REQUEST FOR ADDITIONAL INFORMATION 230-2028 REVISION 0

2/26/2009

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No. 52-021

SRP Section: 07.03 - Engineered Safety Features Systems
Application Section: Section 07.03 - Engineered Safety Features Systems

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

07.03-1

MHI is requested to address GDCs 10, 15 and 16 in Chapter 7 of the DC-FSAR with regards to the ESF system. The DC-FSAR does not address compliance with GDCs 10, 15 and 16 in Section 7.3 or Table 7.1-2, and refers to Chapters 4, 5, and 6, respectively. These GDCs ensure that certain design conditions are not exceeded for AOOs or PAs. Chapter 3.1 addresses compliance with these GDCs but does not address the function of the ESFAS and ESF control systems. Address the occurrence of AOOs and PAs with respect to GDCs 10, 15, and 16 and the ESFAS and ESF control systems function and I&C capability to actuate these systems. Address compliance with GDCs 10, 15, and 16 with respect to the ESFAS and ESF control systems in Chapter 3.1, Chapter 7.3, and Table 7.1-2.

07.03-2

MHI is requested to address GDCs 34, 35, 38 and 41 in Chapter 7 of the DC-FSAR with regards to the ESF system. The DC-FSAR does not address compliance with GDCs 34, 35, 38 and 41 in Section 7.3 or Table 7.1-2, and refers to Chapters 5 and 6. Chapter 3.1 addresses compliance with these GDCs but does not address the function of the ESFAS and ESF control systems. To complete a review of the ESF control systems for conformance to the requirements for testability, operability with onsite and offsite electrical power, and single failures, the DC-FSAR needs to address compliance with these GDCs. Address compliance with GDCs 34, 35, 38, and 41 with respect to the ESFAS and ESF control systems in Chapter 3.1, Chapter 7.3, and Table 7.1-2.

07.03-3

The DC-FSAR does not address compliance with GDCs 33 and 44 in Section 7.3 or Table 7.1-2, and refers to Chapter 9. Chapter 3.1 addresses compliance with these GDCs but does not address the function of the ESFAS and ESF control systems. To complete the review of the applicant's proposed design criteria, design bases, and safety classification for the cooling systems, and the requirements for system performance of necessary functions during normal, abnormal, and accident conditions, assuming loss of offsite power and a single failure, and that system portions can be isolated so the safety function of the system is not compromised, the staff needs to ensure compliance with GDCs 33 and 44. Address compliance with GDCs 33 and 34 with respect to the ESFAS and ESF control systems in Chapter 3.1, Chapter 7.3, and Table 7.1-2.

07.03-4

MHI is requested to address applicability of RG 1.151 with regards to the ESF system in the DC-FSAR. The DC-FSAR does not cite compliance with RG 1.151 for the ESFAS or ESF control systems in Table 7.1-2. However, DC-FSAR Table 1.9.1-1 (Tier 2) and MUAP-07004-P cite compliance with RG 1.151 but not specifically with respect to ESFAS or ESF control systems. MHI is requested to address conformance with RG 1.151 in DC-FSAR Table 7.1-2.

07.03-5

MHI is requested to address compliance with BTP 7-13 with respect to the ESFAS and ESF control systems in DC-FSAR. DC-FSAR Table 7.1-2 does not cite compliance with BTP 7-13 for ESFAS; however, MUAP-07004-P cites compliance with BTP 7-13 will be in the plant licensing documentation, as does Table 1.9.2-7 (Tier 2).

07.03-6

MHI is requested to explain how independence between the RPS and the ESF is achieved, whether sensors are shared between the reactor trip system and the engineered safety system, how this relates to the defense-in-depth (D3) approach used in the US-APWR, and what subsystems are used to achieve D3 in the US-APWR. This should be adequately explained in the DC-FSAR/

The description of how the ESF system is actuated by signals from the RPS suggest that the ESF is not independent of the RPS and cannot function without the RPS. Current guidelines for D3 (e.g., BTP 7-19) indicate independence among control, trip, engineered safety features, and post accident monitoring systems as an appropriate defense-in-depth approach. If an alternative D3 approach is used, the difference between the US-APWR and conventional approaches needs to be briefly explained and the document where this approach is described needs to be referenced.

07.03-7

MHI is requested to explain how a failure of one of the subsystems of an ESF train is detected, and how such a failure affects the response of the corresponding SLS train. This should be adequately explained in the DC-FSAR.

Figure 7.3-1 of the DC-FSAR shows that each ESF train has two redundant subsystems (CPU 1A1 and CPU 1A2). The diagram also suggests that each of these subsystems processes the same set of trip/no trip information from all four protection system trains, and actuate the necessary ESF systems and/or components to mitigate abnormal and/or accident condition(s). Each of the ESF subsystems (of a single train) communicates its information to redundant SLS subsystems (of a single train) via the safety system bus. It is not clear whether the communication protocol is such that a failure of an ESF subsystem is detected by the corresponding ESF train, by the corresponding SLS subsystem, or by any of the SLS subsystems.

07.03-8

Identify the FMEA section, table, or report that describes which process or processes were assigned to which controller, and how the failure analyses was performed to reach such decisions. This should be adequately addressed in the DC-FSAR.

The DC-FSAR states that plant process systems are assigned to controllers based on consideration of maintenance, potential SLS equipment failures, and optimization of controller performance. Multiple process systems are assigned to the same controller or a single process system is assigned to multiple controllers only if the plant effects of controller failure and maintenance are demonstrated to be acceptable, based on the FMEA. The staff needs to review the FMEA analysis for adequate assurance that the design complies with the single failure criterion.

07.03-9

MHI is requested to explain in detail and with figures, the priority logic portions of the SLS, showing all inputs to the priority logic, which actuators use such priority logic, and how the diverse actuation requirements are met.

The SLS has portions with priority logic "to accommodate signals from the diverse actuation system." Position 2 of Section 2, "Command Prioritization," of Interim Staff Guidance DI&C-ISG-04, states that "priority modules used for diverse actuation signals should be independent of the remainder of the digital system, and should function properly regardless of the state or condition of the digital system. If these recommendations are not satisfied, the applicant should show how the diverse actuation requirements are met. The staff needs further clarification to make a determination as to whether the design of the SLS satisfies this guidance.

07.03-10

MHI is requested to identify if the priority module identified in Section 7.3.1.5.8.2 contain any software? If so describe the processes used to assure the quality of the software. If the priority module does not include any software, describe the process for accepting any software tools used to assure the quality of the design of the priority module.

Clause 5.3, "Quality," of IEEE Std 603-1998, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," requires safety system equipment to be designed, manufactured, inspected, installed, tested, operated, and maintained in accordance with a prescribed quality assurance program. Guidance on the application of this criterion for safety system equipment employing digital computers and programs or firmware is found in IEEE Std 7-4.3.2-1993. Priority modules are safety-related systems, and the staff requires assurance that any software that is part of the priority module has undergone the same V&V as the rest of the safety system. If the priority module does not contain any software, then Position 6 of Section 2, "Command Prioritization," of DI&C-ISG-04 requires software used in the design, testing, maintenance, etc. of a priority module to be subject to all of the applicable guidance in Regulatory Guide 1.152, which endorses IEEE Std 7-4.3.2-2003 (with comments). This

includes software applicable to any programmable device used in support of the safety function of a prioritization module, such as programmable logic. Position 6 of Section 2 of DI&C-ISG-04 also states that validation of design tools used for programming a priority module or a component of a priority module is not necessary if the device directly affected by those tools is 100% tested before being released for service. The staff needs to know the design details and the process of accepting the software tools to make an assessment of the adequacy of the quality of the priority module.

07.03-11

MHI is requested to identify if the priority module identified in Section 7.3.1.5.8.2 of the SLS train control one component, or does it control more than one component? If a priority module controls more than one component, show how the independence requirement above is met.

Position 4 of Section 2, “Command Prioritization,” of Interim Staff Guidance DI&C-ISG-04, states that a priority module may control one or more components, but that if a priority module controls more than one component, then all of the recommendations stated in the ISG also apply to each of the actuated components.

07.03-12

MHI is requested to provide in Sections 7.3.2.8, and 7.2.2.8, “Equipment Qualification,” of Chapter 7 of US-APWR DC-FSAR, a concise but sufficient information of the environmental qualification results, to enable adequate review without having to refer to (several) other reports. A reference to another report providing further details may be contained in the DC-FSAR. However, the reviewer should only have to resort to this if there are questions regarding the results or if further details of the testing methodology are required.

Sections 7.3.2.8 and 7.2.2.8, “Equipment Qualification,” of the DC-FSAR refers to Subsection 7.1.3.7 for details of the qualification of the safety systems. This section states that the PSMS is qualified for worst-case environmental and seismic requirements for the place of its installation. However, it does not provide details of the tests, nor does it point to any report(s) that document the test procedure and results. The DC-FSAR states that details of PSMS qualification testing may be found in TR MUAP-07004-P, Sections 5.2.1 through 5.2.5. However, these sections only describe environmental design features and service conditions. They do not provide environmental, seismic, and EMI/RFI test results, nor do they reference any test reports. Section 5.2.1 of TR MUAP-07004-P states that the PSMS is located in the main control room, remote shutdown room and I&C equipment rooms so that it is not influenced by external effects such as tornadoes, hurricanes and floods. It also states that the PSMS is located in areas where the radiation influence is negligible (i.e. up to 103 rads (10 Gy)). Section 5.2.2 of the same reference further states that the PSMS, including the Safety VDU, is classified as Class 1E Seismic Category 1, and that the system is qualified to maintain physical integrity and all functionality during and after an Operating Basis Earthquake and a Safe Shutdown Earthquake. The DC-FSAR refers to TR MUAP-07005-P for further details regarding the seismic testing.

Details of seismic qualification testing are provided in Section 5.2 of TR MUAP-07005-P, although this TR is not referenced in the US-APWR DC-FSAR in regard to seismic qualification testing.

07.03-13

MHI requested to provide sufficient information to show that, for the cases in which manual ESF actuation is used as the second and only means of providing signal diversity, the response time requirement for the safety function is met.

The US-APWR DC-FSAR does not contain sufficient information for assessing the adequacy of providing manual ESF actuation as the only means for achieving signal diversity. Part F of Section II, “Review Procedures,” of Chapter 7.3, “Engineered Safety Features Systems,” of the SRP allows manual activation to be used as the alternate, diverse means, of ESF actuation if it is consistent with the response time requirements of the function (i.e., for the mitigation of the accident scenario).

07.03-14

MHI is requested to provide equipment location drawings for the ESF per RG 1.206, Section C.I.7.3.1.2. Section 7.3.1.2, with regards to the SLS controllers, states that "I/O for each train in the US-APWR is remotely distributed throughout the plant." At this discussion reference should be made to the equipment location drawings. Also, is the remote I/O located in harsh environment areas or areas which would require qualification beyond normal mild environment criteria?

07.03-15

MHI is requested to identify how Clause 6.2.1 of IEEE Std 603-1991 is met for the ESF System. Clause 6.2.1 of IEEE Std. 603-1991 states that "means shall be provided in the control room to implement manual initiation at the division level of the automatically initiated protective actions. The means provided shall minimize the number of discrete operator manipulations and shall depend on the operation of a minimum of equipment." Regulatory Guide 1.62 states in Regulatory Position C.4 the staff position for what constitutes "operation of a minimum of equipment." The ESF manual system level initiation path, presented in Figure 7.3-1, does apparently use common digital components with the automatic protection line. MHI is requested to thoroughly explain by text and confirmation via figures, how Clause 6.2.1 of IEEE Std. 603-1991 and RG 1.62 is met by the US-APWR for ESF manual actuations.