Enclosure 3

UAP-HF-08070
Docket No. 52-021

MHI's Response to NRC's Requests for Additional Information

on

Topical Report MUAP-07006-P(R1) Defense-in-Depth and Diversity

April 2008
(Non-Proprietary)

MHI's Responses to NRC's Requests for Additional Information on Topical Report MUAP-07006-P(R1) Defense-in-Depth and Diversity

Non Proprietary Version

April 2008

INTRODUCTION

This report documents Mitsubishi Heavy Industries' (MHI's) responses to U.S. Nuclear Regulatory Commission's (NRC's) request for additional information (RAI) on the MHI Topical Report, MUAP-07006-P (R1), "Defense-in-Depth and Diversity".

This report describes the responses for three (3) requests for information from the NRC.

The first RAI letter, "Mitsubishi Nuclear Energy Systems, Inc. - Request for Additional Information on US-APWR Topical Report MUAP-07006-P, Defense-In-Depth and Diversity", was issued on March 25, 2008 (ML080790297).

The second RAI letter, "Second Request for Additional Information on US-APWR Topical Report MUAP-07006-P, Defense-In-Depth And Diversity", was issued on April 2, 2008 (ML080880164).

The third RAI, "Human-Factors Engineering-Related Requests for Additional Information for MHI Topical Report MUAP-07006-P(R1), Defense-in-Depth And Diversity", was provided to MHI in draft form on April 22, 2008.

RESPONSE TO THE FIRST RAI (MARCH 25, 2008)

Following provides the responses for the first RAI, "Mitsubishi Nuclear Energy Systems, Inc. - Request for Additional Information on US-APWR Topical Report MUAP-07006-P, "Defense-in-Depth and Diversity", issued on March 25, 2008.

RAI-01

Could a faulty sensor compromise the integrity of a train of RPS/ESFAS while also providing an erroneous value to the Diverse Actuation System (DAS)?

Response

As shown in Figure 6.0-1 of Topical Report MUAP-07006, common sensors are applied for normal reactor trip (RT) and engineered safety feature (ESF) actuation in the protection and safety monitoring system (PSMS), and diverse RT/ESF actuation in the DAS. Thus, a faulty sensor can send erroneous values to RPS/ESFAS in PSMS and DAS. However, the integrity of the RT logic and ESF actuation logic in RPS/ESFAS cannot be compromised by a single faulty sensor due to 2-out-of-4 configurations for RT and ESF actuations. The DAS also uses 2-out-of-4 configurations for diverse RT and ESF actuations. Thus, a single faulty sensor can not compromise the integrity of any of the four trains of the RPS/ESFAS or DAS.

It is noted that MHI uses only analog sensors for the shared sensors applied to PSMS and DAS. These sensors cannot be adversely affected by the software common cause failure (CCF) postulated in BTP 7-19. Therefore, it is acceptable to use common sensors for the RPS/ESFAS and DAS. As exemplified by the following statements, BTP 7-19 was specifically written to address only software common cause failures:

- Digital instrumentation and control (I&C) systems can be vulnerable to common-cause failures caused by software errors, which could defeat the redundancy achieved by hardware architecture.
- The four-point position in the BTP is based on the NRC concern that software design errors are a credible source of common-cause failures. Software cannot typically be proven to be error-free and is therefore considered susceptible to common-cause failures because identical copies of the software are present in redundant channels of safety-related systems.
- However, despite high quality of design and use of defensive design measures, software errors may still defeat safety functions in redundant, safety-related channels.
- These displays and controls provide plant operators with information and control capabilities that are not subject to common-cause failures due to software errors in the plant's automatic digital I&C safety system because they are independent and diverse from that system.

In addition, sensor diversity is not required per the following statements in SRP Section 7.8-III:

- 10 CFR 50.62 requires diversity from the sensor output
- Equipment diversity is required from the sensors/transmitters
- For mitigating systems other than diverse RTSs (e.g., auxiliary feedwater), diversity is required from the sensors
- Sensors need not be of a diverse design or manufacturer

RAI-02

Provide a description (and figure if necessary) of how sensor values (or signals) are transmitted to the RPS and ESFAS systems.

Response

Topical Report MUAP-07006 is intended to focus primarily on the description of the DAS and its diversity from the RPS/ESFAS within the PSMS. The details of the RPS and ESFAS are provided in Topical Report MUAP-07004, "Safety I&C System Description and Design Process". Figure 4.1-4 of MUAP-07004 shows the sensor interface to the PSMS and the shared signal propagation for RT and ESF functions. The signal processing is described in Section 4.1-b subsections (1) and (2) of MUAP-07004.

In summary, sensor signals which are common to RT/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 RT and ESF function due to 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 RT and ESF function. The voting logic outputs required for RT 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.

RAI-03

Discuss the combining of the RPS and ESFAS into an integrated system and how it impacts the defense-in-depth philosophy and the four echelons of defense against Common Cause Failures (CCFs).

Response

As described in Section 4.1 of Topical Report MUAP-07006, the four echelons of defense in MHI's design are the human system interface system (HSIS), PSMS, PCMS and DAS. Table 4.1-1 of MUAP-07006 shows the correlation between these echelons and the echelons described in the guidance of BTP 7-19. It is noted that MHI does not consider the RPS and ESFAS 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.

Section 5.1 of MUAP-07006 and Section A.5.16 of MUAP-07004 describe the defensive measures used to minimize the potential for CCF within the RPS/ESFAS echelon. This includes redundancy, functional diversity and separation of functions.

The RT and ESF function is maintained by a redundant configuration (4-train system) of PSMS. The four-train configuration, including independence between the redundant trains, is fully described in MUAP-07004.

The defense against CCF through functional diversity and separation of functions within the RPS/ESFAS is described in Section 9.1 of MUAP-07006. In summary, each train of the RPS consists of two separate digital controllers, as shown in Figure 4.1-4 of MUAP-07004. Two or more initiating signals are identified for many postulated events in the safety analysis described in US-APWR DCD Chapter 15. Typical examples of this functional diversity are shown in Table 9.1-1 of MUAP-07006. The actual functional diversity for the US-APWR is shown in DCD Table 7.2-5. A table will be provided by June 2, 2008, to show the functional diversity for each AOO and PA (where functional diversity is available).

These two initiating signals are assigned to the two digital controllers. Each functionally diverse digital controller within a train processes the signal through bistable and voting logic to initiate a RT signal.

It is noted that Draft Interim Staff Guidance (ISG) on Diversity and Defense in-Depth (D3) Task Working Group Problems 3, 4, 5, and 6 in Digital Instrumentation and Control Systems (8/7/2007 ML072190581) states the following:

> *The RTS and ESFAS functions may be combined into a single digital platform if the criteria of the ISG addressing Problems 1 and 2 are met.*

MHI's design complies with the ISG for Problems 1 and 2.

RAI-04

Clarify the type information shared between the RPS and ESFAS. In addition, please explain the operation of the ESFAS given the failure of the RPS to communicate a sensor/calculated value (i.e., will the RPS value be ignored, or will it be interpreted as a trip signal?).

Response

The description of the RPS and ESFAS is provided in Topical Report MUAP-07004. Figure 4.1-4 of MUAP-07004 shows the sensor interface to the PSMS and the shared signal propagation for RT and ESF functions. The signal processing is described in Section 4.1-b subsections (1) and (2) of MUAP-07004.

In summary, 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 which 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.

It is noted that 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.

RAI-05

Discuss the interconnections between the Reactor Trip System (RTS) and ESFAS and demonstrate that the functions required by the Anticipated Transient Without Scram (ATWS) rule (10 CFR 50.62) are not impaired.

Response

The DAS provides the ATWS mitigation function required by the ATWS rule (10 CFR 50.62). The sensor signals required for the DAS function are interfaced from the RPS section of the PSMS. These signals are transmitted to DAS through analog distribution modules and isolation modules in RPS prior to any digital processing within the PSMS. The output signals from the DAS are interfaced directly to plant components (for reactor trip) or to plant components via the Power Interface (PIF) modules within the safety logic system (SLS) section of the PSMS (for turbine trip and emergency feedwater actuation). The PIF modules are conventional devices located after all digital processing within the PSMS. Conformance to the ATWS rule is described in Topical Report MUAP-07006, Appendix B. Appendix B includes Figures B-1 and B-2, which show all signal interfaces between the PSMS and DAS. As shown in these figures, the ATWS functions of the DAS have no interface with the RTS/ESFAS interconnections, which are in the digital processing portion of the PSMS. Therefore, the ATWS functions cannot be affected, in any way, by these digital interfaces within the PSMS.

RAI-06

Discuss the sensor signals, interpreted (converted) sensor values, or calculations based on sensor signals that are transmitted from the Protection and Safety Monitoring System (PSMS) to the ESFAS.

Response

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. This signal processing is described in Topical Report MUAP-07004 Section 4.1-b subsections (1) and (2). A summary description of this processing is also provided in the response to RAI-02.

RAI-07

Provide that portion of the Defense-in-Depth and Diversity analysis that evaluates the four echelons of defense against CCFs that includes the RPS and ESFAS.

Response

The response to RAI-03 describes the four echelons of defense in MHI's design. MUAP-07006 includes the analysis that evaluates these four echelons of defense against CCFs. Section 5.1 of MUAP-07006 describes the "Defenses to Minimize the Potential for CCF". This section is applicable to the HSIS, PSMS and PCMS, which are the three digital echelons for which software CCFs are considered. Despite these defensive measures, that minimize the potential for software CCFs, Section 5.4 describes the "Extent of the Software CCF". This section states, very conservatively, that a software CCF is postulated to coexist in all three digital echelons at the time of an anticipated operational occurrence (AOO) or postulated accident (PA). Section 5.5 describes the "Effects of the Software CCF" on these digital echelons. This section explains the basis of the CCF failure mode considered in the D3 Coping Analysis. Since the software CCF is postulated to adversely affect all digital echelons, the D3 Coping Analysis demonstrates the ability to cope with all AOOs and PAs using only the DAS. Section 7 of MUAP-07006 provides the "Diversity Analysis" which demonstrates that the DAS is not affected by the CCF that is postulated to adversely affect the three digital echelons. Appendix A of MUAP-07006 summarizes the response to Point 1 of BTP 7-19, as follows:

The defense-in-depth and diversity within the MHI I&C system has been assessed in this topical report. The potential for CCF is minimized based on diversity between the echelons of defense and within the echelons of defense. The diversity features within and between each echelon of defense are shown in Table 4.1-1 and 4.1-2. The diversity within the RPS functions of the PSMS is shown in Table 9.1-1.

<u>RAI-08</u>

Discuss the collection and transmission of data to the ESFAS trains.

<u>Response</u>

Please see the response to RAI-06.

<u>RAI-09</u>

Please provide the probabilistic risk assessment (PRA) information including the process, assumptions, data, uncertainties, and types of errors and failures modeled (including maintenance, human errors, recovery factors, CCFs), and results so that the integrated RPS/ESFAS with functional diversity are adequately assessed.

<u>Response</u>

Topical Report MUAP-07006 and Technical Report MUAP-07014, "Defense-in Depth and Diversity Coping Analysis", are intended to fulfill the requirements of BTP 7-19. The PRA is not within the scope of information required by BTP 7-19.

The PRA information of the US-APWR is described in US-APWR Design Control Document (DCD) Chapter 19 and Technical Report MUAP-07030, "US-APWR Probabilistic Risk Assessment". Discussion about CCF is described in chapter 8 "Common Cause Analysis". Also functional diversity and system dependency is described in chapter 4 "System Dependency". (Figure 4.1-12 shows model of functional diversity within the RPS)

<u>RAI-10</u>

Address the issue of a potential software CCF failing both the RPS/ESFAS at the RPS/ESFAS interface.

<u>Response</u>

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.

Regarding the PRA information about CCF, see the response to RAI-09.

RAI-11

Discuss the results of functional diversity vs. separation, including the model, assumptions, data and sources, and comparison to operational experience. Also address hardware and software, such as what is shared, CCFs, etc.

Response

There are many design features or defensive measures to minimize the potential for CCF, including functional diversity and separation, as described in Topical Report MUAP-07006 Section 5.1. The functional diversity and separation of these diverse functions, within the RPS is described in Section 9.1 of MUAP-07006. The functional diversity and separation between the PSMS and PCMS is described in Section 4.2.5 of MUAP-07004.

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.

In addition to the sharing of sensors, bistables and voting functions between the RPS and ESFAS, these subsystems and the PCMS also share a common design for their basic hardware and software components (i.e. the MELTAC digital platform). Section 5.1 of MUAP-07006 describes the defensive measures that minimize the potential for design defects that could lead to CCF in these basic MELTAC components. However to be very conservative MHI assumes a CCF affects and disables all digital control and protection systems controlled by MELTAC, as described in MUAP-07006 Section 5.4.

Regarding the PRA information about modeling of the digital I&C system, see the response to RAI-11.

RAI-12

Clarify the operation of the Power Interface (PIF) Modules and discuss input and output signals, hardware and software components, and system interfaces.

Response

The functional configuration of the PIF module is described in Topical Report MUAP-07006 Section 6.2.4 and Figure 6.2-5. The PIF is also described in Section 4.1.2.4 and Appendix A.8 of MUAP-07005.

Figure 12-1 below and the following description provide additional design clarification. The PIF module consists of three parts (i.e., communication interface part, interposing logic part and switching device part).

It is noted that the DAS output signals are interfaced with the interposing logic part of the PIF module via an isolation module that contains only conventional non-software components. The DAS, the isolation module and the components used for the DAS signal interface within the PIF module, utilize only conventional hardwired circuits. Therefore the DAS function is not affected by any software CCF in the PSMS.

Detailed configuration of PIF module and technical information will be attached to the Topical Report MUAP-07006.

Figure 12-1 Simplified Configuration of PIF Module

RAI-13

Provide details of how the ATWS function is actually implemented. In addition, it appears that there are too few sensors shared by too many systems, including common mode failure. For example, the isolation device(s) could compromise defense-in-depth objective of the design. Address any CCFs of the software of the isolation devices or the sensors. Is a postulated failure or series of failures of any aspect of any channel for these common devices a part of the safety basis of this design? Request you provide information to support the determination that no combination of failed sensors or artifacts of any one or combination of common sensor channels will negatively affect safety system operation due to CCF?

Response

Conformance to 10 CFR 50.62 is described in the Topical Report MUAP-07006 Appendix B. ATWS mitigation functions are provided by the DAS. Figure B-1 of MUAP-07006 shows the implementation of the Turbine Trip and EFW Actuation functions. Figure B-2 of MUAP-07006 shows the implementation of the reactor trip functions. As required by 10CFR50.62, all ATWS mitigation functions of the DAS are diverse from the reactor trip functions of the RPS, with the exception of the input sensors, which are shared by both systems.

A failure of the isolation module cannot compromise the defense-in-depth objective of the design. This is because the isolation module is only used for the diverse function by the DAS. The sensor signal used for the normal function by the RPS does not pass through the isolation module. Therefore, even if there is a CCF within the isolation module, only the DAS would be affected. However, it is noted that the isolation module is a conventional analog device; there is no potential for a software CCF in the isolation module.

Therefore, the only failure that could potentially compromise both the RPS and the DAS would be a CCF of the sensors. Sharing of input sensors is permitted by 10CFR50.62, and sharing of sensors is permitted by BTP 7-19, as long as these sensors are not subject to a software CCF. MHI uses only analog sensors for these functions. These sensors are fully qualified for their accident environment and have many years of proven reliability in nuclear safety applications. Therefore, there is essentially no potential for CCF of these sensors. It is noted that sharing of sensors reduces the hazard that would result from adding additional penetrations into the plant's pressure boundaries to accommodate additional sensors.

RAI-14

Identify the software failure modes for the digital systems, their likelihood, and the effects of their occurrence. Specifically, please address how failure modes other than "fails to function" could impact the actuation and operation of the DAS.

Response

The failure modes and effects of the digital system are described Section 5.5 of MUAP-07006 "Effects of the Software CCF". In summary, the D3 Coping Analysis considers CCFs that result in a fail-as-is (i.e. fails to function) condition in the PSMS and PCMS concurrent with AOOs and PAs. The D3 Coping Analysis does not consider CCFs that result in output state changes (i.e., spurious actuation to the de-energized or energized state) concurrent with AOOs and PAs. The basis for this is that an undetected hidden defect that results in fail-as-is conditions may affect multiple systems over time and may still exist when an AOO or PA occurs. However a hidden defect that results in output state changes is immediately detectable by operators. Operators can correct this defect before it affects multiple systems (i.e. before it becomes a CCF) and prior to an AOO or PA. Software defects that result in spurious actuation of individual systems are evaluated, and are bounded by the AOOs which are considered in the safety analysis.

Therefore, a CCF that results in spurious actuation concurrent with an AOO or PA is not considered in the D3 Coping Analysis. MHI's analysis and design basis are consistent with DI&C-ISG-02 Diversity and Defense-in-Depth Issues, which states:

> *For these reasons, spurious trips or actuations of safety-related digital protection systems resulting from CCFs do not need to be addressed beyond what is already set forth in plant design basis evaluations.*

It is noted that when evaluating the fail as-is (fails to function) condition of the PSMS, it was assumed that the PSMS could be in a mode that is generating output signals that would be considered non-safe. For example, 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 due to 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 due to CCF, this non-safe closed control signal would be maintained.

To accommodate these situations, Section 6.2.4 of MUAP-07006 explains how 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. So, 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 PIF module gives priority to the safe state, regardless of which system PSMS/PCMS or DAS is demanding this state. The PIF priority logic cannot be affected by a CCF in the PSMS/PCMS or a failure in the DAS. So regardless of the failure, the safe state can always be achieved by the operable (non-failed) system.

As described above, fail as-is is the only condition analyzed in the D3 Coping Analysis. However, it is noted that if a failure in PSMS/PCMS resulted in spurious generation of non-safe control signals, the same priority logic in the PIF module would always ensure the DAS can achieve the safe state for all components.

MHI's design of the priority logic within the PIF module is consistent with Interim Staff Guidance DI&C-ISG-04, 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.*

RAI-14a

The staff requirements memorandum to SECY 93-087, dated July 21, 1993, states in full, "inasmuch as common mode failures are beyond design-basis events, the analysis of such events should be on a best-estimate basis." This is different than stating that "common mode failures are beyond design-basis events." This statement does not say that there are not any CCFs that may not need to be considered as single failures as implied by the quote portion of the sentence, but that such events "should be considered on a best-estimate basis." Please address this difference.

Response

MHI agrees that for some safety system designs there may be CCFs that need to be considered single failures. However, MHI's understanding is that the statement in SECY 93-087 "common mode failures are beyond design-basis events" is based on two key assumptions (1) that the system in question meets the separation and independence criteria for Class 1E systems, which ensures single failures cannot propagate between multiple divisions, and (2) the system meets the Class 1E quality and qualification criteria, which minimizes the potential for common design or manufacturing defects. MHI has demonstrated, through MUAP-07004 and MUAP07005, that these assumptions are applicable to the PSMS. Therefore, for the PSMS, there are no CCFs that need to be considered single failures and it is correct to conclude that "common mode failures are beyond design-basis events". This is consistent with Interim Staff Guidance (ISG) on "Diversity and Defense-in-Depth Issues", September 26, 2007. The ISG says;

> *Since digital system CCFs are not classified as single failures, postulated digital system CCFs should not be assumed to be a single random failure in design basis evaluations. Consequently, best-estimate techniques can be employed in performing analyses to evaluate the effect of digital system CCFs coincident with design basis events.*

RAI-14b

Did the Failure Mode and Effect Analysis (FMEA) consider failure mechanisms that are recognized as being highly unlikely, but could affect multiple components? Without the FMEA table included in the topical report, it is not apparent that all components and failure modes have been considered. Does the FMEA systematically identify and evaluate the failure modes for all components and include failure modes such as loss of function, but also low or high values, timing issues, maintenance, etc.?

Response

As explained in the response to RAI-14, the failure modes and effects of the digital system are described Section 5.5 of MUAP-07006 "Effects of the Software CCF". This section considers failures which result in fail as-is output conditions, and failures which result in spurious output state changes (to safe or unsafe states). These three conditions bound all PSMS failure modes regardless of what may have been the failure initiator. The D3 Coping Analysis addresses the failures that result in a fail as-is condition. The plants safety analysis considers failures that result in spurious output state changes.

RAI-14c

Did the FMEA consider the coincident occurrence of otherwise single failures (i.e., multiple failures, such as software CCF, loss of all power, fire, flood)?

Response

The effects of software defects are considered in the D3 Coping Analysis and in the plant's safety analysis, as described in the response to RAI-14b. The safety analysis also considers loss of all power to a single PSMS division and spurious actuations which may result from credible single failures. Based on the PSMS architecture these are limited to spurious actuations of single controller groups (i.e. redundant controller pairs). The safe shutdown analysis for fire conditions, DCD Appendix 9A, considers spurious actuation of one or more control functions in one PSMS division. Flooding is not considered a credible failure due to the location of I&C equipment (away from pipe break hazards), design of I&C cabinets (which prevents water intrusion) and floor drains in I&C equipment locations.(Flood protection concept is described in DCD 3.4.1)

RAI-15

Please confirm that the DAS functions and other Defense-in-Depth and Diversity - related functions are consistent with the portions of the accident analysis that support the Defense-in-Depth and Diversity analysis.

Response

There are primarily two areas of consistency required between the functions described in MUAP-07006 and the accident analysis:

1. As discussed in the response to RAI-03, MHI credits functional diversity to minimize the potential for CCF in the PSMS. However, functional diversity within the PSMS is not credited in the D3 Coping Analysis. To be very conservative the D3 Coping Analysis assumes the CCF affects and disables all digital control and protection systems in their entirety, including those that are functionally diverse. The defense against CCF through functional diversity and separation of functions within the RPS/ESFAS is described in Section 9.1 of MUAP-07006. Typical examples of this functional diversity are shown in Table 9.1-1 of MUAP-07006. The actual functional diversity for the US-APWR is shown in DCD Table 7.2-5. A table will be provided by June 2, 2008, to show the functional diversity for each AOO and PA (where functional diversity is available).

2. The D3 Coping Analysis in Technical Report MUAP-07014 demonstrates conformance to the acceptance criteria of BTP 7-19 for each AOO and PA described in the accident analysis, with a concurrent CCF in the RPS/ESFAS. Many assumptions for each event are consistent with the assumptions of the safety analysis. However, some assumptions differ since the D3 Coping Analysis uses best estimate methods, as allowed by BTP 7-19. Any differences are explained and justified in MUAP-07014.

RAI-16

Identify any and all common components between and within the RTS, ESFAS, and DAS divisions and systems. Discuss the CCF susceptibilities for these common components and address their likelihood of occurrence.

Response

The ESFAS receives its inputs from the RPS, so almost all RPS components are also common to ESFAS. In addition, the RPS and ESFAS utilize the same MELTAC platform, which includes the basic hardware and software design. Section 5.1 of MUAP-07006 and Section A.5.16 of MUAP-07004 describe the defensive measures used to minimize the potential for CCF within the RPS and ESFAS. Because of these defensive measures, there is minimal potential for CCF.

The only common components for normal / diverse reactor trip function in DAS and PSMS (RPS) are sensors. MHI uses only analog sensors for these functions. These sensors are fully qualified for their accident environment and have many years of proven reliability in nuclear safety applications. Therefore, there is essentially no potential for CCF of these sensors.

Common components for normal / diverse ESF actuation function in DAS and PSMS (RPS, ESFAS, and SLS) are sensors and PIF modules. Sensors are discussed above. PIF modules are discrete digital devices; therefore there is no susceptibility to software CCF. PIF modules are very simple binary logic/switching devices, therefore there is minimal potential for other CCFs in these devices. It is noted that, as explained in MUAP-07006 Appendix B and shown in Figure B-2, the PIF module is not used by the RPS for normal reactor trip functions. So there is no commonality between RPS and ATWS mitigation functions.

The description for common sensor is described in Topical Report MUAP-07006 Section 5.2. The detail description for common PIF module is described in Topical Report MUAP-07006 Section 6.2.4 and 9.4.

RAI-17

What measures are used to reduce or limit the potential for inadvertent actuation and challenges to the diverse instrumentation and controls safety systems?

Response

Topical Report MUAP-07006 Section 5.6 describes the features of the DAS that minimize the "Potential for Adverse Interaction" with the PSMS, due to inadvertent actuation. The following is a summary of those features:

- 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 reactor trip. The blocking function uses status signals that are directly obtained from actuated components. This ensures 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. This blocking function is shown in Section 6.2.2.2 of MUAP-07006.

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.

Therefore, spurious actuation signals from DAS, which correspond to a non-preferred state, cannot block the PSMS from achieving the preferred safe state. The PIF module is described in the response to RAI-12.

Multiple sections of Topical Report MUAP-07004 describe features of the PSMS that prevent spurious actuation of the RPS and ESFAS. The following is a summary of those features:

- 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 Safety Logic System (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.

As discussed above, the PIF modules in the PSMS ensure that even if a spurious actuation of an SLS controller group occurs (which generates control signals corresponding to the non-preferred safe state of a plant component), spurious actuation cannot prevent the DAS from positioning the plant component to the preferred safety state.

RAI-18

Once initiated, will the ATWS mitigation logic and DAS the mitigation function go to completion?

Response

As described in Topical Report MUAP-07006 Section 6.2.2.1 (2), once initiated, the DAS functions are latched. Therefore, all DAS mitigation functions for all AOOs (including ATWS) and PAs will go to completion.

RAI-19

Provide a listing of Anticipated Operational Occurrence (AOO)s and Postulated Accident (PA)s considered in the design of the diverse instrumentation and control systems and identify the potential concurrent CCFs that can disable or cause erratic or erroneous operation of the PSMS and PCMS. Discuss the effects of those failures.

Response

The list of AOOs and PAs for the US-APWR are described in DCD Chapter 15. These same events are analyzed with concurrent CCFs in Technical Report MUAP-07014. This report considers CCFs that affect only the PSMS and CCFs that affect both the PSMS and PCMS.

RAI-19a

The coping analysis does not consider CCFs that result in output state changes (i.e., spurious actuation to de-energized or energized state).

Response

This statement is correct. For the basis of this, please see the response to RAI-14.

RAI-20

Identify and discuss those cases where functional diversity does not exist within the PSMS for each AOO and PA.

Response

As discussed in the response to RAI-03, MHI credits functional diversity to minimize the potential for CCF in the PSMS. However, functional diversity within the PSMS is not credited in the D3 Coping Analysis. To be very conservative the D3 Coping Analysis assumes the CCF affects and disables all digital control and protection systems in their entirety, including those that are functionally diverse.

RAI-21

Identify and discuss those events where the signal used to produce a reactor trip is not diverse from the signals for ESF actuation.

Response

As explained in the response to RAI-04, the ESFAS receives its inputs from the RPS. Therefore, the same sensors, bistables and voting logic are used for both functions. As explained in the response to RAI-03, the RPS and ESFAS are not separate echelons of defense, but rather complimentary echelons. A common cause failure of the RPS/ESFAS echelon is accommodated by the DAS.

RAI-22

Provide or discuss the Defense-in-Depth and Diversity Coping Analysis, along with a reference. Include a listing and explanation of events under each category of "equivalent protection," expertly judged," and "analyzed."

Response

Topical Report MUAP-07006 is intended to provide the D3 Coping Analysis generic methodology, not the specific coping analysis for a particular plant. As stated in the Abstract of MUAP-07006, "The D3 Coping Analysis for specific plants, which is based on the generic methods described in this topical report, is provided in Plant Licensing Documentation." The essence of this statement is reiterated in Section 3.4(6), Section 8.1, Table 10.0-1 and Appendix A (Point 2) of MUAP-07006.

The "Plant Licensing Documentation" for the US-APWR is technical report MUAP-07014, which is referenced in Section 7.8 of the US-APWR DCD. Mitsubishi Nuclear Energy Systems, Inc. (MNES) submitted technical report MUAP-07014, "US-APWR Defense-in-Depth and Diversity Coping Analysis" for NRC review by letter dated December 31, 2007 (Ref. ML080280404). MUAP-07014 describes the Defense-in-Depth and Diversity (D3) coping analysis for the US-APWR in support of the D3 design information provided in the US-APWR design certification application. This technical report provides an evaluation of each event in Chapter 15 of the US-APWR DCD. The original version of technical report MUAP-07014, version R0, did not categorize plant events in accordance with the methodology described in MUAP-07006. MUAP-07014 is currently being revised to include this categorization. This revision will be submitted to the NRC by June 20, 2008.

The following explanation is provided to help in understanding how each of the DCD Chapter 15 events will be mapped to one of the three groups reiterated in the RAI text above ("equivalent protection," expertly judged," and "analyzed").

The left column of Table 22-1 below identifies the five event categories currently defined in Section 4.6 of MUAP-07014. These categories describe the response of a given DCD Chapter 15 event to a loss of normal reactor trip and ESFAS actuation. The first category is used for events that have sufficiently low initiating event frequency and diverse means of early warning detection. An example of such an event is the double-ended large break LOCA for which diverse leak detection is provided to prompt actions that further minimize the potential for this event. The D3 coping analysis demonstrates that the diverse leak detection system provides adequate coverage for the pipe breaks under consideration, and that there is sufficient diverse HSI to achieve and maintain hot shutdown from the diverse HSI panel (DHP). The D3 coping analysis also demonstrates the ability to achieve and maintain cold shutdown using the DHP and local controls (as required). The design attributes for local controls credited in the D3 Coping Analysis, including immunity from the CCF and state based priority, will be added to the next revision of MUAP-07006. Therefore, Category 1 is considered to be in the "expertly judged" group.

There are a number of DCD Chapter 15 events that do not result in a reactor trip or ESFAS mitigating action and that have been shown to meet the AOO acceptance criteria in the conservative DCD analysis. These events are classified in the coping analysis as Category 2. If these events were reanalyzed with an assumed common-cause failure of the reactor trip and ESFAS actuation, and no CCF in the PCMS, their response would be identical to the DCD because no trips or ESFAS signals are assumed in the DCD Chapter 15 analysis, and the PCMS is assumed to fail in the worst case condition. An example of such an event is the increase in main steam flow event. Similar to Category 1, no transient analysis is performed for the coping analysis, and Category 2 is considered to be in the "equivalent protection" group defined by topical report MUAP-07006-P.

There are three normal automatic reactor trip functions that are duplicated by the Diverse Actuation System (High Pressurizer Pressure, Low Pressurizer Pressure, and Low Steam Generator Water Level). For events in DCD Chapter 15 that credit these specific reactor trips, if a common-cause failure disabled the normal automatic reactor trip or ESFAS actuation functions, an automatic DAS trip would occur on the same trip function. The loss of normal feedwater flow event is an example of such an event (normally trips and initiates EFWS on Low Steam Generator Water Level). However, the DAS trip setpoints are less conservative than the RPS/ESFAS setpoints and they are delayed by 10 seconds. Similar to Category 1 and 2, for most events in Category 3 there is no transient analysis performed for the D3 coping analysis. Instead, the additional effect of setpoint/delay is "expertly judged" to have minimal impact on the event scenario. Therefore, most events in Category 3 are considered to be in the "expertly judged" group defined by topical report MUAP-07006-P. If the effect of the setpoint/delay cannot be "expertly judged" to have minimal impact, the event is "analyzed".

There are groups of events that, when analyzed without automatic reactor trips, will approach the same or similar condition; if one of these events is analyzed and found to meet the acceptance limit, all of them will meet the same limit. The RCP locked rotor and RCP sheared shaft events are examples of this. The limiting core condition for both of these events in the absence of an automatic reactor trip occurs at the same or similar condition after the reactor coolant pump comes to a complete stop. In such cases, the D3 coping analysis technical report provides a transient analysis for one of the events (assigns it to Category 5 or "analyzed" group) and assigns the other similar events to Category 4 ("expertly judged" group). Table 4.6-1 in the D3 coping analysis technical report MUAP-07014 provides the list of Chapter 15 events with a summary of the basis for individual event categorization. The next revision of MUAP-07014 will provide the detailed basis for concluding that the BTP 7-19 acceptance criteria has been met for each event.

Table 22-1: D3 Coping Analysis Categories and D3 Topical Report Groups

D3 Coping Analysis Category		D3 Topical Report Group
Category 1	Event has a very low probability of occurrence	"expertly judged"
Category 2	RTS and/or engineered safety features (ESF) not actuated and no adverse impact	"equivalent protection"
Category 3	Event mitigated by DAS and no adverse impact	"expertly judged" or "analyzed"
Category 4	Event similar to other event and no adverse impact	"expertly judged"
Category 5	Analysis required and results show acceptance criterion is met	"analyzed"

RAI-23

Discuss the ability to detect and mitigate each AOO or PA using the DAS for Type 1, 2, and 3 Failures, including a discussion of sensor diversity within the PSMS for each AOO and PA.

Response

Per NUREG/CR-6303 Type 1 failures are control system failures that result in plant transients that require protective actions for mitigation. Section 7.3.1 of MUAP-07006 explains the basis for concluding that all PCMS failures are bounded by the AOOs analyzed in Chapter 15 of the Safety Analysis. The ability to detect and mitigate each AOO, concurrent with a CCF that affects the PSMS or a CCF that affects the PSMS and other sections of the PCMS, using the DAS, is described in the D3 Coping Analysis MUAP-07014.

Per NUREG/CR-6303 Type 2 failures do not directly cause plant transients but are undetected failures that are manifested only when a demand is received to actuate a component or system. As explained in Section 7.3.2 of MUAP-07006, the PSMS and PCMS are assumed to have Type 2 failures when an AOO or PA occurs. The ability to detect and mitigate each AOO or PA, concurrent with a CCF that affects the PSMS or a CCF that affects the PSMS and the PCMS, using the DAS, is described in the D3 Coping Analysis MUAP-07014.

Per NUREG/CR-6303 Type 3 failures occur because the primary sensors expected to respond to a design-basis event produce anomalous readings. As explained in the response to RAI-03, the defense against this CCF is provided through functional diversity in the RPS/ESFAS. Defense for this failure is not provided in the DAS. Within the RPS/ESFAS two or more diverse initiating signals are identified for many events in the safety analysis described in US-APWR DCD Chapter 15. Typical examples of this functional diversity are shown in Table 9.1-1 of MUAP-07006. The actual functional diversity for the US-APWR is shown in DCD Table 7.2-5.

RAI-24

Discuss the operating experience of the PSMS, PCMS, and DAS, including, but not limited to, identifying any failures, detectable failures, diagnostics, failure modes.

Response

The MELTAC platform is applied to the PSMS and PCMS. The history of the MELTAC platform is described in Section 7.1 of MUAP-07005. In summary, as of the date of that document (July 2007), the MELTAC platform had accumulated more than 20,000,000 operating hours in nuclear applications since 1987. The platform continues to be operational in more than 50 applications in five nuclear power plants. MELCO tracks and evaluates all failures in accordance with their corrective actions program described in Section 6.2.2 of MUAP-07005. As stated in Section 7.1 (d) "No plant system has ever suffered shutdown due to software- or hardware-related problems."

The self-diagnostic functions within the MELTAC platform are described in MUAP-07005, as follows:

- Controller – Section 4.1.5
- VDU – Section 4.2.3
- Communications – Sections 4.3.2.4 and 4.3.3.3

Section 7.4 of MUAP-07005 describes the Failure Mode and Effects Analysis (FMEA) methodology for MELTAC components. This methodology defines the failure modes at the controller level. As stated in this section, failures that "affect the control function must be detected either by the self-diagnosis function ...or by the Application Software." Therefore there are no undetectable failures. Section 6.5.1 of MUAP-07004 describes the FMEA methodology applied at the system level for safety system applications that use the MELTAC platform (e.g., PSMS). For the US-APWR, the FMEA analysis for the RPS and ESFAS are provided in DCD Sections 7.2.3.1 and 7.3.3.1, respectively. These FMEAs demonstrate conformance to the single failure criteria and to the fail-safe requirements of each system.

The operating history of DAS components is described in Section 6.2.1.7 of MUAP-07006. In summary, the DAS uses analog and relay components that are common in Japanese conventional non-digital safety systems. As stated in this section, the DAS is designed and manufactured using a nuclear quality program that conforms to 10 CFR 50 Appendix B. This program includes documented error reporting, tracking and corrective actions.

As stated in Section 3.3 (1) of MUAP-07006 the DAS conforms to the testing criteria for Protection System Actuation Functions (i.e., all DAS functions can be tested). Specific test functions are described in Sections 6.2.1.4 and 6.2.2.3(3) of MUAP-07006. As stated Section 3.6(1) of MUAP-07006 the DAS is not a source of single failure that can adversely affect the safety systems. In addition, the DAS is designed so that credible single failures, including failures resulting from fire and seismic events, will not cause spurious actuations that could adversely affect safety functions. These failure mode conclusions are the result of independence between the 2-out-of-2 DAS subsystem configuration, and the DAS Seismic Category II classification.

RAI-24a

Please discuss whether the failure mode "disables" is limited to "fails" such that no signal is generated or does it include false signals.

Response

The D3 Coping Analysis addresses the CCFs that result in a fail as-is condition. The plants safety analysis considers failures that result in spurious output state changes. Please see the response to RAI-14 and 17. As explained in these responses, the PIF module gives priority to the control signal that will put the component in its safe state. So regardless of the PSMS or DAS failure mode (fail as-is, or fail with spurious output state changes), the safe component state can always be achieved.

RAI-25

This does not account for the transmittal of a faulty signal or value. Because of the shared PIF modules, are there any postulated CCFs that could prevent the proper operation of the PSMS and PCMS and impact the DAS?

Response

The configuration and state based priority of PIF module are described in the responses to RAI-12 and RAI-14.

The common part of the PIF module, which is utilized by the PSMS/PCMS and DAS, is not susceptible to software CCF because the common part consists of only conventional binary components. In addition, if a faulty signal is generated by PSMS/PCMS or DAS, the state based priority logic, within this part of the PIF module, ensures actuation to the predefined safe state of the component cannot be blocked by that faulty signal. Thus, the shared PIF module does not prevent the proper operation of the PSMS and PCMS and does not impact the DAS, due to software CCF.

It is noted that BTP 7-19 requires consideration of software CCF, and therefore permits the use of common non-software based devices between RPS/ESFAS and DAS. However, the ATWS rule 10CFR50.62 requires consideration of all CCFs (i.e. hardware and software) for diversity between RT and ATWS mitigation functions. Based on this, the PIF module is used only for ATWS mitigation functions; it is not used for RT functions.

RAI-25a

The only failure mode evaluated in the coping analysis is "fail as is." Please discuss that other failure modes are not considered.

Response

The failure modes and effects of the digital system are described Section 5.5 of MUAP-07006 "Effects of the Software CCF". In summary, the D3 Coping Analysis considers CCFs that result in a fail-as-is (i.e., fails to function) condition in the PSMS and PCMS concurrent with AOOs and PAs. The failure mode that results in output state changes is detectable and can be corrected before it affects multiple systems (i.e. before it becomes a CCF) and prior to an AOO and PA. Therefore, failures that result in output state changes of individual systems are considered single failures. Single failures are considered in the plant's safety analysis.

Please see the response to RAI-14.

RAI-26

Identify and explain any differences and changes with an explanation on why the change is appropriate from the Chapter 15 analysis compared with the best estimate analysis for each AOO.

Response

From an instrumentation and control system perspective, the "Major differences between the Chapter 15 Safety Analysis and the D3 Coping Analysis" are provided in Section 8.1 of MUAP-07006. These are repeated here:

- All the safety functions of the digital safety system are considered to be disabled by a CCF.
- Any single failure assumption in systems and components is not applied.
- Any action of the control system which mitigates the event is not considered.
- Normal control actions which may lead the event to an adverse situation are considered.
- Spurious actuations of control or safety systems which may lead the event to an adverse situation are not considered.
- Off-site power is available through the event except the Loss of Offsite Power event.
- The plant is at nominal operating conditions, not at the outside limit of any control band or operating limit.
- All systems and equipment are operable, with the exception of equipment that is licensed for unlimited bypass or out of service. Equipment licensed for unlimited bypass or out of service is assumed to be inoperable.

Bullet three, above, is intended to cover the case where the PSMS CCF also affects all of the control functions of the PCMS. Bullet four is intended to cover the case where the PCMS is unaffected by the CCF. These assumptions are different from the Chapter 15 analysis, which examines each control system to define the worst case aggravating condition (i.e. normal automatic control or manual control). Section 8.1 of MUAP-07006 will be revised to clarify these points.

It is noted that the current version of MUAP-07014 assumes that for all AOOs and PAs SG water level control is unaffected by the CCF. This is because the SG water level control system is very critical in maintaining a continuous feed-flow steam-flow balance. SG water level control system malfunctions induced by software defects (fail as-is or output state changes) will immediately affect the regulation of the water level, which will cause plant alarms/trips from DAS. Therefore, the self announcing nature of this control system failure will be immediately detected. These software defects will be corrected prior to AOOs or PAs. Detailed evaluation of the feedwater control behavior based on actual plant data will be supplied in June 2, 2008.

Additional key differences from the Chapter 15 analysis, from the plant perspective, are described below. These will be added to the next revision of MUAP-07006.

1. Reactor Operating Mode

   The Chapter 15 safety analysis considers worst case operating conditions, which include low power and refueling conditions. In the D3 coping analysis, the plant is assumed to be operated at rated power. This assumption covers most of the operational time interval of the plant which means this assumption covers the most likely plant conditions for events with concurrent CCF.

2. Core Conditions

   - In the Chapter 15 analysis, all transients are assumed to begin with the most severe power distributions that are within the technical specifications. In general, the axial power distribution in the D3 Coping Analysis is assumed to be consistent with the core burn-up.

Any exceptions to this are noted in the analysis.

- In the Chapter 15 analysis maximum and minimum core characteristics are chosen in combinations that result in the most conservative event results. These combinations do not always correspond to realistic plant conditions. In the D3 coping analysis the moderator temperature coefficient is assumed to be the realistic negative values based on the core design that the moderator temperature coefficient is less than 0 pcm/°F in hot zero power condition at the Beginning Of Cycle (BOC). This assumption is consistent with technical specifications, which require verifying the moderator temperature coefficient is within the upper limit prior to entering MODE 1 after each refueling.

- In the D3 coping analysis, the Doppler power coefficient and the Doppler temperature coefficient are assumed considering 20% margin on the core design value. This margin is smaller than the margin used in the DCD Chapter 15 safety analyses, but this is still a conservative value.

3. Equipment Capacity
   The Chapter 15 analysis uses worst case conservative capacities for safety injection system and emergency feedwater system (e.g. flow rates). The D3 coping analysis uses nominal capacities.

The US-APWR D3 Coping Analysis, MUAP-07014, explains how these generic changes affect the Chapter 15 analysis for each plant event.

RAI-27

Identify and explain any differences and changes with an explanation on why the change is appropriate from the Chapter 15 analysis compared with the best estimate analysis for each PA.

Response

Please see the response to RAI-26.

RAI-28

Did the Defense-in-Depth and Diversity coping analysis evaluate CCFs, disabling the two separate scenarios; the reactor trip functions and then the ESFAS functions, that cause spurious actuations as well as preventing actuations? Did this assume that, by providing a diverse means of protection, this did not effect the DAS?

Response

The AOOs and PAs analyzed in the US-APWR D3 Coping Analysis, MUAP-07014, consider concurrent CCF in the PSMS including RPS and ESFAS, as the worst case bounding condition. This is based on the following:

1. As explained in the response to RAI-02, signals that actuate the ESFAS originate in the RPS. Therefore, a CCF that disables the RPS also disables the ESFAS.

2. As explained in RAI-14, CCFs occur over time. Therefore, it is possible that a software defect could result in a CCF in the ESFAS, prior to it affecting the RPS. Although very unlikely, an AOO/PA could occur during this interval. So, the AOO/PA could occur with a

concurrent CCF in the ESFAS and not a concurrent CCF in the RPS. The RPS actuates on the same parameters as the DAS, and on more parameters than the DAS. Therefore, the consideration of only DAS trip functions in the D3 Coping Analysis is the most limiting condition. Reactor trips generated by the RPS that may occur prior to the trips assumed for the DAS would improve all D3 coping analysis results.

The failure modes and effects of the digital system are described Section 5.5 of MUAP-07006 "Effects of the Software CCF". As explained in the response to RAI-14, the only failure mode of the PSMS evaluated in the D3 Coping Analysis is "fail as is." Spurious actuations of the PSMS are self-announcing and corrected prior to becoming CCFs, therefore they are considered single failures in the plant's safety analysis.

RAI-29

Please identify all shared hardware and software between the RPS/ESFAS and the DAS (including the PIF Modules) and discuss the effects of its failure, including CCF susceptibilities. Discuss whether other failure modes besides "disable" were addressed. If not, please discuss why "disable" is the only failure mode addressed and the appropriateness of this assumption.

Response

As described in the response to RAI-16, shared hardware between the PSMS (including RPS/ESFAS) and DAS for normal and diverse functions is limited to sensors and PIF modules. These devices are not affected by software CCF, as described in the response to RAI-16. Therefore, CCF is not considered in these devices. Single failures in these devices, including fail as-is and spurious state changes, are accommodated through the four train redundancy of the PSMS. These single failures are considered in the plant's safety analysis. In addition, due to the 2-out-of-4 voting logic in the DAS, the DAS will not spuriously actuate due to any single sensor failures.

DAS consists of conventional analog device so that there is no shared software between the PSMS and DAS.

RAI-30

In those cases where plant response analysis shows that the protective action is not required for at least 30 minutes, the protective action may be performed by manual operator actions. Demonstrate that sufficient information and controls (safety or non-safety), independent and diverse from the RPS, are provided in the main control room, and that the information displays and controls are not subject to the same CCF. For those events where manual operator actions are required before 30 minutes, please demonstrate that sufficient information and controls are provided, and discuss any possible conflicts in training and procedures for evaluating when to take action prior to 30 minutes.

Response

The US-APWR D3 Coping Analysis, MUAP-07014, defines the specific information and controls used for all credited manual operator actions for each specific plant event. In general, these devices are part of the DAS Human Systems Interface (HSI) Panel (DHP). The DAS, including all HSI components on the DHP, are analog. Section 7 of MUAP-07006 provides an analysis to demonstrate that the DAS, including the DHP, is not subject to the software CCF (postulated by BTP 7-19), that adversely affects the digital RPS/ESFAS. If the D3 coping analysis credits any other HSI (i.e. not on the DHP) the immunity of that HSI from the postulated CCF is separately justified in the D3 coping analysis.

Manual actions for event mitigation with a concurrent CCF are based on simple Special Event EOPs which cover immediate mitigation actions and subsequent actions. The use of Special Event EOPs is supported by simulator training and on-going Human Performance Monitoring. The following is a general description of how manual actions are credited:

As described in DCD Section 7.8 and Topical Report MUAP-07006 Section 6, generation of a DAS system level actuation signal (reactor trip, turbine trip, MFW isolation, or EFW actuation) also actuates an audible summary alarm on the diverse HSI panel (DHP). In addition, the DHP provides indication of the specific input parameter that caused the system level actuation (high pressurizer pressure, low pressurizer pressure, or low steam generator water level). These are referred to as first-out alarms in Section 6.3.2.1(4) of MUAP-07006.

Since the DAS actuation is delayed, and is blocked if the RPS actuates correctly, these alarms will not occur under non-CCF conditions. These alarms are redundantly processed using 2-out-of-3 logic taken twice (2-out-of-2), to minimize the potential for erroneous nuisance alarms. Therefore, these unique alarms prompt immediate entry into Special Event Emergency Operating Procedures (EOPs) with no prior event or alarm diagnosis.

Based on the unique prompting alarm, the operator starts taking "immediate CCF post- trip action" using the indications and controls on the DHP. For the US-APWR the specific indications and controls are defined in Tables 7.8-2 and 7.8-4 of the DCD. The "CCF immediate post-trip actions" are described as follows.

- Verify both the reactor and the turbine have tripped (through neutron flux and main steam line pressure indications on the DHP)
- Verify sufficient emergency feedwater into each SG (through SG water level indications on the DHP)
- Control EFW flow rate using the DHP T_{cold} indicator and EFW control valves
- Event specific immediate action(s) based on the first-out indication

Although most events will be mitigated or terminated at the stage of "CCF immediate post-trip action", the procedures direct the operator to continue to monitor the event following the post-trip action to ensure that plant conditions stabilize.

To illustrate manual actions SBLOCA and SGTR events are described below:

The DAS automatic low pressurizer pressure trip will trip the reactor for a SGTR or a SBLOCA with a concurrent CCF. The operator will detect an event with CCF based on the unique DAS actuation alarm on the DHP. Then the operator will take "immediate CCF post-trip actions".

For the SGTR or SBLOCA the DHP first-out indication will be "low pressurizer pressure". Based on this indication, the Special Event Emergency Operating Procedures (EOPs) will direct the operator to manually start the SI pump from the DHP. Based on the Special Event EOP, another operator will be directed to check the radiation monitoring system (RMS) board located outside the main control room (MCR). RMS indication alerts the operator to a SGTR occurrence and that operator identifies the ruptured SG to the operator at the DHP. This conclusion can also be confirmed by comparing the SG water levels on the DHP. The operator in front of the DHP will manually terminate the EFW into the ruptured SG. This action must be taken approximately 40 minutes from the initial DAS trip and prompting alarm. This time would be approximately 30 minutes from the DAS prompting alarm for the case of the CCF also affecting the PCMS, including the SG water level control system. The operator will take additional procedure-based actions following the termination of EFW. Later in the event, the operator can also use information on the DHP to monitor subcooling margin for the purpose of terminating SI flow and controlling the secondary cooldown using the intact steam generators.

A similar series of automated actions, alarms, indications and manual actions (in response to decreasing pressurizer pressure), occurs for a SBLOCA with CCF. However, in this case the radiation monitoring system (RMS) board outside MCR does not indicate the occurrence of an SGTR. The operator who checks the RMS will notify the operator at the DHP that no SGTR has occurred. SBLOCA is almost terminated at this stage.

In summary, 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 MCR or outside the MCR, are supported by a thermal hydraulic analysis, which defines the Time Available for the operator action, and a human factor engineering (HFE) analysis, which defines the Time Required to take the action. Sufficient margin is demonstrated between Time Available and Time Required to ensure the feasibility of the manual action with high confidence.

During the COL stage, when EOPs have been developed and a simulator is available, the ability to take these manual operator actions will be validated. During plant operation, ongoing operator training and human performance monitoring will support the required actions times.

RAI-31

Containment level sump level and airborne particulate radioactivity monitoring are diverse methods of detecting a reactor coolant pressure boundary leak. What third methods are under consideration?

Response

As stated in Section 6.2.3 (5) of MUAP-07006. "The third method is plant specific and will be identified in Plant Licensing Documentation." For the US-APWR, the third method is defined in Section 7.8.1.1.4 of the DCD as "Containment Air Coolers Condensate Flow Rate".
As stated in Section 7.8.1.1.4 of the DCD, at least one of the three functions is implemented in the DAS to monitor RCS leakage.

Section 6.2.3(5) of MUAP-07006 will be revised to be consistent with the DCD, as follows:

> At least one of these monitoring functions is implemented in the DAS with diversity from the PSMS. Therefore this function(s) is not affected by a CCF that disables the PSMS.
>
> If a small leak should occur in the RCS, the leak detection alarm(s) and indicator(s) prompt manual operator actions that allow the plant to be shutdown before the small leak can degrade. This manual operator action minimizes the potential for a LBLOCA coincident with a CCF in the PSMS.

RAI-32

Provide justification on why the PIF Module is not susceptible to a CCF.

Response

The PIF module is described in the response to RAI-12 and Topical Report MUAP-07006 Section 6.2.4. The common part of the PIF module uses only conventional binary logic components (i.e. no software). Therefore, the common part of the PIF module is not subject to software CCF. It is suitable for use by both the PSMS and DAS, when conducting the coping analysis for AOO/PA with concurrent software CCF, as required by BTP 7-19.

As explained in Appendix B of MUAP-07006, the PIF module is susceptible to hardware CCF. Therefore, it is used for ATWS mitigation functions, but not used by the RPS.

RAI-33

Please clarify the definition "higher level in the system architecture."

Response

The words "higher level in the system architecture" are in MUAP-07006 Section 6.2.4. Hardware based logic within the PIF module is used to prioritize component control signals between the PSMS controller outputs and the outputs from the DAS. These words pertain to the software based logic, which is used in the PSMS to prioritize safety signals over non-safety signals that originate from the PCMS. Control signals are processed through this software priority logic prior to being processed by the priority logic in the PIF module. The PIF module provides the last logic processing prior to the plant component. Therefore, this priority logic is considered to be at a "higher level in the system architecture".

In the overall architecture of the I&C system shown in Figure 4.0-1 of Topical Report MUAP-07006, the unit bus is located in the upper level, which is above the controllers of the PSMS. All non-safety control signals, except those from DAS, interface to the PSMS controllers via the unit bus. Within the PSMS controllers software logic prioritizes all safety signals (regardless of state or function) over all non-safety signals.

RAI-34

Does the statement "safety signals from within the PSMS always have priority over signals from all non-safety equipment, with the exception of DAS which uses state based priority" mean that other nonsafety signals (besides the DAS) transmit/receive data, communicate, or interface with the PSMS?

Response

Yes, this is correct. The overall I&C system description and configuration are described in Topical Report MUAP-07004 Section 4.0. The PSMS interfaces with the non-safety PCMS. These interfaces are described in Section 4.2.5 and 5.1.1 of MUAP-07004.

The PSMS interfaces with the non-safety PCMS for various control and indication functions. For example, safety signals in the PSMS are transferred to non-safety system for interlock of non-safety component or for indication on Operational VDU (non-safety HSI). In addition, the PSMS receives non-safety signals, such as non-safety interlock signals and manual control signals from Operational VDUs. Class 1E priority logic software within the PSMS ensures these non-safety signals cannot adversely affect any safety functions due to normal control states or failure control states. The priority logic and the design of the PSMS/PCMS digital data communication interface conform with the requirements of DI&C-ISG-04.

RAI-35

Please discuss why it is ok to use the same sensors for PSMS/ESFAS and DAS, with all signals then being transmitted to a common PIF Module.

Response

The response to RAI-01 explains how the design of the PSMS and DAS accommodate single sensor failures. The 2-out-of-4 voting logic in both systems ensures a single sensor failure will not prevent actuation of any division in either system, nor cause spurious actuation of any division in either system.

The response to RAI-16 explains that MHI uses only well proven analog sensors, therefore there is minimal potential for sensor CCF. The response to RAI-23 explains the functional diversity within the RPS that provides defense-in-depth for this low probability CCF. However, it is noted that sensor CCF is outside the scope of 10CFR50.62 and outside the scope of BTP 7-19.

As explained in the response to RAI-25, the PIF module is not subject to software CCF; therefore it is acceptable for use in meeting the requirements of BTP 7-19. The PIF module is a very simple device, so it is also unlikely to have any hardware based CCF. Regardless, CCF of the PIF module is considered in the design basis, so it is not commonly used in the RPS and the ATWS mitigation functions of the DAS.

RAI-36

Is there a communication independence between the PSMS and the DAS?

Response

As described in Topical Report MUAP-07006, 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, as described in Section 6.2.1.3 of Topical Report MUAP-07006. These isolation devices are part of the PSMS and therefore meet all fault isolation requirements of RG 1.75 and IEEE-384. Thus there is communication independence between the PSMS and the DAS. Since communication isolators are part of the PSMS, they are described in numerous sections of MUAP-07004.

RAI-37

Please address handshaking or communication that would compromise functional independence of the PSMS and DAS.

Response

Please see the response to RAI-36.

Only conventional analog or binary signal interfaces are used between PSMS and DAS. Therefore, there is no handshaking or communication that would compromise functional independence of the PSMS and DAS.

RAI-38
Please discuss the "conventional" hardware of the PIF Module.

Response
A description of a PIF module is shown in the response to RAI-12 and Topical Report MUAP-07006 Section 6.2.4.

"Conventional" means utilizing no software. For example, conventional hardware is relay, wiring module, solid state device, etc., as described in Topical Report MUAP-07006 Section 6.2.1.2. The part of the PIF module used by DAS operation uses conventional hardware (solid state device and no software).

RAI-39
Show that the "conversion to discrete signal" and "switching of control circuit" are easily verifiable steps. Is there any self-testing or diagnostic running within the PIF Module? What is the format of the digital signal from the "Control signal from CPU"?

Response
The configuration of the PIF module is described in the response to RAI-12.

[ ]

As described in Section 4.1.2.4 of Topical Report MUAP-07005 "Safety System Digital Platform -MELTAC", the Power Interface (PIF) Modules have the same I/O Bus interfaces as in the I/O modules. The self diagnosis functions of the I/O Bus and I/O modules are described in MUAP-07005 Sections 4.1.5.2.2 and 4.1.5.5, respectively. This includes cyclic redundancy check (CRC) checks and communication timeout checks for the I/O Bus communication.

The "Control signal from CPU" is a binary encoded data communication signal, including address and CRC data. This communication is based on RS-485 protocol and managed by the communication controller in the Bus Master module in the MELTAC controller and in the PIF module. The Bus Master module is described in Section 4.1.2.1.3 of Topical Report MUAP-07005.

RAI-40
The topical report states that the PIF Modules are described in the *MELTAC Digital Platform Topical Report*; this report does not provide any more information than the topical report under review. Please describe the PIF Modules in detail in this topical report or the *MELTAC Digital Platform Topical Report*. A simple device might best be shown with a schematic.

Response
The additional description of PIF module is shown in Figure 12-1 in the response to RAI-12.

This figure will be added to next revision of Topical Report MUAP-07004.
Detailed configuration of PIF module and technical information including type of used device, software free design, priority of signals will be attached to the Topical Report MUAP-07006

RAI-40a

Is the Output Module in Topical Report MUAP-07004, "Safety I&C System Description and Design Process," July 2007, the same component as the PIF Module in Topical Report MUAP-07006? If not, please explain the differences and clarify the uses of each component.

Response

In MUAP-07004 "output module" or "D/O" is the PIF module, which is the output device of the SLS for an actuator, in all places except the output devices of the RPS for reactor trip. For example, the RPS output devices are in Figures 4.4-1 and 6.5-2. The RPS uses a D/O module, instead of the PIF module. The D/O module is different from the PIF module mainly on no interposing logic part and low capacity for switching current. Detail specifications for the D/O and PIF modules are described in Topical Report MUAP-07005 "Safety System Digital Platform -MELTAC" Appendix A.5 and A.8, respectively.
Detailed information about difference between D/O module and PIF module will be attached to the Topical Report MUAP-07006

RAI-41

A PIF Module combines normal control, manual, auto safety, and auto DAS. What examples of "these components" that are used in nuclear plants are referred to in Point 4 (page 51 of the topical report)? Describe the similarities and differences.

Response

The portion of the PIF module that is common to PSMS and DAS combines signals from PSMS controllers with signals from DAS and status or equipment protection signals from plant components. Manual and auto control signals from safety and non-safety systems are combined through priority logic in the PSMS controllers, not in the PIF module. Diverse manual and auto control signals from DAS are combined outside the PIF module.

The portion of the PIF module which is used by both the PSMS and DAS utilizes conventional solid state components that are the same as the solid state components used in current operating nuclear plants. These are primarily binary logic integrated circuits and Field Effect Transistor output switching devices.

RAI-42

Outline how leak detection (i.e., leak-before-break) will be used in the defense-in-depth and diversity strategy and how it will comply with 10 CFR Part 50, Appendix A, General Design Criterion 4 and the NRC's guidance for use of leak-before-break analysis?

Response

Please see the response to RAI #2 in the second RAI.

The leak detection in MHI's D3 coping strategy is not taking credit for the requirement of GDC 4 and the leak-before-break analysis.

RESPONSE TO THE SECOND RAI (APRIL 2, 2008)

Following provides the responses for the second RAI, "Second Request for Additional Information on US-APWR Topical Report MUAP-07006-P, "Defense-In-Depth and Diversity", is issued on April 2, 2008.

RAI #1 – Analyzed Events

In Technical Report MUAP-07014(R0), "Defense-in-Depth and Diversity Coping Analysis," the only events analyzed in the Defense-in-Depth and Diversity Coping Analysis are Partial Loss of Forced Reactor Flow and Uncontrolled Control Rod Assembly Withdrawal at Power. Pursuant to SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs," dated April 2, 1993, and Branch Technical Position (BTP) 7-19, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs," dated April 2, 1993, the NRC staff requests that you provide a list of each postulated Common Cause Failure (CCF) or each event that is evaluated in the Safety Analysis Report, using best-estimate methods or Chapter 15 analysis methods. Also, provide the analysis results for each event analyzed demonstrating compliance with the acceptance criteria set in SECY-93-087 and BTP 7-19 for the Defense-in-Depth and Diversity assessment.

Response

Based on BTP 7-19, all US-APWR DCD Chapter 15 events, including both AOOs and PAs, are considered in the D3 coping analysis, Technical Report MUAP-07014. The report demonstrates that for all events the 10CFR100 radiological release criteria are met, and that primary coolant pressure boundary and containment integrity are maintained, in accordance with the acceptance criteria of BTP 7-19. To demonstrate conformance to the BTP 7-19 acceptance criteria, the technical report evaluates the following plant parameters for each Chapter 15 event with CCF:

(1) Pressure Boundary
(2) Core Coolability
(3) Dose

The primary mitigating functions for each plant parameter are explained below:

(1) Pressure Boundary
For reactor coolant pressure boundary (RCPB) integrity, the pressurizer pressure increase is mitigated by the pressurizer safety valve and the DAS. The pressurizer safety valve is designed to release the maximum surge flow to the pressurizer assuming a turbine trip without a reactor trip, as long as the steam generator secondary side has sufficient water inventory. The DAS includes the low steam generator water level trip function, thus the reactor trips from this signal before steam generator dry-out occurs. The DAS also actuates EFW to maintain adequate SG water level. Thus, the integrity of RCPB is maintained.

(2) Core Coolability
For core coolability, the SRP criteria are for pressure boundary and dose. Dose evaluations are not necessary if core coolability is maintained. For most events, core coolability is demonstrated by evaluating DNB. The technical report shows that no DNB occurs in the events analyzed.

(3) Dose
Events that do not challenge core coolability meet the 10 CFR 100 dose guidelines (10% for AOO and 100% for PA).

The DAS and appropriate manual actions based on simple EOPs provide an event termination time that is similar to the DCD evaluation. Therefore, the 10 CFR 100 criteria are also met (10% for AOO and 100% for PA).

Table 4.6-1 of MUAP-07014 summarizes the core coolability evaluation results for all Chapter 15 events. The table below adds the evaluation results for Pressure Boundary and Dose. The next revision of MUAP-07014, which will be submitted by June 20, 2008, will include this table, and it will provide the evaluation basis for all results.

Table: Results for acceptance criteria in Chapter 15 safety analysis assuming CCF

Section	Title	AOO /PA	Acceptance criteria			
			Pressure Boundary	Core Coolability		Dose
				Category	Evaluation	
15.1.1	Decrease in Feedwater Temperature as a Result of Feedwater System Malfunctions	AOO	The RCS pressure increase is mitigated by the pressurizer safety valve and the DAS. (See Section 4.5)	2	The event could result in no significant adverse consequence without RTS/ESF actuation.	Events that do not challenge core coolability meet 10 CFR 100 dose guidelines for PAs and 10% of the guideline for AOOs.
15.1.2	Increase in Feedwater Flow as a Result of Feedwater System Malfunctions	AOO		2	The event could result in no significant adverse consequence without RTS/ESF actuation.	
15.1.3	Increase in Steam Flow as a Result of Steam Pressure Regulator Malfunction	AOO		2	The event could result in no significant adverse consequence without RTS/ESF actuation.	
15.1.4	Inadvertent Opening of a Steam Generator Relief or Safety Valve	AOO	N/A	-	N/A	N/A
15.1.5	Steam System Piping Failures Inside and Outside of Containment	PA	The RCS pressure increase is mitigated by the pressurizer safety valve and the DAS. (See Section 4.5)	2	This event could result in no significant adverse consequence without RTS/ESF actuation.	Events that do not challenge core coolability meet 10 CFR 100 dose guidelines.
15.2.1	Loss of External Load	AOO		3	The event could be mitigated by DAS and DNBR remains above the 95/95 DNBR limit.	Events that do not challenge core coolability meet 10% of the 10 CFR 100 guideline.
15.2.2	Turbine Trip	AOO		3	Same as 15.2.1 with CCF	
15.2.3	Loss of Condenser Vacuum	AOO		3	Same as 15.2.1 with CCF	
15.2.4	Closure of Main Steam Isolation Valve	AOO		3	Same as 15.2.1 with CCF	
15.2.5	Steam Pressure Regulator Failure	BWR	N/A	-	N/A	N/A

Section	Title	AOO /PA	Acceptance criteria			
			Pressure Boundary	Core Coolability		Dose
				Category	Evaluation	
15.2.6	Loss of Non-Emergency AC Power to the Station Auxiliaries	AOO	The RCS pressure increase is mitigated by the pressurizer safety valve and the DAS. (See Section 4.5)	2	The loss of the non-emergency AC power causes the loss of power supply for the motor generator (M/G) set and result in the rod cluster control assembly (RCCA) trip, which does not cause the DNBR violation.	Events that do not challenge core coolability meet 10 CFR 100 dose guidelines for PAs and 10% of the guideline for AOOs.
15.2.7	Loss of Normal Feedwater Flow	AOO		3	The event could be mitigated by DAS and DNBR remains above the 95/95 DNBR limit.	
15.2.8	Feedwater System Pipe Break Inside and Outside Containment	AOO PA		3	The event could be mitigated by DAS and DNBR remains above the 95/95 DNBR limit.	
15.3.1.1	Partial Loss of Forced Reactor Coolant Flow	AOO		5	Event Analyzed. See section 4.6.2	
15.3.1.2	Complete Loss of Forced Reactor Coolant Flow	AOO		2	The loss of the non-emergency AC power causes the loss of power supply for the M/G set and result in the RCCA trip, which does not cause the DNBR violation.	
15.3.2	Flow Controller Malfunctions	BWR	N/A	-	N/A	N/A
15.3.3	Reactor Coolant Pump Rotor Seizure	PA	The RCS pressure increase is mitigated by the pressurizer safety valve and the DAS. (See Section 4.5)	4	This event could be severer than the result of the 15.3.1.1 event with CCF, but meet to the acceptance criteria for PA.	Events that do not challenge core coolability meet 10 CFR 100 dose guidelines.

Section	Title	AOO /PA	Acceptance criteria			
			Pressure Boundary	Core Coolability		Dose
				Category	Evaluation	
15.3.4	Reactor Coolant Pump Shaft Break	PA	The RCS pressure increase is mitigated by the pressurizer safety valve and the DAS. (See Section 4.5)	4	This event could be severer than the result of the 15.3.1.1 event with CCF, but meet to the acceptance criteria for PA.	Events that do not challenge core coolability meet 10 CFR 100 dose guidelines.
15.4.1	Uncontrolled Control Rod Assembly Withdrawal from a Subcritical or Low Power Startup Condition	AOO	N/A	-	N/A	N/A
15.4.2	Uncontrolled Control Rod Assembly Withdrawal at Power	AOO	The RCS pressure increase is mitigated by the pressurizer safety valve and the DAS. (See Section 4.5)	5	Event Analyzed. See section 4.6.1	Events that do not challenge core coolability meet 10 CFR 100 dose guidelines for PAs and 10% of the guideline for AOOs.
15.4.3	Control Rod Misoperation (System Malfunction or Operator Error)	AOO PA		2	The event could result in no significant adverse consequence without RTS/ESF actuation.	
15.4.4	Startup of an Inactive Loop or Recirculation Loop at an Incorrect Temperature	-	N-1 loop operation is not permitted in US-APWR.	-	N-1 loop operation is not permitted in US-APWR.	N-1 loop operation is not permitted in US-APWR.
15.4.5	Flow Controller Malfunction Causing an Increase in BWR Core Flow Rate	BWR	N/A	-	N/A	N/A
15.4.6	Inadvertent Decrease in Boron Concentration in the Reactor Coolant System	AOO	The RCS pressure increase is mitigated by the pressurizer safety valve and the DAS. (See Section 4.5)	3	This event is a slow transient due to low positive reactivity insertion rate. This slow transient provides sufficient time to take corrective manual action.	Events that do not challenge core coolability meet 10% of the 10 CFR 100 dose guidelines.

Section	Title	AOO /PA	Acceptance criteria			
			Pressure Boundary	Core Coolability		Dose
				Category	Evaluation	
15.4.7	Inadvertent Loading and Operation of a Fuel Assembly in an Improper Position	PA	N/A	-	N/A	N/A
15.4.8	Spectrum of Rod Ejection Accidents	PA	The RCS pressure increase is mitigated by the pressurizer safety valve and the DAS. (See Section 4.5)	4	This event could be severer than the result of the 15.4.2 event with CCF, but meet to the acceptance criteria for PA.	Events that do not challenge core coolability meet 10 CFR 100 dose guidelines.
15.4.9	Spectrum of Rod Drop Accidents in a BWR	BWR	N/A	-	N/A	N/A
15.5.1	Inadvertent Operation of Emergency Core Cooling System that Increases Reactor Coolant Inventory	AOO	The ECCS can not inject into the RCS at nominal, at-power operating pressure.	-	The ECCS can not inject into the RCS at nominal, at-power operating pressure.	The ECCS can not inject into the RCS at nominal, at-power operating pressure.
15.5.2	Chemical and Volume Control System Malfunction that Increases Reactor Coolant Inventory	AOO	The RCS pressure increase is mitigated by the pressurizer safety valve and the DAS. (See Section 4.5)	2	The event could result in no significant adverse consequence without RTS/ESF actuation.	Events that do not challenge core coolability meet 10% of the 10 CFR 100 dose guidelines.
15.6.1	Inadvertent Opening of a PWR Pressurizer Pressure Relief Valve or a BWR Pressure Relief Valve	AOO	The RCS pressure increase is mitigated by the pressurizer safety valve and the DAS. (See Section 4.5)	3	The event could be mitigated by DAS and DNBR remains above the 95/95 DNBR limit.	Events that do not challenge core coolability meet 10% of the 10 CFR 100 dose guidelines.
15.6.2	Radiological Consequences of the Failure of Small Lines Carrying Primary Coolant Outside Containment	AOO	The RCS pressure increase is mitigated by the pressurizer safety valve and the DAS. (See Section 4.5)	2	The event could result in no significant adverse consequence without RTS/ESF actuation.	DAS and appropriate manual actions are comparable to the DCD evaluation. Therefore, 10 CFR 100 is also met.

Section	Title	AOO /PA	Acceptance criteria			
			Pressure Boundary	Core Coolability		Dose
				Category	Evaluation	
15.6.3	Radiological Consequences of Steam Generator Tube Failure	PA	The RCS pressure increase is mitigated by the pressurizer safety valve and the DAS. (See Section 4.5)	3	The DAS and manual operations can lead to no significant adverse consequence without RTS and EFS.	DAS and appropriate manual actions are comparable to the DCD evaluation. Therefore, 10 CFR 100 is also met.
15.6.4	Radiological Consequences of Main Steam Line Failure Outside Containment (BWR)	BWR	N/A	-	N/A	N/A
15.6.5	Loss-of-Coolant Accidents Resulting from Spectrum of Postulated Piping Breaks within the Reactor Coolant Pressure Boundary	PA	Large break LOCA with CCF has a very low probability of occurrence.	1/3	The DAS and manual operations can lead to no significant adverse consequence without RTS and EFS at small break LOCA. This event is Category 3. Large break LOCA with CCF has a very low probability of occurrence. This event is Category 1.	SBLOCA that do not challenge core coolability meet 10 CFR 100 dose guidelines. Large break LOCA with CCF has a very low probability of occurrence.

RAI #2 – Large Break Loss-of-Coolant Accident (LBLOCA) Analysis

MHI identifies a LBLOCA as an accident with extremely low probability and states that SECY-93-087 identifies a CCF as a beyond design basis event based on its extremely low probability of occurrence. Therefore, MHI did not perform a Defense-in-Depth and Diversity Coping Analysis for LBLOCA.

Response

Topical Report MUAP-07006 describes only the generic methodology for D3 Coping Analysis. As stated in the Abstract of MUAP-07006, "The D3 Coping Analysis for specific plants, which is based on the generic methods described in this topical report, is provided in Plant Licensing Documentation." The essence of this statement is reiterated in Section 3.4(6), Section 8.1, Table 10.0-1 and Appendix A (Point 2) of MUAP-07006.

The "Plant Licensing Documentation" for the US-APWR is technical report MUAP-07014, which is referenced in Section 7.8 of the US-APWR DCD. This technical report describes the D3 coping analysis for the US-APWR. This technical report is currently being revised to provide an evaluation of each event in Chapter 15 of the US-APWR DCD, including LBLOCA.

RAI #2 Continued

The US-APWR D3 Coping analysis will follow the generic D3 coping strategy for LBLOCA presented in MUAP-07006. This coping strategy credits the unique alarms from the leak detection system to prompt manual operator actions. These alarms are not subject to the CCF that affects the PSMS and PCMS. The US-APWR D3 Coping Analysis demonstrates the operators' ability to achieve safe shutdown and thereby mitigate the LBLOCA.

In addition, MHI makes numerous statements throughout its submittal regarding taking credit for reactor coolant system (RCS) leak detection for LBLOCA mitigation. In both Section 8.3 of Topical Report MUAP-07006-P(R1) and Section 4.2 of Technical Report MUAP-07014(R0), MHI states the LBLOCA is mitigated based on early detection of small leaks in the RCS and manual operator actions that ensure the plant is shutdown so that small leaks can be repaired before they can become large breaks.

In Section 9.3 of Topical Report MUAP-07006-P(R1) MHI states the following:

> *"The DAS [diverse actuation system] includes diverse processing and display of leak measurement sensors as described in Section 6.2.3. The DAS credits this diverse leak detection which allows operators to detect and mitigate the leak even if the PSMS [protection and safety monitoring system] and PCMS [plant control and monitoring system] not operating correctly due to an undetected latent CCF. This is consistent with BTP-19, the System 80+ Design Control Document, and the NRC's SER of that DCD, NUREG-1462, which state credit for leak detection is accepted ... because (1) LBLOCAs and MSLBs ... in combination with a CCF ... is highly unlikely (2) I&C equipment possesses sufficient diversity and simplicity including manual controls ... and instrumentation ..."*

In the US-APWR Design Control Document (DCD), MHI references the Standard Review Plan issued by the NRC staff in March 2007, which includes BTP 7-19. However, MHI's statements are inconsistent with the regulatory analysis contained in BTP 7-19. It appears that these statements are based on a previous version of the NRC staff's technical position (BTP HICB-19) regarding taking credit for leak before break detection for LBLOCA and main steam line break (MSLB) events. BTP 7-19, which supersedes the previous version issued by the NRC staff (dated June 1997), does not allow credit for leak detection for LBLOCA and/or MSLB with a CCF.

Response

While MHI's D3 coping strategy includes leak detection, it is not based solely on leak detection; therefore it is not taking credit for leak-before-break to "exclude [LBLOCA] from the design basis" as allowed for the dynamic effects associated with postulated pipe ruptures in 10CFR50 GDC-4. The generic D3 coping strategy 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 only a single input with a single setpoint (eg. low pressurizer pressure), and therefore allow near 100% 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 the PSMS CPU 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, MHI does not credit this low potential for CCF concurrent with other AOOs or PAs (ie. a CCF is considered concurrent with all other AOOs and PAs in MHIs D3 Coping strategy).

Therefore, 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. The diverse leak detection function, which prompts a deterministic operator action to depressurize the plant and thereby mitigate the LBLOCA, supplements this primary coping strategy by providing additional defense-in-depth.

MHI's coping strategy for LBLOCA, which includes credit for leak detection, is consistent with BTP 7-19. BTP 7-19 includes the section entitled *"Justification for Not Correcting Specific Vulnerabilities".* The version of BTP 7-19 considered when MHI developed the D3 coping strategy for the Japanese APWR (and is now applied to the US-APWR) included the following statement:

> *For example, I&C system vulnerability to common-mode failure affecting the response to large-break loss-of-coolant accidents and main steam line breaks has been accepted in the past. This acceptance was based upon the provision of primary and secondary coolant system leak detection, and pre-defined operating procedures that together enable operators to detect small leaks and take corrective actions before a large break occurs.*

While this specific example has been removed from the current version of BTP 7-19, the current version of BTP 7-19 does not preclude crediting leak detection in the D3 coping strategy. There continues to be precedents for NRC approval of D3 coping strategies that include leak detection. These prior approvals have not been rescinded.

It is noted, that these prior NRC approvals were based primarily on the credit for leak detection. MHI's coping strategy for LBLOCA provides additional defensive measures, which reduce the potential for CCF in the RPS/ESFAS compared to previous designs. These defensive measures provide an additional defense-in-depth layer, which adds significant safety conservatism, and therefore goes beyond the NRC approval basis for prior applications.

It is also noted, that MHI's D3 coping strategy, which credits defensive measures that essentially eliminate the potential for CCF concurrent with LBLOCA, is consistent with the industry's position under discussion in DI&C TWGs 2 and 3. The inclusion of leak detection, and the deterministic demonstration of safe shutdown in MHI's D3 Coping Analysis, provides an additional defense-in-depth layer, which adds significant safety conservatism, and therefore goes beyond the current industry position.

RAI #2 Continued

a) SECY-93-087 states, "inasmuch as common mode failures are beyond design-basis events, the analysis of such events should be on a best-estimate basis." Therefore, a Defense-in-Depth and Diversity coping analysis for LBLOCA with CCF should be performed using a best-estimate basis. The NRC staff requests that MHI analyze and submit the Defense-in-Depth and Diversity Coping Analysis results for LBLOCA with CCF using a best-estimate basis. The Defense-in-Depth and Diversity Coping Analysis may credit a mitigation method other than leak detection.

Response

The next revision to MUAP-07014 will describe the coping strategy for LBLOCA, including the demonstration of safe shutdown. It will be based on the generic coping strategy presented in MUAP-07006, which credits the low frequency of the LBLOCA, the unlikelihood of a CCF in the PSMS concurrent with LBLOCA, and use of leak detection to prompt manual operator actions to achieve safe shutdown.

RAI #2 Continued

In Section 9.3 of Topical Report MUAP-07006-P(R1) MHI states, "A mitigation strategy that considers the low probability of LBLOCA is also consistent with nuclear regulations in most international countries and with 10 CFR 50.62, which requires diverse mitigation only for higher frequency AOOs."

b) Nowhere is it stated in 10 CFR 50.62 that diverse mitigation is only required for higher frequency Anticipated Operational Occurrence. The NRC staff requests that MHI clarify what is meant by this statement.

Response

MHI did not mean to imply that 10CFR50.62 is applicable only to those AOOs that are higher frequency than others. This sentence was meant to imply only that AOOs are higher frequency events than Postulated Accidents, which are not within the scope of 10CFR50.62. MHI will reword this sentence as follows:

> "A mitigation strategy that considers the low probability of LBLOCA is also consistent with nuclear regulations in most international countries and with 10 CFR 50.62.

RESPONSE TO THE THIRD DRAFT RAI (APRIL 22, 2008)

1. Page 37, section 7.2.4, "Human Diversity" – Please explain what is meant by the sentence, "The design person for the DAS is different from the design person for the PSMS and PCMS."

   Response
   This means that because there are two separate design engineers, there is a reduction in the potential of CCF due to misinterpretation or misunderstanding of functional or system design requirements or translation of those requirements into actual design hardware or software.

2. Page 41, section 7.14, "Guideline 14: Manual Operator Action" – Please explain what is meant by, "The DAS provides diverse analog data processing and HSI for at least one key variable for each critical safety function." What criteria are used to determine if one or more variables are needed to establish diversity for a critical safety function? Also, is there a distinct HSI for each variable related to a critical safety function or a distinct HSI for each critical safety function?

   Response
   The variables provided for indication of each critical safety function are identified in Table 7.8-2 of the DCD. This list is consistent with the Type B variables defined in Table 7.5-3 of the DCD. As defined in IEEE 497, Type B variables provide primary information to the control room operators to assess the plant critical safety functions. The subset of Type B variables selected for the DHP is based on review of historical EOPs for US and Japanese PWRs, which define key variables for monitoring each critical safety function. These EOPs are generally applicable to the US-APWR.

   The diversity pertains to the hardware/software between the PSMS/PCMS and DAS, not the diversity of sensors or monitored variables.

   There are distinct indicators for each critical function variable on the DHP. Each variable is unique to a single critical function.

3. Page, 44, section "Manual Action Analysis Method" - Please explain what is meant by the statements, "In addition, all manual actions credited in the D3 Coping Analysis are included in the HFE Program described in the HSI System Topical Report. This program includes these actions in Human Reliability Analysis and HSI Validation using a dynamic high fidelity simulator." Specifically, where in section 5.6, "Human Reliability Analysis," of Topical Report MUAP-07007-P (R1), is an explanation/analysis of credited manual actions for the D3 Coping Analysis included?

   Response
   Section 5.6 defines the process of Human Reliability Analysis. As stated in this section, "the HFE design gives special attention to those plant scenarios, risk-important human actions, and HSIs that have been identified by PRA/HRA as being important to plant safety and reliability." Manual actions credited in the D3 Coping Analysis are considered in the PRA. For manual actions credited in the D3 Coping Analysis that are identified by the PRA/HRA as being risk significant, the HFE analysis and HSI design

that supports these actions will be given special attention during all other elements of the HFE program. Therefore, Section 5.6 does not identify any human actions as risk significant; instead, this is the result of the PRA/HRA process.