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

September 13, 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-11314

Subject: **MHI's Responses to US-APWR DCD RAI for Chapter 7, Response to the Additional Questions from the NRC**

References: 1) "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.

2) "REQUEST FOR ADDITIONAL INFORMATION 698-5490 REVISION 2, SRP Section: 07.01 – Instrumentation and Controls – Introcuction, Application Section: 07.01.03" dated March 7, 2011.

3) "REQUEST FOR ADDITIONAL INFORMATION 710-5493 REVISION 2, SRP Section: 07.09 – Data Communication Systems, Application Section: 07.01, 07.09" dated February 28, 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, and enclosure 4 and 5 are the amended responses to the RAIs contained within Reference 2 and 3.

Enclosure 6 and 7 are the response to additional questions from the NRC on conference calls held from July to September and public meeting held on July 20th and 21st.

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

This letter includes copies of the proprietary version of documents (Enclosures 2, 4 and 6), copies of the non-proprietary version of documents (Enclosures 3, 5 and 7), and the Affidavit of Yoshiki Ogata (Enclosure 1) which identifies the reasons MHI respectfully requests that all materials designated as "Proprietary" in Enclosures 2 and 4 be withheld from public disclosure pursuant to 10 C.F.R. § 2.390 (a)(4).

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.

D081
NRO

Sincerely,

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

Enclosures:

1. Affidavit of Yoshiki Ogata
2. Response to Request for Additional Information for Chapter 7 (Proprietary Version)
3. Response to Request for Additional Information for Chapter 7 (Non-Proprietary Version)
4. Amended Response to Request for Additional Information for Chapter 7 (Proprietary Version)
5. Amended Response to Request for Additional Information for Chapter 7 (Non-Proprietary Version)
6. Response to the Additional Questions from the NRC (Proprietary Version)
7. Response to the Additional Questions from the NRC (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-11314

MITSUBISHI HEAVY INDUSTRIES, LTD.

AFFIDAVIT

I, Yoshiki Ogata, state as follows:

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

2. In accordance with my responsibilities, I have reviewed the enclosed documents 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
   - Response to the Additional Questions from the NRC

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 13th day of September, 2011.

Y. Ogata

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

Enclosure 3

Docket No. 52-021
UAP-HF-11314

Response to Request for Additional Information for Chapter 7

September 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

09/13/2011

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 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 Section 7.8 will be revised to incorporate the requested changes. (See Attachment-3.)

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

09/13/2011

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 Section 7.8, MUAP-07004 and MUAP-07030 based on this design change. (See Attachment -3, 4 and 5.)

Figure 07.08-24 System Configuration of DAS

Impact on DCD
DCD Section 7.8 will be revised to incorporate the requested changes. (See Attachment-3.)

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

~~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.

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

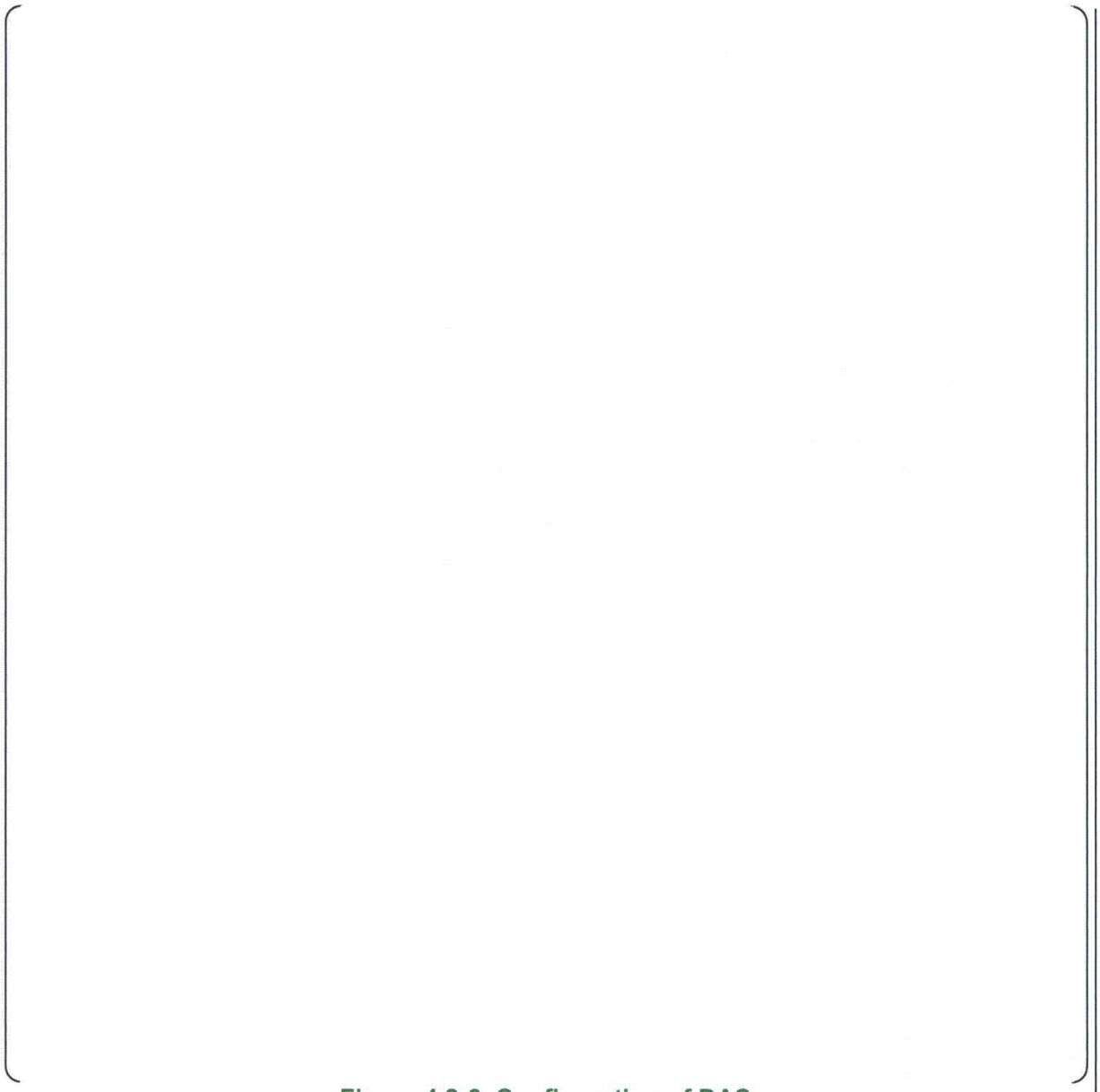


Figure 4.2-6 Configuration of DAS

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.

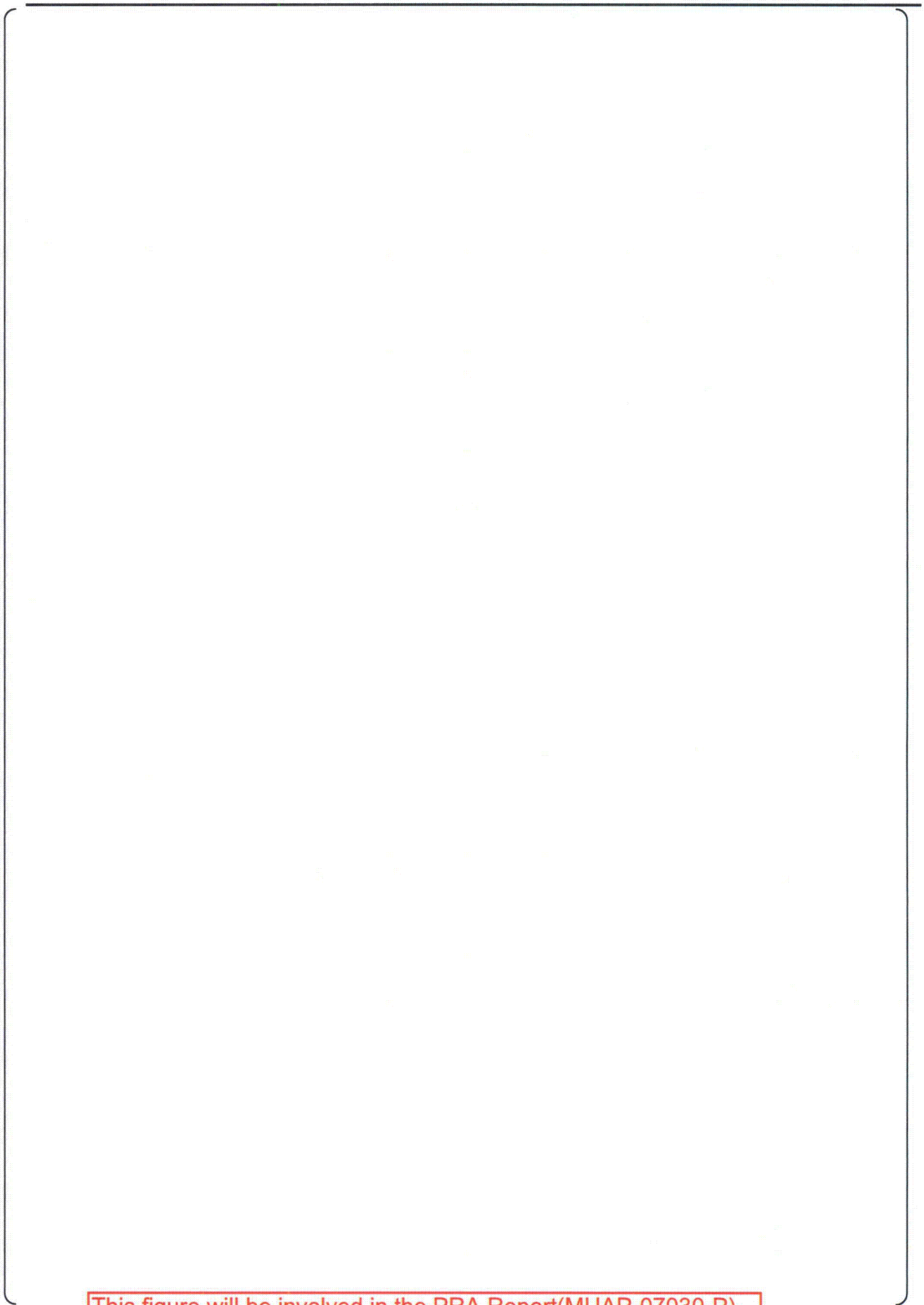
The fire protection analysis demonstrates the ability to achieve safe shutdown with a fire in one fire zone of the plant and the following failures of I&C equipment within that fire zone:

- 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).

Enclosure 5

Docket No. 52-021
UAP-HF-11314

Amended Response to Request for Additional Information
for Chapter 7

September 2011

Non-Proprietary Version

This Enclosure includes following response of RAIs

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

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

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

09/13/2011

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No. 52-021

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

QUESTION NO. : 07.01-26

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

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

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

ANSWER:

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

The self-diagnostic features are also confirmed by manual periodic tests (i.e., CHANNEL CALIBRATION, TADOT, Safety VDU TEST, COT – Digital, ALT – Digital) and continuous on-line tests (CHANNEL CHECK) that are diverse from the self-diagnostic features. These tests confirm the operability of each MELTAC controller in the PSMS, thereby ensuring that failures have not been missed by the self-diagnostic features.

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

As to the CHANNEL CHECK, the operability of the automated non-safety channel check is confirmed by the continuous self-diagnostic features within the PCMS during plant operation, and confirmed manually by the periodic CANNEL CALIBRATION test. The US-APWR is designed for OLM including all I&C equipment. Therefore, most CHANNEL CALIBRATION will be conducted during plant operation, except for transmitters that are inaccessible. However, there is only one CHANNEL CHECK function within the PCMS which is used for all channels. Therefore, a test of that function for any channel confirms its operability for all channels. In addition, the communication of channel data to the CHANNEL CHECK function is the same communication used between the PSMS and PCMS for display of the channels on the PCMS HSI. This communication interface is also continuously self-tested by both the PCMS and PSMS. Therefore, the automatic CHANNEL CHECK meets the guidance of BTP 7-17.

Since the automated non-safety CHANNEL CHECK performs only a monitoring function (ie. there is no control or protective action as a result of the CHANNEL CHECK), there is no potential for adverse safety to non-safety interaction.

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

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

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

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

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

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

The TS periodic manual surveillance tests confirm the functionality of the self-diagnostic features, thereby complying with 10 CFR Part 50 Appendix B, Criterion XII and BTP 7-17.

The calibration equipment which will be used to during CHANNEL CALIBRATION as described in Section 4.2 must also satisfy the requirements of 10 CFR Part 50 Appendix B, Criterion XII,

"Control of Measuring and Test Equipment," which requires in part that measures be established to assure that measuring and testing devices used in activities affecting quality are properly controlled, calibrated, and adjusted at specified periods to maintain accuracy with necessary limits.

The function of the Memory Integrity Check is implemented in the MELTAC engineering tool. MHI requires the augmented quality to the function of the Memory Integrity Check implemented in the MELTAC engineering tool and will perform the qualification control in accordance with Appendix D of the US-APWR Software Program Manual.

As to the CHANNEL CHECK, MHI requires the augmented quality to the function of the automatic CHANNEL CHECK. This function will be performed in the Reactor Control System which has the augmented quality.

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

Impact on Safety I&C Technical Report

MUAP-07004 Rev.6 is revised as follows:

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

The integrity of safety-related function of the PSMS is continuously checked by their self-diagnostic features. The verification of the self-diagnostic features in the PSMS is confirmed through two diverse test methods:

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

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

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

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

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

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

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

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

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

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

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

4.4.1 Manual Testing

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

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

  The Reliability Analysis method, which demonstrates the need to conduct this test no

more frequently than once per 24 months, is described in Section 6.5. However, this test may be conducted more frequently, if required by the reliability of the reactor trip breakers. The test frequency for the reactor trip breakers is described in the US-APWR DCD Chapter 16.

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

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

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

  ( )

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

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

  ( )

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

  There is no test corresponding~~similar to~~ the safety VDU TEST in conventional plants. For the PSMS, this test is credited to confirm the touch response and display operability of the S-VDUs, the interface between the S-VDU and the S-VDU controllers, program

memory processing, communication and display capability of the S-VDU and the S-VDU controllers. This test overlaps with platform self-diagnostic tests as shown in Figure 4.4-4.

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

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

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

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

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

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

- Final Actuation Outputs (TRIP ACTUATION DEVICE OPERATIONAL TEST)

[ ]

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

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

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

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

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

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

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

4.4.2 Manual Calibration (CHANNEL CALIBRATION)

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

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

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

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

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

This manual calibration is equivalent to tests of process measurement devices in conventional plants. For the PSMS, this manual calibration is credited to confirm the process measurement devices, the interface from those devices to the PSMS, input signal processing, program memory processing, communication and display capability of the RPS

or ESFAS (depending on which controller processes the input), This test overlaps with platform self-diagnostic tests and automated CHANNEL CHECK as shown in Figure 4.4-4.

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

MUAP-07004 Rev.8 will be revised as follows:

The second paragraph of Section 4.3 of MUAP-07004 Rev.8 will be revised as follows:

In addition to platform diagnostic features, the redundant system inputs from different trains are continuously compared to detect failed/drifting instrumentation or input modules. This comparison is performed continuously in ~~the Unit Management Computer~~ the Reactor Control System of the PCMS; deviations are alarmed in the MCR. This automatic CHANNEL CHECK is credited to replace manual CHANNEL CHECK in plant technical specification surveillances.

The first paragraph of Section 4.4 of MUAP-07004 Rev.8 will be revised as follows.

The integrity of most safety-related function of the PSMS is continuously checked by ~~their~~ the PSMS self-diagnostic features and CHANNEL CHECK performed by the PCMS. The continuous ~~PSMS~~ self-diagnostic features enhance the reliability of the PSMS and allow ~~elimination~~ extending the surveillance frequency of most manual surveillances required for Technical Specification compliance. In addition, the self-diagnostic features simplify the manual surveillance tests.

Section 4.4.1 of MUAP-07004 Rev.8 will be revised as follows:

This test ensures the integrity of the software credited to execute system safety-related functions, including correct setpoints, constants and logic functions. This test also ensures the integrity of the software credited to execute self-diagnostic functions. The function of the Memory Integrity Check is designed with augmented quality and maintained in accordance with Appendix D of the US-APWR Software Program Manual. The Memory Integrity Check overlaps with platform self-diagnostic tests, automated cross-channel tests and manual tests described above and as shown in Figure 4.4-4.

Impact on DCD

The following has been already added to the end of Subsection 7.1.3.10 of the DCD Revision 3 Tracking Report Rev.0, MHI Ref. UAP-HF-11260.

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

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

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

Impact on PRA
There is no impact on the PRA.

Impact on Technical / Topical Reports
Impact on the Technical Report, MUAP-07004 is described in the above answer.

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

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

09/13/2011

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No. 52-021

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

QUESTION NO. : 07.09-23

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

ANSWER:

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

MHI has removed references to cyber security from DCD Tier 2 Chapter 7 (Subsections 7.1.3.1.7, 7.7.2.10 and 7.9.2.6) in DCD Rev. 3. COL item 7.9 (1) and related descriptions will be deleted as shown in Attachment-1.

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

In addition, all references to cyber security in Technical Reports have removed or the term "cyber security" will be replaced with "secure development and operational environment" to be consistent with DG-1249.

Impact on DCD
A COL item 7.9 (1) and related descriptions will be deleted as shown in Attachment-1.

Impact on R-COLA
Corresponding change to delete a COL item 7.9 (1) will need to be incorporated in the R-COLA.

Impact on S-COLA
Corresponding change to delete a COL item 7.9 (1) will need to be incorporated in the S-COLA.

Impact on PRA
There is no impact on the PRA.

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

In addition, the safety-related controllers within the PSMS include electrical and communication isolation to ensure that the deterministic processing of the safety-related functions can not be affected due to failures or communication errors from the unit bus or maintenance network. ~~Table 7.2-8 and Table 7.3-7~~Appendix G of the Safety I&C Technical Report (Reference 7.9-2) which shows the FMEA for reactor trip and ESF actuation in the PSMS include failure mode and effects of the DCSs. DCD_07.01-30 DCD_07.02-7 DCD_07.02-7

Security-Related Information - Withheld under 10 CFR 2.390 (SRI) DCD_07.01-30 DCD_07.01-30 DCD_07.01-30

7.9.2.6 Cyber Security

The use of computer systems for various functions at nuclear power plants including digital I&C systems increases the potential for threats from cyber intrusions.

~~The COL Applicant is to provide a description of cyber security provisions.~~ DCD_07.09-23

7.9.2.7 Independence

The DCS ensures electrical independence between PSMS ~~divisions~~trains and between the PSMS and PCMS to meet the single failure criterion. Summary descriptions of the independence design are described below.~~In addition, electrical independence is maintained within the PSMS and PCMS, where the communication interfaces cross fire areas of the MCR and RSR.~~ DCD_07.01-30 DCD_07.09-12

Each PSMS and PCMS controller/processor protects itself against DCS errors or failures that could disrupt its internal application functions, thereby ensuring communications independence. For more detailed discussion on the methods used to ensure independence between digital systems in different ~~safety~~ trains and between safety-related and non-safety systems refer to Subsections 7.1.3.4, ~~and~~ 7.1.3.5~~,~~ and 7.1.4 and MUAP-07004 Appendix A.5.6, ~~and~~ Appendix B.5.6 and Appendix F. DCD_07.01-30 DCD_07.09-12

~~All PSMS DCS cables, with the exception of its maintenance networks, are routed in accordance with IEEE Std 384-1992 (Reference 7.9-5) to ensure physical independence of each division. PSMS maintenance network cables, which are non-safety, are routed with other non-safety cables, including PCMS DCS cables.~~

7.9.2.11 EMI/RFI Susceptibility

The PSMS DCS is qualified to the EMI/RFI testing requirements of RG 1.180 (Reference 7.9-7), refer to the ~~MUAP-07005~~MELTAC Platform Technical Report (Reference 7.9-1) Section 5.3. DCD_07.01-30

The PCMS DCS uses the same hardware and software components as the PSMS DCS.

7.9.2.12 Defense-In-Depth and Diversity

There is no credit for continued the DCS operability in the ~~defense-in-depth-and-diversity-coping-analysis~~The D3 Coping Analysis Technical Report (Reference 7.9-18) (i.e., the DCS is assumed to fail due to CCF). The DCS is not used by the conventional analog and hardwired DAS. A discussion on defense in depth and diversity is provided in the D3 Topical Report ~~MUAP-07006~~ (Reference 7.9-8). DCD_07.01-30 DCD_07.01-30

7.9.2.13 Seismic Hazards

All safety-~~related~~ DCS components and hardware are ~~Class 1E~~safety-related qualified and are in an appropriately qualified structure. Where non-safety portions of the DCS interface with the safety-related portions, qualified ~~isolators~~isolation devices are used which preserve the seismic qualifications of the safety-related portions. Refer to the ~~MUAP-07005~~MELTAC Platform Technical Report (Reference 7.9-1) Section 4.1 and 5.2 for the related details. DCD_07.01-30 DCD_07.01-30

The operational VDUs and unit bus are also tested to demonstrate operability after an SSE. In addition, the testing demonstrates that there are no erroneous signals generated that can adversely affect the PSMS or PCMS systems.

7.9.3 Analysis

Detailed compliance to the GDC, IEEE Std 603-1991 (Reference 7.9-9) and IEEE Std 7-4.3.2-2003 (Reference 7.9-10) are described in the~~MUAP-07004~~ Safety I&C Technical Report (Reference 7.9-2) Section 3.0, Appendix A and B. DCD_07.01-30

The FMEA demonstrates that failures in the DCS do not adversely affect the safety-related function of the PSMS or cause erroneous safety-related function actuation, refer to the~~MUAP-07005~~ MELTAC Platform Technical Report (Reference 7.9-1) Section 7.4.

7.9.4 Combined License Information

COL 7.9(1) ~~*The COL Applicant is to provide a description of cyber security provisions.*~~*Deleted* DCD_07.09-23

7.9.5 References

7.9-1 Safety System Digital Platform -MELTAC-, MUAP-07005-P Rev.6 (Proprietary) and MUAP-07005-NP Rev.6 (Non-Proprietary), October 2010.

Enclosure 7

Docket No. 52-021
UAP-HF-11314

Response to Additional Questions from the NRC

September 2011

Non-Proprietary Version

Responses to the Additional Questions from the NRC
(Sheet 1 of 10)

No	Additional Questions from the NRC	Response to the Questions from MHI	Documents to be Revised
1	Feedback on self-Testing and diagnostics credited towards replacement of standard surveillance, issued at the public meeting held on July 20, 2011.	N/A	N/A
1-1	"The safety classification and quality of the hardware and software used to perform periodic testing should be equivalent to that of the tested system." MHI has some aspects of self testing and diagnostics built into the safety system software meet this criteria. Staff finds these safety aspects acceptable.	N/A	N/A
1-2	"The safety classification and quality of the hardware and software used to perform periodic testing should be equivalent to that of the tested system." However, MHI additionally uses non-safety equipment for periodic testing and has not demonstrated this criterion.	See answers to questions 1-3 and 1-4.	N/A
1-3	On software tools, BTP 7-14, Guidance of Software Reviews, states "The SCMP should include a description of the process used to maintain and track purchased items, such as software tools used to make the final product. A qualification procedure should be provided, and a method of tracking tool history, bug lists, and errata sheets should enable the applicant/licensee to track." (MHI's MELTAC technical report) The Memory Integrity Check is proposed to be done with the Engineering Tool on the Safety System CPU modules. Although not clearly identified in Software Program Manual, this tool appears to be a non-safety item with no additional controls or qualifications applied.	The Memory Integrity Check confirms the integrity of all program memory that controls all safety-related functions, including self-diagnostic features. The function of the Memory Integrity Check is implemented in the MELTAC engineering tool. Based on the NRC comment, MHI requires the augmented quality to the function of the Memory Integrity Check implemented in the MELTAC engineering tool and will perform the qualification control in accordance with Appendix D of the US-APWR Software Program Manual. Section 4.4.1 of MUAP-07004 will be revised as follows: This test ensures the integrity of the software credited to execute system safety-related functions, including correct setpoints, constants and logic functions. This test also ensures the integrity of the software credited to execute self-diagnostic functions. The function of the Memory Integrity Check is designed with augmented quality and	MUAP-07004

No	Additional Questions from the NRC	Response to the Questions from MHI	Documents to be Revised
		maintained in accordance with Appendix D of the US-APWR Software Program Manual. The Memory Integrity Check overlaps with platform self-diagnostic tests, automated cross-channel tests and manual tests described above and as shown in Figure 4.4-4.	
1-4	"If automatic test features are credited with performing surveillance test functions, provisions should be made to confirm the execution of the automatic test during plant operation." The automated non-safety CHANNEL CHECK is being proposed to replace the operator implemented CHANNEL CHECK. A means of confirming the execution of this check during operation needs to be identified. CHANNEL CALIBRATION is not done during plant operation, therefore it cannot be used to confirm operation of the automatic test. There is no sufficient information on the docket how or why the CHANNEL CHECK is implemented in the PCMS. (This should be identified in the FMEA, per IEEE Std 352, as a safety to non-safety system interaction)	Readings on instrumentation channels derived from the redundant RPS trains are continuously compared with in the PCMS. In the current design, this comparison is performed by the Unit Management Computer. The operability of the automated non-safety channel check is confirmed by the continuous self-diagnostic features within the PCMS during plant operation, and confirmed manually by the periodic CANNEL CALIBRATION test. The US-APWR is designed for OLM including all I&C equipment. Therefore, most CHANNEL CALIBRATION will be conducted during plant operation, except for transmitters that are inaccessible. However, there is only one CHANNEL CHECK function within the PCMS which is used for all channels. Therefore, a test of that function for any channel confirms its operability for all channels. In addition, the communication of channel data to the CHANNEL CHECK function is the same communication used between the PSMS and PCMS for display of the channels on the PCMS HSI. This communication interface is also continuously self-tested by both the PCMS and PSMS. Therefore, the automatic CHANNEL CHECK meets the guidance of BTP 7-17. Based on the NRC comment on the qualification control of the test equipment, MHI requires the augmented quality to the function of the automatic CHANNEL CHECK. This function will be performed in the Reactor Control System which has the augmented quality Since the automated non-safety CHANNEL CHECK performs only a monitoring function (i.e., there is no control or protective action as a result of the CHANNEL	MUAP-07004

No	Additional Questions from the NRC	Response to the Questions from MHI	Documents to be Revised
		CHECK), there is no potential for adverse safety to non-safety interaction. The second paragraph of Section 4.3 of MUAP-07004 will be revised as follows: In addition to platform diagnostic features, the redundant system inputs from different trains are continuously compared to detect failed/drifting instrumentation or input modules. This comparison is performed continuously in ~~the Unit Management Computer~~ the Reactor Control System of the PCMS; deviations are alarmed in the MCR. This automatic CHANNEL CHECK is credited to replace manual CHANNEL CHECK in plant technical specification surveillances.	
1-5	The staff guidance states that testing of safety system software should be conducted by hardware and software with classification and quality equipment of those of the safety system.	See answers to questions 1-3 and 1-4.	N/A
1-6	Staff guidance presents that the software tools used to develop, test and assist in the V&V of Safety Related Software should be validated and qualified.	Validation and qualification of tools is not required, since manual V&V is conducted for all basic software and all application software.	N/A
1-7	Once the tools and their quality are properly identified, the effectiveness (i.e., reliability) of these software tests vs. others already implemented in the software and the standard surveillances, would have to be presented.	The first paragraph of Section 4.4 of MUAP-07004 will be revised as follows: The integrity of most safety-related function of the PSMS is continuously checked by ~~their~~ the PSMS self-diagnostic features and CHANNEL CHECK performed by the PCMS. The continuous ~~PSMS~~ self-diagnostic features enhance the reliability of the PSMS and allow ~~elimination~~ extending the surveillance frequency of most manual surveillances required for Technical Specification compliance. In addition, the self-diagnostic features simplify the manual surveillance tests.	MUAP-07004

No	Additional Questions from the NRC	Response to the Questions from MHI	Documents to be Revised
1-8	Clarification on Question 1-7 The effectiveness of the Memory Integrity Check vs. the software checks, already being done by the diagnostics in the safety system software, needs to be compared. The amount of overlap of the software faults found and the reliability of the MIC and if it can determine expected changes vs. unexpected changes or errors.	The following table shows the comparison of the Memory Integrity Check (Bit-by-bit check tool) and Self-diagnosis Memory Check. Memory Integrity Check by Bit-by-bit check tool is the function to manually check that intended data is properly written. This function is also used to confirm that the data has not changed unexpectedly. The Self-diagnosis Memory Check is the function to detect memory corruption during operation.	N/A

Memory Integrity Check v.s. Self-diagnosis Memory Check

	Checked by	Process overview	Effectiveness
Memory Integrity Check	Bit-by-bit check tool	Compare data in the Engineering Tool and data in the controller bit by bit.	Any bit corruptions can be detected. This tool can detect unexpected changes, because memory is compared to latest copy of authorized software that resides in the Tool.
Self-diagnosis Memory Check (CRC Check)	Basic software (MELTAC Platform)	Calculate a CRC value at a constant cycle and compare it with a value calculated during controller boot-up	All 1-bit corruptions can be detected. Almost all 2- or more-bit corruptions can be detected. (It is very unlikely that the CRC values match if two or more bits are corrupted.) This function can detect unexpected changes after controller boot-up, because CRC computed by self-diagnosis is compared to the value computed during controller boot-up. However, it cannot detect unexpected changes that exist prior to controller boot-up, since all subsequent CRC values are compared to the boot up value.

Responses to the Additional Questions from the NRC
(Sheet 5 of 10)

No.	Additional Questions from the NRC	Response to the Questions from MHI	Documents to be Revised
2-1	Is there a justification why the DHP on the DAS doesn't use/need all of the parameters which are credited in Chapter 15 Safety Analyses?	Please refer to "Summary for US-APWR Diverse Actuation System (DAS) Functions Selection Basis" (Attachment-1).	N/A
2-2	Why doesn't the DAS use other signals, such as low SG pressure, low RCS flow, high neutron flux, high SG water level, etc., as signals for DAS automatic actuation?		
3-1	JEXU-1015-1009, Rev. 4, P. 5 Section 3.1.3, states "The MELTAC engineering tool enhances the safety function by allowing ongoing monitoring of degrading safety system performance and detailed diagnosis of grouped trouble alarms." Also, Section 3.2.3, P.49, Engineering (Maintenance) Network, analyzes message errors when the Maintenance Network is connected to the controller during controller operation. The staff cannot conclude the MELTAC engineering tool enhances the safety function or sufficient independence is provided between safety systems and other systems when the Maintenance Network is connected to the controller during operation. Therefore MHI is requested to remove the statement and the section identified (any other reference in this document) where the Maintenance Network is permanently connected and discussed. Note that since this technical report is applicable to only US-APWR, connection of the engineering tool via the maintenance network is temporary and should be stated as such.	The following phrases will be removed to clarify that the connection of the engineering tool via the maintenance network is temporary. 1) The Maintenance Network is permanently connected to MELTAC controller 2) "The MELTAC engineering tool enhances the safety function by allowing ongoing monitoring" Section 3.1.1 and 3.2.3 will be revised as shown in the markup of JEXU-1015-1009 (Attachment-2).	MELTAC Platform ISG-04 Conformance Analysis (JEXU-1015-1009)
3-2	Throughout JEXU-1015-1009, Rev. 4, MELTAC Platform ISG-04 Conformance Analysis, there is	The term of "special reprogramming tool" is not appropriate and will be changed to "ROM writing	MELTAC Platform ISG-04 Conformance Analysis

	reference to "special programming tools" used to program the memory device in the CPU Module during design and maintenance activities. MHI is requested to identify these tools in this document and in the Software Program Manual, MUAP-07017. The descriptions should include all their specific functions. Also, the guidelines of BTP 7-14 on controlling, tracking and qualifying should be addressed for these items in the SPM as well.	tool". Section 3.1.10 will be revised as shown in the markup of JEXU-1015-1009 (Attachment-2). The ROM writing tool has been defined in Basic SPM (Section 3.1.4.5) with its applicability of BTP 7-14. The MELTAC Technical Report (MUAP-07005) will be revised to include a reference to the Basic SPM to identify the ROM writing tool as shown in the markup of MUAP-07005 (Attachment-3). As described in Section 3.1.4.5 of Basic SPM, the ROM writing tool itself is not verified, and independent V&V of the binary module written by the tool is performed. Whether basic and application software data are appropriately written to F-ROM of the PSMS controller is confirmed by the bit-by-bit check function of the MELTAC engineering tool. Based on the discussion at the public meeting held on July 20, in order to conform to the guidance of BTP 7-14 and 17, the bit-by-bit check function of the MELTAC engineering tool is developed under augmented quality in accordance with the US-APWR Software Program Manual (MUAP-07017).	(JEXU-1015-1009), MELTAC Technical Report (MUAP-07005)
4	Question D3 Coping Analysis report, MUAP-07014 (R3) [ML11160A115]:		
4-1	a. On Section 3.3, "Diverse Actuation System	The unique prompting alarm for "Diverse	D3 Coping Analysis

	Functions," of MUAP-07014, Revision 3, it has the "Diverse emergency core cooling system actuation" as one of the unique prompting alarms on the DHP to initiate operator action based on Special Event EOPs. i. But on the latest RAI response (ML11160A098/9) for question 07.08-6 (RAI #5325), it states this last bullet as "DAS automatic SI actuation." The RAI response is not consistent with the latest MUAP-07014 revision.	emergency core cooling system actuation" will be deleted in MUAP-07014, Revision 4 because it is no longer necessary.	Technical Report MUAP-07014
4-2	b. On Section 3.4, "Operator Actions," states: "Based on the unique automatic actuation alarms (including first out indication), the operator starts taking actions using the indications and controls on the diverse HSI panel (DHP)." i. But on the latest RAI response (ML11160A098/9) for question 07.08-6 (RAI #5325), it states that MHI would add the words "immediate CCF event specific" to the statement above. Why was this part of MHI's response not included on the latest revision of the D3 Coping Analysis?	The RAI response, Question 07.08-6, will be revised to be consistent with the current description of MUAP-07014, Revision 3, because "immediate action" is no longer applied.	RAI 677-5325 Q07.08-6
4-3	c. On Section 3.5.3, Erroneous Signals, p. 3-11, (5) ECCS Actuation, states: "The DAS low-low pressurizer pressure ECCS automatic actuation is credited to mitigate LOCA events. This automatic actuation is blocked only when the DAS receives signals hardwired directly from the safety injection (SI) pump switchgear (i.e. downstream of the postulated digital CCF)." i. Shouldn't automatic actuation also be blocked at normal pressure and during normal cool down/depressurization activities supporting a plant shutdown? The staff request MHI to elaborate on the description of the block or describe when it is NOT	The description in Section 3.5.3 will be revised in MUAP-07014, Revision 4, to clearly describe on the manual block of the DAS as shown in Attachment-4.	D3 Coping Analysis Technical Report MUAP-07014 See Attachment-4

<table>
<tr><td></td><td>blocked? Is this really the “only” time this automatic actuation is blocked. Similar language of using the word “only” to describe the DAS blocks is used in other sections of MUAP-07014, R3.</td><td></td><td></td></tr>
<tr><td>4-4</td><td>d. Section 5.6.5., pg. 5-41, “The DAS can provide automatic ECCS actuation within at least 128.0 seconds (including time delay from pump starting to full flow).”
i. The staff is asking MHI to clarify the use of a ‘128 seconds’ time delay of DAS automatic actuation for the event analysis? It is not apparent to the staff why the DAS has a designed delay of 120 seconds for this event. (see also DCD Rev 4 mark-up, Table 7.8-6 for the 120 seconds DAS delay on a low-low pressurizer pressure signal)</td><td>To avoid undesirable actuation of DAS despite the functional integrity of PSMS, time delay of ECCS actuation from PSMS is assumed to be 113 sec (without offsite power). This delay time is made up of the followings:

<table><tr><td>Response time of sensor and digital controller</td><td>3.0 sec</td></tr><tr><td>GTG start and load delay time</td><td>100.0 sec</td></tr><tr><td>Sequence time delay and margin</td><td>7.0 sec</td></tr><tr><td>Response time of digital controller and electrical circuit</td><td>3.0 sec</td></tr><tr><td>Total</td><td>113.0 sec</td></tr></table>
If the SI pumps fail to start from PSMS within 120 sec allowing for 7.0 sec margin toward the above 113 sec delay time, DAS starts to actuate the SI pumps as a CCF that disables functions of the PSMS could occur.
In the D3 analysis, 3 sec of response time of DAS and 5 sec of SI pump time to full flow are allowed as time margin and SI pumps are assumed to be started from DAS within 128 sec.

Subsection 7.8.1.2.3 of the US-APWR DCD will be revised as shown in Attachment-5.</td><td>DCD Subsection 7.8.1.2.3

See Attachment-5 (Yellow highlighted)</td></tr>
<tr><td>5</td><td>Question D3 Coping Analysis report, MUAP07014 (R4 draft and RAI responses):</td><td></td><td></td></tr>
<tr><td>5-1</td><td>a. On Section 5.6.5.1 (2) (b), “Large Break</td><td>i. Please refer to MHI’s response to No. 1-4 above.</td><td>DCD Subsection 7.8.1.2.2</td></tr>
</table>

<table>
<tr>
<td></td>
<td>Loss-of-Coolant Accident (LBLOCA)," states: "The DAS ECCS actuation analytical limit reaches at least 10 seconds after the beginning of the break. After that, the DAS can provide automatic ECCS actuation within at least 128.0 seconds (including time delay from pump starting to full flow)."
i. MHI should provide a justification for the reason for having a 128 seconds time delay for DAS automatic actuation for this event. This question was discussed on the public conference call on 06/30/2011 and MHI agreed on providing additional information to the staff to clarify this issue.
ii. In addition, the staff is also asking for clarification on the Low SG Water Level 10/150 seconds time delay for the turbine-driven and motor-driven EFW pumps, respectively, as seen on the draft response to RAI 07.08-17 (RAI#753-5742), on the mark-up of Table 7.8-6. MHI should add this topic to the current action items list or the NRC staff can write an RAI document this request.</td>
<td>ii. For turbine-driven and motor-driven EFW pumps, time delays of their actuation are assumed to be 6 sec and 128 sec (without offsite power), respectively. The followings are the breakdown of these time delays.
<table>
<tr><th></th><th>Turbine-Driven</th><th>Motor-Driven</th></tr>
<tr><td>Response time of sensor and digital controller</td><td>3.0 sec</td><td>3.0 sec</td></tr>
<tr><td>GTG start and load delay time</td><td>N/A</td><td>100.0 sec</td></tr>
<tr><td>Sequence time delay and margin</td><td>N/A</td><td>22.0 sec</td></tr>
<tr><td>Response time of digital controller and electrical circuit</td><td>3.0 sec</td><td>3.0 sec</td></tr>
<tr><td>Total</td><td>6.0 sec</td><td>128.0 sec</td></tr>
</table>
If the turbine-driven EFW pumps fail to start from PSMS within 10 sec allowing for 4.0 sec margin toward the above 6 sec delay time, DAS starts to actuate the turbine-driven EFW pumps as a countermeasure against CCF that disables functions of the PSMS could occur. DAS also starts to actuate the motor-driven EFW pumps after 150 sec time delay allowing for 22 sec margin toward the above 128 sec delay time.

Subsection 7.8.1.2.2 of the US-APWR DCD will be revised as shown in Attachment-5.</td>
<td>See Attachment-5 (Yellow highlighted)</td>
</tr>
</table>

Responses to the Additional Questions from the NRC
(Sheet 10 of 10)

5-2	On changes to Table 7.8-6 as part of the draft response to RAI 07.08-17 (RAI# 753-5742), the NRC staff is asking for clarification on why the "Channel Uncertainty" of the Low SG Water Level instrumentation has been changed from a previous use of a 3% uncertainty span to the use of a 13.2%?	Channel Uncertainty (CU) of the Low SG Water Level in Table 7.8-6 is changed in order to keep consistency with the CU described in Table 6-24 of the Setpoint Methodology Technical Report, MUAP-09022 Rev.2.	-
5-3	In Section 3.5.3 (1) the following statement was added to the descriptions of the signals which states "The diverse actuation signal from DAS is manually defeated in the condition that the pressurizer pressure below the P-11 setpoint." i. The way this statement is written is confusing. It seems as though it is saying that DAS is always manually defeated (blocked) if the pressurizer pressure is below the P-11 setpoint. MHI should clarify this statement.	The description in Section 3.5.3 will be revised in MUAP-07014, Revision 4, to clearly describe on the manual block of the DAS, as shown in Attachment-4.	D3 Coping Analysis Technical Report MUAP-07014 See Attachment-4

Summary for US-APWR Diverse Actuation System (DAS) Functions Selection Basis

August, 2011 by MHI

This paper summarizes selection basis for automatic actuations and indicators in the US-APWR DAS.

Automatic Actuations

The following functions which have less than 10 minutes allowable time for manual actuations are automatically actuated by the US-APWR DAS.

- Emergency Feedwater Actuation
- SI Pump Actuation
- Automatic Reactor Trip, Turbine Trip and Main Feedwater Isolation

The automatic actuations are initiated from the following signals. The automatic Reactor Trip, Turbine Trip and Main Feedwater Isolation is initiated from;

Automatic Actuations	DAS Automatic Actuation Signals
Emergency Feedwater Actuation	low steam generator (SG) water level
SI Pump Actuation	low-low pressurizer pressure
Automatic Reactor Trip, Turbine Trip and Main Feedwater Isolation	low steam generator (SG) water level low pressurizer pressure high pressurizer pressure

The above three automatic reactor trip actuation signals can reasonably cover a wide range of Anticipated Operational Occurrences (AOO) and Postulated Accidents (PA) concurrent with a digital Common Cause Failure (CCF). Table 1 shows possible DAS reactor trip signal for each Ch.15 event.

- low pressurizer pressure for events which result in an increase in heat removal by the secondary system and decrease in reactor coolant inventory
- high pressurizer pressure for events which result in a decrease in heat removal by the secondary system, decrease in reactor coolant system flow rate and reactivity and power distribution anomalies
- low steam generator (SG) water level for events which result in a decrease in

secondary-side system inventory

D3 coping analysis (Best-Estimated) confirms that all events concurrent with a digital CCF which do not reach the above three reactor trip initiation are successfully mitigated.

Table 1: Possible DAS Reactor Trip Signals for Ch.15 Events (Sheet 1of 2)

Section	Event Title	Possible DAS Reactor Trip Signals
15.1	**Increase in Heat Removal by the Secondary System**	
15.1.1	Decrease in Feedwater Temperature as a Result of Feedwater System Malfunctions	Low pressurizer pressure
15.1.2	Increase in Feedwater as a Result of Feedwater System Malfunctions	Low pressurizer pressure
15.1.3	Increase in Steam Flow as Result of Steam Pressure Regulator Malfunction	Low pressurizer pressure
15.1.4	Inadvertent Opening of a Steam Generator Relief or Safety Valve	Low pressurizer pressure
15.1.5	Steam System Piping Failures Inside and Outside of Containment	Low pressurizer pressure Low SG water level
15.2	**Decrease in Heat Removal by the Secondary System**	
15.2.1	Loss of External Load	High pressurizer pressure
15.2.2	Turbine Trip	High pressurizer pressure
15.2.3	Loss of Condenser Vacuum	High pressurizer pressure
15.2.4	Closure of Main Steam Isolation Valve	High pressurizer pressure
15.2.5	Steam Pressure Regulator Failure	High pressurizer pressure
15.2.6	Loss of Non-Emergency AC Power to the Station Auxiliaries	High pressurizer pressure Low SG water level
15.2.7	Loss of Normal Feedwater Flow	High pressurizer pressure Low SG water level
15.2.8	Feedwater System Pipe Break Inside and Outside Containment	High pressurizer pressure Low SG water level
15.3	**Decrease in Reactor Coolant System Flow Rate**	
15.3.1.1	Partial Loss of Forced Reactor Coolant Flow	High pressurizer pressure
15.3.1.2	Complete Loss of Forced Reactor Coolant Flow	High pressurizer pressure
15.3.2	Flow Controller Malfunctions	N/A [NOTE]
15.3.3	Reactor Coolant Pump Rotor Seizure	High pressurizer pressure
15.3.4	Reactor Coolant Pump Shaft Break	High pressurizer pressure

NOTE: The event is only applicable to BWRs and is not applicable to the US-APWR.

Table 1: Possible DAS Reactor Trip Signals for Ch.15 Events (Sheet 2of 2)

15.4	**Reactivity and Power Distribution Anomalies**	
15.4.1	Uncontrolled Control Rod Assembly Withdrawal from a Subcritical or Low Power Startup Condition	High pressurizer pressure
15.4.2	Uncontrolled Control Rod Assembly Withdrawal at Power	High pressurizer pressure
15.4.3	Control Rod Misoperation (System Malfunction or Operator Error)	High pressurizer pressure
15.4.4	Startup of an Inactive Loop or Recirculation Loop at an Incorrect Temperature	N-1 loop operation is not permitted in US-APWR.
15.4.5	Flow Controller Malfunction Causing an Increase in BWR Core Flow Rate	N/A NOTE
15.4.6	Inadvertent Decrease in Boron Concentration in the Reactor Coolant System	High pressurizer pressure
15.4.7	Inadvertent Loading and Operation of a Fuel Assembly in an Improper Position	This event is caused by administrative errors during fuel loading. No transient occurs for this event.
15.4.8	Spectrum of Rod Ejection Accidents	High pressurizer pressure
15.4.9	Spectrum of Rod Drop Accidents in a BWR	N/A NOTE
15.5	**Increase in Reactor Coolant Inventory**	
15.5.1	Inadvertent Operation of Emergency Core Cooling System that Increases Reactor Coolant Inventory	The ECCS can not inject into the RCS at nominal, at-power operating pressure.
15.5.2	Chemical and Volume Control System Malfunction that Increases Reactor Coolant Inventory	High pressurizer pressure
15.6	**Decrease in Reactor Coolant Inventory**	
15.6.1	Inadvertent Opening of a PWR Pressurizer Pressure Relief Valve or a BWR Pressure Relief Valve	Low pressurizer pressure
15.6.2	Radiological Consequences of the Failure of Small Lines Carrying Primary Coolant Outside Containment	Low pressurizer pressure
15.6.3	Radiological Consequences of Steam Generator Tube Failure	Low pressurizer pressure
15.6.4	Radiological Consequences of Main Steam Line Failure Outside Containment (BWR)	N/A NOTE
15.6.5	Loss-of-Coolant Accidents Resulting from Spectrum of Postulated Piping Breaks within the Reactor Coolant Pressure Boundary	Low pressurizer pressure

NOTE: The event is only applicable to BWRs and is not applicable to the US-APWR.

Indicators

The following variables provided on the diverse HSI panel (DHP) (DCD Table 7.8-2) are monitored by analog indicators. This reasonable set of key indicators that provide for critical safety functions is sufficient for supporting all manual control actions based on D3 coping analysis and for achieving and maintaining stable plant conditions. The DHP provides at least a single indicator for each variable below. The indication of variable can be selectable between channels to accommodate a channel that may be failed or in bypass.

Critical Safety Function	Variables	Number of Channel
Reactivity Control	Wide Range Neutron Flux	1
RCS Integrity	Pressurizer Pressure	1
	Reactor Coolant Pressure	1
Core Heat Removal	Reactor Coolant Cold Leg Temperature	1 per Loop
RCS Inventory Control	Pressurizer Water Level	1
Secondary Heat Sink	SG Water Level	1 per SG
	Main Steam Line Pressure	1 per SG
Containment Integrity	Containment Pressure	1

3.1.3. ISG-04 1.3

Requirement
A safety channel should not receive any communication from outside its own safety division unless that communication supports or enhances the performance of the safety function. Receipt of information that does not support or enhance the safety function would involve the performance of functions that are not directly related to the safety function. Safety systems should be as simple as possible. Functions that are not necessary for safety, even if they enhance reliability, should be executed outside the safety system. A safety system designed to perform functions not directly related to the safety function would be more complex than a system that performs the same safety function, but is not designed to perform other functions. The more complex system would increase the likelihood of failures and software errors. Such a complex design, therefore, should be avoided within the safety system.
Analysis

3.1.4. ISG-04 1.4

Requirement
The communication process itself should be carried out by a communications processor separate from the processor that executes the safety function, so that communications errors and malfunctions will not interfere with the execution of the safety function. The communication and function processors should operate asynchronously, sharing information only by means of dual-ported memory or some other shared memory resource that is dedicated exclusively to this exchange of information. The function processor, the communications processor, and the shared memory, along with all supporting circuits and software, are all considered to be safety-related, and must be designed, qualified, fabricated, etc., in accordance with 10 C.F.R. Part 50, Appendix A and B. Access to the shared memory should be controlled in such a manner that the function processor has priority access to the shared memory to complete the safety function in a deterministic manner.

3.1.10. ISG-04 1.10

Requirement
Safety division software should be protected from alteration while the safety division is in operation. On-line changes to safety system software should be prevented by hardwired interlocks or by physical disconnection of maintenance and monitoring equipment. A workstation (e.g. engineer or programmer station) may alter addressable constants, setpoints, parameters, and other settings associated with a safety function only by way of the dual-processor / shared-memory scheme described in this guidance, or when the associated channel is inoperable. Such a workstation should be physically restricted from making changes in more than one division at a time. The restriction should be by means of physical cable disconnect, or by means of keylock switch that either physically opens the data transmission circuit or interrupts the connection by means of hardwired logic. "Hardwired logic" as used here refers to circuitry that physically interrupts the flow of information, such as an electronic AND gate circuit (that does not use software or firmware) with one input controlled by the hardware switch and the other connected to the information source: the information appears at the output of the gate only when the switch is in a position that applies a "TRUE" or "1" at the input to which it is connected. Provisions that rely on software to effect the disconnection are not acceptable. It is noted that software may be used in the safety system or in the workstation to accommodate the effects of the open circuit or for status logging or other purposes.
Analysis

3.2.3. Engineering (Maintenance) Network

The table below analyzes message errors only from the perspective of the safety controller, not the MELTAC engineering tool.

The table is applicable when the controller(s) is connected to the Maintenance Network. ~~The temporary or permanent connection of the controller(s) to the Maintenance Network is application dependent. For applications where the controllers are only temporarily connected,~~ The MELTAC Controller is only temporarily connected to the Maintenance Network. This temporary connection is under administrative controls to ensure that before a controller(s) is connected to the Maintenance Network it is formally taken out of service with appropriate management of affected plant technical specifications.

4.3.2.5.2 Summary of the design feature for the interdivisional communication

This section discusses the summary of the design feature for the interdivisional communication on the Control Network.
The receiving process in the data flow from the O-VDU to the COM will be discussed in this section.
In the Control Network interface, there are design policies and network check methods that provide the necessary means to comply with the requirements of ISG-04 for communication.
[

]

4.3.3.5.2 Summary of the design feature for the interdivisional communication

This section discusses the summary of the design feature for the interdivisional communication on the Data Link.

[

]

(3) Conformance to ISG-04
The conformance of ISG-04 is shown in MELTAC platform ISG-04 Conformance Analysis (JEXU-1015-1009) and Appendix D of this technical report.

3.5.3 Erroneous Signals

Since the DAS includes blocking logic, which prevents DAS actuation if the PSMS actuates correctly, the DAS functions could be blocked by erroneous signals (i.e., signals indicating that the protection system has actuated correctly, when it actually has not). To avoid any potential for erroneous signals that may be generated by the digital CCF, the signals used to block the DAS actuation are obtained from sources that are not affected by the digital CCF, as follows:

(1) Reactor Trip, Turbine Trip and Main Feedwater Isolation

The DAS automatic reactor trip, automatic turbine trip and automatic main feedwater isolation functions are blocked only when the DAS receives signals hardwired directly from the reactor trip ~~switchgear~~ breaker and low turbine emergency oil pressure signals (i.e., down stream of the postulated digital CCF) in the condition that the pressurizer pressure is above the P-11 setpoint. The diverse actuation signal from DAS is manually defeated in the condition that the pressurizer pressure below the P-11 setpoint during normal shutdown operations. These hardwired signals indicate that the required number of circuit breakers and turbine emergency trip oil pressure trip signal have correctly actuated. If either actuation is unsuccessful, the DAS will generate backup reactor trip, backup turbine trip and backup main feedwater isolation signals. For example, if there is a partial CCF in the PSMS that affects only reactor trip, the PSMS will actuate turbine trip and main feedwater isolation, and the DAS will actuate reactor trip. Similarly, if there is a partial CCF in the PSMS that affects only turbine trip, the PSMS will actuate reactor trip and main feedwater isolation, and the DAS will actuate turbine trip.

A partial CCF could also result in failure of the main feedwater isolation function of the PSMS, but may not affect the reactor trip and turbine trip functions of the PSMS. For this scenario, the DAS will receive successful reactor trip and turbine trip feedback, which will result in blocking all three functions, including DAS actuation of main feedwater isolation. To accommodate this partial CCF condition, the main feedwater isolation valves are diversely closed by both the PSMS (by actuating binary pilot solenoids) and PCMS (by actuating modulating electro-pneumatic positioners). Since this failure only affects the main feedwater function of the PSMS (not all functions), the software defect cannot be in the PSMS Basic Software (which is common to all functions). Instead, the software defect must be in PSMS software that is unique to the main feedwater isolation function (i.e., the solenoid component control Application Software, or the portion of the MELTAC Basic Software that executes those unique binary solenoid application functions). Therefore, the PCMS main feedwater isolation function, which controls the valve's modulating positioners, is not adversely affected, because it does not rely on the same Application Software or Basic Software used to actuate binary solenoids, as in the PSMS.

(2) EFW Actuation

The DAS automatic actuation of emergency feedwater is blocked only when the DAS receives signals hardwired directly from the motor driven EFW pump switchgear and the turbine driven EFW pump control valves (i.e., down stream of the postulated digital CCF) in the condition that the pressurizer pressure is above the P-11 setpoint. The diverse actuation signal from DAS is manually defeated in the condition that the pressurizer

pressure below the P-11 setpoint during normal shutdown operations. These hardwired signals indicate that the required number of EFW pumps have correctly actuated. If the PSMS EFW pump actuation is unsuccessful, the DAS will generate backup EFW actuation signals.

It is noted, that there are also valves in the EFW flow lines. Therefore, it could be postulated that the EFW pumps would start as expected, but a partial CCF could prevent opening the valves. However, this failure does not need to be considered, because during normal plant operating conditions, the EFW flow line valves are open. If these valves are closed for any reason, this state can be detected by an indication in MCR. This will prompt correct positioning of these valves to their required normally open position, prior to a Chapter 15 event. Since BTP-19 allows the use of best estimate methods, only normal pre-event plant conditions are considered in the D3 Coping Analysis. It is also noted, that spurious closure of these valves due to CCF, concurrent with a design basis event, does not need to be considered, as discussed in Section 5.5 of MUAP-07006 and Section 4 of DI&C Interim Staff Guidance 02.

(3) Main Steam Line Radiation (N-16) Alarm

The DAS N-16 high radiation alarm is credited to prompt manual action to mitigate the SGTR event. This alarm is blocked only when the DAS receives signals hardwired directly from an output of the PCMS, which generates the PCMS N-16 alarm in the condition that the pressurizer pressure is above the P-11 setpoint. The diverse actuation signal from DAS is manually defeated in the condition that the pressurizer pressure below the P-11 setpoint during normal shutdown operations. These hardwired signals indicate that the required PCMS N16 alarm has correctly actuated. If the PCMS N-16 alarm actuation is unsuccessful due to CCF, the alarm processor will not generate this output and the DAS will generate a backup N-16 alarm.

For the SGTR event, there are no PSMS automated actions credited in the Chapter 15 analysis, and no DAS automated actions credited in the D3 coping analysis. Therefore, if the PCMS correctly generates the N-16 alarm, operators are prompted to take the mitigating actions credited in the Chapter 15 analysis.

(4) High-High Steam Generator Water Level Alarm

The DAS high-high steam generator water level alarm is not credited to prompt diverse manual actions for any event in the D3 coping analysis. The alarm is provided only to support operator tasks after diverse mitigation actions are prompted by other alarms. This alarm is blocked only when the DAS receives signals hardwired directly from the reactor trip ~~switchgear~~ breaker (i.e., down stream of the postulated digital CCF) in the condition that the pressurizer pressure is above the P-11 setpoint. The diverse actuation signal from DAS is manually defeated in the condition that the pressurizer pressure below the P-11 setpoint during normal shutdown operations. These hardwired signals indicate that the required number of circuit breakers have correctly actuated. If the reactor trip actuation is successful, the manual actions credited in the D3 coping analysis are not needed. This is true regardless of any partial CCF conditions that may block other PSMS functions. Therefore, it is appropriate to block the DAS high-high steam generator water level prompting alarm.

(5) Emergency Core Cooling System Actuation

The DAS low-low pressurizer pressure ECCS automatic actuation is credited to mitigate LOCA events. This automatic actuation is blocked only when the DAS receives signals hardwired directly from the safety injection (SI) pump switchgear (i.e., down stream of the postulated digital CCF) in the condition that the pressurizer pressure is above the P-11 setpoint. The diverse actuation signal from DAS is manually defeated in the condition that the pressurizer pressure below the P-11 setpoint during normal shutdown operations. These hardwired signals indicate that the required number of SI pumps have correctly actuated. If the SI pump actuation is unsuccessful, due to a CCF, the DAS actuates ECCS automatically.

It is noted, that there are also valves in the SI flow lines. Therefore, it could be postulated that the SI pumps would start as expected, but a partial CCF could prevent opening the valves. However, this failure mode does not need to be considered, because during normal plant operating conditions, the SI flow line valves are open. If these valves are closed for any reason, this state can be detected by an indication in MCR. This will prompt correct positioning of these valves to their required normally open position, prior to a Chapter 15 event. Since BTP-19 allows the use of best estimate methods, only normal pre-event plant conditions are considered in the D3 coping analysis. It is also noted, that spurious closure of these valves due to CCF, concurrent with a design basis event, does not need to be considered, as discussed in Section 5.5 of MUAP-07006 and Section 4 of DI&C Interim Staff Guidance 02.

3.5.4 Failure to Actuate with False Indications

Conditions that result in failure of a credited PSMS function and erroneous indication that the function did actually actuate are precluded, as follows:

- If actuation and indication rely on a common software block (either directly or indirectly), they will both fail together (i.e., no actuation and no indication).
- If actuation and indication rely on different software blocks, per NUREG 6303 only one block is assumed to fail in the CCF analysis.
    - If the actuation block fails, there is no actuation but correct indication of no actuation. For this condition, the operator will take diverse manual actions.
    - If the indication block fails, there is correct actuation but erroneous indication of no actuation. For this condition, the operator will take diverse manual actions.

Therefore, there is no potential for failure of the PSMS to actuate, with conflicting indications that inhibit operator response. It is also noted that if the PSMS fails to actuate, DAS prompting alarms will be generated as discussed above. Since single failures cannot generate spurious DAS prompting alarms, operators will be trained to respond to DAS prompting alarms, regardless of other control room indications. The DAS alarms will prompt operators to initiate special event EOPs for CCF conditions.

7.8.1.2.2 Emergency Feedwater Actuation

EFW is automatically actuated on a low SG water level signal. 2-out-of-4 voting logic is utilized for the low SG water level signals from each SG.

The interface and configuration of the SG water level signals is as described above.

Diversity from the EFW actuation function in the PSMS is maintained from sensor input up to the power interface module. This automatic DAS EFW function is automatically blocked when status signals are received indicating that the PSMS EFW function has actuated correctly. Correct actuation is indicated when 2-out-of-4 status signals are received from limit switch contacts on the steam inlet valves to the turbine driven EFW pumps and from auxiliary contacts on the motor starters controlling the motor driven EFW pumps, as shown in Figure 7.8-3. For turbine-driven and motor driven EFW pumps, time delays of their actuation by the PSMS are assumed to be 6 sec and 128 sec (without offsite power), respectively. Table 7.8-8 shows the breakdown of the delay time. If the turbine-driven EFW pumps fail to start from PSMS within 10 sec allowing for 4.0 sec margin toward the above 6 sec delay time, DAS starts to actuate the turbine-driven EFW pumps as a countermeasure against CCF that disables functions of the PSMS could occur. DAS also starts to actuate the motor-driven EFW pumps after 150 sec time delay allowing for 22 sec margin toward the above 128 sec delay time. The EFW pump status signals are interfaced from the PSMS, prior to any software processing, to each DAAC, as shown in Figure 7.8-1. MIC-03-07-00008

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. DCD_07.08-16

7.8.1.2.3 ECCS Actuation DCD_07.01-30

ECCS is automatically actuated on a low - low pressurizer pressure signal. 2-out-of-4 voting logic is utilized for the four pressurizer pressure low- low signals. MIC-03-07-00005

The interface and configuration of the pressurizer pressure signals is as described above.

Diversity from the ECCS actuation function in the PSMS is maintained from sensor input up to the power interface module. This automatic DAS ECCS function is automatically blocked when status signals are received indicating that the PSMS ECCS function has actuated correctly. Correct actuation is indicated when 2-out-of-4 status signals are received from auxiliary contacts on the motor starters controlling the Safety Injection (SI) pumps, as shown in Figure 7.8-4. The time delay of ECCS actuation by the PSMS is assumed to be 113 sec (without offsite power). Table 7.8-9 shows the breakdown of the delay time. If the SI pumps fail to start from PSMS within 120 sec allowing for 7.0 sec margin toward the above 113 sec delay time, DAS starts to actuate the SI pumps as a CCF that disables functions of the PSMS could occur. In the D3 analysis, 3 sec of response time of DAS and 5 sec of SI pump time to full flow are allowed as time margin and SI pumps are assumed to be started from DAS within 128 sec. The SI pump status signals are interfaced from the PSMS, prior to any software processing, to each DAAC, as shown in Figure 7.8-1. MIC-03-07-00008

Table 7.8-8 Breakdown of Delay Time for DAS EFW Actuation

MIC-03-07-00008

Delay Factor	Delay Time [sec]	
	Turbine Driven	Motor Driven
Response time of sensor and digital controller	3.0	3.0
GTG start and load delay time	N/A	100.0
Sequence time delay and margin	N/A	22.0
Response time of digital controller and electrical circuit	3.0	3.0
Total	6.0	128.0

Table 7.8-9 Breakdown of Delay Time for DAS ECCS Actuation

MIC-03-07-00008

Delay Factor	Delay Time [sec]
Response time of sensor and digital controller	3.0
GTG start and load delay time	100.0
Sequence time delay and margin	7.0
Response time of digital controller and electrical circuit	3.0
Total	113.0