

REQUEST FOR ADDITIONAL INFORMATION 240-2035 REVISION 0

3/2/2009

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No. 52-021

SRP Section: 07.07 - Control Systems

Application Section: Section 07.07 - Control Systems

QUESTIONS for Instrumentation, Controls and Electrical Engineering 1 (AP1000/EPR Projects) (ICE1)

07.07-1

Correct the inconsistencies between the columns "PCMS" and "Related Section in US-APWR DCD" in Table 7.1-2.

The control systems not required for the safety are provided by the PCMS as described in Section 7.7 in the DCD Tier 2. This review is based on the I&C system column "PCMS" and the column titled "Related Section in US-APWR DCD." Of the CFR requirements listed in SRP Table 7-1 as applicable to control systems not required for safety, Table 7.1-2 in the DCD Tier 2 cites compliance only with 10 CFR 52.47(b)(1) and 52.80(a) through a reference to Tier 1. Table 7.1-2 cites compliance with other 10 CFR sections for the PCMS but does not refer to Section 7.7 as a related section in the DCD in the column titled "Related Section in US-APWR DCD." Inconsistencies such as this prevent a thorough review of the regulatory requirements applicable to the PCMS.

07.07-2

Discuss compliance with GDC 1 in relation to the PCMS. Update Table 7.1-2 if necessary.

GDC 1 sets the quality standards and records for SSCs important to safety. The DCD does not cite compliance with GDC 1 for the PCMS. Because the PCMS implements control functions not required for safety, GDC 1 is applicable in that the functions performed by the PCMS do not interfere with the safety-related functions. In addition, the control system must be appropriately designed and be of sufficient quality to minimize the potential for challenges to safety systems. Compliance with GDC 1 as it relates to control systems not required for safety and the PCMS is not indicated in Table 7.1-2, nor discussed in Section 3.1 of the DCD.

07.07-3

Discuss compliance with GDC 10 in relation to the PCMS. Update Table 7.1-2 if necessary.

Table 7.1-2 in the DCD does not cite compliance with the GDC 10, but refers to Chapter 4, "Reactor" of the DCD Tier 2. Per Table 7-1 and Appendix 7.1-A of the SRP, GDC-10 is applicable to the PCMS. The staff reviewed the aforementioned chapter in the DCD

REQUEST FOR ADDITIONAL INFORMATION 240-2035 REVISION 0

and confirmed that compliance with the GDC 10 is cited. Section 3.1.2.1.1 addresses the reactor protection system setpoints being chosen to support design margins and that the protection and control systems are designed with appropriate margin to assure that acceptable fuel design limits are not exceeded during any condition of normal operation. Compliance with GDC 10 is not indicated in Table 7.1-2 and discussed in Section 3.1 of the DCD as it relates to the protection system and control system setpoints, and appropriate margin.

07.07-4

Discuss compliance with GDC 15 in relation to the PCMS. Update Table 7.1-2 if necessary.

GDC 15 requires that the reactor coolant system and associated auxiliary, control, and protection systems be designed with sufficient margin to assure that the design conditions of the reactor coolant pressure boundary are not exceeded during any condition of normal operation, including anticipated operational occurrences.” Compliance with the GDC 15 is not cited in Table 7.1-2 of the DCD, but a reference to Chapter 5, “Reactor Coolant and Connecting Systems” is made. The staff reviewed Chapter 5 and confirmed that conformance to the GDC 15 is cited in the document. Section 3.1.2.6.1 addresses the reactor protection system setpoints being chosen based on steady state and transient analyses in DCD Chapter 15 and that the protection and control systems are designed with appropriate margin to assure that the reactor coolant pressure boundary limits are not exceeded during any condition of normal operation. Compliance with GDC 15 is not indicated in Table 7.1-2 and discussed in Section 3.1 of the DCD as it relates to the protection system and control system setpoints and the reactor coolant pressure boundary limits.

07.07-5

Discuss compliance with GDC 28 in relation to the PCMS. Update Table 7.1-2 if necessary.

GDC 28 requires that the reactivity control systems be designed with appropriate limits on the potential amount and rate of reactivity increase in the event of postulated reactivity accidents. Table 7.1-2 does not cite compliance with the GDC 28 but references Chapter 15. The staff reviewed the chapter and confirmed that compliance with the GDC 28 is cited; compliance is also cited in Chapter 16, Appendix B, “US-APWR Technical Specifications.” Section 3.1.3.9.1 indicates that GDC 28 is applicable for the determination of protection system setpoints and that the reactivity control systems are designed with appropriate limits on the potential amount and rate of reactivity increase. Compliance with GDC 28 is not indicated in Table 7.1-2 and discussed in Section 3.1 of the DCD as it relates to the protection system and control system setpoints, and appropriate limits of reactivity and rate of increase.

REQUEST FOR ADDITIONAL INFORMATION 240-2035 REVISION 0

07.07-6

Discuss compliance with GDC 44 in relation to the PCMS. Update Table 7.1-2 if necessary.

GDC 44 requires that a system to transfer heat from structures, systems, and components important to safety to an ultimate heat sink (UHS) be provided. Table 7.1-2 does not cite GDC 44 as it relates to control systems not required for safety, but makes reference to Chapter 9, "Auxiliary Systems." The component cooling water system (CCWS) and the essential service water system (ESWS) provide heat transfer from plant safety-related components to the UHS. The staff reviewed Chapter 9 and confirmed that the safety design bases of both systems cite the GDC 44. Section 3.1.4.15.1 indicates that suitable leak detection will be provided. Compliance with GDC 44 is not indicated in Table 7.1-2 and discussed in Section 3.1 of the DCD as it relates to the protection system and control system setpoints, and leak detection.

07.07-7

Discuss the discrepancy between the columns "PCMS" and "Related Section in US-APWR DCD" in DCD Table 7.1-2 with respect to the SRM to SECY 93-087.

SRP Table 7-1 identifies SRM to SECY 93-087 II.Q as providing acceptable guidance for defense against common-mode failures in digital systems for control systems not required for safety. SRM to SECY 93-087 II.T is acceptable guidance for control room annunciator reliability, although SRP Table 7-1 does not indicate that is applied specifically to control systems not required for safety (i.e., Section 7.7). DCD Table 7.1-2 indicates conformance with both parts of the SRM for the PCMS but does not indicate that it is applicable to Section 7.7 of the DCD in column titled "Related Section in US-APWR DCD".

07.07-8

Discuss conformance with RG 1.105 in relation to the PCMS and the relationship between the normal trip setpoints and the safety-related trip setpoints. Update Table 7.1-2 if necessary.

RG 1.105 endorses Part 1 of ISA-S67.04-1994 and is used to determine the setpoints for safety-related instrumentation. SRP Table 7-1 and SRP Appendix 7.1-A, Section 4(g) indicate/state that RG 1.105 applies to all I&C systems. Table 7.1-2 in the DCD Tier 2 does not cite conformance with RG 1.105 for control systems not required for safety (i.e., the PCMS). RG 1.105 does apply to the PCMS in that it depicts the normal trip setpoint in relation to the safety-related trip setpoints.

07.07-9

Discuss conformance with RG 1.152 in relation to the PCMS and the barriers between the PCMS and the PSMS to prevent interference. Update Table 7.1-2 if necessary.

REQUEST FOR ADDITIONAL INFORMATION 240-2035 REVISION 0

RG 1.152 provides a basis for evaluating conformance of computers with GDC 21, and applies to all I&C safety systems and supporting data communication systems. RG 1.152, Rev. 2 endorses IEEE Std 7-4.3.2-2003 with reservations. Table 7.1-2 in the DCD Tier 2 does not cite conformance with RG 1.152. Clause 5.6(a) of IEEE Std 7-4.3.2-2003 states that "Barrier requirements shall be identified to provide adequate confidence that the nonsafety functions cannot interfere with the performance of the safety functions of the software or firmware. The barriers shall be designed in accordance with the requirements of this standard. The nonsafety software is not required to meet these requirements." RG 1.152 does apply to the PCMS in that it cannot interfere with the performance of the PSMS.

07.07-10

Discuss conformance with RGs 1.168–1.171 in relation to the PCMS. Address the similarities and differences between the MELTAC Platforms for the PSMS and the PCMS. Update Table 7.1-2 if necessary.

Because the operating history of the MELTAC Platform used in the PCMS is used as a basis to provide information on any software errors to credit the reliability of the MELTAC Platform used in the PSMS, any similarities and differences between the platforms history and use must be well understood. RGs 1.169–1.171 apply to digital computer software used in safety systems of nuclear power plants. Note that RG 1.169 endorses IEEE Std 828-1990 that "also applies to non-critical software." Because the MELTAC Platform is used in the PSMS and the PCMS, these RGs (or similar Japanese regulations) were used in the development of the PCMS software; however, Table 7.1-2 does not indicate this.

07.07-11

Discuss conformance with RGs 1.180 in relation to the PCMS and the emissions from nonsafety-related systems and their potential effect on safety systems. Update Table 7.1-2 if necessary.

RG 1.180 identifies electromagnetic environment operating envelopes, design, installation and test practices acceptable to the staff for addressing the effects of electromagnetic interference/radio frequency interference (EMI/RFI), and power surges on I&C systems and components important to safety. Table 7.1-2 in the DCD Tier 2 does not cite conformance with RG 1.180 for the PCMS, and references Sections 7.2 through 7.6 and Section 7.9 of the DCD Tier 2. The practices endorsed in RG 1.180 apply to both safety-related I&C systems and non-safety-related I&C systems whose failures can affect safety functions. While nonsafety-related systems are not part of the RG, control of EMI/RFI from these systems is necessary to ensure that safety-related I&C systems can continue to perform properly in the nuclear power plant environment. When feasible, the emissions from nonsafety-related systems should be held to the same levels as safety-related systems.

REQUEST FOR ADDITIONAL INFORMATION 240-2035 REVISION 0

07.07-12

Discuss conformance with RG 1.204 in relation to the PCMS, the isolation provided between the safety and nonsafety system, and potential interaction between the systems because of lightning. Update Table 7.1-2 if necessary.

RG 1.204 provides a basis for evaluating conformance of I&C systems and components to 10 CFR 50 and GDC 2. RG 1.204 provides guidance in the design and installation of lightning protection systems to assure that electrical transients resulting from lightning phenomena do not render I&C systems important to safety inoperable or cause spurious operation of such systems. Table 7.1-2 in the DCD Tier 2 does not cite conformance with RG 1.204 for the PCMS, and references Chapter 8, "Electrical Systems" of the DCD Tier 2. In general, nonsafety-related equipment does not fall under the guidelines presented in RG 1.204, but nonsafety-related equipment is included if its failure can impact the function and performance of safety-related equipment. The review based on RG 1.204 is to ensure that proper isolation exists between the PCMS and the PSMS such that a failure in the PCMS will not affect the PSMS.

07.07-13

Discuss conformance with BTP 7-11 in relation to the PCMS and the isolation provided between the safety and nonsafety system. Update Table 7.1-2 if necessary.

BTP 7-11 provides guidelines for the use of electrical isolation devices to allow connections between redundant portions of safety systems or between safety systems and non-safety systems. BTP 7-11 deals with the criteria and methods used to confirm that the design of isolation devices assures that credible failures in the connected non-safety or redundant channels will not prevent the safety system from meeting their required functions. Table 7.1-2 in the DCD does not cite conformance with BTP 7-11 for the PCMS but does cite conformance with BTP 7-11 for the PSMS (i.e., RPS, ESFAS, LSL, and Safety HSI). Additionally, describe how the isolation devices used address the criteria in BTP 7-11.

07.07-14

Discuss conformance with BTP 7-12 in relation to the PCMS and the procedure used to establish setpoints. Update Table 7.1-2 if necessary.

BTP 7-12 provides guidelines for reviewing the process an applicant/licensee follows to establish and maintain instrument setpoints. Table 7.1-2 in the DCD Tier 2 does not cite conformance with BTP 7-12, but references Sections 7.2 through 7.6 and Section 7.9. The US-APWR will require a setpoint list identifying safety setpoints and non-safety setpoints for functions providing protective functions important to safety or that are relevant to conformance with technical specification limiting conditions for operation. In addition, a description of the setpoint methodology and procedures used in determining setpoints, including information sources, scope, assumptions, interface reviews, and statistical methods is needed. Table 7.1-2 in the DCD does not cite conformance with BTP 7-12 for the PCMS but does cite conformance with BTP 7-12 for the PSMS (i.e., RPS, ESFAS, and SLS).

REQUEST FOR ADDITIONAL INFORMATION 240-2035 REVISION 0

07.07-15

Discuss conformance with BTP 7-14 in relation to the PCMS. Update Table 7.1-2 if necessary.

BTP 7-14 provides guidelines for evaluating software life-cycle processes for digital computer-based I&C systems. Table 7.1-2 in the DCD Tier 2 does not cite conformance with BTP 7-14 for the PCMS, but references Sections 7.2 through 7.6 and Section 7.9. Because the MELTAC Platform is used in the PSMS and the PCMS, these BTP 7-14 was used in the development of the PCMS software; however, Table 7.1-2 does not indicate this. Table 7.1-2 in the DCD does not cite conformance with BTP 7-14 for the PCMS but does cite conformance with BTP 7-14 for the PSMS (i.e., RPS, ESFAS, and SLS).

07.07-16

Discuss conformance with BTP 7-17 and demonstrate that the self-test functions of the PCMS cannot either cause the PCMS to interfere with the functioning of the PSMS or themselves directly interfere with the functioning of the PSMS. Update Table 7.1-2 if necessary.

BTP 7-17 provides guidelines for reviewing the design of the self-test and surveillance test provisions. Table 7.1-2 in the DCD Tier 2 does not cite conformance with BTP 7-17 for the PCMS, but references Sections 7.2 through 7.6 and Section 7.9. Although the PCMS and PSMS both use the MELTAC Platform, the software and hardware are not identical between the systems. Conformance with BTP 7-17 and an associated review is to ensure that the PCMS is designed for in-service testability commensurate with the functions to be performed through all modes of plant operation and that the positive aspects of self-test features are not compromised by the additional complexity that may be added to the safety system by the self-test features. In addition, the review needs to assert that the hardware and software design support the required periodic testing. Table 7.1-2 in the DCD cites conformance with BTP 7-17 for the PSMS (i.e., RPS, ESFAS, and SLS) but does not cite conformance with the PCMS.

07.07-17

Discuss conformance with BTP 7-21 in relation to the PCMS and the real-time performance and architectures of the PSMS and PCMS, noting any differences and similarities. Update Table 7.1-2 if necessary.

BTP 7-21 provides guidelines for reviewing digital system real-time performance and system architectures in I&C systems. Table 7.1-2 in the DCD Tier 2 does not cite conformance with BTP 7-21 for the PCMS, but references Sections 7.2 through 7.6 and Section 7.9. To evaluate the performance and correctness expected of the actual plant, some of the criteria described BTP 7-21 may be met by submissions describing a software development process or verification methods that include real-time concerns. Although the PSMS and PCMS both use the MELTAC Platform, the limiting response times, digital computer timing requirements, architecture, design commitments,

REQUEST FOR ADDITIONAL INFORMATION 240-2035 REVISION 0

performance verification, and cyclic bases are not necessarily the same. The similarities, and differences, of the non-safety and safety platforms need to be identified and understood by the staff within the real-time performance criteria and the software development process. Table 7.1-2 in the DCD does not cite conformance with BTP 7-21 for the PCMS but does cite conformance with BTP 7-21 for the PSMS (i.e., RPS, ESFAS, and SLS).

07.07-18

Address the discrepancies between the list of systems in the PCMS between DCD Section 7.7 and TR MUAP-07004-P(R1) Section 4.1.c.

The subsections of Section 7.7.1 in the DCD describe the US-APWR control functions that can affect the performance of critical safety functions. Section 4.1.c of TR MUAP-07004-P describes the major systems within the PCMS echelon. The system lists in the documents do not match:

- The DCD has a nuclear instrumentation system (Section 7.7.1.2) and an in-core instrumentation system (Section 7.7.1.5); TR MUAP-07004-P(R1) has an in-core nuclear instrumentation system (Section 4.1.c(5)).
- The DCD lists a Balance-of-Plant Control as a system (Section 7.7.1.6); TR MUAP-07004-P(R1) does not list a BOP system.
- The DCD lists a Turbine Protection Control (Section 7.7.1.9); TR MUAP-07004-P shows that protection and control are two different systems with different functions (Sections 4.1.c(6) and (8)).
- The DCD lists an auxiliary equipment control system (Section 7.7.1.12); TR MUAP-07004-P does not list this system as part of the PCMS.

The DCD does not list a generator transformer protection system and an AVR/ALR system as part of the PCMS; TR MUAP-07004-P(R1) has a generator transformer protection system (Section 4.1.c(11)) and an AVR/ALR system (Section 4.1.c(12)).

07.07-19

List the process control variables and discuss the automatic and manual control for each of these variables.

GDC 13 is applicable for control systems as it relates to instrumentation and controls provided to monitor variables over anticipated ranges for normal operations, AOOs, and accident conditions. Plant characteristics considered in a plant's Chapter 15 Safety Evaluation contain the following key plant parameters considered in the safety evaluation:

- core power,
- core inlet temperature,
- reactor system pressure,
- core flow, axial and radial power distribution,
- fuel and moderator temperature coefficient,
- void coefficient,
- reactor kinetics parameters,
- available shutdown rod worth, and

REQUEST FOR ADDITIONAL INFORMATION 240-2035 REVISION 0

- control rod insertion characteristics.

Section 7.7.2 states that “The control systems for the US-APWR include the necessary features for manual and automatic control of process variables within the prescribed normal operating limits.” A list and discussion of the process variables and their control is not provided in Section 7.7.

07.07-20

Address by AOO failure modes other than random hardware failures that could be associated with digital systems such as software design errors.

The failure of any control system component or any auxiliary supporting system for control systems should not cause plant conditions more severe than those described in the analysis of AOOs in Chapter 15 of the DCD. The AOOs defined in the plant safety analysis considered in the control function design for the US-APWR are listed in Table 7.7-1 of the DCD. A review of Chapters 7 and 15 did not identify where any of the AOOs in its assessment of software design errors failure modes that could be associated with digital systems (the evaluations did consider random hardware failures.) (The evaluation of multiple independent failures is not intended by this question.)

07.07-21

Section 15.5.2.1 does not address control system failures as an initiator of a CVCS malfunction that increases RCS inventory yet Table 7.7-1 in the DCD indicates that this event is caused by a control system failure. Address this discrepancy.

Section 15.5.2.1 states that “A CVCS malfunction that increases RCS inventory can be caused by an operator error, a test sequence error, or an electrical malfunction. Based on the title of Table 7.7-1—AOOs due to control system failures—this event is caused by a control system failure. If a control system failure can cause a CVCS malfunction that increases RCS inventory, Section 15.5.2.1 should address this. If a control system failure cannot cause a CVCS malfunction that increases RECS inventory, MHI needs to clarify for this review.

07.07-22

Freezing of instrument sensing lines is not addressed in Chapters 7 or 15. Discuss the design of the APWR and how it addresses items a-c below.

Environmental control systems that are credited in the safety analysis for the US-APWR are controlled by the PSMS, not the PCMS. Environmental control systems controlled by the PCMS, such as non-essential area HVAC, heat tracing, and/or forced air-cooling or heating, are considered in the failure analyses. Based on Regulatory Position 5 of RG 1.151, special considerations that should be addressed in the design and installation of instrument sensing lines provided in ISA-S67-02 should be supplemented with the following:

REQUEST FOR ADDITIONAL INFORMATION 240-2035 REVISION 0

- a. Instrument sensing lines that can be exposed to freezing temperatures and that contain or can be expected to contain a condensable mixture or fluid that can freeze should be provided an environmental control system (heating and ventilation or heat tracing) to protect the lines from freezing during extremely cold weather.
- b. The environment associated with those instrument sensing lines in a. that are safety related should be monitored and alarmed so that appropriate corrective action can be taken to prevent loss of or damage to the lines from freezing in the event of loss of the environmental control system.
- c. The environmental control system recommended in a., and for which b. applies, should be electrically independent of the monitoring and alarm system so that a single failure in either system, including their power sources, does not affect the capability of the other system.

The environmental control and monitoring systems of a. and b. should be designed to standards commensurate with their importance to safety and with administrative controls that are implemented to address events or conditions that could render the systems inoperable.

07.07-23

Address inadvertent actions caused via the touch screen VDUs and procedures/design in place to prevent/minimize such occurrences.

AOO 15.1.4 addresses the Inadvertent opening of a steam generator relief or safety valve. AOOs 15.5.1 and 15.5.2 address the inadvertent operation of ECCS and chemical and volume control system malfunction that increases reactor coolant inventory. MUAP-07007-P, *HSI System Description and HFE Process*, addresses touch size area for safety and operational VDUs. The reviewer cannot validate that inadvertent action, such as an unintended touch on a touch sensitive display cannot prevent the actuation of a safety function.

07.07-24

Address RG 1.152, Regulatory Position 2.7 and any techniques used to ensure that system security is intact, including the use of system logs, real time monitoring, and periodic testing.

RG 1.152, Regulatory Position 2.7 states that "The operation lifecycle process involves the use of the safety system by the licensee in its intended operational environment. During the operations phase, the licensee should ensure that the system security is intact by techniques such as periodic testing and monitoring, review of system logs, and real-time monitoring where possible." DCD 7.7 does not address any techniques used to ensure that system security is intact.

07.07-25

Address RG 1.152, Regulatory Position 2.8.2 and the use of periodic audits to determine the effectiveness of the digital safety systems security procedures.

REQUEST FOR ADDITIONAL INFORMATION 240-2035 REVISION 0

RG 1.152, Regulatory Position 2.8.2 states that “The licensee’s quality assurance group (such as information/network security expert) should conduct periodic audits to determine the effectiveness of the digital safety system security procedures.” DCD Section 7.7 does not address the use of periodic audits to determine the effectiveness of the digital safety systems security procedures.

07.07-26

Address RG 1.152, Regulatory Position 2.8.3 and contingencies used for ensuring minimal disruption to critical services given various loss scenarios and undesirable operations of plant digital systems.

RG 1.152, Regulatory Position 2.8.3 states that “The licensee should develop an incident response and recovery plan for responding to digital system security incidents (e.g., intrusions, viruses, worms, Trojan horses, or bomb codes). The plan should be developed to address various loss scenarios and undesirable operations of plant digital systems, including possible interruptions in service due to the loss of system resources, data, facility, staff, and/or infrastructure. The plan should define contingencies for ensuring minimal disruption to critical services in these instances.” DCD Section 7.7 does not address contingencies used for ensuring minimal disruption to critical services given various loss scenarios and undesirable operations of plant digital systems.

07.07-27

Address RG 1.152, Regulatory Position 2.8.4 and periodic computer security self-assessments and audits, changes to safety systems, discovery of anomalies and corrective actions, and V&V of modifications as it relates to security.

RG 1.152, Regulatory Position 2.8.4 states that “The licensee should perform periodic computer system security self-assessments and audits, which are key components of a good security program. The licensee should assess proposed safety system changes and their impact on safety system security; evaluate anomalies that are discovered during operation; assess migration requirements; and assess modifications made including V&V tasks to ensure that vulnerabilities have not been introduced into the plant environment from modifications.” DCD Section 7.7 does not address periodic computer security self-assessments and audits, changes to safety systems, discovery of anomalies and corrective actions, and V&V of modifications as it relates to security.