 7.8.2.3.

Also, communication isolation and independence between divisions is fully explained in the Safety I&C TR, MUAP-07004 and the Platform TR, MUAP-07005.

The alarm signals are an integral part of the PSMS and PCMS data communication, and therefore, the unit bus is applied for inter-division data communication. Signals from safety-related sensors used for alarms are interfaced between safety system and non-safety system via the unit bus. This signal configuration is as the same as the PAM signal configuration as illustrated in Figure 7.5-1. The unit bus communication is fully described in the Safety I&C TR (MUAP-07004) and Platform TR (MUAP-07005) and in DCD Section 7.9. This design meets the requirements of DI&C-ISG-04. More detail for the unit bus is described in DCD Subsection 7.9.1.

Configuration of general alarm signal pass will be added as a new figure.

Impact on DCD

The fourth paragraph in Subsection 7.5.1.3 will be revised as follows. The revision from the response to RAI 07.05-15 is also included.

Alarm annunciations are provided by the PCMS on the alarm VDUs and the LDP, and displayed on the operational VDUs. Safety-related sensors for alarms are interfaced between

safety system and non-safety system via the unit bus as illustrated in Figure 7.5-4. This communication meets the requirements of DI&C-ISG-04. More detail for the unit bus is described in Subsection 7.9.1. The alarm VDU computer and all alarm HSI components, including audible and visual devices, are redundant to ensure operation is not adversely affected by credible malfunctions. The alarm system integrity is checked by self-diagnosis which does not affect alarms and digital control system portion of alarms that have self-diagnosis functions. Alarm signals originate in plant instrumentation or within the controllers of the PCMS and PSMS. These signals are interfaced to the PCMS via the redundant unit bus, described in Section 7.9. The data interface to the PSMS is physically and functionally isolated so as not to affect the safety system in case of failure of the alarm system.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 238-2030 REVISION 0
SRP SECTION: 07.05 – INFORMATION SYSTEMS IMPORTANT TO SAFETY
APPLICATION SECTION: 07.05
DATE OF RAI ISSUE: 2/26/2009

QUESTION NO.: 07.05-14

The issue of annunciator reliability other than asserting that the system has a highly reliable design should be described in Section 7.5. Provide information about annunciator reliability in terms of diversity, testability, and quality.

The DC-FSAR indicates that the alarm VDU computer and all alarm HSI components are redundant. The DC-FSAR does not address the issue of annunciator reliability other than asserting that the system has a highly reliable design. Additional information is required to assess annunciator reliability in terms of diversity, testability, and quality.

ANSWER:

Annunciator redundancy and reliability is described in DCD Subsection 7.5.1.3. Also see the response to RAI 07.05-11 for more detail.

Impact on DCD

There is no impact on the DCD.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 238-2030 REVISION 0
SRP SECTION: 07.05 – INFORMATION SYSTEMS IMPORTANT TO SAFETY
APPLICATION SECTION: 07.05
DATE OF RAI ISSUE: 2/26/2009

QUESTION NO.: 07.05-15

MHI should address the self-testing of annunciators and address any potential interference of this testing with system operation.

Annunciator self-testing is not described in the DC-FSAR. If provided, additional information is required to assure that the self-testing would not interfere with proper system operation.

ANSWER:

Alarms are processed through the controller and data communication portions of the PCMS, which utilize MELTAC equipment, and through the HSIS portion of the PCMS, which utilizes MELCO MR computers. The self-diagnostics in the MELTAC portion of the PCMS is the same as in the PSMS. The self-diagnostics also provided in the HSIS portion of the PCMS (i.e., the MR computers). The self-diagnostics in MR computer occur during "time remaining" during normal operation without failure. Thus there is no interfere features by the MR self-diagnostics during normal operation without failure. When a failure occurs, the self-diagnostics identify the failure by the cut-in (interrupt processing) features.

The impact on the DCD from this RAI response has been included within the response to RAI 07.05-13.

Impact on DCD

There is no impact on the DCD.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 238-2030 REVISION 0
SRP SECTION: 07.05 – INFORMATION SYSTEMS IMPORTANT TO SAFETY
APPLICATION SECTION: 07.05
DATE OF RAI ISSUE: 2/26/2009

QUESTION NO.: 07.05-16

MHI should address annunciator compliance with IEEE 603-1991 in Section 7.5. Based on the list of accidents and credited manual actions provided in Table 7.5-5, the alarms redundancy, independence, reliability and self-testing should be addressed.

The SRM to SECY 93-087, II.T, states that "alarms that are provided for manually controlled actions for which no automatic control is provided and that are required for the safety systems to accomplish their safety functions, shall meet the applicable requirements for Class 1E equipment and circuits." The DC-FSAR indicates that the plant annunciator design is based on SECY-93-087, Item II.T, "Control Room Annunciator (Alarm) Reliability". Both a stronger commitment (i.e. is in full compliance as opposed to based on) and an explanation of how this commitment is carried out is required to approve the annunciator compliance with IEEE 603-1991. Section 7.5.1.3 states that "The highly reliable design of the alarm system makes it suitable for prompting operator attention to all abnormal plant conditions, including those requiring manual operator actions credited in the plant safety analysis. The alarms for credited manual operator actions are developed through an augmented quality program, which includes software V&V." Table 7.5-5 in the DC-FSAR provides a list of accidents and credited manual actions.

ANSWER:

See response to RAI 07.05-11.

Impact on DCD

There is no impact on the DCD.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No. 52-021

RAI NO.: NO. 238-2030 REVISION 0
SRP SECTION: 07.05 – INFORMATION SYSTEMS IMPORTANT TO SAFETY
APPLICATION SECTION: 07.05
DATE OF RAI ISSUE: 2/26/2009

QUESTION NO.: 07.05-17

Staff review of DCD Tier 2 (Rev 1), Section 7.5 indicates insufficient information is presented in regards to functional and design requirements of the post accident monitoring (PAM) for compliance with 10 CFR 50, Appendix A, GDC 13 and GDC 64; and 10 CFR 50.34(f)(2)(xvii). Section 7.2.5.1, states the PAM design is based on several codes, standards, and RGs to include IEEE Std 497-2002, RG 1.97 (Rev 4), and BTP 7-10. Please address the following items and revise the DCD to include this information, or justify their exclusion.

1. Table 7.5-3 (Sheet 2 of 3) has inconsistent and incomplete PAM variable names, ranges, and quantities.
 - (a) For clarity, identify those monitors from the process and effluent radiation monitoring and sampling systems (PERMS), area radiation monitoring system (ARMS), and airborne radioactivity monitoring system used as PAM in Table 7.5-3 with the same monitor number (e.g., RMS-RE-xxx) provided in Section 11.5 (for PERMS) and Section 12.3 (for ARMS and airborne radioactivity monitoring system).
 - (b) One Type E plant vent radiation gas monitor (including high range) to monitor airborne radioactive materials released from plant is listed in Table 7.5-3. In comparison, Table 11.5-3 of Section 11.5 lists 2 plant vent extended radiation gas monitors (RMS-RE-80A for accident mid range and RMS-RE-80B for accident high range) to monitor the concentration of radiation gas released through the plant vent in an accident. Address this discrepancy on PAM quantity for the Type E plant vent radiation gas monitor.
 - (c) One Type E condenser vacuum pump exhaust line radiation monitor (including high range) to monitor airborne radioactive materials released from plant is listed in Table 7.5-3. In comparison, Table 11.5-3 of Section 11.5 lists 2 condenser vacuum pump exhaust line radiation monitors (RMS-RE-81A for accident mid range and RMS-RE-81B for accident high range) to monitor the concentration of radiation gas released through the condenser vacuum pump in an accident. Address this discrepancy on PAM quantity for the Type E condenser vacuum pump exhaust line radiation monitor.
 - (d) One Type E GSS exhaust fan discharge line radiation monitor (including high range) to monitor airborne radioactive materials released from plant is listed in Table 7.5-3. In comparison, Table 11.5-3 of Section 11.5 lists 2 GSS exhaust fan discharge line radiation monitors (RMS-RE-82A for accident mid range and RMS-RE-82B for accident high range) to monitor the concentration of radiation gas in the gland steam in an accident. Address this discrepancy on PAM quantity for the Type E GSS exhaust fan discharge line radiation monitor.

- (e) One Type E MCR area radiation monitor with range of "1E-5 to 1 mR/hr" to monitor area radiation in the MCR is listed in Table 7.5-3. In comparison, Table 12.3-4 of Section 12.3 gives a nominal range of "1E-5 to 1E+0 R/h" for the MCR area radiation monitor (RMS-RE-1). Address this discrepancy on PAM range for the Type E MCR area radiation monitor.
 - (f) Four Type C containment high range area radiation monitors to monitor area radiation inside containment are listed in Table 7.5-3. Table 12.3-4 of Section 12.3 also lists 4 containment high range area radiation monitors that function to control containment ventilation isolation. Clarify the number of containment high range area radiation monitors with 8 detector numbers (RMS-RE-91A/B, RMSRE-92A/B, RMS-RE-94A/B, and RMS-RE-94A/B) listed in Table 12.3-4. In addition, Table 7.5-3 gives a range of "1 to 1E-7 R/hr" for the containment high range area radiation monitor. The staff believes this range should be "1E+0 to 1E+7 R/hr" as given in Table 12.3-4. Address this discrepancy on PAM range for the Type C containment high range area radiation monitors.
 - (g) One Type E TSC area radiation monitor with range of "1E-4 to 1 mR/hr" to monitor area radiation in the TSC is listed in Table 7.5-3. In comparison, Table 12.3-4 of Section 12.3 gives a nominal range of "1E-4 to 1E+1 R/h" for the TSC area radiation monitor (RMS-RE-9). Address this discrepancy on PAM range for the Type E TSC area radiation monitor.
 - (h) The PAM quantity for Type E plant and environs radiation (portable instrumentation) is not provided in Table 7.5-3. Provide the PAM quantity for Type E plant and environs radiation (portable instrumentation).
 - (i) The PAM quantity for Type E plant and environs radioactivity (portable instrumentation) is not provided in Table 7.5-3. Provide the PAM quantity for Type E plant and environs radioactivity (portable instrumentation).
2. Although Table 7.5-3 (Sheet 3 of 3) presents meteorological parameters as a PAM Type E variable, Table 7.5-1 does not list in the selection criteria the requirement to monitor environmental conditions used to determine the impact of releases of radioactive materials through identified pathways (e.g., wind speed, wind direction, and air temperature) as referenced in Section 4.5 b) of IEEE Std 497-2002.
- (a) Revise Table 7.5-1 to add the requirement to monitor environmental conditions to determine the impact of radioactive material releases through identified pathways such as wind speed, wind direction, and air temperature, etc. Provide information on where the monitored function for metrology is discussed in the DCD and how these site-specific Type E meteorological parameters for PAM are addressed by the COL applicant.
 - (b) Provide information on where the procedures presented as Type E source documents in Table 7.5-1 and in (a) mentioned above are discussed in the DCD and how these site-specific procedures for PAM are addressed by the COL applicant.

ANSWER:

1(a) The monitor number of the process monitor and area monitor is identified as following table.

PERMS and ARMS PAM Variable in Table 7.5-3		PERMS and ARMS Monitor Number in Ch 11 and Ch12
Variables	Quantity	
Radioactivity Concentration or Radiation Level in Circulating Primary Coolant	-(Sampling)	N/A (Sampling)
Containment High Range Area Radiation	4	RMS-RE-91A,B (one set), RMS-RE-92A,B (one set), RMS-RE-93A,B (one set), RMS-RE-94A,B (one set)
MCR Area Radiation	1	RMS-RE-1
TSC Area Radiation	1	RMS-RE-9
Plant Vent Radiation Gas Radiation (Including High Range)	1	RMS-RE-21A (normal range), RMS-RE-80A (accident mid range), RMS-RE-80B (accident high range)

Main Steam Line Radiation	1 per Line	RMS-RE-87 (A Loop), RMS-RE-88 (B Loop), RMS-RE-89 (C Loop), RMS-RE-90 (D Loop)
GSS Exhaust Fan Discharge Line Radiation (Including High Range)	1	RMS-RE-44A (normal range), RMS-RE-82A (accident mid range), RMS-RE-82B (accident high range)
Condenser Vacuum Pump Exhaust Line Radiation (Including High Range)	1	RMS-RE-43A (normal range), RMS-RE-81A (accident mid range), RMS-RE-81B (accident high range)
Plant Air Vent High Concentration Sampling System	-(Sampling)	N/A (Sampling)
Airborne Radio Halogens and Particulates (Portable Sampling with Onsite Analysis Capability)	-(Sampling)	N/A (Sampling)
Plant and Environs Radiation (Portable Instrumentation)	-	N/A (Portable Instrumentation)
Plant and Environs Radioactivity (portable instrumentation)	-	N/A (Portable Instrumentation)
MCR Outside Air Intake Radiation	1 of each type	RMS-RE-84A (Gas), RMS-RE-85A (Iodine), RMS-RE-83A (Particulate)
TSC Outside Air Intake Radiation	1 of each type	RMS-RE-101 (Gas), RMS-RE-102 (Iodine), RMS-RE-100 (Particulate)

(b), (c), (d) The plant vent radiation gas, condenser vacuum pump exhaust line, and GSS exhaust fan discharge line monitors each consist of two normal range monitors, one accident mid range monitor and one accident high range monitor. To function as a PAM variable, these monitors need one normal range, one accident mid range and one accident high range. Therefore, the quantity of each of these monitors as PAM is one.

(e) The "mR/hr" unit for this PAM variable is a typographic error; the correct unit is "R/hr". Therefore DCD Table 7.5-3 will be revised to correct the units for this PAM variable.

(f) It is too difficult to cover the measurement range of the containment high range area radiation monitor which is from 1E+0 R/hr to 1E+7 R/hr with one detector. The range is covered with two detectors; one covers the lower range and another covers the upper range, continuously. For that reason, the quantity of containment high range area radiation *monitors* as a variable in Table 7.5-3 is 4, and the quantity as *detectors* in Table 12.3-4 is 8. The "1E-7 R/hr" of upper limit in this PAM range is a typographic error; the correct upper limit is "1E+7 R/hr". Therefore DCD Table 7.5-3 will be revised to correct the range of this PAM variable.

(g) The "mR/hr" unit for this PAM variable is a typographic error; the correct unit is "R/hr". Therefore DCD Table 7.5-3 will be revised to correct the units for this PAM variable.

(h) The required quantity of type E plant and environs radiation monitoring as portable instrumentation is at least one. DCD Table 7.5-3 will be revised to add the quantity of this monitor.

(i) The required quantity of type E plant and environs activity monitoring as portable instrumentation is at least one. DCD Table 7.5-3 will be revised to add the quantity of this monitor.

2(a)

Table 7.5-1, Table 7.5-3, COL 7.5(1) and related descriptions in DCD Subsection 7.5.1.1 will be revised to incorporate the comments in QUESTION NO.07.05-17 item 2(a).

2(b)

The site-specific procedures for type E variables are to be developed by the COL applicant in accordance with the guidance provided in DCD Section 13.5.

Impact on DCD

The seventh paragraph in DCD Subsection 7.5.1.1 will be revised as follows:

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

COL 7.5(1) in Subsection 7.5.4 will be revised as follows:

COL 7.5(1) The COL applicant is to provide a description of site-specific PAM variables related to the or UHS.

Table 7.5-1 in DCD Section 7.5 will be revised as follows:

Table 7.5-1 Summary of PAM Variable Types and Source Documents

Variable Type	Selection Criteria for the Variable Type	Source Documents
A	<ul style="list-style-type: none"> - Planned manually controlled actions for accomplishment of safety-related functions for which there is no automatic control. 	<ul style="list-style-type: none"> - Plant accident analysis licensing basis - Emergency procedure guidelines (EPGs) or EOPs - Plant abnormal operating procedures (AOPs)
B	<ul style="list-style-type: none"> - Assess the process of accomplishing or maintaining plant critical safety functions. 	<ul style="list-style-type: none"> - Functional restoration EPGs or - Plant critical safety functions related EOPs - Plant critical safety function status trees
C	<ul style="list-style-type: none"> - Indicate potential for a breach of fission product barriers - Indicate an actual breach of fission product barriers 	<ul style="list-style-type: none"> - Plant accident analysis licensing basis - Design basis documentation for the fission product barriers - EPGs or EOPs
D	<ul style="list-style-type: none"> - Indicate performance of safety systems - Indicate the performance of required auxiliary support features - Indicate the performance of other systems necessary to achieve and maintain a safe shutdown condition - Verify safety system status 	<ul style="list-style-type: none"> - Plant accident analysis licensing-basis - Event specific EPGs or EOPs - Functional restoration EPGs or EOPs - Plant AOPs
E	<ul style="list-style-type: none"> - Monitor the magnitude of releases of radioactive materials through identified pathways - <u>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)</u> - Monitor radiation levels and radioactivity in the plant environs - Monitor radiation and radioactivity levels in the control room and selected plant areas where access may be required for plant recovery 	<ul style="list-style-type: none"> - Procedures for determining radiological releases through plant identified pathways <u>(See Note.)</u> - Procedures for determining plant environs radiological concentration <u>(See Note.)</u> - Procedures for determining plant habitability <u>(See Note.)</u>

Note: These site-specific procedures are to be developed by the COL applicant in accordance with the guidance provided in DCD Section 13.5.

Table 7.5-3 in DCD subsection 7.5 will be revised as follows:

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

Variable	Range	Monitored Function or System	Quantity	Type
Containment Temperature	32 to 428°F	Containment Cooling Systems	1	D
CCW Header Pressure	0 to 220 psig	Cooling Water System	1 per Line	D
ESW Header Pressure	Plant Specific	Cooling Water System	1 per Line	D
Status of Standby Power and Other Energy Sources Important to Safety <ul style="list-style-type: none"> ▪ Class 1E ac Bus Voltage ▪ Class 1E dc Bus Voltage 	0 to 9 kV ac 0 to 150 V dc	Power Supplies	1 per Bus 1 per Bus	D D
Radioactivity Concentration or Radiation Level in Circulating Primary Coolant	1/2 Tech Spec Limit to 100 Times Tech Spec Limit	Fuel Cladding	-(sampling)	C
Containment High Range Area Radiation ^{*2}	1 to 1E-+7 R/hr	Containment Radiation	4	C
MCR Area Radiation	1E-5 to 1 mR/hr	Area Radiation	1	E
TSC Area Radiation	1E-4 to 1E+1 mR/hr	Area Radiation	1	E
Plant Vent Radiation Gas Radiation ^{*5} (Including High Range)	5E-8 to 1E+5 µCi/cc	Airborne Radioactive Materials Released from Plant	1	E
Main Steam Line Radiation	1E-1 to 1E+3 µCi/cc	Airborne Radioactive Materials Released from Plant	1 per Line	E
GSS Exhaust Fan Discharge Line Radiation ^{*5} (Including High Range)	5E-8 to 1E+5 µCi/cc	Airborne Radioactive Materials Released from Plant	1	E
Condenser Vacuum Pump Exhaust Line Radiation ^{*5} (Including High Range)	5E-8 to 1E+5 µCi/cc	Airborne Radioactive Materials Released from Plant	1	E
Plant Air Vent High Concentration Sampling System	1E-3 to 1E+2 µCi/cc	Airborne Radioactive Materials Released from Plant Particulates and Halogens	-(sampling)	E
Airborne Radio Halogens and Particulates (Portable Sampling with Onsite Analysis Capability)	1E-9 to 1E-3 µCi/cc	Environs Radiation and Radioactivity	-(sampling)	E
Plant and Environs Radiation (Portable Instrumentation)	1E-3 to 1E+4 R/hr, photons 1E-3 to 1E+4 rads/hr, beta Radiations and low-energy photons	Environs Radiation and Radioactivity	- <u>At least 1</u>	E
Plant and Environs Radioactivity (portable instrumentation)	(Isotopic Analysis)	Environs Radiation and Radioactivity	- <u>At least 1</u>	E
MCR Outside Air Intake Radiation	1E-7 to 1E-2 µCi/cc (Gas) 1E-11 to 1E-5 µCi/cc (Iodine) 1E-12 to 1E-7 µCi/cc (Particulate)	Airborne Radioactive Materials taken into MCR	1 of each type	E

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

Variable	Range	Monitored Function or System	Quantity	Type
TSC Outside Air Intake Radiation	1E-7 to 1E-2 $\mu\text{Ci/cc}$ (Gas) 1E-11 to 1E-5 $\mu\text{Ci/cc}$ (Iodine) 1E-12 to 1E-7 $\mu\text{Ci/cc}$ (Particulate)	Airborne Radioactive Materials taken into TSC	1 of each type	E
Meteorological Parameters (Wind Direction, Wind Speed, Estimation of Atmospheric Stability)	N/A Site specific	Meteorology	1 for each	E

Note:

1. The number of quantity for Reactor Coolant Hot Leg Temperature (Wide Range) and Reactor Coolant Cold Leg Temperature (Wide Range) are one per loop because of having a diversity monitoring of each other.
2. An additional channel is assigned for a single failure concurrent with one channel unlimited instrument bypass for RT and ESF function, while the number of quantity required for Type A, B and C redundant PAM variables is two.
3. The number of quantity for SG Water Level (Wide Range) and EFW Flow is one per loop because of having a diversity monitoring function of each other.
4. CS Flow can be monitored to confirm the CS/RHR System Flow due to the sharing feature of RHR system and CS system flow line.
5. These monitors consist of two normal range monitors, one accident mid range monitor and one accident high range monitor. To function as a PAM variable, these monitors need one normal range, one accident mid range and one accident high range.

Impact on COLA

CP34 COL FSAR 7.5 will be revised to incorporate this response (i.e., the revision of COL item 7.5(1) of DCD).

Impact on PRA

There is no impact on the PRA.

**Responses to Request for Additional Information No.239-2033
Revision 0**

**SRP Section 7.6
Interlock Systems Important to Safety**

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

**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.: 07.06-1

Discuss compliance with 10 CFR 50, §50.34(f)(2)(v) and the indication of the status of safety interlocks being provided to operators. Update Table 7.1-2 if necessary.

The column titled "Related Section in US-APWR DCD" in Table 7.1-2 does not cite §50.34(f)(2)(v) as applicable to DCD Section 7.6. This column indicates that §50.34(f)(2)(v) is related to DCD Section 7.5, which states that the abnormal status of all interlocks for the US-APWR is provided via BISI. However, Section 7.5.2.2 only indicates that the BISI design is based on the requirements of §50.34(f)(2)(v); neither Sections 7.5 or 7.6 indicate that BISI for safety interlocks is provided to operators.

ANSWER:

DCD Sections 7.2, 7.3 and 7.6 will be added to Table 7.1-2 as reference of section to conform to 10 CFR 50, §50.34(f)(2)(v). Also the applicability of RG1.47 in Table 7.1-2 will be revised.

Impact on DCD

Item d. of Table 7.1-2 (Sheet 1 of 8) and item b. of Table 7.1-2 (Sheet 3 of 8) will be revised as Attachment 1.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

**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.: 07.06-2

Discuss how the design of interlock systems important to safety meets the requirements of GDCs 10, 15, 16, 28, 33, 34, 35, 38, 41 and 44, (See Table 7-1 of the SRP). Update Table 7.1-2 if necessary.

Table 7.1-2 in the DCD cites compliance with the following GDC for DCD Section 7.6: GDCs 1, 2, 4, 13, 19, 24 and 25; the DCD does not cite compliance with GDCs 10, 15, 16, 28, 33, 34, 35, 38, 41 and 44. The DCD refers to Chapter 4, "Reactor" for conformance with the GDC 10; Chapter 5, "Reactor Coolant System and Connected Systems" for conformance with the GDC 15 and 34; Chapter 6, "Engineered Safety Features" for conformance with the GDC 16, 35, 38 and 41; Chapter 9, "Auxiliary Systems" for conformance with the GDC 33 and 44; and Chapter 15, "Accident Analysis" for conformance with the GDC 28. It is unknown how GDCs 10, 15, 16, 28, 33, 34, 35, 38, 41 and 44 are applied to the design of interlock systems important to safety.

ANSWER:

Reference to these GDCs will be added in Table 7.2-1. GDC 41 is not related to interlock system described in Section 7.6.

Interlock systems important to safety are implemented in the PSMS. The PSMS, including the interlock systems important to safety, conforms to these GDCs, as the part of required systems in GDC. The setpoint methodology and response time methodology ensure adequate margin for the required systems. Compliance to these GDCs is demonstrated primarily through the Chapters 4, 5, 6, 9 and 15.

Impact on DCD

Applicability of GDCs 10, 15, 16, 28, 33, 34, 35, 38, 41 and 44 in Table 7.2-1 will be revised as Attachment 1.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

**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 discharge valves. Justification for the single train CS/RHR discharge valve interlock design is discussed in RAI 07.06-15.

Impact on DCD

There is no impact on the DCD.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

**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.: 07.06-4

Address the use of any digital-based controllers in safety I&C systems, including any COTS computer-based equipment. This would be applicable to stand alone PLCs or field mounted equipment used anywhere within the US-APWR applicable to equipment described in any chapters of the DCD, not just Chapter 7.

Although the BTP 7-18 is identified as applicable to interlock systems important to safety in SRP Table 7-1, the DCD, Table 7.1-2 indicates that it does not apply to the US-APWR because programmable logic controllers (PLC) are not used in safety I&C systems. It is unknown if computer-based controllers are used and embedded in plant systems and components. In addition, it is unknown if any COTS computer-based equipment are used. If computer-based equipment is embedded in plant systems and components, identify how their quality will be demonstrated.

ANSWER:

MELTAC is the only digital controller used in the US-APWR safety systems.

Impact on DCD

There is no impact on the DCD.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

**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.: 07.06-5

Identify those regulations applicable to the interlock systems important to safety, i.e., that are applicable to Section 7.6. Update Table 7.1-2 if necessary.

The DCD cites conformance with BTP 7-1 and BTP 7-2 only for the RPS and the SLS, and with BTP 7-12 only for the RPS, ESFAS and SLS. The DCD refers to Section 7.7 for BTP 7-5. The setup of Table 7-1 and inconsistencies between the I&C System columns and the column titled "Related Sections in the US-APWR DCD" prevents an understanding of how requirements and guidance is applied for the design of interlock systems important to safety.

ANSWER:

Table 7.1-2 shows which US-APWR systems are credited for conformance to the requirement. For the interlocks required by BTP 7-1 and 7-2, the RPS provides sensor monitoring and bistable functions, and the SLS provides the component level interlock logic. The interlocks required by BTP 7-5 are implemented entirely within the PCMS. The setpoint methodology defined in BTP 7-12 is applicable to the setpoints within the RPS, ESFAS and SLS. Therefore, no update to Table 7.1-2 is needed for interlocks. The applicable GDCs will be added in Section 7.6.

Impact on DCD

Following description will be added as the first paragraph in Subsection 7.6.2;

The interlock systems important to safety comply with the following codes and standards:

1. 10 CFR 50.55a(a)(1), "Quality Standards."7.6-3 Revision 5 - March 2007
2. 10 CFR 50.55a(h), "Protection and Safety Systems."
3. 10 CFR Part 50, Appendix A, General Design Criterion (GDC) 1, "Quality Standards and Records."
4. GDC 2, "Design Bases for Protection Against Natural Phenomena."
5. GDC 4, "Environmental and Dynamic Effects Design Bases."
6. GDC 13, "Instrumentation and Control."
7. GDC 19, "Control Room."
8. GDC 24, "Separation of Protection and Control Systems."
9. 10 CFR 50.34(f)(2)(v), "Additional TMI-Related Requirements, Bypass and Inoperable Status Indication"

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

**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.: 07.06-6

Provide a reference to a diagram that shows the valves, piping, and connections of the CS/RHR system that is referred to in Section 7.6.1.2, "CS/RHR Open Block Interlock," second paragraph of the first bulleted item.

In Section 7.6.1.2, "CS/RHR Open Block Interlock," second paragraph of first bulleted item, reference is made to the logic diagram for the interlocks for the valves. While the logic diagrams (Figs. 7.6-2 and 7.6-3) are important, the applicant should also make reference to where the piping diagram (showing the location of the valves, etc.) for the CS/RHR can be found. This will facilitate an understanding of the design and therefore an assessment of how the single failure criterion is met.

ANSWER:

Valve number and diagrams are below:
RHS-MOV-021A, B, C, D (Figure 5.4.7-2)
CSS-MOV-004A, B, C, D (Figure 6.2.2-1)
Reference to valve number and diagrams will be added.

Impact on DCD

The sentence shown below which refer the valve number and piping diagram will be added after the last sentence of second paragraph of first bulleted item in Subsection 7.6.1.2;

For RHS-MOV-021A, B, C, D, the piping diagrams for these valves are shown in Figure 5.4.7-2 in Chapter 5, and for CSS-MOV-004A, B, C, D in Figure 6.2.2-1 of Chapter 6.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

**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.: 07.06-7

Provide a reference to a diagram that shows the valves, piping, and connections of the CS/RHR system that is referred to in Section 7.6.1.2, "CS/RHR Open Block Interlock," second paragraph of the second bulleted item.

In Section 7.6.1.2, "CS/RHR Open Block Interlock," second paragraph of second bulleted item, reference is made to the logic diagram for the interlocks for the valves. While the logic diagrams (Figs. 7.6-1 and 7.6-3) are important, the applicant should also indicate where the circuit diagram (showing the layout and number of the valves, etc.) for the CS/RHR can be found. Provision of this information will facilitate an understanding of the design and therefore an assessment of how the single failure criterion is met.

ANSWER:

Valve number and diagrams are below:

RHS-MOV-001A, B, C, D (Figure 5.4.7-2)

RHS-MOV-002A, B, C, D (Figure 5.4.7-2)

CSS-MOV-004A, B, C, D (Figure 6.2.2-1)

Reference to valve number and diagrams will be added.

Impact on DCD

The sentence shown below which refer the valve number and piping diagram will be added after the last sentence of second paragraph of second bulleted item in Subsection 7.6.1.2;

For RHS-MOV-001A, B, C, D, the piping diagrams for these valves are shown in Figure 5.4.7-2 in Chapter 5, for RHS-MOV-002A, B, C, D in Figure 5.4.7-2 of Chapter 5, and for CSS-MOV-004A, B, C, D in Figure 6.2.2-1 in Chapter 6.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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.: 07.06-8

Provide a reference to a diagram that shows the valves, piping, and connections of the primary makeup water supply to the rest of the system that is referred to in Section 7.6.1.3, "Primary Makeup Water Line Isolation Interlock."

In Section 7.6.1.3, "Primary Makeup Water Line Isolation Interlock," second paragraph, reference is made to the logic diagram for the interlocks for the primary makeup water stop valves. While the logic diagram (Figs. 7.6-4) is important, the applicant should also make reference to where the piping diagram (showing the location and number of the valves, etc.) for the primary makeup water supply connections to the rest of the system can be found. Provision of this information will facilitate an understanding of the design and therefore an assessment of how the single failure criterion is met.

ANSWER:

Valve number and diagrams are below:

CVS-MOV-218 (Figure 9.3.4-1 (Sheet 4 of 7))

CVS-MOV-219 (Figure 9.3.4-1 (Sheet 4 of 7))

Reference to valve number and diagrams will be added.

Impact on DCD

The sentence shown below which refer the valve number and piping diagram will be added after the last sentence of second paragraph of Subsection 7.6.1.3;

For CVS-MOV-218, 219 the piping diagrams for these valves are shown in (Figure 9.3.4-1 (Sheet 4 of 7)) in Chapter 9.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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.: 07.06-9

Provide a reference to a diagram that shows the valves, piping, and connections of the CCW to the rest of the system that is referred to in Section 7.6.1.5, "CCW Supply and Return Header Tie Line Isolation Interlock."

In Section 7.6.1.5, "Primary Makeup Water Line Isolation Interlock," first paragraph below the bulleted items, reference is made to the logic diagram for the interlocks for the isolation valves. While the logic diagram (Figs. 7.6-6) is important, the applicant should also make reference to where the piping diagram (showing the location and number of the valves, etc.) for CCW and its connections to the rest system can be found. This will facilitate an understanding of the design and therefore an assessment of how the single failure criterion is met.

ANSWER:

Valve number and diagrams are below:

NCS-MOV-020A, B, C, D Figure 9.2.2-1 (Sheet 1 of 7)

NCS-MOV-007A, B, C, D Figure 9.2.2-1 (Sheet 2 of 7)

Reference to valve number and diagrams will be added.

Impact on DCD

The sentence shown below which refer the valve number and piping diagram will be added after the last sentence of first paragraph below the bulleted items of Subsection 7.6.1.5;

For NCS-MOV-020A, B, C, D the piping diagrams for these valves are shown in Figure 9.2.2-1 (Sheet 1 of 7) in Chapter 9, and for NCS-MOV-007A, B, C, D in Figure 9.2.2-1 (Sheet 2 of 7) of Chapter 9.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

**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.: 07.06-10

Provide a description of the quality processes used to develop the interlock systems important to safety, or provide a reference that points to the section within the DCD where the quality procedure for Class 1E systems is described.

Section 7.6.2.2, "Quality of Components and Modules," only states that "all interlocks important to safety are implemented using Class 1E components with a corresponding quality program." This statement is insufficient to assess the adequacy of the quality program used.

ANSWER:

The interlocks in Section 7.6 are Class 1E.

The interlocks are implemented within the PSMS. Quality for the PSMS is described in DCD Subsection 7.1.3.

Impact on DCD

There is no impact on the DCD.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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.: 07.06-11

Describe how the interlock systems conform to the interim staff guidance DI&C-ISG-04.

The DCD states that all interlocks important to safety are implemented in the Protection and Safety Monitoring System (PSMS), which is a digital system and also implements other safety functions. The DCD should therefore describe how the interlock systems conform to the interim staff guidance DI&C-ISG-04. The DI&C-ISG-04 guidance specifically addresses issues related to interactions among digital safety divisions and between safety-related equipment and equipment that is not safety-related. The guidance conforms to the principles in IEEE 603-1991 and IEEE 7-4.3.2-2003 by describing means for ensuring independence among redundant safety channels while permitting some degree of interconnection and commonality among those independent channels. Section 7.6.2.3, "Independence," of the DCD only states that "Redundancy and independent train assignments are specifically discussed for each interlock in the sections above."

ANSWER:

Subsection 7.6.1 describes function of important to safety and Figure 7.6-1 to 7.6-6 shows the interlocks. Conformance to the requirements of ISG-04 is described for all PSMS functions, including interlocks important to safety, in Subsection 7.1.3.4.

Impact on DCD

There is no impact on the DCD.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

**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.: 07.06-12

Describe how the interlock systems important to safety conform to the requirements of IEEE Std 603-1991, Clause 5.7, "Capability for Test and Calibration," Clause 5.8, "Information Displays," and Clause 6.5, "Capability for Testing and Calibration."

Item D of Chapter 7.6, "Interlock Systems Important to Safety," of the SRP, requires interlock system important to safety to conform to the requirements of IEEE Std 603-1991, Clause 5.7, "Capability for Test and Calibration," Clause 5.8, "Information Displays," and 6.5, "Capability for Testing and Calibration." Section 7.6.2.4, "System Testing and Inoperable Surveillance," of the DCD only indicates that system testing and inoperable surveillance for all interlocks is described in subsection 7.6.1 of the DCD. However, while subsection 7.6.1 describes the functions of all the interlocks important to safety, it does not describe how the systems conform to the applicable criteria. Section 7.6.2.4, "System Testing and Inoperable Surveillance," of the DCD only states that "System testing and inoperable surveillance for all interlocks is described in Subsection 7.6.1."

ANSWER:

The interlocks in Section 7.6 are Class 1E.

The interlocks are implemented within the PSMS. The PSMS conformance to IEEE Std 603, including testability and BISI, is described generically for all functions in Appendix A of the Safety I&C TR, MUAP-07004. Compliance to IEEE Std 603 is not described separately for each function of the PSMS.

Impact on DCD

There is no impact on the DCD.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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.: 07.06-13

Discuss how the interlock systems important to safety meet the requirements of IEEE Std 7-4.3.2.

The US-APWR interlock systems important to safety are implemented in the PSMS and therefore are digital-based systems. The DCD should therefore discuss how the interlock systems important to safety meet the requirements of IEEE Std 7-4.3.2. Section 7.6.2.5, "Use of Digital Systems," only states that "all interlock systems important to safety are implemented in the PSMS, which is a digital system." It does not address how the requirements of IEEE Std 7-4.3.2 are met, for example. Section 7.6.3, "Analysis," of the DCD does state that detailed compliance to the GDC, IEEE Std 603-1991 and IEEE Std 7-4.3.2-2003 are described in Topical Report MUAP-07004 Section 3.0, Appendix A and B. However, a summary of how the key, applicable criteria are met should be provided in the DCD, with a reference to the Topical Report MUAP-07004 made for any further details required. In Section 7.6.2.5, "Use of Digital Systems," of the DCD only states that "All interlocks important to safety are implemented in the PSMS, which is a digital system."

ANSWER:

The interlocks in Section 7.6 are Class 1E.

The interlocks are implemented within the PSMS. The PSMS conformance to IEEE Std 7-4.3.2, including life cycle processes and digital communication isolation, is described generically for all functions in Appendix B of the Safety I&C TR, MUAP-07004. Compliance to IEEE Std 7-4.3.2 is not described separately for each PSMS function.

Impact on DCD

There is no impact on the DCD.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

**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.: 07.06-14

Discuss whether or not the interlocks are software-based.

The US-APWR interlock systems important to safety are implemented in the PSMS and therefore are digital-based systems. It is not clear whether this means that (1) the interlock logic itself is implemented in software in the PSMS, or (2) only initiating signals originate from the PSMS but that the interlock logic is implemented using discrete components. Section 7.6.2.5, "Use of Digital Systems," of the DCD only states that "All interlocks important to safety are implemented in the PSMS, which is a digital system."

ANSWER:

Interlock signals are processed within software of digital I&C system. The DCD will be clarified to explain the digital processing functions.

Impact on DCD

Subsection 7.6.2.5 will be revised as follows:

All interlocks important to safety are implemented in the PSMS, which is a digital system. This includes sensor monitoring and bistable functions, and interlock logic. The final SLS output (i.e., open or close), which interfaces to the controlled plant component, reflects the result of combining all manual, automatic and interlock control signals.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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.: 07.06-15

Clarify how the guidance in Position 2 of Section B in BTP 7-1, "Guidance on Isolation of Low Pressure Systems from the High Pressure Reactor Coolant Systems," is met.

BTP 7-1 states that "for system interfaces where both valves are motor-operated, the valves should have independent and diverse interlocks to prevent both from opening unless the primary system pressure is below the subsystem design pressure. Also, the valve operators should receive a signal to close automatically whenever the primary system pressure exceeds the subsystem design pressure." In the discussion on the CS/RHR Pump Hot Leg Isolation Valve Open Permissive Interlock (Section 7.6.1.1), it is not clear how these requirements are met.

ANSWER:

The RHR system is able to withstand normal operating RCS pressure without rupture when both CS/RHR Pump Hot Leg Isolation Valves are inadvertently open, as explained in DCD Subsection 5.4.7.

This design is in consideration of intersystem LOCA in order to avoid either damage by overpressurization or the loss of integrity of the low-pressure system and possible radioactive releases. The RHR system is open to the refueling water storage pit (RWSP), which is located in the containment, so the water through these valves is discharged to the RWSP. This design is to prevent radioactive release outside the containment. Power is normally removed from the CS/RHR Pump Hot Leg Isolation Valves to ensure they cannot open inadvertently. (This design feature is described in Subsection 5.4.7.)

Additionally, temperature instruments are installed in the downstream of these valves to detect leakage. (Refer to Subsection 5.2.5)

The guidance in this BTP is intended to avoid either damage by overpressurization or the loss of integrity of the low-pressure system and possible radioactive releases. As described the above, the current design of RHR system has sufficiently high reliability against overpressurization or possible radioactive release, so this design meets the guidance of BTP 7-1.

As for automatical close interlocks, these valves do not receive a signal to close automatically since CS/RHR Pump Suction Relief Valve (RHS-VLV-003A, B, C, D) which are installed downstream of these valves are used for LTOP. The guidance in Position 10 of Section B in BTP

5-2 states that "If pressure relief is from a low-pressure system not normally connected to the primary system, interlocks that would isolate the low-pressure system from the primary coolant system should not defeat the overpressure protection function." In accordance with this guidance, these valves do not have an auto close interlock.

Impact on DCD

There is no impact on the DCD.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

**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. Recharging is a maintenance activity, which occurs only when the accumulator pressure 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

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.

**Responses to Request for Additional Information No.240-2035
Revision 0**

**SRP Section 7.7
Control Systems**

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 240-2035 REVISION 0
SRP SECTION: 07.07 – CONTROL SYSTEMS
APPLICATION SECTION: 07.07
DATE OF RAI ISSUE: 3/2/2009

QUESTION NO.: 07.07-1

Correct the inconsistencies between the columns "PCMS" and "Related Section in USAPWR DCD" in Table 7.1-2.

The control systems not required for the safety are provided by the PCMS as described in Section 7.7 in the DCD Tier 2. This review is based on the I&C system column "PCMS" and the column titled "Related Section in US-APWR DCD." Of the CFR requirements listed in SRP Table 7-1 as applicable to control systems not required for safety, Table 7.1-2 in the DCD Tier 2 cites compliance only with 10 CFR 52.47(b)(1) and 52.80(a) through a reference to Tier 1. Table 7.1-2 cites compliance with other 10 CFR sections for the PCMS but does not refer to Section 7.7 as a related section in the DCD in the column titled "Related Section in US-APWR DCD." Inconsistencies such as this prevent a through review of the regulatory requirements applicable to the PCMS.

ANSWER:

When the PCMS is credited for compliance to the "Applicable Criteria", the symbol "X" is indicated in the "PCMS" column of Table 7.1-2. When the "Applicable Criteria" is related to Section 7.7, the section number "7.7" is indicated in the "Related Section in US-APWR DCD" column of Table 7.1-2. The PCMS is applied not only for functions in Section 7.7, but also applied to functions of information systems important to safety in Section 7.5 and data communication systems in Section 7.9.

When the section number "7.7" is indicated in the "Related Section in US-APWR DCD" column of Table 7.1-2, the "Applicable Criteria" can refer to Section 7.7.

Impact on DCD

There is no impact on the DCD.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 240-2035 REVISION 0
SRP SECTION: 07.07 – CONTROL SYSTEMS
APPLICATION SECTION: 07.07
DATE OF RAI ISSUE: 3/2/2009

QUESTION NO.: 07.07-2

Discuss compliance with GDC 1 in relation to the PCMS. Update Table 7.1-2 if necessary.

GDC 1 sets the quality standards and records for SSCs important to safety. The DCD does not cite compliance with GDC 1 for the PCMS. Because the PCMS implements control functions not required for safety, GDC 1 is applicable in that the functions performed by the PCMS do not interfere with the safety-related functions. In addition, the control system must be appropriately designed and be of sufficient quality to minimize the potential for challenges to safety systems. Compliance with GDC 1 as it relates to control systems not required for safety and the PCMS is not indicated in Table 7.1-2, nor discussed in Section 3.1 of the DCD.

ANSWER:

GDC 1 is also applicable to the PCMS. Table 7.1-2 will be updated.

Impact on DCD

Item a. in Table 7.1-2 (Sheet 1 of 8) will be revised as Attachment 1.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 240-2035 REVISION 0
SRP SECTION: 07.07 – CONTROL SYSTEMS
APPLICATION SECTION: 07.07
DATE OF RAI ISSUE: 3/2/2009

QUESTION NO.: 07.07-3

Discuss compliance with GDC 10 in relation to the PCMS. Update Table 7.1-2 if necessary.

Table 7.1-2 in the DCD does not cite compliance with the GDC 10, but refers to Chapter 4, "Reactor" of the DCD Tier 2. Per Table 7-1 and Appendix 7.1-A of the SRP, GDC-10 is applicable to the PCMS. The staff reviewed the aforementioned chapter in the DCD and confirmed that compliance with the GDC 10 is cited. Section 3.1.2.1.1 addresses the reactor protection system setpoints being chosen to support design margins and that the protection and control systems are designed with appropriate margin to assure that acceptable fuel design limits are not exceeded during any condition of normal operation. Compliance with GDC 10 is not indicated in Table 7.1-2 and discussed in Section 3.1 of the DCD as it relates to the protection system and control system setpoints, and appropriate margin.

ANSWER:

GDC 10 is applicable to the PCMS regarding the appropriate setpoint margin. Table 7.1-2 will be updated.

Impact on DCD

The applicability of GDC 10 in Table 7.1-2 will be revised as Attachment 1.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 240-2035 REVISION 0
SRP SECTION: 07.07 – CONTROL SYSTEMS
APPLICATION SECTION: 07.07
DATE OF RAI ISSUE: 3/2/2009

QUESTION NO.: 07.07-4

Discuss compliance with GDC 15 in relation to the PCMS. Update Table 7.1-2 if necessary.

GDC 15 requires that the reactor coolant system and associated auxiliary, control, and protection systems be designed with sufficient margin to assure that the design conditions of the reactor coolant pressure boundary are not exceeded during any condition of normal operation, including anticipated operational occurrences." Compliance with the GDC 15 is not cited in Table 7.1-2 of the DCD, but a reference to Chapter 5, "Reactor Coolant and Connecting Systems" is made. The staff reviewed Chapter 5 and confirmed that conformance to the GDC 15 is cited in the document. Section 3.1.2.6.1 addresses the reactor protection system setpoints being chosen based on steady state and transient analyses in DCD Chapter 15 and that the protection and control systems are designed with appropriate margin to assure that the reactor coolant pressure boundary limits are not exceeded during any condition of normal operation. Compliance with GDC 15 is not indicated in Table 7.1-2 and discussed in Section 3.1 of the DCD as it relates to the protection system and control system setpoints and the reactor coolant pressure boundary limits.

ANSWER:

GDC 15 is applicable to the PCMS regarding the appropriate setpoint margin. Table 7.1-2 will be updated.

Impact on DCD

The applicability of GDC 15 in Table 7.1-2 will be revised as Attachment 1.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 240-2035 REVISION 0
SRP SECTION: 07.07 – CONTROL SYSTEMS
APPLICATION SECTION: 07.07
DATE OF RAI ISSUE: 3/2/2009

QUESTION NO.: 07.07-5

Discuss compliance with GDC 28 in relation to the PCMS. Update Table 7.1-2 if necessary.

GDC 28 requires that the reactivity control systems be designed with appropriate limits on the potential amount and rate of reactivity increase in the event of postulated reactivity accidents. Table 7.1-2 does not cite compliance with the GDC 28 but references Chapter 15. The staff reviewed the chapter and confirmed that compliance with the GDC 28 is cited; compliance is also cited in Chapter 16, Appendix B, "USAPWR Technical Specifications." Section 3.1.3.9.1 indicates that GDC 28 is applicable for the determination of protection system setpoints and that the reactivity control systems are designed with appropriate limits on the potential amount and rate of reactivity increase. Compliance with GDC 28 is not indicated in Table 7.1-2 and discussed in Section 3.1 of the DCD as it relates to the protection system and control system setpoints, and appropriate limits of reactivity and rate of increase.

ANSWER:

GDC 28 is applicable to the PCMS regarding the appropriate limits on the potential amount and rate of reactivity increase. Table 7.1-2 will be updated.

Impact on DCD

The applicability of GDC 28 in Table 7.1-2 will be revised as Attachment 1.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 240-2035 REVISION 0
SRP SECTION: 07.07 – CONTROL SYSTEMS
APPLICATION SECTION: 07.07
DATE OF RAI ISSUE: 3/2/2009

QUESTION NO.: 07.07-6

Discuss compliance with GDC 44 in relation to the PCMS. Update Table 7.1-2 if necessary.

GDC 44 requires that a system to transfer heat from structures, systems, and components important to safety to an ultimate heat sink (UHS) be provided. Table 7.1-2 does not cite GDC 44 as it relates to control systems not required for safety, but makes reference to Chapter 9, "Auxiliary Systems." The component cooling water system (CCWS) and the essential service water system (ESWS) provide heat transfer from plant safety-related components to the UHS. The staff reviewed Chapter 9 and confirmed that the safety design bases of both systems cite the GDC 44. Section 3.1.4.15.1 indicates that suitable leak detection will be provided. Compliance with GDC 44 is not indicated in Table 7.1-2 and discussed in Section 3.1 of the DCD as it relates to the protection system and control system setpoints, and leak detection.

ANSWER:

GDC 44 is applicable to the I&C system related to CCWS. Table 7.1-2 will be updated.

Impact on DCD

The applicability of GDC 44 in Table 7.1-2 will be revised as Attachment 1.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 240-2035 REVISION 0
SRP SECTION: 07.07 – CONTROL SYSTEMS
APPLICATION SECTION: 07.07
DATE OF RAI ISSUE: 3/2/2009

QUESTION NO.: 07.07-7

Discuss the discrepancy between the columns "PCMS" and "Related Section in US-APWR DCD" in DCD Table 7.1-2 with respect to the SRM to SECY 93-087.

SRP Table 7-1 identifies SRM to SECY 93-087 II.Q as providing acceptable guidance for defense against common-mode failures in digital systems for control systems not required for safety. SRM to SECY 93-087 II.T is acceptable guidance for control room annunciator reliability, although SRP Table 7-1 does not indicate that is applied specifically to control systems not required for safety (i.e., Section 7.7). DCD Table 7.1-2 indicates conformance with both parts of the SRM for the PCMS but does not indicate that it is applicable to Section 7.7 of the DCD in column titled "Related Section in USAPWR DCD".

ANSWER:

When the "Applicable Criteria" is applicable to PCMS, the symbol "X" is indicated in the "PCMS" column of Table 7.1-2. When the "Applicable Criteria" is related to Section 7.7, the section number "7.7" is indicated in the "Related Section in US-APWR DCD" column of Table 7.1-2.

The PCMS is related to the CCF and the alarm. The CCF issue with the SRM is fully described in Section 7.8. The alarm issue with the SRM is fully described in 7.5. Thus the Section "7.7" is not indicated in the "Related Section in US-APWR DCD" column of Table 7.1-2.

Impact on DCD

There is no impact on the DCD.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 240-2035 REVISION 0
SRP SECTION: 07.07 – CONTROL SYSTEMS
APPLICATION SECTION: 07.07
DATE OF RAI ISSUE: 3/2/2009

QUESTION NO.: 07.07-8

Discuss conformance with RG 1.105 in relation to the PCMS and the relationship between the normal trip setpoints and the safety-related trip setpoints. Update Table 7.1-2 if necessary.

RG 1.105 endorses Part 1 of ISA-S67.04-1994 and is used to determine the setpoints for safety-related instrumentation. SRP Table 7-1 and SRP Appendix 7.1-A, Section 4(g) indicate/state that RG 1.105 applies to all I&C systems. Table 7.1-2 in the DCD Tier 2 does not cite conformance with RG 1.105 for control systems not required for safety (i.e., the PCMS). RG 1.105 does apply to the PCMS in that it depicts the normal trip setpoint in relation to the safety-related trip setpoints.

ANSWER:

This RG is for safety function, not for non-safety function. Setpoints for non-safety functions will consider the uncertainties identified by the RG 1.105, but with nominal values that consider normal expected operating conditions. Portions of the RG 1.105 that pertain to trip limits and allowable values will not be applied. RG 1.105 may refer to the setpoint methodology for non-safety function, however, the conformance is not required. Therefore it is not necessary to update Table 7.1-2.

Impact on DCD

There is no impact on the DCD.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 240-2035 REVISION 0
SRP SECTION: 07.07 – CONTROL SYSTEMS
APPLICATION SECTION: 07.07
DATE OF RAI ISSUE: 3/2/2009

QUESTION NO.: 07.07-9

Discuss conformance with RG 1.152 in relation to the PCMS and the barriers between the PCMS and the PSMS to prevent interference. Update Table 7.1-2 if necessary.

RG 1.152 provides a basis for evaluating conformance of computers with GDC 21, and applies to all I&C safety systems and supporting data communication systems. RG 1.152, Rev. 2 endorses IEEE Std 7-4.3.2-2003 with reservations. Table 7.1-2 in the DCD Tier 2 does not cite conformance with RG 1.152. Clause 5.6(a) of IEEE Std 7-4.3.2-2003 states that "Barrier requirements shall be identified to provide adequate confidence that the nonsafety functions cannot interfere with the performance of the safety functions of the software or firmware. The barriers shall be designed in accordance with the requirements of this standard. The nonsafety software is not required to meet these requirements." RG 1.152 does apply to the PCMS in that it cannot interfere with the performance of the PSMS.

ANSWER:

RG 1.152 does not apply to PCMS. Per ISG-04, independence from PCMS failures must be assured by the safety system; the non-safety system cannot be credited. Therefore, no update will be made for Table 7.1-2 from this RAI.

Impact on DCD

There is no impact on the DCD.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 240-2035 REVISION 0
SRP SECTION: 07.07 – CONTROL SYSTEMS
APPLICATION SECTION: 07.07
DATE OF RAI ISSUE: 3/2/2009

QUESTION NO.: 07.07-10

Discuss conformance with RGs 1.168–1.171 in relation to the PCMS. Address the similarities and differences between the MELTAC Platforms for the PSMS and the PCMS. Update Table 7.1-2 if necessary.

Because the operating history of the MELTAC Platform used in the PCMS is used as a basis to provide information on any software errors to credit the reliability of the MELTAC Platform used in the PSMS, any similarities and differences between the platforms history and use must be well understood. RGs 1.169–1.171 apply to digital computer software used in safety systems of nuclear power plants. Note that RG 1.169 endorses IEEE Std 828-1990 that "also applies to non-critical software." Because the MELTAC Platform is used in the PSMS and the PCMS, these RGs (or similar Japanese regulations) were used in the development of the PCMS software; however, Table 7.1-2 does not indicate this.

ANSWER:

The development life cycle for the MELTAC platform, including its origination and operating history in non-safety applications and the differences in the life cycle process for safety and non-safety basic software, is fully described in the Platform TR, MUAP-07005. MHI has already responded to RAIs on this subject during the Staff's review of MUAP-07005. In addition, the NRC has audited all MELTAC software life cycle documentation in Arlington and Kobe.

As explained in Subsection 7.7.2.6, an augmented quality program is provided for a subset of the PCMS applications. This augmented quality program is based on industry standards, including the IEEE standards endorsed by RGs 1.168–1.171. While these standards are considered the basis of the PCMS augmented quality program, they are not required for the PCMS. Therefore, no update will be made for Table 7.1-2 from this RAI.

Impact on DCD

There is no impact on the DCD.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 240-2035 REVISION 0
SRP SECTION: 07.07 – CONTROL SYSTEMS
APPLICATION SECTION: 07.07
DATE OF RAI ISSUE: 3/2/2009

QUESTION NO.: 07.07-11

Discuss conformance with RGs 1.180 in relation to the PCMS and the emissions from nonsafety-related systems and their potential effect on safety systems. Update Table 7.1-2 if necessary.

RG 1.180 identifies electromagnetic environment operating envelopes, design, installation and test practices acceptable to the staff for addressing the effects of electromagnetic interference/radio frequency interference (EMI/RFI), and power surges on I&C systems and components important to safety. Table 7.1-2 in the DCD Tier 2 does not cite conformance with RG 1.180 for the PCMS, and references Sections 7.2 through 7.6 and Section 7.9 of the DCD Tier 2. The practices endorsed in RG 1.180 apply to both safety-related I&C systems and non-safety-related I&C systems whose failures can affect safety functions. While nonsafety-related systems are not part of the RG, 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 nonsafety-related systems should be held to the same levels as safety-related systems.

ANSWER:

The NRC established the basis of the susceptibility envelope defined in RG 1.180 based on a wide industry EMI survey. Since PCMS is the same hardware as PSMS (MELTAC Platform), it is reasonable to conclude that the PCMS does not introduce any extraordinary conducted or radiated emissions that would negate the basis of the susceptibility envelope established by RG 1.180 for safety systems. The similarity of the PCMS to the PSMS is described in the many portion of Chapter 7, as Subsections 7.1.3.8, 7.7.2.6, 7.7.2.8, 7.9.2.1, and 7.9.2.11. Therefore, conformance with RG 1.180, which is only for safety systems, is not required for the PCMS. Therefore, no update will be made for Table 7.1-2 from this RAI. The revision identified below, will be added to Subsection 7.1.3.7.

Impact on DCD

Following sentence will be added after the third paragraph of Subsection 7.1.3.7.

The susceptibility envelope defined in RG 1.180 is applicable to the US-APWR and therefore applicable to the PSMS, because the US-APWR does not include any extraordinary conducted or radiated emissions sources that are not included in operating nuclear power plants today.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 240-2035 REVISION 0
SRP SECTION: 07.07 – CONTROL SYSTEMS
APPLICATION SECTION: 07.07
DATE OF RAI ISSUE: 3/2/2009

QUESTION NO.: 07.07-12

Discuss conformance with RG 1.204 in relation to the PCMS, the isolation provided between the safety and nonsafety system, and potential interaction between the systems because of lightning. Update Table 7.1-2 if necessary.

RG 1.204 provides a basis for evaluating conformance of I&C systems and components to 10 CFR 50 and GDC 2. RG 1.204 provides guidance in the design and installation of lightning protection systems to assure that electrical transients resulting from lightning phenomena do not render I&C systems important to safety inoperable or cause spurious operation of such systems. Table 7.1-2 in the DCD Tier 2 does not cite conformance with RG 1.204 for the PCMS, and references Chapter 8, "Electrical Systems" of the DCD Tier 2. In general, nonsafety-related equipment does not fall under the guidelines presented in RG 1.204, but nonsafety-related equipment is included if its failure can impact the function and performance of safety-related equipment. The review based on RG 1.204 is to ensure that proper isolation exists between the PCMS and the PSMS such that a failure in the PCMS will not affect the PSMS.

ANSWER:

Electrical isolation is maintained between PSMS and PCMS as explained in Subsection 7.1.3.5. Therefore, credible electrical faults cannot propagate from the PCMS to the PSMS. In addition, the PCMS hardware is the same as that of the PSMS (MELTAC Platform), including EMI susceptibility design, as explained in Subsections 7.1.3.8, 7.7.2.6, 7.7.2.8, 7.9.2.1, and 7.9.2.11. Therefore, it is reasonable to conclude that there are no additional lightning induced PCMS failures that would be outside the boundaries of the safety analysis. Therefore, conformance with RG 1.180, which is only for safety systems, is not required for PCMS. Therefore, no update will be made for Table 7.1-2 from this RAI. The revision identified below, will be made to Subsections 7.1.3.5 and 7.1.3.16.

See also responses to RAI 07.01-21 and RAI 07.07-11.

Impact on DCD

The first paragraph of Subsection 7.1.3.5 will be revised as follows.

Physical separation and electrical isolation are provided between the PSMS redundant trains and between the PSMS and non-safety systems, including the PCMS. Isolation devices are incorporated into conventional interfaces, data links, and communication networks that connect

redundant trains, or carry signals to or from non-safety systems. The isolation devices ensure that credible faults, such as short circuits, open circuits, or the application of credible fault voltage do not propagate between systems. Chapter 8, Subsection 8.3.1.1.11 describes conformance to RG 1.204. This conformance bounds the credible electrical surges and faults that are considered for electrical isolation.

The first paragraph of Subsection 7.1.3.16 will be revised as follows.

Credible failures of the PCMS are bounded by the AOOs analyzed in the safety analysis, described in Chapter 15. These PCMS failures are described in Subsection 7.7.2.3. Chapter 8, Subsection 8.3.1.1.11 describes conformance to RG 1.204. This conformance bounds the envelope considered for PCMS EMI susceptibility. The PCMS uses the same hardware as the PSMS, which is qualified to RG 1.180. Therefore, additional lightning induced failures of the PCMS are precluded.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 240-2035 REVISION 0
SRP SECTION: 07.07 – CONTROL SYSTEMS
APPLICATION SECTION: 07.07
DATE OF RAI ISSUE: 3/2/2009

QUESTION NO.: 07.07-13

Discuss conformance with BTP 7-11 in relation to the PCMS and the isolation provided between the safety and nonsafety system. Update Table 7.1-2 if necessary.

BTP 7-11 provides guidelines for the use of electrical isolation devices to allow connections between redundant portions of safety systems or between safety systems and non-safety systems. BTP 7-11 deals with the criteria and methods used to confirm that the design of isolation devices assures that credible failures in the connected non-safety or redundant channels will not prevent the safety system from meeting their required functions. Table 7.1-2 in the DCD does not cite conformance with BTP 7-11 for the PCMS but does cite conformance with BTP 7-11 for the PSMS (i.e., RPS, ESFAS, LSL, and Safety HSI). Additionally, describe how the isolation devices used address the criteria in BTP 7-11.

ANSWER:

In accordance with Section B.3 of BTP 7-11, isolation devices are part of the safety system. Therefore, there is nothing within the PCMS that is credited for isolation of the safety systems. Therefore, PSMS conformance is sufficient; PCMS conformance to BTP 7-11 is not required.

No update will be made for Table 7.1-2 from this RAI.

Impact on DCD

There is no impact on the DCD.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 240-2035 REVISION 0
SRP SECTION: 07.07 – CONTROL SYSTEMS
APPLICATION SECTION: 07.07
DATE OF RAI ISSUE: 3/2/2009

QUESTION NO.: 07.07-14

Discuss conformance with BTP 7-12 in relation to the PCMS and the procedure used to establish setpoints. Update Table 7.1-2 if necessary.

BTP 7-12 provides guidelines for reviewing the process an applicant/licensee follows to establish and maintain instrument setpoints. Table 7.1-2 in the DCD Tier 2 does not cite conformance with BTP 7-12, but references Sections 7.2 through 7.6 and Section 7.9. The US-APWR will require a setpoint list identifying safety setpoints and non-safety setpoints for functions providing protective functions important to safety or that are relevant to conformance with technical specification limiting conditions for operation. In addition, a description of the setpoint methodology and procedures used in determining setpoints, including information sources, scope, assumptions, interface reviews, and statistical methods is needed. Table 7.1-2 in the DCD does not cite conformance with BTP 7-12 for the PCMS but does cite conformance with BTP 7-12 for the PSMS (i.e., RPS, ESFAS, and SLS).

ANSWER:

Refer to the answer of 07.07-08, regarding the setpoint methodology for the PCMS.

Impact on DCD

There is no impact on the DCD

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 240-2035 REVISION 0
SRP SECTION: 07.07 – CONTROL SYSTEMS
APPLICATION SECTION: 07.07
DATE OF RAI ISSUE: 3/2/2009

QUESTION NO.: 07.07-15

Discuss conformance with BTP 7-14 in relation to the PCMS. Update Table 7.1-2 if necessary.

BTP 7-14 provides guidelines for evaluating software life-cycle processes for digital computer-based I&C systems. Table 7.1-2 in the DCD Tier 2 does not cite conformance with BTP 7-14 for the PCMS, but references Sections 7.2 through 7.6 and Section 7.9. Because the MELTAC Platform is used in the PSMS and the PCMS, these BTP 7-14 was used in the development of the PCMS software; however, Table 7.1-2 does not indicate this. Table 7.1-2 in the DCD does not cite conformance with BTP 7-14 for the PCMS but does cite conformance with BTP 7-14 for the PSMS (i.e., RPS, ESFAS, and SLS).

ANSWER:

See also response to RAI 07.07-10. Although the PCMS software life cycle refers to the guidance of BTP 7-14, as previously discussed, the purpose of Table 7.1-2 is to identify the systems that are credited in the US-APWR for compliance to regulations and standards. Since BTP 7-14 is applicable only to safety systems, only the PSMS is credited for compliance. . Therefore BTP 7-14 will not be added to Table 7.1-2 for the PCMS.

Impact on DCD

There is no impact on the DCD.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 240-2035 REVISION 0
SRP SECTION: 07.07 – CONTROL SYSTEMS
APPLICATION SECTION: 07.07
DATE OF RAI ISSUE: 3/2/2009

QUESTION NO.: 07.07-16

Discuss conformance with BTP 7-17 and demonstrate that the self-test functions of the PCMS cannot either cause the PCMS to interfere with the functioning of the PSMS or themselves directly interfere with the functioning of the PSMS. Update Table 7.1-2 if necessary.

BTP 7-17 provides guidelines for reviewing the design of the self-test and surveillance test provisions. Table 7.1-2 in the DCD Tier 2 does not cite conformance with BTP 7-17 for the PCMS, but references Sections 7.2 through 7.6 and Section 7.9. Although the PCMS and PSMS both use the MELTAC Platform, the software and hardware are not identical between the systems. Conformance with BTP 7-17 and an associated review is to ensure that the PCMS is designed for in-service testability commensurate with the functions to be performed through all modes of plant operation and that the positive aspects of self-test features are not compromised by the additional complexity that may be added to the safety system by the self-test features. In addition, the review needs to assert that the hardware and software design support the required periodic testing. Table 7.1-2 in the DCD cites conformance with BTP 7-17 for the PSMS (i.e., RPS, ESFAS, and SLS) but does not cite conformance with the PCMS.

ANSWER:

The PSMS is completely isolated from the PCMS, including electrical and communications isolation. In addition, there are no safety functions of the PSMS that rely on any functions of the PCMS. Therefore, there are no functions of the PCMS, including its self-testing functions, that can adversely affect the safety functions of the PSMS. Therefore, conformance to BTP 7-17 is not required for the PCMS and no update will be made for Table 7.1-2.

Since the signal selection algorithm (SSA) is credited to ensure failures in the PSMS do not cause erroneous operation of the PCMS, a discussion of SSA testing will be added to Section 7.1.3.16, as shown below:

Impact on DCD

Following sentence will be added after the third paragraph of Subsection 7.1.3.16.

The SSA is continuously tested as follows:

- The PCMS employs the same self-test features as the PSMS. These features are described in Section 4.1.5 of Topical Report MUAP-07005.
- The basic software configuration and application software configuration, within the PCMS

controller, is periodically confirmed by the same manually initiated method described in Section 4.1.4.1.c of Topical Report MUAP-07005.

Since the SSA uses only digital values obtained from the PSMS via the unit bus, all functions of the SSA are completely covered by self-testing; no additional manual tests are required. The digital values obtained from the PSMS are confirmed during channel calibration for the safety sensors.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 240-2035 REVISION 0
SRP SECTION: 07.07 – CONTROL SYSTEMS
APPLICATION SECTION: 07.07
DATE OF RAI ISSUE: 3/2/2009

QUESTION NO.: 07.07-17

Discuss conformance with BTP 7-21 in relation to the PCMS and the real-time performance and architectures of the PSMS and PCMS, noting any differences and similarities. Update Table 7.1-2 if necessary.

BTP 7-21 provides guidelines for reviewing digital system real-time performance and system architectures in I&C systems. Table 7.1-2 in the DCD Tier 2 does not cite conformance with BTP 7-21 for the PCMS, but references Sections 7.2 through 7.6 and Section 7.9. To evaluate the performance and correctness expected of the actual plant, some of the criteria described BTP 7-21 may be met by submissions describing a software development process or verification methods that include real-time concerns. Although the PSMS and PCMS both use the MELTAC Platform, the limiting response times, digital computer timing requirements, architecture, design commitments, performance verification, and cyclic bases are not necessarily the same. The similarities, and differences, of the non-safety and safety platforms need to be identified and understood by the staff within the real-time performance criteria and the software development process. Table 7.1-2 in the DCD does not cite conformance with BTP 7-21 for the PCMS but does cite conformance with BTP 7-21 for the PSMS (i.e., RPS, ESFAS, and SLS).

ANSWER:

The digital computer real-time performance is fully applicable to digital safety system, but not applicable to digital non-safety system. For example the BTP 7-21 needs Limiting Response Times and Digital Computer Timing Requirements in the acceptance criteria. These acceptance criteria are only applicable to the safety system. Since there is no credit for non-safety system real time performance in the safety analysis, no update will be made for Table 7.1-2 from this RAI.

Impact on DCD

There is no impact on the DCD.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 240-2035 REVISION 0
SRP SECTION: 07.07 – CONTROL SYSTEMS
APPLICATION SECTION: 07.07
DATE OF RAI ISSUE: 3/2/2009

QUESTION NO.: 07.07-18

Address the discrepancies between the list of systems in the PCMS between DCD Section 7.7 and TR MUAP-07004-P(R1) Section 4.1.c.

The subsections of Section 7.7.1 in the DCD describe the US-APWR control functions that can affect the performance of critical safety functions. Section 4.1.c of TR MUAP-07004-P describes the major systems within the PCMS echelon. The system lists in the documents do not match:

- The DCD has a nuclear instrumentation system (Section 7.7.1.2) and an in-core instrumentation system (Section 7.7.1.5); TR MUAP-07004-P(R1) has an in-core nuclear instrumentation system (Section 4.1.c(5)).
- The DCD lists a Balance-of-Plant Control as a system (Section 7.7.1.6); TR MUAP-07004-P(R1) does not list a BOP system.
- The DCD lists a Turbine Protection Control (Section 7.7.1.9); TR MUAP-07004-P shows that protection and control are two different systems with different functions (Sections 4.1.c(6) and (8)).
- The DCD lists an auxiliary equipment control system (Section 7.7.1.12); TR MUAP-07004-P does not list this system as part of the PCMS.

The DCD does not list a generator transformer protection system and an AVR/ALR system as part of the PCMS; TR MUAP-07004-P(R1) has a generator transformer protection system (Section 4.1.c(11)) and an AVR/ALR system (Section 4.1.c(12)).

ANSWER:

The PCMS systems described in the Safety I&C TR, MUAP-07004 are typical MHI design. The PCMS systems described in the DCD are specific for the US-APWR design. The next revision of Section 4.1.c of the Safety I&C TR, MUAP-07004 will clarify that the systems are typical and that exact systems are described plant licensing documentation (e.g., the US-APWR DCD).

Impact on DCD

There is no impact on the DCD.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 240-2035 REVISION 0
SRP SECTION: 07.07 – CONTROL SYSTEMS
APPLICATION SECTION: 07.07
DATE OF RAI ISSUE: 3/2/2009

QUESTION NO.: 07.07-19

List the process control variables and discuss the automatic and manual control for each of these variables.

GDC 13 is applicable for control systems as it relates to instrumentation and controls provided to monitor variables over anticipated ranges for normal operations, AOOs, and accident conditions. Plant characteristics considered in a plant's Chapter 15 Safety Evaluation contain the following key plant parameters considered in the safety evaluation:

- core power,
- core inlet temperature,
- reactor system pressure,
- core flow, axial and radial power distribution,
- fuel and moderator temperature coefficient,
- void coefficient,
- reactor kinetics parameters,
- available shutdown rod worth, and
- control rod insertion characteristics.

Section 7.7.2 states that "The control systems for the US-APWR include the necessary features for manual and automatic control of process variables within the prescribed normal operating limits." A list and discussion of the process variables and their control is not provided in Section 7.7.

ANSWER:

Section 7.7 describes all process variables and controls. The process control parameters and the control method are summarized in Table 07.07-19, along with a reference to the appropriate section of the DCD, which provides a detailed description. Other items in the Staff's RAI are not controlled but are simply parameters which are based on calculated values. It is noted that core power is not directly controlled; it is indirectly controlled by controlling RCS temperature, which is included in Table 07.07-19.

Table 07.07-19 The Process Control Parameters and Control Method Description

Process control variables	How to control the process control variables
Reactor coolant average temperature (Tavg)	The Tavg is automatically controlled by the rod control function. (Refer to DCD Subsection 7.7.1.1.1)
Pressurizer pressure	The pressurizer pressure is automatically controlled by the pressurizer control function. (Refer to DCD Subsection 7.7.1.1.5)
Pressurizer water level	The pressurizer water level is automatically controlled by the pressurizer water level control function. (Refer to DCD Subsection 7.7.1.1.7)
Steam generator water level	The steam generator water level is automatically controlled by the steam generator water level control function. (Refer to DCD Subsection 7.7.1.1.9)
Steam header pressure	The steam header pressure is automatically controlled by the turbine bypass control function, when turbine bypass control is in steam header pressure control mode. (Refer to DCD Subsection 7.7.1.1.11)

Impact on DCD

Following table will be added in DCD Section 7.7.

Table 7.7-4 Process Control Parameters and Control Method Description

Process control variables	How to control the process control variables
Reactor coolant average temperature (Tavg)	The Tavg is automatically controlled by the rod control function. (Refer to DCD Subsection 7.7.1.1.1)
Pressurizer pressure	The pressurizer pressure is automatically controlled by the pressurizer control function. (Refer to DCD Subsection 7.7.1.1.5)
Pressurizer water level	The pressurizer water level is automatically controlled by the pressurizer water level control function. (Refer to DCD Subsection 7.7.1.1.7)
Steam generator water level	The steam generator water level is automatically controlled by the steam generator water level control function. (Refer to DCD Subsection 7.7.1.1.9)
Steam header pressure	The steam header pressure is automatically controlled by the turbine bypass control function, when turbine bypass control is in steam header pressure control mode. (Refer to DCD Subsection 7.7.1.1.11)

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 240-2035 REVISION 0
SRP SECTION: 07.07 – CONTROL SYSTEMS
APPLICATION SECTION: 07.07
DATE OF RAI ISSUE: 3/2/2009

QUESTION NO.: 07.07-20

Address by AOO failure modes other than random hardware failures that could be associated with digital systems such as software design errors.

The failure of any control system component or any auxiliary supporting system for control systems should not cause plant conditions more severe than those described in the analysis of AOOs in Chapter 15 of the DCD. The AOOs defined in the plant safety analysis considered in the control function design for the US-APWR are listed in Table 7.7-1 of the DCD. A review of Chapters 7 and 15 did not identify where any of the AOOs in its assessment of software design errors failure modes that could be associated with digital systems (the evaluations did consider random hardware failures.) (The evaluation of multiple independent failures is not intended by this question.)

ANSWER:

Section 5.1.8 of the Safety I&C TR, MUAP-07004, defines the control system failures that are considered in the safety analysis. These failures bound random single hardware failures and random single software failures. Single hardware or software failures can directly affect only the functions performed by a single controller group due to partitioning of functions into separate controller groups. The indirect affect of erroneous signals that interface between controller groups that may result from a single controller group failure, are also considered. The failures that must be considered in the safety analysis are only single failures. Design errors, which may exist within the software of multiple partitioned controllers are considered common cause failures, not single failures, and therefore are beyond the design basis of the safety analysis. The controller groups with control function assignments are listed in Table 7.7-2 as respect to the defense in depth.

Impact on DCD

There is no impact on the DCD.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 240-2035 REVISION 0
SRP SECTION: 07.07 – CONTROL SYSTEMS
APPLICATION SECTION: 07.07
DATE OF RAI ISSUE: 3/2/2009

QUESTION NO.: 07.07-21

Section 15.5.2.1 does not address control system failures as an initiator of a CVCS malfunction that increases RCS inventory yet Table 7.7-1 in the DCD indicates that this event is caused by a control system failure. Address this discrepancy.

Section 15.5.2.1 states that "A CVCS malfunction that increases RCS inventory can be caused by an operator error, a test sequence error, or an electrical malfunction. Based on the title of Table 7.7-1—AOOs due to control system failures—this event is caused by a control system failure. If a control system failure can cause a CVCS malfunction that increases RCS inventory, Section 15.5.2.1 should address this. If a control system failure cannot cause a CVCS malfunction that increases RECS inventory, MHI needs to clarify for this review.

ANSWER:

The words "electrical malfunction" used in Chapter 15 are meant to encompass all electrical systems, including control system failures.

Impact on DCD

There is no impact on the DCD.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No. 52-021

RAI NO.: NO. 240-2035 REVISION 0
SRP SECTION: 07.07 – CONTROL SYSTEMS
APPLICATION SECTION: 07.07
DATE OF RAI ISSUE: 3/2/2009

QUESTION NO.: 07.07-22

Freezing of instrument sensing lines is not addressed in Chapters 7 or 15. Discuss the design of the APWR and how it addresses items a-c below.

Environmental control systems that are credited in the safety analysis for the US-APWR are controlled by the PSMS, not the PCMS. Environmental control systems controlled by the PCMS, such as non-essential area HVAC, heat tracing, and/or forced air-cooling or heating, are considered in the failure analyses. Based on Regulatory Position 5 of RG 1.151, special considerations that should be addressed in the design and installation of instrument sensing lines provided in ISA-S67-02 should be supplemented with the following:

- a. Instrument sensing lines that can be exposed to freezing temperatures and that contain or can be expected to contain a condensable mixture or fluid that can freeze should be provided an environmental control system (heating and ventilation or heat tracing) to protect the lines from freezing during extremely cold weather.
- b. The environment associated with those instrument sensing lines in a. that are safety related should be monitored and alarmed so that appropriate corrective action can be taken to prevent loss of or damage to the lines from freezing in the event of loss of the environmental control system.
- c. The environmental control system recommended in a., and for which b. applies, should be electrically independent of the monitoring and alarm system so that a single failure in either system, including their power sources, does not affect the capability of the other system.

The environmental control and monitoring systems of a. and b. should be designed to standards commensurate with their importance to safety and with administrative controls that are implemented to address events or conditions that could render the systems inoperable.

ANSWER:

RG 1.151 requires the environmental control systems that prevent freezing in instrument sensing lines. The safety-related sensing lines of the US-APWR that can be exposed to cold weather condition meet the guideline of a, b, c, and d in section 5.2.2.4 of ISA-S67-02.

DCD Subsection 7.1.3.7 describes the conformance to RG 1.151. RG 1.151 endorses ISA-S67-02. Thus the ISA-S67-02 is also applicable to the US-APWR design. ISA-S67-02 will be added as the references.

Impact on DCD

The fifth paragraph in Subsection 7.1.3.7 will be revised as follows.

Instrument sensing lines are specified to be protected in compliance with RG 1.151 (Reference 7.1-11) which endorses ISA-S67-02, including freeze protection.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 240-2035 REVISION 0
SRP SECTION: 07.07 – CONTROL SYSTEMS
APPLICATION SECTION: 07.07
DATE OF RAI ISSUE: 3/2/2009

QUESTION NO.: 07.07-23

Address inadvertent actions caused via the touch screen VDUs and procedures/design in place to prevent/minimize such occurrences.

AOO 15.1.4 addresses the Inadvertent opening of a steam generator relief or safety valve. AOOs 15.5.1 and 15.5.2 address the inadvertent operation of ECCS and chemical and volume control system malfunction that increases reactor coolant inventory. MUAP-07007-P, *HSI System Description and HFE Process*, addresses touch size area for safety and operational VDUs. The reviewer cannot validate that inadvertent action, such as an unintended touch on a touch sensitive display cannot prevent the actuation of a safety function.

ANSWER:

The HFE TR, MUAP-07007, "HSI System Description and HFE Process" Subsection 4.5.3 a. describes "an HSI interlock function which requires double action for executing the operation in order to avoid erroneous manipulation." The interlock function will prevent inadvertent action, such as an unintended touch on a touch sensitive display cannot prevent the actuation of a safety function, and it complies with the latest Interim Staff Guidance on Highly-Integrated Control Rooms - Communications Issues (HICRc), September 28, 2007's STAFF POSITION for Section 3, MULTIDIVISIONAL CONTROL AND DISPLAY STATIONS, 5. Malfunctions and Spurious Actuations:.

In addition to features that prevent inadvertent touch actuation, the automated safety functions and interlocks have priority within the PSMS control logic over most manual commands, as described in the response to RAI 07.03-9. Therefore, manual commands (whether valid or inadvertent), cannot prevent the actuation of a safety function, except the pull-lock function. The pull-lock function has additional interlocks, as explained in the response to RAI 07.03-9.

Impact on DCD

There is no impact on the DCD.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No. 52-021

RAI NO.: NO. 240-2035 REVISION 0
SRP SECTION: 07.07 – CONTROL SYSTEMS
APPLICATION SECTION: 07.07
DATE OF RAI ISSUE: 3/2/2009

QUESTION NO.: 07.07-24

Address RG 1.152, Regulatory Position 2.7 and any techniques used to ensure that system security is intact, including the use of system logs, real time monitoring, and periodic testing.

RG 1.152, Regulatory Position 2.7 states that "The operation lifecycle process involves the use of the safety system by the licensee in its intended operational environment. During the operations phase, the licensee should ensure that the system security is intact by techniques such as periodic testing and monitoring, review of system logs, and real-time monitoring where possible." DCD 7.7 does not address any techniques used to ensure that system security is intact.

ANSWER:

Cyber security is described in Subsection 7.9.2.6. More detailed cyber security information including controls applicable to the plant's operating phase and the PCMS defensive layer is described in the US-APWR Cyber Security Program Technical Report, MUAP-08003. Although the PCMS defensive layer encompasses many of the cyber security requirements of RG1.152, since the PCMS does not perform a safety function, this regulatory guide is applicable only to the PSMS.

Impact on DCD

Following sentences will be added after the third paragraph in Subsection 7.7.2.10.

Cyber security control of the PCMS is described in Subsection 7.9.2.6.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No. 52-021

RAI NO.: NO. 240-2035 REVISION 0
SRP SECTION: 07.07 – CONTROL SYSTEMS
APPLICATION SECTION: 07.07
DATE OF RAI ISSUE: 3/2/2009

QUESTION NO.: 07.07-25

Address RG 1.152, Regulatory Position 2.8.2 and the use of periodic audits to determine the effectiveness of the digital safety systems security procedures.

RG 1.152, Regulatory Position 2.8.2 states that "The licensee's quality assurance group (such as information/network security expert) should conduct periodic audits to determine the effectiveness of the digital safety system security procedures." DCD Section 7.7 does not address the use of periodic audits to determine the effectiveness of the digital safety systems security procedures.

ANSWER:

The cyber security is described in Subsection 7.9.2.6. More detail cyber security information including the periodic audits is described in the US-APWR Cyber Security Program Technical Report, MUAP-08003. Although the PCMS defensive layer encompasses the cyber security audit requirements of RG1.152, since the PCMS does not perform a safety function, this regulatory guide is applicable only to the PSMS.

Impact on DCD

There is no impact on the COLA.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 240-2035 REVISION 0
SRP SECTION: 07.07 – CONTROL SYSTEMS
APPLICATION SECTION: 07.07
DATE OF RAI ISSUE: 3/2/2009

QUESTION NO.: 07.07-26

Address RG 1.152, Regulatory Position 2.8.3 and contingencies used for ensuring minimal disruption to critical services given various loss scenarios and undesirable operations of plant digital systems.

RG 1.152, Regulatory Position 2.8.3 states that "The licensee should develop an incident response and recovery plan for responding to digital system security incidents (e.g., intrusions, viruses, worms, Trojan horses, or bomb codes). The plan should be developed to address various loss scenarios and undesirable operations of plant digital systems, including possible interruptions in service due to the loss of system resources, data, facility, staff, and/or infrastructure. The plan should define contingencies for ensuring minimal disruption to critical services in these instances." DCD Section 7.7 does not address contingencies used for ensuring minimal disruption to critical services given various loss scenarios and undesirable operations of plant digital systems.

ANSWER:

The cyber security is described in Subsection 7.9.2.6. More detail cyber security information including the incident response and recovery plan is described in the US-APWR Cyber Security Program Technical Report, MUAP-08003. Although the PCMS defensive layer encompasses the cyber security incident response requirements of RG1.152, since the PCMS does not perform a safety function, this regulatory guide is applicable only to the PSMS.

Impact on DCD

There is no impact on the DCD.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 240-2035 REVISION 0
SRP SECTION: 07.07 – CONTROL SYSTEMS
APPLICATION SECTION: 07.07
DATE OF RAI ISSUE: 3/2/2009

QUESTION NO.: 07.07-27

Address RG 1.152, Regulatory Position 2.8.4 and periodic computer security self-assessments and audits, changes to safety systems, discovery of anomalies and corrective actions, and V&V of modifications as it relates to security.

RG 1.152, Regulatory Position 2.8.4 states that "The licensee should perform periodic computer system security self-assessments and audits, which are key components of a good security program. The licensee should assess proposed safety system changes and their impact on safety system security; evaluate anomalies that are discovered during operation; assess migration requirements; and assess modifications made including V&V tasks to ensure that vulnerabilities have not been introduced into the plant environment from modifications." DCD Section 7.7 does not address periodic computer security self-assessments and audits, changes to safety systems, discovery of anomalies and corrective actions, and V&V of modifications as it relates to security.

ANSWER:

The cyber security is described in Subsection 7.9.2.6. More detail cyber security information including the configuration control for changes is described in the US-APWR Cyber Security Program Technical Report, MUAP-08003. Although the PCMS defensive layer encompasses the cyber security self-assessment requirements of RG1.152, since the PCMS does not perform a safety function, this regulatory guide is applicable only to the PSMS.

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.

**Responses to Request for Additional Information No.228-2021
Revision 0**

**SRP Section 7.8
Diverse Instrumentation and Control Systems**

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 228-2021 REVISION 0
SRP SECTION: 07.08 – DIVERSE INSTRUMENTATION AND CONTROL SYSTEMS
APPLICATION SECTION: 07.08
DATE OF RAI ISSUE: 2/26/2009

QUESTION NO.: 07.08-1

A figure of the DAS should be provided in Section 7.8 of the DCD.

A complete description of DAS is provided in the TR *Defense-in-Depth and Diversity* (MUAP-07006-P, R2) with a figure of the DAS system architecture shown in Fig. 6.0-1. This figure provides needed insight into the design of the DAS and its interface with the PSMS.

ANSWER:

Reference to Figure 6.0-1 will be added to Section 7.8.

Impact on DCD

Following sentence will be added at the end of second paragraph of Section 7.8.

For a figure of the DAS system architecture, refer to Figure 6.0-1 of Topical Report Defense-in-Depth and Diversity, MUAP-07006-P.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 228-2021 REVISION 0
SRP SECTION: 07.08 – DIVERSE INSTRUMENTATION AND CONTROL SYSTEMS
APPLICATION SECTION: 07.08
DATE OF RAI ISSUE: 2/26/2009

QUESTION NO.: 07.08-2

Address the test, maintenance, surveillance, and calibration procedures for the DAS.

The DAS can be tested manually by injecting simulated input signals to confirm its function actuation setpoints, designed logic functions, and required system outputs. Spurious actuation from any one subsystem, during testing, is precluded by the system design of 2-out-of-2 logic that must be satisfied to generate an actuation signal. DAS output signals are tested to the inputs of the SLS power interface module. This testing overlaps with periodic testing of the SLS, which provides complete testing of all power interface module functions. SRP 7.8 states that for system testing and surveillance, the applicant/licensee should identify the test, maintenance, surveillance, and calibration procedures. These provisions should be consistent with the guidance of Generic Letter 85-06. The ATWS mitigation system should be testable at power (up to, but not necessarily including, the final actuation device).

ANSWER:

DAS has two subsystems and output of two subsystems is configured with 2-out-of-2. Therefore, one subsystem output does not actuate plant component. Therefore each subsystem can be tested separately at power.

[]

Since the description of DAS testing is generic to all DAS applications, it will be added to the Safety I&C TR, MUAP-07004 at the next revision.

Impact on DCD

There is no impact on the DCD.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 228-2021 REVISION 0
SRP SECTION: 07.08 – DIVERSE INSTRUMENTATION AND CONTROL SYSTEMS
APPLICATION SECTION: 07.08
DATE OF RAI ISSUE: 2/26/2009

QUESTION NO.: 07.08-3

Address the performance requirements for which credit is taken in the mitigation of design basis events (e.g., dynamic response, accuracy).

According to SRP 7.8, performance requirements should be identified. MHI performed a D3 analysis on the I&C system that assumes a CCF of the digital protection and control systems. Because the DAS is composed only of analog and discrete digital devices, it provides diversification from the digital safety I&C system; the analog DAS is unaffected by a software CCF and remains available to perform its intended function. The Defense-in-Depth and Diversity Coping Analysis (MUAP-07014) considers CCFs that result in a fail-as-is (i.e., fails to function) condition in the PSMS and PCMS concurrent with AOOs and PAs. The review should confirm that the applicant/licensee verifies conformance to these requirements by validation testing and surveillance. However, Section 7.8 of the DCD did not address any of these performance requirements for the diverse I&C system (i.e., DAS).

ANSWER:

As described in MHI Technical Report Defense-in-Depth and Diversity Coping Analysis, MUAP-07014, Section 4.4, Table 4.4-1, each of diverse reactor trips is assumed 10 seconds as time delay. The instrument accuracy for DAS is described in DCD Chapter 7, Section 7.8, and Table 7.8-6. These specifications are considered in the Technical Report MUAP-07014. Periodic surveillance is managed by Chapter 16, Technical Specifications.

Impact on DCD

There is no impact on the DCD.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 228-2021 REVISION 0
SRP SECTION: 07.08 – DIVERSE INSTRUMENTATION AND CONTROL SYSTEMS
APPLICATION SECTION: 07.08
DATE OF RAI ISSUE: 2/26/2009

QUESTION NO.: 07.08-4

Address the environment for the diverse I&C equipment.

Although MUAP-07006-P indicates that the diverse I&C system equipment as installed will be qualified for the environment that could exist during the events for which the equipment is assumed to respond and that the environment for the APWR I&C components is expected to be a mild environment, this is not addressed in the DCD.

ANSWER:

DHP is located in the MCR and DAACs are located in Class 1E Electrical Room. These are non hazard area. Descriptions to show DHP and DAACs location will be added to Section 7.8.

Impact on DCD

The first paragraph of Subsection 7.8.1.1 will be revised as follows;

The DHP, which is located in the MCR, consists of conventional hardwired switches, conventional indicators for key parameters of all critical safety functions, and audible and visual alarms. The DHP installed equipment is used for manual control and actuations credited in the defense in depth and diversity coping analysis. Actuation status of each safety system actuated from the DHP can be confirmed by monitoring the safety function process parameters displayed on the DHP. The DHP is powered by a non-Class 1E UPS and located in the MCR. Therefore the DHP is qualified as Seismic Category II.

Following paragraph will be added next to the last paragraph of Subsection 7.8.1.2;

The DAACs are located in separate Class 1E Electrical Rooms. Therefore the DAACs are Seismic Category II.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 228-2021 REVISION 0
SRP SECTION: 07.08 – DIVERSE INSTRUMENTATION AND CONTROL SYSTEMS
APPLICATION SECTION: 07.08
DATE OF RAI ISSUE: 2/26/2009

QUESTION NO.: 07.08-5

Address the setpoint methodology, calculation and reviews to be employed on the DAS setpoints.

BTP 7-12 is applicable to DAS which should be included as setpoint program. ISAS67.04-1994, Part I, Section states that as safety significance of various types of setpoints important to safety may differ, and thus a less rigorous setpoint determination method for certain functional units and limiting conditions of operation may be applied. The use of a graded approach allows a less rigorous setpoint determination method based on the safety significance of the instrument function. However, the grading technique chosen by the applicant/licensee should be consistent with the standard and should consider and bound all known applicable uncertainties regardless of setpoint application. Additionally, the application of the standard using a graded approach is also appropriate for non-safety system instrumentation maintaining design limits in the technical specifications.

ANSWER:

Diverse actuation system (DAS) is the non-safety I&C system. In Defense-in-Depth and Diversity Coping Analysis Technical Report, MUAP-07014, the DAS nominal setpoint is used for the coping analysis because the best estimate condition is assumed in this analysis. The DAS nominal setpoint considers DAS instrument uncertainty identified in BTP 7-12 to prevent DAS actuation before PSMS.

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.

**Responses to Request for Additional Information No.231-2037
Revision 0**

**SRP Section 7.9
Data Communication Systems**

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 231-2037 REVISION 0
SRP SECTION: 07.09 – DATA COMMUNICATION SYSTEMS
APPLICATION SECTION: 07.09
DATE OF RAI ISSUE: 2/26/2009

QUESTION NO.: 07.09-1

MHI is required to comply with 10 CFR 50.34(f)(2)(v) and 50.62 in relation to the DCSs. MHI is requested to discuss this in Section 7.9 and Table 7.1-2 should be updated to reflect this requirement.

Table 7.1-2 in the DC-FSAR cites compliance with various regulations applicable to the DCS with the exception of §50.34(f)(2)(v) and §50.62. §50.34(f)(2)(v) requires licensees to provide for automatic indication of the bypassed and operable status of safety systems. The DCSs support ATWS mitigation functions and RTS functions. The staff cannot determine if the DCS adequately supports RTS and ESFAS functions as necessary to sense accident conditions and AOOs in order to initiate protective actions consistent with the accident analysis presented in Chapter 15 of the DC-FSAR, without compliance with the above regulations known.

ANSWER:

Section 7.9 will be added to Table 7.1-2 as the conformance to §50.34(f)(2)(v). Refer to response to RAI 7.6-1.

Also the column "Safety DCS" will be added in Table 7.1-2 as one of I&C system.

Impact on DCD

The column "Safety DCS" will be added in Table 7.1-2 as Attachment 1.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 231-2037 REVISION 0
SRP SECTION: 07.09 – DATA COMMUNICATION SYSTEMS
APPLICATION SECTION: 07.09
DATE OF RAI ISSUE: 2/26/2009

QUESTION NO.: 07.09-2

MHI is requested to address compliance with GDC 24 in relation to the DCSs and the interfaces between the DCS and plant operating control systems in the DC-FSAR. This information will aid the staff in its determination that the system satisfies the requirements of IEEE Std 603-1991 with regard to control and protection system interactions. Update Table 7.1-2 if necessary.

SRP Table 7-1 and SRP 7.9 cite/discuss compliance with GDC 24. SRP 7.9 indicates that GDC 24 is applicable to all DCSs. This means that GDC 24 is applicable to data links (e.g., RPS/ESFAS links), the control network (e.g., within and between safety/nonsafety links), and the maintenance network. Section 3.1 of the DC-FSAR discusses compliance with GDC 24 but Table 7.1-2 does not cite compliance for data communications. To assess if the DCS satisfies the requirements of GDC 24, the staff requires sufficient information to evaluate the DCS and plant operating control systems and the interactions between the control and protection system interactions.

ANSWER:

Table 7.1-2 already indicates that GDC 24 is applicable to all I&C system. In addition Section "7.9", Data Communication Systems, is cited in the column of "Related Section in US-APWR DCD".

Therefore, no update will be made for Table 7.1-2 from this RAI.

All interfaces between the PCMS and PSMS, as described in previous sections of the DCD, are via the DCS. Compliance with GDC 24 is previously described for these interfaces.

Impact on DCD

There is no impact on the DCD.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 231-2037 REVISION 0
SRP SECTION: 07.09 – DATA COMMUNICATION SYSTEMS
APPLICATION SECTION: 07.09
DATE OF RAI ISSUE: 2/26/2009

QUESTION NO.: 07.09-3

MHI is requested to address in Section 7.9 of the DC-FSAR conformance with RG 1.47 in relation to the DCS, and the philosophy and criteria for bypass and inoperable status indication. Update Table 7.1-2 if necessary.

RG 1.47 describes an acceptable method of complying with the requirements of Appendix B to 10 CFR 50 with regard to indicating the inoperable status of a portion of the protection system. The design of the PSMS and ESFAS allows certain safety-related functions to be bypassed or made inoperable during the performance of periodic tests or maintenance. Experiences at operating plants indicate that when the measures used to indicate inoperable status consist solely of administrative procedures, the operator is not always fully aware of the ramifications of each bypassed or inoperable component. An acceptable way of aiding the operator's knowledge of plant status is to supplement administrative procedures with automatic indication of the bypass or inoperability of each redundant portion of a system that performs a function important to safety. The USAPWR allows bypassed or inoperable functions but it is unknown if the indication follows the guidance provided in RG 1.47.

ANSWER:

Sections 7.2, 7.3, 7.6 and 7.9 will be added in Table 7.1-2 as the conformance with RG1.47. Refer to response to RAI 7.6-1.

The DCS is used to transmit bypassed or inoperable conditions from the PSMS to the PCMS for BISI display on the LDP. But the DCS itself, is not monitored for bypassed or inoperable conditions because it is in continuous use, it is fully redundant within each division, and is not taken out of service for any planned periodic maintenance or tests.

Impact on DCD

There is no impact on the DCD.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 231-2037 REVISION 0
SRP SECTION: 07.09 – DATA COMMUNICATION SYSTEMS
APPLICATION SECTION: 07.09
DATE OF RAI ISSUE: 2/26/2009

QUESTION NO.: 07.09-4

MHI is requested to identify in Section 7.9 compliance with the guidelines of RG 1.204 in relation to the DCS, the isolation provided between the safety and nonsafety system, and potential interaction between the systems because of lightning. Update Table 7.1-2 if necessary.

RG 1.204 provides a basis for evaluating conformance of I&C systems and components to 10 CFR 50 and GDC 2. RG 1.204 provides guidance in the design and installation of lightning protection systems to assure that electrical transients resulting from lightning phenomena do not render I&C systems important to safety inoperable or cause spurious operation of such systems. Table 7.1-2 in the DC-FSAR Tier 2 does not cite conformance with RG 1.204 for the DCS. With respect to the DCS, the review is to ensure that proper communication and isolation exists between the PCMS and PSMS.

ANSWER:

See response to RAI 07.01-21. The part of the DCS, which is within the PSMS, is qualified to the requirements of RG 1.180. The MELTAC DCS hardware and software within the PCMS is the same as the MELTAC DCS hardware and software within the PCMS.

Impact on DCD

There is no impact on the DCD.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 231-2037 REVISION 0
SRP SECTION: 07.09 – DATA COMMUNICATION SYSTEMS
APPLICATION SECTION: 07.09
DATE OF RAI ISSUE: 2/26/2009

QUESTION NO.: 07.09-5

MHI is requested to address conformance with the SRM to SECY 93-087 II.Q and II.T in relation to the DCS; any potential common-mode failures; and the applicable EPRI requirements for redundancy, independence, and separation. This should be addressed in the DC-FSAR and update Table 7.1-2 if necessary.

Table 7.1-2 does not cite conformance with the SRM to SECY 93-087 in the DC-FSAR for the DCS. Section II.Q requires an evaluation of diversity and defense-in-depth and allows the use of a nonsafety system if the system is of sufficient quality. To demonstrate that vulnerabilities to common-mode failures have adequately been addressed and when analyzing each postulated common-mode failure for each event that is evaluated in the accident analysis section of the DC-FSAR requires consideration of DCS failures. Section II.T requires that the alarm system meet the applicable EPRI requirements for redundancy, independence, and separation.

ANSWER:

The CCF issue of SRM to SECY 93-087 II.Q is fully described in Section 7.8. In summary, the DCS is assumed to fail due to CCF. Therefore, the DCS is not credited in coping with CCF conditions.

The alarm issue of SRM to SECY 93-087 II.T is fully described in 7.5. The DCS is used to transmit alarm signals between the controllers of the PSMS and PCMS, the alarm processing computer and VDUs in the MCR and RSR. The DCS is fully redundant to meet the high reliability requirements of the SRM to SECY 93-087 II.T.

Therefore, "7.9" is added for SRM to SECY 93-087 II.T in Table 7.1-2 from this RAI.

Impact on DCD

The section "7.9" will be added as the related DCD section in item b. of SRM in Table 7.1-2 (Sheet 3 of 8) as Attachment 1.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 231-2037 REVISION 0
SRP SECTION: 07.09 – DATA COMMUNICATION SYSTEMS
APPLICATION SECTION: 07.09
DATE OF RAI ISSUE: 2/26/2009

QUESTION NO.: 07.09-6

MHI is requested to address conformance with BTP 7-19 guideline in relation to the DCS, any potential common-mode failures, and the propagation of erroneous data. Update Table 7.1-2 if necessary.

Table 7.1-2 does not cite conformance with BTP 7-19 for the DCS. Table 1.9.1-7 indicates that BTP 7-19 is applicable without any exceptions identified. Digital I&C systems can be vulnerable to common-cause failures caused by software errors, which could defeat the redundancy achieved by hardware architecture. Failures in the communication system—either by not transmitting data, transmitting erroneous data, or by generating false data—can cause failures in one or more trains.

ANSWER:

The conformance with BTP 7-19 is fully described in Section 7.8, and the D3 TR, MUAP-07006. While BTP 7-19 covers DCS, the related section is sufficient to refer Section 7.8.

Therefore, no update will be made for Table 7.1-2 from this RAI. See response to 07.09-5, above, regarding CCF.

Impact on DCD

There is no impact on the COLA.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 231-2037 REVISION 0
SRP SECTION: 07.09 – DATA COMMUNICATION SYSTEMS
APPLICATION SECTION: 07.09
DATE OF RAI ISSUE: 2/26/2009

QUESTION NO.: 07.09-7

MHI is requested to address the differences between a temporary connection of the engineering tool in TR MUAP-07005 and a permanent connection for the engineering tool in the DC-FSAR and revise the documents accordingly. Also, the methods used to verify the authenticity and integrity of the application software must be addressed in docketed information.

The continuous connection described in the Section 7.9.1.5 of the DC-FSAR is different from the temporary connection of the engineering tool described in TR MUAP-07005. In addition, the engineering tool can be used to change application setpoints and constants, and update controller software. IEEE 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," Clause 5.3.2, "Software tools" requires"

- that either a test tool validation program be used to provide confidence that the software tool functions properly, or
- that the software tool be used in a manner such that defects not detected by the software tool will be detected by V&V activities

The authenticity and integrity of the application software is verified by the software installation procedure as described in TR MUAP-07005. The differences between a temporary connection and a permanent connection should be provided in the DC-FSAR, as should the verification of the authenticity and integrity of the application software.

ANSWER:

The engineering tool is permanently connected to digital systems for the US-APWR design. The Platform TR, MUAP-07005 will be revised to incorporate the permanent connection.

The authenticity and integrity of the controller Application Software (as well as the controller Basic Software) is confirmed via the Channel Operability Test or Actuation Logic Test, as defined in Chapter 16.1.1. During both of these periodic surveillance tests, the controller memory is fully checked as described in Section 4.1.4.1c of MUAP-07005, and Section 4.4.1 of the Safety I&C TR, MUAP-07004.

Impact on DCD

There is no impact on the DCD.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 231-2037 REVISION 0
SRP SECTION: 07.09 – DATA COMMUNICATION SYSTEMS
APPLICATION SECTION: 07.09
DATE OF RAI ISSUE: 2/26/2009

QUESTION NO.: 07.09-8

MHI is requested to include in Section 7.9 of the DC-FSAR a concise description of the quality of the components and modules of the DCS and the quality of the design process and its relationship with NQA-1, so as to enable a review of the quality of the DCS. Refer the reader to specific section of Chapter 17 of the DC-FSAR for further details if necessary.

Section 7.9.2.1, "Quality of Components Module," contains very little information regarding the quality of the components of the DCS, but refers the reviewer to Chapter 17 of the DC-FSAR. Section 7.9.2.1 should contain a concise but sufficient amount of information to enable a review of the quality of the DCS components and modules.

Based on the limited information provided, the acceptability of the component quality is contingent upon acceptance of the quality plan provided in Chapter 17.

ANSWER:

The explanation will be added in accordance with this RAI.

Impact on DCD

The first sentence in Subsection 7.9.2.1 will be revised as follows.

The PSMS includes the safety bus, data links, I/O bus, and safety VDU communications. The MELTAC platform is applied for all safety DCS components and follows the PSMS QA program. The quality of PSMS components and modules and the quality of the PSMS design process is controlled by a program that meets the requirements of ASME NQA-1-1994 (Reference 7.9-3). Conformance to ASME NQA-1-1994 is described further in Chapter 17.

The PCMS includes the unit bus, data links, I/O Bus, and the unit management PCMS computers. The PCMS data communications uses the same hardware as the PSMS. The PCMS has a similar quality program to the PCMSPSMS, without the same level of documentation.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 231-2037 REVISION 0
SRP SECTION: 07.09 – DATA COMMUNICATION SYSTEMS
APPLICATION SECTION: 07.09
DATE OF RAI ISSUE: 2/26/2009

QUESTION NO.: 07.09-9

MHI is requested to revise the following typographical error. In the second sentence of the second paragraph of section 7.9.2.1, "Quality of Components and Modules," of USAPWR Chapter 7, change the second "PCMS" to "PSMS." The sentence should now read "The PCMS has a similar quality program to the PSMS, without the same level of documentation."

Section 7.9.2.1, "Quality of Components and Modules," states that "The PCMS has a similar quality program to the PCMS, without the same level of documentation." This is a typographical error and should be corrected.

ANSWER:

The revision will be made. See response to RAI 07.09-8.

Impact on DCD

There is no impact on the DCD.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 231-2037 REVISION 0
SRP SECTION: 07.09 – DATA COMMUNICATION SYSTEMS
APPLICATION SECTION: 07.09
DATE OF RAI ISSUE: 2/26/2009

QUESTION NO.: 07.09-10

MHI is requested to provide, in the DC-FSAR, a summary of the DCS software quality program and how it meets BTP 7-14 in sufficient detail to enable an adequate review to be performed, and provide appropriate reference(s) that will provide further details if required.

Section 7.9.2.2 of the DC-FSAR describes the software quality of the DCSs of the USAPWR. MHI applies its MELCO's safety system digital platform MELTAC to the PSMS and PCMS systems. The DC-FSAR states that the software quality program for the MELTAC basic software is discussed in TR MUAP-07005 Section 6.0, that a summary of the software quality program for the system application software is discussed in TR MUAP-07004 Section 6.0, and that a description of the application software quality program is provided in the Software Program Manual for US-APWR Technical Report MUAP-07017. The above shows that the entire software quality description in the DCFSAR consists of a series of references to other reports. This is not sufficient for an adequate review of the software quality of the data communication components and modules. At least a summary of the DCS software quality program and how it meets BTP 7-14 should be provided in this DC-FSAR to enable an adequate review to be performed. Appropriate reference(s) can then be mentioned that will provide further supporting details if required.

ANSWER:

The summary of Software Program Manual Technical Report, MUAP-07017 will be added.

Impact on DCD

Subsection 7.9.2.2 will be revised as follows.

7.9.2.2 Software Quality

The safety related portions of the DCS are part of the PSMS. The non-safety related portions of the DCS are part of the PCMS. All portions of the DCS consist of MELTAC basic software, which handles the communication protocol and self-diagnostics, and application software, which handles the actual data being transmitted.

MHI applies its MELCO's safety system digital platform MELTAC to PSMS and PCMS systems of US-APWR. Details of the software quality program for the MELTAC basic software are discussed in Topical Report MUAP-07005 Section 6.0. A summary of the software quality program for the system PSMS application software is discussed in Topical Report

MUAP-07004 Section 6.0. A description of the application software quality program is provided in the Software Program Manual for US-APWR Technical Report MUAP-07017 (Reference 7.9-4).

The Software Program Manual (SPM) Technical Report describes the processes, which ensure the reliability and design quality of the PSMS application software throughout its entire software lifecycle. The SPM also provides the software program plans based on the guidance of BTP 7-14. By following this SPM, the PSMS application software achieves high functionality and high quality including data communication systems as follows.

- Application software for the PSMS achieves a quality level expected for nuclear plant safety functions.
- Application software provides the required safety functions.
- The processes and procedures described in the SPM are based on established technical and document control requirements, practices, rules and industrial standards.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No. 52-021

RAI NO.: NO. 231-2037 REVISION 0
SRP SECTION: 07.09 – DATA COMMUNICATION SYSTEMS
APPLICATION SECTION: 07.09
DATE OF RAI ISSUE: 2/26/2009

QUESTION NO.: 07.09-11

MHI is requested to provide a more detailed analysis on the docket and preferably in Section 7.9.2.3 of how the DCSs meet the regulatory position of BTP 7-21.

The staff performed a review of the documentation in the DC-FSAR regarding performance requirements of the DCSs. Section 7.9.2.3 of the DC-FSAR briefly describes the system performance requirements, including brief descriptions of system deterministic timing (Section 7.9.2.3.1), real time performance (Section 7.9.2.3.2), time delays within the DCS (Section 7.9.2.3.3) and data rates and bandwidth (Section 7.9.2.3.4). None of these sections contains sufficient information in and of itself to enable an adequate review to be performed, but points to other reports which may themselves point to inadequately referenced reports. For example, Section 7.9.2.3.2, "Real Time Performance," of the DC-FSAR states that "for each safety function an analysis has been performed which demonstrates that the actual system response time is less than the response time required by the plant safety analysis," and refers to TR MUAP-07004 Section 6.5 (which should actually be Section 6.5.3) for the details. Section 6.5.3, "Response Time Analysis Method," of TR MUAP-07004-P uses the response time model for reactor trip to illustrate the response time analysis method used. This model requires knowing the response time of the digital controller used in the digital loop. TR MUAP-07004-P states that the response time calculation method for the digital controller "is described in the Digital Platform Topical Report," but does not provide the document number for this report. A summary of how the DCS meets performance requirements per BTP 7-21 should be provided in the DC-FSAR in sufficient detail to enable an adequate review to be performed.

ANSWER:

The conformance to BTP7-21 will be added in Subsection 7.9.2.3.

In addition, the document related to Subsection 7.9.2.3 (performance test for response time) will be available for more detail information.

Impact on DCD

The first paragraph will be added in Subsection 7.9.2.3.

7.9.2.3 Performance Requirements

DCS in digital I&C system of the US-APWR meets the performance of required functions. The

performance of the digital I&C system including DCS conforms to the guideline of BTP 7-19, "Guidance on Digital Computer Real-Time Performance".

The documents related to Subsection 7.9.2.3 (performance requirements) including the conformance to BTP 7-19 will be available by September 2009 for more detail information..

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 231-2037 REVISION 0
SRP SECTION: 07.09 – DATA COMMUNICATION SYSTEMS
APPLICATION SECTION: 07.09
DATE OF RAI ISSUE: 2/26/2009

QUESTION NO.: 07.09-12

MHI is requested to identify how the DCS meets the single failure criterion in the DCFSAR, preferably in Section 7.9.2.4.

The US-APWR DC-FSAR briefly discusses (in one short paragraph) potential hazards and how the DCS addresses single failures in Section 7.9.2.4. The DC-FSAR states that "self-diagnostic features described in Topical Report MUAP-07004 Section 4.3, detect DCS errors or failures. All DCS errors and failures are analyzed in the FMEA, which demonstrates that there are no single failures that can result in loss of the safety function." In numerous instances, the TRs refer to "credible" single failures rather than single failures. The purpose and what the single failure analysis shows are not discussed.

ANSWER:

Within the DCS, there are independent safety busses, maintenance networks, data links and I/O busses for each division. In addition, the non-safety unit bus is isolated from the safety system. In all cases independence includes electrical independence and communications independence. Therefore, safety divisions are independent of each other and independent of non-safety divisions. Per IEEE 379, once independence is established between redundant divisions, the single failure criteria are satisfied.

Impact on DCD

There is no impact on the DCD.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 231-2037 REVISION 0
SRP SECTION: 07.09 – DATA COMMUNICATION SYSTEMS
APPLICATION SECTION: 07.09
DATE OF RAI ISSUE: 2/26/2009

QUESTION NO.: 07.09-13

MHI is requested to provide a summary of the self diagnostic feature and any hazards of the DCS, but in sufficient detail to enable an adequate review to be performed.

Section 7.9.2.4 references Section 4.3, "PSMS Self-diagnostics Features," of TR MUAP-07004, which indicates that the self diagnostic features of the digital platform continuously check the integrity of processing and communication components as well as the range of process inputs. In addition, the redundant system inputs from different trains are continuously compared to detect failed/drifted instrumentation or input modules. This comparison is performed continuously in the Unit Management Computer of the PCMS; deviations are alarmed in the MCR. If the necessary information provided in the TR is not in Section 7.9.2.4 it should at least be referenced specifically.

ANSWER:

MHI will add the references for self-diagnostic features from the Platform TR, MUAP-07005.

Impact on DCD

The first paragraph in Subsection 7.9.2.4 will be revised as follows.

7.9.2.4 Potential Hazards and Single Failures

The self-diagnostic features described in Topical Report MUAP-07004 Section 4.3, detect DCS errors or failures. The MELTAC controller has separate self-diagnostic features for each of the DCS related modules as described in Topical Report MUAP-07005 Section 4.1.5 and Section 4.3. All DCS errors and failures are analyzed in the FMEA, which demonstrates that there are no single failures that can result in loss of the safety function. The FMEA identifies errors or failures that can result in failures or inadvertent actuation of single divisions, which are bounded by the plant safety analysis.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 231-2037 REVISION 0
SRP SECTION: 07.09 – DATA COMMUNICATION SYSTEMS
APPLICATION SECTION: 07.09
DATE OF RAI ISSUE: 2/26/2009

QUESTION NO.: 07.09-14

MHI is to provide the results of the Failure Modes and Effects Analysis (FMEA) in sufficient detail to enable a review. Also, provide a complete reference to the detailed FMEA report in the DC-FSAR.

In Section 7.9.2.4, "Potential Hazards and Single Failures" of the DC-FSAR the only discussion on FMEA is the statement that "All DCS errors and failures are analyzed in the FMEA, which demonstrates that there are no single failures that can result in loss of the safety function." This statement is made without a reference to any particular FMEA analysis or report. Section 4.3, "PSMS Self diagnostic Features" of MUAP-07004, is referenced but is only one paragraph long, and refers to *Digital Platform Topical Report* for further details. This one-paragraph discussion in and of itself does not provide sufficient detail to allow an adequate staff review to be performed, even when consulting a TR for additional information. Additionally, a description of the FMEA process or what guidance the process followed is not provided. The FMEA should address failures to the black-box, module level for components in the I&C design (e.g. communication modules).

ANSWER:

The portions of the DCS that are used for reactor trip and ESF actuation functions are covered by the FMEA for reactor trip system and ESF actuation system in Tables 7.2-8 and Table 7.3-7, respectively.

For more detail, the FMEA report including overall I&C system of the US-APWR, which will be available as stated in the RAI 07.03-8 response will also encompass DCS failures.

Impact on DCD

Following sentence will be added after the second paragraph in Subsection 7.9.2.4.

Table 7.2-8 and Table 7.3-7 which shows the FMEA for reactor trip and ESF actuation in the PSMS include failure mode and effects of the DCSs.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

4/28/2009

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

RAI NO.: NO. 231-2037 REVISION 0
SRP SECTION: 07.09 – DATA COMMUNICATION SYSTEMS
APPLICATION SECTION: 07.09
DATE OF RAI ISSUE: 2/26/2009

QUESTION NO.: 07.09-15

MHI is requested to address how the DCS addresses communication independence and conformance with RG 1.152 in the DC-FSAR Section 7.9.

There is insufficient information in Section 7.9.2.7 to allow a review of logical independence of the DCS. In particular, the DC-FSAR does not discuss how the DCS meets communication independence per RG 1.152. The only discussion on communication independence is the statement that "each PSMS and PCMS controller/processor protects itself against DCS errors or failures that could disrupt its internal application functions, thereby ensuring communications independence." The DC-FSAR does not discuss how this protection "against DCS errors or failures" is actually achieved.

ANSWER:

General description for the conformance with the independence is described in Subsection 7.1.3.4. Subsection 7.9.2.7 describes the specific description for data communication systems. The reference of the Safety I&C TR, MUAP-07004 will be added for the communication independence.

Impact on DCD

Following sentence will be added after the second paragraph in Subsection 7.9.2.7.

For more detailed discussion on the methods used to ensure independence between digital systems in different safety trains and between safety and non-safety systems refer to Subsections 7.1.3.4 and 7.1.3.5, and Topical Report MUAP-07004 Appendix A.5.6 and Appendix B.5.6.

Impact on COLA

There is no impact on the COLA.

Impact on PRA

There is no impact on the PRA.

Attachment 1 Revised Table 7.1-2

**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	
		1. 10 CFR 50 and 52							
a.	50.55a(a)(1)	Quality Standards for Systems Important to Safety	X	X	X	X	X		7.2 to 7.6, 7.9
b.	50.55a(h)(2)	Protection Systems (IEEE Std 603-1991 or IEEE Std 279-1971)	X	X	X	X	X		7.2 to 7.6, 7.9
c.	50.55a(h)(3)	Safety Systems (IEEE Std 603-1991)	X	X	X	X	X		7.2 to 7.6, 7.9
d.	50.34(f)(2)(v) [I.D.3]	Bypass and Inoperable Status Indication	X	X	X	X	X	X	7.2, 7.3, 7.5, 7.6
e.	50.34(f)(2)(xi) [II.D.3]	Direct Indication of Relief and Safety Valve Position			X		X	X	7.5
f.	50.34(f)(2)(xii) [II.E.1.2]	Auxiliary Feedwater System Automatic Initiation and Flow Indication	X	X	X	X	X		7.3, 7.5
g.	50.34(f)(2)(xvii) [II.F.1]	Accident Monitoring Instrumentation	X		X	X	X	X	7.5
h.	50.34(f)(2)(xviii) [II.F.2]	Instrumentation for the Detection of Inadequate Core Cooling	X			X	X		7.5
i.	50.34(f)(2)(xiv) [II.E.4.2]	Containment Isolation Systems	X	X	X	X	X		7.3
j.	50.34(f)(2)(xix) [II.F.3]	Instruments for Monitoring Plant Conditions Following Core Damage	X			X	X		7.5
k.	50.34(f)(2)(xx) [II.G.1]	Power for Pressurizer Level Indication and Controls for Pressurizer Relief and Block Valves	X		X	X	X		7.4, 7.5
l.	50.34(f)(2)(xxii) [II.K.2.9]	Failure Mode and Effect Analysis of Integrated Control System							N/A to US-APWR
m.	50.34(f)(2)(xxiii) [II.K.2.10]	Anticipatory Trip on Loss of Main Feedwater or Turbine Trip							N/A to US-APWR
n.	50.34(f)(2)(xxiv) [II.K.3.23]	Central Reactor Vessel Water Level Recording							N/A to US-APWR

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

Applicable Criteria	Title	I&C System							Related Section in US-APWR DCD	
		RPS	ESFAS	SLS	Safety HSI	Safety DCS	PCMS	DAS		
o.	50.62	Requirements for Reduction of Risk from Anticipated Transients without Scram							X	7.8
p.	52.47(b)(1)	ITAAC for Standard Design Certification	X	X	X	X	X	X	X	Refer to Tier 1
q.	52.80(a)	ITAAC for Combined Licensee Applications	X	X	X	X	X	X	X	Refer to Tier 1
		2. GDC 10 CFR 50 Appendix A								
a.	GDC 1.	Quality Standards and Records	X	X	X	X	X	X	X	7.2 to 7.6, 7.9
b.	GDC 2	Design Bases for Protection Against Natural Phenomena	X	X	X	X	X	X	X	7.2 to 7.9
c.	GDC 4	Environmental and Dynamic Effects Design Bases	X	X	X	X	X	X	X	7.2 to 7.9
d.	GDC 10	Reactor Design	X	X	X	X	X	X		7.2, 7.3, 7.6, 7.7, Refer to Chapter 4
e.	GDC 13	Instrumentation and Control	X	X	X	X	X	X	X	7.2 to 7.9
f.	GDC 15	Reactor Coolant System Design	X	X	X	X	X	X		7.2, 7.3, 7.6, 7.7, Refer to Chapter 5
g.	GDC 16	Containment Design	X	X	X	X	X	X		7.2, 7.3, 7.6, 7.7, Refer to Chapter 6
h.	GDC 19	Control Room	X	X	X	X	X	X	X	7.2 to 7.9
i.	GDC 20	Protection System Functions	X	X	X	X	X			7.2 to 7.6, 7.9
j.	GDC 21	Protection Systems Reliability and Testability	X	X	X	X	X			7.2 to 7.6, 7.9
k.	GDC 22	Protection System Independence	X	X	X	X	X			7.2 to 7.6, 7.9
l.	GDC 23	Protection System Failure Modes	X	X	X	X	X			7.2 to 7.6, 7.9
m.	GDC 24	Separation of Protection and Control Systems	X	X	X	X	X	X	X	7.2 to 7.9
n.	GDC 25	Protection System Requirements for Reactivity Control Malfunctions	X	X	X	X	X			7.2 to 7.6, 7.9
o.	GDC 28	Reactivity Limits	X	X	X	X	X	X		7.6, Refer to Chapter 15

Table 7.1-2 Regulatory Requirements Applicability Matrix
(per NUREG-0800 Standard Review Plan (SRP) Sec. 7.1 Rev. 5)
(Sheet 3 of 8)

Applicable Criteria		Title	I&C System						PCMS	DAS	Related Section in US-APWR DCD
			RPS	ESFAS	SLS	Safety HSI	Safety DCS				
p.	GDC 29	Protection Against AOOs	X	X	X	X	X	X		7.2 to 7.7, 7.9	
q.	GDC 33	Reactor Coolant Makeup	X	X	X	X	X	X		7.3, 7.6, Refer to Chapter 9	
r.	GDC 34	Residual Heat Removal	X	X	X	X	X	X		7.3, 7.4, 7.6, Refer to Chapter 5	
s.	GDC 35	Emergency Core Cooling	X	X	X	X	X	X		7.3, 7.4, 7.6, Refer to Chapter 6	
t.	GDC 38	Containment Heat Removal	X	X	X	X	X	X		7.3, 7.4, 7.6, Refer to Chapter 6	
u.	GDC 41	Containment Atmosphere Cleanup	X	X	X	X	X	X		7.3, 7.6 Refer to Chapter 6	
v.	GDC 44	Cooling Water	X	X	X	X	X	X		7.3, 7.6, Refer to Chapter 9	
		3. Staff Requirements Memoranda									
a.	SRM to SECY 93087 II.Q	Defense Against Common-Mode Failures in Digital I&C Systems	X	X	X	X	X	X	X	7.8	
b.	SRM to SECY 93087 II.T	Control Room Annunciator (Alarm) Reliability						X		7.5, 7.9	
		4. RGs									
a.	RG 1.22	Periodic Testing of Protection System Actuation Functions	X	X	X	X	X			7.2 to 7.6, 7.9	
b.	RG 1.47	Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety System	X	X	X	X	X	X		7.2, 7.3, 7.5, 7.6, 7.9	
c.	RG 1.53	Application of the Single-Failure Criterion to Safety Systems	X	X	X	X	X			7.2 to 7.6, 7.9	
d.	RG 1.62	Manual Initiation of Protection Actions	X	X	X	X	X			7.2, 7.3	
e.	RG 1.75	Independence of Electrical Safety Systems	X	X	X	X	X	X	X	7.2 to 7.9	

Table 7.1-2 Regulatory Requirements Applicability Matrix
(per NUREG-0800 Standard Review Plan (SRP) Sec. 7.1 Rev. 5)
(Sheet 4 of 8)

Applicable Criteria		Title	I&C System							Related Section in US-APWR DCD
			RPS	ESFAS	SLS	Safety HSI	Safety DCS	PCMS	DAS	
f.	RG 1.97	Instrumentation for Light Water Cooled Nuclear Power Plants to Assess Plant Conditions During and Following an Accident and Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants	X	X	X	X	<u>X</u>	X		7.5
g.	RG 1.105	Setpoints for Safety-related Instrumentation	X	X	X		<u>X</u>			7.2 to 7.6, 7.9
h.	RG 1.118	Periodic Testing of Electric Power and Protection Systems	X	X	X	X	<u>X</u>			7.2 to 7.6, 7.9
i.	RG 1.151	Instrument Sensing Lines	X					X	X	7.2 to 7.6
j.	RG 1.152	Criteria for Use of Computers in Safety Systems of Nuclear Power Plants	X	X	X	X	<u>X</u>			7.2 to 7.6, 7.9
k.	RG 1.168	Verification, Validation, Reviews and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants	X	X	X	X	<u>X</u>			7.2 to 7.6, 7.9
l.	RG 1.169	Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants	X	X	X	X	<u>X</u>			7.2 to 7.6, 7.9
m.	RG 1.170	Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants	X	X	X	X	<u>X</u>			7.2 to 7.6, 7.9
n.	RG 1.171	Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants	X	X	X	X	<u>X</u>			7.2 to 7.6, 7.9

**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
o.	RG 1.172	Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants	X	X	X	X	X			7.2 to 7.6, 7.9
p.	RG 1.173	Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants	X	X	X	X	X			7.2 to 7.6, 7.9
q.	RG 1.174	An Approach for Using PRA in Risk-informed Decisions on Plant-Specific Changes to the Licensing Basis								N/A
r.	RG 1.177	An Approach for Plant-Specific Risk-Informed Decision Making: technical specifications								N/A
s.	RG 1.180	Guidelines for Evaluating Electromagnetic and Radiofrequency Interference in Safety-Related I&C Systems	X	X	X	X	X			7.2 to 7.6, 7.9
t.	RG 1.189	Fire Protection for Operating Nuclear Power Plants	X	X	X	X	X	X	X	7.2 to 7.9
u.	RG 1.200	An Approach for Determining the Technical Adequacy of PRA Results for Risk-Informed Activities								Refer to Chapter 19
v.	RG 1.204	Guidelines for Lightning Protection of Nuclear Power Plants								Refer to Chapter 8 (Subsection 8.3.1.1.11)

Table 7.1-2 Regulatory Requirements Applicability Matrix
(per NUREG-0800 Standard Review Plan (SRP) Sec. 7.1 Rev. 5)
(Sheet 6 of 8)

Applicable Criteria		Title	I&C System						Related Section in US-APWR DCD	
			RPS	ESFAS	SLS	Safety HSI	Safety DCS	PCMS		DAS
w.	RG 1.209	Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants	X	X	X	X	<u>X</u>			7.2 to 7.6, 7.9
		5. BTPs								
a.	BTP 7-1	Guidance on Isolation of Low-Pressure Systems from the High-Pressure RCS	X		X		<u>X</u>			7.6
b.	BTP 7-2	Guidance on Requirements on Motor-Operated Valves in the Emergency Core Cooling System (ECCS) Accumulator Lines	X		X		<u>X</u>			7.6
c.	BTP 7-3	Guidance on Protection System Trip Point Changes for Operation with Reactor Coolant Pumps Out of Service								N/A (US-APWR does not have a situation for restrictive setpoints)
d.	BTP 7-4	Guidance on Design Criteria for Auxiliary Feedwater Systems	X	X	X	X	<u>X</u>			7.3
e.	BTP 7-5	Guidance on Spurious Withdrawals of Single Control Rods in Pressurized Water Reactors						X		7.7
f.	BTP 7-6	Guidance on Design of I&Cs Provided to Accomplish Changeover from Injection to Recirculation Mode								N/A (US-APWR does not have the Recirculation Mode.)
g.	BTP 7-7	Not used								N/A

Table 7.1-2 Regulatory Requirements Applicability Matrix
(per NUREG-0800 Standard Review Plan (SRP) Sec. 7.1 Rev. 5)
(Sheet 7 of 8)

Applicable Criteria	Title	I&C System							Related Section in US-APWR DCD	
		RPS	ESFAS	SLS	Safety HSI	Safety DCS	PCMS	DAS		
h.	BTP 7-8	Guidance on Application of RG 1.22	X	X	X	X	<u>X</u>			7.2 to 7.6, 7.9
i.	BTP 7-9	Guidance on Requirements for RPS Anticipatory Trips	X				<u>X</u>			7.2
j.	BTP 7-10	Guidance on Application of RG 1.97	X		X	X	X	X		7.5
k.	BTP 7-11	Guidance on Application and Qualification of Isolation Devices	X	X	X	X	<u>X</u>			7.2 to 7.6, 7.9
l.	BTP 7-12	Guidance on Establishing and Maintaining Instrument Setpoints	X	X	X		<u>X</u>			7.2 to 7.6, 7.9
m.	BTP 7-13	Guidance on Cross-Calibration of Protection System Resistance Temperature Detectors	X							7.2, 7.3
n.	BTP 7-14	Guidance on Software Reviews for Digital Computer-Based I&C Systems	X	X	X	X	<u>X</u>			7.2 to 7.6, 7.9
o.	BTP 7-15	Not used								N/A
p.	BTP 7-16	Not used								N/A
q.	BTP 7-17	Guidance on Self-Test and Surveillance Test Provisions	X	X	X	X	<u>X</u>			7.2 to 7.6, 7.9
r.	BTP 7-18	Guidance on Use of Programmable Logic Controllers in Digital Computer-Based I&C Systems								N/A
s.	BTP 7-19	Guidance on Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based I&C Systems	X	X	X	X	<u>X</u>	X	X	7.8

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

Applicable Criteria		Title	I&C System						Related Section in US-APWR DCD
			RPS	ESFAS	SLS	Safety HSI	<u>Safety DCS</u>	PCMS	
t.	BTP 7-20	Not used							N/A
u.	BTP 7-21	Guidance on Digital Computer Real-Time Performance	X	X	X	X	<u>X</u>		7.2 to 7.6, 7.9