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

February 27, 2012

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-12052

Subject: **MHI's Responses to US-APWR DCD RAI for Chapter 7**

References: 1) "REQUEST FOR ADDITIONAL INFORMATION 833-6058 REVISION 3, SRP Section: 07-14 Branch Technical Position – Guidance on Software Reviews for Digital Computer Based Instrumentation and Controls Systems, Application Section: Software Program Manual" dated September 29, 2011.

2) "REQUEST FOR ADDITIONAL INFORMATION 837-5945 REVISION 3, SRP Section: 07.01 – Instrumentation and Controls – Introduction, Application Section: 07.01" dated October 11, 2011.

3) "REQUEST FOR ADDITIONAL INFORMATION 688-5273 REVISION 2, SRP Section: 07.07 – Control Systems, Application Section: 07.07" dated January 31, 2011.

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

Enclosures 2 and 3 are the responses to RAIs contained within Reference 1 and 2, and enclosure 4 is the amended responses to RAIs contained within Reference 3.

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

This letter includes copies of the proprietary version of documents (Enclosure 2), copies of the non-proprietary version of documents (Enclosure 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).

One version (Enclosure 2) includes certain information, designated pursuant to the Commission guidance as sensitive unclassified non-safeguards information, referred to as security-related information ("SRI"), that is to be withheld from public disclosure under 10 C.F.R. § 2.390. The information that is SRI is identified by brackets. The second version (Enclosure 3) omits the SRI and is suitable for public disclosure. In the public version, the

D081
NRO

SRI is replaced by the designation "[Security-Related Information - Withheld under 10 CFR 2.390]."

Enclosure 4 does not include any proprietary or security-related information.

Please contact to Mr. Joseph Tapia, General Manager of Licensing Department, Mitsubishi Nuclear Energy Systems, Inc. if the NRC has questions concerning any aspect of this submittal. His contact information is provided below.

Sincerely,

Y. Ogata

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

Enclosures:

1. Affidavit of Yoshiki Ogata
2. Response to Request for Additional Information for Chapter 7
   (Proprietary Version containing Security Related Information)
3. Response to Request for Additional Information for Chapter 7
   (Non-Proprietary Version not containing Security Related Information)
4. Amended Response to Request for Additional Information for Chapter 7
   (Non-Proprietary Version)

CC: J. A. Ciocco
J. Tapia

Contact Information
Joseph Tapia, General Manager of Licensing Department
Mitsubishi Nuclear Energy Systems, Inc.
1001 19th Street North, Suite 710
Arlington, VA 22209
E-mail: joseph_tapia@mnes-us.com
Telephone: (703) 908 – 8055

Enclosure 1

Docket No. 52-021
MHI Ref: UAP-HF-12052

MITSUBISHI HEAVY INDUSTRIES, LTD.

AFFIDAVIT

I, Yoshiki Ogata, state as follows:

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

2. In accordance with my responsibilities, I have reviewed the enclosed documents 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).

   Enclosed Documents:
   - Response to Request for Additional Information for Chapter 7

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

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

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

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

7. Public disclosure of the referenced information would assist competitors of MHI in their

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

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

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

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

Executed on this 27th day of February, 2012.

Y. Ogata

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

Enclosure 3

Docket No. 52-021
UAP-HF-12052

Response to Request for Additional Information for Chapter 7

February 2012

Non-Proprietary Version

This Enclosure includes following response of RAIs

RAI No. 833-6058 Revision 3, Question No.: 07-14 Branch Technical Position-45

RAI No. 833-6058 Revision 3, Question No.: 07-14 Branch Technical Position-49

RAI No. 833-6058 Revision 3, Question No.: 07-14 Branch Technical Position-51

RAI No. 833-6058 Revision 3, Question No.: 07-14 Branch Technical Position-55

RAI No. 837-5945 Revision 3, Question No.: 07.01-44

2/27/2012

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No. 52-021

RAI NO.:	**No.833-6058 Revision 3**
SRP SECTION:	**07-14 Branch Technical Position - Guidance on Software Reviews for Digital Computer-Based Instrumentation and Controls Systems**
APPLICATION SECTION:	**Software Program Manual**
DATE OF RAI ISSUE:	**9/29/2011**

QUESTION NO. : 07-14 Branch Technical Position-45

Software Management Plan Questions
10 CFR 50.55a(a)(1) requires that structures, systems, and components must be designed, fabricated, erected, constructed, tested, and inspected to quality standards commensurate with the importance of the safety function to be performed. 10 CFR 50, Appendix A, General Design Criterion (GDC) 1, "Quality Standards and Records," requires in part that systems and components important to safety be designed, fabricated, erected, and tested to quality standards commensurate with the importance of the safety functions to be performed. Where generally recognized codes and standards are used, they should be identified and evaluated to determine their applicability, adequacy, and sufficiency, and should be supplemented or modified as necessary to ensure a quality product consistent with the required safety function.

BTP 7-14, B.3.1.1, states that Clause 3, "Project Management Process," of IEEE Std. 1074-1995, which is endorsed by Regulatory Guide 1.173, describes an acceptable approach to software project management to satisfy the cited regulation.

General Questions

(1) Throughout the Software Program Manual, the applicant stated conformance to NRC endorsed IEEE standards. The staff requests the applicant to state explicit conformance to NRC Regulatory Guides since they contain regulatory positions that are not necessarily a part of the endorsed standards.

Software Management Plan Specific Questions

(2) Section 3.1.2 of the SPM states that the division of responsibility between companies for fulfilling a particular organizational role for a specific life cycle phase, or for fulfilling all organizational roles for a specific life cycle phase, shall be defined in each US-APWR Project Plan. The staff interprets the use of other companies, which may involve personnel, tools or material, to be subcontractors or suppliers to the applicant. Per IEEE Std. 1074, subcontracting is part of "Resource Allocations" which is part of Project Initiation. Staff requests MHI to address subcontracting element in the Project Plan information (per IEEE Std. 1074) in Section 3.1.1.1 of the SPM or an appropriate section of the SPM

(3) Section 3.1.2 Organization/Responsibilities and Table 3.2-1, Activity: Develop Project Plan, of the SPM do not identify any inputs to the project plan. This should be consistent with the

Input Information in Section 3.1.6.1 of IEEE Std. 1074, as endorsed by RG 1.173. Both the Table and Section 3.1.2 should be consistent with each other on the input information required for Project Plans as well. In particular, identification of contractual requirements is an external process that should be identified as an input of the project plan. The staff requests MHI to address these issues associated with the Input Information.

(4) Section 3.1.9 of the SPM states training and qualification of DTE and VVTE shall include technical competencies, software engineering competencies, and the PSMS application software life cycle process knowledge as determined by the DTM and VVTM, respectively. Section 3.9 of the SPM states compliance to all sections of IEEE Std. 1228¬1994. The staff did not see details for conformance with Clause 4.3.3, Staff Qualifications and Training, which discusses safety-related software training. The staff requests MHI to address this clause. A way to address this is to add tasks (a) through (f) listed in Clause 4.3.3 of IEEE Std. 1228-1994 to the appropriate section of the SPM.

(5) Tier 1, Table 2.5.1-6, ITAAC No. 24, all six "Acceptance Criteria" relating to the SPM state "are performed in accordance with the SPM." The staff requests MHI to revise these acceptance criteria to state "are performed in accordance with BTP 7-14 with the specific exceptions as noted in the US-APWR SPM."

(6) The staff requests MHI to update the Requirements Traceability Matrix definition in Appendix A to reflect the definition in BTP 7-14 Section A.3 Definitions and the central process characteristic identified by Section B.3.3 Acceptance Criteria for Design Outputs.

ANSWER:

(1) Conformance statements to the following Regulatory Guides will be added to each plan.

- RG 1.152, Rev. 3
- RG 1.153, Rev. 1
- RG 1.168, Rev. 1
- RG 1.169, Rev. 0
- RG 1.170, Rev. 0
- RG 1.171, Rev. 0
- RG 1.172, Rev. 0
- RG 1.173, Rev. 0

The revision of RG 1.152 in Section 5 will be updated from Rev. 2 to Rev. 3.

Table 1 shows conformance and exception to above Regulatory Guides. To state explicit conformance and exception to the regulatory positions described in Table1, the applicable section of each corresponding SPM plan will be revised as follows:

The following bullet will be added to Section 3.1.10:

- <u>Section C of RG 1.173 Rev. 0 (Reference 22)</u>

The following bullet will be added to Section 3.2.9:

- <u>Section C of RG 1.152 Rev. 3 (Reference 17)</u>
- <u>Section C of RG 1.153 Rev. 1 (Reference 30)</u>
- <u>Section C of RG 1.172 Rev. 0 (Reference 21)</u>
- <u>Section C of RG 1.173 Rev. 0 (Reference 22)</u>

The following bullet will be added to Section 3.3.8:

- Section C of RG 1.152 Rev. 3 (Reference 17)
- Section C of RG 1.68 Rev. 1 (Reference 18)
- Section C of RG 1.173 Rev. 0 (Reference 22)

The following bullet will be added to Section 3.4.6:

- Section C of RG 1.173 Rev. 0 (Reference 22)

The following bullet will be added to Section 3.5.6:

- Section C of RG 1.173 Rev. 0 (Reference 22)

The following bullet will be added to Section 3.6.8:

- Section C of RG 1.173 Rev. 0 (Reference 22)

The following bullet will be added to Section 3.7.6:

- Section C of RG 1.173 Rev. 0 (Reference 22)

The following bullet will be added to Section 3.8.7:

- Section C of RG 1.173 Rev. 0 (Reference 22)

The first bullet of Section 3.9.9 will be revised as follows:

- Section C~~.3~~ of RG 1.173 Rev. 0 (Reference 22)

The following bullet will be added to Section 3.10.8:

- Section C of RG 1.152 Rev. 3 (Reference 17)
- Section C of RG 1.68 Rev. 1 (Reference 18)
- Section C of RG 1.173 Rev. 0 (Reference 22)

The following bullet will be added to Section 3.11.12:

- Section C of RG 1.152 Rev. 3 (Reference 17)
- Section C of RG 1.69 Rev. 0 (Reference 19)
- Section C of RG 1.173 Rev. 0 (Reference 22)

The following bullet will be added to Section 3.12.8:

- Section C of RG 1.152 Rev. 3 (Reference 17)
- Section C of RG 1.68 Rev. 1 (Reference 18)
- Section C of RG 1.170 Rev. 0 (Reference 20)
- Section C of RG 1.171 Rev. 0 (Reference 21)
- Section C of RG 1.173 Rev. 0 (Reference 22)

Item 17 of Section 5 of the SPM will be revised as follows:

17. Regulatory Guide 1.152 Revision ~~2~~3, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants".

(2) The following description will be added below the first paragraph of Section 3.1.2 of the SPM.

Subcontractors and suppliers shall be managed in accordance with Section 7 "Control of purchased material, equipment, and services" of Topical Report PQD-HD-1995 "Quality Assurance Program Description" (Reference 27).

(3) Table 3.2-1 will be revised to be consistent with Section 3.1.2 which identifies input information of the Project Plan, including "contractual requirements".

The inputs of "Develop Project Plan (P-2)" of Table 3.2-1 will be revised as follows:

~~N/A (External)~~

- Project Purpose
- Reference to the latest applicable versions of the output documents from the Plant Requirements Phase (for compliance with applicable regulations, code and standards)
- Project-specific customer requirements
- Project schedule
- Project budget

(4) The related sections will be revised to address staff qualification and training for Software Safety Analysis Engineer (SSE) per Clause 4.3.3 of IEEE Std. 1228-1994.

The first paragraph of Section 3.1.9 of the SPM will be revised as follows:

DTE, including individuals assigned to perform the software safety analyses activities described in the SSP (Section 3.9 of this SPM) shall be trained and qualified prior to performing any of the activities assigned to the DT as described in this SPM. The DTM is responsible for assuring that DTE are trained and qualified for their assigned activities. Staff qualification and training for SSE is described in Section 3.9.7.3 of the SPM.

Section 3.9.7.3 of the SPM will be revised as follows:

3.9.7.3 Staff Qualifications and Training

The staff qualifications and training plan to comply with Section 3.1.5-3 of NUREG/CR-6101 and Section 4.3.3 of IEEE Std 1228-1994 is described in Section 3.7 "STrngP" of the SPM. This plan shall specify the qualifications for personnel who will perform, at a minimum, the following tasks:

a) Define safety requirements
b) Design and implement safety-critical portions of the system
c) Perform software safety analysis tasks
d) Test safety-critical features
e) Audit software safety plan implementation
f) Perform process certification

(5) Since conformance and exception to BTP 7-14 has already demonstrated in the US-APWR SPM (MUAP-070017), MHI does not think that the acceptance criteria of this ITTAC should include conformance to BTP 7-14 other than the US-APWR SPM. However, since the original acceptance criteria does not clearly identify which kind of software program manual should be applied, the acceptance criteria of Tier 1, Table 2.5.1-6, ITAAC Items 24.i to 24.vi will be revised as follows:

24.i The plant requirements phase result summary report exists and concludes that the plant requirements phase activities of PSMS software are performed in accordance with the US-APWR SPM.

24.ii The system requirements phase result summary report exists and concludes that the system requirements phase activities of PSMS software are performed in accordance with the US-APWR SPM.

24.iii The design requirements phase result summary report exists and concludes that the design phase activities of PSMS software are performed in accordance with the US-APWR SPM.

24.iv The implementation phase result summary report exists and concludes that the implementation phase activities of PSMS software are performed in accordance with the US-APWR SPM.

24.v The test phase result summary report exists and concludes that the test phase activities of PSMS software are performed in accordance with the US-APWR SPM.

24.vi The installation phase result summary report exists and concludes that the installation phase activities of PSMS software are performed in accordance with the US-APWR SPM.

(6) The definition of Requirement Traceability Matrix in Appendix A of the SPM will be revised as follows:

Requirement Traceability Matrix (RTM) [~~IEEE Std 610.12-1990~~ BTP 7-14]
~~A matrix that records the relationship between two or more products of the development process; for example, a matrix that records the relationship between the requirements and the design of a given software component.~~
An RTM shows every requirement, broken down in to sub-requirements as necessary, and what portion of the software requirement, software design description, actual code, and test requirement addresses that system requirement.

Impact on DCD
The acceptance criteria of Tier 1, Table 2.5.1-6, ITAAC Items 24.i to 24.vi will be revised as answered above. (See Attachment-1.)

Tables 1.9.1-1 and 1.9.2-7 will be revised as shown in Attachment-2.

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

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

Impact on PRA
There is no impact on the PRA.

Impact on Technical / Topical Reports
MUAP-07017, "US-APWR Software Program Manual" will be revised as answered above.

Table 1: Conformance and Exception to Regulatory Guides

Regulatory Position		Applicable SPM Section	Exception
RG 1.152 R3	C	3.2, 3.3, 3.10, 3.11, 3.12, Appendix C	No exception
RG 1.153 R1	C	3.2	No exception
RG 1.168 R1	C	3.3, 3.10, 3.12	No exception
RG 1.169 R0	C	3.11	No exception
RG 1.170 R0	C	3.12	No exception
RG 1.171 R0	C	3.12	No exception
RG 1.172 R0	C	3.2	No exception
RG 1.173 R0	C	3.1, 3.2, 3.3, 3.4, 3.5, 3.6, 3.7, 3.8, 3.9, 3.10, 3.11, 3.12	C4.1 Temporary changes are not made that would allow continuation of installation activities or tests of the affected parts of the software. Installation and testing of unaffected parts of the software (e.g., other controllers) may continue without requiring any temporary changes. (See Answer to Question 07-14 Branch Technical Position-48, Item 3) C5 There is no tailored software used in PSMS. (See Answer to Question 07-14 Branch Technical Position-48, Item 3)

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

2/27/2012

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No. 52-021

RAI NO.:	**No.833-6058 Revision 3**
SRP SECTION:	**07-14 Branch Technical Position - Guidance on Software Reviews for Digital Computer-Based Instrumentation and Controls Systems**
APPLICATION SECTION:	**Software Program Manual**
DATE OF RAI ISSUE:	**9/29/2011**

QUESTION NO. : 07-14 Branch Technical Position-49

Software Maintenance Plan
10 CFR 50.55a(a)(1) requires that structures, systems, and components must be designed, fabricated, erected, constructed, tested, and inspected to quality standards commensurate with the importance of the safety function to be performed.

10 CFR 50, Appendix A, General Design Criterion (GDC) 1, "Quality Standards and Records," requires in part that systems and components important to safety be designed, fabricated, erected, and tested to quality standards commensurate with the importance of the safety functions to be performed. Where generally recognized codes and standards are used, they should be identified and evaluated to determine their applicability, adequacy, and sufficiency, and should be supplemented or modified as necessary to ensure a quality product consistent with the required safety function.

Section B.3.1.6 of BTP 7-14 and Clause 6.3 of IEEE Std. 1074-1995, as endorsed by RG 1.173, provide an acceptable approach for software maintenance plans.

1) Section 3.6.2 of the SPM states "MHI is responsible (for) receiving the Licensee report described above..." The staff requests MHI to identify which responsible organization (e.g., MHI or MNES) addresses licensee reports.

2) Section 3.6.6.4 of the SPM, Maintenance of Commercial Dedication, states "There are no commercial grade items used in the PSMS including application software." The SPM should address the recurring procurement of commercial grade parts that MHI receives from suppliers which do not have a nuclear quality assurance program. The staff requests MHI to identify the specific procedure used for commercial grade dedication.

ANSWER:

(1) The DT of the customer and/or MHI are the responsible organization for addressing the application software maintenance activities report. To clearly identify the responsibilities and

the scope of the SPM, Section 3.6.2, Section 3.6.6.1 and the first paragraph of Section 3.6.6.2 of the SPM will be revised as follows:

3.6.2 Organization/Responsibilities

If a PSMS fault or defect is identified during the Operations and Maintenance Phase of the PSMS application software life cycle, the following organizations shall have the following responsibilities (details are described in Section 3.6.6):

(1) ~~Licensee (Customer)~~ Engineering Organization

The ~~Licensee~~ engineering organization, trained and qualified to perform operability determination and evaluations, is responsible for ~~determining~~ evaluating operability of affected Systems, Structures and Components as described in the facility Technical Specifications, and for initiating internal and external reporting as described in Chapter 17 (Quality Assurance Program) of the facility Final Safety Analysis Report (FSAR). Application software maintenance activities performed by the ~~Licensee~~ engineering organization shall be reported, evaluated and initiated in a manner equivalent to the steps described in this SMaintP.

(2) ~~Mitsubishi Heavy Industries, Ltd (MHI)~~ Design Team (DT)

~~MHI~~ The DT is responsible for receiving-and addressing the ~~Licensee~~-report described above, promptly initiating internal and external reports, and tracking identified corrective actions to closure as described in the SQAP (Section 3.3 of this SPM)

~~(3) Design Team (DT)~~

The DT is responsible for responding to internal reports of PSMS application software failures, defects or other nonconforming conditions, determining the root cause, extent of condition, and corrective actions, and implementing the identified corrective actions including initiating a Notice of Defect report, if required, as described in the SQAP (Section 3.3 of this SPM).

(~~4~~3) Verification and Validation Team (VVT)

The VVT is responsible for Maintenance Phase V&V activities as described in the SVVP (Section 3.10 of this SPM).

3.6.6.1 Activity: Failure Detecting and Reporting

The DT shall provide the methodology for identifying, assessing, and recording failures of the PSMS during plant operation in an Operation and Maintenance Manual to be provided ~~to the Licensee~~ before the Operations and Maintenance Phase. As a minimum, the methodology in the Operation and Maintenance Manual shall include requirements for identifying the date and time of a PSMS failure, a brief description of the failure (including the state of the system at the beginning of the occurrence), information retrieved using the MELTAC engineering tool, and a description of immediate corrective actions taken by the ~~Licensee~~ operation personnel and engineering organization.

(1) ~~Licensee~~ Engineering Organization

Upon discovery of a PSMS failure, the ~~Licensee~~ operation personnel and engineering organization, which may include design engineers, system engineers, maintenance engineers or training engineers, shall identify, assess, and record failure data as described in the Operation and Maintenance Manual, and attach it to an internal report

to be initiated in accordance with their internal procedures for Issue Reporting and Corrective Action as described in Chapter 17 (QAP) of the facility FSAR.

If the error is likely due to a PSMS defect or nonconforming condition, the ~~Licensee~~ engineering organization shall promptly report the condition to ~~MHI~~ the DT, and if the nonconforming condition is determined by the ~~Licensee~~ engineering organization to be a defect as described in 10 CFR 21, a Notice of Defect report shall be initiated in accordance with the ~~Licensee's~~ internal procedures of the engineering organization as described in Chapter 17 of the facility FSAR.

The ~~Licensee~~ engineering organization shall also ~~determine~~ evaluate operability of affected Systems, Structures and Components in accordance with the facility Technical Specifications.

(2) ~~MHI~~ Design Team (DT)

In response to the ~~Licensee~~ engineering organization report provided in Step (1), ~~MHI~~ the DT shall promptly initiate a Nonconformance Report as described in Section 15 "Nonconforming, Materials, Parts, or Components" of Topical Report PQD-HD-19005 "Quality Assurance Program Description" (Reference 27). ~~MHI~~ The DT shall ~~assign~~ have the responsibility for determining the root cause, extent of condition, and corrective actions ~~to the Design Team~~ (described in Section 2.2 of this SPM).

3.6.6.2 Activity: Fault Correction

The DT shall collect and analyze the operational failure data to be provided by the ~~Licensee~~ engineering organization, which may include design engineers, system engineers, maintenance engineers, or training engineers, as described in Section 3.6.6.1.

To clearly require independency between the engineering organization and the VVT, the following description will be added after the second paragraph of Section 2.2.1.

Figure 2.2-1 describes the typical organization structure from the plant requirement phase to the installation phase. The organization after the operation and maintenance phase may be changed; however, regardless of the organization changes made, the independence of the VVT from the DT, and the independent reporting relationship for the QA organization shall always be maintained.

To clearly the responsibility after the operation and maintenance phase, the first paragraph of Section 3.2.6.7.1 will be revised as follows;

The ~~customer~~ engineering organization, which may include design engineers, system engineers, maintenance engineers, or training engineers, has the primary responsibility ~~of operating and maintaining~~ for operations and maintenance support of the PSMS as described in the SOP (section 3.8 of this SPM) and the SMaintP (Section 3.6 of this SPM).

(2) This SPM is applied to the application software and basic software (by reference to the Basic SPM) of the PSMS and augmented quality systems. There are no commercial grade items used in the PSMS software as described in Section 3.6.6.4 of the SPM. Therefore, there is no specific procedure necessary for commercial grade dedication.

Impact on DCD

There is no impact on the DCD.

Impact on R-COLA

There is no impact on the R-COLA.

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

Impact on PRA
There is no impact on the PRA.

Impact on Technical / Topical Reports
MUAP-07017, "US-APWR Software Program Manual" will be revised as answered above.

2/27/2012

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No. 52-021

RAI NO.:	**No.833-6058 Revision 3**
SRP SECTION:	**07-14 Branch Technical Position - Guidance on Software Reviews for Digital Computer-Based Instrumentation and Controls Systems**
APPLICATION SECTION:	**Software Program Manual**
DATE OF RAI ISSUE:	**9/29/2011**

QUESTION NO. : 07-14 Branch Technical Position-51

Software Safety Plan Questions
10 CFR 50.55a(a)(1) requires that structures, systems, and components must be designed, fabricated, erected, constructed, tested, and inspected to quality standards commensurate with the importance of the safety function to be performed.

10 CFR 50, Appendix A, General Design Criterion (GDC) 1, "Quality Standards and Records," requires in part that systems and components important to safety be designed, fabricated, erected, and tested to quality standards commensurate with the importance of the safety functions to be performed. Where generally recognized codes and standards are used, they should be identified and evaluated to determine their applicability, adequacy, and sufficiency, and should be supplemented or modified as necessary to ensure a quality product consistent with the required safety function.

BTP 7-14, Section B.3.19 provides guidance to evaluate software safety plans (SSPs).

1) The applicant commits to IEEE Std. 1228-1994, which requires an independent safety organization. Does MHI intend to have a separate, independent safety organization? Or is the responsibility not separate from the responsibility to produce a safety software system? The staff requests MHI to clearly address this.

2) Sections 3.9.7.11 of the SPM, Previously Developed or Purchase Software, appears to have conflicting statements, "This SPM ...which controls all application software of the PSMS including the basic software for each US-APWR project." versus "The Basic SPM shall be controlled by MELCO..." The staff requests MHI to reconcile these statements.

3) Section 3.9.8.3.4 of the SPM, Test Specification Evaluation, states that "Any task, or subtask, which cannot be tested, is documented..." The staff requests MHI to clarify what is meant by 'tasks that cannot be tested.' RG 1.172, Regulatory Position C.2.5 states all requirements should be verifiable and should be modified or restated as necessary so that it is possible to verify each one (requirement).

4) Section 3.9.8.1.3 of the SPM, Criticality Analysis, states "The criticality analysis for the communication interface between the PCMS and the PSMS has been performed in Appendix

D of the technical report MUAP-07004 "Safety I&C System Description and Design Process." The staff notes that the referenced Appendix D is limited in scope (e.g., Operational VDU Spurious Commands) and limited in content (discusses credible failures of O-VDU can lead to spurious control command control) and does not address the criticality analysis characteristics of IEEE Std 1012. A criticality analysis is expected to be an evaluation of the entire system not just of the O-VDU interface. The criticality analysis, per IEEE Std. 1012-1998, should determine the functionality of each software module or subsystem and assign a SIL level classification for each software module or subsystem based on the safety function. The staff requests MHI to address this issue.

ANSWER:

1) As described in Section 3.9.2 "Organization/Responsibilities", the DT Engineers who have the responsibility to design and to produce safety system software will perform all activities related to the Software Safety Plan (SSP). The DTM (Design Team Manager) has all responsibilities for the overall conduct of the SSP. The independent VVT is responsible for assuring the requirements of the SSP, including IEEE Std. 1228-1994 requirements, are followed throughout the PSMS application software life cycle process.

   The second paragraph of Section 3.9.2 will be revised as follows;

   > The VVT, independent from the DT, is responsible for assuring the requirements of the SSP are followed throughout the PSMS application software life cycle process.

2) The scope of the basic software is described in Section 1.2 of the SPM as follows

   This SPM describes both the application and basic software lifecycle of the PSMS. However, the MELTAC platform, including the life cycle process for the basic software, is described in MUAP-07005 (Reference 2) and is addressed in this SPM to ensure that the as-built basic software is developed and controlled by MELTAC Platform Basic Software Program Manual (Reference 24).

   The purpose of the description "The Basic SPM shall be controlled by MELCO..." is to clarify that the life cycle process of the MELTAC Basic Software is controlled by MELCO and is not shifted to the customer of each US-APWR project.

   The fifth paragraph of Section 3.9.7.11 will be revised as follows;

3) The meaning of "tasks that cannot be tested" is "tasks that cannot be tested by the validation test" and these tasks are validated by other tests or verified by analyses.

   The Item (2) in the second paragraph of Section 3.9.8.3.4 will be revised as follows;

   > Any task, or subtask, which cannot be tested by the validation test, is documented and clearly identified that there is no impact on safety, ~~has been determined~~ as demonstrated by other tests or analyses.

4) The criticality analysis, per IEEE Std. 1012-1998, is to determine the functionality of each software module or subsystem and assign a SIL level classification for each software module or subsystem based on the safety function. And, the critically analysis for the entire PSMS has been performed, and all PSMS application software are assigned as the highest software integrity level (SIL) 4, and all life cycle process including the independent V&V which are described in the US-APWR SPM will be applied to all application software of the PSMS as described in the first paragraph of Section 3.9.8.1.3.

   Therefore, the second paragraph of Section 3.9.8.1.3 will be eliminated as follows;

   ~~In addition, the communication interface with the PCMS must be assessed for impacts that can lead to the PSMS system failures. The criticality analysis of the PCMS and the PSMS communications interface is a structured evaluation of the software characteristics for severity of impact of system failure, system degradation, and failure to meet software requirements or system objectives. The criticality analysis for the communication interface between the PCMS and the PSMS has been performed in Appendix D of the technical report MUAP-07004 "Safety I&C System Description and Design Process".~~

Impact on DCD
There is no impact on the DCD.

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

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

Impact on PRA
There is no impact on the PRA.

Impact on Technical / Topical Reports
MUAP-07017, "US-APWR Software Program Manual" will be revised as answered above.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

2/27/2012

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No. 52-021

RAI NO.:	**No.833-6058 Revision 3**
SRP SECTION:	**07-14 Branch Technical Position - Guidance on Software Reviews for Digital Computer-Based Instrumentation and Controls Systems**
APPLICATION SECTION:	**Software Program Manual**
DATE OF RAI ISSUE:	**9/29/2011**

QUESTION NO. : 07-14 Branch Technical Position-55

Secure Development and Operational Environment Questions, Appendix C of the Software Program Manual
10 CFR 50.55a(h), "Protection and Safety Systems," requires compliance with the requirements of IEEE Std. 603-1991, which is a system-level standard that contains requirements related to access controls. Clause 5.9 of IEEE Std. 603-1991, "Control of Access" , states that design shall permit the administrative control of access to safety system equipment. And that these administrative controls shall be supported by provisions within the safety systems, by provision in the generating station design, or by a combination thereof.

1) Appendix C of the SPM quoted regulatory positions from Revision 2 of RG 1.152. Since the SPM submittal, NRC has issued Revision 3 of RG 1.152. The staff requests MHI to update Appendix C to reflect revised regulatory position languages from Revision 3 of RG 1.152.

2) Section C.1, Introduction, of Appendix C states that JEXU-1012-1132, "MELTAC Platform Basic Software Program Manual," states compliance to the secure development and operational environment requirements of RG 1.152, Revision 2 for future changes to the basic software. The staff requests MHI to clarify what is meant by "compliance...for future changes to the basic software." Also, the staff requests MHI to clearly describe whether or not the MELTAC system (basic software development) meets the SDOE guidance of RG 1.152, Revision 3.

3) Section C.2.1 of Appendix C states that {[ ]}. MHI states that {[ ]}. The staff requests MHI to elaborate on {[ ]}.

4) Section C.2.4.3 of Appendix C states that {[ ]}. The staff requests MHI to clarify what is meant by {[ ]}.

5) Section 3.4 of Appendix C states that unauthorized changes of test results, or not reporting adverse findings documented in the test logs, are excluded by reviews performed by the VVT. This statement is not clear. The staff requests MHI to clearly explain and expand the sentence for clarity. The staff understands that test reports are controlled via the SCMP, and that the QA organization may audit V&V documents.

6) Section 3.5 of Appendix C states that {[

]}. The staff requests MHI to expand on what is meant by {[ ]}.

ANSWER:

1) Appendix C of the US-APWR SPM will be updated to reflect revised regulatory position language from Revision 3 of RG 1.152 as shown in Attachment-3 of this response.

2) The secure development and operational environment for the design, production and maintenance of the MELTAC platform basic software is described in JEXU-1012-1132 "MELTAC Platform Basic Software Program Manual". And, the conformance to the secure development and operational environment requirements of RG 1.152, Rev. 3 for future changes to the basic software is also described in JEXU-1012-1132 "MELTAC Platform Basic Software Program Manual."

   The fourth paragraph of Appendix C Section 1 "Introduction" of the US-APWR SPM will be revised as shown in Attachment-3 of this response.

3) The descriptions and commitments on the following issues will be added to the second paragraph in "Analysis" column of Appendix C Section C.2.1 (Staff Position 3) of the US-APWR SPM as shown in Attachment-3 of this response.

   - Allowed conditions when the MELTAC Engineering Tool to connect the PSMS.
   - Measures to prevent potential unauthorized access or changes to the PSMS.

4) The clear description with proper examples on what is meant by highly deterministic and visible behaviors will be added to the second and the third paragraph in "Analysis" column of Appendix C Section C.2.4.2 (Staff Position-1) of the US-APWR SPM as shown in Attachment-3 of this response.
   Note) Section number is corrected from C.2.4.3 to C.2.4.2.

5) The clear and expanded descriptions to the sentence "unauthorized changes of test results, or not reporting adverse findings documented in the test logs, are excluded by reviews performed by the VVT." will be added to the first paragraph of Appendix C Section C.3.4 of the US-APWR SPM as shown in Attachment-3 of this response.

6) The clear and expanded descriptions of the meaning to the sentence "other design features." will be added to the tenth paragraph of Appendix C Section C.3.5 of the US-APWR SPM as shown in Attachment-3 of this response.

Impact on DCD

There is no impact on the DCD.

Impact on R-COLA

There is no impact on the R-COLA.

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

Impact on PRA
There is no impact on the PRA.

Impact on Technical / Topical Reports
See Attachment-3.

Table 2.5.1-6 RT System and ESF System Inspections, Tests, Analyses, and Acceptance Criteria (Sheet 7 of ~~9~~10)

MIC-03-07-0 0003
MIC-03-07-0 0004

Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
20. Deleted.	20. Deleted.	20. Deleted.
21. The RT logic of the PSMS is designed to fail to a safe state such that loss of electrical power to a division of PSMS results in a trip condition for that division. Loss of electrical power to a division of the PSMS ESF logic does not result in ESF actuation.	21. A test will be performed by disconnecting the electrical power to each division of the as-built PSMS.	21. Each division of the as-built RT logic of the as-built PSMS fails to a safe state upon loss of electrical power to the division (i.e., results in a trip condition for that division), and loss of electric power to a division of the as-built PSMS ESF logic does not result in ESF actuation.
22. The RT and ESF actuation instrumentation that is required to function during normal operation, anticipated operational occurrence (AOO) and postulated accident (PA) conditions is provided with adequate range to monitor normal operating, AOO and PA events. The monitored variables are listed in Tables 2.5.1-2 and 2.5.1-3.	22. An inspection of the as-built RT and ESF actuation instrumentation ranges will be performed.	22. The ranges of the as-built PSMS RT and ESF actuation instrumentation that is required to function during normal operation, anticipated operational occurrences (AOO) and postulated accident (PA) conditions, and that is listed in Tables 2.5.1-2 and 2.5.1-3, meet design requirements.
23. The PSMS provides the interlocks important to safety identified in Table 2.5.1-4.	23. A test of the as-built PSMS will be performed.	23. The as-built PSMS provides the interlocks important to safety identified in Table 2.5.1-4 when the simulated plant process signals reach a predetermined limit.
~~24. The PSMS hardware and software are developed and managed by the Basic and Application Software Program Manuals that meet the regulatory requirements for Class 1E safety systems, and which encompasses the entire product life cycle including software V&V and configuration management.~~	~~24. Inspections of the as-built hardware and software life cycle documentation of the PSMS will be performed.~~	~~24. The as-built PSMS hardware and software are developed and managed by the Basic and Application Software Program Manuals that meet the regulatory requirements for Class 1E safety systems, and which encompasses the entire product life cycle including software V&V and configuration management.~~

MIC-03-07-0 0003

Table 2.5.1-6 RT System and ESF System Inspections, Tests, Analyses, and Acceptance Criteria (Sheet 8 of ~~9~~10) MIC-03-07-00003 MIC-03-07-00004

Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria	
24. Software Program Manual (SPM) is implemented to manage the PSMS software lifecycle process in each software lifecycle phase.	24.i An inspection will be performed for the plant requirements phase result summary report of PSMS software in accordance with the SPM.	24.i The plant requirements phase result summary report exists and concludes that the plant requirements phase activities of PSMS software are performed in accordance with the US-APWR SPM.	MIC-03-07-00003 DCD_07-14_BTP-45
	24.ii An inspection will be performed for the system requirements phase result summary report of PSMS software in accordance with the SPM.	24.ii The system requirements phase result summary report exists and concludes that the system requirements phase activities of PSMS software are performed in accordance with the US-APWR SPM.	DCD_07-14_BTP-45
	24.iii An inspection will be performed for the design phase result summary report of PSMS software in accordance with the SPM.	24.iii The design requirements phase result summary report exists and concludes that the design phase activities of PSMS software are performed in accordance with the US-APWR SPM.	DCD_07-14_BTP-45
	24.iv An inspection will be performed for the implementation phase result summary report of PSMS software in accordance with the SPM.	24.iv The implementation phase result summary report exists and concludes that the implementation phase activities of PSMS software are performed in accordance with the US-APWR SPM.	DCD_07-14_BTP-45
	24.v An inspection will be performed for the test phase result summary report of PSMS software in accordance with the SPM.	24.v The test phase result summary report exists and concludes that the test phase activities of PSMS software are performed in accordance with the US-APWR SPM.	DCD_07-14_BTP-45

Table 2.5.1-6 RT System and ESF System Inspections, Tests, Analyses, and Acceptance Criteria (Sheet 9 of ~~9~~10)

MIC-03-07-00003
MIC-03-07-00004

Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
	24.vi An inspection will be performed for the installation phase result summary report of PSMS software in accordance with the SPM.	24.vi The installation phase result summary report exists and concludes that the installation phase activities of PSMS software are performed in accordance with the US-APWR SPM.
25.a ~~Manual controls from the operational VDU are blocked from the safety VDU and can be disabled manually from the safety VDU. The logic in the SLS blocks non-safety signals from the PCMS when any safety function signal is present, such as a safety interlock or ESF actuation signal.~~Manual control signals from the safety VDU override and can disable manual control signals from the operational VDU to the PSMS by the priority logic in the PSMS.	25.a A Test~~s~~ of the as-built PSMS, including safety VDU, will be performed using simulated signals.	25.a ~~Manual controls from the operational VDU are blocked from the as-built safety VDU and can be disabled manually from the as-built safety VDU. The logic in the as-built SLS blocks non-safety signals from the PCMS when any safety function signal is present, such as a safety interlock or ESF actuation signal.~~Simulated manual control signals from the as-built safety VDU override and can disable simulated manual control signals from the operational VDU to the PSMS by the priority logic in the as-built PSMS.
25.b Automatic ESFAS actuation signals identified in Table 2.5.1-3 and the interlocks important to safety identified in Table 2.5.1-4 override the manual and automatic control signals from the PCMS ~~control signals~~to the safety-related components by the priority logic in the PSMS.	25.b A test of the as-built PSMS will be performed by using simulated signals~~to confirm that simulated ESFAS actuation signals identified in Table 2.5.1-3 and the interlocks important to safety identified in Table 2.5.1-4 override as-built PCMS control signals~~.	25.b ~~As-built PCMS control signals are overridden by s~~Simulated automatic ESFAS actuation signals identified in Table 2.5.1-3 and ~~the~~automatic interlock~~s~~ signals important to safety identified in Table 2.5.1-4 in the as-built PSMS override the simulated manual and automatic control signals from the PCMS to the safety-related components by the priority logic in the as-built PSMS.

MIC-03-07-00003
DCD_07-14_BTP-45
MIC-03-07-00004

Table 1.9.1-1 US-APWR Conformance with Division 1 Regulatory Guides (Sheet 14 of 20)

Reg Guide Number	Title	Status	Corresponding Chapter/Section/ Subsection
1.150	Ultrasonic Testing of Reactor Vessel Welds During Preservice and Inservice Examinations (Rev. 1, February 1983)	Withdrawn.	
1.151	Instrument Sensing Lines (Rev. 0, July 1983)	Conformance with no exceptions identified.	7.1.3.7
1.152	Criteria for Digital Computers in Safety Systems of Nuclear Power Plants (~~Rev. 2, January 2006~~Rev. 3, July 2011)	Conformance with no exceptions identified.	~~7.9.2.6~~7.1.3.17
1.153	Criteria for Safety Systems (Rev. 1, June 1996)	Conformance with no exceptions identified.	7.1.2, 8.1.5.3
1.154	Format and Content of Plant-Specific Pressurized Thermal Shock Safety Analysis Reports for Pressurized Water Reactors (Rev. 0, January 1987)	Not applicable.	N/A
1.155	Station Blackout (Rev. 0, August 1988)	Conformance with no exceptions identified.	8.1.5.3
1.156	Environmental Qualification of Connection Assemblies for Nuclear Power Plants (Rev. 0, November 1987)	Conformance with no exceptions identified.	8.1.5.3
1.157	Best-Estimate Calculations of Emergency Core Cooling System Performance (Rev. 0, May 1989)	Conformance with exceptions. C.3.13-14 applies to BWR only.	15.6.5
1.158	Qualification of Safety-Related Lead Storage Batteries for Nuclear Power Plants (Rev. 0, February 1989)	Conformance with no exceptions identified.	8.1.5.3
1.159	Assuring the Availability of Funds for Decommissioning Nuclear Reactors (Rev. 1, October 2003)	Not applicable. RG applies to a site-specific operational program.	N/A
1.160	Monitoring the Effectiveness of Maintenance at Nuclear Power Plants (Rev. 2, March 1997)	Not applicable. RG applies to a site-specific operational program.	N/A
1.161	Evaluation of Reactor Pressure Vessels with Charpy Upper-Shelf Energy Less Than 50 Ft-Lb (Rev. 0, June 1995)	Not applicable. RG applies to a site-specific operational program.	N/A
1.162	Format and Content of Report for Thermal Annealing of Reactor Pressure Vessel (Rev. 0, February 1996)	Not applicable. RG applies to a site-specific program to restore strength to the reactor vessel lost by irradiation.	N/A

DCD_07-14_BTP-45

Table 1.9.1-1 US-APWR Conformance with Division 1 Regulatory Guides (Sheet 16 of 20)

Reg Guide Number	Title	Status	Corresponding Chapter/Section/ Subsection
1.173	Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants (Rev. 0, September 1997)	~~Conformance with no exceptions identified.~~ Conformance with exceptions. C4.1: Temporary changes are not made that would allow continuation of installation activities or tests of the affected parts of the software. Installation and testing of unaffected parts of the software (e.g., other controllers) may continue without requiring any temporary changes. C5: There is no tailored software used in PSMS.	7.1.3.17
1.174	An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis (Rev. 1, November 2002)	Not applicable. RG applies to a site-specific analysis.	N/A
1.175	An Approach for Plant-Specific, Risk-Informed Decision making: Inservice Testing (Rev. 0, August 1998)	Not applicable. RG applies to a site-specific analysis.	N/A
1.176	An Approach for Plant-Specific, Risk-Informed Decisionmaking: Graded Quality Assurance (Rev. 0, August 1998)	Withdrawn	
1.177	An Approach for Plant-Specific, Risk-Informed Decisionmaking: Technical Specifications (Rev. 0, August 1998)	Not applicable. RG applies to a site-specific analysis.	N/A
1.178	An Approach for Plant-Specific Risk-Informed Decisionmaking for Inservice Inspection of Piping (Rev. 1, September 2003)	Not applicable. RG applies to a site-specific analysis.	N/A
1.179	Standard Format and Content of License Termination Plans for Nuclear Power Reactors (Rev. 0, January 1999)	Not applicable. RG applies to a site-specific operational program.	N/A
1.180	Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems (Rev. 1, October 2003)	Conformance with no exceptions identified.	7.1.3.7, 8.1.5.3, 9.5.2

DCD_07-14_BTP-45

Table 1.9.2-7 US-APWR Conformance with Standard Review Plan Chapter 7 Instrumentation and Controls (Sheet 2 of 22)

SRP Section and Title	SRP Excerpt Indicating Acceptance Criteria for DCD	Status	Appears in DCD Chapter/Section
7.1 Instrumentation and Controls – Introduction (continued)	SRP Appendix 7.1-D provides guidance for evaluating conformance to SRP acceptance criteria contained in IEEE Std. 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," as endorsed by Regulatory Guide 1.152, Revision ~~2~~3, "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants."		
7.1-T Table 7-1 Regulatory Requirements, Acceptance Criteria, and Guidelines for Instrumentation and Control Systems Important to Safety	SRP Table 7-1 identifies the regulatory requirements (denoted by "R"), and SRP acceptance criteria (denoted by "A") and their applicability to the various sections of Chapter 7 of the safety analysis report (SAR).	Conformance with no exceptions identified.	7.1
Appendix 7.1-A: Acceptance Criteria and Guidelines for Instrumentation and Control Systems Important to Safety	(Note: This appendix is referenced from SRP 7.1 and contains many pages of acceptance criteria drawn from other regulatory documents such as 10 CFR General Design Criteria, Regulatory Guides, other SRP sections, Branch Technical Positions, national standards, etc.).	Conformance with no exceptions identified.	7.1
Appendix 7.1-B: Guidance for Evaluation of Conformance to IEEE Std. 279	(Note: This appendix is referenced from SRP 7.1 and contains many pages of acceptance criteria drawn from IEEE Standard 279, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations.")	Not applicable. US-APWR complies with IEEE Standard 603, which supersedes IEEE 279 for newer plants.	N/A

DCD_07-14_BTP-45

Table 1.9.2-7 US-APWR Conformance with Standard Review Plan Chapter 7 Instrumentation and Controls (Sheet 3 of 22)

SRP Section and Title	SRP Excerpt Indicating Acceptance Criteria for DCD	Status	Appears in DCD Chapter/Section
Appendix 7.1-C: Guidance for Evaluation of Conformance to IEEE Std. 603	(Note: This appendix is referenced from SRP 7.1 and contains many pages of acceptance criteria drawn from IEEE Standard 603, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations")	Conformance with no exceptions identified.	7.1
Appendix 7.1-D: Guidance for Evaluation of Conformance to IEEE Std. 7-4.3.2	(Note: This appendix is referenced from SRP 7.1 and contains many pages of acceptance criteria drawn from Standard IEEE/ANS 7-4.3.2-1982, "American Nuclear Society and IEEE Standard Application Criteria for Programmable Digital Computer Systems in Safety Systems of Nuclear Power Generating Stations.")	Conformance with no exceptions identified.	7.1
7.2 Reactor Trip System	1. SRP Appendix 7.1-C provides SRP acceptance criteria for safety system compliance with 10 CFR 50.55a(h). 2. SRP Appendix 7.1-B provides SRP acceptance criteria for protection system compliance with 10 CFR 50.55a(h) (2). 3. IEEE Std 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," as endorsed by Regulatory Guide 1.152, Revision ~~2~~3, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," provides guidance on applying the safety system criteria to computer-based safety systems. SRP Appendix 7.1-D provides SRP acceptance criteria for safety and protection systems using digital computer-based technology. 4. Item II.Q, "Defense Against Common-Mode Failures in Digital Instrument and Control Systems," of the Staff Requirements Memorandum on SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light Water Reactor (ALWR) Designs," provides guidance on Diversity and Defense-in-Depth. SRP BTP 7-19 provides additional guidance.	Conformance with no exceptions identified.	7.2
7.3 Engineered Safety Features Systems	1. SRP Appendix 7.1-C provides SRP acceptance criteria for safety system compliance with 10 CFR 50.55a(h). 2. SRP Appendix 7.1-B provides SRP acceptance criteria for protection system compliance with 10 CFR 50.55a(h).	Conformance with no exceptions identified.	7.3

DCD_07-14_BTP-45

Table 1.9.2-7 US-APWR Conformance with Standard Review Plan Chapter 7 Instrumentation and Controls (Sheet 4 of 22)

SRP Section and Title	SRP Excerpt Indicating Acceptance Criteria for DCD	Status	Appears in DCD Chapter/Section
7.3 Engineered Safety Features Systems (continued)	3. IEEE Std 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," as endorsed by Regulatory Guide 1.152, Revision ~~2~~3, "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants," provides guidance on applying the safety system criteria to computer-based safety systems. SRP Appendix 7.1-D provides SRP acceptance criteria for safety and protection systems using digital computer-based technology. 4. Item II.Q, "Defense Against Common-Mode Failures in Digital Instrument and Control Systems," of the Staff Requirements Memorandum on SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light Water Reactor (ALWR) Designs," provides guidance on Diversity and Defense-in-Depth. SRP BTP 7-19 provides additional guidance.		
7.4 Safe Shutdown Systems	1. SRP Appendix 7.1-C provides SRP acceptance criteria for safety system compliance with 10 CFR 50.55a(h). 2. SRP Appendix 7.1-B provides SRP acceptance criteria for protection system compliance with 10 CFR 50.55a(h). 3. SRP Appendix 7.1-D provides SRP acceptance criteria for the digital I&C compliance with IEEE Std 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," as endorsed by Regulatory Guide 1.152, Revision ~~2~~3, "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants."	Conformance with no exceptions identified.	7.4

DCD_07-14_BTP-45

DCD_07-14_BTP-45

Table 1.9.2-7 US-APWR Conformance with Standard Review Plan Chapter 7 Instrumentation and Controls (Sheet 5 of 22)

SRP Section and Title	SRP Excerpt Indicating Acceptance Criteria for DCD	Status	Appears in DCD Chapter/Section
7.5 Information Systems Important to Safety	1. SRP Appendix 7.1-C provides SRP acceptance criteria for safety system compliance with 10 CFR 50.55a(h). 2. SRP Appendix 7.1-B provides SRP acceptance criteria for protection system compliance with 10 CFR 50.5i5a(h). 3. SRP Appendix 7.1-D provides SRP acceptance criteria for the application of the requirements of IEEE Std. 603-1991 to digital I&C. Appendix 7.1-D discusses the application of the guidance in IEEE Std. 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," as endorsed by Regulatory Guide 1.152, Revision ~~2~~3. 4. Item II.Q, "Defense Against Common-Mode Failures in Digital Instrument and Control Systems," of the Staff Requirements Memorandum on SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light Water Reactor (ALWR) Designs," provides guidance on Diversity and Defense-in-Depth. SRP BTP 7-19 provides additional guidance. 5. Regulatory Guide 1.97, Revision 2, 3, and 4, describe methods acceptable to the NRC staff for providing instrumentation to monitor variables for accident conditions. For plants with operating licenses issued before June 2006, Regulatory Guide 1.97, Revision 2 and 3, are still effective. Licensees of these plants may, however, convert to the criteria of Revision 4 or use the criteria of Revision 4 when performing modifications that do not involve a conversion. The guidance contained in Regulatory Position 1 of Regulatory Guide 1.97, Revision 4, should be followed in these cases. Plants that obtained an operating license after June 2006 should reference the guidance of Regulatory Guide 1.97, Revision 4. SRP BTP 7-10 provides guidance on the application of Regulatory Guide 1.97.	Conformance with no exceptions identified.	7.5
7.6 Interlock Systems Important to Safety	1. SRP Appendix 7.1-C provides SRP acceptance criteria for safety system compliance with 10 CFR 50.55a(h). 2. SRP Appendix 7.1-B provides SRP acceptance criteria for protection system compliance with 10 CFR 50.55a(h).	Conformance with no exceptions identified.	7.6

DCD_07-14_BTP-45

Table 1.9.2-7 US-APWR Conformance with Standard Review Plan Chapter 7 Instrumentation and Controls (Sheet 6 of 22)

SRP Section and Title	SRP Excerpt Indicating Acceptance Criteria for DCD	Status	Appears in DCD Chapter/Section
7.6 Interlock Systems Important to Safety (continued)	3. SRP Appendix 7.1-D provides SRP acceptance criteria for digital I&C compliance with IEEE Std 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," as endorsed by Regulatory Guide 1.152, Revision ~~2~~3, "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants."		
7.7 Control Systems	1. SRP Appendix 7.1-C provides SRP acceptance criteria for safety system compliance with 10 CFR 50.55a(h). Although compliance with IEEE Std. 603-1991 is required by 10 CFR 50.55a(h) only for safety systems, the criteria of IEEE Std. 603-1991 may be used as review guidance for any I&C system. Therefore, for control systems, the reviewer may use the concepts in IEEE Std. 603-1991 as a starting point. 2. SRP Appendix 7.1-B provides SRP acceptance criteria for protection system compliance with 10 CFR 50.55a(h). 3. SRP Appendix 7.1-D provides SRP acceptance criteria for digital I&C compliance with IEEE Std. 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," as endorsed by Regulatory Guide 1.152, Revision ~~2~~3, "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants." 4. Item II.Q, "Defense Against Common-Mode Failures in Digital Instrument and Control Systems," of the Staff Requirements Memorandum on SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light Water Reactor (ALWR) Designs," provides guidance on Defense-in-Depth and Diversity. SRP BTP 7-19 provides additional guidance.	Conformance with no exceptions identified.	7.7

DCD_07-14_BTP-45

DCD_07-14_BTP-45

Table 1.9.2-7 US-APWR Conformance with Standard Review Plan Chapter 7 Instrumentation and Controls (Sheet 7 of 22)

SRP Section and Title	SRP Excerpt Indicating Acceptance Criteria for DCD	Status	Appears in DCD Chapter/Section
7.8 Diverse Instrumentation and Control Systems	1. For plants with a digital RTS or ESFAS, the NRC position on D3 should be especially noted. This position is contained in Item II.Q, "Defense Against Common-Mode Failures in Digital Instrument and Control Systems," of the Staff Requirements Memorandum on SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs." SRM requirements applicable to diverse I&C functions are as follows: "If a postulated common-mode failure could disable a safety function, then a diverse means, with a documented basis that the diverse means is unlikely to be subject to the same common-mode failure [as the safety system], shall be required to perform either the same function [as the safety system function that is vulnerable to common mode failure] or a different function [that provides adequate protection]. The diverse or different function may be performed by a non-safety system if the system is of sufficient quality to perform the necessary functions under the associated event conditions." "A set of displays and controls located in the main control room shall be provided for manual system-level actuation of critical safety functions and monitoring of parameters that support the safety functions. The displays and controls shall be independent and diverse from the safety computer system[s] ..." 2. SRP Appendix 7.1-C provides SRP acceptance criteria for safety system compliance with 10 CFR 50.55a(h). 3. SRP Appendix 7.1-B provides SRP acceptance criteria for protection system compliance with 10 CFR 50.55a(h). 4. SRP Appendix 7.1-D provides SRP acceptance criteria for digital I&C compliance with IEEE Std 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," as endorsed by Regulatory Guide 1.152, Revision ~~2~~3.	Conformance with no exceptions identified.	7.8
7.9 Data Communication Systems	1. SRP Appendix 7.1-C provides SRP acceptance criteria for safety system compliance with 10 CFR 50.55a(h). 2. SRP Appendix 7.1-B provides SRP acceptance criteria for protection system compliance with 10 CFR 50.55a(h).	Conformance with no exceptions identified.	7.9

DCD_07-14_BTP-45

Table 1.9.2-7 US-APWR Conformance with Standard Review Plan Chapter 7 Instrumentation and Controls (Sheet 8 of 22)

SRP Section and Title	SRP Excerpt Indicating Acceptance Criteria for DCD	Status	Appears in DCD Chapter/Section
7.9 Data Communication Systems (continued)	3. SRP Appendix 7.1-D provides SRP acceptance criteria for digital I&C compliance with IEEE Std. 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," as endorsed by Regulatory Guide 1.152, Revision ~~2~~3.		
Appendix 7-A: General Agenda, Station Site Visits	This SRP Appendix establishes standards for general agendas and site visits. It does not establish any unique acceptance criteria.	Not applicable. SRP establishes no specific acceptance criteria.	N/A
Appendix 7-B Acronyms, Abbreviations, and Glossary	This SRP Appendix establishes standardized acronyms, abbreviations, and glossary. It does not establish any unique acceptance criteria.	Not applicable. SRP establishes no specific acceptance criteria.	N/A

DCD_07-14_BTP-45

Appendix C Software Secure Development and Operational Environment Features

1. Introduction

This Appendix C describes conformance of the design, production and maintenance of the PSMS application software to the secure development and operational environment requirements of RG 1.152, Rev.3.

The PSMS provides many design features and defensive strategies to addressing the issue of application software secure development and operational environment ~~design features~~ as described in this Technical Report, MUAP-07017 "US-APWR Software Program Manual", and the following related documents;

a. Design Control Document (DCD) for the US-APWR Section 7.9
b. Safety I&C System Description and Design Process, MUAP-07004
c. Safety System Digital Platform -MELTAC-, MUAP-07005
d. MELTAC Platform Basic Software Program Manual, JEXU-1012-1132

The secure development and operational environment for the design, production and maintenance of the PSMS application software is described in this Technical Report, MUAP-07017 "US-APWR Software Program Manual".

The MELTAC digital platform is applied to the PSMS. The secure development and operational environment for the design, production and maintenance of the MELTAC digital platform basic software is described in ~~Technical Report,~~ JEXU-1012-1132 "MELTAC Platform Basic Software Program Manual (Reference 24)" The conformance to ~~describes compliance to~~ the secure development and operational environment requirements of RG 1.152, Rev. ~~2~~3 for future changes to the basic software is also described in JEXU-1012-1132 "MELTAC Platform Basic Software Program Manual (Reference 24)".

2. Conformance to RG 1.152 Rev.3

This Appendix C describes conformance of the secure development and operational environment for the design, production and maintenance of the PSMS application software to the requirements of RG 1.152, Rev. 3. The section numbers follow the sections in RG 1.152, rev.3. This conformance description excludes PSMS application software life cycle process phases for Section 2.6 "Installation, Checkout, and Acceptance Testing", Section 2.7 "Operations Phase", Section 2.8 "Maintenance Phase", and Section 2.9 "Retirement Phase". Security features for these life cycle process phases are addressed in other regulatory guidance, such as RG 5.71 "Cyber Security Programs for Nuclear Facilities". Therefore addressing compliance to security related regulatory criteria for these life cycle process phases is outside the scope of this Appendix C.

C.2.1 Concepts Phase

Staff Position 1

Requirement
In the concepts phase, the licensee ~~and developer~~ should identify digital safety system design features ~~that should be implemented~~ required to establish a secure operational environment for the system. A licensee should describe these design features as part of its

application.
Analysis
Security-Related Information - Withheld Under 10 CFR 2.390
Evaluation
Compliance

Staff Position 2

Requirement
The licensee ~~and developer~~ should ~~perform an~~ assess~~ment to identify~~ the digital safety system's potential susceptibility to inadvertent access and undesirable behavior from connected systems over the course of the system's life_cycle that could degrade ~~the system's~~ its reliable operation. This assessment should identify the potential challenges to maintaining a secure operational environment for the digital safety system and ~~the challenges to maintaining~~ a secure development environment for ~~the system's~~ development life_cycle phases. The results of the analysis should be used to establish design feature requirements (for both hardware and software) to establish a secure operational environment and protective measures ~~that are required~~ to maintain it~~a secure development environment~~.
Analysis
Security-Related Information - Withheld Under 10 CFR 2.390

{{[Security-Related Information - Withheld Under 10 CFR 2.390]}}

Evaluation
Compliance

Staff Position 3

Requirement
The licensee should not ~~implement~~ allow remote access to the safety system. For the purpose of this guidance, remote access is defined ~~to be~~ as the ability to access a computer, node, or network resource that performs a safety function or that can ~~impact~~ affect the safety function from a computer or node that is located in an area with less physical security ~~(e.g., outside the protected area)~~ than the safety system (e.g., outside the protected area). Other NRC staff positions and guidance govern unidirectional and bidirectional data communications between safety and nonsafety digital systems.
Analysis
{{[Security-Related Information - Withheld Under 10 CFR 2.390]}}
Evaluation
Compliance

C.2.2 Requirements Phase

C.2.2.1 System Features

Staff Position 1

Requirement
The licensees ~~and developers~~ should define the ~~secure operational environment~~ functional performance requirements and system configuration for a secure operational environment; interfaces external to the systems; and ~~the~~ requirements for qualification, human factors engineering, data definitions, documentation for the software and hardware, installation and acceptance, operation and execution, and maintenance.

Analysis
Security-Related Information - Withheld Under 10 CFR 2.390
Evaluation
Compliance

Staff Position 2

Requirement
The design feature requirements intended to maintain a secure operating environment and ensure reliable system operation should be part of the overall system requirements. Therefore, the verification ~~and validation~~ process of the ~~overall system~~ requirements phase should ensure the correctness, completeness, accuracy, testability, and consistency of the system's ~~secure operational environment design~~ SDOE feature ~~requirements~~.
Analysis
Security-Related Information - Withheld Under 10 CFR 2.390

Security-Related Information - Withheld Under 10 CFR 2.390
Evaluation
Compliance

Staff Position 3

Requirement
Requirements specifying the use of pre-developed software and systems (e.g., reused software and commercial off-the-shelf (COT) systems) should address the reliability of the safety system (e.g., by using pre-developed software functions that have been tested and are supported by operating experience).
Analysis
Security-Related Information - Withheld Under 10 CFR 2.390
Evaluation
Compliance

C.2.2.2 Development Activities

Requirement
During the ~~development of~~ requirements phase, ~~measures~~ the licensee should ~~be taken to ensure that the requirements development process and documentation are secure such that the system does not contain undocumented code (e.g., backdoor coding and dead code), unwanted functions or applications, and any other coding that could adversely impact the integrity or reliability of the digital safety system~~ prevent the introduction of unnecessary or extraneous requirements that may result in inclusion of unwanted or unnecessary code.
Analysis
Security-Related Information - Withheld Under 10 CFR 2.390
Evaluation
Compliance

C.2.3 Design Phase

C.2.3.1 System Features

Staff Position 1

Requirement
The safety system ~~secure operational environment~~ design features for a secure operational environment identified in the system requirements specification should be translated into specific design configuration items in the system design description. Licensees should be aware that digital safety systems will be considered Critical Digital Assets and must adhere to the requirements of 10 CFR 73.54. Regulatory Guide 5.71 describes an acceptable defensive architecture to comply with 10 CFR 73.54. The architecture described in the guidance would have licensees place all digital safety systems in the highest level of their defensive architecture and only permit one-way communication (if any communication is desired) from the digital safety system to other systems in lower levels of the defensive architecture. Licensees should be aware that Section B.1.4 of Appendix B to Regulatory Guide 5.71 notes that one-way communications should be enforced using hardware mechanisms. A licensee's adherence to the provisions of 10 CFR 73.54 will be evaluated per regulatory programs specific to that regulation. The safety system ~~secure operational environment~~ design configuration items for a secure operational environment intended to ensure reliable system operation should address control over (1) physical and logical access to the system functions, (2) use of safety system services, and (3) data communication with other systems. Design configuration items that incorporate pre-developed software into the safety system should address how ~~the predeveloped~~ this software will not challenge the secure operational environment for the safety system.
Analysis
Security-Related Information - Withheld Under 10 CFR 2.390

Security-Related Information - Withheld Under 10 CFR 2.390

Evaluation
Compliance

Staff Position 2

Requirement
Physical and logical access control features should be based on the results of the assessment performed in the concepts phase of the life_cycle. The results of this assessment may identify the need for more complex access control measures, such as combination of knowledge (e.g., password), property (e.g., key and smart-card), or personal features (e.g., fingerprints), rather than just a password.
Analysis

Security-Related Information - Withheld Under 10 CFR 2.390

Security-Related Information - Withheld Under 10 CFR 2.390

Evaluation
Compliance

C.2.3.2 Development Activities

Requirement
During the design phase, ~~The development~~ measures should ~~delineate the standards and procedures that will confirm with the applicable design controls to ensure that the system design products (hardware and software) do not contain undocumented code (e.g., back door coding), unwanted functions or applications, and any other coding that could adversely impact the reliable operation of the digital safety system~~ be taken to prevent the introduction of unnecessary design features or functions that may result in the inclusion of unwanted or unnecessary code.
Analysis
Security-Related Information - Withheld Under 10 CFR 2.390
Evaluation
Compliance

C.2.4 Implementation Phase

C.2.4.1 System Features

Requirement
The developer should ensure that the transformation ~~of the secure operational environment~~ from the system design specification to design configuration items of the secure operational environment ~~from the system design specification~~ is correct, accurate, and complete.
Analysis
Security-Related Information - Withheld Under 10 CFR 2.390
Evaluation
Compliance

C.2.4.2 Development Activities

Staff Position 1

Requirement
The developer should implement secure operational environment procedures and standards to minimize and mitigate any inadvertent or inappropriate alternations of the development system. The developer's standards and procedures should include testing, (such as scanning), as appropriate, to address undocumented code or functions that might (1) allow unauthorized access or use of the system or (2) cause systems to behave outside of the system requirements or in an unreliable manner. The developer should account for hidden functions and vulnerable features embedded in the code, ~~and~~ their purpose and their impact on the integrity and reliability of the safety system. These functions should be removed or (as a minimum) addressed (e.g., as part of the failure modes and effects analysis of the application code) to prevent any unauthorized access or ~~impact~~ degradation of the reliability of the safety system.
Analysis
Security-Related Information - Withheld Under 10 CFR 2.390

Security-Related Information - Withheld Under 10 CFR 2.390

Evaluation
Compliance

Staff Position 2

Requirement
COTS systems are likely to be proprietary and generally unavailable for review. In addition, a reliable method may not exist for ~~use in~~ determining the complete set of system behaviors inherent in a given operating system (e.g., operating system suppliers often do not provide access to the source code for operating systems and callable code libraries). In such cases, unless the application developer can modify such systems, the ~~development activity~~ developer should ensure that the features within the operating system do not compromise the required ~~secure operational environment~~ design features of the secure operational environment so as to degrade ~~system in such each a manner that~~ the reliability of the digital safety system ~~would be degraded~~.
Analysis
Security-Related Information - Withheld Under 10 CFR 2.390

Security-Related Information - Withheld Under 10 CFR 2.390

Evaluation
N/A

C.2.5 Test Phase

C.2.5.1 System Features

Requirement
The secure operational environment design requirements and configuration items intended to ensure reliable system operation should be part of the validation effort for the overall system requirements and design configuration items. Therefore, ~~secure operational environment~~ design configuration items for the secure operational environment are just one element of the overall system validation. Each system ~~secure operational environment~~ design features of the secure operational environment should be validated to verify that the implemented feature achieves its intended function to protect against inadvertent access ~~and/~~or the efforts of undesirable behavior of connected systems and does not degraded the safety system's reliability.
Analysis
Security-Related Information - Withheld Under 10 CFR 2.390

Security-Related Information - Withheld Under 10 CFR 2.390
Evaluation
Compliance

C.2.5.2 Development Activities

Requirement
The developer should correctly configure and enable the ~~secure operational environment~~ design features of the secure operational environment ~~correctly~~. The developer should also test the system hardware architecture, external communication devices, and configurations for unauthorized pathways and system integrity. Attention should be focused on built-in original equipment manufacturer features.
Analysis
Security-Related Information - Withheld Under 10 CFR 2.390
Evaluation
Compliance

C.2.6 Summary

The scope of the PSMS application software secure development and operational environment responsibilities include the Plant Requirements Phase through the Test Phase, as described in RG 1.152, rev.3. The combination of the information in the following documents and this

document (MUAP-07017) fully address the software and data secure development and operational environment issues associated with the PSMS application software;

a. Design Control Document (DCD) for the US-APWR Section 7.9
b. Safety I&C System Description and Design Process, MUAP-07004
c. Safety System Digital Platform -MELTAC-, MUAP-07005
d. MELTAC Platform Basic Software Program Manual, JEXU-1012-1132

The secure operational environment design for the PSMS application software for installation, checkout and acceptance testing, operation, maintenance, and retirement life cycle phases are outside the scope of this SPM.

3. Secure Development and Operational Environment Assessment for Potential Unauthorized Changes of PSMS Application Software

Left without a secure development and operational environment, the PSMS application software may be incorrectly changed by unauthorized activities of a user or developer. The potential unauthorized activities of the PSMS application software development, from the System Requirements Phase through the Test Phase, are as follows;

Security-Related Information - Withheld Under 10 CFR 2.390

The following generic defenses against undesired PSMS application software changes is performed throughout each phase of the PSMS application software life cycle process as discussed in Section 3.1.4 of this SPM:

Security-Related Information - Withheld Under 10 CFR 2.390

Security-Related Information - Withheld Under 10 CFR 2.390

In addition to the general secure development and operational environment design defenses described above, additional the secure development and operational environment measures for specific life cycle process of the PSMS application software are described below.

3.1 Defense against Unauthorized Changes in Requirements Phase

Security-Related Information - Withheld Under 10 CFR 2.390

The SysRS and related documents are checked by the VVT which is specified by this SPM. Therefore, the insertion of undesired requirements that introduce the secure development and operational environment vulnerabilities would be detected and corrected. The VVT review assures that the PSMS application software secure development and operational environment

requirements are correctly included and unauthorized functionality is not included. The VVT participants, review scope, and review findings are documented as required by the SVVP in Section 3.10 which are specified by this SPM. The SysRS for the PSMS application software and related documents are versioned and released as required by the Software Configuration Management Plan (SCMP) which are specified by Section 3.11 of this SPM.

The secure development and operational environment measures that ensure the System Requirements Phase output products are protected from unauthorized alteration after the IV&V and final approval are described in the following Table 3.1.

Table 3.1: Secure Development and Operational environment Measures of the Requirements Phase Software and Documents Development/Storage Environment

Security-Related Information - Withheld Under 10 CFR 2.390

The secure development and operational environment design assessment conducted through the IV&V of the System Requirements Phase output products, confirms the System Requirement Phase output products adequately reflect the secure development and operational environment design features of the Plant Requirements Phase, and that no ~~unintended~~ unwanted, unneeded and undocumented functions have been added.

3.2 Defense against Unauthorized Changes in Design Phase

The SysDD is developed during this phase, in accordance with the SDP and SSP, based on the SysRS which is output of the System Requirements Phase, and provides the necessary system, functional requirements, detail functions and logics, software specifications and hardware specifications and software and hardware interface requirements.

Security-Related Information - Withheld Under 10 CFR 2.390

{[Security-Related Information - Withheld Under 10 CFR 2.390]}

Multiple SysDD are prepared for the various functions of the PSMS (e.g., RPS, ESFAS, SLS, etc.). When each SysDD is completed by the DT, the VVT, as indicated in Section 2.2 of this SPM, shall verify each SysDD. The VVT review shall ensure that all PSMS application software requirements identified in the SysRS are properly reflected in the SysDD. In addition, the VVT shall ensure there are no additional functions that are not traceable to the SysRS. Verification of the SysDD shall be performed in accordance with Section 3.10 of this SPM.

The SysDD and related documents are checked by the VVT which is specified by this SPM. Therefore, the insertion of undesired designs introducing the secure development and operational environment vulnerabilities would be detected and corrected. The VVT review assures that the secure development and operational environment requirements are correctly included and unauthorized functionality is not included. The IV&V review assures that the functionality specified by the SysRS and related documents are included and built into the SysDD and related documents. The VVT participants, review scope, and review findings are documented as required by the SVVP which are specified by this SPM. The SysDD and related documents are versioned and released as required by the SCMP which are specified by Section 3.11 of this SPM.

The secure development and operational environment measures that ensure the Design Phase output products are protected from unauthorized alteration after the IV&V and final approval are described in Table 3.1 and 3.3.

The secure development and operational environment design assessment conducted through the IV&V of the Design Phase output products, confirms the Design Phase output products adequately reflect the secure development and operational environment design features of the System Requirements Phase and that no ~~unintended~~ unwanted, unneeded and undocumented functions have been added.

3.3 Defense against Unauthorized Changes in Implementation Phase

The PSMS application software is implemented on each target safety system in the PSMS hardware during this phase, in accordance with the SDP and SSP. Input from the SysRS and the SysDD provides the necessary information to implement the PSMS application software.

The DT shall be responsible for developing, maintaining and updating the PSMS application software, in accordance with the design documented in the SysRS and the SysDD, and design process defined in this SPM.

{[Security-Related Information - Withheld Under 10 CFR 2.390]}

Security-Related Information - Withheld Under 10 CFR 2.390

Software units generated during this phase are tested by the VVT in accordance with the STP and the SVVP which are specified in Sections 3.12 and 3.10 of this SPM, respectively.

The PSMS application software is checked by the VVT which is specified by this SPM. Therefore, the insertion of undesired designs introducing secure development and operational environment vulnerabilities would be detected and corrected. The VVT review assures that the secure development and operational environment requirements are correctly included and unauthorized functionality is not included. The VV review assures that the functionality specified by the SysDD and related documents are included and built into the application software documents. The VVT participants, review scope, and review findings are documented as required by the SVVP which are specified by this SPM. The PSMS application software is versioned and released as required by the SCMP which are specified by Section 3.11 of this SPM.

Security-Related Information - Withheld Under 10 CFR 2.390

Table 3.3: Secure Development and Operational Environment Measures of the Post-Design Phase Software Development/Storage Environment

Security-Related Information - Withheld Under 10 CFR 2.390

The VVT participants, review scope, and review findings are documented as required and specified by the SVVP in Section 3.10 of this SPM. The PSMS application software and related documents are versioned and released as required by the SCMP which are specified by Section 3.11 of this SPM.

Security-Related Information - Withheld Under 10 CFR 2.390

The integration personnel shall confirm the following points to evaluate the integration results;

Security-Related Information - Withheld Under 10 CFR 2.390

The secure development and operational environment design assessment conducted through IV&V of the Implementation Phase output products, confirms the Implementation Phase output products adequately reflect the secure development and operational environment design features of the Design Phase, and that not ~~unintended~~ unwanted, unneeded and undocumented functions have been added.

3.4 Defense against Unauthorized Changes in Test Phase

Test reports contain a summary of the test results and attachments with all detailed results and logs, and the configuration of the test environment. The component and system V&V tests are managed by the VVT and performed under control of the VVT. The VVT audits all tests and reviews all detail test results and test logs. Therefore, the VVT can detect unauthorized changes of test results, or not reporting adverse findings documented in the test logs, and these issues are excluded by reviews performed by the VVT in accordance with the SVVP in Section 3.10 of this SPM.

{{ Security-Related Information - Withheld Under 10 CFR 2.390 }}

3.5 PSMS Design Features to Minimize Application Software Secure Development and Operational Environment Vulnerabilities

The PSMS has multiple defensive layers and secure development and operational environment features to minimize the potential for unauthorized changes of the PSMS application software and thereby protect the system from secure development and operational environment vulnerabilities.

{{ Security-Related Information - Withheld Under 10 CFR 2.390 }}

Security-Related Information - Withheld Under 10 CFR 2.390

Security-Related Information - Withheld Under 10 CFR 2.390

4. Conclusion

The PSMS application software exhibits different degrees of susceptibility to unauthorized changes by a user or developer at different phases of the PSMS application software life cycle process. The analysis in the previous sections addressed life cycle phases, from the System Requirements Phase to the Test Phase, to a detail commensurate with the potential for unauthorized changes by a user or developer, and to a level of detail appropriate for the each life cycle phase. The measures imposed by the PSMS engineering procedures assure that all countermeasures against unauthorized changes at any time in the PSMS application software development life cycle are adequately addressed.

The secure development and operational environment design assessments conducted through IV&V for each subsequent PSMS application software life cycle process confirm that the secure development and operational environment related design features are progressing through the development process, in accordance with this SPM. In addition, these secure development and operational environment design assessments ensure ~~unintended~~ unwanted, unneeded and undocumented functions have not been introduced at any point in the PSMS application software life cycle process.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

2/27/2012

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

RAI NO.:	**No. 837-5945 Revision 3**
SRP SECTION:	**07.01 – Instrumentation and Controls - Introduction**
APPLICATION SECTION:	**07.01 – Instrumentation and Controls - Introduction**
DATE OF RAI ISSUE:	**10/11/2011**

QUESTION NO. : 07.01-44

GDC 22, "Protection system independence," requires in part that the protection system be designed to assure that the effects of natural phenomena and of normal operating, maintenance, and testing do not result in loss of protection function.

10 CFR 50.55a(h), "Protection and Safety Systems," requires compliance with IEEE Std. 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," and the correction sheet dated January 30, 1995. Particularly, Criterion 5.5, System Integrity, states "The safety systems shall be designed to accomplish their safety functions under the full range of applicable conditions enumerated in the design basis." IEEE Std 7-4.3.2-2003, Section 5.5.2, states "Test and calibration functions shall not adversely affect the ability of the computer to perform its safety function." Branch Technical Position (BTP) 7-17 states, as part of the acceptance criteria for surveillance testing that, "The safety classification and quality of the hardware and software used to perform periodic testing should be equivalent to that of the tested system."

Several methods of software checks, which are of the same classification as the safety system as BTP 7-17 states, have been identified in the MELTAC safety system software. However the software to implement the memory integrity check (MIC) is not of the same safety classification nor has the efficiency of this check been identified versus that of the checks in the safety system software. It has not been identified if it checks for different types of errors and the reliability of those checks. The staff requests MHI to identify the relative effectiveness of the checksum, the CRC and other safety system software checks versus that of the memory integrity check. Particularly, the amount of overlap in terms of types of software faults and the reliability of the memory integrity check. The staff requests MHI to address if there have been tests and analyses to determine the rate at which the memory integrity check will identify errors and if it can determine expected errors (changes) vs. unexpected errors.

ANSWER:

The following table summarizes the differences between the Memory Integrity Check (MIC), which is conducted every 24 months, and Self-diagnosis Memory Check (SMC), which is conducted continuously on-line, including the effectiveness of these two functions.

Memory Integrity Check vs. Self-diagnosis Memory Check

The versions of the application software and the basic software are controlled through software configuration management. The application software is controlled and maintained in accordance with the Software Configuration Management Plan as described in "US-APWR Software Program Manual" (MUAP-07017). The basic software is controlled and maintained in accordance with the Software Configuration Management Plan contained in "MELTAC Platform Basic Software Program Manual" (JEXU-1012-1132).

The following table summarizes the software differences that can be detected by the MIC and SMC.

Detectable errors by the MIC and SMC

The following features minimize the potential for unexpected software change errors that could result in total PSMS failure between test intervals: (1) Access Control: the PSMS software is physically secured, as described in Section 7.9.2.5 of the DCD, and (2) Software Configuration Management: the PSMS software is maintained in accordance with Section 3.11 of "US-APWR Software Program Manual" (MUAP-07017).

Software design of the MIC function will be performed under an approved App.B-based QAP, assuring that the software quality of the MIC function is equivalent to that of a safety system. Therefore, the design for surveillance testing complies with the guidance of BTP 7-17.

As described in Section 4.4.1 of "Safety I&C System Description and Design Process" (MUAP-07004), the MIC is conducted with the train for the controller to be tested in a bypass condition. Administrative controls assure the remaining three trains are still in service. This ensures that performance of the MIC will not result in a loss of safety function of the PSMS.

Impact on DCD
There is no impact on the DCD.

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

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

Impact on PRA
There is no impact on the PRA.

Impact on Technical / Topical Report

Section 4.4.1 of MUAP-07004 will be revised as follows:

> This function is used during periodic surveillance tests to confirm that the software in the controller is the same as the off-line version, and therefore has not changed. This test confirms the functional integrity of PSMS software applications without the need to perform functional logic tests. The Memory Integrity Check (MIC) is conducted with the train for the controller to be tested in a bypass condition. Administrative controls assure the remaining three trains are still in service. This ensures that performance of the MIC will not result in a loss of safety function of the PSMS.
>
> As described in the MELTAC Technical Report, MUAP-07005, Section 4.1.7.2, software design of the MIC function will be performed under an approved Appendix B program. This assures that the software quality of the MIC function is equivalent to that of a safety system. Therefore, the design for surveillance testing complies with the guidance of BTP 7-17.
>
> The following features minimize the potential for unexpected software change errors that could result in total PSMS failure between test intervals: (1) Access Control: the PSMS software is physically secured, as described in Section 7.9.2.5 of the DCD, and (2) Software Configuration Management: the PSMS software is maintained in accordance with Section 3.11 of "US-APWR Software Program Manual" (MUAP-07017).

Section 4.1.7.2 of MUAP-07005 will be revised as follows.

> 4.1.7.2 Software Memory Integrity

The MELTAC engineering tool includes a manually initiated Memory Integrity check (MIC) function which ~~automatically~~ compares the software memory in the controller, bit by bit, with a controlled copy of the software stored off-line.
This function is used during the Software Memory Integrity Test to ~~confirm~~ provide confirmation that the software in the controller is the same as the off-line version, and, therefore, has not changed or failed. This test confirms the functional integrity of both the ~~controller~~ basic software and application software residing in the controller. The Software Memory Integrity Test is conducted periodically for every controller in the system.

By confirming the basic software, the Software Memory Integrity ~~t~~Test confirms the CPU instructions stored in F-ROM for all MELTAC functions described throughout this document, including the self-diagnostic functions. By confirming the application software, the Software Memory Integrity ~~t~~Test also confirms the CPU instructions stored in F-ROM for all functional logic required for the safety functions of the application.

The following table summarizes the differences between the Software Memory Integrity Test which is conducted periodically, and Self-diagnosis Memory Check (see Section 4.1.5.2.1) which is conducted continuously on-line, including the effectiveness of these two functions.

Table 4.1-8 Software Memory Integrity Test vs. Self-diagnosis Memory Check

The versions of the application software and the basic software are controlled through software configuration management. The application software is controlled and maintained under the Software Configuration Management Plan as described in "US-APWR Software Program Manual" (MUAP-07017). The basic software is controlled and maintained in accordance with the Software Configuration Management Plan contained in the "MELTAC Platform Basic Software Program Manual" (JEXU-1012-1132).

The following table summarizes the software differences that can be detected by the MIC and Self-diagnosis Memory Check.

Table 4.1-9 Detectable errors by the MIC and SMC

The periodic manual tests (the process input and output test, and the safety VDU test) ensure the CPU is capable of executing instructions from both F-ROM for basic software and F-ROM for application software. This encompasses the instructions that control continuous self-diagnostics, and the instructions that control the safety functions of monitoring process measurements and actuating plant components. Therefore, through the aggregate of periodic manual tests and continuous self-diagnostic tests, the complete functionality of the safety system is confirmed.

Docket No. 52-021
MHI Ref: UAP-HF-12052

Enclosure 4

Docket No. 52-021
UAP-HF-12052

Amended Response to Request for Additional Information
for Chapter 7

February 2012

Non-Proprietary Version

This Enclosure includes following response of RAIs

RAI No. 688-5273 Revision 2, Question No.: 07.07-32

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

02/27/2012

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No. 52-021

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

QUESTION NO. : 07.07-32

In subsection 7.7.2.6, "Use of Digital Systems," of the US-APWR DCD, it states that "*The PCMS and PSMS utilize the same basic software. In addition, the PCMS application software is developed using a structured process similar to that applied to development of the PSMS application software.*" Similarly, in subsection 5.1.8 of MUAP-07004 (Revision 5), "Safety I&C System Description and Design Process," it states that "*The MELTAC platform that is applied to the PCMS is essentially the same as the MELTAC platform applied to the PSMS.*"

In the Abstract of MUAP-07005 (Revision 6), "Safety System Digital Platform – MELTAC -," it states that "*the MELTAC Platform has been developed using a rigorous safety related design process that ensures suitable hardware and software quality and reliability for critical applications such as the Reactor Protection System or Engineered Safety Features Actuation System.*" SRP Section 7.7, "Control Systems;" under the section "Review Procedures," states that "*To minimize the potential for control system failures that could challenge safety systems, control system software should be developed using a structured process similar to that applied to safety system software. Elements of the review process may be tailored to account for the lower safety significance of control system software. Refer to SRP Appendix 7.0-A and SRP Appendix 7.1-D for guidance on digital system review.*" Please clarify what exactly are the differences between the MELTAC platform for the PCMS compared to that of the PSMS?

Also, identify which functions in the PCMS are important to safety, if any? If so, what are the additional requirements, and the process, beyond the non-safety (software and hardware) PCMS which will be applied? Ensure that the function discussed in MUAP-07004 (Revision 5), "Safety I&C System Description and Design Process," Appendix A, section A.6.3 is included in your response.

ANSWER:

1. The differences between the MELTAC Platform for the PCMS compared to that of the PSMS are quality assurance methods including software life cycle processes.
2. Scope of non-safety systems but required augmented quality will be identified in Section 7.1.3.20 of the DCD Rev. 4 (Attachment-1). Quality assurance requirement and equipment qualification requirement will be provided in Section 3.2.2 of the DCD Rev. 4 (Attachment-2). Especially, software life cycle requirements, including V&V, is provided in Appendix D of "Software Program Manual, MUAP-07017 Rev. 4" (Attachment-3).
3. Section 7.1.3.20 of the DCD Rev. 4 will be revised to incorporate the function discussed in A.6.3 of "Safety I&C System Description and Design Process, MUAP-07004 Rev. 5".

Impact on DCD

Following description will be added in section 7.1.3.20 of the DCD Rev. 4 (See Attachment-1).

7.1.3.20 Augmented Quality Systems

The System Quality Group Classifications are described in Subsection 3.2.2.5. The actual scopes of augmented quality systems and the regulatory requirements applied for each system are shown in Table 7.1-5. These systems are classified as Equipment Class 5. On the other hands, systems that have impact on continuous power generation are classified as Class 9.

The quality assurance requirement and equipment qualification requirement to Class 5 and 9 systems are as follows:

(1) Quality Assurance Requirements

- The pertinent QA requirement of 10 CFR 50, Appendix B is applied to Class 5 and 9 systems as described in Subsection 3.2.2.5.
- For application software of Class 5 systems, Appendix D of the US-APWR Software Program Manual (Reference 7.1-18) is applied.

(2) Equipment Qualification

- Equipment Qualification Program (Reference 7.1-25) is applied to Class 5 systems.
- Industry standards are applied to Class 9 systems.

Table 7.1-5 of the DCD Rev. 4 will be added as described in Attachment-1.

Impact on R-COLA

There is no impact on the R-COLA.

Impact on S-COLA

There is no impact on the S-COLA.

Impact on PRA

There is no impact on the PRA.

Impact on Technical / Topical Reports
There is no impact on the Technical / Topical Reports.

Federal Regulations (CFR), Part 50, Appendix B (Reference 7.1-19), and IEEE Std 7-4.3.2-2003 (Reference 7.1-20).

7.1.3.19 Identification

I&C equipments identification follows the guidance of RG 1.75, which endorses IEEE Std 384~~.~~-1992 (Reference 7.1-23). 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. DCD_07.01-30

Identification shall not require frequent use of reference material.

- Train A: Red with white lettering
- Train B: Green with white lettering
- Train C: Blue with white lettering
- Train D: Yellow with ~~B~~black lettering DCD_07.01-30
- Non-safety train: White with ~~B~~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.

7.1.3.20 Augmented Quality Systems DCD_07.01-27 DCD_07.01-32

The System Quality Group Classifications are described in Subsection 3.2.2.5. The actual scopes of augmented quality systems and the regulatory requirements applied for each system are shown in Table 7.1-5. These systems are classified as Equipment Class 5. On the other hands, systems that have impact on continuous power generation are classified as Class 9.

The quality assurance requirement and equipment qualification requirement to Class 5 and 9 systems are as follows:

(1) Quality Assurance Requirements DCD_07.01-27

- The pertinent QA requirement of 10 CFR 50, Appendix B is applied to Class 5 and 9 systems as described in Subsection 3.2.2.5. DCD_07.01-32
- For application software of Class 5 systems, Appendix D of the US-APWR Software Program Manual (Reference 7.1-18) is applied. This Appendix D establishes augmented quality requirements for the application software of the Equipment Class 5 systems and for the integration of the application software, basic software and hardware through integration testing.

(2) Equipment Qualification

- Equipment Qualification Program (Reference 7.1-25) is applied to Class 5 systems.
- Industry standards are applied to Class 9 systems.

7.1.4 Safety-Related Digital I&C Design Conformance to Essential Safety Criteria

DCD_07.01-25

A key design basis of the UR-APWR is to apply digital I&C technology to the PSMS. The purpose of this section is to describe overview of the PSMS design conformance to the following four essential safety criteria and one subjective attribute-simplicity.

1) Redundancy

2) Independence

3) Determinism (to ensure response time of data processing and communication)

4) Diversity

5) Simplicity

The above safety criteria are embodied in the underlying basis of IEEE Std 603-1991 (Reference 7.1-15). This section does not address conformance with all of the other IEEE Std 603-1991 criteria nor all of the other applicable regulatory guidance, codes, and standards; these items are described in the Safety I&C Technical Report (Reference 7.1-2).

The PSMS consists of the following five digital systems as shown in Figure 7.1-1.

1) Reactor protection system (RPS)

2) Engineered safety features actuation system (ESFAS)

3) Safety logic system (SLS)

4) Communication system (COM)

5) Safety-related human system interface system (HSIS)

DCD_07.07-32

Table 7.1-5 Scope of the Augmented Quality Systems

Items	Specific requirements for non-safety system	Augmented Quality
Safety Functions Controlled by O-VDUs	DI&C-ISG-04	Required
Safety Parameter Display System (SPDS)	10 CFR 50.34 (f)(2)(iv), "Additional TMI-Related Requirements" regarding the SPDS Control	Required
	NUREG 0737 Supplement 1, "Clarification of TMI Action Plan Requirements - Requirements for Emergency Response Capability", with respect to SPDS	Required
Alarms for Credited Manual Operator Actions	SECY-93-087, Item II. T, "Control Room Annunciator (Alarm) Reliability"	Required
Signal Selection Algorithm (SSA)	RG 1.153, "Criteria for Safety Systems"	Required
	IEEE 603-1991, Clause 6.3 "Interaction between the Sense and Command features and other Systems"	Required
Risk-significant non-safety I&C system	Risk-significant non-safety I&C system identified in Table 17.4-1	Required
Diverse Instrumentation and Control System	BTP 7-19, "Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems"	Required
	Generic Letter 85-06, "Quality Assurance Guidance for ATWS Equipment That Is Not Safety-Related"	Required

Note)

1. Bypass and Inoperable Indication (BISI): There is no augmented quality requirement.
2. Post Accident Monitoring Instrumentation: Type A, B, C and D are implemented in the PSMS and there is no augmented requirement for Type E.
3. Leak Detection System: Seismic required systems are implemented in the PSMS and there is no augmented requirement for others.

Attachment-2 to Response to RAI 688-5273 Question 07.07-32

Table 3.2-5 Classification of I&C systems (Sheet 1 of 3)

System	Equipment Class	Location	IEEE 603 Class	Quality[(1)] Assurance	Equipment[(2)] Qualification	Seismic[(3)] Category	Notes[(4)]
1. PSMS							
Reactor Protection System	3	R/B	Class 1E	1	1	I	
ESF Actuation System	3	R/B	Class 1E	1	1	I	
Safety Logic System	3	R/B	Class 1E	1	1	I	
Safety VDU Processor	3	R/B	Class 1E	1	1	I	
Communication System	3	R/B	Class 1E	1	1	I	
Safety Bus	3	R/B	Class 1E	1	1	I	
2. PCMS (DCS)							
Reactor Control System	5	A/B	N/A	2	1	NS	4, 6
CRDM Control System	9	A/B	N/A	2	2	NS	
Radiation Monitoring System	9	A/B	N/A	2	2	NS	
Rod Position Indication System	9	PCCV	N/A	2	2	NS	
Incore Nuclear Instrumentation System	9	A/B	N/A	2	2	NS	
BOP Control System	9	A/B	N/A	2	2	NS	
Turbine Protection System	9	A/B	N/A	2	2	NS	
Turbine EHG Control System	9	A/B	N/A	2	2	NS	
Electrical Control System	9	A/B	N/A	2	2	NS	
Unit Bus	5	R/B, A/B	N/A	2	1	NS	1, 2, 3, 4

Table 3.2-5 Classification of I&C systems (Sheet 2 of 3)

System	Equipment Class	Location	IEEE 603 Class	Quality[(1)] Assurance	Equipment[(2)] Qualification	Seismic[(3)] Category	Notes[(4)]
3. PCMS (HSIS)							
Alarm VDU Computer	5	A/B	N/A	2	1	NS	3
Operational VDU Computer (for OC)	5	A/B	N/A	2	1	NS	1, 2
Operating Procedure VDU Computer (for OC)	10	A/B	N/A	3	2	NS	
Large Display Computer (for LDP)	10	A/B	N/A	3	2	NS	
Alarm Logic Computer	5	A/B	N/A	2	1	NS	3
Process Recording Computer	10	A/B	N/A	3	2	NS	
Unit Management Computer	10	A/B	N/A	3	2	NS	
Operational VDU Computer (for TSC)	10	AC/B	N/A	3	2	NS	
Large Display Computer (for TSC)	10	AC/B	N/A	3	2	NS	
Supervisor Console	10	R/B	N/A	3	2	II	
Shift Technical Advisor Console	10	R/B	N/A	3	2	II	
Large Display Panel	10	R/B	N/A	3	2	II	
Station Bus	10	A/B	N/A	3	2	NS	
4. PSMS/PCMS							
Operator Console	3	R/B	Class 1E	1	1	I	
Remote Shutdown Console	3	R/B	Class 1E	1	1	I	

Table 3.2-5 Classification of I&C systems (Sheet 3 of 3)

System	Equipment Class	Location	IEEE 603 Class	Quality Assurance (1)	Equipment Qualification (2)	Seismic Category (3)	Notes (4)
5. DAS							
Diverse Actuation System	5	R/B	N/A	2	1	I (5)	5
Diverse HSI Panel	5	R/B	N/A	2	1	I (5)	5
6. Local							
Reactor Trip Breaker	3	R/B	Class 1E	1	1	I	
MG Set	5	R/B	N/A	2	1	NS	5

Notes:

(1) Identification number for "Quality Assurance"

1. The QA requirement of 10 CFR 50, Appendix B is applied.
   "Software Program Manual" (MUAP-07017) is applied.
2. The pertinent QA requirement of 10 CFR 50, Appendix B is applied.
   For Class 5 systems, Appendix D of "Software Program Manual" (MUAP-07017) is applied.
3. Industry Standards, ISO 9001, etc, are applied.

(2) Identification number for "Equipment Qualification"

1. "Equipment Qualification Program" (MUAP-08015) are applied.
2. Industry standards are applied.

For EMC/RFI emission, RG 1.180 is applied so that safety-related I&C equipment has no adverse EMC/RFI impact.

(3) Following augmented qualification requirements are applied concurrent with SSE, and IEEE 344-1987 is applied.

- Reactor Control System shall retain the function described in Note (4) 4, 6.
- Operational VDU Computer shall retain the function described in Note (4) 1, 2.
- Alarm VDU Computer and Alarm Logic Computer shall retain the function described in Note (4) 3.
- Unit Bus shall retain the functions described in Note (4) 1, 2, 3, 4.
- Diverse Actuation System and Diverse HSI Panel shall retain the function described in Note (4) 5.

(4) Identification number for "Note"

1. Safety Functions Controlled by O-VDU
2. Safety Parameter Display System (SPDS)
3. Alarms for Credited Manual Operator Actions
4. Signal Selection Algorithm (SSA)
5. Diverse Instrumentation and Control System
6. Risk-significant non-safety I&C system

(5) The DAS is categorized as Equipment Class 5 in accordance with its required non-safety-related function to cope with software common cause failure which is a beyond design basis event. On the other hand, the DAS is designed as Seismic Category I and powered by Class 1E UPSs, to cope with software common cause failure concurrent with seismic events.

<u>Attachment-3 to Response to RAI 688-5273 Question 07.07-32</u>

Appendix D Software Program Manual for Augmented Quality Systems

1. Scope

The basic and application software of the PSMS is classified as Class 1E as defined in IEEE Std 603-1991, and the basic and application software is classified as software integrity level 4 in accordance with Chapter 1 of RG 1.168 Rev. 1. The PSMS application software complies with this US-APWR Software Program Manual.

The Plant Control and Monitoring System (PCMS) is classified as a non- safety related system, but several subsystems and components in the PCMS have specific regulatory requirements. Therefore, these PCMS subsystems and components are classified as augmented quality. The System Quality Group Classifications are described in DCD Section 3 "Design of Structures, Systems, Components, and Equipment." The PCMS subsystems and components classified as augmented quality are categorized as Equipment Class 5, whereby they must meet selected QA requirements of 10 CFR 50 Appendix B as described in Section 3.2.2.5 of the DCD.

The equipment classes of all systems are listed in Table 3.2-2 of DCD Chapter 3, and the systems which are categorized as Equipment Class 5 require the augmented quality classification. The actual scopes of the augmented quality systems and the applied regulatory requirements for each system are described in Table 7.1.5 of DCD Chapter 7.

2. Software Life Cycle Requirements

The software life cycle processes of the PCMS application software selected for the augmented quality systems are listed in Table D-1.

2.1 Basic Software
For the hardware and basic software of the augmented quality PCMS subsystems and components, the pertinent QA requirements of 10 CFR 50, Appendix B as described in Section 3.2.2.5 of the DCD are required in the same manner as other Equipment Class 5 SSCs, such as structures, structural components, non digital I&C and electrical components.

The augmented quality program for the selected PCMS subsystem and component application software, which includes integration and final validation testing, encompasses the basic software and hardware. Therefore a unique basic software and hardware augmented quality program is not required.

2.2 Application Software
For the application software of the augmented quality PCMS subsystems and components, the software life cycle control requirements which are specified by this US-APWR Software Program Manual are applied as described in Table D-1.

Table D-1: Applicability of US-APWR SPM to Application Software of PCMS functions with augmented quality

Software Plans	Applicability
Software Management Plan (SMP)	A
Software Development Plan (SDP)	A
Software Quality Assurance Plan (SQAP)	N/A(1)
Software Integration Plan (SIntP)	A
Software Installation Plan (SInstP)	A
Software Maintenance Plan (SMaintP)	A
Software Training Plan (STrngP)	A
Software Operations Plan (SOP)	A
Software Safety Plan (SSP)	N/A
Software Verification and Validation Plan (SVVP)	A(2)
Software Configuration Management Plan (SCMP)	A
Software Test Plan (STP)	A
Output Documents	A(3)
Appendix C	A

Note: A-applicable N/A-not applicable
(1) Based on QA requirements for Equipment Class 5 Systems in Section 3.2.2.5 of the DCD.
(2) All V&V activities are conducted. However activities may be conducted by the Design Team or the V&V Team, and V&V independence is not required.
(3) Documents provided by VVT are not applicable.