REQUEST FOR ADDITIONAL INFORMATION 231-2037 REVISION 0

2/26/2009

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No. 52-021

SRP Section: 07.09 - Data Communication Systems
Application Section: Section 07.09 - Data Communication Systems

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

07.09-1

MHI is required to comply with 10 CFR 50.34(f)(2)(v) and 50.62 in relation to the DCSs. MHI is requested to discuss this in Section 7.9 and Table 7.1-2 should be updated to reflect this requirement.

Table 7.1-2 in the DC-FSAR cites compliance with various regulations applicable to the DCS with the exception of §50.34(f)(2)(v) and §50.62. §50.34(f)(2)(v) requires licensees to provide for automatic indication of the bypassed and operable status of safety systems. The DCSs support ATWS mitigation functions and RTS functions. The staff cannot determine if the DCS adequately supports RTS and ESFAS functions as necessary to sense accident conditions and AOOs in order to initiate protective actions consistent with the accident analysis presented in Chapter 15 of the DC-FSAR, without compliance with the above regulations known.

07.09-2

MHI is requested to address compliance with GDC 24 in relation to the DCSs and the interfaces between the DCS and plant operating control systems in the DC-FSAR. This information will aid the staff in its determination that the system satisfies the requirements of IEEE Std 603-1991 with regard to control and protection system interactions. Update Table 7.1-2 if necessary.

SRP Table 7-1 and SRP 7.9 cite/discuss compliance with GDC 24. SRP 7.9 indicates that GDC 24 is applicable to all DCSs. This means that GDC 24 is applicable to data links (e.g., RPS/ESFAS links), the control network (e.g., within and between safety/nonsafety links), and the maintenance network. Section 3.1 of the DC-FSAR discusses compliance with GDC 24 but Table 7.1-2 does not cite compliance for data communications. To assess if the DCS satisfies the requirements of GDC 24, the staff requires sufficient information to evaluate the DCS and plant operating control systems and the interactions between the control and protection system interactions.

07.09-3

MHI is requested to address in Section 7.9 of the DC-FSAR conformance with RG 1.47 in relation to the DCS, and the philosophy and criteria for bypass and inoperable status indication. Update Table 7.1-2 if necessary.

RG 1.47 describes an acceptable method of complying with the requirements of Appendix B to 10 CFR 50 with regard to indicating the inoperable status of a portion of the protection system. The design of the PSMS and ESFAS allows certain safety-related functions to be bypassed or made inoperable during the performance of periodic tests or maintenance. Experiences at operating plants indicate that when the measures used to indicate inoperable status consist solely of administrative procedures, the operator is not always fully aware of the ramifications of each bypassed or inoperable component. An acceptable way of aiding the operator's knowledge of plant status is to supplement administrative procedures with automatic indication of the bypass or inoperability of each redundant portion of a system that performs a function important to safety. The US-APWR allows bypassed or inoperable functions but it is unknown if the indication follows the guidance provided in RG 1.47.

07.09-4

MHI is requested to identify in Section 7.9 compliance with the guidelines of RG 1.204 in relation to the DCS, 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 DC-FSAR Tier 2 does not cite conformance with RG 1.204 for the DCS. With respect to the DCS, the review is to ensure that proper communication and isolation exists between the PCMS and PSMS.

07.09-5

MHI is requested to address conformance with the SRM to SECY 93-087 II.Q and II.T in relation to the DCS; any potential common-mode failures; and the applicable EPRI requirements for redundancy, independence, and separation. This should be addressed in the DC-FSAR and update Table 7.1-2 if necessary.

Table 7.1-2 does not cite conformance with the SRM to SECY 93-087 in the DC-FSAR for the DCS. Section II.Q requires an evaluation of diversity and defense-in-depth and allows the use of a nonsafety system if the system is of sufficient quality. To demonstrate that vulnerabilities to common-mode failures have adequately been addressed and when analyzing each postulated common-mode failure for each event that is evaluated in the accident analysis section of the DC-FSAR requires consideration of DCS failures. Section II.T requires that the alarm system meet the applicable EPRI requirements for redundancy, independence, and separation.

07.09-6

MHI is requested to address conformance with BTP 7-19 guideline in relation to the DCS, any potential common-mode failures, and the propagation of erroneous data. Update Table 7.1-2 if necessary.

Table 7.1-2 does not cite conformance with BTP 7-19 for the DCS. Table 1.9.1-7 indicates that BTP 7-19 is applicable without any exceptions identified. Digital I&C systems can be vulnerable to common-cause failures caused by software errors, which could defeat the redundancy achieved by hardware architecture. Failures in the communication system—either by not transmitting data, transmitting erroneous data, or by generating false data—can cause failures in one or more trains.

07.09-7

MHI is requested to address the differences between a temporary connection of the engineering tool in TR MUAP-07005 and a permanent connection for the engineering tool in the DC-FSAR and revise the documents accordingly. Also, the methods used to verify the authenticity and integrity of the application software must be addressed in docketed information.

The continuous connection described in the Section 7.9.1.5 of the DC-FSAR is different from the temporary connection of the engineering tool described in TR MUAP-07005. In addition, the engineering tool can be used to change application setpoints and constants, and update controller software. IEEE 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," Clause 5.3.2, "Software tools" requires"

- that either a test tool validation program be used to provide confidence that the software tool functions properly, or
- that the software tool be used in a manner such that defects not detected by the software tool will be detected by V&V activities

The authenticity and integrity of the application software is verified by the software installation procedure as described in TR MUAP-07005. The differences between a temporary connection and a permanent connection should be provided in the DC-FSAR, as should the verification of the authenticity and integrity of the application software.

07.09-8

MHI is requested to include in Section 7.9 of the DC-FSAR a concise description of the quality of the components and modules of the DCS and the quality of the design process and its relationship with NQA-1, so as to enable a review of the quality of the DCS. Refer the reader to specific section of Chapter 17 of the DC-FSAR for further details if necessary.

Section 7.9.2.1, "Quality of Components Module," contains very little information regarding the quality of the components of the DCS, but refers the reviewer to Chapter 17 of the DC-FSAR. Section 7.9.2.1 should contain a concise but sufficient amount of information to enable a review of the quality of the DCS components and modules.

Based on the limited information provided, the acceptability of the component quality is contingent upon acceptance of the quality plan provided in Chapter 17.

07.09-9

MHI is requested to revise the following typographical error. In the second sentence of the second paragraph of section 7.9.2.1, "Quality of Components and Modules," of US-APWR Chapter 7, change the second "PCMS" to "PSMS." The sentence should now read "The PCMS has a similar quality program to the PSMS, without the same level of documentation."

Section 7.9.2.1, "Quality of Components and Modules," states that "The PCMS has a similar quality program to the PCMS, without the same level of documentation." This is a typographical error and should be corrected.

07.09-10

MHI is requested to provide, in the DC-FSAR, a summary of the DCS software quality program and how it meets BTP 7-14 in sufficient detail to enable an adequate review to be performed, and provide appropriate reference(s) that will provide further details if required.

Section 7.9.2.2 of the DC-FSAR describes the software quality of the DCSs of the US-APWR. MHI applies its MELCO's safety system digital platform MELTAC to the PSMS and PCMS systems. The DC-FSAR states that the software quality program for the MELTAC basic software is discussed in TR MUAP-07005 Section 6.0, that a summary of the software quality program for the system application software is discussed in TR MUAP-07004 Section 6.0, and that a description of the application software quality program is provided in the Software Program Manual for US-APWR Technical Report MUAP-07017. The above shows that the entire software quality description in the DC-FSAR consists of a series of references to other reports. This is not sufficient for an adequate review of the software quality of the data communication components and modules. At least a summary of the DCS software quality program and how it meets BTP 7-14 should be provided in this DC-FSAR to enable an adequate review to be performed. Appropriate reference(s) can then be mentioned that will provide further supporting details if required.

07.09-11

MHI is requested to provide a more detailed analysis on the docket and preferably in Section 7.9.2.3 of how the DCSs meet the regulatory position of BTP 7-21.

The staff performed a review of the documentation in the DC-FSAR regarding performance requirements of the DCSs. Section 7.9.2.3 of the DC-FSAR briefly describes the system performance requirements, including brief descriptions of system deterministic timing (Section 7.9.2.3.1), real time performance (Section 7.9.2.3.2), time delays within the DCS (Section 7.9.2.3.3) and data rates and bandwidth (Section 7.9.2.3.4). None of these sections contains sufficient information in and of itself to enable

an adequate review to be performed, but points to other reports which may themselves point to inadequately referenced reports. For example, Section 7.9.2.3.2, "Real Time Performance," of the DC-FSAR states that "for each safety function an analysis has been performed which demonstrates that the actual system response time is less than the response time required by the plant safety analysis," and refers to TR MUAP-07004 Section 6.5 (which should actually be Section 6.5.3) for the details. Section 6.5.3, "Response Time Analysis Method," of TR MUAP-07004-P uses the response time model for reactor trip to illustrate the response time analysis method used. This model requires knowing the response time of the digital controller used in the digital loop. TR MUAP-07004-P states that the response time calculation method for the digital controller "is described in the Digital Platform Topical Report," but does not provide the document number for this report. A summary of how the DCS meets performance requirements per BTP 7-21 should be provided in the DC-FSAR in sufficient detail to enable an adequate review to be performed.

07.09-12

MHI is requested to identify how the DCS meets the single failure criterion in the DC-FSAR, preferably in Section 7.9.2.4.

The US-APWR DC-FSAR briefly discusses (in one short paragraph) potential hazards and how the DCS addresses single failures in Section 7.9.2.4. The DC-FSAR states that "self-diagnostic features described in Topical Report MUAP-07004 Section 4.3, detect DCS errors or failures. All DCS errors and failures are analyzed in the FMEA, which demonstrates that there are no single failures that can result in loss of the safety function." In numerous instances, the TRs refer to "credible" single failures rather than single failures. The purpose and what the single failure analysis shows are not discussed.

07.09-13

MHI is requested to provide a summary of the self diagnostic feature and any hazards of the DCS, but in sufficient detail to enable an adequate review to be performed.

Section 7.9.2.4 references Section 4.3, "PSMS Self-diagnostics Features," of TR MUAP-07004, which indicates that the self diagnostic features of the digital platform continuously check the integrity of processing and communication components as well as the range of process inputs. In addition, the redundant system inputs from different trains are continuously compared to detect failed/drifting instrumentation or input modules. This comparison is performed continuously in the Unit Management Computer of the PCMS; deviations are alarmed in the MCR. If the necessary information provided in the TR is not in Section 7.9.2.4 it should at least be referenced specifically.

07.09-14

MHI is to provide the results of the Failure Modes and Effects Analysis (FMEA) in sufficient detail to enable a review. Also, provide a complete reference to the detailed FMEA report in the DC-FSAR.

In Section 7.9.2.4, “Potential Hazards and Single Failures” of the DC-FSAR the only discussion on FMEA is the statement that “All DCS errors and failures are analyzed in the FMEA, which demonstrates that there are no single failures that can result in loss of the safety function.” This statement is made without a reference to any particular FMEA analysis or report. Section 4.3, “PSMS Self diagnostic Features” of MUAP-07004, is referenced but is only one paragraph long, and refers to *Digital Platform Topical Report* for further details. This one-paragraph discussion in and of itself does not provide sufficient detail to allow an adequate staff review to be performed, even when consulting a TR for additional information. Additionally, a description of the FMEA process or what guidance the process followed is not provided. The FMEA should address failures to the black-box, module level for components in the I&C design (e.g. communication modules).

07.09-15

MHI is requested to address how the DCS addresses communication independence and conformance with RG 1.152 in the DC-FSAR Section 7.9.

There is insufficient information in Section 7.9.2.7 to allow a review of logical independence of the DCS. In particular, the DC-FSAR does not discuss how the DCS meets communication independence per RG 1.152. The only discussion on communication independence is the statement that “each PSMS and PCMS controller/processor protects itself against DCS errors or failures that could disrupt its internal application functions, thereby ensuring communications independence.” The DC-FSAR does not discuss how this protection “against DCS errors or failures” is actually achieved.