

REQUEST FOR ADDITIONAL INFORMATION 701-5229 REVISION 0

2/28/2011

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No. 52-021

SRP Section: 07.09 - Data Communication Systems

Application Section: 7.9

QUESTIONS for Instrumentation, Controls and Electrical Engineering 2 (ESBWR/ABWR Projects)
(ICE2)

07.09-19

MHI is requested to additional information to demonstrate how staff guidance in DI&C- ISG-04, Staff Position 1.8, is met. Staff Position 1.8 of ISG-04 states that "Data exchanged between redundant safety divisions or between safety and nonsafety divisions should be processed in a manner that does not adversely affect the safety function of the sending divisions, the receiving divisions, or any other independent divisions."

US-APWR DCD Tier 2, Section 7.9.2.7 only provides a general description of the DCS communication independence. MHI is requested to provide all types of data exchange (voting logic, bypass, etc..) between safety divisions. For each data exchange, demonstrate how communication independence between safety divisions is maintained in sufficient detail (by expanding the currently submitted information).

07.09-20

MHI is requested to demonstrate in additional detail how guidance in ISG-04, Staff Position 1.8, is met. Staff Position 1.8 of ISG-04 states that "Data exchanged between redundant safety divisions or between safety and nonsafety divisions should be processed in a manner that does not adversely affect the safety function of the sending divisions, the receiving divisions, or any other independent divisions."

Section 3.2.8 of TR JEXU-1015-1009-P (R3) and Appendix E, Section E1, "Staff Position 1.8," of TR MUAP-07004-P (R5) provide conflicting information with regard to whether the priority logic is being implemented at application level. The former document discusses logic implementation at the application level (the latter document), while the latter refers to the former document.

MHI is requested to provide all data exchanged between redundant safety divisions or between safety and nonsafety divisions, priority logic for each such exchange, and describe how data exchange for each applicable input would not adversely affect the safety function of the sending divisions, the receiving divisions, or any other independent divisions.

REQUEST FOR ADDITIONAL INFORMATION 701-5229 REVISION 0

07.09-21

Staff Position 1.3 of ISG-04 states, in part, that “Receipt of information from outside the division, and the performance of functions not directly related to the safety function, if used, should be justified. It should be demonstrated that the added system/software complexity associated with the performance of functions not directly related to the safety function and with the receipt of information in support of those functions does not significantly increase the likelihood of software specification or coding errors, including errors that would affect more than one division.”

MHI is requested to demonstrate in additional detail how the guidance in ISG-04, Staff Position 1.3, is met. The demonstration should include whether potential software coding errors from non-safety operational VDUs could affect one or more than one safety division and how to mitigate these problems.

07.09-22

MHI is requested to demonstrate in additional detail how guidance in ISG-04, Staff Position 1.12, is met. Staff Position 1.12 states, in part, that “Communication faults should not adversely affect the performance of required safety functions in any ways. Faults, including communication faults, originating in nonsafety equipment, do not constitute "single failures" as described in the single failure criterion of 10 C.F.R. Part 50, Appendix A.”

DCD Tier 2, Section 7.9.2.7 refers to Appendix A of Technical Report MUAP-07004 for methods used to ensure independence between safety trains and between safety and non-safety systems. TR MUAP-07004, Appendix A, Section A.5.6.3.1 states, in part, that “Signals from the PSMS are transmitted to the PCMS and DAS through conventional analog/binary isolation devices or fiber optic cables. Conventional analog/binary isolators are part of the safety system and are tested to confirm that credible failures on the non-safety side of the isolation device do not prevent the PSMS from meeting its performance requirements.”

MHI is requested to address the following:

- For communication independence, TR MUAP-07004 states only that the communication modules are separate from processing modules. It is not clear that this method alone can prevent all communication errors. MHI is requested to address how the effects of the communication errors listed below are mitigated. Provide a separate explanation for each of the errors listed.

- Data corruption¹
- Unintended repetition¹
- Incorrect sequence¹
- Data loss¹
- Unacceptable delay¹
- Unexpected data insertion¹
- Invalid data “masquerade” as valid ones¹
- Incorrect address/wrong destination¹
- Broadcast storm¹
- Commission fault
- Inconsistency¹
- Excessive jitter¹

REQUEST FOR ADDITIONAL INFORMATION 701-5229 REVISION 0

- Data collision¹
- Buffer overflow¹
- Out of range¹
- Incorrect ordering¹
- Out of sync¹
- Incorrect encoding/decoding¹
- Interruption

¹ Source: RG 1.152, DI&C-ISG-04, and NUREG/CR 6991, "Design Practices for Communications and Workstations in Highly Intergraded Control Rooms"