

REQUEST FOR ADDITIONAL INFORMATION 275-2133 REVISION 1

3/11/2009

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No. 52-021

SRP Section: 14.03.05 - Instrumentation and Controls - Inspections, Tests, Analyses, and Acceptance Criteria

Application Section: 14.3.5 Instrumentation and Controls - Inspections, Tests, Analyses, and Acceptance Criteria

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

14.03.05-22

Provide a figure of the DAS, clearly showing its interface with the PSMS.

The design description provided in Tier 1 includes a narrative that states the system purpose, significant performance characteristics and safety functions, whether it is safety-related or not, system location, key design features, seismic and ASME code classifications, description of system operation, major controls and displays, logic circuits, interlocks, Class 1E power sources and divisions, equipment to be qualified for harsh environments (and other than harsh for certain I&C equipment), and interface requirements. Not provided however, is a simplified schematic figure of the DAS in Tier 1. Although figures are not required generally for simple non-safety significant systems, per Appendix A of SRP 14.3, "the amount of information depicted is based on the safety significance of the SSCs." The DAS interfaces with the PSMS. A figure is necessary to understand this interface.

14.03.05-23

Address the possible use of digital components in the DAS. If any digital equipment is used in the DAS, revise the DCD (Tiers 1 and 2) accordingly.

Item 5 in Table 2.5.3-4 shows that the quality of DAS components and modules and the quality of the DAS design process (including the software life cycle process for digital equipment) are controlled by an augmented quality program that meets the regulatory requirements that will be inspected to ensure that the as-built design meets commitments. DCD Tier 2, Section 7.8 states that "The DAS design consists of conventional equipment that is totally diverse and independent from the MELTAC platform of the PSMS and PCMS, so that a beyond design basis CCF in these digital systems will not impair the DAS functions." The indication of a software life-cycle process associated with a conventional (i.e., analog) system is confusing.

Similar to Item 5, Item 3 in Table 2.5.3-4 indicates that the DAS functions, including input/output interfaces, signal processing and HSI, are diverse from software used within the PSMS. This statement does not indicate that digital equipment will be used in the DAS but the acceptance criterion indicates that "The as-built DAS equipment is diverse from software used within the as-built PSMS. The difference may be use of different

REQUEST FOR ADDITIONAL INFORMATION 275-2133 REVISION 1

technology (e.g., analog vs. digital), or different operating system and different application software." The terms "may be," different operating system, and different application software" imply that the DAS may use digital equipment, yet the DAS is a "conventional" analog system. Changing it to a digital system would invalidate the D3 approach and analysis for the US-APWR.

14.03.05-24

Do the tests associated with Item 2 in Table 2.5.3-4 include tests of the manual controls as well as simulated signal inputs to test the system?

Item 2 in Table 2.5.3-4 indicates the DAS has the capability for the following functions:

- Operates with both DAAC divisions operable (i.e., in a two-out-of-two configuration), or with one division manually tripped and one division operable.
- The system can be tested manually without causing component actuation which would disturb plant operations.
- Loss of power or removal of a module does not cause spurious DAS actuation.
- Capability to bypass failed sensors functions.

A test of the as-built DAS will be performed to ensure that the as-built function of the DAS meets the design commitment. The interfaces between the DAS and PSMS are verified and tested under the ITAACs associated with the PSMS. It is unknown if these tests include a test of the manual controls and a test of the system using simulated signal inputs.

14.03.05-25

Address any ITAACs on DCS components that have safety-significance and interfaces with external networks.

Section 7.9 of Tier 2 of the DCD gives information on additional DCS components that have safety-significance, such as safety VDU communication, station bus and external network interface. As stated in Appendix A to Section 14.3 of the SRP, the design descriptions in Tier 1 should include a narrative and simplified figures. External network interface, for instance, provides a firewalled interface from the PCMS and PSMS to external networks, but it is not mentioned in Tier 1. These components should be treated at the Tier 1 level, and specific ITAAC entries be added.

14.03.05-26

Discuss the applicability of IEEE Std 603-1991 Section 4.8 to the DCS as it relates to an ITAAC for those conditions that have the potential to cause a functional degradation of the DCS.

Based on the requirements of IEEE Std 603-1991, Section 4.8, the ITAAC should include analysis of the conditions that have the potential to causing functional degradation of safety systems (e.g., missiles, pipe breaks, fires, loss of ventilation,

REQUEST FOR ADDITIONAL INFORMATION 275-2133 REVISION 1

spurious operation of fire suppression systems, operator error, failure in non-safety-related systems).

Because the DCS is a safety-related system and provides interface functions for other safety systems, the ITAAC for the DCS should address the requirements set forth by Section 4.8 of IEEE Std 603-1991. The ITAAC can be stated as Item 8 of Table 2.5.1-5 specifically for the DCS components or Item 8 of Table 2.5.1-5 could be expanded to include DCS components.

14.03.05-27

Address the issues set forth by Section 5.5 of IEEE Std. 603-1991 with respect to an ITAAC to analyze or demonstrate that the safety-related portions of the DCS have been designed to accomplish their safety functions under the full range of applicable conditions enumerated in the design basis.

Based on the requirements of IEEE Std 603-1991, Section 5.5, the ITAAC should include analysis or demonstration to show that the safety systems have been designed to accomplish their safety functions under the full range of applicable conditions enumerated in the design basis.

Item 2 in Table 2.5.6-1 requires type tests and/or analyses be performed on the DCS equipment to ensure that the DCS provides adequate throughput to meet the response time requirements for all safety functions. The staff reviewed the information provided in Tier 1 and the ITAAC given in Table 2.5.6-1, and cannot conclude that Section 5.5 of IEEE Std 603-1991 is properly addressed in the ITAAC. Will there be an ITAAC to perform any analyses to show that the safety systems have been designed to accomplish their safety functions under the full range of applicable conditions enumerated in the design basis?

14.03.05-28

Address the issues set forth by Section 5.6 of IEEE Std. 603-1991 with respect to an ITAAC to analyze or demonstrate that there is physical, electrical, and communications independence between redundant portions of the safety systems, between different DCS safety systems and effects of a DBE, and between the DCS and other systems.

Based on the requirements of IEEE Std 603-1991, Section 5.6, the ITAAC should include analysis or demonstration to show that there is physical, electrical, and communications independence between redundant portions of a safety system, between safety systems and effects of a DBE, between safety systems and other systems.

The staff reviewed Section 2.5 and the ITAAC in Tier 1 of the DCD and concluded that Section 5.6 of IEEE Std. 603-1991 is not properly addressed. Specifically, Item 15 in Table 2.5.1-5 could be expanded, or a new entry for applications other than the RT and ESF systems, to include confirmation of physical, electrical and communications separation.

REQUEST FOR ADDITIONAL INFORMATION 275-2133 REVISION 1

14.03.05-29

Address the issues set forth by Section 5.7 of IEEE Std. 603-1991 with respect to an ITAAC to analyze or demonstrate that the safety-related portions of the DCS have the capability to be tested and calibrated while retaining the systems' capability to accomplish its safety functions.

Based on the requirements of IEEE Std 603-1991, Section 5.7, the ITAAC should include analysis or demonstration to show that the safety systems have the capability to test and calibrate safety system equipment while retaining the systems' capability to accomplish their safety functions.

The MELTAC controller has separate self-diagnostic features for each of the DCS-related modules. It is assumed no periodic manual surveillance tests are required for DCS functions. It is unclear if Item 2 in Table 2.5.6-1 includes a test of the on-line diagnostics for the DCS to ensure that the diagnostics do not interrupt plant control. Address any ITAACs associated with self-diagnostics of the DCS systems.

14.03.05-30

Address the issues set forth by Section 5.12 of IEEE Std. 603-1991 with respect to an ITAAC to analyze or demonstrate that auxiliary supporting features do not degrade the safety-related portions of the system below an acceptable level.

Based on the requirements of IEEE Std 603-1991, Section 5.12, the ITAAC should include analysis or demonstration to show that auxiliary supporting features meet all requirements of this standard, and do not degrade the safety systems below an acceptable level.

This criterion applies to all safety systems and applicability its to all sections of 2.5. For example, the primary support system for the DCS is electrical power. While Items 1 and 2 in Table 2.5.6-1 indicate that the DCS will be inspected and type tests will be performed, it is unclear if the inspections and tests include electric power. For example, does the ITAAC for Item 2 include test for confirm electrical supply configurations for the DCS? Do the tests include a loss of power test for each division?

14.03.05-31

Address the applicability of GDC 19 to the DCS with respect to an ITAAC to verifying that communications exist that support instruments and controls within the control room to allow actions to be taken to maintain the nuclear power unit in a safe condition during shutdown, including shutdown following an accident.

Based on the requirements of GDC 19, the ITAAC should verify that (1) actions can be taken in the control room to safely operate the nuclear power unit under normal conditions, and maintain it in a safe condition under accident conditions, including LOCAs, and (2) adequate radiation protection has been provided to permit access to, and occupancy of, the control room under accident conditions, for the duration of the accident, without personnel receiving radiation exposures in excess of the total effective dose equivalent (TEDE) of 0.05 Sv (5 rem) specified in 10 CFR 50.2.

REQUEST FOR ADDITIONAL INFORMATION 275-2133 REVISION 1

GDC 19 is applicable to the DCS in the US-APWR in that the DCSs have been provided to support instruments and controls within the control room to allow actions to be taken to maintain the nuclear power unit in a safe condition during shutdown, including shutdown following an accident. An ITAAC verifying that the plant can be maintained in a safe condition under accident conditions, including LOCAs, and that adequate radiation protection has been provided to permit access to, and occupancy of, the control room under accident conditions was not found in the Tier 1 documentation.