

REQUEST FOR ADDITIONAL INFORMATION 255-2110 REVISION 1

3/3/2009

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

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

14.03.05-10

Provide clarification on the commitment to provide information on all Class 1E cabinets, in Sections 2.5.1, 2.5.2, 2.5.4 and 2.5.6, layout and wiring details and indicate if an ITAAC will be performed to ensure that the cabinet layout and wiring conforms to the design.

In SRP Section 14.3, Section I. "Design Descriptions and Figures" for I&C equipment, states the cabinet and layout and wiring should be included in the hardware architecture descriptions.

14.03.05-11

Provide a discussion on the technically relevant Unresolved Safety Issues (USIs)/Generic Safety Issues (GSIs), Three Mile Island (TMI) items and operating experience related to the RT system and ESF systems in the ITAAC for the applicable Sections of 2.5.

To ensure that the ITAAC reflect the resolutions of technically relevant USIs/GSIs, TMI items, and operating experience requires that these be evaluated in Tier 1. SRP Section 14.3, states "Ensure that the ITAAC reflect the resolutions of technically relevant USIs/GSIs, TMI items, and operating experience." The staff did not find reference to USI/GSIs, TMI items and operating experience related to the RT system and ESF systems in the ITAAC. Revise the information in Tier 1 and Tier 2 of the DCD to include any reference to USI/GSIs, TMI items and operating experience, and modify the ITAAC.

14.03.05-12

Address the applicability of IEEE Std. 603-1991, Section 4.6 with respect to an ITAAC to verify the number and locations of sensors in the RT and ESF safety systems that have a spatial dependence.

Based on the requirements of IEEE Std 603-1991, Section 4.6, the ITAAC should include identification in the as-built design of the minimum number and locations of sensors having spatial dependence that are required for protective actions.

REQUEST FOR ADDITIONAL INFORMATION 255-2110 REVISION 1

The staff conducted a review of the DCD Tier 1 and Tier 2 as well as the ITAAC in Table 2.5.1-5 and concluded that no information is given on the minimum number and locations of spatially dependent sensors. Provide as-built information that establishes the minimum number and locations of the spatially dependent sensors that the RT and ESF systems required for protective actions (i.e., revise the ITAAC in Table 2.5.1-5 to address the requirements of Section 4.6 of IEEE Std. 603-1991).

14.03.05-13

Address the applicability of IEEE Std. 603-1991, Section 5.10 with respect to an ITAAC to verify that RT and ESF systems have been designed to facilitate timely recognition, location, replacement, repair, and adjustment of malfunctioning equipment.

Based on the requirements of IEEE Std 603-1991, Section 5.10, the ITAAC should verify that the safety systems have been designed to facilitate timely recognition, location, replacement, repair, and adjustment of malfunctioning equipment.

Design description given in Section 2.5.1.1 does not address any particular design commitment to facilitate timely recognition, location, replacement, repair, and adjustment of malfunctioning equipment. The staff considers that Section 5.10 of IEEE Std. 603-1991 requires that the safety system be designed for easy maintenance and repair. Therefore an ITAAC should be created to verify the as built design of the PSMS provides the operator and maintenance personnel with the necessary alarms and monitoring indications for the timely recognition and adjustment of malfunctions within the PSMS.

14.03.05-14

Address the applicability of IEEE Std. 603-1991, Section 6.3 with respect to an ITAAC to analyze or demonstrate that no single credible event can cause a non-safety system action that results in a condition, which requires RT or ESF action and can concurrently prevent that protective action in sense and command feature channels that are designated to provide principal protection against the condition.

Based on the requirements of IEEE Std 603-1991, Section 6.3, the ITAAC should include analysis or demonstration to show that no single credible event (including the event's direct and consequential results) can cause a non-safety system action that results in a condition, which requires protective action and can concurrently prevent that protective action in sense and command feature channels that are designated to provide principal protection against the condition.

The staff reviewed the information in DCD Tier 1 and the ITAAC in Table 2.5.1-5, and concluded that no analysis is provided that addresses the requirement of Section 6.3 of IEEE Std. 603-1991. The information in DCD Tier 1 should be revised to include an analysis on the interaction between sense and command features and other systems, and modify the ITAAC in Section 2.5.1, accordingly.

REQUEST FOR ADDITIONAL INFORMATION 255-2110 REVISION 1

14.03.05-15

Address the applicability of IEEE Std. 603-1991, Section 6.5 with respect to an ITAAC to analyze or demonstrate that there are means for checking, with a high-degree of confidence, the operational availability of each sense and command feature input sensor that may be required for the RT or ESF function during reactor operation.

Based on the requirements of IEEE Std 603-1991, Section 6.5, the ITAAC should include analysis or demonstration to show that there are means for checking, with a high-degree of confidence, the operational availability of each sense and command feature input sensor that may be required for a safety function during reactor operation.

Item 17 in Table 2.5.1-5 addresses online testing capability of individual PSMS channels or divisions without impeding the safety function. Item 17 requires that a single channel or division bypass capabilities in the PSMS will be tested to ensure that a single channel or division can be bypassed to allow on-line testing, maintenance, or repair without impeding the safety function. However, a specific ITAAC is not provided to demonstrate the availability of each sense-and-command sensor that may be required for a safety function. Section 2.5.1 in DCD Tier 1 should address the availability test for each sense-and-command-feature input sensor, and provide technical means to demonstrate the availability of such a sensor.

14.03.05-16

Address the applicability of IEEE Std. 603-1991, Section 7.3 with respect to an ITAAC to analyze or demonstrate that the RT and ESF systems are designed so that once initiated, the protective actions of “execute features” should proceed to completion.

Based on the requirements of IEEE Std 603-1991, Section 7.3, the ITAAC should include that once initiated, the protective actions of the execute features shall go to completion.

Section 2.5.1.1, “Design Description” states that automatically- or manually-initiated PSMS protection functions are sealed-in to ensure that the protective actions go to completion. The staff considers that Items 1 and 2 of the ITAAC in Table 2.5.1-5 verify the functional arrangement of the RPS and ESF, respectively. Because, completion of protective actions is given as part of the design commitment, the staff expects that this test will be a part of the inspection of the as built RPS and ESF. The staff concludes that Section 7.3 of IEEE Std. 603-1991 would be properly addressed by the ITAAC with a corresponding ITAAC in Table 2.5.1-5.

14.03.05-17

Please revise the description of operation to indicate how the completion of safe shutdown protective actions is analyzed or demonstrated.

Based on the requirements of IEEE Std 603-1991, Section 5.2, the ITAAC should verify or demonstrate that the safety systems are designed so that, once initiated (automatically or manually), the intended sequence of protective actions of the “execute

REQUEST FOR ADDITIONAL INFORMATION 255-2110 REVISION 1

features” should continue until completion, and deliberate operator action is required to return the safety systems to normal.

The completion of protective active is a part of the design of the PSMS that is verified as part of the design. A commitment to verify or demonstrate the completion of safe shutdown protective actions is not provided in the Section 2.5.2.

14.03.05-18

Add an ITAAC that specifically addresses the requirement of IEEE Std 603-1991, Section 5.9 to verify administrative control of the safety equipment to inspect the locks and physical security measures by which administrative control of the RSR can be implemented.

Based on the requirements of IEEE Std 603-1991, Section 5.9, the ITAAC in Section 2.5.2 should verify that the safety system design permits administrative control of access to safety system equipment.

DCD Tier 2, Subsection 7.4.1.5 Item 8 describes the security controls for access to the RSR and the transfer switches for transferring control to the RSR. Access to the room is administratively controlled. The Remote Shutdown Console (RSC) and the transfer switches are locked and the keys are administratively controlled. The inspection should specifically indicate that the locks and physical security measures are in place in the as-built hardware to provide administrative control of access and transfer of control to the RSR.

14.03.05-19

An inspection ITAAC should be added to verify all safety system equipment is properly identified per the requirements of IEEE Std 603-1991, Section 5.11. Based on these requirements, the ITAAC inspection should verify that (1) safety system equipment is distinctly identified for each redundant portion of a safety system, (2) identification of safety system equipment is distinguishable from any identifying markings placed on equipment for other purposes, and (3) identification of safety system equipment and its divisional assignments does not require frequent use of reference material.

Also, add an ITAAC that specifically addresses the requirement of IEEE Std 603-1991, Section 5.11 to inspect the operational VDUs and safety HSI for identification of redundant systems and distinguishing markings of the variables monitored and controlled such the divisional assignments do not require frequent use of reference material.

The distinct identification of safety equipment monitored and controlled when conducting safe shutdown operation is an important characteristic of the displayed information on the operational VDUs and the safety grade HSI. The inspection should verify that the displays have uniquely and correctly identified the redundant portions of safety systems that are needed for safe shutdown.

REQUEST FOR ADDITIONAL INFORMATION 255-2110 REVISION 1

14.03.05-20

Address the applicability of IEEE Std 603-1991, Section 6.3 with respect to an ITAAC to analyze or demonstrate that no single credible event involving the operational VDU and safety grade HSI can cause a non-safety system action that results in a condition, which requires RT or ESF action and can concurrently prevent that protective action in sense and command feature channels that are designated to provide principal protection against the condition.

Based on the requirements of IEEE Std 603-1991, Section 6.3, the ITAAC should include analysis or demonstration to show that no single credible event can cause a non-safety system action that results in a condition, which requires protective action and can concurrently prevent that protective action in sense and command feature channels that are designated to provide principal protection against the condition.

The staff reviewed the information in DCD Tier 1 and the ITAAC in Table 2.5.2-3, and concluded that no analysis is provided that addresses the requirement of Section 6.3 of IEEE Std 603-1991. Specifically, the concern that a conflicting signal between the operational VDU and the safety grade HSI should be addressed in an inspection or test. The information in DCD Tier 1 should be revised to include analysis or demonstration that no single credible interaction between sense and command features of the operational VDUs and the safety grade VDUs can cause and other systems, and the ITAAC, possibly in Section 2.5.2, should be modified accordingly.

REQUEST FOR ADDITIONAL INFORMATION 255-2110 REVISION 1

14.03.05-21

MHI is requested to expand many of the items of Section 2.5.1 to apply to the safety related portions of the other Sections of 2.5, which includes 2.5.2, Systems Required for Safe Shutdown, 2.5.4, Information Systems Important to Safety, and 2.5.6, Data Communication Systems, or provide justification why these items would apply to those sections.

There are many items in Section 2.5.1 which apply to all safety systems, or portions of systems which are safety related, and paraphrase the requirements of IEEE Std 603 which is invoked by 10 CFR 50.55(a)(h). This includes items 5 (seismic qualification), 7 (emi/rfi qualification), 8 (protection from natural hazards), 9 (divisional power supplies), 10 (independence), 12 (access control) etc. It is suggested that a matrix, or table, be provided identifying these common items and then unique items to these sections. Example:

IEEE 603 Section Criteria (Example)	Section 2.5.1	Section 2.5.2	Section 2.5.3	Section 2.5.4	Section 2.5.5	Section 2.5.6
5.4	X	X		X		X
(Example) Information & Controls for Operator Action	X	X		X		