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

April 28, 2009

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

Attention: Mr. Jeffrey A. Ciocco,

Docket No. 52-021
MHI Ref: UAP-HF-09216

**Subject: MHI's Responses to US-APWR DCD RAI No. 255-2110 Revision 1**

**Reference:** 1) "Request for Additional Information No. 255-2110 Revision 1, SRP Section: 14.03.05 – Instrumentations and Controls- Inspections, Tests, Analyses, and Acceptance Criteria Application Section: Section 14.3.5 of DCD" dated March 3, 2009.

With this letter, Mitsubishi Heavy Industries, Ltd. ("MHI") transmits to the U.S. Nuclear Regulatory Commission ("NRC") a document entitled "Responses to Request for Additional Information No. 255-2110 Revision 1."

Enclosed are the responses to Questions 14.03.05-10 through 14.03.05-21 that are contained within Reference 1.

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

Sincerely,

Y. Ogata

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

Enclosure:

1. Responses to Request for Additional Information No. 255-2110 Revision 1

CC: J. A. Ciocco
C. K. Paulson

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

D081
NRO

Docket No. 52-021
MHI Ref: UAP-HF-09216

Enclosure 1

UAP-HF-09216
Docket No. 52-021

# Responses to Request for Additional Information No. 255-2110
Revision 1

April 2009

## RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

**04/28/2009**

**US-APWR Design Certification**

**Mitsubishi Heavy Industries**

**Docket No. 52-021**

**RAI NO.:** **NO. 255-2110 REVISION 1**

**SRP SECTION:** **14.03.05 - Instrumentation and Controls- Inspections, Tests, Analyses, and Acceptance Criteria**

**APPLICATION SECTION:** **SECTION 14.3.5**

**DATE OF RAI ISSUE:** **03/03/2009**

---

**QUESTION NO.: 14.03.05-10**

Provide clarification on the commitment to provide information on all Class 1E cabinets, in Sections 2.5.1, 2.5.2, 2.5.4 and 2.5.6, layout and wiring details and indicate if an ITAAC will be performed to ensure that the cabinet layout and wiring conforms to the design.

In SRP Section 14.3, Section I. "Design Descriptions and Figures" for I&C equipment, states the cabinet and layout and wiring should be included in the hardware architecture descriptions.

---

**ANSWER:**

Class 1E I&C room locations are shown on Tier 1 drawing Figure 2.2-5. Control and interlock signal paths are shown on Tier 1 drawings such as Figures 2.5.1-1, 2.5.1-2, and 2.5.1-3. ITAAC will verify the key elements of the design descriptions. Greater detail is provided in Tier 2 Chapter 7 drawings.

Room layouts and arrangements will be developed during detailed design and are not now available. Internal cabinet layouts and wiring diagrams will be created during detailed design. ITAAC to verify conformance to the design descriptions, and to address specific design aspects such as environmental qualification, redundancy, electrical separation and independence as applicable, will include the Class 1E cabinets and wiring. Therefore MHI believes an ITAAC to ensure that the cabinet layout and wiring conforms to the design is not needed.

The following tables will be revised to add ITAAC for functional arrangement:

Table 2.5.2-3 Systems Required for Safe Shutdown Inspections, Tests, Analyses, and Acceptance Criteria. Note that Table 2.5.2-3 is revised by the following Questions:

- 14.03.05- 10, add ITAAC item 6
- 14.03.05- 17, add ITAAC Item 7
- 14.03.05- 18, add ITAAC Item 4
- 14.03.05- 19, add ITAAC Item 5

Table 2.5.4-2 Information Systems Important to Safety Inspections, Tests, Analyses, and Acceptance Criteria

**Impact on DCD**

See Attachment 1 for a mark-up of Tier 1 Section 2.5 with the changes as shown below.

**Table 2.5.2-3 Systems Required for Safe Shutdown Inspections, Tests, Analyses, and Acceptance Criteria**

| Design Commitment | Inspections, Tests, Analyses | Acceptance Criteria |
|---|---|---|
| 6. The functional arrangement of the Safe Shutdown System is as described in the Design Description and as shown in Figure 2.5.2-1. | 6. An inspection of the as-built Safe Shutdown System will be performed. | 6. The as-built Safe Shutdown System conforms to the functional arrangement as described in the Design Description and as shown in Figure 2.5.2-1. |

**Table 2.5.4-2 Information Systems Important to Safety Inspections, Tests, Analyses, and Acceptance Criteria**

| Design Commitment | Inspections, Tests, Analyses | Acceptance Criteria |
|---|---|---|
| 4. The functional arrangement of the Information Systems Important to Safety is as described in the Design Description and as shown in Figure 2.5.4-1 | 4. An inspection of the as-built Information Systems Important to Safety will be performed. | 4. The as-built Information Systems Important to Safety conform to the functional arrangement as described in the Design Description and as shown in Figure 2.5.4-1. |

**Impact on COLA**

There is no impact on the COLA.

**Impact on PRA**

There is no impact on the PRA.

## RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

**04/28/2009**

**US-APWR Design Certification**

**Mitsubishi Heavy Industries**

**Docket No. 52-021**

**RAI NO.:** **NO. 255-2110 REVISION 1**

**SRP SECTION:** **14.03.05 - Instrumentation and Controls- Inspections, Tests, Analyses, and Acceptance Criteria**

**APPLICATION SECTION:** **SECTION 14.3.5**

**DATE OF RAI ISSUE:** **03/03/2009**

---

**QUESTION NO.: 14.03.05-11**

Provide a discussion on the technically relevant Unresolved Safety Issues (USIs)/Generic Safety Issues (GSIs), Three Mile Island (TMI) items and operating experience related to the RT system and ESF systems in the ITAAC for the applicable Sections of 2.5.

To ensure that the ITAAC reflect the resolutions of technically relevant USIs/GSIs, TMI items, and operating experience requires that these be evaluated in Tier 1. SRP Section 14.3, states "Ensure that the ITAAC reflect the resolutions of technically relevant USIs/GSIs, TMI items, and operating experience." The staff did not find reference to USI/GSIs, TMI items and operating experience related to the RT system and ESF systems in the ITAAC. Revise the information in Tier 1 and Tier 2 of the DCD to include any reference to USI/GSIs, TMI items and operating experience, and modify the ITAAC.

---

**ANSWER:**

MHI has performed a comprehensive review of Unresolved Safety Issues (USIs) / Generic Safety Issues (GSIs), Three Mile Island (TMI) items and operating experience to assess relevance to the US-APWR design. The results of the review are presented in DCD Tier 2 Section 1.9. Specifically, Section 1.9.3 addresses Generic Issues and includes Table 1.9.3-1 which summarizes each issue and provides reference to the DCD Section that addresses the specific aspects of the issue. As a result of the review provided in Table 1.9.3-1, there are no items that are referenced to DCD Tier 2 Sections 7.2 for the Reactor Trip System or 7.3 for Engineered Safety Features. Therefore, there are no ITAAC that need to reflect the resolutions of technically relevant USIs or GSIs in Tier 1 Section 2.5.

Table 1.9.3-2 "Location of Description for Additional TMI-Related Requirements" provides an itemization of the location in the DCD that describe the requirements for the TMI Action Plan items. As a result of the review provided in Table 1.9.3-2, one item III.D.3.3 references DCD Section 7.3.1.5 pertaining to radiation monitoring for accident conditions. ESF signals for Containment Purge isolation and Main Control Room Air Intake isolation are generated from radiation monitors. These ESF signal actuations are tested as specified in Table 2.5.1-4, ITAAC item 14. However, these signals are provided in the US-APWR design as a result of diversity and not as a direct result of the TMI-related action plan item. It is felt that this item does not warrant

specific delineation in Tier 1 Section 2.5, but reflects that which is common to all ITAAC sections pertaining to the impact of USIs/GSIs, TMI items and operating experience. Therefore, to comply with the intent of the SRP to evaluate these items in Tier 1, a general revision to Tier 1 Section 1.2 is considered prudent rather than delineation of each item in the individual systems sections.

Section 1.9.4.2 pertains to plant reliability and safety improvements that are guided by operating and regulatory experience. MHI has incorporated many measures into the US-APWR to improve safety. Tables 1.9.4-2, 1.9.4-3 and 1.9.5-1 through 1.9.5-4 detail the relevance of the various events and NRC guidance documents. The items detailed are generally incorporated as fundament elements of design such as the inclusion of a four train reactor protection system. There are no specific design attributes that require specific ITAAC to reflect the resolutions of technically relevant operating and regulatory experience.

**Impact on DCD**

See Attachment 2 for a mark-up of Tier 1 Section 1.2, with the following changes:

The following will be added to Tier 1 Section 1.2:

> "... those of safety-significant systems, and some site-specific systems are described only by their name. **Relevant Unresolved Safety Issues (USIs) / Generic Safety Issues (GSIs), Three Mile Island (TMI) items and operating experience are considered in the US-APWR design and reflected in the Tier 2 document upon which this Tier 1 document is based.**
>
> The Tier 1 document contains no proprietary information."

**Impact on COLA**

There is no impact on the COLA.

**Impact on PRA**

There is no impact on the PRA.

## RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

**04/28/2009**

**US-APWR Design Certification**

**Mitsubishi Heavy Industries**

**Docket No. 52-021**

**RAI NO.:** **NO. 255-2110 REVISION 1**

**SRP SECTION:** **14.03.05 - Instrumentation and Controls- Inspections, Tests, Analyses, and Acceptance Criteria**

**APPLICATION SECTION:** **SECTION 14.3.5**

**DATE OF RAI ISSUE:** **03/03/2009**

---

**QUESTION NO.: 14.03.05-12**

Address the applicability of IEEE Std. 603-1991, Section 4.6 with respect to an ITAAC to verify the number and locations of sensors in the RT and ESF safety systems that have a spatial dependence.

Based on the requirements of IEEE Std 603-1991, Section 4.6, the ITAAC should include identification in the as-built design of the minimum number and locations of sensors having spatial dependence that are required for protective actions.

The staff conducted a review of the DCD Tier 1 and Tier 2 as well as the ITAAC in Table 2.5.1-5 and concluded that no information is given on the minimum number and locations of spatially dependent sensors. Provide as-built information that establishes the minimum number and locations of the spatially dependent sensors that the RT and ESF systems required for protective actions (i.e., revise the ITAAC in Table 2.5.1-5 to address the requirements of Section 4.6 of IEEE Std. 603-1991).

---

**ANSWER:**

MHI Topical Report entitled "Safety I&C System Description and Design Process," MUAP-07004, addresses IEEE-603-1991 requirements for spatially dependent sensors. MUAP-07004 is referenced in DCD Tier 2, Chapter 7 (e.g., Reference 7.9-2), and includes the following description typical of spatially dependent sensors:

> "Thermowell-mounted resistance temperature detectors (RTDs) installed in each reactor coolant loop provide the hot and cold leg temperature signals required for input to the protection and control functions. The hot leg temperature measurement in each loop is accomplished using three fast-response, dual-element, narrow-range RTDs. The three thermowells in each hot leg are mounted approximately 120 degrees apart in the cross sectional plane of the piping, to obtain a representative temperature sample. The temperatures measured by the three RTDs are different due to hot leg temperature streaming and vary as a function of thermal power. The PSMS averages these signals to generate a hot leg average temperature.

Radially varying cold leg temperature is not a concern because the RTDs are located downstream of the reactor coolant pumps. The pumps provide mixing of the coolant so that radial temperature variations do not exist.

Radial neutron flux is not a spatially dependent concern because of core radial symmetry. Calculations involving overtemperature and overpower delta T use axial variation in neutron flux. Excore detectors furnish this axially-dependent information to the overtemperature and overpower calculations in the RPS."

DCD Tier 1 Subsection 2.5.1 will be revised to identify the RTS and ESFAS monitored variables that have spatial dependency, and include an ITAAC item to verify their consistency with design requirements.

**Impact on DCD**

See Attachment 1 for a mark-up of Tier 1 Section 2.5 with the changes as shown below. The Design Description of Tier 1 Subsection 2.5.1, Table 2.5.1-2 Reactor Trip and Monitored Variables, Table 2.5.1-3 ESF Actuations and Monitored Parameters (Sheet 2 of 3), and Table 2.5.1-3 ESF Actuations and Monitored Parameters (Sheet 3 of 3) are revised to identify spatially dependent variables. Only the parameters impacted are marked up below.

Tier 1 Subsection 2.5.1.1, Design Description, will be revised to add the following:

**Spatially dependent sensors that are required for protective actions are identified in Table 2.5.1-2 and Table 2.5.1-3, and have the minimum number of sensors and locations to perform the protective action.**

**Table 2.5.1-2 Reactor Trip and Monitored Variables**

| Actuation Signal | Monitored Variables |
|---|---|
| High Power Range Neutron Flux (Low Setpoint) | Neutron Flux (1) |
| High Power Range Neutron Flux (High Setpoint) | Neutron Flux (1) |
| High Power Range Neutron Flux Positive Rate | Neutron Flux (1) |
| High Power Range Neutron Flux Negative Rate | Neutron Flux (1) |
| Over Temperature ΔT | Reactor Coolant Temperature (2) |
| | Pressurizer Pressure |
| | Neutron Flux (1) |
| Over Power ΔT | Reactor Coolant Temperature (2) |
| | Neutron Flux (1) |

**Notes:**
**1: Power Range Neutron flux is a spatially dependent variable due to axial variations.**
**2. Reactor Coolant System hot leg (3 sensors) are spatially dependent variables.**

**Table 2.5.1-3 ESF Actuations and Monitored Parameters (Sheet 2 of 3)**

| ESF Function | Actuation Signal | Monitored Variables |
|---|---|---|
| Main Feedwater Regulation Valve Closure | Low Tavg coincident with RT (P-4) | Reactor Coolant Temperature (2) |
| | | Reactor Trip (RTB Open) |

Note1: Loop A isolation is initiated by steam generator water level signal and main steam line pressure signal from loop A. All loops are identical (e.g., loop B isolation is initiated by the signal from loop B).

**Note 2: Reactor Coolant System hot leg (3 sensors) are spatially dependent variables.**

**Table 2.5.1-3 ESF Actuations and Monitored Parameters (Sheet 3 of 3)**

| ESF Function | Actuation Signal | Monitored Variables |
|---|---|---|
| Block Turbine Bypass and Cooldown Turbine Bypass Valves | Low-Low Tavg | Reactor Coolant Temperature **(2)** |
| | Manual Actuation | Manual Switch Position (Turbine Bypass Block Switch) |

**Note 2: Reactor Coolant System hot leg (3 sensors) are spatially dependent variables.**

Revise Table 2.5.1-6 (re-numbered from Table 2.5.1-5) to add new ITAAC Item 28 below.

**Table 2.5.1-6 RT System and ESF System Inspections, Tests, Analyses, and Acceptance Criteria**

| Design Commitment | Inspections, Tests, Analyses | Acceptance Criteria |
|---|---|---|
| **28. The spatially dependent sensors that are required for protective actions are identified in Table 2.5.1-2 and Table 2.5.1-3.** | **28. An inspection of the as-built spatially dependent sensors required for protective actions will be performed.** | **28. The as-built PSMS includes the minimum number and locations of spatially dependent sensors that are required for protective actions as identified in Table 2.5.1-2 and Table 2.5.1-3.** |

**Impact on COLA**

There is no impact on the COLA.

**Impact on PRA**

There is no impact on the PRA.

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

04/28/2009

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No. 52-021

RAI NO.: NO. 255-2110 REVISION 1

SRP SECTION: 14.03.05 - Instrumentation and Controls- Inspections, Tests, Analyses, and Acceptance Criteria

APPLICATION SECTION: SECTION 14.3.5

DATE OF RAI ISSUE: 03/09/2009

---

QUESTION NO.: 14.03.05-13

Address the applicability of IEEE Std. 603-1991, Section 5.10 with respect to an ITAAC to verify that RT and ESF systems have been designed to facilitate timely recognition, location, replacement, repair, and adjustment of malfunctioning equipment.

Based on the requirements of IEEE Std 603-1991, Section 5.10, the ITAAC should verify that the safety systems have been designed to facilitate timely recognition, location, replacement, repair, and adjustment of malfunctioning equipment.

Design description given in Section 2.5.1.1 does not address any particular design commitment to facilitate timely recognition, location, replacement, repair, and adjustment of malfunctioning equipment. The staff considers that Section 5.10 of IEEE Std. 603- 1991 requires that the safety system be designed for easy maintenance and repair. Therefore an ITAAC should be created to verify the as built design of the PSMS provides the operator and maintenance personnel with the necessary alarms and monitoring indications for the timely recognition and adjustment of malfunctions within the PSMS.

---

ANSWER:

The Design Description and Table 2.5.1-6 (re-numbered from Table 2.5.1-5) ITAAC Item 17 will be revised to address the concern.

**Impact on DCD**

See Attachment 1 for a mark-up of Tier 1 Section 2.5, with the following changes:

Revise the Tier 1 Design Description Section 2.5.1.1 to add the additional text as follows:

> "The PSMS can perform its protective functions in the presence of a maintenance bypass. The PSMS automatically removes operating bypasses when permissive conditions are not met. **The PSMS is designed to facilitate the timely recognition, location, replacement, repair and adjustment of malfunctioning components or modules. The built-in diagnostics, along with operational VDU alarms and engineering tool provide a mechanism for rapidly identifying and locating malfunctioning assemblies.** A single channel or division can be bypassed to allow on-line testing, maintenance or repair during the plant operation and this capability does not prevent the PSMS from performing its safety function."

Revise Tier 1 Table 2.5.1-6 (re-numbered from Table 2.5.1-5) ITAAC Item 17.

| Design Commitment | Inspections, Tests, Analyses | Acceptance Criteria |
|---|---|---|
| **17.a The PSMS is designed to facilitate the timely recognition, location, replacement, repair and adjustment of malfunctioning components or modules.** | **17.a An inspection of the as-built PSMS will be performed.** | **17a. The as-built PSMS is designed to facilitate the timely recognition, location, replacement, repair and adjustment of malfunctioning components or modules.** |
| 17.**b** A single channel or division of the PSMS can be bypassed to allow on-line testing, maintenance or repair without impeding the safety function. | 17.**b**Tests will be performed to confirm the as-built channel or division bypass capabilities and to confirm the function of the bypass interlock logic. | 17.**b** A single channel or division of the as-built PSMS can be bypassed to allow on-line testing, maintenance or repair without impeding the safety function. |

**Impact on COLA**

There is no impact on the COLA.

**Impact on PRA**

There is no impact on the PRA.

## RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

**04/28/2009**

**US-APWR Design Certification**

**Mitsubishi Heavy Industries**

**Docket No. 52-021**

**RAI NO.:** NO. 255-2110 REVISION 1

**SRP SECTION:** 14.03.05 - Instrumentation and Controls- Inspections, Tests, Analyses, and Acceptance Criteria

**APPLICATION SECTION:** SECTION 14.3.5

**DATE OF RAI ISSUE:** 03/03/2009

---

**QUESTION NO.: 14.03.05-14**

Address the applicability of IEEE Std. 603-1991, Section 6.3 with respect to an ITAAC to analyze or demonstrate that no single credible event can cause a non-safety system action that results in a condition, which requires RT or ESF action and can concurrently prevent that protective action in sense and command feature channels that are designated to provide principal protection against the condition.

Based on the requirements of IEEE Std 603-1991, Section 6.3, the ITAAC should include analysis or demonstration to show that no single credible event (including the event's direct and consequential results) can cause a non-safety system action that results in a condition, which requires protective action and can concurrently prevent that protective action in sense and command feature channels that are designated to provide principal protection against the condition.

The staff reviewed the information in DCD Tier 1 and the ITAAC in Table 2.5.1-5, and concluded that no analysis is provided that addresses the requirement of Section 6.3 of IEEE Std. 603-1991. The information in DCD Tier 1 should be revised to include an analysis on the interaction between sense and command features and other systems, and modify the ITAAC in Section 2.5.1, accordingly.

---

**ANSWER:**

The Design Description will be revised and Table 2.5.1-5 will be added to supplement the Tier 1 response to IEEE 603-1991 Section 6.3. Tier 2 Section 7.1.3.16 contains additional description of the Signal Selection Algorithms used. Also, a new ITAAC Item 26 will be added to Table 2.5.1-6 (re-numbered from Table 2.5.1-5). See also the response to Question 14.03.05- 21 below.

**Impact on DCD**

See Attachment 1 for a mark-up of Tier 1 Section 2.5 with the changes as shown below. Insert additional text in the Tier 1 Section 2.5.1 Design Description as follows:

> "...the PSMS. Figure 2.5.1-3 shows the configuration of the ESFAS, SLS, safety VDU and operational VDU.
>
> **The Signal Selector Algorithm (SSA) of the PCMS ensures that the PCMS does not take an erroneous control action based on a single instrument channel failure or a single RPS train failure that results in a condition which requires RT or ESF action. The SSAs are provided in the PCMS to the Monitored Variables which are commonly used in the PSMS and PCMS as listed in Table 2.5.1-5.**
>
> The PSMS cabinets are located in a secure area with key locks and alarms. The PSMS equipment is provided with a clear means of identification."

Add Table 2.5.1-5 to add the identify of the variables which use SSA as follows:

**Table 2.5.1-5 Monitored Variables Using Signal Selection Algorithms (SSA)**

| |
|---|
| **Power Range Neutron Flux** |
| **Reactor Coolant Temperature** |
| **Pressurizer Pressure** |
| **Pressurizer Water Level** |
| **Steam Generator Water Level** |
| **Main Steam Line Pressure** |
| **Turbine Inlet Pressure** |

Table 2.5.1-5, *RT System and ESF System Inspections, Tests, Analyses, and Acceptance Criteria*, and references thereto will be re-numbered to Table 2.5.1-6 as shown in Attachment 1.

**Impact on DCD (Continued)**

Revise Table 2.5.1-6 to add new ITAAC Item 26 below.

| Design Commitment | Inspections, Tests, Analyses | Acceptance Criteria |
|---|---|---|
| 26. A Signal Selector Algorithm (SSA) is provided in the PCMS for the Monitoring Variables as listed in Table 2.5.1-5 to ensure the PCMS does not take an erroneous control action that results in a condition which requires RT or ESF action to consider a single instrument channel failure or a single RPS train failure. | 26. An inspection of the as-built SSA functional arrangement will be performed. | 26. The as-built PSMS and PCMS conform to the functional arrangement of the SSA functions as described in the design description and Table 2.5.1-5. |

**Impact on COLA**

There is no impact on the COLA.

**Impact on PRA**

There is no impact on the PRA.

## RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

**04/28/2009**

**US-APWR Design Certification**

**Mitsubishi Heavy Industries**

**Docket No. 52-021**

**RAI NO.:** **NO. 255-2110 REVISION 1**

**SRP SECTION:** **14.03.05 - Instrumentation and Controls- Inspections, Tests, Analyses, and Acceptance Criteria**

**APPLICATION SECTION:** **SECTION 14.3.5**

**DATE OF RAI ISSUE:** **03/03/2009**

---

**QUESTION NO.: 14.03.05-15**

Address the applicability of IEEE Std. 603-1991, Section 6.5 with respect to an ITAAC to analyze or demonstrate that there are means for checking, with a high-degree of confidence, the operational availability of each sense and command feature input sensor that may be required for the RT or ESF function during reactor operation.

Based on the requirements of IEEE Std 603-1991, Section 6.5, the ITAAC should include analysis or demonstration to show that there are means for checking, with a high-degree of confidence, the operational availability of each sense and command feature input sensor that may be required for a safety function during reactor operation.

Item 17 in Table 2.5.1-5 addresses online testing capability of individual PSMS channels or divisions without impeding the safety function. Item 17 requires that a single channel or division bypass capabilities in the PSMS will be tested to ensure that a single channel or division can be bypassed to allow on-line testing, maintenance, or repair without impeding the safety function. However, a specific ITAAC is not provided to demonstrate the availability of each sense-and-command sensor that may be required for a safety function. Section 2.5.1 in DCD Tier 1 should address the availability test for each sense and- command-feature input sensor, and provide technical means to demonstrate the availability of such a sensor.

---

**ANSWER:**

MHI Topical Report entitled "Safety I&C System Description and Design Process," MUAP-07004, addresses IEEE-603-1991 requirements for the operational availability of each sense and command feature input sensor. MUAP-07004 is referenced in DCD Tier 2, Chapter 7 (e.g., Reference 7.9-2), and includes the following description of the typical means for checking the operational availability of each PSMS input sensor:

> Input sensors from each PSMS are compared continuously in the PCMS to detect abnormal deviations. This comparison occurs after the analog to digital conversion in the PSMS so it also checks the accuracy of PSMS components. PSMS sensors periodically stimulated to calibrate the sensor for expected time dependent drift. The readout for this calibration also occurs after the analog to digital conversion in the PSMS, so it also checks

the accuracy of PSMS components.

As requested, a new ITAAC Item 27 will be added to Table 2.5.1-6 (re-numbered from Table 2.5.1-5). The Design Description of DCD Tier 1 Subsection 2.5.1 will be revised to include the design commitment.

**Impact on DCD**

Tier 1 Subsection 2.5.1.1, Design Description, will be revised to add the following:

> **Input sensors from each PSMS are compared continuously in the PCMS to detect abnormal deviations for checking, with a high-degree of confidence, the operational availability of each PSMS input sensor that may be required for a safety function during reactor operation.**

See Attachment 1 for a mark-up of Tier 1 Section 2.5 with the changes as shown below.
Revise Table 2.5.1-6 (re-numbered from Table 2.5.1-5) to add new ITAAC Item 27 as follows:

| Design Commitment | Inspections, Tests, Analyses | Acceptance Criteria |
|---|---|---|
| **27. Input sensors from each PSMS are compared continuously in the PCMS to detect abnormal deviations for checking, with a high-degree of confidence, the operational availability of each PSMS input sensor that may be required for a safety function during reactor operation.** | **27. An inspection of the as-built PSMS and PCMS functions will be performed.** | **27. The input sensors from each as-built PSMS are compared continuously in the as-built PCMS to detect abnormal deviations.** |

**Impact on COLA**

There is no impact on the COLA.

**Impact on PRA**

There is no impact on the PRA.

## RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

**04/28/2009**

**US-APWR Design Certification**

**Mitsubishi Heavy Industries**

**Docket No. 52-021**

**RAI NO.:** NO. 255-2110 REVISION 1

**SRP SECTION:** 14.03.05 - Instrumentation and Controls- Inspections, Tests, Analyses, and Acceptance Criteria

**APPLICATION SECTION:** SECTION 14.3.5

**DATE OF RAI ISSUE:** 03/03/2009

---

**QUESTION NO.: 14.03.05-16**

Address the applicability of IEEE Std. 603-1991, Section 7.3 with respect to an ITAAC to analyze or demonstrate that the RT and ESF systems are designed so that once initiated, the protective actions of "execute features" should proceed to completion.

Based on the requirements of IEEE Std 603-1991, Section 7.3, the ITAAC should include that once initiated, the protective actions of the execute features shall go to completion.

Section 2.5.1.1, "Design Description" states that automatically- or manually-initiated PSMS protection functions are sealed-in to ensure that the protective actions go to completion. The staff considers that Items 1 and 2 of the ITAAC in Table 2.5.1-5 verify the functional arrangement of the RPS and ESF, respectively. Because, completion of protective actions is given as part of the design commitment, the staff expects that this test will be a part of the inspection of the as built RPS and ESF. The staff concludes that Section 7.3 of IEEE Std. 603-1991 would be properly addressed by the ITAAC with a corresponding ITAAC in Table 2.5.1-5.

---

**ANSWER:**

Tier 1 DCD Table 2.5.1-6 (re-numbered from Table 2.5.1-5), Item 14 will be enhanced to address the requirement that protective action go through to completion and that operator action is required to reset, per IEEE 603-1991 Sections 5.2 and 7.3.

**Impact on DCD**

See Attachment 1 for a mark-up of Tier 1 Section 2.5, with the following changes to ITAAC Item 14 in Table 2.5.1-6 (re-numbered from Table 2.5.1-5):

| Design Commitment | Inspections, Tests, Analyses | Acceptance Criteria |
|---|---|---|
| 14a. The PSMS initiates automatic reactor trips and ESF actuations, identified in Tables 2.5.1-2 and 2.5.1-3, when the plant process signals reach a predetermined limit. | 14a. A test of the as-built PSMS will be performed. | 14a. The as-built PSMS initiates automatic reactor trips and ESF actuations, identified in Tables 2.5.1-2 and 2.5.1-3, when the plant process signals reach a predetermined limit. |
| **14b. Once initiated (automatically or manually), the intended sequences of safety-related functions of the PSMS continue until completion, and, after completion, deliberate operator action is required to return the safety related systems to normal.** | **14b. A test of the as-built PSMS will be performed.** | **14b. Once initiated (automatically or manually), the intended sequences of safety-related functions of the as-built PSMS continue until completion, and, after completion, deliberate operator action is required to return the safety related systems to normal.** |

**Impact on COLA**

There is no impact on the COLA.

**Impact on PRA**

There is no impact on the PRA.

## RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

**04/28/2009**

**US-APWR Design Certification**

**Mitsubishi Heavy Industries**

**Docket No. 52-021**

**RAI NO.:** NO. 255-2110 REVISION 1

**SRP SECTION:** 14.03.05 - Instrumentation and Controls- Inspections, Tests, Analyses, and Acceptance Criteria

**APPLICATION SECTION:** SECTION 14.3.5

**DATE OF RAI ISSUE:** 03/03/2009

---

**QUESTION NO.: 14.03.05-17**

Please revise the description of operation to indicate how the completion of safe shutdown protective actions is analyzed or demonstrated.

Based on the requirements of IEEE Std 603-1991, Section 5.2, the ITAAC should verify or demonstrate that the safety systems are designed so that, once initiated (automatically or manually), the intended sequence of protective actions of the "execute features" should continue until completion, and deliberate operator action is required to return the safety systems to normal.

The completion of protective active is a part of the design of the PSMS that is verified as part of the design. A commitment to verify or demonstrate the completion of safe shutdown protective actions is not provided in the Section 2.5.2.

---

**ANSWER:**

Safe shutdown is accomplished from either the MCR or the Remote Shutdown Console using manual controls available on safety-related and non-safety related displays. DCD Tier 1 Table 2.5.1-6 (re-numbered from Table 2.5.1-5), ITAAC Item 14 above (question 14.03.05-16) addresses this question for actions originating from the MCR.

Of the functions available at the RSC identified in Table 2.5.2-1, manual reactor trip is the only function required to be available from the RSC which must meet the requirements of IEEE Std 603-1991, Section 5.2. This is not addressed in the existing DCD Tier 1 Table 2.5.2-3, Revision 1; therefore it will be revised.

**Impact on DCD**

See Attachment 1 for a mark-up of Tier 1 Section 2.5 with the changes as shown below.
Tier 1 DCD Table 2.5.2-3, Revision 1 will be revised to add a new ITAAC Item 7.

Note that Table 2.5.2-3 is revised by the following Questions:
14.03.05- 10, add ITAAC item 6
14.03.05- 17, add ITAAC Item 7
14.03.05- 18, add ITAAC Item 4
14.03.05- 19, add ITAAC Item 5

| Design Commitment | Inspections, Tests, Analyses | Acceptance Criteria |
|---|---|---|
| **7. Upon manual reactor trip from the RSC, once initiated, the intended sequences of safety-related functions of the execute features continue until completion.** | **7. A test of the as-built RSC will be performed.** | **7. Upon manual reactor trip from the as-built RSC, once initiated, the intended sequences of safety-related functions of the execute features continue until completion.** |

The DCD Tier 1 Subsection 2.5.2.1 Design Description will be revised to include the new ITAAC Item 7 design commitment as shown in Attachment 1.

**Impact on COLA**

There is no impact on the COLA.

**Impact on PRA**

There is no impact on the PRA.

## RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

**04/28/2009**

**US-APWR Design Certification**

**Mitsubishi Heavy Industries**

**Docket No. 52-021**

**RAI NO.:** NO. 255-2110 REVISION 1

**SRP SECTION:** 14.03.05 - Instrumentation and Controls- Inspections, Tests, Analyses, and Acceptance Criteria

**APPLICATION SECTION:** SECTION 14.3.5

**DATE OF RAI ISSUE:** 03/03/2009

---

**QUESTION NO.: 14.03.05-18**

Add an ITAAC that specifically addresses the requirement of IEEE Std 603-1991, Section 5.9 to verify administrative control of the safety equipment to inspect the locks and physical security measures by which administrative control of the RSR can be implemented.

Based on the requirements of IEEE Std 603-1991, Section 5.9, the ITAAC in Section 2.5.2 should verify that the safety system design permits administrative control of access to safety system equipment.

DCD Tier 2, Subsection 7.4.1.5 Item 8 describes the security controls for access to the RSR and the transfer switches for transferring control to the RSR. Access to the room is administratively controlled. The Remote Shutdown Console (RSC) and the transfer switches are locked and the keys are administratively controlled. The inspection should specifically indicate that the locks and physical security measures are in place in the as-built hardware to provide administrative control of access and transfer of control to the RSR.

---

**ANSWER:**

As requested, a new ITAAC item will be added to Table 2.5.2-3 for the Remote Shutdown System, and the associated design commitment will be included in the Subsection 2.5.2.1 Design Description. The ITAAC item will address the physical means of enabling access control (e.g., RSC location in the RSR with key access, and MCR alarm and indication for RSC access). Administrative controls governing access to the RSC and transfer switches apply during plant operation and will be covered by procedures consistent with DCD Tier 2 Subsection 7.4.1.5.

**Impact on DCD**

See Attachment 1 for a mark-up of Tier 1 Section 2.5, with the following changes:

Revise Table 2.5.2-3 to add new ITAAC Item below.

Note that Table 2.5.2-3 is revised by the following Questions:
14.03.05- 10, add ITAAC item 6
14.03.05- 17, add ITAAC Item 7
14.03.05- 18, add ITAAC Item 4
14.03.05- 19, add ITAAC Item 5

| Design Commitment | Inspections, Tests, Analyses | Acceptance Criteria |
|---|---|---|
| **4. The RSC is located in the RSR. The RSR is capable of being locked to prevent inadvertent access. Access to the RSC, and the MCR/RSC transfer systems including the transfer switches, is through secured areas with key access. Any access to these areas is indicated and alarmed in the MCR.** | **4. An inspection of the as-built systems required for safe shutdown will be performed.** | **4. The as-built RSC is located in the RSR. The as-built RSR is capable of being locked to prevent inadvertent access. Access to the RSC, and the MCR/RSC transfer systems including the transfer switches, is through secured areas with key access. Any access to these areas is indicated and alarmed in the as-built MCR.** |

The DCD Tier 1 Subsection 2.5.2.1 Design Description will be revised to include the new ITAAC Item 4 design commitment as shown in Attachment 1.

**Impact on COLA**

There is no impact on the COLA.

**Impact on PRA**

There is no impact on the PRA.

## RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

**04/28/2009**

**US-APWR Design Certification**

**Mitsubishi Heavy Industries**

**Docket No. 52-021**

**RAI NO.:** NO. 255-2110 REVISION 1

**SRP SECTION:** 14.03.05 - Instrumentation and Controls- Inspections, Tests, Analyses, and Acceptance Criteria

**APPLICATION SECTION:** SECTION 14.3.5

**DATE OF RAI ISSUE:** 03/03/2009

---

**QUESTION NO.: 14.03.05-19**

An inspection ITAAC should be added to verify all safety system equipment is properly identified per the requirements of IEEE Std 603-1991, Section 5.11. Based on these requirements, the ITAAC inspection should verify that (1) safety system equipment is distinctly identified for each redundant portion of a safety system, (2) identification of safety system equipment is distinguishable from any identifying markings placed on equipment for other purposes, and (3) identification of safety system equipment and its divisional assignments does not require frequent use of reference material.

Also, add an ITAAC that specifically addresses the requirement of IEEE Std 603-1991, Section 5.11 to inspect the operational VDUs and safety HSI for identification of redundant systems and distinguishing markings of the variables monitored and controlled such the divisional assignments do not require frequent use of reference material.

The distinct identification of safety equipment monitored and controlled when conducting safe shutdown operation is an important characteristic of the displayed information on the operational VDUs and the safety grade HSI. The inspection should verify that the displays have uniquely and correctly identified the redundant portions of safety systems that are needed for safe shutdown.

---

**ANSWER:**

This response revises the Tier 1 Table 2.5.1-6 (re-numbered from Table 2.5.1-5) Item 13 ITAAC by adding that the identification shall not require frequent use of reference material. This ITAAC addresses all of the equipment in Table 2.5.1-1, including all PSMS and VDUs in the MCR.

**Impact on DCD**

See Attachment 1 for a mark-up of Tier 1 Section 2.5, with the following changes:

ITAAC Item 13 in Table 2.5.1-6 (re-numbered from Table 2.5.1-5) will be revised as follows:

| Design Commitment | Inspections, Tests, Analyses | Acceptance Criteria |
|---|---|---|
| 13. Redundant safety equipment of the PSMS and field equipment listed in Table 2.5.1-1 are provided with a clear means of identification. **Identification shall not require frequent use of reference material.** | 13. An inspection of the as-built equipment will be performed. | 13. Documentation exists that describes distinct color coding for each redundant division. The as-built equipment listed in Table 2.5.1-1 complies with the color coding documentation. **Identification shall not require frequent use of reference material.** |

The Subsection 2.5.1.1 Design Description will be revised to include the additional design commitment text added to ITAAC Item 13 in Table 2.5.1-6, as shown in Attachment 1.

This response further applies to the Safety Related portions of the Safe Shutdown System. This ITAAC addresses all VDUs in the RSR.

Table 2.5.2-3 will be revised to add new ITAAC Item 5 below:

Note that Table 2.5.2-3 is revised by the following Questions:
14.03.05- 10, add ITAAC item 6
14.03.05- 17, add ITAAC Item 7
14.03.05- 18, add ITAAC Item 4
14.03.05- 19, add ITAAC Item 5

| Design Commitment | Inspections, Tests, Analyses | Acceptance Criteria |
|---|---|---|
| **5. Redundant safety related equipment of the Safe Shutdown System are provided with a clear means of identification. Identification shall not require frequent use of reference material.** | **5. An inspection of the as-built equipment will be performed.** | **5. Documentation exists that describes distinct color coding for each redundant division. The as-built equipment of the Safe Shutdown System complies with the color coding documentation. Identification shall not require frequent use of reference material.** |

The Subsection 2.5.2.1 Design Description will be revised to include the design commitment of ITAAC Item 5 in Table 2.5.2-3, as shown in Attachment 1

**Impact on COLA**

There is no impact on the COLA.

**Impact on PRA**

There is no impact on the PRA.

## RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

**04/28/2009**

**US-APWR Design Certification**

**Mitsubishi Heavy Industries**

**Docket No. 52-021**

**RAI NO.:** NO. 255-2110 REVISION 1

**SRP SECTION:** 14.03.05 - Instrumentation and Controls- Inspections, Tests, Analyses, and Acceptance Criteria

**APPLICATION SECTION:** SECTION 14.3.5

**DATE OF RAI ISSUE:** 03/03/2009

---

**QUESTION NO.: 14.03.05-20**

Address the applicability of IEEE Std 603-1991, Section 6.3 with respect to an ITAAC to analyze or demonstrate that no single credible event involving the operational VDU and safety grade HSI can cause a non-safety system action that results in a condition, which requires RT or ESF action and can concurrently prevent that protective action in sense and command feature channels that are designated to provide principal protection against the condition.

Based on the requirements of IEEE Std 603-1991, Section 6.3, the ITAAC should include analysis or demonstration to show that no single credible event can cause a non-safety system action that results in a condition, which requires protective action and can concurrently prevent that protective action in sense and command feature channels that are designated to provide principal protection against the condition.

The staff reviewed the information in DCD Tier 1 and the ITAAC in Table 2.5.2-3, and concluded that no analysis is provided that addresses the requirement of Section 6.3 of IEEE Std 603-1991. Specifically, the concern that a conflicting signal between the operational VDU and the safety grade HSI should be addressed in an inspection or test. The information in DCD Tier 1 should be revised to include analysis or demonstration that no single credible interaction between sense and command features of the operational VDUs and the safety grade VDUs can cause and other systems, and the ITAAC, possibly in Section 2.5.2, should be modified accordingly.

---

**ANSWER:**

The request pertaining to IEEE Std 603-1991, Section 6.3, is specifically expressed above in regard to the Safe Shutdown System as described in Section 2.5.2. In question 14.03.05-14 above, a new ITAAC Item is added in to Table 2.5.1-6 (re-numbered from Table 2.5.1-5) to specifically address IEEE Std 603-1991, Section 6.3. As noted in response to question 14.03.05-21 below, the requirements of the ITAAC of Table 2.5.1-6 are extended to all applicable sections of Section 2.5 including the Safe Shutdown System.

With regard to a conflicting signal between the operational VDU and the safety grade HSI, the following description is included in MHI Topical Report entitled "Safety I&C System Description and Design Process," MUAP – 07004 which is referenced in DCD Tier 2, Chapter 7 (e.g., Reference 7.9-2),

Manual controls from the Safety VDU can have priority over any non-safety controls from the PCMS. A continuous erroneous signal from operational VDU can be blocked by manually disabling all signals from the Operational VDU within the PSMS. This enable/disable function is controlled from the Safety VDU for each PSMS train. In addition, 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 ESFAS signal.

As requested, a new ITAAC Item 25 will be added to Table 2.5.1-6 (re-numbered from Table 2.5.1-5). The Design Description of DCD Tier 1 Subsection 2.5.1 will be revised to include the design commitment. The requirements of the ITAAC of Table 2.5.1-6 are extended to all applicable sections of Section 2.5 including the Safe Shutdown System in Section 2.5.2.

**Impact on DCD**

Tier 1 Subsection 2.5.1.1, Design Description, will be revised to add the following:

**Manual controls from the Operational VDU can be blocked and disabled by 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 ESFAS signal.**

See Attachment 1 for a mark-up of Tier 1 Section 2.5 with the changes as shown below.
Revise Table 2.5.1-6 (re-numbered from Table 2.5.1-5) to add new ITAAC Item 25 as follows:

| Design Commitment | Inspections, Tests, Analyses | Acceptance Criteria |
|---|---|---|
| **25. Manual controls from the Operational VDU can be blocked and disabled by 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 ESFAS signal.** | **25. An inspection of the as-built PSMS functions will be performed.** | **25. Manual controls from the Operational VDU can be blocked and disabled by 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 ESFAS signal.** |

**Impact on COLA**

There is no impact on the COLA.

**Impact on PRA**

There is no impact on the PRA.

## RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

**04/28/2009**

**US-APWR Design Certification**

**Mitsubishi Heavy Industries**

**Docket No. 52-021**

**RAI NO.:** **NO. 255-2110 REVISION 1**

**SRP SECTION:** **14.03.05 - Instrumentation and Controls- Inspections, Tests, Analyses, and Acceptance Criteria**

**APPLICATION SECTION:** **SECTION 14.3.5**

**DATE OF RAI ISSUE:** **03/03/2009**

---

**QUESTION NO.: 14.03.05-21**

MHI is requested to expand many of the items of Section 2.5.1 to apply to the safety related portions of the other Sections of 2.5, which includes 2.5.2, Systems Required for Safe Shutdown, 2.5.4, Information Systems Important to Safety, and 2.5.6, Data Communication Systems, or provide justification why these items would apply to those sections.

There are many items in Section 2.5.1 which apply to all safety systems, or portions of systems which are safety related, and paraphrase the requirements of IEEE Std 603 which is invoked by 10 CFR 50.55(a)(h). This includes items 5 (seismic qualification), 7 (emi/rfi qualification), 8 (protection from natural hazards), 9 (divisional power supplies), 10 (independence), 12 (access control) etc. It is suggested that a matrix, or table, be provided identifying these common items and then unique items to these sections. Example:

| | Section | Section | Section | Section | Section | Section |
|---|---|---|---|---|---|---|
| IEEE 603 Criteria | 2.5.1 | 2.5.2 | 2.5.3 | 2.5.4 | 2.5.5 | 2.5.6 |
| (Example) 5.4 | X | X | | X | | X |
| (Example) Information & Controls for Operator Action | X | X | | X | | |

---

**ANSWER:**

A new table will be provided, similar to the format suggested. The design bases of the safety related systems are completely described in the applicable MHI Topical Reports. MHI reviewed IEEE 603-1991 to identify criteria that warrant treatment in Tier 1 and verification by ITAAC. These criteria will be tabulated in DCD Tier 2 and cross-referenced to the applicable Tier 1 information

Where no ITAAC item currently exists, a new ITAAC item will be provided.

**Impact on DCD**

See Attachment 1 for a mark-up of Tier 1 Section 2.5 with the changes as shown below.

Existing Tier 1 Revision 1 ITAAC have been revised to address NRC Questions. New ITAAC Items 25 – 28 are added to Table 2.5.1-6 (re-numbered from Table 2.5.1-5) to address RAI questions and IEEE Sections by this RAI as follows:

ITAAC Item 25 Question No.: 14.03.05-21, IEEE 603-1991 Section 6.3
ITAAC Item 26 Question No.: 14.03.05-14, IEEE 603-1991 Section 6.3
ITAAC Item 27 Question No.: 14.03.05-15, IEEE 603-1991 Section 6.5
ITAAC Item 28 Question No.: 14.03.05-12, IEEE 603-1991 Sections 4.4 and 4.6

**Impact on DCD (Continued)**

See Attachment 3 for a mark-up of Tier 2 Section 14.3 with the changes as shown below.

Revise Tier 2 Subsection 14.3.4.5 to add the following as shown in Attachment 3:

**Conformance of the I&C systems' design to criteria in IEEE 603-1991, with cross references to applicable Tier 1 information including ITAAC, is provided in table 14.3-8.**

Add Table 14.3-8, *IEEE 603-1991 Compliance Matrix by DCD Tier 1 Section*, as shown in Attachment 3.

**Impact on COLA**

There is no impact on the COLA.

**Impact on PRA**

There is no impact on the PRA.

**Attachment 1**

**US-APWR DCD Tier 1 Section 2.5 Mark-up**

**RESPONSE TO RAI No. 255-2110 Revision 0**

Attachment 1

RAI 255
14.03.05-13

## 2.5 INSTRUMENTATION AND CONTROLS

### 2.5.1 Reactor Trip System and Engineered Safety Feature Systems

#### 2.5.1.1 Design Description

The reactor trip (RT) system and the engineered safety feature (ESF) system consist of the protection and safety monitoring system (PSMS) and the field equipment. The PSMS includes the reactor protection system (RPS), the engineered safety features actuation system (ESFAS), the safety logic system (SLS) and the safety grade human system interface system (HSIS). The PSMS consists of four safety divisions.

The purpose of the PSMS is to provide protection against unsafe reactor operation during steady-state and transient power operation by automatically tripping the reactor and actuating necessary engineered safety features. These functions are referred to as the RT system and the ESF system. The safety grade HSIS includes conventional switches for manual actuation of reactor trip and ESF actuation. Table 2.5.1-1 shows equipment names and classifications of the PSMS and the field equipment for the RT system and the ESF system.

Figures 2.5.1-1 and 2.5.1-2 show the configuration of the RPS, ESFAS, and SLS for implementation of the RT system and the ESF system, respectively. Figure 2.5.1-3 shows the configuration of the ESFAS, SLS, HSIS and diverse actuation system (DAS) for implementation of the safety grade component control system. Figure 2.5.1-4 shows the configuration of the reactor trip breakers (RTBs).

The PSMS is located in areas that provide protection from accident related hazards such as missiles, pipe breaks, and flooding. The redundant divisions of the PSMS are isolated from each other and isolated from non-safety systems. Each division of the PSMS is electrically independent, and by placement in different equipment rooms is physically separated from other safety divisions. The redundant divisions of the PSMS are configured for the RT system and the ESF system functions, as shown in Figures 2.5.1-1 and 2.5.1-2. The redundancy in combination with safety division independence, separation, and isolation provided for each PSMS division, ensure protection from a single failure preventing actuation of a safety function. Isolation is provided between the PSMS and the plant control and monitoring system (PCMS) to ensure failures in the PCMS cannot adversely affect the PSMS.

The PSMS initiates automatic reactor trips and ESF actuations, identified in Table 2.5.1-2 and 2.5.1-3, when the plant process signals reach a predetermined limit (setpoint). The PSMS signals are derived from direct measurements. Automatically or manually initiated PSMS protection functions are sealed-in to ensure that the protective actions go to completion. A deliberate operator action is required to reset the seal-in feature. There are no interlocks that prevent manual PSMS actuations. The PSMS can perform its protective functions in the presence of a maintenance bypass. The PSMS automatically removes operating bypasses when permissive conditions are not met. **The PSMS is designed to facilitate the timely recognition, location, replacement,**

**repair and adjustment of malfunctioning components or modules. The built-in diagnostics, along with operational VDU alarms and engineering tool provide a mechanism for rapidly identifying and locating malfunctioning assemblies.** A single channel or division can be bypassed to allow on-line testing, maintenance or repair during the plant operation and this capability does not prevent the PSMS from performing its safety function. For many measurement channels and many division level functions, the PSMS can perform its safety function with a single failure and with one channel or division bypassed, or with two channels or divisions bypassed (but without an additional single failure). The technical specifications distinguish the functions for which these capabilities are applicable.

**Input sensors from each PSMS are compared continuously in the PCMS to detect abnormal deviations for checking, with a high-degree of confidence, the operational availability of each PSMS input sensor that may be required for a safety function during reactor operation.**

**Spatially dependent sensors that are required for protective actions are identified in Table 2.5.1-2 and Table 2.5.1-3, and have the minimum number of sensors and locations to perform the protective action.**

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.

The RT and ESF actuation setpoints of the PSMS are determined using a proven nuclear industry standard methodology. This methodology accounts for uncertainties in determination of device setpoints to maintain adequate margin between analytical limits and device setpoints.

The PSMS and the field equipment listed in Table 2.5.1-1 are qualified to meet environmental, seismic and EMI/RFI (electromagnetic interference and radio frequency interference) condition without loss of the function for the analyzed design basis events. The equipment is designed and manufactured under a quality program that ensures highly reliable and safe operation.

The safety VDUs and the safety VDU processors, which are part of the PSMS, provide monitoring and control for the safety-related plant components and instrumentation, including monitoring and control for the credited manual operator actions. The operational VDUs, which are part of the PCMS, also provide monitoring and control for the safety-related plant components and instrumentation, including the monitoring and control for the credited manual operator actions. In addition, the operational VDUs provide monitoring for the critical safety functions, monitoring of automatic ESF actuations, and automatic indications whenever a protective function is either bypassed or inoperable. Isolation is provided between the PSMS and the operational VDU to ensure that credible failures of the operational VDU do not degrade the performance of the PSMS. Figure 2.5.1-3 shows the configuration of the ESFAS, SLS, safety VDU and operational VDU.

**The Signal Selector Algorithm (SSA) of the PCMS ensures that the PCMS does not take an erroneous control action based on a single instrument channel failure or a single RPS train failure that results in a condition which requires RT or ESF action. The SSAs are provided in the PCMS to the Monitored Variables which are commonly used in the PSMS and PCMS as listed in Table 2.5.1-4.**

**Manual controls from the Operational VDU can be blocked and 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 ESFAS signal.**

The PSMS cabinets are located in a secure area with key locks and alarms. The PSMS equipment is provided with a clear means of identification. **Identification shall not require frequent use of reference material.**

Each division of the PSMS is supplied from two safety-related Class 1E power sources to ensure reliability.

The PSMS and the field equipment provide the safety-related interlocks important to safety. These interlocks are listed in Table 2.5.1-4. The PSMS provides the operator with automatic indications whenever an interlock function is either bypassed or inoperable.

The PSMS hardware and software are developed in accordance with a design process, qualification program and quality assurance (QA) program that conform to the U.S. regulatory requirements for the Class 1E safety systems. These programs encompass the entire product life cycle including software verification and validation (V&V), configuration management, and cyber security.

### 2.5.6.1 Inspections, Tests, Analyses, and Acceptance Criteria

Table ~~2.5.1-5~~ **2.5.1-6** describes the ITAAC for the RT system and the ESF system.

Attachment 1

RAI 255
14.03.05-12

**Table 2.5.1-2 Reactor Trip and Monitored Variables**

| Actuation Signal | Monitored Variables |
|---|---|
| High Source Range Neutron Flux | Neutron Flux |
| High Intermediate Range Neutron Flux | Neutron Flux |
| High Power Range Neutron Flux (Low Setpoint) | Neutron Flux **(1)** |
| High Power Range Neutron Flux (High Setpoint) | Neutron Flux **(1)** |
| High Power Range Neutron Flux Positive Rate | Neutron Flux **(1)** |
| High Power Range Neutron Flux Negative Rate | Neutron Flux **(1)** |
| Over Temperature ΔT | Reactor Coolant Temperature **(2)** |
| | Pressurizer Pressure |
| | Neutron Flux **(1)** |
| Over Power ΔT | Reactor Coolant Temperature **(2)** |
| | Neutron Flux **(1)** |
| Low Reactor Coolant Flow | Reactor Coolant Flow |
| Low Reactor Coolant Pump Speed | Reactor Coolant Pump Speed |
| Low Pressurizer Pressure | Pressurizer Pressure |
| High Pressurizer Pressure | Pressurizer Pressure |
| High Pressurizer Water Level | Pressurizer Water Level |
| Low Steam Generator Water Level | Steam Generator Water Level |
| High-High Steam Generator Water Level | Steam Generator Water Level |
| ECCS Actuation | Refer to ECCS Actuations in Table 2.5.1-3. |
| Manual Actuation | Manual Switch Position<br>(Reactor Trip Switch) |

**Notes:**

**1: Power Range Neutron flux is a spatially dependent variable due to axial variations.**

**2. Reactor Coolant System hot leg (3 sensors) are spatially dependent variables.**

Attachment 1

RAI 255
14.03.05-12

**Table 2.5.1-3 ESF Actuations and Monitored Parameters (Sheet 2 of 3)**

| ESF Function | Actuation Signal | Monitored Variables |
|---|---|---|
| Emergency Feedwater Actuation | ECCS Actuation | ECCS Actuation Signal |
| | Low Steam Generator Water Level | Steam Generator Water Level |
| | Loss of Offsite Power | Class 1E 6.9kV Bus Voltage |
| | Manual Actuation | Manual Switch Position<br>(Emergency Feedwater Actuation Switch) |
| Emergency Feedwater Isolation Loop A (Loop B, C, D) *1 | Low Main Steam Line Pressure | Main Steam Line Pressure |
| | High Steam Generator Water level | Steam Generator Water Level |
| | Manual Actuation | Manual Switch Position<br>(Emergency Feedwater Isolation Switch) |
| Main Control Room Isolation | ECCS Actuation | ECCS Actuation Signal |
| | High Main Control Room Outside Air Intake Radiation | Main Control Room Outside Air Intake Gas Radiation |
| | | Main Control Room Outside Air Intake Iodine Radiation |
| | | Main Control Room Outside Air Intake Particulate Radiation |
| | Manual Actuation | Manual Switch Position<br>(Main Control Room Isolation Switch) |
| Main Feedwater Regulation Valve Closure | Low $T_{avg}$ coincident with RT (P-4) | Reactor Coolant Temperature **(2)** |
| | | Reactor Trip (RTB Open) |
| Main Feedwater Isolation | High-High Steam Generator Water Level | Steam Generator Water Level |
| | ECCS Actuation | ECCS Actuation Signal |
| | Manual Actuation | Manual Switch Position<br>(Main Feedwater Isolation Switch) |

Note1: Loop A isolation is initiated by steam generator water level signal and main steam line pressure signal from loop A. All loops are identical (e.g., loop B isolation is initiated by the signal from loop B).
**Note 2: Reactor Coolant System hot leg (3 sensors) are spatially dependent variables.**

Attachment 1

RAI 255
14.03.05-12

**Table 2.5.1-3 ESF Actuations and Monitored Parameters (Sheet 3 of 3)**

| ESF Function | Actuation Signal | Monitored Variables |
|---|---|---|
| CVCS Isolation | High Pressurizer Water Level | Pressurizer Water Level |
| | Manual Actuation | Manual Switch Position<br>(CVCS Isolation Switch) |
| Block Turbine Bypass and Cooldown Turbine Bypass Valves | Low-Low $T_{avg}$ | Reactor Coolant Temperature **(2)** |
| | Manual Actuation | Manual Switch Position<br>(Turbine Bypass Block Switch) |

**Note 2: Reactor Coolant System hot leg (3 sensors) are spatially dependent variables.**

**Table 2.5.1-4 Interlocks Important to Safety**

| |
|---|
| Containment Spray/Residual Heat Removal Pump Hot Leg Isolation Valve Open Permissive Interlock |
| Simultaneous-Open Block Interlock with Residual Heat Removal Discharge Line Containment Isolation Valve and Containment Spray Header Containment Isolation Valve |
| Simultaneous-Open Block Interlock with Containment Spray/Residual Heat Removal Pump Hot Leg Isolation Valve and Containment Spray Header Containment Isolation Valve |
| Reactor Makeup Water Line Isolation Interlock |
| Accumulator Discharge Valve Open Interlock |
| Component Cooling Water Supply and Return Header Tie Line Isolation Interlock |

Attachment 1

RAI 255
14.03.05-14

**Table 2.5.1-5 Monitored Variables Using Signal Selection Algorithms (SSA**

| |
|---|
| **Power Range Neutron Flux** |
| **Reactor Coolant Temperature** |
| **Pressurizer Pressure** |
| **Pressurizer Water Level** |
| **Steam Generator Water Level** |
| **Main Steam Line Pressure** |
| **Turbine Inlet Pressure** |

RAI 255
14.03.05-14

Attachment 1

**Table 2.5.1-~~5~~6 RT System and ESF System Inspections, Tests, Analyses, and Acceptance Criteria (Sheet 1 of 8)**

| Design Commitment | Inspections, Tests, Analyses | Acceptance Criteria |
|---|---|---|
| 1. The functional arrangement of the RPS is as described in the design description and as shown in Figures 2.5.1-1 and 2.5.1-2. | 1. An inspection of the as-built RPS will be performed. | 1. The as-built RPS conforms to the functional arrangement as described in the design description and as shown in Figures 2.5.1-1 and 2.5.1-2. |
| 2. The functional arrangements of the ESFAS, SLS, HSIS and DAS are as described in the design description and as shown in Figures 2.5.1-2 and 2.5.1-3. | 2. An inspection of the as-built ESFAS, SLS, HSIS and DAS will be performed. | 2. The as-built ESFAS, SLS, HSIS and DAS conform to the functional arrangement as described in the design description and as shown in Figures 2.5.1-2 and 2.5.1-3. |
| 3. The functional arrangement of the RTB is as described in the design description and as shown in Figure 2.5.1-4. | 3. An inspection of the as-built RTB will be performed. | 3. The as-built RTB conforms to the functional arrangement as described in the design description and as shown in Figure 2.5.1-4. |
| 4. The PSMS and MCR division level switches provide manual initiation for reactor trip and ESF actuations identified in Tables 2.5.1-2 and 2.5.1-3. | 4. A test of the as-built equipment will be performed. | 4. The as-built PSMS and MCR division level switches provide manual initiation for reactor trip and ESF actuations identified in Tables 2.5.1-2 and 2.5.1-3. |

Attachment 1

RAI 255
14.03.05-14

**Table 2.5.1-~~5~~6 RT System and ESF System Inspections, Tests, Analyses, and Acceptance Criteria (Sheet 2 of 8)**

| Design Commitment | Inspections, Tests, Analyses | Acceptance Criteria |
|---|---|---|
| 5. The seismic Category I equipment, identified in Table 2.5.1-1, can withstand seismic design basis loads without loss of safety function. | 5.i Inspection will be performed to verify that the seismic Category I as-built equipment identified in Table 2.5.1-1 are located in the containment and reactor building. | 5.i The seismic Category I as-built equipment identified in Table 2.5.1-1 is located in the containment and reactor building. |
| | 5.ii Type tests and/or analyses of seismic Category I equipment will be performed. | 5.ii The result of the type tests and/or analyses concludes that the seismic Category I equipment can withstand seismic design basis loads without loss of safety function. |
| | 5.iii Inspection will be performed on the as-installed equipment including anchorage. | 5.iii The as-installed equipment including anchorage is seismically bounded by the tested or analyzed conditions. |
| 6. The Class 1E equipment identified in Table 2.5.1-1 as being qualified for a harsh environment is designed to withstand the environmental conditions that would exist before, during, and following a design basis event without loss of safety function for the time required to perform the safety function. | 6.i Type tests and/or analyses will be performed on Class 1E equipment located in a harsh environment. | 6.i The results of the type tests and/or analyses conclude that the Class 1E equipment identified in Table 2.5.1-1 as being qualified for a harsh environment can withstand the environmental conditions. |
| | 6.ii Inspections will be performed on the as-installed Class 1E equipment and the associated wiring, cables, and terminations located in a harsh environment. | 6.ii The as-installed Class 1E equipment and the associated wiring, cables, and terminations identified in Table 2.5.1-1 as being qualified for a harsh environment are bounded by type tests and/or analyses. |

RAI 181
14.03.05-04
RAI 255
14.03.05-14

Attachment 1

**Table 2.5.1-56 RT System and ESF System Inspections, Tests, Analyses, and Acceptance Criteria (Sheet 3 of 8)**

| Design Commitment | Inspections, Tests, Analyses | Acceptance Criteria |
|---|---|---|
| 7. The RPS, ESFAS, SLS, safety VDU processor, and safety VDU are qualified to meet the electromagnetic conditions that would exist before, during, and following a design basis accident, with respect to its location in the facility, without loss of safety function for the time required to perform the safety function. | 7. Type tests and/or analyses will be performed on the equipment. | 7. **A report exists and concludes that the** ~~The~~ RPS, ESFAS, SLS, safety VDU processor, and safety VDU are qualified ~~for its specific application.~~ **to meet the electromagnetic conditions that would exist before, during, and following a design basis accident, with respect to its location in the facility, without loss of safety function for the time required to perform the safety function.** |
| 8. The Class 1E equipment listed in Table 2.5.1-1 is located in a facility area that provides protection from natural phenomena hazards such as tornadoes, and accident related hazards such as missiles, pipe breaks and flooding. | 8. An inspection of the as-built equipment location will be performed. | 8. The as-built equipment listed in Table 2.5.1-1 is located in a plant area that provides protection from natural phenomena hazards such as tornadoes, and accident related hazards such as missiles, pipe breaks and flooding. |
| 9. The Class 1E equipment listed in Table 2.5.1-1 is powered from **two safety related power sources: the first source is** its respective Class 1E division **and the second source is from another division to ensure reliable power to each PSMS.** | 9. **Inspection of the as-built equipment** ~~Tests.~~ will be performed ~~on the equipment by providing a simulated test signal in each Class 1E division~~. | 9. **The Class 1E equipment listed in Table 2.5.1-1 is powered from two safety related power sources: the first source is its respective Class 1E division and the second source is from another division to ensure reliable power to each PSMS.** ~~The simulated test signal exists at the as-built Class 1E equipment identified in Table 2.5.1-1 under tests in the as-built PSMS and field equipment.~~ |

Attachment 1

RAI 181
14.03.05-05
RAI 255
14.03.05-14

**Table 2.5.1-~~5~~6 RT System and ESF System Inspections, Tests, Acceptance Criteria (Sheet 4 of 8)**

| Design Commitment | Inspections, Tests, Analyses | Acceptanc |
|---|---|---|
| 10.a The PSMS and field equipment listed in Table 2.5.1-1 redundant divisions are physically and electrically independent of each other and physically and electrically independent of any non-safety divisions.<br><br>**Physical independence is provided by distance or barriers, which prevent propagation of fire or electrical faults. Electrical independence is achieved by using independent power sources and electrical circuits for each safety division and by using** ~~The redundant divisions of the PSMS and field equipment listed in Table 2.5.1-1 are isolated from each other and are isolated from non-safety systems (including auxiliary features) by~~ qualified **electrical fault** isolation devices ~~and qualified communication interface devices~~ **at interfaces between redundant divisions and interfaces between safety and non-safety divisions.** | 10.a.i An inspection of the as-built equipment ~~location~~ will be performed. | 10.a.i The results of the inspection conclude that:<br>1) The as-built physical independence is provided by distance or barriers, which prevent propagation of fire or electrical faults.<br>2) The as-built electrical independence is achieved by **maintaining separate power sources and electrical circuits for each division and by** fiber optic cable ~~communication~~ interfaces, conventional isolators, or other proven isolation methods or devices~~.~~ **at interfaces between redundant divisions and interfaces between safety and non-safety divisions.** ~~3) The as-built communication independence is achieved by communication processing functions that are independent of trip and actuation processing functions.~~ |
| | 10.a.ii Type tests and/or analyses of the isolation devices will be performed | 10.a.ii The results of the type **tests** and/or analyses conclude that the isolation devices prevent credible faults. |
| **10.b Digital communication independence is achieved between redundant divisions of the PSMS and field equipment listed in Table 2.5.1-1 or between non-safety divisions and the PSMS and field equipment listed in Table 2.5.1-1, by communication processing functions that are independent of trip and actuation processing functions.** | **10.b.i An inspection of the as-built equipment will be performed.** | **10.b The as-built communication independence is achieved by communication processing functions that are independent of trip and actuation processing functions** |
| | **10.b.ii Type tests and/or analyses of the communication processing devices will be performed.** | |

RAI 181
14.03.05-06
RAI 255
14.03.05-14
14.03.05-16
14.03.05-19

Attachment 1

**Table 2.5.1-~~5~~6 RT System and ESF System Inspections, Tests, Acceptance Criteria (Sheet 5 of 8)**

| Design Commitment | Inspections, Tests, Analyses | Acceptance Criteria |
|---|---|---|
| 11. The PSMS provides the operator with: (1) automatic non-safety HSIS indications of the bypassed or inoperable **status indication (BISI) for** protective actions and (2) the ability to manually actuate ~~the display.~~ **BISI for protective actions.** | 11. A test of the as-built equipment will be performed. | 11. The as-built PSMS provides the operator with: (1) **automatic** non-safety HSIS indications of bypassed **or** ~~and~~ inoperable **protective actions** ~~status;~~ and (2) the ability to manually actuate **BISI for** these **protective actions.** ~~indications~~. |
| 12. The PSMS cabinets have key locks and alarms, and are located in a secure area of the facility. | 12.i A test of the as-built PSMS cabinets will be performed for key lock and alarms. | 12.i Each cabinet of the as-built PSMS has a key lock and appropriate alarm measures. |
| | 12.ii An inspection of the as-built PSMS cabinets will be performed for the installed location. | 12.ii Each cabinet of the as-built PSMS is located in the secure area of the facility. |
| 13. Redundant safety equipment of the PSMS and field equipment listed in Table 2.5.1-1 are provided with a clear means of identification. **Identification shall not require frequent use of reference material.** | 13. An inspection of the as-built equipment will be performed. | 13. Documentation exists that describes distinct color coding for each redundant division. The as-built equipment listed in Table 2.5.1-1 complies with the color coding documentation. **Identification shall not require frequent use of reference material.** |
| 14**a**. The PSMS initiates automatic reactor trips and ESF actuations, identified in Tables 2.5.1-2 and 2.5.1-3, when the plant process signals reach a predetermined limit. | 14**a**. A test of the as-built PSMS will be performed. | 14**a**. The as-built PSMS initiates automatic reactor trips and ESF actuations, identified in Tables 2.5.1-2 and 2.5.1-3, when the plant process signals reach a predetermined limit. |
| **14b. Once initiated (automatically or manually), the intended sequences of safety-related functions of the PSMS continue until completion, and, after completion, deliberate operator action is required to return the safety related systems to normal.** | **14b. A test of the as-built PSMS will be performed.** | **14b. Once initiated (automatically or manually), the intended sequences of safety-related functions of the as-built PSMS continue until completion, and, after completion, deliberate operator action is required to return the safety related systems to normal.** |

RAI 181
14.03.05-06
14.03.05-08
RAI 255
14.03.05-13
14.03.05-14

Attachment 1

**Table 2.5.1-~~5~~6 RT System and ESF System Inspections, Tests, A and Acceptance Criteria (Sheet 6 of 8)**

| Design Commitment | Inspections, Tests, Analyses | Acceptance Criteria |
|---|---|---|
| 15. **Deleted.** ~~Means are provided to ensure independence between the PSMS and PCMS, using appropriate isolation methods.~~ | 15. **Deleted.** ~~An inspection will be conducted verifying isolation between the PSMS and PCMS.~~ | 15. **Deleted,** ~~The as-built means are provided to ensure independence between the PSMS and PCMS, using appropriate isolation methods~~ |
| 16. The PSMS signals are derived from direct measurements. | 16. An inspection of the as-built PSMS will be performed. | 16. The as-built PSMS signals are derived from direct measurements. |
| **17.a The PSMS is designed to facilitate the timely recognition, location, replacement, repair and adjustment of malfunctioning components or modules.** | **17.a An inspection of the as-built PSMS will be performed.** | **17.a The as-built PSMS is designed to facilitate the timely recognition, location, replacement, repair and adjustment of malfunctioning components or modules**. |
| 17.**b** A single channel or division of the PSMS can be bypassed to allow on-line testing, maintenance or repair without impeding the safety function. | 17.**b** Tests will be performed to confirm the as-built channel or division bypass capabilities and to confirm the function of the bypass interlock logic. | 17.**b** A single channel or division of the as-built PSMS can be bypassed to allow on-line testing, maintenance or repair without impeding the safety function. |
| 18. The PSMS automatically removes operating bypasses when permissive conditions are not met. | 18. A test of the as-built PSMS will be performed. | 18. The as-built PSMS automatically removes operating bypasses when permissive conditions are not met. |
| 19. The PSMS setpoints are determined using a methodology based on proven nuclear industry standards. **This methodology provides** allowance for uncertainties between analytical limits and device setpoints ~~is determined using this methodology~~. | 19. An inspection will be performed to define the as-built PSMS setpoints in accordance with the acceptable methodology. | 19 The ~~allowance for uncertainties between the as-built analytical limits and the~~ as-built PSMS setpoints **are** ~~is~~ determined using the acceptable methodology**, which provides allowance for uncertainties between analytical limits and device setpoints based on proven nuclear industry standards**. |

RAI 181
14.03.05-06
RAI 255
14.03.05-14

Attachment 1

**Table 2.5.1-~~5~~6 RT System and ESF System Inspections, Tes and Acceptance Criteria (Sheet 7of 8)**

| Design Commitment | Inspections, Tests, Analyses | Acceptance Criteria |
|---|---|---|
| 20. Each division of the PSMS and field equipment listed in Table 2.5.1-1 is supplied from two safety-related Class 1E power sources. Either power source is sufficient to power each division of the PSMS. | 20. A test of the as-built equipment will be performed. | 20. ~~Each division of the as-built equipment listed in Table 2.5.1-1 is supplied from two safety-related Class 1E power sources.~~ **Each division of the as-built PSMS and field equipment listed in Table 2.5.1-1 is supplied from two safety-related Class 1E power sources. Either power source is sufficient to power each division of the as-built PSMS.** |
| 21. The PSMS logic is designed to fail to a safe state such that loss of electrical power to a division of PSMS results in a reactor trip condition for that division. Loss of electrical power 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 PSMS **will fail to a safe state upon loss of electrical power to the division (i.e.,** results in a reactor trip condition for that division), **and loss** ~~.Loss~~ of electric power does not result in ESF actuation. |
| 22. The 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 operating events. The monitored variables are listed in Tables 2.5.1-2 and 2.5.1-3. | 22. An inspection of the as-built **instrumentation** ~~system~~ will be performed. | 22. The as-built instrumentation **that is required to function during normal operation, anticipated operational occurrence (AOO) and postulated accident (PA) conditions and** that is listed in Tables 2.5.1-2 and 2.5.1-3 is provided with adequate range to monitor operating events. |
| 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 a life cycle process that meets the regulatory requirements for Class 1E safety systems, and which encompasses the entire product life cycle including software V&V, configuration management and cyber security. | 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 **a** ~~the~~ life cycle process that meets the regulatory requirements for Class 1E safety systems**, and which encompasses the entire product life cycle including software V&V, configuration management and cyber security.** |

RAI 255
14.03.05-12
14.03.05-14
14.03.05-15
14.03.05-20

Attachment 1

**Table 2.5.1-~~5~~6 RT System and ESF System Inspections, Tests, Analyses, and Acceptance Criteria (Sheet 8of 8)**

| Design Commitment | Inspections, Tests, Analyses | Acceptance Criteria |
|---|---|---|
| 25. Manual controls from the Operational VDU can be blocked and disabled by 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 ESFAS signal. | 25. An inspection of the as-built PSMS functions will be performed. | 25. Manual controls from the Operational VDU can be blocked and disabled by 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 ESFAS signal. |
| 26. A Signal Selector Algorithm (SSA) is provided in the PCMS for the Monitoring Variables as listed in Table 2.5.1-5 to ensure the PCMS does not take an erroneous control action that results in a condition which requires RT or ESF action to consider a single instrument channel failure or a single RPS train failure. | 26. An inspection of the as-built SSA functional arrangement will be performed. | 26. The as-built PSMS and PCMS conform to the functional arrangement of the SSA functions as described in the design description and Table 2.5.1-5. |
| 27. Input sensors from each PSMS are compared continuously in the PCMS to detect abnormal deviations for checking, with a high-degree of confidence, the operational availability of each PSMS input sensor that may be required for a safety function during reactor operation. | 27. An inspection of the as-built PSMS and PCMS functions will be performed. | 27. The input sensors from each as-built PSMS are compared continuously in the as-built PCMS to detect abnormal deviations. |
| 28. The spatially dependent sensors that are required for protective actions are identified in Table 2.5.1-2 and Table 2.5.1-3. | 28. An inspection of the as-built spatially dependent sensors required for protective actions will be performed. | 28. The as-built PSMS includes the minimum number and locations of spatially dependent sensors that are required for protective actions as identified in Table 2.5.1-2 and Table 2.5.1-3. |

Attachment 1

RAI 255
14.03.05-17
14.03.05-18

## 2.5.2 Systems Required for Safe Shutdown

### 2.5.2.1 Design Description

The safe shutdown is achieved from the MCR or the remote shutdown room (RSR) using safety-related instrumentation and control (I&C) systems of the PSMS, including the RPS, ESFAS, SLS and safety VDUs. The operational VDUs may also be used for monitoring safety-related instrumentation and manually controlling safety components. The normal shutdown can be achieved using non-safety instrumentation and non-safety component controls via the PCMS, including the operational VDUs, in addition to the above safety-related I&C systems. There are no plant systems specifically and solely dedicated for the safe and normal shutdown systems.

**The Remote Shutdown Console (RSC) is located in the RSR. The RSR is capable of being locked to prevent inadvertent access. Access to the RSC, and the MCR/RSC transfer systems including the transfer switches, is through secured areas with key access. Any access to these areas is indicated and alarmed in the MCR.**

The systems required for the safe shutdown perform two basic functions. First, they provide the necessary reactivity control to maintain the core in a sub-critical condition. Second, the systems provide the RHR capability to maintain adequate core cooling. A boration capability is provided to compensate for xenon decay and to maintain the required core shutdown margin.

Manual controls through the safety VDUs or the operational VDUs in the MCR or the RSR, allow operators to transition to and maintain hot standby, and transition to and maintain cold shutdown. If the MCR is uninhabitable, the same control and monitoring of the safe shutdown and the normal shutdown functions can be performed from the RSR. Transfer of control from the MCR to the RSR is provided for each PSMS division and for the PCMS. When the MCR is enabled, failures in the RSR, including electrical faults due to fire, cannot adversely affect the ability to achieve and maintain the safe shutdown from the MCR. Similarly, when the RSR is enabled, failures in the MCR, including electrical faults due to fire, cannot adversely affect the ability to achieve and maintain safe shutdown from the RSR.

**Upon manual reactor trip from the RSC, once initiated, the intended sequences of safety-related functions of the execute features continue until completion.**

Figure 2.5.2-1 shows the configuration of the SLS and HSIS for implementation of the safe shutdown functions. The safe shutdown can be achieved and maintained using redundant plant instrumentation and components, through redundant divisions of the PSMS. The PSMS redundancy, independence, testability, qualification, quality and life cycle descriptions of Subsection 2.5.1 are also applicable to the safe shutdown functions of the PSMS.

RAI 255
14.03.05-19

Attachment 1

**Redundant safety related equipment of the Safe Shutdown System are provided with a clear means of identification. Identification shall not require frequent use of reference material.**

The safe shutdown functions and related process systems are identified in Tables 2.5.2-1 and 2.5.2-2.

### 2.5.2.2 Inspections, Tests, Analyses, and Acceptance Criteria

Table 2.5.2-3 describes the ITAAC for the systems required for safe shutdown.

RAI 255
14.03.05- 10
14.03.05-17
14.03.05-18
14.03.05-19

Attachment 1

**Table 2.5.2-3 Systems Required for Safe Shutdown Inspections, Tests, Analyses, and Acceptance Criteria (Sheet 2 of 2)**

| Design Commitment | Inspections, Tests, Analyses | Acceptance Criteria |
|---|---|---|
| 4. The RSC is located in the RSR. The RSR is capable of being locked to prevent inadvertent access. Access to the RSC, and the MCR/RSC transfer systems including the transfer switches, is through secured areas with key access. Any access to these areas is indicated and alarmed in the MCR. | 4. An inspection of the as-built systems required for safe shutdown will be performed. | 4. The as-built RSC is located in the RSR. The as-built RSR is capable of being locked to prevent inadvertent access. Access to the RSC, and the MCR/RSC transfer systems including the transfer switches, is through secured areas with key access. Any access to these areas is indicated and alarmed in the as-built MCR. |
| 5. Redundant safety related equipment of the Safe Shutdown System are provided with a clear means of identification. Identification shall not require frequent use of reference material. | 5. An inspection of the as-built equipment will be performed. | 5. Documentation exists that describes distinct color coding for each redundant division. The as-built equipment of the Safe Shutdown System complies with the color coding documentation. Identification shall not require frequent use of reference material. |
| 6. The functional arrangement of the Safe Shutdown System is as described in the Design Description and as shown in Figure 2.5.2-1. | 6. An inspection of the as-built Safe Shutdown System will be performed. | 6 The as-built Safe Shutdown System conforms to the functional arrangement as described in the Design Description and as shown in Figure 2.5.2-1. |
| 7. Upon manual reactor trip from the RSC, once initiated, the intended sequences of safety-related functions of the execute features continue until completion. | 7. A test of the as-built RSC will be performed. | 7. Upon manual reactor trip from the as-built RSC, once initiated, the intended sequences of safety-related functions of the execute features continue until completion. |

RAI 181
14.03.05-06
RAI 255
14.03.05- 10

Attachment 1

**Table 2.5.4-2 Information Systems Important to Safety Inspe Analyses, and Acceptance Criteria**

| Design Commitment | Inspections, Tests, Analyses | Acceptance Criteria |
|---|---|---|
| 1. Information systems important to safety (PAM, BISI, alarms, SPDS) are appropriately displayed and alarmed in the MCR, RSR, TSC and EOF, as appropriate. | 1. A test will be performed to demonstrate alarm, display and control capabilities for information systems important to safety. | 1. The as-built information systems important to safety (PAM, BISI, alarms, SPDS) are appropriately displayed and alarmed in the MCR, RSR, TSC and EOF, as appropriate. |
| 2. Information and controls for credited manual operator actions are provided in the MCR. | 2. A test of the as-built PSMS and PCMS will be performed. | 2. The as-built information and controls for credited manual operator actions are provided in the MCR. |
| 3. The field instrumentation for the PAM variables identified in Table 2.5.4-1 as being qualified for a harsh environment is designed to withstand the environmental conditions that would exist before, during, and following a design basis event without loss of safety function for the time required to perform the safety function. | 3.i Type tests and/or analyses will be performed on the field instrumentation located in a harsh environment. | 3.i The results of the type tests and/or analyses conclude that the field instrumentation **for the PAM variables** identified in Table 2.5.4-1 as being qualified for a harsh environment can withstand the environmental conditions. **that would exist before, during, and following a design basis event without loss of safety function for the time required to perform the safety function.** |
| | 3.ii Inspections will be performed on the **as –built** field instrumentation and the associated wiring, cables, and terminations located in a harsh environment. | 3.ii The ~~as-installed~~ **as –built** field instrumentation and the associated wiring, cables, and terminations identified in Table 2.5.4-1 as being qualified for a harsh environment, are bounded by type tests and/or analyses. |
| **4. The functional arrangement of the Information Systems Important to Safety is as described in the Design Description and as shown in Figure 2.5.4-1.** | **4. An inspection of the as-built Information Systems Important to Safety will be performed.** | **4. The as-built Information Systems Important to Safety conform to the functional arrangement as described in the Design Description and as shown in Figure 2.5.4-1.** |

**Attachment 2**

**US-APWR DCD Tier 1 Section 1.0 Mark-up**

**RESPONSE TO RAI No. 255-2110 Revision 0**

The separate Tier 2 document provides more-detailed information on the plant design. This information is to be approved but not certified by NRC. Information contained in the Tier 1 document was derived from the Tier 2 document.

The Tier 1 document is organized into three chapters, with this chapter providing introductory information.

Chapter 2 identifies site parameters and provides design descriptions and associated ITAAC for different aspects of the US-APWR standard design. The content of the design descriptions and the tables that provide ITAAC are discussed further in Section 1.4.

Chapter 3 addresses interface requirements focused on the safety design attributes and performance characteristics that ensure that the site-specific portion of the design is in conformance with the certified design. The site-specific portions of the design are those portions of the design that are dependent on characteristics of the site, such as the design of the ultimate heat sink. This chapter also identifies the scope of the design to be certified by specifying the systems that are completely or partially out of scope of the certified design.

In each chapter section or subsection, tables follow the text and figures follow the tables. The tables and figures are identified by numbers associated with the section or subsection in which they appear. For example, Figure 2.4.1-1 is the first figure in Subsection 2.4.1. Pages are numbered sequentially and identified by both the section number and the page number within that section.

The Tier 1 document addresses all major plant systems and structures, including systems not important to safety, in order to completely define the US-APWR design. However, descriptions of site-specific systems provide less technical information than those of safety-significant systems, and some site-specific systems are described only by their name. Relevant Unresolved Safety Issues (USIs) / Generic Safety Issues (GSIs), Three Mile Island (TMI) items and operating experience are considered in the US-APWR design and reflected in the Tier 2 document upon which this Tier 1 document is based.

The Tier 1 document contains no proprietary information.

## 1.3 DEFINITIONS

The following definitions are used in the design descriptions and the related ITAAC to ensure precision and consistency.

**Acceptance criteria** refer to the performance, physical condition, or analysis result for an SSC, to demonstrate that the design requirement/commitment is met.

**Analysis** means a calculation, mathematical computation, or engineering/ technical evaluation. Engineering or technical evaluations could include, but are not limited to, comparisons with operating experience or design of similar SSCs.

**As-built** means the physical properties of the SSC following the completion of its installation or construction activities at its final location at the plant site.

**Attachment 3**

**US-APWR DCD Tier 2 Section 14.3 Mark-up**

**RESPONSE TO RAI No. 255-2110 Revision 0**

- GDC 21, "Protection System Reliability and Testability," as it pertains to protection system reliability and testability requirements
- GDC 22, "Protection System Independence," as it pertains to protection system independence requirements
- GDC 23, "Protection System Failure Modes," as it pertains to protection system failure modes requirements
- GDC 24, "Separation of Protection and Control Systems," as it pertains to separation of protection systems from control systems
- GDC 25, "Protection System Requirements for Reactivity Control Malfunctions," as it pertains to protection system requirements for reactivity control malfunctions
- GDC 29, "Protection Against Anticipated Operational Occurrences," as it pertains to protection against anticipated operational occurrences (AOOs).

ITAAC are also provided for documentation of a high-quality software design process consistent with each of the management, implementation, and resource characteristics shown in branch technical position (BTP) 7-14, "Guidance on Software Reviews for Digital Computer-Based Instrumentation and Controls Systems," (Ref 14.3-28) in SRP Chapter 7 (Ref 14.3-29).

Conformance of the I&C systems' design to criteria in IEEE 603-1991, with cross references to applicable Tier 1 information including ITAAC, is provided in table 14.3-8.

Design descriptions for I&C equipment follow guidelines of Appendix C.II.1-A of RG 1.206 (Reference 14.3-1) and address the following matters:

- Hardware architecture, describing all hardware modules, cabinet layout and wiring, seismic and environmental control requirements, and power sources
- Software architecture, describing design specifications, code listings, and build documents and providing installation configuration tables
- RGs that have specific recommendations
- Operating experience, including safety-significant problems identified by NRC
- Policy issues raised for the standard designs
- New design features, such as communications between various portions of the digital system or other systems
- Any insights or key assumptions identified through the PRA (Table 14.3-1)
- Generic safety issue resolutions that have resulted in design/operational features

## Table 14.3-8 IEEE 603-1991 Compliance Matrix by DCD Tier 1 Section

### (Sheet 1 of 4)

| IEEE Std. 603-1991 | | Tier 1 DCD Subsection Number | | | | | |
|---|---|---|---|---|---|---|---|
| **Section Number** | **Section Title or Topic** | **2.5.1 (PSMS)** | **2.5.2 (SSD)** | **2.5.3 (DAS)** | **2.5.4 (PAM/BISI/ SPDS et. al.)** | **2.5.5 (PCMS)** | **2.5.6 (DCS)** |
| 4.4 and 4.6 | Number and location of sensors; spatial dependence | X Table 2.5.1-6 Item # 28 | (1) (5) | N/A | (1) (5) | N/A | N/A |
| 4.8 | Potential for functional degradation | X Table 2.5.1-6 Item # 7, 8 | (1) (5) | N/A | (1) (5) | N/A | (1) (5) Table 2.5.6-1 Item # 4 |
| 5.1 | Single Failure | X Table 2.5.1-6 Item # 10, 21 | (1) (5) | N/A | (1) (5) | N/A | N/A |
| 5.2 and 7.3 | Completion of Protective Action | X Table 2.5.1-6 Item # 14 | (1) (5) Table 2.5.2-3 Item # 7 | N/A | (1) (5) | N/A | N/A |
| 5.3 | Quality | (2) | (2) | (2) | (2) | (2) | (2) |
| 5.4 | Equipment Qualification | X Table 2.5.1-6 Item # 5, 6, 7 | (1) (5) | N/A | (1) (5) | N/A | (1) (5) |
| 5.5 | System Integrity | X Table 2.5.1-6 Item # 5, 6, 7, 8, 22 | (1) (5) | N/A | (1) (5) | N/A | (1) (5) Table 2.5.6-1 Item # 2 |

## Table 14.3-8 IEEE 603-1991 Compliance Matrix by DCD Tier 1 Section

### (Sheet 2 of 4)

| IEEE Std. 603-1991 | | Tier 1 DCD Subsection Number | | | | | |
|---|---|---|---|---|---|---|---|
| Section Number | Section Title or Topic | 2.5.1 (PSMS) | 2.5.2 (SSD) | 2.5.3 (DAS) | 2.5.4 (PAM/BISI/ SPDS et. al.) | 2.5.5 (PCMS) | 2.5.6 (DCS) |
| 5.6 | Independence | X Table 2.5.1-6 Item # 10, 15 | (1) (5) | N/A | (1) (5) | N/A | (1) (5) |
| 5.7 and 6.5 | Capability for test and Calibration | X Table 2.5.1-6 Item # 17, 27 | (1) (5) | N/A | (1) (5) | N/A | (1) (5) Table 2.5.6-1 Item # 2 |
| 5.8 | Information Displays | X Table 2.5.1-6 Item # 16 | (1) (5) | N/A | (1) (5) | N/A | N/A |
| 5.9 | Control of Access | X Table 2.5.1-6 Item # 12 | (1) (5) Table 2.5.2-3 Item # 4 | N/A | (1) (5) | N/A | N/A |
| 5.10 | Repair | X Table 2.5.1-6 Item # 17 | (1) (5) | N/A | (1) (5) | N/A | N/A |
| 5.11 | Identification | X Table 2.5.1-6 Item # 13 | (1) (5) Table 2.5.2-3 Item # 5 | N/A | (1) (5) | N/A | N/A |
| 5.12 | Auxiliary Features | X Table 2.6.3-3 Item # 1, 8, 9, 14 | (1) (5) | N/A | (1) (5) | N/A | N/A |
| 5.13 | Multi Unit Stations | (3) | (3) | (3) | (3) | (3) | (3) |

## Table 14.3-8 IEEE 603-1991 Compliance Matrix by DCD Tier 1 Section

### (Sheet 3 of 4)

| IEEE Std. 603-1991 | | Tier 1 DCD Subsection Number | | | | | |
|---|---|---|---|---|---|---|---|
| Section Number | Section Title or Topic | 2.5.1 (PSMS) | 2.5.2 (SSD) | 2.5.3 (DAS) | 2.5.4 (PAM/BISI/ SPDS et. al.) | 2.5.5 (PCMS) | 2.5.6 (DCS) |
| 5.14 | Human Factors Considerations | X Tier 1, Section 2.9 | | | | | |
| 4.9 and 5.15 | Reliability | (4) | (4) | (4) | (4) | (4) | (4) |
| 6.1 and 7.1 | Automatic Control | X Table 2.5.1-6 Item # 11, 14, 18, 23 | (1) (5) | N/A | (1) (5) | N/A | N/A |
| 6.2 and 7.2 | Manual Control | X Table 2.5.1-6 Item # 4, 11 | (1) (5) | N/A | (1) (5) | N/A | N/A |
| 6.3 | Interaction between Sense and Command Features | X Table 2.5.1-6 Item # 25, 26 | (1) (5) | N/A | (1) (5) | N/A | N/A |
| 6.4 | Derivation of System Inputs | X Table 2.5.1-6 Item # 16 | (1) (5) | N/A | (1) (5) | N/A | N/A |
| 6.6 and 7.4 | Operating Bypasses | X Table 2.5.1-6 Item # 17, 18 | (1) (5) | N/A | (1) (5) | N/A | N/A |

Attachment 3

RAI 255
14.03.05-21

## Table 14.3-8 IEEE 603-1991 Compliance Matrix by DCD Tier 1 Section

(Sheet 4 of 4)

| IEEE Std. 603-1991 | | Tier 1 DCD Subsection Number | | | | | |
|---|---|---|---|---|---|---|---|
| Section Number | Section Title or Topic | 2.5.1 (PSMS) | 2.5.2 (SSD) | 2.5.3 (DAS) | 2.5.4 (PAM/BISI/ SPDS et. al.) | 2.5.5 (PCMS) | 2.5.6 (DCS) |
| 6.7, 7.5, and 8.3 | Maintenance Bypass | X Table 2.5.1-6 Item # 17 | (1) (5) | N/A | (1) (5) | N/A | N/A |
| 6.8 | Setpoints | X Table 2.5.1-6 Item # 19 | (1) (5) | N/A | (1) (5) | N/A | N/A |
| 8.1 | Electrical Power Sources | X Table 2.5.1-6 Item # 9, 20, 21 | (1) (5) | N/A | (1) (5) | N/A | N/A |

Table Notes:

X means full compliance. The applicable ITAAC Table and Item # is identified in the cell:

N/A The IEEE Std. 603-1991 Section is Not Applicable.

(1) Safety-related portions only.

(2) No ITAAC is required for this criterion. See the description of the 10 CFR 50, Appendix B, Quality Assurance Program that is applied to the design, fabrication, construction, and test of the safety-related structures, systems, and components provided as part of the preliminary Safety Evaluation Report as required by 10 CFR 50.34(a)(7).

(3) Multi Unit Stations are not applicable to the US APWR since the US APWR is a single unit.

(4) No specific ITAAC is required for this criterion. Reliability of I&C systems is considered in the PRA and addressed by D-RAP program ITAAC Item 1 in Table 2.13-1.

(5) The ITAAC item identified for Section 2.5.1 is applicable to the Safety Related portions of Section 2.5.2, Section 2.5.4, and Section 2.5.6.