TABLE OF CONTENTS

SAFETY EVALUATION BY THE OFFICE OF NEW REACTORS

LICENSING TOPICAL REPORT MUAP-07006-P (REVISION 2)

"DEFENSE-IN-DEPTH AND DIVERSITY"

MITSUBISHI HEAVY INDUSTRIES, LTD.

MD 6881

1.0 INTRODUCTION

By letter dated April 10, 2007, Agencywide Documents Access and Management System ADAMS Accession Number ML071080429), Mitsubishi Heavy Industries, Ltd. (MHI) submitted a request for U.S. Nuclear Regulatory Commission (NRC) staff to review Topical Report MUAP-07006, "Defense-in-Depth and Diversity", Revision 0. Specifically, MHI requested NRC staff to review and approve a defense-in-depth and diversity (D3) approach for instrumentation and control (I&C) systems designed for MHI's United States Advanced Pressurized Water Reactor (US-APWR) and the current operating nuclear power plants. In response to the NRC staff's comments raised at a nonpublic (proprietary) meeting on June 12, 2007, MHI submitted Revision 1 (ADAMS number ML072010414) for this topical report on July 3, 2007 (ADAMS number ML072010409). MHI submitted supplements dated April 25, 2008 (ADAMS number ML081200217), and June 2, 2008 (ADAMS number ML081550234), which provided additional information requested by the NRC staff in requests dated March 25, 2008 (ADAMS number ML080790297), and April 2, 2008 (ADAMS number ML080880164), and an additional submittal dated April 22, 2008 (ADAMS number ML081130675).

By letter dated June 20, 2008 (ADAMS number ML081770157), MHI submitted Revision 2 (ADAMS number ML081770168) for this topical report as a result of the responses to requests for additional information (RAI) by the NRC staff.

By letter dated January 2, 2008 (ADAMS number ML073540238), the NRC staff identified their intent to review MHI's approach to D3 delineated in this topical report for the US-APWR I&C systems, which is an integral part of, and referenced in, the US-APWR design certification application. In the letter, the NRC staff stated that the topical report was not accepted for review for current operating nuclear power plants. This is due to the inability to adequately address, in one topical report, the unique aspects of D3 for all operating plants. Therefore, the topical report, and this safety evaluation (SE), is applicable to the US-APWR design certification application only.

This topical report describes MHI's design basis approach to D3 for I&C systems applied to its US-APWR nuclear power plant design. This approach includes design features and processes that minimize the potential for common-cause failures (CCF) in the digital safety systems and a diverse backup system to cope with an Anticipated Operational Occurrence (AOO) or a Postulated Accident (PA) with a concurrent CCF. The MHI D3 approach includes best estimate analysis methods to demonstrate this coping capability. This topical report is intended to provide the D3 generic methodology, not the specific coping analysis for the US-APWR.

Technical Report MUAP-07014, “Defense-In-Depth and Diversity Coping Analysis,” Revision 0, for the US-APWR, which is based on the generic methods described in this topical report, was provided as part of the US-APWR design certification application and addresses the specific coping analysis.

The diverse backup system identified by MHI is the Diverse Actuation System (DAS). The safety system described in this topical report, and the US-APWR design certification application, is referred to as the Protection and Safety Monitoring System (PSMS). The overall architecture of the MHI I&C system, and the PSMS description and design process are described in Topical Report MUAP-07004-P, “Safety I&C System Design and Process,” Revision 1 (Ref. 6.1-1). The non-safety system, the Plant Control and Monitoring System (PCMS), is described in this topical report only to the extent necessary to understand the impact a CCF may have on the PCMS and the effect of that CCF on coping with an AOO or PA.

2.0 REGULATORY EVALUATION

The acceptance criteria used as the basis for the review of MHI’s D3 approach by the staff of the NRC are set forth in NUREG-0800, “Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants,” hereafter referred to as the Standard Review Plan (SRP) (Ref. 6.1-2). This document sets forth a method for compliance with applicable sections of Title 10, Part 50, of the *Code of Federal Regulations* (CFR), “Domestic Licensing of Production and Utilization Facilities,” (Ref. 6.1-3) and 10 CFR Part 52, “Licenses, Certifications, and Approvals for Nuclear Power Plants.” (Ref. 6.1-4).

Chapter 7 of the SRP, “Instrumentation and Controls,” Revision 4, dated June 1997, was the primary section of the SRP used for this review. Revision 5 of Chapter 7 was issued in March 2007. MHI first submitted the topical report for review in April 2007, referencing Revision 4 of Chapter 7 of the SRP. 10 CFR 52.47(a)(9) identifies that applicants are to reference the SRP revision in effect six months prior to docketing the application and the US-APWR design certification application was docketed on March 10, 2008. Since the topical report was submitted a month after the new revision of Chapter 7 was issued, the staff finds it acceptable that MHI referenced Revision 4 of Chapter 7, but the staff performed its review according to Revision 5. The following are the regulatory requirements identified in Chapter 7 of the SRP as being applicable to D3 approaches:

10 CFR 50.55a(a)(1)
10 CFR 50.55a(h)
10 CFR 50.62
Appendix A to 10 CFR Part 50

In particular, the following General Design Criteria (GDC) of 10 CFR Part 50 are applicable:

GDC 1, “Quality Standards and Records”
GDC 13, “Instrumentation and Control”
GDC 19, “Control Room”
GDC 22, “Protection System Independence”
GDC 24, “Separation of Protection and Control Systems”
GDC 29, “Protection Against Anticipated Operational Occurrences”

The following NUREG-Series publications, generic letter (GL), policy paper and interim staff guidance (ISG) provide information, recommendations, and guidance. In addition, they serve as acceptable bases for implementing the above-noted requirements in the D3 approach for I&C systems in nuclear power plant design.

- Specific Sections of SRP, Chapter 7:
  - Section 7.1, Instrumentation and Controls– Introduction
  - Section 7.3, Engineered Safety Features Systems
  - Section 7.8, Diverse Instrumentation & Control Systems
- SRP Branch Technical Position (BTP) Instrumental and Control Branch (HICB)-190, "Guidance for Evaluation of Diversity and Defense-In-Depth in Digital Computer-Based Instrumentation and Control Systems"
- NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems" (Ref. 6.1-5)
- GL 85-06, "Quality Assurance [QA] Guidance for Anticipated Transient Without Scram (ATWS) Equipment that is not Safety-Related" (Ref. 6.1-6)
- SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs" (Ref. 6.1-7)
- DI&C-ISG-02, "Diversity and Defense-in-Depth Issues" (Ref. 6.1-8)
- DI&C-ISG-04, "Highly-Integrated Control Rooms - Communications Issues (HICRc)" (Ref. 6.1-9)

3.0 TECHNICAL EVALUATION

3.1 Design Considerations

The ability to cope with CCFs in the software of the PSMS and PCMS is provided by the DAS. The DAS is designed to provide monitoring of key safety parameters and back-up automatic/ manual actuation of the safety and non-safety components required to mitigate AOOs and PAs should they occur. The design concepts of the DAS are fully described in this topical report. The DAS system architecture is shown in Figure 1 with a brief description provided below.

Figure 1. DAS system architecture [Source: MUAP-07006-P, Rev. 2]

The DAS is classified as a non-safety system that consists of conventional analog and binary digital (discrete) components. The DAS does not control safety-related or non-safety related systems under normal plant conditions; this is performed by the PSMS and the PCMS. The components in the DAS are diverse from the Mitsubishi Electric Total Advanced Controller (MELTAC) Platform, as described in Topical Report MUAP-07005-P, "Safety System Digital Platform – MELTAC," Revision 2 (Ref. 6.1-10), which is used by MHI to implement the fully-digital PSMS and PCMS. Thus, a postulated software CCF that adversely affects the PSMS and PCMS digital systems will not impair the DAS function.

The DAS provides manual system level actuation controls for critical safety functions. Manual actuation is provided for all critical functions at the system level (e.g., reactivity level, core heat removal, reactor coolant inventory, and containment isolation). Where time is insufficient for manual operator action, the DAS provides automatic actuation of the plant safety functions needed for accident mitigation.

The DAS includes internal redundancy (i.e., two redundant cabinets per train, called diverse automatic actuation cabinet (DAAC)) to prevent spurious actuation of automatic and manual functions because of single component failures. Both trains need to provide an actuation signal for the DAS function to occur.

The DAS shares sensor inputs with the PSMS through analog interfaces that are not subject to postulated software CCFs in the PSMS. Specifically, the sensors and their isolation devices are analog technology, which is not susceptible to a software CCF.

Digitization of the sensor signals for the PSMS occurs after the analog signal is split, isolated, and sent to the DAS. Qualification of the isolation devices is to be addressed as part of the US-APWR design certification application. This is Application-Specific Action Item (ASAI) 5-1 (see table 5-1).

The output from each DAS train, now in conventional discrete binary form, is transmitted to the corresponding train in the Safety Logic System (SLS), which is part of the PSMS. The DAS output signal is passed through a discrete binary isolation module prior to entering the SLS. Inside the SLS, the discrete binary DAS output signal enters a Power Interface (PIF) Module. The PIF Modules interface control signals to plant components. This PIF Module is described in more detail in Section 3.4 of this safety evaluation report (SER).

3.1.1 Integrated Reactor Protection System and Engineered Safety Feature Actuation System

Figure 2 illustrates how two diverse sensor values are provided to the processors in each of the four PSMS divisions (one sensor value to the processor in Group 1, the other sensor signal to the processor in Group 2 within the same division). Analog sensor values are transmitted through an isolator to the DAS; the same sensor signals are then digitized and transmitted to the PSMS.

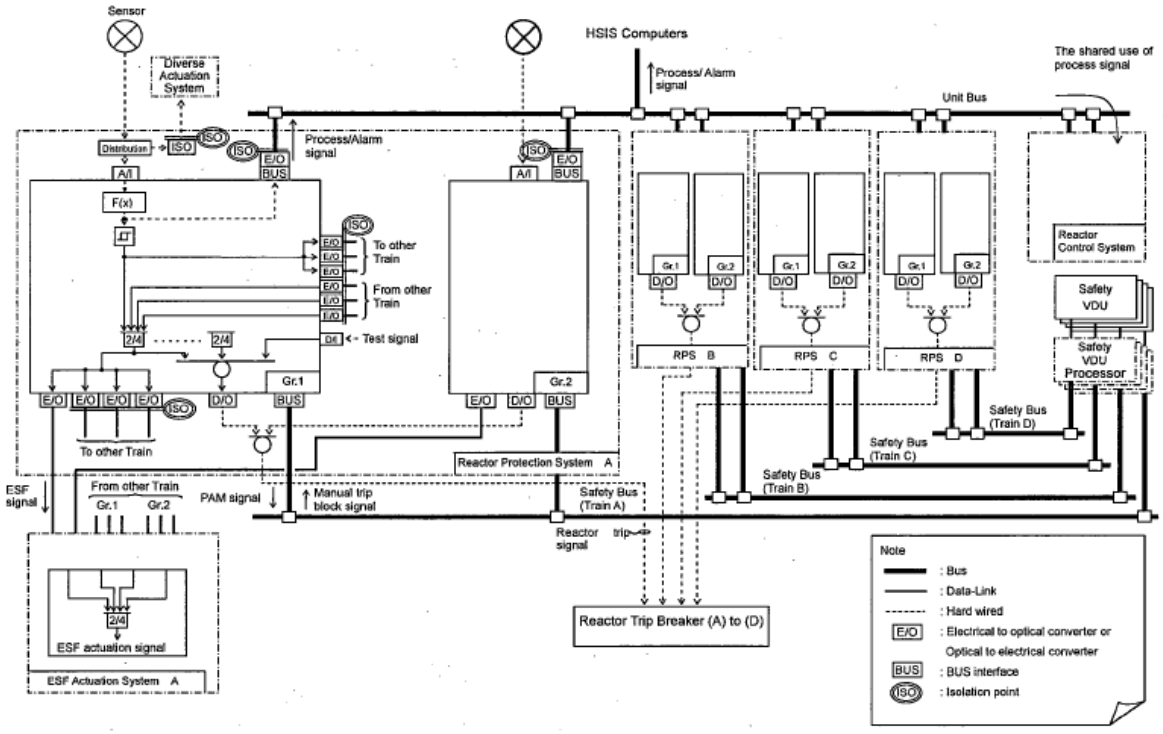

Figure 2. RPS and ESFAS interface [Source: MUAP-07004-P, Rev. 2]

Sensor signals common to reactor trip and/or engineered safety feature actuation system (ESFAS) are transmitted to the reactor protection system (RPS) of the PSMS. The sensor signals are processed through setpoint comparison function blocks (bistables). There are separate bistables for each reactor trip and engineered safety feature (ESF) when there are differences in setpoint values. Bistable outputs from each train of the PSMS are combined using a 2-out-of-4 voting logic scheme. The voting logic outputs for a reactor trip are interfaced to the reactor trip breakers. The voting logic outputs for ESF actuation are transmitted to the ESFAS section of the PSMS.

Each ESFAS train processes the signals from all four respective trains in the PSMS divisions with 2-out-of-4 voting logic for the ESF actuation. Further description of the PSMS architecture is provided in Topical Report MUAP-07004-P, "Safety I&C System Description and Design Process," Revision 1.

3.1.2 Echelons of defense

SRP HICB-19 lists the four echelons of defense against CCFs as:

- Control System − the control system echelon consists of non-safety equipment that routinely prevents reactor excursions toward unsafe regimes of operation and is used in the normal operation of the reactor.

- Reactor Trip System (RTS) – the RTS echelon consists of safety equipment designed to reduce reactivity rapidly in response to an uncontrolled excursion.

- Engineered Safety Features Actuation System − the ESFAS echelon consists of safety equipment that removes heat or otherwise assists in maintaining the integrity of the three physical barriers to radioactive release (cladding, vessel, and containment).

- Monitoring and Indicators − The monitoring and indicators echelon consists of sensors, displays, data communication systems, and manual controls required for operators to respond to reactor events.

Interim staff guidance DI&C-ISG-02 notes that the four echelons of defense described in SRP BTP 7-19 are only conceptual and do not imply that these echelons of defense must be independent or diverse. Rather, where a postulated CCF impairs a safety function, a plant response in accordance with Section 3, Acceptance Criteria, of SRP BTP 7-19 should be demonstrated, regardless of the echelons of defense that may be affected. The ISG further states that the RTS and ESFAS functions may be combined into a single digital platform if the criteria of Staff Positions 1 and 2 of the ISG [adequate diversity and manual operator actions, respectively] are addressed.

The four echelons of defense proposed by MHI in this topical report are the (1) Human System Interface System, (2) PSMS, (3) PCMS, and (4) DAS. As indicated in response to RAI-03 (Ref. 6.1-11), MHI stated that it does not consider the RPS and ESFAS as separate echelons of defense, but rather complimentary integrated echelons of defense. This is because the safety analysis does not credit these functions independently. Where the ESFAS is credited, it is

always credited in conjunction with the RPS. The ESFAS alone does not provide adequate plant protection for any event. Since the ESFAS alone does not provide an echelon of defense, combining the RPS and ESFAS into an integrated system is acceptable to the staff so long as the issues of adequate diversity and manual operator actions are adequately addressed in the plant licensing documentation.

3.1.3 Manual Operator Actions

With respect to manual operator actions, DI&C-ISG-02 states that manual operator actions may be credited for responding to events in which the protective action subject to a CCF is not required for at least the first 30 minutes. The basis to limit dependence on the operator as the independent and diverse backup for automatic RPS actions that are required to be performed in less than 30 minutes following a CCF event provides three main advantages:

1. The operators are provided sufficient time to evaluate a potentially hazardous situation;

2. The design process is improved; and

3. The safety review is simplified.

In the US-APWR, various safety systems are required to operate at different times for different AOOs and PAs. Operator actions may be required within 30 minutes for some events such as feedwater line break and small break loss-of-coolant accidents. Section 8.2 of the topical report states that operator action time to mitigate the event is measured from the time the prompting DAS alarm is provided. The target minimum operator action time is 10 minutes. If action is needed earlier than 10 minutes, the function is generally automated [emphasis added]. Any operator actions credited prior to 30 minutes are justified based on human factors engineering (HFE) evaluation. Justification includes assessments of available information, the decision making process, and expected steps leading to the credited action. In response to RAI-30 (Ref. 6.1-11), MHI states that for those events where manual operator actions are required, the DAS provides sufficient independent information and controls to allow operators to provide the necessary protective action. All time critical manual actions required in the main control room (MCR), or outside the MCR, are supported by a thermal hydraulic analysis which defines the time available for the operator action and an HFE analysis which defines the time required for taking action. Sufficient margin is demonstrated between time available and time required to ensure the feasibility of the manual action with high confidence. When emergency operating procedures have been developed and a simulator is available, the ability to take these manual operator actions will be validated. During plant operation, on-going operator training and human performance monitoring will support the required actions times. For a large-break loss-of-coolant accident (LBLOCA), manual operator action is credited to achieve safe shutdown of the plant based on early indications of the leak detection function. The LBLOCA and leak detection function is discussed in Section 3.3 of this report.

The staff reviewed the information provided in the topical report for manual operator actions in case of a CCF of the PSMS. The staff understands that MHI is proposing a manual operation action strategy that differs from the guidance in DI&C-ISG-02. Specifically, DI&C-ISG-02 states that manual actions may be credited for actions that do not need to be performed within the first 30 minutes of an event. However, MHI proposes manual actions for actions that do not need to

be performed within the first 10 minutes of an event. The staff did not have sufficient information in order to assess the concept of manual actions after the first 10 minutes of an event. Therefore, within the scope of this topical report, the staff does not approve the concept of manual actions in less than 30 minutes. The scope of the topical report and MHI's response to RAI-30 demonstrate that all justification for manual operator actions will be provided in the US-APWR design certification documentation. Particularly, the acceptability of methods and analysis used to determine reliance on manual operator actions, including those actions within 30 minutes, is to be provided from the staff's review of the US-APWR design certification application and Topical Report, MUAP-07007-P, "HSI [Human Systems Interface] System Design Description and HFE [Human Factors Engineering] Process."

Also, the staff will use guidance in a forthcoming ISG on "Crediting Manual Operator Actions for Diverse Actuation of Safety System" in making its safety determination. This is ASAI 5-2.

3.1.4 Anticipated Transient Without Scram (ATWS)

The MHI design strategy for coping with CCFs in the software of the PSMS and PCMS involves the use of the DAS to provide monitoring of key safety parameters and back-up automatic/manual actuation of the safety and non-safety components required to mitigate anticipated operational occurrences and accidents. The US-APWR design also addresses the requirements of 10 CFR 50.62, "Requirements for reduction of risk from anticipated transients with out scram (ATWS) events for light-water-cooled nuclear power plants," using the DAS. Appendix B of the topical report addresses conformance to 10 CFR 50.62.

10 CFR 50.62 provides the requirements for ATWS mitigation systems. Specifically, 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 and be independent (from sensor output to the final actuation device) from the existing reactor trip system.

The analog sensor signals required for the DAS function are interfaced (via isolation devices) prior to digital processing in the PSMS. The output signals from the DAS are interfaced directly to plant components (for reactor trip) or to plant components via the PIF Modules (for turbine trip and emergency feedwater actuation).

The staff finds that the DAS is sufficiently diverse from the RPS portion of the PSMS since the DAS is an analog system, making it diverse from the digital MELTAC platform which is used in the PSMS. While the DAS uses the same sensor signals as the PSMS, these signals are isolated between the sensor and the DAS. The output signals of the DAS are sent to the appropriate PIF Modules to initiate the auxiliary feedwater system and initiate a turbine trip. To address the reliability aspects of the DAS, MHI stated that the DAS was developed using the Japanese nuclear QA program and it allows for each DAS cabinet circuitry to be tested individually while the reactor unit is on-line. Section 3.2.2 provides additional discussion regarding the QA and testability aspects of the DAS. Therefore, because of the provisions for QA and testability aspects of the DAS and, since the equipment between the sensor output and

the final actuation devices is diverse from the equipment used by the PSMS to initiate a reactor trip, the staff finds that the design concepts for the DAS meet the requirements of 10 CFR 50.62(c)(1).

Although specific to pressurized water reactors manufactured by Combustion Engineering or Babcock and Wilcox, MHI proposed design concepts to address 10 CFR 50.62(c) (2), which requires the following:

> Each pressurized water reactor manufactured by Combustion Engineering or by Babcock and Wilcox must have a diverse scram system from the sensor output to interruption of power to the control rods. This scram system must be designed to perform its function in a reliable manner and be independent from the existing reactor trip system (from sensor output to interruption of power to the control rods).

The normal reactor trip function from the PSMS is diverse and independent from the reactor trip function provided by the DAS as shown below:

- Computer-based technology is used for the normal reactor trip in PSMS; conventional technology (analog and solid-state logic) is used for the diverse reactor trip in the DAS.
- The DAS reactor trip function uses a subset of the same sensors used for the normal reactor trip function in the PSMS (there is no requirement in 10 CFR 50.62 for sensor diversity).
- The normal reactor trip from PSMS breaks power to the control rod drive mechanism using the reactor trip breaker; the diverse reactor trip from DAS breaks the power of the control rod drive mechanism by de-energizing the motor-generator set.
- The interface signals between PSMS and DAS are isolated by conventional isolation modules to ensure independence.

Since the DAS also sends a signal to remove power to the motor-generator set that powers the control rod drive mechanism, the staff finds that there is a diverse means of interrupting power to the control rods. Therefore, the staff finds that the design concepts for the DAS meets 10 CFR 50.62(c)(2).

3.1.5 Functional Diversity

Although the RPS and ESFAS are integrated, MHI states that functional diversity is provided within the integrated RPS/ESFAS because there are two separate subsystems in each train. For each AOO and PA, each subsystem processes diverse sensor inputs that can each detect the event and initiate protective actions. For example, one input may be a temperature input to one group and the other a pressure input to the other group, within each train.

Instead of separating RPS and ESFAS, functional diversity is provided within the integrated RPS/ESFAS through two separate subsystems in each train. For each design basis accident each subsystem processes diverse sensor inputs that can each detect the design basis accident and initiate protective actions. In response to RAI-11 (Ref. 6.1-11), MHI states:

> In the PSMS, the ESFAS is actuated by bistable functions that are also used for the RPS. This sharing of functions in the digital PSMS is the same as the sharing of functions between the RPS and ESFAS in prior MHI analog protection systems. This is also the same as the sharing of functions between RPS and ESFAS in Westinghouse analog and digital protection systems and Combustion Engineering analog and digital protection systems. There are more than 30 years of operating experience in the US and more than 30 years of operating experience in Japan with this type of shared RPS/ESFAS architecture.

The ESFAS is a subsystem of the PSMS. Sensor signals used in the ESFAS are processed, initially, within the RPS section of the PSMS, prior to transmission to the ESFAS section of the PSMS. In response to RAI-02 (Ref. 6.1-11), MHI states that sensor signals which are common to reactor trip/ESF actuation, are transmitted to the RPS section of the PSMS. The sensor signals are processed through setpoint comparison function blocks (bistables) in the RPS. There are separate bistables for each reactor trip and ESF function when there are setpoint differences. Bistable outputs from each train of the PSMS are combined within the RPS using 2-out-of-4 voting logic. The voting logic is associated with each bistable, so it is separate for each reactor trip and ESF function when there are setpoint differences. The voting logic outputs required for reactor trip are interfaced to the reactor trip breakers. The voting logic outputs, which are required for ESF actuation, are transmitted to the ESFAS section of the PSMS. Each ESFAS train processes the signals from all four RPS trains with 2-out-of-4 voting logic for the ESF actuation.

Each separate division of the RPS receives signals from various sensors. Within each division, the RPS compares these sensor values to trip setpoints. The binary outputs of the comparators are shared between each division and then processed through 2-out-of-4 voting logic. The output of the RPS voters, corresponding to the sensors that are required for ESF actuation, are transmitted to each division of the ESFAS. Each ESFAS division processes the signals from the four RPS divisions through 2-out-of-4 voting logic for ESF actuation. Thus a failure of one or two divisions of the RPS to communicate a sensor/calculated value does not affect the accomplishment of the ESF actuation in any ESF division. The signal processing is described in Topical Report MUAP-07004, “Safety I&C System Description and Design Process,” Revision 1. The data communication interface between each RPS division and each ESFAS division is continuously monitored through the PSMS self-diagnostics. If a communication interface fails, an equipment failure alarm is generated in the MCR. The ESFAS does not consider a failed communication interface as an active trip path in its 2-out-of-4 voting logic.

The D3 analysis assumes that a software CCF fails the RPS (or ESFAS) and concludes that diversity for reactor trip exists with the DAS. Because of the RPS/ESFAS interface, a software CCF in the RPS could fail both the RPS and ESFAS. In response to RAI-10, (Ref. 6.1-11), MHI stated:

> A software defect in the interface between the RPS and ESFAS is most likely to result in a detectable failure of the digital communications interface. This failure would be detected by the self-diagnostics within the ESFAS and alarmed in the MCR. This defect would then be corrected prior to it resulting in a CCF of the ESFAS concurrent with an AOO or PA. A software defect in the digital communications interface that remains undetected could result in a CCF of the ESFAS concurrent with an AOO or PA. If this undetectable defect is limited to the RPS/ESFAS digital communications interface, there would be no CCF in the RPS or in the PCMS. However, if this undetectable defect exists in all digital communications interfaces of this same type (i.e., Data Link as described in Section 4.3.3 of MUAP-07005), it would also result in a CCF of the RPS.

Also, the staff noted that in the US-APWR, the RPS and ESFAS are not considered to be different echelons of defense. Because DAS would be unaffected by a software CCF that failed the RPS/ESFAS interface, DAS would remain available. Because the DAS is not affected by the CCF that is postulated to adversely affect the three digital echelons, the potential for CCF is minimized based on diversity between the echelons of defense. CCF coping strategies include fault avoidance/minimization through redundancy and diversity, and fault tolerance through the detection and removal of faults. All three systems, RPS, ESFAS and DAS use the same functionally diverse sensor inputs for actuation. Although a faulty sensor could compromise the integrity of a train of RPS/ESFAS while also providing an erroneous value to the DAS, the integrity of the reactor trip logic and ESF actuation logic in RPS/ESFAS cannot be compromised by a single faulty sensor due to 2-out-of-4 configurations for reactor trip and ESF actuations. The DAS also uses 2-out-of-4 configurations for diverse reactor trip and ESF actuations. Thus, a single faulty sensor would not compromise the integrity of any of the four trains of the RPS/ESFAS or DAS. MHI uses only analog sensors as applied to the PSMS and DAS.

In summary, the staff identifies in the topical report that MHI proposes functional diversity between the two subsystems within a single division. Each subsystem would execute functions that incorporate signal diversity from the other subsystem within its division. MHI did not credit the functional diversity within the PSMS to address the defense-in-depth and diversity of overall I&C system against software CCFs. Therefore, the staff did not review and neither approves nor disapproves the functional diversity concepts within the division. Instead, the staff reviewed what MHI did credit, which is the diversity and defense-in-depth between the proposed echelons of defense; namely between the PSMS, PCMS, Human Systems Interface Systems (HSIS), and the DAS.

3.2 Review of Diversity and Defense-in-Depth

While the NRC considers CCFs in digital systems to be beyond design basis events, US-APWR design certification applicant shall ensure that digital RPS is protected against CCFs. As with ATWS mitigation systems, if a postulated digital system CCF could disable a safety function, then a diverse means, with a documented basis that the diverse means is not subject to the same CCF, should be included in the overall system design. This diverse means should

perform either the same function or a different function that will mitigate accidents or events that require the safety function which is assumed to have failed by the postulated CCF. The diverse or different function may be performed by a non-safety system if the system is of sufficient quality to perform under the associated event conditions.

The following documents were used during the review to assess the DAS and its diversity and defense-in-depth attributes:

- SECY 93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs"
- SRP Section 7.8, "Diverse Instrumentation and Control Systems"
- SRP HICB-19, "Guidance For Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems"
- NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems"

3.2.1 Conformance to SECY 93-087

The Commission, in response to SECY 93-087, notes that inasmuch as common-mode failures are beyond design-basis events, the analysis of such events should be on a best-estimate basis. The four items given in Subsection II.Q, as revised by the Commission in the staff requirements memorandum (SRM) for SECY 93-087 are as follows:

1. The applicant shall assess the defense-in-depth and diversity of the proposed instrumentation and control system to demonstrate that vulnerabilities to common-mode failures have adequately been addressed.

2. In performing the assessment, the vendor or applicant shall analyze each postulated common-mode failure for each event that is evaluated in the accident analysis section of the Safety Analysis Report (SAR) using best-estimate methods. The vendor or applicant shall demonstrate adequate diversity within the design for each of these events.

3. If a postulated common-mode failure could disable a safety function, then a diverse means, with a documented basis that the diverse means is unlikely to be subject to the same common-mode failure, shall be required to perform either the same function or a different function. The diverse or different function may be performed by a non-safety system if the system is of sufficient quality to perform the necessary function under the associated event conditions.

4. A set of safety grade displays and controls located in the main control room shall be provided for manual, system-level actuation of critical safety functions and monitoring of parameters that support the safety functions. The displays and controls shall be independent and diverse from the safety computer system identified in items 1 and 3 above.

MHI assessed the D3 of the US-APWR I&C system in Section 7 of the topical report. Section 7 assesses the diversity between the PSMS and the PCMS and the diversity between the PSMS and the DAS. Since, the PSMS and the PCMS are both implemented with the digital MELTAC platform, MHI considers a software CCF that could disable both systems. Because the DAS is composed only of conventional analog and binary devices, it provides sufficient diversification from the digital safety I&C system; the analog DAS is unaffected by a software CCF and remains available to perform its intended function. Based on the assessment performed in Section 7, and the consideration of a software CCF that disables both the PSMS and the PCMS, the staff finds that item as quoted above is adequately addressed. Based on the diverse technology (analog vs. digital) between the DAS and the PSMS, the staff finds that item as quoted above, has been adequately addressed by MHI.

To accommodate those situations where the PSMS is operating in a mode that is generating output signals that would be considered non-safe, the hardwired priority logic within the PIF module combines the outputs from the PSMS/PCMS and the DAS, and gives priority to the pre-defined safe state of the component.[1] This is consistent with DI&C-ISG-04, (Ref. 6.1-9) which states:

> Safety-related commands that direct a component to a safe state must always have the highest priority and must override all other commands. Commands that originate in a safety-related channel but which only cancel or enable cancellation of the effect of the safe-state command (that is, a consequence of a Common-Cause Failure in the primary system that erroneously forces the plant equipment to a state that is different from the designated "safe state"), and which do not directly support any safety function, have lower priority and may be overridden by other commands.

MHI proposed in the topical report that the priority logic in the PIF Module is designed and built with discrete digital components (versus microprocessor-based or programmable logic technology). Therefore, the logic could be considered hardware-based and not susceptible to a software CCF. The staff did not review the design of the PIF Module to verify that the priority logic is hardware-based and of sufficient quality to determine the absence of a software CCF. The staff will make the final determination of the potential for a CCF in the PIF Module during the review of Topical Report MUAP-07005-P, “Safety System Digital Platform – MELTAC” Revision 1. Thus, the staff’s determination of the I&C system’s design consistency with DI&C-ISG-04, will be dependent on that review. The demonstration that the PIF Module priority logic is hardware-based and not susceptible to a software CCF is identified as ASAI 5-3.

[1] As an example of a non-safe state, consider that the PSMS would normally keep a containment isolation valve open, but the safe state of this valve is closed. If the PSMS fails as-is because of a CCF, this non-safe open control signal would be maintained. Similarly, the PSMS may normally keep a turbine-driven emergency feedwater (T/D-EFW) pump actuation valve closed, but the safe state of this valve is open. If the PSMS fails as-is because of a CCF, this non-safe closed control signal would be maintained. To accommodate these situations, the hardwired priority logic within the PIF Module combines the outputs from the PSMS/PCMS and the DAS, and always gives priority to the pre-defined safe state of the component. For the examples above, this means that for the containment isolation valve, priority is given to the closed state control signal, and for the T/D-EFW pump actuation valve, priority is given to the open state control signal. The case where there is a potential for two safe states is discussed in Section 3.2.2 (h), Conformity to SRP 7.8, “Diverse Instrumentation and Control Systems”, Potential for Inadvertent actuation.

In order to address item 2, Technical Report MUAP-07014, "Defense-In-Depth and Diversity Coping Analysis," Revision 1 (Ref. 6.1-12), will provide the remaining D3 analysis information for the US-APWR. The analysis is to be based on the generic methods described in this topical report and provided as part of the US-APWR design certification application. MUAP-07014 will provide an evaluation of each event in Chapter 15 of the US-APWR Design Certification-Final Safety Analysis Report. Subsequently, MUAP-07014 is to address item 2 above, which states that a vendor or applicant is to analyze each postulated CCF for each event that is evaluated in the accident analysis section of the safety analysis report using best estimate methods. Additional discussion and ASAIs regarding the coping analysis are provided in Section 3.2.3 of this SER.

Item 4 requires manual controls and independent and diverse monitoring of critical safety functions. The Diverse Human System Interface Panel (DHP) in the MCR contains a set of displays and controls that provide for manual system-level actuation of critical safety functions and for monitoring of parameters that indicate the status of those critical safety functions. System level manual actuation is also provided on the DHP in the MCR for all automated functions. In addition, indications and manual controls are provided on the DHP for operating systems and components. In addition, indications and manual controls are provided on the DHP to operate components which:

- should be operated frequently (e.g., depressurization valves used during a steam generator (SG) tube rupture)

- should be operated at the same time (e.g., closure of containment isolation valves).

The associated components required for each critical safety function to be actuated by the DAS and the required types of actuation are summarized in Table 1. The typical monitoring variables for the DAS are identified in Table 2. The specific monitoring variables and controls for the US-APWR design certification application are to be identified. This is ASAI 5-4.

The PSMS and DAS share sensors for indications. The sensor signals are interfaced to the DHP prior to any digitalization in the PSMS. Conventional analog isolators in the PSMS assure independence. The point at which the manual controls are connected to safety equipment is upstream of any potential CCF in the computer-based safety system. Therefore, the staff finds that item 4 of Subsection II Q of SECY 93-087 will be addressed upon satisfactory completion of ASAI 5-4.

The topical report proposes two system-level manual actuations; one for the DAS and one for the PSMS. While the staff finds the system-level manual actuation concept for DAS addresses item 4 of Subsection II.Q of SECY 93-087, the concept of having two system-level manual actuations would need to be addressed from a human factors aspect in the US-APWR design certification application. This is to be addressed as part of ASAI 5-4.

Table 1. DAS Safety Functions and Typical Components

Safety Function / Associated Components	Number of Components	Actuation Type
Diverse Reactor Trip (M-G set trip)	2 M-G sets	Automatic/Manual (MCR)
Turbine Trip	2 trip solenoids	Automatic/Manual (MCR)
Turbine-Driven Emergency Feed Water Pump	2 pumps	Automatic/Manual (MCR)
Emergency Core Cooling System (ECCS) Pump	2 pumps	Manual (MCR)
Pressurizer Depressurization Valve	1 Valve	Manual (MCR)
Steam Generator Depressurization Valve	1 Valve / SG	Manual (MCR)
SG Blowdown Isolation Valve	1 Valve / SG	Automatic/Manual (MCR)
Main Feed Water Control Valve (Close)	1 Valve / SG	Automatic/Manual (MCR)
Emergency Feed Water Control Valve	1 Valve / SG	Manual (MCR)
Steam Line Isolation Valve		Manual (Local)
Containment Isolation Valves	1 Train	Manual (MCR)
Containment Spray Pump		Manual (Local)

3.2.2 Conformance to Section 7.8 and Standard Review Plan

The objectives of SRP Section 7.8 are to assure that the ATWS mitigation systems and equipment are designed and installed in accordance with the requirements of 10 CFR 50.62, and that other diverse I&C systems within the scope of this section comply with the NRC position on D3. The acceptance criteria in SRP 7.8 are based on meeting the relevant requirements of the following Commission regulations: 10 CFR 50.55a(a)(1); 50.55a(h); 10 CFR 50.62; and 10 CFR Part 50, Appendix A, GDCs 1, 13, 19, 24, and 29.

The following are the nine major design considerations emphasized per the guidance of SRP Section 7.8 with respect to the diversity of the I&C systems:

(a) Design Basis

SRP Section 7.8 states that the design bases should be described in the SAR for each diverse I&C system and that the design bases should, as a minimum, address the following topics:

- The specific design requirements identified in 10 CFR 50.62, as applicable, and any other applicable design requirements.
- Identification of conditions that require protective action by the diverse I&C systems. For DAS, these events are identified in the applicant/licensee's D3 analysis. For ATWS mitigation systems, these events are limited to anticipated operational occurrences.
- Identification by the applicant/licensee of the bounding events and the bases in the analyses that are presented or referenced in SAR Chapter 15.

Identification of the range of transient and steady-state conditions for both the energy supply and the environment during normal, abnormal, and accident conditions under which the system must perform.

– Identification of performance requirements. The performance requirements for which credit is taken in the mitigation of design basis events (e.g., dynamic response, accuracy) should be identified. The review should confirm that the applicant/licensee verifies conformance to these requirements by validation testing and surveillance.

MHI states that Technical Report MUAP-07014, "Defense-In-Depth and Diversity Coping Analysis," Revision 0, will confirm that the DAS copes with a CCF in the digital safety system that occurs concurrent with US-APWR DCD Chapter 15 safety analysis events (AOOs/PAs) in terms of the pressure boundary integrity, the coolability and the radiation release based on the CCF acceptance criteria. The analysis also will show the ATWS criteria for the design certification Chapter 15 events assuming a CCF. Although the US-APWR uses functional diversity to minimize the potential for CCF in the PSMS, functional diversity within the PSMS is not credited in Technical Report MUAP-07014. That analysis conservatively evaluates the system assuming that a CCF disables all digital control and protection systems in their entirety, including those that are functionally diverse. In addition, mitigating functions of the control system that use the same digital platform are assumed to be disabled by the same CCF. Many assumptions for each event are consistent with the assumptions of the safety analysis. However, some assumptions differ since Technical Report MUAP-07014 uses best estimate methods, as allowed by SRP acceptance criteria. Any differences will be explained and justified in Technical Report MUAP-07014. Additional discussion and ASAIs regarding the analysis of design basis events and AOOs is provided in Section 3.2.3 of this SER.

The response time of the DAS automatic actuation is to be considered in Technical Report MUAP-07014, "Defense-In-Depth and Diversity Coping Analysis," Revision 0. Delay of all the DAS-related components from sensor to actuator is considered in the response time. Also, a functional timer delay prevents actuation of DAS before normal operation of the PSMS has considered. Setpoints for the DAS automatic actuation are based on nominal equipment accuracies of the related components, including sensors shared between DAS and the PSMS and equipment that is unique to the DAS, such as analog bistables. Adequate margin is taken into consideration in establishing the setpoints of DAS so that DAS does not actuate before PSMS. The final determination of the setpoints and the response time of the DAS will be addressed as ASAI 5-5.

(b) Quality of components and modules

GL 85-06, "Quality Assurance Guidance for [ATWS] Equipment That is Not Safety-Related," provides guidance for the QA of non-safety-related ATWS mitigation equipment. The topical report cites GL 85-06 in its list of references but does not address the guidance provided by the GL. However, the topical report states that the DAS was originally developed under a Japanese nuclear quality program that is equivalent to 10 CFR Part 50, Appendix B. An approved 10 CFR Part 50, Appendix B QA program is now in effect for all equipment. GL 85-06 states that the use of Appendix B as a reference does not indicate that the guidance in this letter [GL 85-06] imposes any Appendix B requirements on non-safety-related ATWS equipment, and, therefore, NRC would not judge compliance with this generic letter by using Appendix B or its

associated regulatory guides. Instead, NRC's inspections will focus on the implementation and effectiveness of the quality controls. The enclosure to GL 85-06 provides the explicit QA guidance for ATWS mitigation equipment.

The staff evaluated the quality and reliability aspects of the DAS to meet 10 CFR 50.62. While MHI stated that the DAS was developed using the Japanese nuclear QA program, MHI would need to make available information demonstrating that the QA applied to the DAS addresses the QA guidance found in GL 85-06. Subsequently, the staff would need to verify that the QA guidance of GL 85-06 is adequately addressed. This is ASAI 5-6.

(c) System testing and surveillance

In response to Regulatory Guide 1.118, “Periodic Testing of Electric Power and Protection Systems,” the applicant identified that all DAS functions are testable. Many component failures within the DAS, such as power supply failure, are alarmed. Each DAS cabinet can be tested separately with the plant on-line without actuating plant components.

(d) Power supply availability

Power sources are available during and following a loss of offsite power. The power supply for the DAAC, including the relay for manual actuation circuits, is supplied from the non-safety Uninterrupted Power Supply (UPS). The power supply from the non-safety UPS is described in the Topical Report MUAP-07004-P, “Safety I&C System Description and Design Process,” Revision 1. The DHP is activated by the permission switch in the power breaker for the DHP.

(e) Environmental qualification

The DAS is a non-safety system located in a mild environment. A mild environment is an environment that would, at no time, be significantly more severe than the environment that would occur during normal plant operation, including AOOs.

(f) System status

The actuation status of the systems and components actuated by DAS is confirmed through the monitoring of safety function parameters. Conventional analog indicators are provided on the DHP to monitor the process parameters for all critical safety functions. Table 2 provides a listing of a typical set of variables to be monitored on the DHP. The ranges and sensors are the same but isolated from the PCMS and the PSMS. The indicators are diverse from PCMS and PSMS so that operators can monitor the plant condition during all failures of the digital monitoring system that are caused by CCF. The specific monitoring variables and controls for the US-APWR design certification application are to be identified in ASAI 5-4.

(g) Independence from the protection systems

DAS functions are independent and diverse from the RPS and ESFAS. ATWS mitigation system is diverse from the RPS from the sensor output to the final actuation device. To determine the independence from the protection systems, the staff evaluated the common components between and within the RPS, ESFAS, and DAS divisions and systems and the CCF susceptibilities for these common components and their likelihood of occurrence. The

common components used by the DAS and PSMS (RPS/ESFAS) are sensors on the input end and the PIF Modules on the output end (for ESFAS only). MHI uses only analog sensors. The staff will make the final determination of the potential for a CCF in the PIF Module during the review of Topical Report MUAP-07005-P, "Safety System Digital Platform –MELTAC," Revision 1. The submittal by the US-APWR Design Certification Applicant and acceptance by the NRC staff of the PIF Module is identified as ASAI 5-3.

Table 2. Typical Monitoring Variables for DAS

Variables	Number of Channels
Intermediate Range Neutron Flux	1
Pressurizer Pressure	1
RCS Pressure Wide Range	1
RCS Cold Leg Temperature (Tcold)	1 / loop
Pressurizer Level	1
Steam Generator Water Level	1 / SG
Main Steam Line Pressure	1 / SG
Containment Pressure	1

(h) Potential for inadvertent actuation

The diverse I&C systems design should limit the potential for inadvertent actuation and challenges to safety systems. The features of the DAS and PSMS that minimize inadvertent actuations are summarized below:

- The DAS has two subsystems.

- Both DAS subsystems use conventional analog/relay technology with an energize-to-actuate configuration.

- Each subsystem of the DAS separately receives and processes four channels of input sensors from the PSMS. Two-out-of-four sensors must reach their trip limits before a DAS subsystem will actuate.

- DAS actuation is blocked if the PSMS actuates a reactor trip. The blocking function uses status signals that are directly obtained from actuated components to ensure that there is no false blocking from a point in the actuation signal path that could be subsequently affected by a PSMS CCF. The blocking function for each DAS subsystem is independent.

The RPS section of the PSMS actuates on 2-out-of-4 isolated and independent input sensors.

- There are eight reactor trip circuit breakers, also arranged in a 2-out-of-4 configuration.
- Each ESFAS train actuates on 2-out-of-4 inputs from the RPS.
- ESFAS is energized-to-actuate.
- Within each train of the SLS, ESF component controls are segmented into several controller groups. A spurious actuation of any single controller group is considered in the plant's accident analysis.

The PIF Modules in the PSMS ensure that even if a DAS spurious actuation occurs, spurious actuation cannot prevent the PSMS from performing its safety functions. For most plant components there is only one safe state, and the DAS can only generate signals that correspond to that safe state. Therefore, if spurious DAS signals are generated, components are positioned to their safe state. For the few plant components that have two safe states (depending on plant conditions), such as emergency feedwater isolation valves, a preferred safe state is defined (typically the feed state, not the isolation state). The priority logic in the PIF Module ensures the preferred state can be achieved by either the DAS or the PSMS.

In summary, the staff finds that spurious actuation signals from the DAS, which correspond to a non-preferred state, cannot block the PSMS from achieving the preferred safe state and the potential for challenges to the PSMS are acceptably limited.

(i) Manual initiation capability

With regards to Regulatory Guide 1.62, “Manual Initiation of Protective Actions,” the topical report states all DAS functions related to reactor trip and maintaining critical safety functions can be manually initiated at the system level by conventional switches located on the DHP in the MCR. Typical functions are described in this topical report.

(j) Completion of protective action

The ATWS mitigation logic and DAS are designed such that, once initiated, the mitigation function will execute to completion. As described in Section 6.2.2.1(2) of the topical report, once initiated, the DAS functions are latched. Therefore, all DAS mitigation functions for all AOOs (including ATWS) and PAs will go to completion.

(k) D3 analysis

Section 3.2.1 of this SER addresses the D3 analysis as described in the topical report.

3.2.3 Conformance to Branch Technical Position (BTP) HICB-19

SRP BTP HICB-19 provides the four-point position on D3. These positions are those identified in SECY 93-087 and discussed in Section 3.2.1 of this SER. The staff found that MHI will have adequately addressed those positions upon satisfactory completion of the ASAIs identified.

As stated in SRP HICB-19 the applicant should demonstrate compliance with the four-point position described above. To reach a conclusion of acceptability, the following four criteria should be reached and supported by summation of the results of the analysis:

Criteria 1:

> For each anticipated operational occurrence in the design basis occurring in conjunction with each single postulated common-cause failure, the plant response calculated using best-estimate (realistic assumptions) analyses should not result in radiation release exceeding 10% of the 10 CFR Part 100 guideline value or violation of the integrity of the primary coolant pressure boundary. The applicant/licensee should (1) demonstrate that sufficient diversity exists to achieve these goals, (2) identify the vulnerabilities discovered and the corrective actions taken, or (3) identify the vulnerabilities discovered and provide a documented basis that justifies actions not taken.

Each AOO in the design basis is assumed to occur in conjunction with each single postulated CCF that disables the PSMS and PCMS. In Section 8.1, "Event Analysis Method" the topical report states that the "plant response calculated using best-estimate (realistic assumptions) analyses does not result in radiation release exceeding 10 percent of the 10 CFR Part 100 guideline value or violation of the integrity of the primary coolant pressure boundary." An analysis which will address Criteria 1 will be provided in the US-APWR design certification application. This is ASAI 5-7.

Criteria 2:

> For each postulated accident in the design basis occurring in conjunction with each single postulated common-mode failure, the plant response calculated using best-estimate (realistic assumptions) analyses should not result in radiation release exceeding the 10 CFR Part 100 guideline values, violation of the integrity of the primary coolant pressure boundary, or violation of the integrity of the containment (i.e., exceeding coolant system or containment design limits). The applicant/licensee should either (1) demonstrate that sufficient diversity exists to achieve these goals, or (2) identify the vulnerabilities discovered and the corrective actions taken, or (3) identify the vulnerabilities discovered and provide a documented basis that justifies actions not taken.

Each PA in the design basis is assumed to occur in conjunction with each single postulated CCF that disables the PSMS and PCMS. Also in Section 8.1, "Event Analysis Method," the topical report indicates that "the plant response obtained using best-estimate analysis does not result in violation of the integrity of the reactor coolant pressure boundary or the integrity of the

containment, or radiation release exceeding 10 CFR Part 100 guidelines." An analysis which will address Criteria 2 will be provided in the US-APWR design certification application. This is ASAI 5-8.

Criterion 3:

> When a failure of a common element or signal source shared between the control system and the RTS is postulated, and (1) this common-mode failure results in a plant response that requires reactor trip, and (2) the common-mode failure also impairs the trip function, then diverse means that are not subject to or failed by the postulated failure should be provided to perform the RTS function. The diverse means should ensure that the plant response calculated using best-estimate (realistic assumptions) analyses does not result in radiation release exceeding 10 percent of the 10 CFR Part 100 guideline value, or violation of the integrity of the primary coolant pressure boundary.

The staff determined that the DAS addresses Criteria 3 since the analog DAS is diverse from the digital MELTAC Platform (common element) which is used in the PSMS and PCMS. Thus, a postulated CCF that fails the digital systems would not impair the DAS function. Safety or non-safety sensors selected by the plant design are interfaced from within the PSMS or PCMS input modules. These input modules use isolators that connect the analog input signals to the DAS prior to any digital processing. Failure of a single analog signal source in the US-APWR design would not prevent a safety function due to the four redundant divisions in the PSMS and the four redundant channels within each DAAC of the DAS system.

Criteria 4:

> No failure of monitoring or display systems should influence the functioning of the RTS or ESFAS. If plant monitoring system failure induces operators to attempt to operate the plant outside safety limits or in violation of the limiting conditions of operation, the analysis should demonstrate that such operator-induced transients will be compensated for by protection system function.

The monitoring and indication functions are provided by the HSIS which includes the HSI from the PSMS, PCMS and DAS. The safety monitoring, manual reactor trip and manual ESF actuation functions are included in the PSMS. The non-safety PCMS provides monitoring and manual controls to maintain operating limits during normal plant operation.

The non-safety DAS provides monitoring, manual reactor trip and manual ESF actuation that is diverse from the PSMS and PCMS. Communication failures or faulty signals or commands transmitted or generated within the communications systems or monitors are not addressed in the topical report. As discussed in Section 3.2.1, the human factors aspect of two system-level manual actuations are to be addressed as part of ASAI 5-4.

Conformance to NUREG/CR-6303

The staff reviewed the MHI D3 analysis which used the guidance provided in NUREG/CR-6303 and provides 14 guidelines for performing a D3 analysis. MHI has constructed the I&C systems block diagram, conceptually, using the Block Guideline (1). The candidate blocks were examined under the Diversity Guideline (2) to decide which blocks are identical for analysis purposes, and which will be considered diverse, as required by Guideline 7 - Use of Identical Hardware and Software Modules. The analysis was then conducted as required by the general analysis guidelines (4-14), keeping in mind, that the ultimate goal of the analysis is to detect vulnerabilities to the system failure types described in Guideline 3 - System Failure Types. Consequently, MHI addressed all 14 general analysis guidelines and found no significant vulnerabilities.

As stated by the guidance of NUREG/CR-6303, combining the results of the diversity attributes can be used to make an overall decision. Also, as described by the guidance, the clearest distinction between two candidate subsystems would be design diversity, particularly; a non-digital subsystem would easily be considered an optimum diverse alternative to a digital subsystem. This has been provided by MHI in the proposed architecture, the US-APWR PSMS and PCMS are computer-based, software dependent, versus that of the DAS which is comprised of the analog, non-software, based components. General vulnerabilities could potentially appear in the cases studied under Guidelines 10 and 11, diversity for AOO's and PA's, respectively, and may be considered the higher priority than reducing isolated specific vulnerabilities as the guidelines suggest. These will be reviewed in the completion of ASAIs 5-7 and 5-8. The staff also identifies these specific concerns:

- Type 1 Failures:

  Type 1 failures are control system failures that result in plant transients that require protective actions for mitigation. MHI's position is that a software failure that results in spurious actuation of a PCMS function (e.g., Reactivity Control, Pressurizer Control, Steam Generator Level Control, etc.) to the energized or de-energized state is immediately detectable and therefore very unlikely to result in a CCF that affects multiple PCMS functions. MHI considered a CCF that leaves all PCMS functions in the fail-as-is condition and the PSMS is affected by the same CCF and fail-as-is condition. Staff Position 4 of ISG DI&C-ISG-02, "Diversity and Defense-in-Depth Issues," states that software CCFs that cause an undesirable trip or actuation can be detected because these types of failures are self-announcing. However, the staff position states that a simple failure of the total system may not be the worst case failure, particularly when analyzing the time required for identifying and responding to the condition. For example, a failure to trip may not be as limiting as a partial actuation of the emergency core cooling system, with indication of a successful actuation.

  The staff's review of the topical report identified the spurious actuation and the total fail-as-is condition of the PCMS/PSMS and found MHI's treatment of those conditions to be acceptable. However, MHI did not address partial failure of the PCMS/PSMS due to a CCF. Discussion of the partial failure potential of the PSMS and how the D3 strategy addresses such conditions is to be part of the US-APWR design certification application. This is ASAI 5-9.

Type 3 failures –

Type 3 failures occur because the primary sensors expected to respond to a design-basis event produce anomalous readings. The primary defense against a Type 3 failure is to provide diverse sensors for measuring the plant response to an initiating event. The DAS shares the same sensors as the PSMS and PCMS. Therefore the defense for Type 3 failures is not provided in the DAS for a single parameter measured. As NUREG/CR-6303, (Ref. 6.1-5) suggests, at a minimum, there should be sufficient signal diversity to ensure that for each anticipated operational occurrence in the design basis in conjunction with postulated CMFs, the plant shall be brought to a stable hot standby condition. As identified in Section 10 of the topical report, future licensing submittals will address signal diversity.

Overall, the staff finds the MHI D3 analysis in the topical report adequately addresses the guidance in NUREG/CR-6303, subject to the successful completion of the ASAIs.

3.3 Coping Strategy for Large Break Loss-of-Coolant Accidents

3.3.1 Coping Strategy with Leak-Before-Break Detection

Section 9.3 of the topical report, "Credit for Leak Detection in Defense-in-Depth and Diversity Analysis," states that while the D3 Coping strategy for a LBLOCA includes leak detection, it is not solely on leak detection; therefore it is not taking credit for leak-before LBLOCA. The generic D3 methodology for LBLOCA considers several additional factors:

1. The application algorithms for RPS and ESFAS have existed for more than 20 years. These algorithms are very simple. Those which actuate the ECCS have a single input with a single setpoint (e.g., low pressurizer pressure), and therefore allow near 100 percent testing. The operating history and simplicity of these algorithms essentially eliminates the potential for a CCF due to specification or application programming errors.

2. The design of the basic operating system of the MELTAC platform includes defensive measures, such as continuous cyclical input/output and program processing, with single tasking and a single software trajectory. These features ensure that the PSMS executes exactly the same during an AOO or PA as it does at all other times.

3. Item 1 and 2 eliminate the potential for a CCF to be triggered by any AOO or PA. While it can never be claimed that a latent undetected software defect could not still exist at the time of an AOO or PA, the likelihood of this is extremely low due to the infrequency of these events. This is because, unlike hardware, which may have aging mechanisms that increase the potential for CCF over time, operating experience has shown that software defects are revealed as software operating time increases (e.g., by testing, additional applications, additional users, etc). Since the frequency of AOOs and PAs is very low, it is likely that any software defect would have been detected and corrected, so that there is minimal potential for latent defects to still exist at the time of an AOO or PA. Since the frequency

of LBLOCA is significantly lower than for any other AOO or PA, it is reasonable to conclude that there is essentially no potential for a software defect to still remain hidden at the time of the LBLOCA.

To be extremely conservative, the D3 coping strategy does not credit this low potential for CCF concurrent with other AOOs or PAs (i.e., a CCF is considered concurrent with all other AOOs and PAs in the D3 Coping strategy).

Therefore, MHI concludes that the primary coping strategy for LBLOCA is based on the defensive measures within the design of the RPS/ESFAS, which minimize the potential for CCF concurrent with LBLOCA.

3.3.2 Conclusions on Large Break Loss-of-Coolant Accident Coping Strategy

10 CFR Part 50, Appendix A, GDC 4, "Environmental and Dynamic Effects Design Bases," states that the dynamic effects associated with postulated pipe ruptures in nuclear power units may be excluded from the design basis when analyses reviewed and approved by the Commission demonstrate that the probability of fluid system piping rupture is extremely low under conditions consistent with the design basis for the piping. Therefore, the leak-before-break credit was authorized for a very narrow application - consideration of dynamic effects of pipe ruptures. This regulatory position is also discussed in the NRC Inspection Manual, Part 9900; 10 CFR Guidance, "Definition of Leak-Before-Break Analysis and its Application to Plant Piping Systems (Ref. 6.1-13)." Additionally, the staff revised SRP HICB-19 such that the latest revision (Revision 5) is consistent with this very narrow application of leak-before-break credit.

In a RAI dated April 2, 2008, the staff requested MHI to further address their approach to LBLOCA. In the response, dated April 25, 2008, MHI reiterated that MHI's D3 Coping Strategy is not solely based on leak detection and it does not credit leak detection to exclude LBLOCA from the design basis. Rather, the coping strategy is based on defensive measures within the design of the RPS/ESFAS. As explained by MHI, the design attributes are:

- Simplistic algorithms,
- Program processing with single tasking and single software trajectory
- Single input with single setpoint
- Near 100 percent testing
- Low frequency of AOO and PA events

These attributes would support the development of components having high quality and reliability to meet requirements for safety-related digital I&C systems. These requirements include those of Institute of Electrical and Electronics Engineers (IEEE) Std. 603-1991 (Ref. 6.1-14), such as Criterion 5.3 − Quality and Criterion 5.15 − Reliability. These attributes would also help address acceptance criteria found in SRP BTP 7-14, "Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems" and Regulatory Guide 1.152, "Criteria for use of Computers in Safety Systems of Nuclear Power Plants." Despite the high quality of design and use of defensive design measures, software errors may still defeat safety functions in redundant, safety-related channels. Therefore, as set forth in Points 1, 2, and 3 of Item II.Q of the SRM for SECY-93-087, the staff requires that the

applicant/licensee perform a D3 assessment of the proposed digital I&C system to demonstrate that vulnerabilities to common-cause failures have been adequately addressed. Therefore, the staff does not accept these design measures of the RPS/ESFAS or the use of leak detection, as stated in the topical report, as a sufficient D3 coping strategy for the LBLOCA scenario concurrent with CCF. An acceptable strategy for addressing a LBLOCA concurrent with a CCF is needed for the US-APWR design. This is ASAI 5-10.

3.4 PIF Modules and Output Modules

Control signals from the PSMS and PCMS are interfaced to the plant components through PIF Modules. PIF Modules are also used to interface control signals from the DAS. Thus, the PSMS and the DAS interface at a PIF Module. A common PIF Module provides one power interface conversion device for control of one plant component. Because all three systems, PSMS, PCMS, and DAS, use PIF Modules, the potential for a CCF disabling two or more PIF Modules must be addressed.

The DAS provides an analog signal to a PIF Module that also has a digital input from ESFAS. The PIF Module then sends a control signal to the ESFAS components. Control signals from the DAS are interfaced to the PIF Module via conventional hardwired connections and a conventional isolation module in PSMS. The DAS, the isolation module, and the components used for the DAS signal interface within the PIF Module, which utilizes conventional hardwired circuits to prioritize commands from the safety and non-safety systems.

A PIF Module consists of three parts (Figure 3):

- Communication Interface
- Interposing Logic
- Switching Device

Figure 3. PIF Module

MHI states that the DAS consists only of conventional analog devices with no software. The DAS communicates with the PSMS using only conventional analog or binary signals through conventional analog or binary signal isolation devices[3]. In ASAI 5-1, the US-APWR design certification applicant shall demonstrate that the isolation devices are conventional (e.g., non software based devices), completely testable and meet applicable requirements. The staff finds the use of the PIF Module acceptable, with respect to the D3 methodology for the US-APWR, so long as ASAIs 5-1 and 5-3 are adequately satisfied.

4.0 FINDINGS AND CONCLUSIONS

The subsections below will discuss the degree of regulatory compliance met by the MHI designs and design process related to the D3 approach, as well as any licensee actions required before the D3 approach can by used for safety-related applications in nuclear power plants. The

[3] The portion of the PIF Module used by both PSMS and DAS includes only conventional binary components. "Conventional" means no software; that is, conventional hardware is relay, wiring module, solid state device, etc., as described in Section 6.2.1.2 of the topical report.

regulatory requirements used as the basis for this review are set forth in 10 CFR Part 50. Acceptance criteria are based on the SRP, regulatory guides, and industry standards. This section discusses the acceptability of the digital safety systems as it applies to these regulatory requirements.

10 CFR 50.55a(a)(1) and 10 CFR Part 50, Appendix A, GDC 1

10 CFR 50.55a(a)(1) and 10 CFR Part 50, Appendix A, GDC 1, "Quality Standards and Records," require, in part, that structures, systems, and components must be designed, fabricated, erected, constructed, tested, and inspected to quality standards commensurate with the importance of the safety function to be performed. The enclosure to GL 85-06 provides the QA guidance for non-safety-related ATWS equipment diverse I&C systems and components which the DAS is considered. As described in Section 3.2.2(b) of this SE, MHI stated that the DAS was developed using the Japanese nuclear QA standards and on-going QA activities will comply with 10 CFR Part 50, Appendix B. Confirmation by the staff that the QA activities for the DAS were appropriate and implemented was beyond the scope of the topical report and staff review. Completion of ASAI 5-6 will fully address 10 CFR 50.55a(a)(1) and GDC 1 requirements for the DAS. The staff conducted a review of the safety system descriptions in the topical report for conformance to the guidelines in the Regulatory Guides and industry codes and standards applicable to the ATWS mitigation and DAS systems. For the systems and components reviewed, the staff concludes that the applicant adequately identified the guidelines applicable to these systems. Therefore, the staff finds that the requirements of 10 CFR 50.55a(a)(1) and GDC 1 will be met upon satisfactory completion of ASAI 5-6.

10 CFR 50.62

10 CFR 50.62(c)(1) requires that each pressurized water reactor must have equipment from sensor output to final actuation device, that is diverse from the RTS, 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 and be independent (from sensor output to the final actuation device) from the existing RTS. In the topical report, the DAS is used to actuate a reactor trip, turbine trip, and initiate emergency feedwater for ATWS mitigation. As described in Section 3.1.3 of this SE, the equipment used by the DAS is diverse from the RTS since the DAS is developed with analog components and the RTS utilizes digital technology. This diversity exists from the output of the analog sensors to the final actuation devices. Section 3.1.3 also addresses the independence through analog isolation devices between the DAS and the RTS. To provide for reliable functionality of the DAS, Section 3.2.2(b) addresses the QA activities for the DAS and MHI has committed to the full testability of the DAS while the reactor unit is operational.

10 CFR 50.62(c)(2) requires, in part, that each pressurized water reactor manufactured by Combustion Engineering or by Babcock and Wilcox must have a diverse scram system from the sensor output to interruption of power to the control rods. While 10 CFR 50.62(c)(2) is not explicitly required of MHI, the DAS design is such that a diverse reactor trip function is provided. As described in Section 3.1.3 of this report, the DAS equipment generates a diverse reactor trip signal that de-energizes the motor-generator sets feeding power to the control rod drive mechanisms.

Based on the information provided in the topical report, and upon satisfactory completion of the ASAIs, the staff finds that the design concepts presented by MHI will meet 10 CFR 50.62.

10 CFR Part 50, Appendix A, GDC 13 and 19

10 CFR Part 50, Appendix A, GDC 13, "Instrumentation and Control," requires that instrumentation be provided to monitor variables and systems over their anticipated ranges for normal operation, for AOOs, and for accident conditions as appropriate to assure adequate safety. Appropriate controls shall be provided to maintain these variables and systems within prescribed operating ranges. 10 CFR Part 50, Appendix A, GDC 19, "Control Room," requires, in part, that a control room be provided from which actions can be taken to operate the nuclear power unit safely under normal conditions and to maintain it in a safe condition under accident conditions.

The DAS includes the DHP in the MCR. The staff review of the HFE aspects of the DHP and the MCR are described in Topical Report MUAP-07007, "HSI System Design Description and HFE Process," Revision 2. Based on the review of diverse I&C system status information, manual initiation capabilities, and provisions to support safe shutdown represented in the topical report, information is provided to monitor the system over the anticipated ranges for normal operation, for AOOs, and for accident conditions as appropriate to assure adequate safety. Appropriate controls are provided for manual initiation of diverse I&C functions. These manual controls are independent of the digital systems that provide automatic initiation of the same functions. The diverse I&C systems appropriately support actions to operate the nuclear power unit safely under normal conditions and to maintain it in a safe condition under accident conditions. Following staff's acceptability of Topical Report MUAP-07007 and satisfactory completion of ASAI 5-4, the staff will be able to find that the design concepts of the diverse I&C systems satisfies the requirements of 10 CFR Part 50, Appendix A, GDC 13 and 19.

10 CFR Part 50, Appendix A, GDC 22

10 CFR Part 50, Appendix A, GDC 22, "Protection System Independence," requires that the protection system be designed to assure that the effects of natural phenomena, and of normal operating, maintenance, testing, and PAs on redundant channels do not result in loss of the protection function. Design techniques, such as functional diversity or diversity in component design and principles of operation, shall be used to the extent practical to prevent loss of the protection function. The staff evaluated the independence between the non-safety DAS and the safety-related PSMS. Specifically, the staff found that the DAS design concepts appropriately use isolation devices to ensure independence from the safety-related PSMS. The staff also found that MHI demonstrates conformance with the four positions for diversity against common mode failures as discussed in Section 3.2 of this SER. The staff found that MHI will have adequately addressed those positions upon satisfactory completion of the ASAIs identified. Consequently, the staff considers the MHI approach to functional diversity and the diversity in the component design acceptable in minimizing the loss of the overall protective function to the plant. Therefore, the staff finds that the design concepts in the topical report meet GDC 22, subject to ASAI completion.

10 CFR Part 50, Appendix A, GDC 24

10 CFR Part 50, Appendix A, GDC 24, "Separation of Protection and Control Systems," requires that the protection system be separated from control systems to the extent that failure of any single control system component or channel, or failure or removal from service of any single protection system component or channel which is common to the control and protection systems, leaves intact a system satisfying all reliability, redundancy, and independence requirements of the protection system. Interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired.

The DAS is a non-safety system. Redundant divisions of the PSMS are physically and electrically isolated from the DAS. Where safety sensors are shared between the DAS and the PSMS, isolation modules in the PSMS prevent adverse interaction with the safety functions because of DAS failures. The DAS communicates with the PSMS using only conventional analog or binary signals through conventional analog or binary signal isolation devices. These design concepts incorporate the electrical, physical and communication isolation requirements necessary to assure that any single control system component or channel failure will not significantly impair the safety function of the protection system. The staff finds this design acceptable in satisfying the requirements of GDC 24.

10 CFR Part 50, Appendix A, GDC 29

10 CFR Part 50, Appendix A, GDC 29, "Protection Against Anticipated Operational Occurrences," requires that the protection and reactivity control systems be designed to assure an extremely high probability of accomplishing their safety functions in the event of AOOs. The PSMS provides the primary protection against AOOs. The DAS provides backup protection for AOOs through equipment that is diverse from the PSMS and therefore not subject to CCFs that may adversely affect the safety systems. The system components proposed for the digital safety systems will be environmentally and seismically qualified to ensure that they are capable of performing their designated functions while exposed to normal, abnormal, test, accident and post-accident environmental conditions.

The plant response for each AOO is to be evaluated, in conjunction with the postulated CCF that disables the PSMS/PCMS. Based on manual/automatic mitigation actions from the DAS, Technical Report MUAP-07014, "Defense-In-Depth and Diversity Coping Analysis," will demonstrate that, for an AOO coincident with a CCF, 10 CFR Part 100 dose limits will not be exceeded by more than 10 percent and the integrity of the primary coolant pressure boundary is not violated. In addition, the plant response for each PA is evaluated, in conjunction with the postulated CCF that disables the PSMS/PCMS. Based on manual/automatic mitigation actions from the DAS, Technical Report MUAP-07014 will need to demonstrate that the 10 CFR Part 100 dose limits are not exceeded, the integrity of the primary coolant pressure boundary is not violated, and the integrity of the containment is not violated. Technical Report MUAP-07014 will need to demonstrate compliance with the acceptance criteria defined above for each AOO and for each PA and captured in the ASAIs 5-7 and 5-8 in Section 5.0 of this report. Therefore, the staff finds that the design concepts for addressing D3 in this topical report meet the requirements of 10 CFR Part 50, Appendix A, GDC 29.

Based on the information provided in the Topical Report MUAP-07006-P, "Defense-in-Depth and Diversity", Revision 2, and subject to satisfactory completion of the ASAIs identified in Section 5.0 of this SER, the staff concludes that there is reasonable assurance that the MHI D3 design concepts and approach meets the relevant requirements of 10 CFR 50.55a (a)(1), 10 CFR 50.62, and 10 CFR Part 50, Appendix A, GDC 1, 13, 19, 22, 24, and 29 by satisfactorily addressing the acceptance criteria of SRP Section 7.8, HICB-19, and supporting industry standards.

5.0 US-APWR DESIGN CERTIFICATION APPLICATION-SPECIFIC ACTION ITEMS

In Section 10.0, "Future Licensing Submittals," of the topical report summarized additional information related to the topical report that will be submitted for NRC approval in future Plant Licensing Documentation.

As a result of the staff's review, the following US-APWR design certification application specific, or design specific, actions provided in Table 5-1 must be performed when requesting NRC approval for using the approach to D3 delineated in this topical report:

Table 5-1 US-APWR Design Certification Application Specific Action Items

Number	SER Referenced Section	Description
5-1	3.1, 3.4	The US-APWR design certification applicant shall demonstrate that the isolation devices are conventional (e.g., non software based devices) and completely testable in order to meet the independence and isolation requirements of IEEE Std and address fault-isolation criteria of IEEE-384.
5-2	3.1.3	The US-APWR design certification applicant shall demonstrate the acceptability of all manual actions. Also, the concept and application-specific implementation of the priority alarms should be adequately demonstrated.
5-3	3.2.1, 3.2.2	The US-APWR design certification applicant shall demonstrate that the PIF Module is not susceptible to a software CCF.
5-4	3.2.1, 3.2.2, 3.2.3	The US-APWR design certification applicant shall identify the specific controls and indications for the DHP and address human factors aspects for the DAS and PSMS system-level manual actuation means.
5-5	3.2.2	The US-APWR design certification applicant shall provide the final determination of the setpoints and the response time of the DAS.

Table 5-1 US-APWR Design Certification Application Specific Action Items

Number	SER Referenced Section	Description
5-6	3.2.2, 4.0	The US-APWR design certification applicant shall demonstrate that the acceptability of the QA process used for the DAS meets the guidelines of GL 85-06.
5-7	3.2.3	For each AOO in the design basis occurring in conjunction with each single postulated CCF, the US-APWR design certification applicant shall demonstrate that the plant response calculated using best-estimate (realistic assumptions) analyses does not result in radiation release exceeding 10 percent of the 10 CFR Part 100 guideline value or violation of the integrity of the primary coolant pressure boundary.
5-8	3.2.3	For each PA in the design basis occurring in conjunction with each single postulated CCF, the US-APWR design certification applicant should demonstrate that the plant response calculated using best-estimate (realistic assumptions) analyses should not result in radiation release exceeding the 10 CFR Part 100 guideline values, violation of the integrity of the primary coolant pressure boundary, or violation of the integrity of the containment (i.e., exceeding coolant system or containment design limits).
5-9	3.2.4	The US-APWR design certification applicant shall address the partial failures of the PCMS/PSMS and demonstrate an adequate D3 strategy to cope with such failure modes.
5-10	3.3.2	The US-APWR design certification applicant shall provide an acceptable defense in depth and diversity strategy for a LBLOCA concurrent with a CCF of the PSMS.
5-11	5.0	Submittal of all information identified in Section 10.0 of the topical report, “Future Licensing Submittals.”

6.0 Review by the Advisory Committee on Reactor Safeguards (ACRS)

During the 563rd meeting of the ACRS, June 3-4, 2009, the ACRS reviewed the SE for the MHI Topical Report MUAP-07006-P, Revision 2, "Defense-in-Depth and Diversity," for the US-APWR. The Subcommittee on US-APWR also reviewed this matter during a meeting on May 21, 2009. The ACRS documented its findings in a letter the commission dated June 25th, 2009. A copy of this letter is provided in Appendix A. The NRC staff's response, dated July 29th, 2009, is also included in Appendix A.

7.0 REFERENCES

7.1-1 Topical Report MUAP-07004-P, “Safety I&C System Description and Design Process,” Revision 1, Mitsubishi Heavy Industries, Ltd., July 2007 (ML072010356).

7.1-2 NUREG-0800, *Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants*, Chapter 7 – Instrumentation and Controls, Revision 5, U.S. Nuclear Regulatory Commission, Washington, DC, March 2007 (ML070550074).

7.1-3 Title 10 *Code of Federal Regulations* Part 50, “Domestic Licensing of Production and Utilization Facilities.”

7.1-4 Title 10 *Code of Federal Regulations* Part 52, “Licenses, Certifications, and Approvals for Nuclear Power Plants.”

7.1-5 NUREG/CR-6303, *Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems*, U.S. Nuclear Regulatory Commission, December 1994.

7.1-6 Generic Letter 85-06, “Quality Assurance Guidance for ATWS Equipment That is not Safety-Related,” U.S. Nuclear Regulatory Commission, Washington, D.C., April 16, 1995.

7.1-7 SECY-93-087, “Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs,” U.S. Nuclear Regulatory Commission, July 21, 1993 (ML003708056) and the SRM to SECY-93-087 (ML003708021).

7.1-8 Interim Staff Guidance DI&C-ISG-02, “Diversity and Defense-in-Depth Issues,” Revision 1, U.S. Nuclear Regulatory Commission, Washington, DC, September 26, 2007 (ML072540118).

7.1-9 Interim Staff Guidance DI&C-ISG-04, “Highly-Integrated Control Rooms − Communications Issues (HICRc),” Revision 0, U.S. Nuclear Regulatory Commission, Washington, DC, September 28, 2007.

7.1-10 Topical Report MUAP-07005-P, “Safety System Digital Platform-MELTAC,” Revision 2, Mitsubishi Heavy Industries, Ltd., July 2007 (ML082240067).

7.1-11 UAP-HF-08070, Y. Ogata to J.A Ciocco, “MHI’s Responses to Request for Additional Information on Topical Report MUAP-07006-P(R1) Defense-in-Depth and Diversity,” dated April 25, 2008 (ML081200217).

7.1-12 Technical Report MUAP-07014-P/NP, “Defense-In-Depth and Diversity Coping Analysis,” Revision 1, Mitsubishi Heavy Industries, Ltd., June 2008. (ML081770167).

7.1-13 Inspection Manual, Part 9900: 10 CFR Guidance, “Definition of Leak-Before-Break Analysis and its Application to Plant Piping Systems,” U.S. Nuclear Regulatory Commission.

7.1-14 IEEE Std 603-1991, “IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations,” Institute of Electrical and Electronics Engineers, Picataway, NJ.

8.0 LIST OF ACRONYMS

ACRS	Advisory Committee on Reactor Safeguards
ADAMS	Agency Document Access and Management Systems
ALWR	Advanced Light-Water Reactor
AOO	anticipated operational occurrences
APWR	Advanced Pressurized-Water Reactor
ASAI	Application-Specific Action Item
ATWS	anticipated transient without scram
BTP	branch technical position
CCF	common-cause failure
CFR	*Code of Federal Regulations*
D3	defense-in-depth and diversity
DAAC	Diverse Automatic Actuation Cabinet
DAS	Diverse Actuation System
DHP	Diverse Human System Interface (HSI) Panel
ECCS	Emergency Core Cooling Systems
ESF	engineering safety features
ESFAS	Engineered safety feature actuation system
GDC	General Design Criteria
GL	Generic Letter
HICB	Instrumentation and Control Branch
HICRC	Highly-Integrated Control Rooms-Communications Issue
HFE	human factors engineering
HSI	human systems interface
HSIS	Human Systems Interface System
I&C	instrumentation and control
IEEE	Institute of Electrical and Electronics Engineers
IPL	Interposing Logic
ISG	interim staff guidance
LBLOCA	large-break Loss of coolant accident
MCR	main control room
MELTAC	Mitsubishi Electric Total Advanced Controller
MHI	Mitsubishi Heavy Industries
NRC	U.S. Nuclear Regulatory Commission
PA	postulated accident
PCMS	Plant Control and Monitoring System
PIF	Power Interface
PSMS	Protection and Safety Monitoring System
QA	quality assurance
RAI	request for additional information
RPS	reactor protection system
RTS	Reactor Trip System
SAR	Safety Analysis Report
SE	Safety Evaluation
SECY	Secretary of the Commission, Office of the (NRC)
SG	Steam Generator
SLS	Safety Logic System
SER	Safety Evaluation Report
SRP	Standard Review Plan

US-APWR	U.S. Advanced Pressurized-Water Reactor
UPS	Uninterrupted Power Supply

Appendix A

Review by the Advisory Committee on Reactor Safeguards

UNITED STATES
NUCLEAR REGULATORY COMMISSION
ADVISORY COMMITTEE ON REACTOR SAFEGUARDS
WASHINGTON, DC 20555 - 0001

June 25, 2009

Mr. R. W. Borchardt
Executive Director for Operations
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

SUBJECT: SAFETY EVALUATION FOR THE MITSUBISHI HEAVY INDUSTRIES TOPICAL REPORT MUAP-07006-P, REVISION 2, "DEFENSE-IN-DEPTH AND DIVERSITY," RELATED TO THE US-APWR DESIGN

Dear Mr. Borchardt:

During the 563rd meeting of the Advisory Committee on Reactor Safeguards, June 3-4, 2009, we reviewed the Safety Evaluation (SE) for the Mitsubishi Heavy Industries (MHI) Topical Report MUAP-07006-P, Revision 2, "Defense-in-Depth and Diversity," for the U.S. Advanced Pressurized Water Reactor (US-APWR). Our Subcommittee on US-APWR also reviewed this matter during a meeting on May 21, 2009. During these meetings, we had the benefit of discussions with the staff and other stakeholders. We also had the benefit of the documents referenced.

RECOMMENDATION

The Safety Evaluation for Revision 2 of the MHI Topical Report MUAP-07006-P should be issued.

BACKGROUND

In 2007, MHI submitted the Topical Report MUAP-07006-P to the NRC staff for review. This Topical Report describes the MHI generic methodology used to address defense-in-depth and diversity in digital instrumentation and control (I&C) systems. MHI requested that the staff review and approve a defense-in-depth and diversity (D3) approach for digital I&C systems for the US-APWR and the current operating nuclear power plants.

In 2008, the staff notified MHI that it would be limiting the review of the Topical Report to the US-APWR design. This was due to the difficulty in addressing the unique aspects of the D3 approach in one Topical Report for all operating plants. Therefore, the staff's approval of MHI's D3 approach is limited to the US-APWR design. In addition, some aspects of the D3 approach could not be fully evaluated without reviewing more of the design-specific information in the associated Design Control Document or other topical and technical reports. The staff identified 11 design certification application specific action items to be evaluated during design certification reviews.

2

DISCUSSION

The MHI digital I&C system is built on the Mitsubishi Electric Total Advanced Controller Platform used in several of the Japanese nuclear power plants. It is a fully digital four channel system that includes a safety-related protection and safety monitoring system (PSMS) and a non-safety plant control and monitoring system (PCMS). The engineered safety features actuation system (ESFAS) is a subsystem of the PSMS. The PSMS includes many design features to minimize the potential for hardware or software failures. However, the design does not rely on these features to meet the regulatory requirements for defense-in-depth and diversity in the event of software common-cause failures (CCF) within the PSMS. To address the potential software CCF events, MHI credits a diverse actuation system (DAS) which is separate from the PSMS and PCMS and is not safety related.

DAS is an analog system with no software-based components. It consists of two trains located in separate fire zones. The control panel for DAS is located in the control room. The DAS shares sensor inputs with the PSMS through interfaces that are not subject to postulated software CCFs. The sensors and their isolation devices are analog components. Some of the outputs from the PSMS, PCMS, and DAS use common power interface modules to control or actuate some components. The DAS provides an analog signal to a power interface module that also has a digital input from ESFAS. The power interface module then sends a control signal to the ESFAS components. The staff identified two design certification application specific action items needed to provide assurance that a software CCF within the power interface modules cannot disable both the DAS and ESFAS systems. One application specific action item requires demonstration that the isolation devices are non-software based devices and completely testable. The other application specific action item requires demonstration that the power interface module is not susceptible to a software CCF.

To minimize spurious actuations, both trains of DAS must operate to initiate a reactor scram. DAS is automatically bypassed if it receives feedback from the safety components that they have been actuated by the PSMS. If DAS actuation is necessary, it initiates a reactor scram using means diverse from the PSMS. This is accomplished by shutting off the motor-generator sets that power the rod control system. The staff found that the DAS provides adequate diversity from the PSMS and satisfies the requirements for mitigation of an Anticipated Transient Without Scram (ATWS).

The DAS is automated for Anticipated Operational Occurrences (AOOs) and postulated accidents that require action within 10 minutes. These automatic actions include reactor trip, turbine trip, emergency feedwater actuation, and main feedwater isolation. MHI is proposing to take credit for manual operator actions within the first 30 minutes for certain events. The staff identified this as a design certification application specific action item, to be addressed during the design certification review. The staff will use the guidance from a forthcoming Interim Staff Guidance (ISG), “Crediting Manual Operator Actions for Diverse Actuation of Safety System,” in making its safety determination. The human factors engineering analysis of the time to complete the required manual actions and the adequacy of the plant transient analysis used to establish the time available will be evaluated during the design certification review to assess the acceptability of crediting manual operator actions during the first 30 minutes of a transient.

3

The coping strategy for large-break loss-of-coolant accidents (LBLOCA) in the Topical Report is based on arguments made by the designers and defensive measures within the design of the RPS/ESFAS, which reduce the potential for CCF concurrent with LBLOCA. These include the quality and reliability of the Mitsubishi Electric Total Advanced Controller design, recognition that CCFs are not triggered by AOOs or postulated accidents, the low frequency of LBLOCAs, and the DAS leak monitoring system. The staff found this coping strategy to be unacceptable because LBLOCAs are possible and leak-before break is not applicable. Therefore, the staff initiated an application specific action item requiring MHI to enhance its coping strategy for the US-APWR and submit it as part of the design certification review.

The staff concluded that the defense-in-depth and diversity approach documented in the Topical Report and responses to the Requests for Additional Information conform with regulatory requirements. This conclusion is subject to the satisfactory completion of the 11 design certification application specific action items documented in the SE. We concur with the staff's conclusion.

The SE for the MHI Topical Report MUAP-07006-P, Revision 2, should be issued.

Sincerely,

/RA/

Mario V. Bonaca
Chairman

References:

- U.S. Nuclear Regulatory Commission, Safety Evaluation by the Office of New Reactors, Licensing Topical Report MUAP-07006-P, Rev. 2, "Defense-in-Depth, and Diversity," dated June 2009 (ML091100381)

- Mitsubishi Heavy Industries, US-APWR Topical Report MUAP-07006-P, Revision 2, "Defense-in-Depth, and Diversity," dated June 2008 (ML081770168)

July 29, 2009

Dr. Mario V. Bonaca, Chairman
Advisory Committee on Reactor Safeguards
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

SUBJECT: SAFETY EVALUATION FOR THE MITSUBISHI HEAVY INDUSTRIES TOPICAL REPORT MUAP-07006-P, REVISION 2, "DEFENSE-IN-DEPTH AND DIVERSITY," RELATED TO THE U.S. ADVANCED PRESSURIZED WATER REACTOR DESIGN

Dear Dr. Bonaca:

On behalf of the U.S. Nuclear Regulatory Commission, I would like to thank you for your June 25, 2009, letter, which provided the Advisory Committee on Reactor Safeguards' (ACRS or Committee) views on the staff's safety evaluation for the Mitsubishi Heavy Industries, Ltd. (MHI), Topical Report MUAP-07006-P, Revision 2, "Defense-in-Depth and Diversity," for the U.S. Advanced Pressurized Water Reactor. Your letter was in response to discussions with the staff and MHI during the 563rd meeting of the ACRS, held June 3-4, 2009, and recommended approval.

We accept your recommendation and will issue the "Defense-in-Depth and Diversity" safety evaluation. The staff appreciates the Committee's continued interest and collaborative efforts with the staff on MHI's "Defense-in-Depth and Diversity."

Sincerely,

/RA Bruce S. Mallett for/

R. W. Borchardt
Executive Director
for Operations

cc: Chairman Jaczko
Commissioner Klein
Commissioner Svinicki
SECY