REQUEST FOR ADDITIONAL INFORMATION 239-2033 REVISION 0

3/2/2009

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No. 52-021

SRP Section: 07.06 - Interlock Systems Important to Safety
Application Section: Section 07.06 - Interlock Systems Important to Safety

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

07.06-1

Discuss compliance with 10 CFR 50, §50.34(f)(2)(v) and the indication of the status of safety interlocks being provided to operators. Update Table 7.1-2 if necessary.

The column titled “Related Section in US-APWR DCD” in Table 7.1-2 does not cite §50.34(f)(2)(v) as applicable to DCD Section 7.6. This column indicates that §50.34(f)(2)(v) is related to DCD Section 7.5, which states that the abnormal status of all interlocks for the US-APWR is provided via BISI. However, Section 7.5.2.2 only indicates that the BISI design is based on the requirements of §50.34(f)(2)(v); neither Sections 7.5 or 7.6 indicate that BISI for safety interlocks is provided to operators.

07.06-2

Discuss how the design of interlock systems important to safety meets the requirements of GDCs 10, 15, 16, 28, 33, 34, 35, 38, 41 and 44, (See Table 7-1 of the SRP). Update Table 7.1-2 if necessary.

Table 7.1-2 in the DCD cites compliance with the following GDC for DCD Section 7.6: GDCs 1, 2, 4, 13, 19, 24 and 25; the DCD does not cite compliance with GDCs 10, 15, 16, 28, 33, 34, 35, 38, 41 and 44. The DCD refers to Chapter 4, “Reactor” for conformance with the GDC 10; Chapter 5, “Reactor Coolant System and Connected Systems” for conformance with the GDC 15 and 34; Chapter 6, “Engineered Safety Features” for conformance with the GDC 16, 35, 38 and 41; Chapter 9, “Auxiliary Systems” for conformance with the GDC 33 and 44; and Chapter 15, “Accident Analysis” for conformance with the GDC 28. It is unknown how GDCs 10, 15, 16, 28, 33, 34, 35, 38, 41 and 44 are applied to the design of interlock systems important to safety.

07.06-3

Discuss how GDCs 20, 21, 22, 23, and 29 are applied to the design of interlock systems important to safety. Update Table 7.1-2 if necessary.

Though not listed in SRP Table 7-1 as applicable to information systems required for safety, DCD Table 7.1-2 cites compliance with GDCs 20, 21, 22, 23 and 29 for the PSMS in Section 7.6. Section 7.6 indicates that detailed compliance to the GDC is described (in general, not specifically related to interlock systems) in TR MUAP-07004-

P(R1) Section 3. It is unknown how GDCs 20, 21, 22, 23, and 29 are applied to the design of interlock systems important to safety.

07.06-4

Address the use of any digital-based controllers in safety I&C systems, including any COTS computer-based equipment. This would be applicable to stand alone PLCs or field mounted equipment used anywhere within the US-APWR applicable to equipment described in any chapters of the DCD, not just Chapter 7.

Although the BTP 7-18 is identified as applicable to interlock systems important to safety in SRP Table 7-1, the DCD, Table 7.1-2 indicates that it does not apply to the US-APWR because programmable logic controllers (PLC) are not used in safety I&C systems. It is unknown if computer-based controllers are used and embedded in plant systems and components. In addition, it is unknown if any COTS computer-based equipment are used. If computer-based equipment is embedded in plant systems and components, identify how their quality will be demonstrated.

07.06-5

Identify those regulations applicable to the interlock systems important to safety, i.e., that are applicable to Section 7.6. Update Table 7.1-2 if necessary.

The DCD cites conformance with BTP 7-1 and BTP 7-2 only for the RPS and the SLS, and with BTP 7-12 only for the RPS, ESFAS and SLS. The DCD refers to Section 7.7 for BTP 7-5. The setup of Table 7-1 and inconsistencies between the I&C System columns and the column titled “Related Sections in the US-APWR DCD” prevents an understanding of how requirements and guidance is applied for the design of interlock systems important to safety.

07.06-6

Provide a reference to a diagram that shows the valves, piping, and connections of the CS/RHR system that is referred to in Section 7.6.1.2, “CS/RHR Open Block Interlock,” second paragraph of the first bulleted item.

In Section 7.6.1.2, “CS/RHR Open Block Interlock,” second paragraph of first bulleted item, reference is made to the logic diagram for the interlocks for the valves. While the logic diagrams (Figs. 7.6-2 and 7.6-3) are important, the applicant should also make reference to where the piping diagram (showing the location of the valves, etc.) for the CS/RHR can be found. This will facilitate an understanding of the design and therefore an assessment of how the single failure criterion is met.

07.06-7

Provide a reference to a diagram that shows the valves, piping, and connections of the CS/RHR system that is referred to in Section 7.6.1.2, “CS/RHR Open Block Interlock,” second paragraph of the second bulleted item.

In Section 7.6.1.2, “CS/RHR Open Block Interlock,” second paragraph of second bulleted item, reference is made to the logic diagram for the interlocks for the valves. While the logic diagrams (Figs. 7.6-1 and 7.6-3) are important, the applicant should also indicate where the circuit diagram (showing the layout and number of the valves, etc.) for the CS/RHR can be found. Provision of this information will facilitate an understanding of the design and therefore an assessment of how the single failure criterion is met.

07.06-8

Provide a reference to a diagram that shows the valves, piping, and connections of the primary makeup water supply to the rest of the system that is referred to in Section 7.6.1.3, “Primary Makeup Water Line Isolation Interlock.”

In Section 7.6.1.3, “Primary Makeup Water Line Isolation Interlock,” second paragraph, reference is made to the logic diagram for the interlocks for the primary makeup water stop valves. While the logic diagram (Figs. 7.6-4) is important, the applicant should also make reference to where the piping diagram (showing the location and number of the valves, etc.) for the primary makeup water supply connections to the rest of the system can be found. Provision of this information will facilitate an understanding of the design and therefore an assessment of how the single failure criterion is met.

07.06-9

Provide a reference to a diagram that shows the valves, piping, and connections of the CCW to the rest of the system that is referred to in Section 7.6.1.5, “CCW Supply and Return Header Tie Line Isolation Interlock.,”

In Section 7.6.1.5, “Primary Makeup Water Line Isolation Interlock,” first paragraph below the bulleted items, reference is made to the logic diagram for the interlocks for the isolation valves. While the logic diagram (Figs. 7.6-6) is important, the applicant should also make reference to where the piping diagram (showing the location and number of the valves, etc.) for CCW and its connections to the rest system can be found. This will facilitate an understanding of the design and therefore an assessment of how the single failure criterion is met.

07.06-10

Provide a description of the quality processes used to develop the interlock systems important to safety, or provide a reference that points to the section within the DCD where the quality procedure for Class 1E systems is described.

Section 7.6.2.2, “Quality of Components and Modules,” only states that “all interlocks important to safety are implemented using Class 1E components with a corresponding quality program.” This statement is insufficient to assess the adequacy of the quality program used.

07.06-11

Describe how the interlock systems conform to the interim staff guidance DI&C-ISG-04.

The DCD states that all interlocks important to safety are implemented in the Protection and Safety Monitoring System (PSMS), which is a digital system and also implements other safety functions. The DCD should therefore describe how the interlock systems conform to the interim staff guidance DI&C-ISG-04. The DI&C-ISG-04 guidance specifically addresses issues related to interactions among digital safety divisions and between safety-related equipment and equipment that is not safety-related. The guidance conforms to the principles in IEEE 603-1991 and IEEE 7-4.3.2-2003 by describing means for ensuring independence among redundant safety channels while permitting some degree of interconnection and commonality among those independent channels. Section 7.6.2.3, “Independence,” of the DCD only states that “Redundancy and independent train assignments are specifically discussed for each interlock in the sections above."

07.06-12

Describe how the interlock systems important to safety conform to the requirements of IEEE Std 603-1991, Clause 5.7, “Capability for Test and Calibration,” Clause 5.8, “Information Displays,” and Clause 6.5, “Capability for Testing and Calibration.”

Item D of Chapter 7.6, “Interlock Systems Important to Safety,” of the SRP, requires interlock system important to safety to conform to the requirements of IEEE Std 603-1991, Clause 5.7, “Capability for Test and Calibration,” Clause 5.8, “Information Displays,” and 6.5, “Capability for Testing and Calibration.” Section 7.6.2.4,” System Testing and Inoperable Surveillance,” of the DCD only indicates that system testing and inoperable surveillance for all interlocks is described in subsection 7.6.1 of the DCD. However, while subsection 7.6.1 describes the functions of all the interlocks important to safety, it does not describe how the systems conform to the applicable criteria. Section 7.6.2.4, ”System Testing and Inoperable Surveillance,” of the DCD only states that “System testing and inoperable surveillance for all interlocks is described in Subsection 7.6.1."

07.06-13

Discuss how the interlock systems important to safety meet the requirements of IEEE Std 7-4.3.2.

The US-APWR interlock systems important to safety are implemented in the PSMS and therefore are digital-based systems. The DCD should therefore discuss how the interlock systems important to safety meet the requirements of IEEE Std 7-4.3.2. Section 7.6.2.5, “Use of Digital Systems,” only states that “all interlock systems important to safety are implemented in the PSMS, which is a digital system.” It does not address how the requirements of IEEE Std 7-4.3.2 are met, for example. Section 7.6.3,”Analysis,” of the DCD does state that detailed compliance to the GDC, IEEE Std 603-1991 and IEEE Std 7- 4.3.2-2003 are described in Topical Report MUAP-07004 Section 3.0, Appendix A and B. However, a summary of how the key, applicable criteria are met should be provided in the DCD, with a reference to the Topical Report MUAP-07004 made for any

further details required. In Section 7.6.2.5, “Use of Digital Systems,” of the DCD only states that “All interlocks important to safety are implemented in the PSMS, which is a digital system."

07.06-14

Discuss whether or not the interlocks are software-based.

The US-APWR interlock systems important to safety are implemented in the PSMS and therefore are digital-based systems. It is not clear whether this means that (1) the interlock logic itself is implemented in software in the PSMS, or (2) only initiating signals originate from the PSMS but that the interlock logic is implemented using discrete components. Section 7.6.2.5, “Use of Digital Systems,” of the DCD only states that “All interlocks important to safety are implemented in the PSMS, which is a digital system."

07.06-15

Clarify how the guidance in Position 2 of Section B in BTP 7-1, “Guidance on Isolation of Low Pressure Systems from the High Pressure Reactor Coolant Systems,” is met.

BTP 7-1 states that “for system interfaces where both valves are motor-operated, the valves should have independent and diverse interlocks to prevent both from opening unless the primary system pressure is below the subsystem design pressure. Also, the valve operators should receive a signal to close automatically whenever the primary system pressure exceeds the subsystem design pressure.” In the discussion on the CS/RHR Pump Hot Leg Isolation Valve Open Permissive Interlock (Section 7.6.1.1), it is not clear how these requirements are met.

07.06-16

Describe in detail the “Pull Lock” feature of the motor operated isolation valve (MOIV), the conditions under which this feature could be used and, assuming this feature of the MOIV, how the accumulator discharge design meets position 4 of BTP 7-2, “Guidance on Requirements of Motor-Operated Valves in the Emergency Core Cooling System Accumulator Lines.”

In Section 7.6.1.4, which describes the ECCS accumulator interlock system, it is stated that if the (MOIV) was closed in the “Pull Lock” mode, the accumulator discharge valves will not automatically open, therefore the affected accumulator will be un-available for its designed ESF function. This appears to violate Position 4 of BTP 7-2, which requires “utilization of a safety injection signal to remove automatically (override) any bypass feature that may be provided to allow an isolation valve to be closed for short periods of time…” The DCD indicates that the "Pull Lock" function is described in Topical Report MUAP-07007 Section 4.5.3.a. However, the staff's review of this document for the referenced section showed that Section 4.5.3.a of the Topical Report MUAP-07007, "HSI System Description and HFE Process,” only discusses operation-related information display features of ON/OFF switches. The only reference to the “Pull Lock” feature is a display button in Figure 4.5-4, “Soft Operation Switch Moving Feature.”