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

November 29, 2011

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

Attention: Mr. Jeffrey A. Ciocco

Docket No. 52-021
MHI Ref: UAP-HF-11412

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

**References:** 1) "REQUEST FOR ADDITIONAL INFORMATION 829-6059 REVISION 3, SRP Section: 07.08 – Diverse Instrumentation and Control Systems, Application Section: 07.08" dated September 19, 2011.

2) "REQUEST FOR ADDITIONAL INFORMATION 830-6056 REVISION 3, SRP Section: 07.08 Branch Technical Position – Guidance for Application of Regulatory Guide 1.22, Application Section: 07.08" dated September 22, 2011.

3) "REQUEST FOR ADDITIONAL INFORMATION 833-6058 REVISION 3, SRP Section: 07.14 Branch Technical Position – Guidance on Software Reviews for Digital Computer-Based Instrumentation and Controls Systems, Application Section: Software Program Manual" dated September 29, 2011.

4) "REQUEST FOR ADDITIONAL INFORMATION 775-5836 REVISION 3, SRP Section: 07.08 – Diverse Instrumentation and Control Systems, Application Section: 07.08" dated June 28, 2011.

5) "MHI's Responses to US-APWR DCD RAI for Chapter 7, Response to the Additional Questions from the NRC", ML11258A153 (MHI Ref: UAP-HF-11314), dated September 13, 2011.

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

Enclosure 2 and 3 are the responses to RAIs contained within Reference 1, 2 and 3, and enclosure 4 and 5 are the amended responses to the RAI contained within Reference 4. The responses submitted with Reference 5 are revised according to the staff's comments provided in conference calls held in October 2011.

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

D081
NRO

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

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

Sincerely,

Takayuki Mori for

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

Enclosures:

1. Affidavit of Takayuki Mori

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

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

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

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

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

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

# Enclosure 1

Docket No. 52-021
MHI Ref: UAP-HF-11412

**MITSUBISHI HEAVY INDUSTRIES, LTD.**

**AFFIDAVIT**

I, Takayuki Mori, state as follows:

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

2. In accordance with my responsibilities, I have reviewed the enclosed documents have determined that portions of the document contain proprietary information that should be withheld from public disclosure. Those pages containing proprietary information are identified with the label "Proprietary" on the top of the page and the proprietary information has been bracketed with an open and closed bracket as shown here "[ ]". The first page of the document indicates that all information identified as "Proprietary" should be withheld from public disclosure pursuant to 10 C.F.R. § 2.390 (a)(4).

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

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

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

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

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

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

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

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

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

Executed on this 29th day of November, 2011.

Takayuki Mori

Takayuki Mori,
Engineering Manager- Licensing Promoting Group in APWR Promoting Department
Mitsubishi Heavy Industries, LTD.

Enclosure 3

Docket No. 52-021
UAP-HF-11412

Response to Request for Additional Information for Chapter 7

November 2011

Non-Proprietary Version

# This Enclosure includes following response of RAIs

RAI No. 829-6059 Revision 3, Question No.: 07.08-25

RAI No. 830-6056 Revision 3, Question No.: 07.08 Branch Technical Position-1

RAI No. 830-6056 Revision 3, Question No.: 07.08 Branch Technical Position-2

RAI No. 830-6056 Revision 3, Question No.: 07.08 Branch Technical Position-3

RAI No. 830-6056 Revision 3, Question No.: 07.08 Branch Technical Position-4

RAI No. 830-6056 Revision 3, Question No.: 07.08 Branch Technical Position-5

RAI No. 833-6058 Revision 3, Question No.: 07-14 Branch Technical Position-47

RAI No. 833-6058 Revision 3, Question No.: 07-14 Branch Technical Position-48

RAI No. 833-6058 Revision 3, Question No.: 07-14 Branch Technical Position-50

RAI No. 833-6058 Revision 3, Question No.: 07-14 Branch Technical Position-52

RAI No. 833-6058 Revision 3, Question No.: 07-14 Branch Technical Position-53

RAI No. 833-6058 Revision 3, Question No.: 07-14 Branch Technical Position-54

## RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

**11/29/2011**

**US-APWR Design Certification**

**Mitsubishi Heavy Industries**

**Docket No. 52-021**

| | |
|---|---|
| **RAI NO.:** | **NO.829-6059 REVISION 3** |
| **SRP SECTION:** | **07.08 – DIVERSE INSTRUMENTATION AND CONTROL SYSTEMS** |
| **APPLICATION SECTION:** | **07.08 – DIVERSE INSTRUMENTATION AND CONTROL SYSTEMS** |
| **DATE OF RAI ISSUE:** | **9/19/2011** |

---

**QUESTION NO. :** 07.08-25

BTP 7-19 Revision 5, Section 3 "Acceptance Criteria," on page 7-19-7 specifically states that *"...the displays and controls should be sufficient for the operator to monitor and control the following critical safety functions: reactivity level, core heat removal, reactor coolant inventory, containment isolation, and containment integrity."*

DCD Chapter 7.8, Table 7.8-2, shows the variables monitored by the DAS. As seen on Table 7.8-2, reactivity control, core heat removal, reactor coolant inventory and containment integrity are monitored as part of the DAS variables on the DHP. But these variables do not specifically address how the DAS monitors the containment isolation function as stated in BTP 7-19. The DAS has various manual conventional actuation switches available in the DHP for operator control of these functions, including a manual containment isolation switch which closes all major containment isolation valves at once, as mentioned on page 3-4 of MUAP-07014 Revision 3. The staff does not find how the DAS specifically monitors containment isolation on the DHP and requests MHI to clarify how the DAS monitors that the containment isolation function has occurred.

---

**ANSWER:**

As described in Subsection 7.8.1.1.3 of the US-APWR DCD, the DHP provides the indications, required in BTP 7-19, for monitoring of parameters that support safety functions. These indications are sufficient to support and monitor all manual control actions to maintain all critical safety functions including the containment isolation and containment integrity.

The DHP provides indication of the containment pressure. It does not provide indication for each containment isolation valve position. The design basis is as follows:

In BTP 7-19 Revision 6 (draft) Section B.1.2, the critical safety function is defined as "Containment Conditions"; containment isolation and containment integrity are not specifically

defined within the context of "Plant Critical Safety Functions" as they are in Revision 5. This change is consistent with Section 6 "Echelons of Defense" in ISG-02.

The containment conditions cannot be monitored only by the containment isolation valve position, because there are many other potential breach paths from the containment to the atmosphere than the path through the containment isolation valves. To monitor containment conditions, the DHP includes containment pressure. Monitoring containment pressure is more comprehensive than monitoring the position of the containment isolation valves because it encompasses any breaches in the containment, not just penetrations that have automatic isolation valves. If any containment penetration remains unisolated or there is any breach in the containment, the containment pressure will decrease after the accident. Therefore, the containment isolation function can be indirectly monitored by the containment pressure instrumentation on the DHP.

In addition, BTP 7-19 allows a "best estimate analysis" which does not require consideration of additional failures concurrent with the CCF. This was implied in BTP 7-19 Revision 5 which states "the diverse or different function may be performed by a non-safety system". It is explicitly stated in Revision 6 (draft) "single failures concurrent with a CCF are not required to be postulated". Therefore, when the switch for DHP containment isolation is manually actuated, containment isolation is credited to occur correctly. Based on the best estimate analysis, the containment conditions can be monitored and verified by the pressure indication on the DHP. Therefore, no needs to monitor the status of the each containment isolation valve on the DHP.

The design basis for including indication of containment pressure on the DHP, but not including indication of each containment isolation valve position, will be added to Section 7.8.1.1.3.

**Impact on DCD**
Subsection 7.8.1.1.3 of US-APWR DCD will be revised as shown in Attachment-1.

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

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

**Impact on PRA**
There is no impact on the PRA.

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

This completes MHI's response to the NRC's question.

actuation signals are blocked when the MCR/RSR transfer is activated, refer to ~~MUAP-07004~~the Safety I&C Technical Report (Reference 7.8-3) Figure 4.2-1. DCD_07.01-30

The manual actuation switches listed above are sufficient to take all manual actions credited in the D3 Coping Analysis Technical Report ~~MUAP-07014~~(Reference 7.8-2), which demonstrates the ability to maintain all critical safety functions and achieve hot standby. Hot standby can be maintained for an extended period-of-time by direct operation of local power distribution and switching devices that are not affected by the CCF in the PSMS. DCD_07.01-30

#### 7.8.1.1.2 Alarms

When the DAS system level actuation signals are generated for (1) reactor trip, turbine trip, and MFW isolation, or for (2) EFW actuation ~~are generated, a summary~~or for (3) ECCS actuation, alarm for these functions is also actuated on the DHP. The diverse audible alarm is activated to notify the operators. The first out alarm panel, on the DHP, indicates the specific input parameter that has caused the system level actuation of reactor Trip, turbine trip and MFW isolation. MIC-03-07-00005 DCD_07.01-29

Failure information about the DAS, such as power supply failure, or module de-energized~~ation~~ or removal, is alarmed as a "DAS failure summary alarm" on the Alarm VDU in the MCR. The configuration of the DAS alarms is described in Topical Report MUAP-07006 Subsection 6.2.2.1. High main steam radiation (N16) and high-high steam generator water level are alarmed and indicated on DHP. DAS alarms for high main steam radiation (N-16) and high-high steam generator water level are blocked during non CCF conditions, as described in Subsection 3.5.3 of the D3 Coping Analysis Technical Report (Reference 7.8-2). The duration of the blocking logic delay considers actuation times associated with emergency load sequencing conditions. When the blocking time delay expires, the DAS remains blocked if the status of plant components indicates the PSMS has actuated correctly. These block, shown in Figure 7.8-2, Figure 7.8-3, Figure 7.8-4, Figure 7.8-5 and Figure 7.8-6 consider both complete CCF and partial CCF conditions. The blocking logic considers both complete CCF and partial CCF conditions. Section 3.5 of D3 Coping Analysis Technical Report (Reference 7.8-2) provides the analysis for these conditions. The D3 Coping Analysis Technical Report (Reference 7.8-2)~~Technical Report MUAP-07014~~ provides the specific information of the alarm credited for D3 coping analysis. MIC-03-07-00001 DCD_07.08-16 DCD_07.01-30 DCD_07.08-16

#### 7.8.1.1.3 Indicators

The analog indicators provided on the DHP are identified in Table 7.8-2. These indicators are sufficient to support all manual control actions credited in Technical Report MUAP-07014, which demonstrates the ability to maintain all critical safety functions, and achieve and maintain hot standby.

The DHP provides indication of the containment pressure. It does not provide indication for each containment isolation valve position. The design basis is as follows: Monitoring containment pressure is more comprehensive than monitoring the position of the containment isolation valves because it encompasses any breaches in the containment, not just penetrations that have automatic isolation valves. In addition, BTP 7-19 allows a "best estimate analysis" which does not require consideration of additional failures DCD_07.08-25

concurrent with the CCF. Therefore, when the switch for DHP containment isolation is manually actuated, containment isolation is credited to occur correctly. Based on the best estimate analysis, the containment conditions can be monitored and verified by the pressure indication on the DHP. DCD_07.08-25

### 7.8.1.2 Diverse Automatic Actuation Cabinet

Each DAAC provides for automatic actuation of critical systems, which are required to be actuated within first 10 minutes of an event (refer to Table 7.8-3 for system actuation times). The defense in depth and diversity coping analysis provides justification for manual operator actions credited after 10 minutes.

Safety-related sensors selected by the plant design for the DAS input are interfaced from within the PSMS or PCMS input modules. These input modules utilize analog distribution modules and isolation modules that connect the input signals to the DAS prior to any digital processing. Therefore, a software CCF within the PSMS or PCMS does not affect the DAS automation function or the display of plant parameters on the DHP. The MELTAC input module design of the PSMS or PCMS is described in ~~MUAP-07005~~the MELTAC Platform Technical Report (Reference 7.8-4) Section 4.0. DCD_07.01-30

~~The DAS has two analog logic subsystems, one each located in one of the two DAACs.~~ DCD_07.08-24

DCD_07.01-30

Within each DAAC, input signals are compared to their setpoint values and if the monitored value is greater than or less than its setpoint, a partial trip/actuation signal is generated. RT signals and/or ESF actuation signals are generated from each DAAC through voting logic of its input signals. The voting logic (2-out-of-4) for each specific monitored parameter is shown in Table 7.8-4. Table 7.8-6 provides range, accuracy, and setpoint for each diverse actuation variables.

The DAS actuation signals from ~~both~~four DAAC subsystems are configured at their destination using 2-out-of-2 voting logic after taking 1-out-of-2 voting logic twice to execute actuation of RT and ESF systems. DCD_07.08-24 DCD_07.01-30

The monitored signals are isolated from the PSMS and interfaced to the separate subsystems in each DAAC. Process variables monitored for automatic actuation functions are: (a) Pressurizer pressure (4 channels each for low and high-pressure signals), (b) SG water level (4 channels, one per each SG for low level signals).

The numbers of channels required for each automatic actuation function are based on the following considerations:

- No single failure spuriously actuates the DAS.
- ~~Unlimited b~~Bypass of a single channel does not cause the DAS automatic function to be inoperable, prevent decisions regarding credited manual actions or prevent monitoring critical safety functions. DCD_07.01-30

The defeat switch can be manually actuated during plant heatup and cooldown conditions to prevent actuation of the DAS when it is not needed. This is an administratively controlled operating bypass.

## RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

**11/29/2011**

**US-APWR Design Certification**

**Mitsubishi Heavy Industries**

**Docket No. 52-021**

| | |
|---|---|
| **RAI NO.:** | **NO. 830-6056 REVISION 3** |
| **SRP SECTION:** | **07-08 BRANCH TECHNICAL POSITION – GUIDANCE FOR APPLICATION OF REGULATORY GUIDE 1.22** |
| **APPLICATION SECTION:** | **7.8** |
| **DATE OF RAI ISSUE:** | **9/22/2011** |

**QUESTION NO. : 07-08 Branch Technical Position-1**

**Regulatory guidance:**
NUREG-0800, Appendix 18-A, Section C states, "A diversity and defense-in-depth (D3) analysis should include the justification of any operator actions that are credited for response to an AOO/PA concurrent with software CCF as described in BTP 7-19.

**Evaluation:**
MUAP-07006, Section 3.1.3 states: Operator actions may be required within 30 minutes for some events such as feedwater line break and small break loss-of-coolant accidents. MUAP-07014 contains no mention of operator actions for a feedwater line break.

**Question:**
Are there manual actions associated with feedwater line breaks?

**ANSWER:**

No manual actions from the Diverse HSI Panel (DHP) are needed to mitigate the feedwater line break event within the first 10 minutes of the event. However, as shown in MUAP-07006 Table 6.1-2, manual isolation of EFW to the faulted SG is needed in order to maintain hot shutdown conditions. This is achieved by manually closing the EFW control valve on the DHP. The evaluation of the time required and time available for this manual action are described below.

MHI performed a sensitivity analysis to evaluate the time available for the isolation of EFW to the faulted SG assuming that one EFW pump is out of service due to maintenance. Unless specifically listed below, the assumptions, input parameters and initial conditions assumed in this sensitivity analysis are the same as the DCD Chapter 15 safety analysis.

Figure 07-08-1.1 and Figure 07-08-1.2 show the sensitivity analysis transient results for RCP outlet pressure and hot leg temperature, respectively. In the analysis, the manual EFW isolation is assumed to occur 15 minutes after the DAS automatic reactor trip. These results show that the peak RCP outlet pressure is below 3200 psig and the RCS temperature decreases since the available EFW flow is sufficient to remove decay heat. In addition, the DNB in this sensitivity analysis is bounded by the DNB of the loss of normal feedwater flow in MUAP-07014 (R5) Section 5.2.7 and thus core coolability is maintained. Therefore, the sensitivity analysis results show that the time available for manual EFW isolation is at least 15 minutes.

The time required for each manual action is evaluated based on MHI simulator experience. The evaluated time required is summarized in Table 07-08-1.1. As shown in the table, the total time required is 10 minutes, which is less than the 15 minutes available described above. Therefore, there is sufficient margin between the time required and the time available for the manual EFW isolation in the feedwater line break event. Note that the time required will be verified using table top walkthroughs and validated using a high fidelity dynamic simulator, as described in the D3 coping analysis technical report. Verification and validation activities will employ senior reactor operators and HFE experts.

Table 07-08-1.1: Feedwater System Pipe Break Inside and Outside Containment

| | |
|---|---|
| **Failure mode** | PSMS: disabled<br>PCMS: disabled/available |
| **Prompting Alarm** | DAS automatic reactor trip actuation alarm |

| **Operator Actions** | **Time required** |
|---|---|
| Move to DHP | 0.5 minutes |
| Confirm procedure in manual | 0.5 minutes |
| Energize DHP with Permissive Switch for DAS HSI | 0.5 minutes |
| Follow steps in the procedure for this event to isolate emergency feedwater flow to the affected SG by using EFW control valve on DHP | 8.5 minutes |
| | Total time required 10.0 minutes |

Figure 07.08-1.1 RCP Outlet Pressure versus Time
Feedwater System Pipe Break Inside and Outside Containment

Figure 07.08-1.2 Hot Leg Temperature of Faulted Loop versus Time
Feedwater System Pipe Break Inside and Outside Containment

**Impact on DCD**
There is no impact on the DCD.

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

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

**Impact on PRA**
There is no impact on the PRA.

**Impact on Technical / Topical Reports**
Subsection 5.2.8 (2) in Technical Report MUAP-07014 will be revised as follows.

(2) Core Coolability
This event in the DCD is bounded by the minimum DNBR for the DCD Section 15.2.7 ~~event,~~ Feedwater System Pipe Break Inside and Outside Containment in that DNB does not occur due to ~~by~~ the low steam generator water level reactor trip. Although the diverse low steam generator water level reactor trip analytical limit is lower and the delay time is greater than that of the RTS, DNB is not a significant adverse consequence considering the axial power distribution for the BOC. On the other hand, DNB is mitigated by the effect of the RCS cool down because of the discharge of twophase flow from the feedwater line after the nozzle in the faulted steam generator ~~perforated nozzle~~ is uncovered by the secondary water in this event. Therefore, the core coolability is maintained for this event concurrent with a CCF. ~~This event is categorized as an "expertly judged" event for core coolability.~~

As indicated above, no manual actions from the DHP are needed to mitigate the feedwater line break event within the first 10 minutes of the event. However, as shown in MUAP-07006 Table 6.1-2 (Reference 3), manual isolation of EFW to the faulted SG is needed in order to maintain hot shutdown conditions. This is achieved by manually closing the EFW control valve on the DHP. The evaluated time available for this manual action is at least 15 minutes. The time required for each manual action is evaluated based on MHI operational experience. The evaluated time required is summarized in Table 5.2.8-1. As shown in the table, the total time required is 10 minutes, which is less than the 15 minutes available described above. Therefore, there is sufficient margin between the time required and the time available for the manual EFW isolation in the feedwater line break event.

**Table 5.2.8-1: Feedwater System Pipe Break Inside and Outside Containment**

| | |
|---|---|
| **Failure mode** | PSMS: disabled<br>PCMS: disabled/available |
| **Prompting Alarm** | DAS automatic reactor trip actuation alarm |

| **Operator Actions** | **Time required** |
|---|---|
| Move to DHP | 0.5 minutes |
| Confirm procedure in manual | 0.5 minutes |
| Energize DHP with Permissive Switch for DAS HSI | 0.5 minutes |
| Follow steps in the procedure for this event to isolate emergency feedwater flow to the affected SG by using EFW control valve on DHP | 8.5 minutes |
| | Total time required 10.0 minutes |

This completes MHI's response to the NRC's question.

## RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

**11/29/2011**

**US-APWR Design Certification**

**Mitsubishi Heavy Industries**

**Docket No. 52-021**

| | |
|---|---|
| **RAI NO.:** | **NO. 830-6056 REVISION 3** |
| **SRP SECTION:** | **07-08 BRANCH TECHNICAL POSITION – GUIDANCE FOR APPLICATION OF REGULATORY GUIDE 1.22** |
| **APPLICATION SECTION:** | **7.8** |
| **DATE OF RAI ISSUE:** | **9/22/2011** |

**QUESTION NO. : 07-08 Branch Technical Position-2**

**Regulatory guidance:**
NUREG-0800, Appendix 18A, Section C states, "A diversity and defense-in-depth (D3) analysis should include the justification of any operator actions that are credited for response to an AOO/PA concurrent with software CCF as described in BTP 7-19.

**Evaluation:**
Technical Report *Defense-In-Depth and Diversity Coping Analysis* (MUAP-07014), Rev 4., Section 3.3 states: "The Diverse HSI Panel (DHP), which is located in the main control room (MCR), contains conventional switches for manual actuation of the systems and the components which are required to cope with a CCF." (Emphasis added)

The list from the MUAP is reproduced below along with the staff's understanding of how the action is used. Some of these actions do not appear to be credited in the Best Estimate analyses summarized in section 5 of MUAP-07014.

- Manual reactor trip / Turbine trip / Main feedwater isolation
  Staff understanding: Credited as the diverse reactor trip function and in the SGTR response; otherwise, redundant to automatic signal
- Manual emergency feedwater actuation
  Staff understanding: Not credited - Redundant to automatic signal
- Manual emergency core cooling system (ECCS) actuation
  Staff understanding: Not credited - Redundant to automatic signal
- Manual containment isolation
  Staff understanding: Not addressed in section 5 but appears to be a manual action operators would have to perform.
- Manual operation of emergency feedwater control valves
  Staff understanding: Credited in SGTR for isolation of affected S/G
- Manual operation of main steam depressurization valves
  Staff understanding: Credited in SGTR for depressurization and equalization of pressure between RCS and SG
- Manual operation of safety depressurization valve

Staff understanding: Credited in SGTR for depressurization and equalization of pressure between RCS and SG

- Manual operation of main steam isolation valves: 4 switches
  Staff understanding: Credited in SGTR for isolation of affected S/G

**Questions:**

1. Correct any errors or omissions in this list.
2. If containment isolation is credited please include these manual actions in the analysis descriptions in section 5.

**ANSWER:**

MUAP-07014 (R5) assumes the following manual switches to mitigate Ch.15 events concurrent with CCF.

- Manual reactor trip / Turbine trip / Main feedwater isolation for the diverse reactor trip function is credited in the SGTR event as shown in Figure 5.6.3-1 in MUAP-07014 (R5). This is consistent with the staff understanding above.

- Manual emergency feedwater actuation is not credited because DAS can automatically initiate emergency feedwater actuation. This is consistent with the staff understanding above.

- Manual emergency core cooling system (ECCS) actuation is not credited because Diverse Actuation System (DAS) can automatically initiate ECCS actuation. This is consistent with the staff understanding above.

- Manual containment isolation is used to isolate containment in LOCA events. Containment is isolated to reduce the potential risk of releasing radiological materials when plant parameters, such as containment pressure, alert operators to the potential need for manual containment spray to maintain containment integrity. As described in MUAP-07014 (R5), the time available for manual containment spray actuation is more than 24 hours in LOCA events concurrent with CCF. Note that this is somewhat different from the staff understanding above.

- Manual operation of emergency feedwater control valves is used to control SG water level during any event. The valves are also credited to isolate the affected SG for an SGTR as shown in Figure 5.6.3-1 in MUAP-07014 (R5). In addition, isolation of EFW to the affected SG during a feedwater line break is performed as described in the response to Question 07-08 Branch Technical Position-1 of this RAI. Note that this is somewhat different from the staff understanding above.

- Manual operation of main steam depressurization valves is credited to maintain hot shutdown conditions and cool down the reactor coolant system in an SGTR event as shown in Figure 5.6.3-1 in MUAP-07014 (R5). Note that this is somewhat different from the staff understanding above.

- Manual operation of safety depressurization valve is credited to equalize pressures during an SGTR event as shown in Figure 5.6.3-1 in MUAP-07014 (R5). This is consistent with the staff understanding above.

- Manual operation of main steam isolation valves is credited in an SGTR event as shown in Figure 5.6.3-1 in MUAP-07014 (R5). This is consistent with the staff understanding above.

**Impact on DCD**
There is no impact on the DCD.

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

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

**Impact on PRA**
There is no impact on the PRA.

**Impact on Technical / Topical Reports**
As indicated in the question, the operator action to manually isolate containment is not explicitly described in the applicable subsections of Section 5. Therefore, MUAP-07014 will be revised to include this manual action in the appropriate analysis descriptions and also in Table 3.4-1. The third paragraph of Subsection 5.6.5.1 (1) will be revised as follows.

> For LBLOCA, the pressurizer pressure decreases rapidly to reach the automated ECCS actuation setpoint. This results in the DAS SI actuation and a DHP alarm. The operator continues to check the plant parameters on the DHP for preparation of containment spray actuation. The time available from the reactor trip actuation alarm to manual actuation of containment spray and to isolate containment on the DHP is more than 24 hrs. Within this duration the containment pressure is maintained less than the ultimate pressure of 216 psia. This time is sufficient for manual containment isolation on the DHP and manual actuation of containment spray using local controls. HFE analysis to confirm sufficient margin between time available and time required for local actions as discussed in Section 3.4.

The second paragraph of Subsection 5.6.5.2 (1) will be revised as follows.

> For SBLOCA, the pressurizer pressure decreases rapidly to reach the reactor trip setpoint and also the SI pump shutoff head. The DAS starts the SI pumps based on low-low pressurizer pressure. After the SI pumps are automatically started along with the actuation alarm on the DHP, the operator continues to check the plant parameters on the DHP. The time available from the reactor trip actuation alarm to manual actuation of the containment spray and to isolate containment on the DHP is more than 24 hrs. Within this duration the containment pressure is maintained less than the ultimate pressure of 216 psia. This time is sufficient for manual containment isolation on the DHP and manual actuation of the containment spray using local controls. HFE analysis to confirm sufficient margin between time available and time required for local actions as discussed in Section 3.4.

This completes MHI's response to the NRC's question.

## RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

**11/29/2011**

**US-APWR Design Certification**

**Mitsubishi Heavy Industries**

**Docket No. 52-021**

| | |
|---|---|
| **RAI NO.:** | **NO. 830-6056 REVISION 3** |
| **SRP SECTION:** | **07-08 BRANCH TECHNICAL POSITION – GUIDANCE FOR APPLICATION OF REGULATORY GUIDE 1.22** |
| **APPLICATION SECTION:** | **7.8** |
| **DATE OF RAI ISSUE:** | **9/22/2011** |

**QUESTION NO. : 07-08 Branch Technical Position-3**

**Regulatory guidance:**
NUREG-0800, Appendix 18A, Analysis criterion 4: The sequence of actions uses only alarms, controls, and displays that would be available in the MCR and operable during the assumed CCF scenario(s), as documented in the Failure Modes and Effects Analysis.

**Evaluation:**
MUAP-07006, Rev. 2 (accepted), Section 3.1.3 states, "Any operator actions credited prior to 30 minutes are justified based on human factors engineering (HFE) evaluation."

MUAP-07014, Rev. 4, Section 3.4 (bottom of page 3-6) states, "As described in MUAP-07006, any operator actions credited in the D3 coping analysis are justified based on a Human Factor Engineering (HFE) evaluation."

Several paragraphs later in MUAP-07014, Section 3.4 states, "Tasks for all credited time critical manual operator actions will be analyzed according to the Special Event procedures to confirm adequate time margin between time available and time required."

Since MUAP-07006 doesn't actually say what MUAP-07014 says and MUAP-07014 has statements that could be interpreted inconsistently, the staff is asking for MHI to confirm that all manual actions credited in the coping analysis are justified with an HFE evaluation. Many of the manual actions that occur greater than 30 minutes are local actions and thus are inconsistent with regulatory guidance which suggests that any DAS credited actions should be implemented from the control room. The staff is reviewing the use of local manual action as an alternate method and has used the HFE evaluation (and subsequent V&V) as the basis for accepting local manual actions.

**Questions:**
1. Confirm MUAP-07014 statement that, "any operator actions credited in the D3 coping analysis are justified based on a Human Factor Engineering (HFE) evaluation."
2. Is reference to MUAP-07006 appropriate?

**ANSWER:**

Response to the Question No.1
This is correct. Any operator actions credited in the D3 coping analysis are justified by HFE evaluation. Since actions after 30 minutes are not considered time critical, the HFE evaluation is conducted to confirm HSI suitability and availability, with reasonable consideration of time constraints, i.e., MHI does not plan to document a detailed assessment of time margin between time available and time required, based on the steps in the special event EOPs.

Response to the Question No.2
Yes, there is no inconsistency between MUAP-07006 and MUAP-07014. An HFE evaluation is conducted for all credited actions, as described in MUAP-07006.

**Impact on DCD**
There is no impact on the DCD.

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

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

**Impact on PRA**
There is no impact on the PRA.

**Impact on Technical / Topical Reports**
The sixth paragraph of Subsection 3.4 of MUAP-07014 will be revised as follows.

> As described in MUAP-07006, any operator actions credited in the D3 coping analysis are justified based on a Human Factor Engineering (HFE) evaluation (Reference 11 and 12). Since actions after more than 30 minutes are not considered time critical, the HFE evaluation is conducted to confirm HSI suitability and availability, with reasonable consideration of time constraints. As shown in Table 3.4-1 the list of required operator tasks associated with the mitigation of an event with a concurrent CCF is considerably simplified compared with the tasks necessary for mitigating events without a concurrent CCF.

This completes MHI's response to the NRC's question.

## RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

**11/29/2011**

**US-APWR Design Certification**

**Mitsubishi Heavy Industries**

**Docket No. 52-021**

| | |
|---|---|
| **RAI NO.:** | **NO. 830-6056 REVISION 3** |
| **SRP SECTION:** | **07-08 BRANCH TECHNICAL POSITION – GUIDANCE FOR APPLICATION OF REGULATORY GUIDE 1.22** |
| **APPLICATION SECTION:** | **7.8** |
| **DATE OF RAI ISSUE:** | **9/22/2011** |

**QUESTION NO. : 07-08 Branch Technical Position-4**

**Regulatory guidance:**
NUREG-0800, Appendix 18A, Analysis criterion 1: The analysis establishes the time available using an analysis method and acceptance criteria consistent with the guidance of BTP 7-19. The basis for the time available is documented.

**Evaluation:**
MHI's Responses to NRC's RAIs on Topical Report MUAP-07006-P(R1) Defense-in-Depth and Diversity (UAP-HF-08070-P, Revision 0), Response To The Second RAI (APRIL 2, 2008) pgs29-30, RAI #1-analyzed events states:

"SBLOCA violates the integrity of RCPB as an initiator. Therefore, the containment vessel (CV) integrity should be maintained. The US-APWR Probabilistic Risk Assessment, MUAP-07030 shows that for SBLOCA the operator has 4.91 hrs for manual actuation of CV spray to prevent the violation of CV integrity. DAS provides the low pressurizer pressure reactor trip actuation prompting alarm and the CV pressure indicator alerts the operator to the potential need for manual actions to maintain CV integrity. The design attributes for local controls credited in the D3 Coping Analysis, including immunity from the CCF and state based priority, will be added to the next revision of MUAP-07006."

MUAP-07014 states that the operator has 24 hours to start containment spray

**Questions:**
Why is there a difference in the time required for operator action between these two documents?

**ANSWER:**

MUAP-07014 (R1) states "The US-APWR Probabilistic Risk Assessment, MUAP-07030 (Reference 10) shows that[ ] This was changed in MUAP-07014 (R2) to "The US-APWR Probabilistic Risk Assessment, MUAP-07030 (Reference 10) shows that[

]This same revision added "The time available from the reactor trip actuation alarm to manual actuation of the containment spray is more than 24 hrs". Therefore, the inconsistency between the two documents has already been corrected.

Table 6.1-2 in MUAP-07006-P-A Rev.2 shows that manual actuation of containment spray for SBLOCA is not needed before 30 minutes. Although MUAP-07006-P-A Rev.2 does not provide a detailed value for the time available, it is consistent with MUAP-07014 in stating that the time available is greater than 30 minutes.

Although not specifically addressed in this RAI question, MHI would like to clarify some additional items regarding the consistency between MUAP-07006-P-A Rev. 2 and MUAP-07014:

1) For an SGTR, Table 6.1-2 in MUAP-07006-P-A Rev. 2 indicates that isolation of the secondary system, including closure of the MSIVs, is not needed before 30 minutes. This is consistent with the statement in MUAP-07014 that says "for an SGTR concurrent with CCF under realistic conditions, the time available for main steam isolation should be more than 30 minutes." However, MUAP-07014 also describes that manual switches for the MSIVs are provided on the DHP to allow for isolation of the ruptured SG before 30 minutes as an additional conservatism and to be consistent with the DCD Chapter 15 assumption.
2) Table 6.1-2 in MUAP-07006-P-A Rev.2 does not indicate the expected time for actions for a large break LOCA (LBLOCA). As a result, the Application-Specific Action Item 5.10 indicates that an LBLOCA concurrent with a CCF of the PSMS should be addressed. To address this Application-Specific Action for the US-APWR design certification, the D3 coping analysis of the LBLOCA in MUAP-07014 credits the DAS automatic actuation of the ECCS. Therefore, this is not an inconsistency between MUAP-07014 and MUAP-07006-P-A Rev.2

MHI will revise Technical Report MUAP-07014 (as shown below) to clarify some of the information discussed above. However, no changes to MUAP-07006-P-A Rev.2 are necessary.

**Impact on DCD**
There is no impact on the DCD.

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

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

**Impact on PRA**
There is no impact on the PRA.

**Impact on Technical / Topical Reports**
The second paragraph of Subsection 5.6.5.2 (1) in Technical Report MUAP-07014 will be revised as follows.

> (1) Pressure Boundary Integrity
> An SBLOCA event violates the integrity of the RCPB as the event initiator. Therefore, the event acceptance criterion is that the containment integrity should be maintained.

For SBLOCA, the pressurizer pressure decreases rapidly to reach the reactor trip setpoint and also the SI pump shutoff head. The DAS starts the SI pumps based on low-low pressurizer pressure. After the SI pumps are automatically started along with the actuation alarm on the DHP, the operator continues to check the plant parameters on the DHP. Table 6.1-2 in MUAP-07006-P-A Rev.2 (Reference 3) shows that manual actuation of containment spray for SBLOCA is not needed before 30 minutes, but does not quantify the actual time available for this action. The time available from the reactor trip actuation alarm to manual actuation of the containment spray is more than 24 hrs. Within this duration the containment pressure is maintained less than the ultimate pressure of 216 psia. This time is sufficient for manual actuation of the containment spray using local controls. HFE analysis to confirm sufficient margin between time available and time required for local actions as discussed in Section 3.4.

## RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

**11/29/2011**

**US-APWR Design Certification**

**Mitsubishi Heavy Industries**

**Docket No. 52-021**

| | |
|---|---|
| **RAI NO.:** | **NO. 830-6056 REVISION 3** |
| **SRP SECTION:** | **07-08 BRANCH TECHNICAL POSITION – GUIDANCE FOR APPLICATION OF REGULATORY GUIDE 1.22** |
| **APPLICATION SECTION:** | **7.8** |
| **DATE OF RAI ISSUE:** | **9/22/2011** |

**QUESTION NO. : 07-08 Branch Technical Position-5**

**Regulatory guidance:**
The analysis establishes the time available using an analysis method and acceptance criteria consistent with the guidance of BTP 7-19. The basis for the time available is documented.

**Evaluation:**
The time available, time required, available margin and the basis for these numbers is not clear for the SGTR event. The following compiles the data the staff has extracted from the DCD chapter 15 design basis analysis and the MUAP-07014 Best estimate analysis.

| | | | |
|---|---|---|---|
| SGTR occurs | T=0 | | |
| Receive MS line radiation alarm | Ch. 15 – alarm occurs within 2 min. of event | | |
| Operator moves to DHP | T=.5 min total=2.5min | | |
| Select special event EOP | T=.5 min total=3.0min | | |
| Operator energizes DHP manual controls | T=.5 min total=3.5min | | |
| Follow steps in procedure | | 07014 – total time through this step is 15 min | |
| • Operators manually trip reactor | T=1.5 min total=15min | Ch 15 – operators assumed to trip Rx 15 minutes after SGTR | |
| • Operators manually isolate the ruptured SG | T=5 min total=20min Ch. 15 – assumes 10 minutes from alarm initiation for operator to identify ruptured SG | Duration of activity is from Ch 15. 07014 indicates time available is 30 min | Margin = 10 min |

| | | | |
|---|---|---|---|
| • Operators start RCS cooldown by manually opening MSDVs | T=5 min total=25min | Duration of activity is from Ch 15<br>Time available? | Margin? |
| • Press equalization, Operator reduces RCS pressure using SDV | ? | Time available? | Margin? |
| • Operator secures ECCS | ? | Time available? | Margin? |

**Questions:**
1. Correct errors or omissions on this table.
2. Ensure Time available, Time required and margin are explicitly addressed in Chapter 5 of MUAP-07014.

**ANSWER:**

The procedure for responding to an SGTR concurrent with a CCF directs the operator to take a number of manual actions. The DHP provides the following manual switches for the performance of most of these SGTR-specific manual actions.

- Manual reactor trip switch
- EFW control valve switches and main steam isolation valve switches necessary to isolate the affected steam generator
- Main steam depressurization valve switches necessary to cool down the primary coolant system
- Pressurizer safety depressurization valve switch necessary to equalize pressure between the primary and secondary coolant systems

The other manual action in the procedure is to terminate SI, which must be done using local controls. However, as described in the D3 coping analysis technical report, MUAP-07014, local actions do not require special clothing or access to equipment in restricted locations for the US-APWR.

The DCD Ch. 15 SGTR analysis includes a dose case and an SG overfill case. The analysis assumes conservative operator action times considering the completion time for components such as valves opening/closing. Therefore, the same operator action times assumed in the DCD Ch. 15 are conservatively assumed as the time available for the manual actions in the D3 coping analysis of the SGTR.

In the DCD Ch. 15 SGTR analysis for the dose evaluation case, the completion time for the manual reactor trip is assumed to be within 15 minutes from event initiation. (Note that the DCD Ch. 15 SG overfill case assumes an automatic reactor trip on high-high SG level prior to 15 minutes. Since this reactor trip is not available on the DAS, only the manual reactor trip at 15 minutes is credited in MUAP-070114.) The isolation of the affected SG is assumed to be completed 5 minutes after the manual reactor trip and then initiation of the RCS cooldown and pressure equalization is assumed to occur 5 minutes after that. Therefore, these values are assumed as the time available for those actions in the D3 coping analysis as shown below in

Table 07-08-5.1. Local action is required for the termination of SI in CCF conditions. Therefore, MHI performed a sensitivity analysis to evaluate the time available from the time when SI termination conditions are achieved to the time of SG overfill. Unless specifically listed below, the assumptions, input parameters and initial conditions assumed in this sensitivity analysis are the same as the DCD Chapter 15 safety analysis.

Figure 07-08-5.1 through Figure 07-08-5.3 show the sensitivity analysis transient results for RCS pressure, steam generator pressure, and steam generator water volume, respectively. The analysis results show that the SI termination criteria are met at { } as indicated in Figure 07-08-5.1. The ruptured SG volume at { } is well below the maximum secondary volume as shown in Figure 07-08-5.3. Therefore, there is at least 10 minutes available for the operators to manually terminate SI after the SI termination criteria have been met.

The time required for each manual action is evaluated based on MHI operation experience. The evaluated time required and the time available described above are summarized below in Table 07-08-5.1. As shown in the table, each operator action has sufficient margin between the time required and the time available. Note that the time required will be verified using table top walkthroughs and validated using a high fidelity dynamic simulator, as described in the D3 coping analysis technical report. Verification and validation activities will employ senior reactor operators and HFE experts.

The D3 coping analysis technical report will be revised to include the information provided in this RAI response.

Table 07-08-5.1: Manual Action Times for Steam Generator Tube Rupture with CCF

| | Elapsed Time to Completion | Time Available | Time Required | | Margin |
|---|---|---|---|---|---|
| SGTR occurs | 0 min | 15 min | - | | - |
| Receive main steam line radiation alarm | 2 min | | - | Total = 15 min | Note 1 |
| Operators move to DHP | 15 min | | 0.5 min | | |
| Select special event EOP | | | 0.5 min | | |
| Operators energize DHP with Permissive Switch for DAS HSI | | | 0.5 min | | |
| Operators manually trip reactor on DHP | | | - | | |
| Operators manually isolate the ruptured SG on DHP | 20 min | 5 min | 2 min | | 3 min |
| Operators cool down RCS by manually opening MSDVs on DHP and Operators reduce RCS pressure (for pressure equalization) using SDV on DHP | 25 + $X^{Note2}$ min | 5 min | 3.5 min | | 1.25 min |
| Operators secure ECCS using local controls after SI termination conditions are achieved | 35 + $X^{Note2}$ + $Y^{Note3}$ min | 10 min (Total time available from the alarm initiation is more than 30 minutes) | 5 min | | 5 min |

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

Note 2: X is the amount of time from the start of the RCS cooldown to when primary and secondary pressures have been equalized. The value of X is determined by a transient system analysis. In the DCD Ch. 15 analysis, X is approximately 20 minutes.

Note 3: Y is the amount of time from when primary and secondary pressures have been equalized to when SI termination conditions are achieved. The value of Y is determined by a transient system analysis. In the DCD Ch. 15 analysis, Y is approximately 1 minute.

Figure 07.08-5.1 RCS Pressure versus Time
Steam Generator Tube Rupture – SG Overfill Analysis

Figure 07.08-5.2 Steam Generator Pressure versus Time
Steam Generator Tube Rupture – SG Overfill Analysis

Figure 07.08-5.3 Steam Generator Water Volume versus Time
Steam Generator Tube Rupture – SG Overfill Analysis

**Impact on DCD**
There is no impact on the DCD.

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

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

**Impact on PRA**
There is no impact on the PRA.

**Impact on Technical / Topical Reports**
The last four sentences of the second paragraph of Subsection 5.6.3 (3) in Technical Report MUAP-07014 will be revised as follows.

> The sequence of operator actions and the evaluated time required and the time available are ~~is~~ shown in Table 5.6.3-1. The DHP and local control provides adequate indication and control for the performance of SGTR-specific manual actions (same as assumed in the DCD and described above for an SGTR without CCF). ~~The time margin for manual reactor trip is sufficient to accommodate operator errors.~~ As shown in the table, each operator action has sufficient margin between the time required and the time available. HFE analysis to confirm sufficient margin between time available and time required for local actions is discussed in Section 3.4.

Table 5.6.3-1 in Technical Report MUAP-07014 will be replaced with the revised table on the following page:

**Table 5.6.3-1:**
**Radiological Consequences of Steam Generator Tube Failure in the case that a CCF in the PSMS also Affects All of the Control Functions of PCMS**

| **Failure mode** | **PSMS: disabled**<br>**PCMS: disabled** |
|---|---|
| **Prompting Alarm** | **Main steam line radiation (N-16) alarm** |

| **Operator Actions** | **Elapsed Time to Completion** | **Time Available** | **Time Required** | |
|---|---|---|---|---|
| SGTR occurs | 0 min | 15 min[Note 1] | - | |
| Receive main steam line radiation alarm | 2 min | | - | Total = 15 min |
| Operators move to DHP | 15 min | | 0.5 min | |
| Select special event EOP | | | 0.5 min | |
| Operators energize DHP with Permissive Switch for DAS HSI | | | 0.5 min | |
| Operators manually trip reactor on DHP | | | - | |
| Operators manually isolate the ruptured SG on DHP | 20 min | 5 min | 2 min | |
| Operators cool down RCS by manually opening MSDVs on DHP and Operators reduce RCS pressure (for pressure equalization) using SDV on DHP | 25 + $X^{Note2}$ min | 5 min | 3.5 min | |
| Operators secure ECCS using local controls after SI termination conditions are achieved | 35 + $X^{Note2}$ + $Y^{Note3}$ min | 10 min (Total time available from the alarm initiation is more than 30 minutes) | 5 min | |

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

Note 2: X is the amount of time from the start of the RCS cooldown to when primary and secondary pressures have been equalized. The value of X is determined by a transient system analysis. In the DCD Ch. 15 analysis, X is approximately 20 minutes.

Note 3: Y is the amount of time from when primary and secondary pressures have been equalized to when SI termination conditions are achieved. The value of Y is determined by a transient system analysis. In the DCD Ch. 15 analysis, Y is approximately 1 minute.

This completes MHI's response to the NRC's question.

## RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

**11/29/2011**

**US-APWR Design Certification**

**Mitsubishi Heavy Industries**

**Docket No. 52-021**

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

**QUESTION NO. :** 07-14 Branch Technical Position-47

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

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

BTP 7-14, Section B.3.1.3 provides guidance in evaluating a Software Quality Assurance Plan (SQAP). Clause 5.3.1 of IEEE Std. 7-4.3.2-2003, as endorsed by RG 1.152, provides guidance on software quality assurance. IEEE Std. 7-4.3.2-2003, Clause 5.3.1, states in part that "Guidance for developing software QA plans can be found in...IEEE Std 730-1998."

1) Section 3.3.8 of the SPM states that IEEE Std. 730-2002 is referenced by IEEE Std. 7-4.3.2-2003. This is not accurate. The staff requests MHI to correct the error. A way to correct is to state "IEEE Std. 730-2002 is an update to IEEE Std. 730-1998, and the latter is referenced by IEEE Std. 7-4.3.2-2003."

2) A SQAP that claims conformance with IEEE Std. 730-2002 should have the format prescribed in Section 4 of the standard. The standard lists the following 16 sections: purpose, reference documents, management, documentation, standards and practice, software reviews, test, problem reporting and corrective action, tools and methodologies, media control, supplier control, records, training, risk management, glossary, and SQAP change procedure. However, SQAP of the SPM has only the following eight sections: purpose, organization/responsibilities, security, measurement, procedures, record keeping, methods/tools, and standards, and these eight sections do not cover all of the 16 topics required for conformance. Applicants do not necessarily have to have 16 individual sections but applicants are expected to clearly address all 16 topics. Also, certain topics may be

discussed in other sections of the SPM – if so, just make a reference to it. For example, Clause 4.16 of IEEE Std. 730-2002 states that there should be procedures for modifying the SQAP and maintaining a history of such changes. MHI may already have such a procedure and the responsible organization - if so, point to it. The staff requests MHI to address this issue.

3) IEEE Std. 730-2002, Clause 4.3.1, states that the organization responsible for preparing and maintaining the SQAP shall be identified. The staff requests MHI to identify the responsible organization for preparing and maintaining the SQAP.

4) IEEE Std. 730-2002, Clause 4.4, states that SQAP is to identify the documentation governing the development, verification and validation, use, and maintenance of the software, and to list which documents are to be reviewed or audited for adequacy. IEEE Std. 730-2002, Clause 4.4.2, lists the minimum documentation requirements: SRD, SDD, V&V plans, V&V reports, user docs, SCMP, etc...The staff requests MHI to address these documentation requirements of Clause 4.4.

5) IEEE Std. 730-2002, Clause 4.5.2, states as a minimum, the following information is to be provided: documentation standards, design standards, coding standards, commentary standards, testing standards and practices, and selected SQA product and process metrics. The staff requests MHI to address this clause.

6) IEEE Std. 730-2002, Clause 4.6.2, states as a minimum, the following 10 software reviews shall be conducted: Software specifications review, architecture design review, detailed design review, verification and validation plan review, functional audit, physical audit, in-process audits, managerial reviews, SCMP review, and post-implementation review. MHI has addressed management reviews, functional audit, physical audit, in-process audits, and a partial design review. The staff requests MHI to address the remaining software reviews as well as any other reviews and audits identified in Clause 4.6.3 of IEEE Std. 730-2002.

7) IEEE Std. 730-2002, Clause 4.11, states that SQAP shall state the provisions for assuring that software provided by suppliers meets established requirements. The staff requests MHI to address this supplier control clause.

8) IEEE Std. 730-2002, Clause 4.15, states that SQAP shall contain a glossary of terms unique to SQAP. Staff requests MHI to address this glossary clause. If there are no SQAP terms unique to this plan, then state so. Sections 3.3.4 and 3.4.3 of SPM discuss software hazards are anomalies. The staff requests MHI to clarify the definitions of software hazards and anomalies.

9) IEEE Std. 730-2002, Clause 4.8, states that SQAP shall describe practices and procedures to be followed for reporting, tracking, and resolving problems or issues identified in both software items and the software development and maintenance process. The staff requests MHI to address this clause.

10) Section 3.3.5.4 of the SPM discusses problem reporting and corrective action, and states that application software hazards, problems and issues that constitute a condition averse to quality shall immediately result in initiation of a Nonconformance Report as described in PQD-HD-19005. The staff requests MHI to specify what constitutes a condition adverse to quality – in other words, what barrier must be met before a Nonconformance Report is initiated – examples would also be helpful.

---

**ANSWER:**

1) Referenced standard in Section 3.3.8 of the US-APWR SPM will be corrected to IEEE Std. 730-1998 which is referenced by IEEE Std. 7-4.3.2-2003.

2) The SQAP of the US-APWR SPM conforms to IEEE Std. 730-1998. Only the Subsection "Glossary" is added to Section 4 of IEEE Std. 730-2002 compared to IEEE Std.730-1998. Terminology used in the US-APWR SPM is in accordance with the definitions of IEEE Std. 610.12-1990, and described in Appendix A.

IEEE Std. 730-1998 requires the SQAP to include the following 15 topics:

· Purpose
Subsection 3.3.1 of the SPM describes the specific purpose and scope of the SQAP.

· Reference documents
Section 5 of the SPM lists the specific documents referenced in the SQAP.

· Management
Subsection 3.3.2 of the SPM describes the organization, tasks and responsibilities for the SQAP.

· Documentation
Section 4 of the SPM describes the output documents of each organization. In order to clearly describe conformance to the IEEE Std. 730-1998, Section 3.3 of the SPM will be revised. Please refer to MHI's response to question No.4 below.

· Standards, practices, conventions, and metrics
Please refer to MHI's response to question No.5 below.

· Reviews and audits
Please refer to MHI's response to question No.6 below.

· Test
Subsection 3.3.5.5 of the SPM declares application software test activities shall cover all functional and performance requirements as described in the SVVP and the STP.

· Problem reporting and corrective action
Subsection 3.3.5.4 of the SPM describes the problem reporting and corrective action methods. In order to describe the specific organizational responsibilities and procedures, Subsection 3.3.5.4 will be revised. Please refer to MHI's response to ~~the~~ question No.9 below.

· Tools, techniques, and methodologies
Subsection 3.3.7 describes the tools and methods that support SQA.

· Code control
Subsection 3.3.5.6 describes that the code and media shall be controlled in accordance with the SCMP (Section 3.11 of the SPM).

· Media control
See above response on the item "Code control".

· Supplier control
Please refer to response to question No.7 below.

· Records collection, maintenance, and retention
Subsection 3.3.6 describes the SQA documents to be retained.

· Training
Subsection 3.3.5.7 describes that training activities shall be planned and conducted as described in the STrngP (Section 3.7 of the SPM).

· Risk management
Subsection 3.3.5.8 describes that risk management methods and tools are described in the SMP (Section 3.1 of the SPM).

3) The QA Department is responsible for preparing and maintaining the SQAP. The second paragraph of item (1) in Subsection 3.3.2 will be revised as follows.

The QA Department is responsible for assuring that the planned software development and V&V activities are appropriately conducted by the organizations responsible for those activities as described in this SPM, in accordance with implementing procedures as described in Section 1 "Organization" of Topical Report PQD-HD-19005 "Quality Assurance Program Description" (Reference 27). In addition, The QA Department is responsible for preparing and maintaining this SQAP.

The following description will be added after the last paragraph of Section 2.1.

Individual plan described in Section 3 is a summary of implementing procedures and should be maintained by the organization responsible of those procedures.

4) Documentation required in Clause 4.4 of IEEE Std. 730-1998 are described or listed in the SPM. The following description will be added as Subsection 3.3.5.9

**3.3.5.9 Documentation**
Section 4 of this SPM lists the output documents created during the development, V&V, use and maintenance of PSMS application software. These documents are to be checked for adequacy through the review and audits described in Subsection 3.3.5.2.

5) Standards are listed in Section 5. Metrics are described in Section 3.3.5.1 of the SPM. Section 3.3.5.1 of the SPM will be revised to include a reference to applicable standards. The following description will be added before the first paragraph of Subsection 3.3.5.1.

Section 5 lists the regulatory guidance and industry standards to be used in this SPM. These standards address the topics of documentation standards, design standards, test standards and software quality assurance products.

6) The SRR, the PDR and the CDR are included in the Design Review described in Section 3.3.5.2 of the SPM. The SVVPR (Software Verification and Validation Plan Review) and the SCMPR (Software Configuration Management Plan Review) are included in the Management Review.

The following description will be added after the first paragraph of item (1) Management Reviews in Subsection 3.3.5.2.

Management reviews described in this section corresponds to the following reviews required to be conducted in accordance with IEEE Std. 730-1998 (Reference 8).
- Software Verification and Validation Plan Review (SVVR)
- Software Configuration Management Plan Review (SCMPR)

The following description will be added after the third paragraph of item (2) Design Reviews in Subsection 3.3.5.2.

Design reviews described in this section corresponds to the following reviews required to be conducted in accordance with IEEE Std. 730-1998 (Reference 8).

- Software Requirements Review (SRR)
- Preliminary Design Review (PDR)
- Critical Design Review (CDR)

7) The following subsection will be added to Section 3.3 to describe the supplier control.

**3.3.9 Supplier Control**
All of the PSMS application software is provided by MHI. There are no other suppliers of PSMS application software. However, the basic software is supplied by MELCO, and the SQAP requirements for the basic software are described in Section 3.3 of the Basic Software Program Manual (Reference 24). MELCO shall be controlled as an approved supplier of safety related items and services, subject to the provisions of 10 CFR 50 Appendix B and 10 CFR 21.

8) "Software hazard" and "anomaly" are defined in IEEE Std. 610.12-1990 as listed in Appendix A of the SPM. The third paragraph of Subsection 3.3.4 will be revised as follows.

QA Audit findings that detect software hazards (anomalies), not already discovered and documented by either the DT or the VVT (including their independent reviewers), are an indication of a potential weakness in the PSMS application software life cycle process or effectiveness of the overall organization, and merit further investigation. For definition of "software hazards" and "anomalies", refer to Appendix A of this SPM.

9) The NCR described in Section 3.3.5.4 of the SPM is recorded and tracked to be resolved properly based on implementing procedures of the SQAP. The following description will be added after the second paragraph of Subsection 3.3.5.4.

The DTM shall analyze and report the cause of such conditions, corrective actions and preventive actions to be taken. The DT shall conduct the prescribed actions. Changes to the PSMS application software shall be controlled in accordance with this SPM. V&V activities shall be initiated in response to changes due to reported problems as described in Section 3.10 of this SPM. The QAM shall independently confirm that the required corrective ~~action~~ and preventive actions have been implemented satisfactorily.

10) An NCR shall be initiated when any application software hazards, problems and issues adverse to quality are identified all software hazards, problems and issues that have the potential to adversely affect safety functions and related performance characteristics listed in item (1) of Subsection 3.3.5.1 shall be regarded as a condition adverse to quality. Subsection 3.3.5.4 will be revised as follows:

Problem reporting and corrective action procedures shall span the entire PSMS application software life cycle described in this SPM. Identified application software hazards, problems and issues that constitute a condition adverse to quality, that have the potential to adversely affect safety functions and related performance characteristics listed in item (1) of Subsection 3.3.5.1, shall immediately result in initiation of a Nonconformance Report as described in Section 15 "Nonconforming, Materials, Parts, or Components" of Topical Report PQD-HD-19005 "Quality Assurance Program Description" (Reference 27)

**Impact on DCD**
There is no impact on the DCD.

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

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

**Impact on PRA**
There is no impact on the PRA.

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

## RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

**11/29/2011**

**US-APWR Design Certification**

**Mitsubishi Heavy Industries**

**Docket No. 52-021**

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

**QUESTION NO. :** 07-14 Branch Technical Position-48

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

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

Section B.3.1.5 of BTP 7-14 and Clause 6.1 of IEEE Std. 1074-1995, as endorsed by RG 1.173, provide an acceptable approach for software installation plans.

1) Software installation in the development/testing environment should have been addressed in Section 3.5 of the SPM. The staff requests MHI to address software installation in the development or test environment per Clause 6.1.1 of IEEE Std. 1074¬1995.

2) Section 3.5.4 of the SPM states "If no software changes occur between the System V&V Test and the Installation Phase, it is acceptable to proceed to Section 3.5.4.4." The staff requests MHI to clarify or explain the statement. How does MHI know that software was not physically altered or changed on the system between these phases? Should there be some process or procedure to verify that the software installed is the desired version?

3) RG 1.173, Regulatory Positions 4.1 (Temporary Work-Around), 4.2 (Installation), and 5 (Tailoring Software) provide clarifications to IEEE Std. 1074-1995 with respect to installation and operation of new or modified safety system software. The staff requests MHI to address these regulatory positions.

**ANSWER:**

(1) The 1st sentence of Section 3.5.4 of the SPM will be revised as follows:

> The necessary steps, methods and tools require for installing the application software in the ~~factory~~ development/test environment prior to Integration and System V&V Tests is described in the Software Integration Plan (SIntP).

(2) The last sentence of Section 3.5.4 of the SPM will be revised as follows:

> If there is no need to change the application software ~~changes occur~~ between the System V&V Test and the Installation Phase, it is acceptable to proceed to Section 3.5.4.4.

(3) RG 1.173, Regulatory Positions 4.1 and 5 are not applicable to the PSMS application software. Temporary changes are not made that would allow continuation of installation activities or tests of the affected parts of the software. Installation and testing of unaffected parts of the software (e.g., other controllers) may continue without requiring any temporary changes. And also there is no tailored software used in the PSMS. Section 3.5.6 of the SPM will be revised as follows:

- Clause 6.1 of IEEE Std 1074-1995 (Reference 6) which is endorsed by RG 1.173 (Reference 22), with following exceptions:
  - Temporary Work-Around of Clause 6.1.1 is not applicable to the PSMS application software because temporary changes are not made that would otherwise allow continuation of installation activities or test of the affected parts of the software.
  - Tailoring software of Clause 6.1.5.2 is not applicable to the PSMS application software because there is no tailored software used in the PSMS application software.

Description for RG 1.173, Regulatory Positions 4.2 will be added after the last paragraph of Section 3.5.4.1.2 of the SPM as follows:

> Installation of new or modified safety system software should only be performed when all functions affected by the software have been declared inoperable according to the plant technical specifications. When software is involved, particularly for distributed software architectures, the determination of affected functions can depend on extremely subtle considerations. As a minimum, all functions performed, in part, by a given software executable should be declared inoperable if the software executable, its configuration, or its operating platform is to be altered; interconnections of all types with other software, hardware, or human elements should also be examined. Before affected functions may be declared operable, the currently approved software, under the SCMP of this SPM, must be installed according to the procedures specified in Section 3.5.4. This ensures that the intended software is installed.

**Impact on DCD**
There is no impact on the DCD.

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

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

**Impact on PRA**
There is no impact on the PRA.

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

## RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

**11/29/2011**

**US-APWR Design Certification**

**Mitsubishi Heavy Industries**

**Docket No. 52-021**

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

---

**QUESTION NO. :** 07-14 Branch Technical Position-50

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

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

Section B.3.1.8 of BTP 7-14 and Clause 6.2 of IEEE Std 1074-1995, as endorsed by RG 1.173, provide an acceptable approach for software operations plans.

1) RG 1.173, Regulatory Positions 4.1, 4.2, and 5 provide clarifications to IEEE Std. 1074-1995 with respect to installation and operation of new or modified safety system software. The staff finds that the SPM has not addressed these positions. The staff requests MHI to address these regulatory positions.

---

**ANSWER:**

(1) As answered in the response to RAI 833-6058 Question 07-14 BTP-48, RG 1.173, Regulatory Positions 4.1 and 5 are not applicable to the PSMS application software. Also, Description for RG 1.173, Regulatory Position 4.2 will be added to Section 3.5.4.1.2 of the SPM.

To relate the NRC's question on the responsibilities and the scope of the SPM which are provided for the SMaintP, Section 3.8.2 and the first paragraph of Section 3.8.5.1 of the SPM will be revised to clearly identified the responsibilities and scope of the SOP as follows;

### 3.8.2 Organization/Responsibilities

(1) Design Team (DT)

The DT is responsible for providing Operation and Maintenance Manuals ~~and submits to customers~~.

~~(2) DT and/or Customers~~

~~The scope of the following responsibility depends on contract terms with customers~~

Problem reporting and corrective actions during the Operations and Maintenance Phase shall be performed in accordance with the Section 3.6 of this SPM.

#### 3.8.5.1 Operations and Maintenance Manual

An Operations and Maintenance manual shall be developed by the DT ~~and provided to customers~~. This manual shall include the following information, as a minimum:

To relate above issues, Section 3.7.1, Section 3.7.2, Section 3.7.3, Section 3.7.4.1.1, the first paragraph of Section 3.7.4.1.2, Section 3.7.5.1 and Section 3.7.5.2 of the SPM will be revised to clearly identify the responsibilities and the scope of the STrngP as follows;

#### 3.7.1 Purpose

The development of quality software products is largely dependent upon knowledgeable and skilled plant personnel for each US-APWR plant. These include MHI technical personnel and management as well as the potential for the ~~customer's~~ plant personnel to be qualified to install, operate and maintain the software. Training is therefore essential for ~~technical~~ plant personnel ~~both for MHI and customer~~. This StrngP provides ~~customer~~ plant personnel training for the MELTAC Platform and the application software of the PSMS.

This STrngP complies with the guidance and standards identified in Section 3.7.6.

#### 3.7.2 Organization/Responsibilities

There are two sets of organizations responsible for being trained and qualified for performing the PSMS application software lifecycle process described in this SPM:

(1) DT and VVT

Training for the Design Team (DT) and the V&V Team (VVT) personnel who are responsible for development, maintenance and V&V activities, such training is the responsibility of the manager of each organization and team as described in Section 2.2 of this SPM~~, and is outside the scope of this STrngP~~.

(2) ~~Customers~~ Plant Personnel

Training for US-APWR plant personnel, including operators, I&C engineers and I&C technicians who are engaged in technical support, operations, and maintenance

activities for the PSMS in the Operation and Maintenance Phase. ~~s~~Specific training procedures for each US-APWR plant, as defined by IEEE Std 1074-1995, are post-development activities and are the responsibility of the ~~customer~~ plant personnel.

~~(3) MHI/MELCO Training Department~~

~~MHI t~~The DT shall provide ~~customer~~ plant personnel training for the application software using the training materials described in Section 3.7.4.1.1. MELCO shall provide ~~customer~~ plant personnel training for the MELTAC Platform as described in Section 3.7.4.1.2.

~~The customer shall develop and maintain training procedures, and shall train and qualify their personnel, including~~ Plant personnel, including operators, I&C engineers and I&C technicians shall be trained in accordance with the training program described in the facility FSAR.

**3.7.3 Measurement**

Training effectiveness shall be measured in accordance with the ~~customer~~ plant personnel training program as described in the facility FSAR.

**3.7.4.1.1 Training for application software**

(1) Develop Training Materials

The DT shall develop and maintain the training materials to be used for training ~~customers~~ plant personnel, and shall contain information for performing technical support and the Operations and Maintenance activities described in the Operations and Maintenance Manual to be delivered to the ~~customer~~ plant personnel as described in the SMaintP (Section 3.6 of this SPM). Training materials shall contain the following information as a minimum:

a. Purpose

b. Learning Objectives

c. PSMS Application Level Content

- Overview of US-APWR Plant
- System Description
- Functional Overview
- Maintenance Methods
- Troubleshooting Methods

d. Suggested Test Questions (against the Learning Objectives)

(2) Train the ~~Customer~~ Trainer for the Plant Personnel

~~MHI shall train customer~~ The trainers for the plant personnel shall be trained by using the Systematic Approach to Training methods developed by the National Academy for Training (INPO), using the materials developed in Step (1), above.

(3) Implement the Training Program

~~Customer~~ The trainers for the plant personnel qualified in accordance with the facility FSAR shall implement the training of ~~customer~~ the plant personnel, including operators, I&C engineers and I&C technicians, in accordance with this STrngP, using the training materials provided in Step (1), above.

**3.7.4.1.2 Training for the MELTAC Platform**

[ ]

**3.7.5.1 Methods and Tools**

Methods and tools used to perform the PSMS application software training shall be defined in accordance with the ~~customer~~ plant personnel training program as described in the facility FSAR.

**3.7.5.2 Training Facilities**

Operator training, qualification and licensing shall be performed in the facilities required and described by the ~~customer~~ plant personnel training program described in the facility FSAR.

**Impact on DCD**
There is no impact on the DCD.

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

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

**Impact on PRA**
There is no impact on the PRA.

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

## RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

**11/29/2011**

**US-APWR Design Certification**

**Mitsubishi Heavy Industries**

**Docket No. 52-021**

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

**QUESTION NO. :** 07-14 Branch Technical Position-52

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

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

BTP 7-14, Section B.3.1.10 provides guidance to evaluate a Software Verification and Validation Plan. BTP 7-14, Section B.3.1.10.1 states that management characteristics of the SVVP should exhibit purpose, organization, oversight, responsibilities, and risks. RG 1.168, Revision 1, endorses IEEE Std. 1012-1998 as providing methods acceptable for meeting the applicable cited regulation.

1) Section 3.10.3 of the SPM states "any V&V process changes that impact this SVVP shall force a revision of this SVVP." The staff requests MHI to address through what mechanism the SVVP is modified.

2) Section 3.10.6.5.2 of the SPM, V&V Task Iterations, states that if any revisions or changes are made to any Design Outputs and/or V&V inputs, the VVTM shall determine which V&V activities and tasks must be performed again. Section B.3.1.12.4 of BTP 7-14 states that "Since modifying software after an error occurs can result in a new error, it is important that the STP require the full set of tests to be run after any modification to the software." The staff requests MHI to address testing coverage (full versus partial) when there are changes to the software.

**ANSWER:**

1) The change of SVVP is performed by VVT according to SCM in section 3.11.2.2 of SPM. The last sentence of the second paragraph of Section 3.10.3 will be revised as follows.

> Any V&V process changes that impact this SVVP shall force a revision of this SVVP in accordance with the SCMP in section 3.11.2.2 of SPM.

2) The testing coverage is determined by the extent of software change, as indicated in Section 3.10.6.3.1.1.1 (2) of SPM.

**Impact on DCD**
There is no impact on the DCD.

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

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

**Impact on PRA**
There is no impact on the PRA.

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

## RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

**11/29/2011**

**US-APWR Design Certification**

**Mitsubishi Heavy Industries**

**Docket No. 52-021**

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

**QUESTION NO. :** 07-14 Branch Technical Position-53

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

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

BTP 7-14, Section B.3.1.11 provides guidance to evaluate the Software Configuration Management Plan. Clause 7.2 of IEEE Std 1074-1995, as endorsed by RG 1.173, provides an acceptable approach to software configuration management.

1) Section 3.11.2.2.1 of the SPM states that only major changes require a CCB meeting, and that for minor changes a CCB meeting is not required. The staff requests MHI to list the types of minor changes, and describe how such minor changes are tracked or controlled if not done through the CCB. In addition, the staff requests MHI to address the minor change process versus the SCR as described in Section 3.11.3.2, Configuration Changes.

2) Section 3.11.3.1.3 of the SPM, Control of Configuration Item, discusses software library. The staff requests MHI to address who (e.g., software librarian) or which group has control of the software library per B.3.1.11.4 of BTP 7-14.

3) Section 3.11.6 of the SPM, SCMP Maintenance, states that the SCMP is the only SCM plan for the US-APWR PSMS application software. However, it does not address which organization has the overall responsibility of maintaining the SCMP. The staff requests MHI to address which organization is responsible overall for maintaining the SCMP.

**ANSWER:**
1)
The fourth paragraph of Section 3.11.2.2.1 will be revised as follows.

~~A CCB meeting is not required for minor changes that do not affect functional or performance requirements or design specifications, or changes to PSMS application software documents that do not affect a software release.~~ The definition of a Minor Change is a change that does not affect functional or performance requirements, or a design modification, or changes to PSMS application documents. Examples of these minor changes are input/output format changes, clarifications, correction of typos, etc. A CCB meeting is not required for minor changes, but minor changes are reviewed and approved by the DT and are a V&V activity. Changes to the PSMS application software are initiated and controlled using an ~~the topics of~~ SCR. This approach is acceptable because these changes (i.e., input/output format changes, clarifications, correction of typos, etc.) are limited by the existing functional requirements. All such changes shall be reviewed and approved as described in the SDP and SQAP (Sections 3.2 and 3.3 of this SPM, respectively), and require independent V&V as described in the SVVP (Section 3.10 of this SPM).

2) The following sentence is added below the second paragraph of Section 3.11.3.1.3.

The DT shall have the control of software libraries. The software libraries shall be stored in a specific, secure, and controlled storage area.

3) Section 3.11.6 will be revised as follows.

This SCMP is the only SCM plan for the US-APWR PSMS application software. The DTM and the DT has the overall responsibility for maintaining the SCMP.

**Impact on DCD**
There is no impact on the DCD.

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

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

**Impact on PRA**
There is no impact on the PRA.

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

## RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

**11/29/2011**

**US-APWR Design Certification**

**Mitsubishi Heavy Industries**

**Docket No. 52-021**

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

---

**QUESTION NO. :** 07-14 Branch Technical Position-54

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

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

BTP 7-14, Section B.3.1.12 provides guidance to evaluate a Software Test Plan. IEEE Std 829-1983, as endorsed by RG 1.170, provides an acceptable method for providing test documentation. IEEE Std. 1008-1987, as endorsed by RG 1.171, provides an acceptable method for satisfying software unit test requirements

1) Section 3.12.2 of the SPM states that the V&V team shall perform all test activities described in the STP and SVVP but did not mention the testing to be completed by the Design Team. Staff requests MHI to address the component or unit testing that the Design Team is involved.

2) Section 3.12.7 of the SPM states that MELTAC engineering tool is used for the test activities described in this STP and SVVP. The staff requests MHI to describe in what kinds of test the engineering tool is used or suited for and to describe limitations of such test tool. Clause 5.3.2 of IEEE Std. 7-4.3.2-2003 states that "the software tool shall be used in a manner such that defecets not detected by the software tool will be detected by V&V activities." The staff also requests MHI to describe test coverage of the automated test tool and tests that must be performed by manual means.

---

**ANSWER:**

1) As described in Section 3.12.1 "Purpose", all tests of the application software are executed as V&V tests. The V&V Team Manager (VVTM) has responsibilities for all test activities described in the SPM. The Design Team Manager (DTM) is not responsible for all test activities.

   The first paragraph of Section 3.12.2 will be revised as follows;

   > The V&V Team (VVT) shall perform all test activities described in this STP and the SVVP (Section 3.10 of this SPM). The V&V Team Manager (VVTM) is responsible for all test activities.

2) The following sentences will be added to Section 3.12.7.

   The MELTAC engineering tool is used in the integration test, the system test, and the acceptance test, in order to establish input conditions (data and Target Application) and to monitor the results of the tests.

   All test case inputs are carried out manually. There is no automatic test function in the MELTAC engineering tool.

**Impact on DCD**
There is no impact on the DCD.

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

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

**Impact on PRA**
There is no impact on the PRA.

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

Enclosure 5

Docket No. 52-021
UAP-HF-11412

Amended Response to Request for Additional Information
for Chapter 7

November 2011

Non-Proprietary Version

# This Enclosure includes following response of RAIs

RAI No. 775-5836 Revision 3, Question No.: 07.08-23

RAI No. 775-5836 Revision 3, Question No.: 07.08-24

## RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

**11/29/2011**

**US-APWR Design Certification**

**Mitsubishi Heavy Industries**

**Docket No. 52-021**

| | |
|---|---|
| **RAI NO.:** | **No.775-5836 Revision 3** |
| **SRP SECTION:** | **07.08 – Diverse Instrumentation and Control Systems** |
| **APPLICATION SECTION:** | **7.8** |
| **DATE OF RAI ISSUE:** | **06/28/2011** |

**QUESTION NO. : 07.08-23**

MHI's D3 Coping Analysis Technical Report, MUAP-07014, Revision 3, section 4.1 under "External Hazards," states the following:
*"In the D3 coping analysis, no external hazards such as earthquakes, fires, or other natural phenomena are assumed to occur concurrent with an event."*

The staff has reviewed MHI's DCD Chapter 19 which shows that the plant risk contribution from external events/hazards may significant compared with that from internal events/hazards. During the May 11-12th public meeting, MHI made a presentation on the subject. Based on the discussion at the meeting, the staff requests MHI to explain how the US-APWR is protected against potential software common cause failures concurrent with risk-significant external event/hazard scenarios. The staff requests MHI to address all risk significant external events/hazards including floods, fires, and earthquakes, or justify why an external event is not applicable.

**ANSWER:**

The US-APWR is protected against potential software common cause failures (CCFs) of digital instrument and control (I&C) systems concurrent with risk-significant internal and external hazards by providing a diverse actuation system (DAS). DAS consists of diverse automatic actuation cabinets (DAACs) and diverse human-system interface panel (DHP).

This response to RAI 07.08-23 discusses the risk significance of DAS failure concurrent with all external events, based on the design change proposed in the response to RAI 07.08-24 (i.e., the design change of DAAC distribution among A, B, C and D-Class 1E electrical room).

DAACs are placed in the A, B, C and D-Class 1E electrical rooms and the DHP is placed in the main control room in the reactor building. These areas are designed to protect impact from various internal and external hazards, such as fire, flooding, seismic and other external events. In addition, the DAACs are located separately in Class 1E electrical rooms, and the redundant configuration of the DAAC ensures that the DAS does not lose its function from a single fire or flood event that occur in the reactor building.

The risk due to internal and external hazards with a concurrent CCF of digital I&C systems are not significant as follows.

- Internal fire

Above additional information on the internal fire PRA will be involved in the PRA Report (MUAP-07030-P) as Attachment-1.

- Internal flooding

Above additional information on the internal flooding PRA will be involved in the PRA Report (MUAP-07030-P) as Attachment-2.

- Seismic

Therefore, to cope with software CCF concurrent with seismic events, MHI will change the seismic category of DAS to Seismic Category I. As a result of this change, The DAS will have sufficient seismic margin against the SSE and the reliability of DAS under seismic events will be enhanced. DCD Tier 2 Section 7.8 and MUAP-07004 will be revised as shown in Attachment-3 and 4.

- Other external hazards

DAS is placed in the reactor building that protects the impact from other external hazards, such as high winds and tornadoes, external flooding, transportation and nearby facility accidents, and other external hazards as described in FSAR Chapter 2, Chapter 3 and Chapter 19.

Therefore, the risk due to external hazards with a concurrent CCF of digital I&C systems is not significant. Detail information of risk assessment is included in the technical report "US-APWR Probabilistic Risk Assessment" MUAP-07030-P.

MHI has revised D3 Coping Analysis Technical Report, MUAP-07014 Revision 4 page 4-1 as follows.

*External hazards*

*In the D3 coping analysis, external hazards such as fire, flooding, seismic and other external hazards are also considered. D3 related equipment is located in reactor building and is designed to protect external hazards. As described in a technical report, "US-APWR Probabilistic Risk Assessment" (MUAP-07030-P), the risk due to external hazards with a concurrent CCF is not significant.*

**Impact on DCD**

DCD Tier 2 Section 7.8 and DCD Tier 1 Subsection 2.5.3 will be revised to incorporate the requested changes. (See Attachment-3 and 6.)

**Impact on R-COLA**

There is no impact on the R-COLA.

**Impact on S-COLA**

There is no impact on the S-COLA.

**Impact on PRA**

There is no impact on the PRA.

**Impact on Technical / Topical Reports**

Impact on the Technical Reports, MUAP-07004, MUAP-07014 and MUAP-07030 is described in above answer. (See Attachment -1, 2 and 4)

## RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

**11/29/2011**

**US-APWR Design Certification**

**Mitsubishi Heavy Industries**

**Docket No. 52-021**

| | |
|---|---|
| **RAI NO.:** | **No.775-5836 Revision 3** |
| **SRP SECTION:** | **07.08 – Diverse Instrumentation and Control Systems** |
| **APPLICATION SECTION:** | **7.8** |
| **DATE OF RAI ISSUE:** | **06/28/2011** |

**QUESTION NO. :** 07.08-24

The US-APWR DAS requires actuation signals from both Diverse Automatic Actuation Cabinet (DAAC) subsystems using a 2-out-of-2 voting logic to initiate actuation of safety-related and non-safety systems required to cope with abnormal plant conditions concurrent with a CCF that disables all functions of the PSMS and PCMS. The DAS uses this 2-out-of-2 logic to prevent spurious actuation of automatic and manual functions due to a single component failure.

Title 10 CFR 50.62(c)(1) states "*Each pressurized water reactor must have equipment from sensor output to final actuation device, that is diverse from the reactor trip system, to automatically initiate the auxiliary (or emergency) feedwater system and initiate a turbine trip under conditions indicative of an ATWS. This equipment must be designed to perform its function in a reliable manner...*"

In Chapter 16 of the US-APWR DCD Revision 3, "Technical Specifications," LCO 3.3.6 states that "*DAS for each function in Table 3.3.6-1 shall be OPERABLE.*" The BASES section of Chapter 16, B 3.3.6, also states that "*DAS is required to be OPERABLE in the MODES specified in Table 3.3.6-1. All functions of the DAS are required to be OPERABLE in MODES 1, 2 and 3 with the pressurizer pressure > P-11.*" This means that when one or more required DAS functions is/are inoperable the applicant would have a completion time of 30 days to restore the required function to OPERABLE status. The loss of any of the functions presented in Table 3.3.6-1 of Chapter 16 makes the DAS system inoperable, including the loss of one of the two DAAC subsystems.

The staff is questioning MHI's approach of using a 2-out-of-2 logic for the DAS cabinets (DAAC) for actuation of the DAS automatic functions. 10 CFR 50.62(c)(1) states that the systems relied upon for ATWS mitigation should be designed to perform their functions in a reliable manner. MHI's US-APWR approach maximizes the protection against spurious trips of the DAS system but the staff does not see the safety benefits in the use of a 2-out-of-2 logic use for the DAS versus that of a traditional 2-out-of-3 logic. The staff requests MHI to justify the use of 2-out-of-2 logic from the reliability and availability perspective as high reliability and availability are expected for a system that provides a vital defense-in-depth for potential common cause failures.

**ANSWER:**

In the current design in DCD Rev.3, the DAS functions are distributed to two diverse automatic

actuation cabinets (DAACs) located in the B and C-Class 1E Electrical Room. To enhance the reliability and availability, the actuation signals from two DAACs are configured with 2-out-of-2 logic and each DAAC has internal redundancy (1-out-of-2 logic). This current DAS configuration has enough reliability and availability for a single failure of DAAC component because no single failure of DAAC component results in failure to actuate or spurious actuation of DAS functions. However, an internal fire/flooding of either of A or B-Class 1E Electrical Room results in the loss of all DAS functions. Based on the discussion at the public meeting held on July 21, 2011, MHI will change the DAAC configuration as shown in Figure 07.08-24 in this response to cope with such an internal fire/flooding.

In this new design, the DAS functions are distributed to four DAACs and each DAAC is located in A, B, C and D-Class 1E Electrical Room such that an internal fire/flooding of either of Class 1E Electrical Room (i.e., one DAAC subsystem failure) does not result in the loss of the DAS functions.

In addition, as answered in the response to RAI 775-5836 Question 07.08-23, the Seismic Category classification of the DAS (DAACs and the DHP cabinet and their components including cabinet power sources) will be changed from Seismic Category II to Seismic Category I. The power sources of the DAS will be also changed from non Class 1E UPSs to Class 1E UPSs designed as Seismic Category I.

MHI will revise the description to DCD Tier 2 Section 7.8, MUAP-07004, MUAP-07030 and DCD Tire 1 Subsection 2.5.3, based on this design change. (See Attachment -3, 4, 5 and 6.)

Figure 07.08-24 System Configuration of DAS

**Impact on DCD**
DCD Tier 2 Section 7.8 and DCD Tier 1 Subsection 2.5.3 will be revised to incorporate the requested changes. (See Attachment-3 and 6.)

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

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

**Impact on PRA**
There is no impact on the PRA.

**Impact on Technical / Topical Reports**

Impact on the Technical Reports, MUAP-07004 and MUAP-07030 is described in above answer. (See Attachment -4 and 5)

## 7.8 Diverse Instrumentation and Control Systems

The DAS is the non-safety diverse instrumentation and control system for US-APWR. The DAS provides monitoring, control and actuation of safety and non-safety systems required to cope with abnormal plant conditions concurrent with a CCF that disables all functions of the PSMS and PCMS. The DAS includes an automatic actuation function, HSI functions located at the diverse HSI panel (DHP), and interfaces with the PSMS and PCMS. The design basis and detailed system description for the DAS are described in the D3 Topical Report ~~MUAP-07006~~ (Reference 7.8-1). Table 7.8-7 shows the supplemental information to Topical Report MUAP-07006-P-A, which is necessary to be clarified. The D~~efense in Depth and Diversity Coping Analysis~~D3, Technical Report ~~MUAP-07014~~ (Reference 7.8-2), demonstrates the ability to maintain all critical safety functions and achieve hot standby using the DAS. DCD_07.01-30 DCD_07.01-30

The DAS design consists of conventional equipment that is totally diverse and independent from the MELTAC platform of the PSMS and PCMS, so that a beyond design basis CCF in these digital systems will not impair the DAS functions. In addition, the DAS includes internal redundancy to prevent spurious actuation of automatic and manual functions due to a single component failure. The DAS is ~~also~~ designed to prevent spurious actuations due to postulated earthquakes and postulated fires. The DAS interfaces with the safety-related process inputs and outputs of the SLS are isolated within these safety-related systems. In addition, hardwired ~~Class 1E~~safety-related logic within the SLS (not affected by a CCF) ensures that control commands originating in the DAS or SLS, which correspond to the desired safety function, always have priority. Therefore, there is no adverse interaction of the DAS with safety functions and no erroneous signals resulting from CCF in the SLS that can prevent the safety function. For a figure of the DAS system architecture, refer to Figure ~~6.0-1 of Topical Report, MUAP-07006~~4.2-6 of MUAP-07004. DCD_07.08-24 DCD_07.01-30 DCD_07.08-24

Within the DAS, manual actuation is provided for systems to maintain all critical safety functions (Refer to Table 7.8-1). For conditions where there is insufficient time for manual operator action, the DAS provides automatic actuation of required plant safety functions needed for accident mitigation. Key parameter indications, diverse audible and visual alarms, and provisions for manual controls are located in a dedicated independent DHP located in the MCR. Conventional hardwired logic hardware and relays for automatic actuation are installed in ~~two~~four diverse automatic actuation cabinets (DAACs), each located in a separate Class 1E electrical room. Each DAAC is powered by a separate ~~non-~~Class 1E UPS. During plant on-line operation, the system can be tested manually without causing component actuation that would disturb plant operations. DCD_07.08-24

### 7.8.1 System Description

The DAS consists of manual HSI functions, which include automatic actuation functions. These functions are located in the DHP and the DAAC, respectively. In addition, the DAS consists of interfacing connections with the PSMS and CRDM motor-generator sets. The DAS receives inputs from qualified analog ~~isolators~~isolation devices located in the RPS or directly from plant components. The DAS provides outputs which interface to the SLS power interface modules via qualified ~~isolators~~isolation devices located in the SLS or directly to plant components. DCD_07.01-30 DCD_07.01-30

Once actuated, either manually or automatically, the DAS signals are latched at the system level. This ensures all DAS functions actuate to completion. The DAS latches can be reset from the defeat switch located on the OC.

The overall DAS architecture is described in Topical Report MUAP-07006 Section 4.0. For manual and automatic system level, actuations from the DAS refer to functional logic diagram Figure 7.2-2 sheet 14.

### 7.8.1.1 Diverse HSI Panel

The DHP, which is located in the MCR, consists of conventional hardwired switches, conventional indicators for key parameters of all critical safety functions, and audible and visual alarms. The DHP installed equipment is used for manual control and actuations credited in the defense in depth and diversity coping analysis. Actuation status of each safety-related system actuated from the DHP can be confirmed by monitoring the safety function process parameters displayed on the DHP. The DHP is powered by a ~~non-~~Class 1E UPS and located in the MCR. ~~Therefore~~Also, the DHP is qualified as Seismic Category ~~II~~I. DCD_07.01-30 DCD_07.08-24 DCD_07.08-23

#### 7.8.1.1.1 Manual Actuation Switches

System level manual actuation is provided on the DHP for all automated functions and for systems required to maintain critical safety functions, which may not be automatically actuated. The following manual actuations are provided from conventional switches on the DHP:

- Reactor trip/turbine trip/MFW isolation: one switch
- EFW actuation: one switch
- ECCS: one switch
- Containment isolation: one switch
- EFW isolation and flow control: four switches (one per SG)
- Control of main steam depressurization valve: four switches (one per SG)
- Control of safety depressurization valve: one switch
- Control of main steam line isolation valve: four switches (one per SG) MIC-03-07-00005

To prevent spurious actuation due to a failure of any of the above switches, a separate manual actuation permissive switch is provided. ~~This is referred to as the "Permissive Switch for DAS HSI."~~ The permissive switch is located in the MCR, but physically separated from the DHP to minimize the affect of fire propagation. The DAS permissive switch is powered by a ~~non-~~Class 1E UPS that is separate from the power to the DHP. Signals from the manual actuation switches and permissive switch are interfaced separately from the MCR to each DAAC; refer to ~~Topical Report~~ MUAP-0700~~6~~4 Section ~~6.0~~4.2.6. To prevent spurious DAS actuation due to the MCR fire, all DAS manual DCD_07.01-30 DCD_07.08-24 DCD_07.08-24

Safety-related sensors selected by the plant design for the DAS input are interfaced from within the PSMS or PCMS input modules. These input modules utilize analog distribution modules and isolation modules that connect the input signals to the DAS prior to any digital processing. Therefore, a software CCF within the PSMS or PCMS does not affect the DAS automation function or the display of plant parameters on the DHP. The MELTAC input module design of the PSMS or PCMS is described in ~~MUAP-07005~~the MELTAC Platform Technical Report (Reference 7.8-4) Section 4.0. DCD_07.01-30 DCD_07.01-30

~~The DAS has two analog logic subsystems, one each located in one of the two DAACs.~~ DCD_07.08-24

Within each DAAC, input signals are compared to their setpoint values and if the monitored value is greater than or less than its setpoint, a partial trip/actuation signal is generated. RT signals and/or ESF actuation signals are generated from each DAAC through voting logic of its input signals. The voting logic (2-out-of-4) for each specific monitored parameter is shown in Table 7.8-4. Table 7.8-6 provides range, accuracy, and setpoint for each diverse actuation variables.

The DAS actuation signals from ~~both~~four DAAC subsystems are configured at their destination using 2-out-of-2 voting logic after taking 1-out-of-2 voting logic twice to execute actuation of RT and ESF systems. DCD_07.08-24 DCD_07.01-30

The monitored signals are isolated from the PSMS and interfaced to the separate subsystems in each DAAC. Process variables monitored for automatic actuation functions are: (a) Pressurizer pressure (4 channels each for low and high-pressure signals), (b) SG water level (4 channels, one per each SG for low level signals).

The numbers of channels required for each automatic actuation function are based on the following considerations:

- No single failure spuriously actuates the DAS.
- ~~Unlimited b~~Bypass of a single channel does not cause the DAS automatic function to be inoperable, prevent decisions regarding credited manual actions or prevent monitoring critical safety functions. DCD_07.01-30

The defeat switch can be manually actuated during plant heatup and cooldown conditions to prevent actuation of the DAS when it is not needed. This is an administratively controlled operating bypass.

The DAS functional logic diagram for automated actuation is included on Figure 7.2-2 sheet 14.

The DAACs are located in separate Class 1E Electrical Rooms. ~~Therefore~~To cope with seismic events, the DAACs are qualified as Seismic Category ~~II~~I. DCD_07.08-24 DCD_07.08-23

#### 7.8.1.2.1 Reactor Trip, Turbine Trip and Main Feedwater Isolation

Reactor trip, turbine trip and MFW isolation are automatically actuated on the following signals:

### 7.8.2 Design Basis Information

#### 7.8.2.1 Single Failure

Since the DAS is a non-safety system, it does not need to meet the single failure criterion for actuation. The DAS subsystems are arranged in a 2-out-of-2 configuration after taking 1-out-of-2 voting logic twice to ensure that the DAS can sustain one random component failure without spurious actuation of either manual or automatic functions. Spurious actuation of single components due to single failures in SLS power interface modules has been considered in the plant safety analysis. DCD_07.08-24

The ~~two~~four DAAC subsystems actuate all required plant components to achieve the required safety function. The number of actuated plant components does not consider additional single failures. For example, for containment isolation valves, only one of the two valves is actuated. This non-redundant configuration is considered in determining the allowable out of service time for plant equipment in the technical specifications. However, the out-of-service condition is considered for the numbers of safety injection pumps and EFW pumps. In addition, unavailable of main steam depressurization valve of the impaired SG line is considered. The DAS actuates all four of these pumps and valves for operability~~,~~ while three is minimum ~~-~~required. ~~-~~The number of actuated components for each DAS function is shown in Table 7.8-5. DCD_07.08-24 MIC-03-07-00001

#### 7.8.2.2 Diversity to Digital Safety and Non-Safety Systems

The DAS utilizes conventional hardware circuits (analog circuits, solid-state logic processing, relay circuits). Therefore, a software CCF in the digital safety-related and non-safety systems (PSMS and PCMS), would not affect the DAS. In addition, the DAS hardware for anticipated transient without scram (ATWS) mitigation functions - Reactor trip, turbine trip, and EFW actuation, is diverse from the RT hardware used in the PSMS. DCD_07.01-30

#### 7.8.2.3 Separation and Independence

The DAS is electrically and physically isolated from the PSMS. Isolation devices (isolation transformers, relays, optical fiber, photo couplers, etc.) are installed in the safety-related system for sharing sensors or transmitting signals between the PSMS and the DAS. These ~~isolators~~isolation devices are part of the safety-related system and are fully qualified. DCD_07.01-30

Isolation devices are installed in the safety-related system for interfacing DAS outputs to power interface module in the SLS. These ~~isolators~~isolation devices are part of the safety-related system and are fully qualified. DCD_07.01-30

#### 7.8.2.4 Testability

The DAS can be tested manually by injecting simulated input signals to confirm its function actuation setpoints, designed logic functions, and required system outputs. Spurious actuation from any one subsystem, during testing, is precluded by the system design of 2-out-of-2 voting logic after taking 1-out-of-2 voting logic twice that must be satisfied to generate an actuation signal. DAS output signals are tested to the inputs of DCD_07.01-30 DCD_07.08-24

the SLS power interface module. This testing overlaps with periodic testing of the SLS, which provides complete testing of all power interface module functions.

### 7.8.2.5 Maintenance Bypass

If an input sensor is failed, the failed sensor signal can be bypassed by a dedicated bypass switch. The switch bypasses only the sensor that has failed. Channel bypass is administratively controlled. Other maintenance bypass functions are not necessary based on the following DAS features:

- The DAS consists of ~~two~~four DAAC subsystems and DAS actuation requires coincident outputs from at least two selected DAAC subsystems satisfying 2-out-of-2 voting logic after taking 1-out-of-2 voting logic twice.~~of both subsystems~~. DCD_07.08-24 DCD_07.08-24
- DAS electrical circuit is designed to actuate when energized. Therefore, loss of power or removal of module does not cause spurious actuation.

### 7.8.2.6 Operating Bypass

The DAS automatic functions can be manually bypassed by the defeat switch, which is a dedicated conventional switch on the OC. The defeat switch is shown in Figure 7.2-2 sheet 14. This switch bypasses ~~both~~four DAAC subsystems. The defeat switch prevents unnecessary automatic DAS actuations due to expected plant conditions during plant startup and shutdown. This operating bypass is reset only by operator action of the above switch. Actuation of the defeat switch is displayed in the MCR on the operational VDU. DCD_07.08-24

Although failure of the defeat switch may result in spurious DAS actuation during startup or shutdown, durations for these plant modes are sufficiently small. Therefore, this failure mode is acceptable.

### 7.8.2.7 Quality

The DAS is a non-safety system designed with augmented quality, as defined by Generic Letter 85-06 (Reference 7.8-5). General requirement of quality assurance and equipment qualification is described in Subsection 7.1.3.20. The following are the ~~key~~additional attributes of the augmented quality program of the DAS: DCD_07.01-27

- Designed specially for nuclear applications using a nuclear quality program that meets the US-APWR QAP descriptions and the guidance in GL 85-06.
- Uses components with a long history of successful operation.
- Uses components that are common in conventional non-digital safety systems.
- Follow a design process that includes independent review by people that were not involved in the original design.

**Table 7.8-7 Supplemental Information to MUAP-07006-P-A (Sheet 5 of 6)**

| No. | Items to be clarified | Corresponding Section of SER for MUAP-07006-A | Resolution | Reference Document and Section | |
|---|---|---|---|---|---|
| 11-4 | Electric power sources for the DAS and the plant components controlled by the DAS | 3.1 GDC 17 | DCD Section 7.8 describes electric power sources for the DAS. Each DAAC is powered by ~~N11 or N12~~Class 1E UPS shown in DCD Fig 8.1-1~~, respectively~~. The DHP is ~~powered only by UPS N11~~also powered by Class 1E UPS. The components actuated by DAS are safety-related, therefore they are powered by safety power source discussed in DCD Section 8.3. The two control rod MG-set motor contactors are self-powered from their respective MG-sets. | DCD Section 7.8 DCD Section 8.1, 8.3 | DCD_07.08-24<br>DCD_07.01-30 |
| 11-5 | Conformance to the requirements in 10 CFR 52.47 Section (a)(1) items iv, vi, and vii. | 3.1 10 CFR 52.47 | The level of design information required by 10 CFR 52.47 is described in the DCD and its references. | DCD and references | |
| 11-6 | Inspections, tests, analyses and acceptance criteria that demonstrate that the DAS has been constructed and will operate in conformity with the Commission's final safety conclusion | 3.1 10 CFR 52.79 | Resolved in DCD ITAAC Table 2.5.3-4. | DCD Tier 1 Table 2.5.3-4 | |
| 11-7 | Specific DAS functions of manual Initiation of Protective Actions | 3.3 RG 1.62 | DCD Subsection 7.8.1.1 describes DAS functions of manual initiation. | DCD Subsection 7.8.1.1 | |
| 11-8 | Specific accident monitoring instrumentation of the DAS | 3.3 RG 1.97 | DCD Subsection 7.8.1.2 describes specific accident monitoring instrumentation of DAS. | DCD Subsection 7.8.1.2 | DCD_07.01-30 |
| 11-9 | Instrument Sensing Lines | 3.3 RG 1.151 | Subsection 7.1.3.7 describes the conformance to RG1.151. The DAS uses the same instruments and instrument sensing lines as the PSMS. | DCD Subsection 7.1.3.7 | |
| 11-10 | Design Acceptance Criteria | 3.4 BTP-16 | BTP-16 has been withheld. There are no design acceptance criteria related to DAS. The ITAAC for DAS are defined in DCD Tier 1 Subsection 2.5.3 | DCD Tier 1 Subsection 2.5.3 | |

The operational VDU and associated processors are not Class 1E. However, they are tested to the same seismic levels as the PSMS. During this testing the operational VDU and associated processors have demonstrated their ability to maintain physical integrity and all functionality during and after an Operating Basis Earthquake and a Safe Shutdown Earthquake.

### 4.2.6 Diverse Actuation System

The non-safety Diverse Actuation System (DAS) provides monitoring and control of safety-related and non-safety plant systems to cope with abnormal plant conditions concurrent with a common cause failure (CCF) that disables all functions of the PSMS and PCMS. This section describes the interfaces of the DAS to the PSMS and PCMS and the HSI functions of the DAS that support plant safety. A more detailed description of the DAS is provided in the Defense-in-Depth and Diversity Topical Report, MUAP-07006.

Safety-related or non-safety sensors selected by the plant design are interfaced from within the PSMS or PCMS input modules. These input modules utilize analog splitters and isolation modules that connected the input signals to the DAS prior to any digital processing. Therefore, a software CCF within the PSMS or PCMS will not affect the DAS function. The input module design is described in the MELTAC Platform Technical Report, MUAP-07005.

Within the DAS manual initiation is provided for all critical functions at the train level (e.g., reactivity level, core heat removal, reactor coolant inventory and containment isolation). Automatic actuation is also provided for functions where time for manual operator action is inadequate.

The DAS has four diverse automatic cabinets (DAACs) and the diverse HSI panel (DHP). The DAS system architecture is shown in Figure 4.2-6. The four DAACs are located in separate Class 1E electrical rooms which are in separate fire or flood zones to cope with internal fire or flood. Failure of one DAAC from internal fire or flood will not affect the DAS automatic functions. In addition, DAS is designed as Seismic Category I to cope with the seismic event concurrent with the software CCF.

The DAS interfaces to non-safety process systems and to redundant trains of safety-related process systems. Since the DAS is a non-safety system it does not need to meet the single failure criteria for actuation. However, the design includes redundant inputs, processing logic and outputs arranged in a 2-out-of-2 configuration after taking 1-out-of-2 voting logic twice to ensure the DAS can sustain one random component failure without spurious actuation of either manual or automatic functions at the system, train or component level.

The Diverse HSI Panel is located within the MCR fire zone. The DAS interface to the PSMS output modules is disabled when the MCR is evacuated using the MCR/RSR Transfer Switches, describe above. This ensures that DAS failures that may result due to MCR fire damage, will not result in spurious actuation of DAS functions and plant components that could interfere with safe shutdown from the RSC. The DAS is not needed when the MCR is evacuated since a plant accident is not postulated concurrent with a MCR evacuation.

The DAS is a non-safety system, therefore it does not need to be tested during plant operation. During plant shutdown, the system can be tested by manually injecting input signals to confirm setpoints, and logic functions and system outputs.

In addition, test functions and indications are built into the system so there is no need to disconnect terminations or use external equipment for test monitoring.

### 4.2.7 Digital Data Communication

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

- The Unit bus provides bi-directional communication between safety-related and non-safety systems for only non-safety functions. The safety-related system and non-safety system are functionally isolated by dedicated communication processors in each safety-related system controller, and priority logic within the safety train that ensure safety-related functions have priority over all non-safety functions. Unit bus uses optical fiber to achieve electrical independence of each train. Physical separation between safety-related and non-safety system is accomplished by locating the safety and non-safety trains in different areas. The Unit bus uses the Control Network digital communication technology described in the Platform Technical Report, MUAP-07005 Section 4.3.2.
- Communications between different trains are one way data link communication between RPS trains, from RPS to ESFAS and safety VDU trains. Functional separation is achieved by communication controllers that are separate from functional processors and voting logic that processes the data from the different trains. Each data link uses optical fiber to achieve electrical independence of each train. Physical separation between safety trains is achieved by locating in different areas. These interfaces are the data link digital data communication technology described in the MELTAC Platform Technical Report, MUAP-07005 Section 4.3.3.
- Bi-directional communications between controllers in one(1) safety train are performed by the Safety Bus. The Safety Bus provides deterministic cyclical data communication. Functional independence is provided by separate communication processors within each controller. Fiber optic cable is provided to enhance EMI susceptibility. The Safety Bus uses the Control Network digital communication technology described in the MELTAC Platform Technical Report, MUAP-07005 Section 4.3.2.
- Bidirectional communication between controllers and their respective I/O modules is provided by the I/O Bus described in the MELTAC Platform Technical Report, MUAP-07005 Section 4.1.
- Bidirectional communication between the PSMS controllers and the MELTAC engineering tool is provided by the Maintenance Network described in the MELTAC Platform Technical Report, MUAP-07005 Section 4.3.4. The PSMS controllers are normally disconnected from the Maintenance Network. Temporary connections are made for equipment trouble shooting and periodic surveillance. Temporary connections are managed by administrative controls and plant technical specifications.

Figure 4.2-5 Overlap Testability for DAS

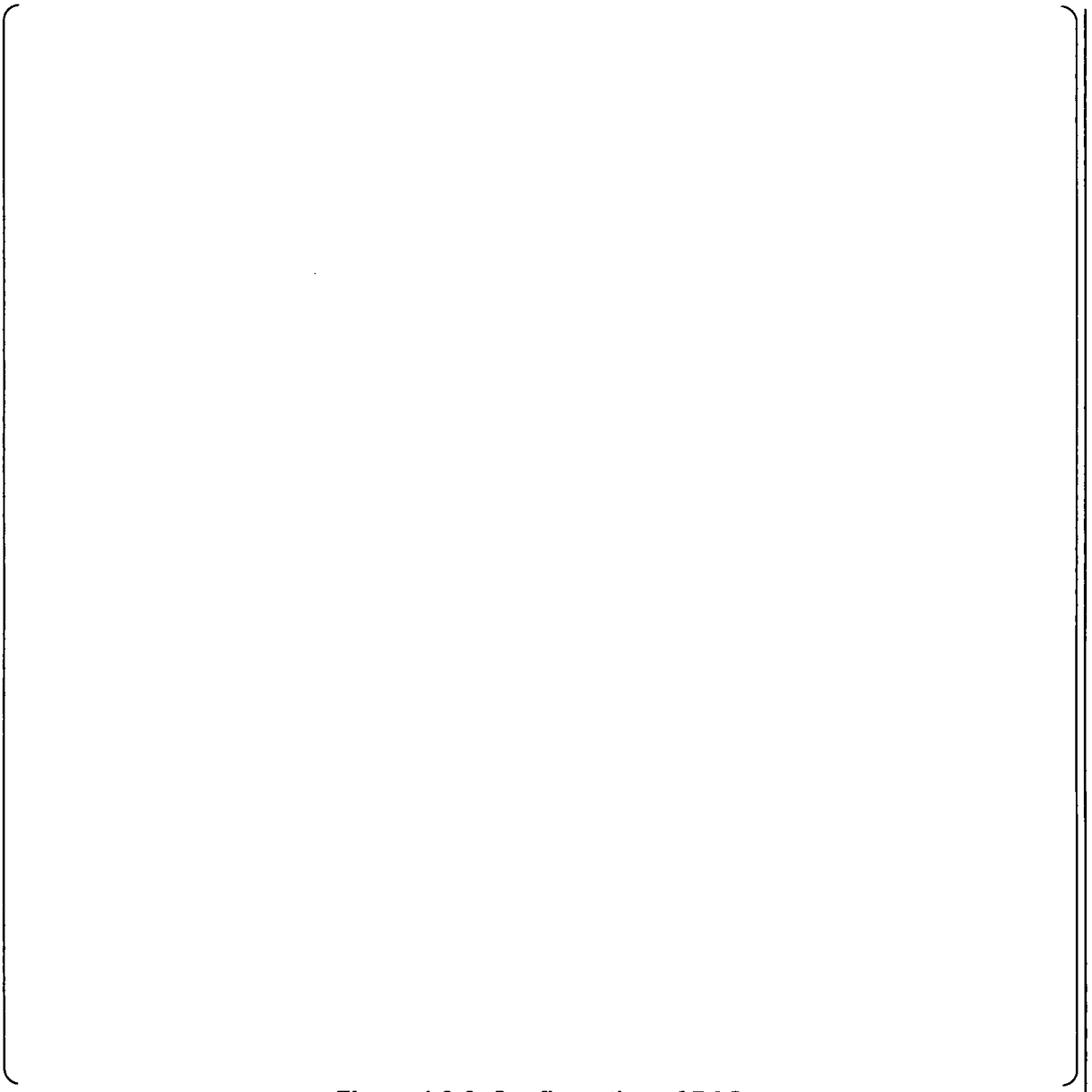


**Figure 4.2-6 Configuration of DAS**

**Figure 5.1-5 State-based Priority in PIF**

EMI qualification analysis also confirms that the characteristics of the EMI environment for the type test bounds the EMI environment of the plant.

### 6.5.8 Fire Protection Analysis

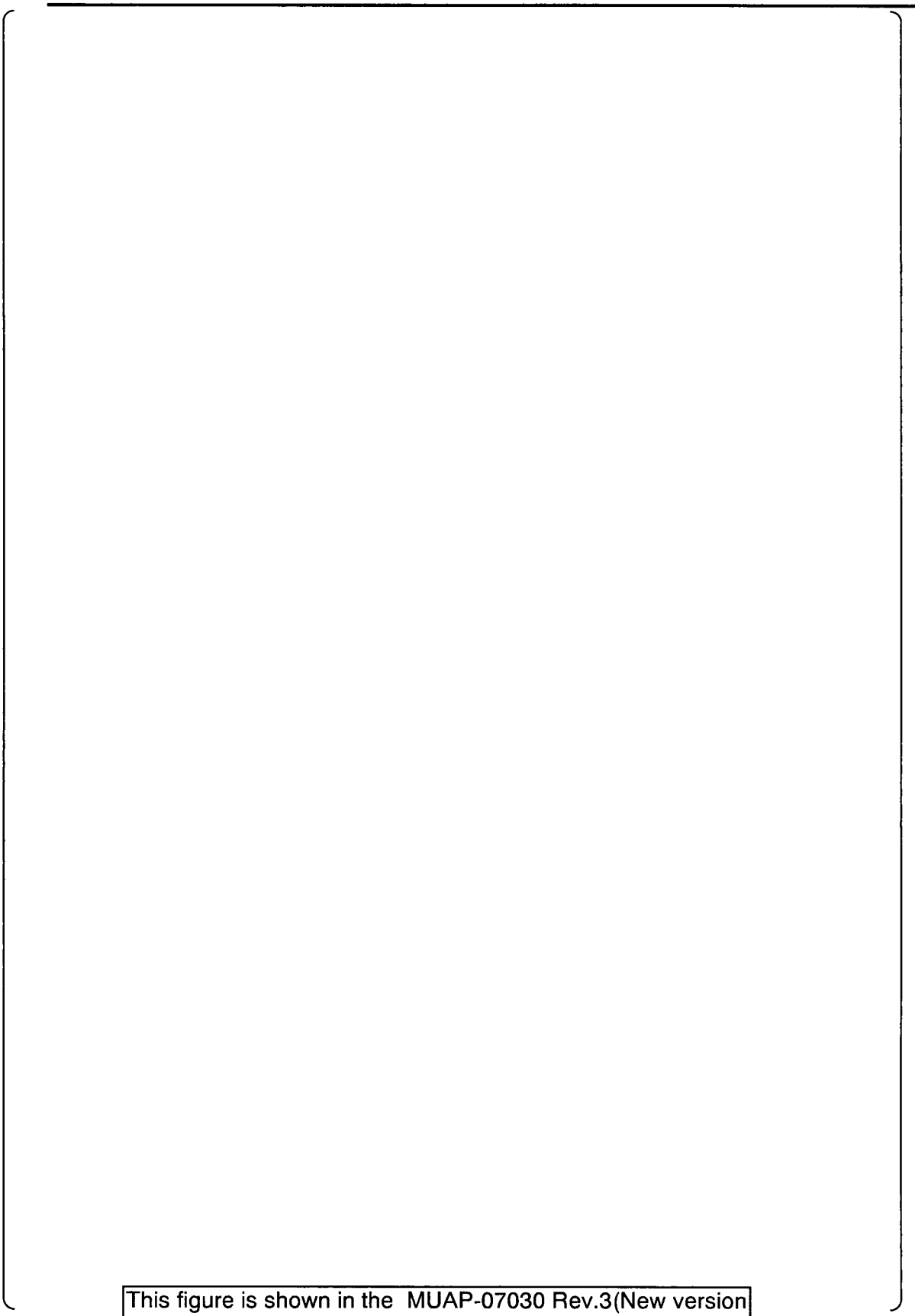
Most components within the PSMS are manufactured from fire retardant materials to minimize the combustible load. The combustible load from the PSMS considered in the fire analysis is estimated based on the total content of flammable materials.

The fire protection analysis demonstrates the ability to achieve safe shutdown with a fire in one fire zone of the plant and the following failures of I&C equipment within that fire zone:

- The failures considered in the fire analysis include short circuits, open circuits and application of worst case credible faults in both common mode and transverse mode.
- The four trains of the PSMS and the PCMS are in five separate fire zones. The fire analysis considers the worst case spurious actuations that can result from the failures identified above for the equipment in the one zone with the fire.
- The MCR and RSC contain only HSI for multiple trains of the PSMS and the PCMS (DAS HSI is discussed below). The HSI is enabled in only one location at a time. A fire occurring in the RSC will have no impact on the plant because the HSI in this location is normally disabled. A fire occurring in the MCR will result in failures (as described above) initially in only one train (safety-related or non-safety), due to physical and electrical separation between trains. The fire will ultimately cause these failures in all trains. However, prior to this the MCR/RSC Transfer Switches will be activated to disable all MCR HSI. Therefore there will be no adverse effects on other trains.
- The DAS HSI is also located in the MCR. This HSI interfaces to all four PSMS trains. The DAS HSI is disabled if the MCR/RSC Transfer Switch is in the RSC position. The DAS HSI contains two circuits (1) permissive circuits and (2) system / component switch circuits. Permissive and switch circuits must both actuate to generate control actions in the PSMS. These two circuits are physically and electrically separated, including a fire barrier. In addition, most components within the DAS are manufactured from fire retardant materials to minimize the combustible load. If a fire starts in one DAS circuit, it will be detected by MCR operators, since the DAS is in a continuously manned location. Therefore, there is sufficient time for activation of the MCR/RSC Transfer Switch so that the DAS interfaces are disabled in the PSMS, before spurious DAS signals, which may be generated due to propagation of the fire, can cause adverse PSMS control actions.
- The automated section of the DAS contains ~~two~~ four subsystems (i.e., DAACs). ~~,~~ The DAS is configured with 2-out-of-2 voting logic after taking 1-out-of-2 voting logic twice ~~which must both actuate~~ to generate ~~any~~ control signals to the PSMS ~~or PCMS~~. These ~~two~~ four subsystems are in separate fire ~~area~~ zone so that a fire in one area may spuriously actuate only one PSMS train.

Figure ~~6.5-4~~4.2-6 shows this fire protection configuration of DAS.
Fire protection and fire protection program are described in DCD Chapter 9.

~~Figure 6.5-4 Configuration of Fire Protection for Diverse Actuation System~~



This figure is shown in the MUAP-07030 Rev.3(New version of Figure 6A.12-2 is shown in the next page).

This figure will be involved in the PRA Report(MUAP-07030-P).

### 2.5.3 Diverse Actuation System

#### 2.5.3.1 Design Description

The DAS is a non-safety system that is diverse from the ~~PSMS software and the digital platform of the PSMS~~PSMS and PCMS digital platform and their software. Therefore, a software or digital platform common cause failure (CCF) in the digital safety and non-safety systems (PSMS and PCMS), would not affect the DAS. The DAS provides monitoring, control and actuation capability of safety and the non-safety systems required to mitigate the AOOs and the PAs, concurrent with a CCF that could disable the functions of the PSMS and the PCMS. DCD_07.08-24

The DAS consists of ~~two~~four subsystems. Each subsystem includes a diverse automatic actuation cabinet (DAAC) located in separate rooms. A diverse HSI panel (DHP) located in the MCR includes HSI components for ~~both DAS~~four DAAC subsystems. A manual actuation permissive switch located in the MCR, but physically separated from the DHP, is required for the manual actuations identified in Tables 2.5.3-2 and 2.5.3-3. DCD_07.08-24 DCD_07.08-24

1.a The functional arrangement of the DAS is as described in the Design Description of Subsection 2.5.3.1 and as shown in Figure 2.5.3-1. Variables monitored by the DAS are as indicated in Table 2.5.3-1.

1.b The DAS is physically separated and electrically independent from the PSMS.

1.c DAS controls are provided in the MCR to manually actuate equipment identified in Table 2.5.3-2, and to manually actuate functions identified in Table 2.5.3-3.

1.d The DAS provides automatic actuation of the equipment and for the functions identified in Tables 2.5.3-2 and 2.5.3-3, respectively, when the monitored variables identified in Table 2.5.3-1 exceed predetermined limits.

1.e The DAS prevents spurious actuation due to single failures or due to a fire or seismic event. Spurious actuations are prevented by the DAS as follows:

- Automatic DAS functions are actuated by ~~two~~four subsystems and DAS actuation needs ~~coincidence of both subsystems~~coincident outputs from at least two selected DAAC subsystems satisfying 2-out-of-2 voting logic after taking 1-out-of-2 voting logic twice. DCD_07.08-24
- The DAS prevents spurious actuation due to a seismic event. Thus the SSE will not result in a DAS failure that adversely affects the PSMS.
- The redundant ~~DAS cabinets~~DAAC subsystems are located in separate fire areas to prevent spurious actuation from a fire in one area. DCD_07.08-24
- Manual DAS functions identified in Tables 2.5.3-2 and 2.5.3-3 require actuation of two switches in the MCR. Separation between the permissive switch and the DHP prevents a fire in one switch location from affecting the other switch location.

2. The DAS has the following capabilities:

- ~~Operates with both DAAC subsystems operable (i.e., in a two-out-of-two configuration), or with one subsystem manually tripped and one subsystem operable.~~ DCD_07.08-24

- The system can be tested manually without causing component actuation.

- Loss of power or removal of a module does not cause spurious DAS actuation.

- Capability to bypass failed sensors functions.

3. The DAS equipment, including input and output interfaces, signal processing and HSI, consists of conventional hardware circuits (analog circuits, solid-state logic processing, relay circuits, switches, indicators).

4. The DAS equipment used for the anticipated transient without scram (ATWS) mitigation (i.e., reactor trip, turbine trip and emergency feedwater actuation) is diverse from the hardware used for the reactor trip function of the PSMS. This design commitment does not apply to measurement instrumentation and signal splitters, which distribute measurement signals to the DAS and the PSMS.

5. Deleted.

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

Table 2.5.3-4 describes the ITAAC for the DAS.

**Table 2.5.3-4 Diverse Actuation System Inspections, Tests, Analyses, and Acceptance Criteria (Sheet 2 of 4)**

| Design Commitment | Inspections, Tests, Analyses | Acceptance Criteria | |
|---|---|---|---|
| 1.d The DAS provides automatic actuation of the equipment and for the functions identified in Tables 2.5.3-2 and 2.5.3-3, respectively, when the monitored variables identified in Table 2.5.3-1 exceed predetermined limits. | 1.d Tests will be performed to verify DAS automatic actuation capability for the as-built equipment listed in Table 2.5.3-2, and to verify the automatic actuation functions in Table 2.5.3-3, using simulated signals. | 1.d The DAS provides automatic actuation of the equipment identified in Table 2.5.3-2, and automatic actuation for the functions identified in Table 2.5.3-3, when the monitored variables identified in Table 2.5.3-1 exceed predetermined limits. | |
| 1.e The DAS prevents spurious actuation due to single failures or due to a fire or seismic event. Spurious actuations are prevented by the DAS as follows:<br>• Automatic DAS functions are actuated by ~~two~~four subsystems and DAS actuation needs ~~coincidence of both subsystems~~coincident outputs from at least two selected DAAC subsystems satisfying 2-out-of-2 voting logic after taking 1-out-of-2 voting logic twice.<br>• The DAS prevents spurious actuation due to a seismic event. Thus the SSE will not result in a DAS failure that adversely affects the PSMS.<br>• The redundant ~~DAS cabinets~~DAAC subsystems are located in separate fire areas to prevent spurious actuation from a fire in one area.<br>• Manual DAS functions identified in Tables 2.5.3-2 and 2.5.3-3 require actuation of two switches in the MCR. Separation between the permissive switch and the DHP prevents a fire from one switch location from affecting the other switch location. | 1.e.i Test and analysis will be performed to verify the as-built DAS prevents spurious actuation due to single failures or due to a seismic event. | 1.e.i A report exists and concludes that the as-built DAS prevents spurious actuation due to single failures or due to a seismic event as follows.<br>• Automatic DAS functions are actuated by ~~two~~four as-built subsystems and DAS actuation needs ~~coincidence of both subsystems~~coincident outputs from at least two selected DAAC subsystems satisfying 2-out-of-2 voting logic after taking 1-out-of-2 voting logic twice.<br>• The as-built ~~DAS~~DAAC subsystems prevents spurious actuation due to a seismic event. | DCD_07.08-24<br>DCD_07.08-24 |

**Table 2.5.3-4 Diverse Actuation System Inspections, Tests, Analyses, and Acceptance Criteria (Sheet 3 of 4)**

| Design Commitment | Inspections, Tests, Analyses | Acceptance Criteria | |
|---|---|---|---|
| | 1.e.ii Test and inspection of the as-built DAS will be performed to verify the existence of a manual permissive switch, to verify the DAS permissive switch is physically located separate from the DHP, and to verify physical separation of redundant DACC cabinets. | 1.e.ii The as-built DAS:<br>• Redundant ~~DAAC cabinets~~DAAC subsystems are located in separate equipment rooms.<br>• Includes a manual permissive switch that prevents spurious manual actuation for those signals with only one manual actuation switch, as identified in Table 2.5.3-3.<br>• The manual permissive switch is physically separated from the DHP to prevent a fire that starts in one switch location from affecting the other switch location. | DCD_07.08-24 |
| 2. The DAS has the following capabilities:<br>• ~~Operates with both DAAC subsystems operable (i.e., in a two out of two configuration), or with one subsystem manually tripped and one subsystem operable.~~<br>• The system can be tested manually without causing component actuation.<br>• Loss of power or removal of a module does not cause spurious DAS actuation.<br>• Capability to bypass failed sensors functions. | 2. Tests of the as-built DAS will be performed. The tests will include tests of the manual controls, loss of power, and module removal, as well as simulated signal inputs to test the system. | 2. A report exists and concludes that the as-built DAS has the following capabilities:<br>• ~~Operates with both as-built DAAC subsystems operable (i.e., in a two out of two configuration), or with one subsystems manually tripped and one subsystems operable.~~<br>• The system can be tested manually without causing component actuation.<br>• Loss of power or removal of a module does not cause spurious DAS actuation.<br>• Capability to bypass failed sensors functions. | DCD_07.08-24 |