

REQUEST FOR ADDITIONAL INFORMATION 778-5866 REVISION 3

7/8/2011

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)

07.09-24

GDC 24 states,

"The protection system shall be separated from control systems to the extent that failure of any single control system component or channel, or failure or removal from service of any single protection system component or channel which is common to the control and protection systems leaves intact a system satisfying all reliability, redundancy, and independence requirements of the protection system. Interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired."

IEEE-603 (incorporated by reference via 50.55a(h)) also requires demonstration of interdivisional independence and high reliability as well for safety system design. ISG-04, Staff Position 1.3 states, in part, that safety systems should be as simple as possible. Functions that are not necessary for safety, even if they enhance reliability, should be executed outside the safety system. A safety system designed to perform functions not directly related to the safety function would be more complex than a system that performs the same safety function, but is not designed to perform other functions. The more complex system would increase the likelihood of failures and software errors. Such a complex design, therefore, should be avoided within the safety system.

Section 7.9.1.1.2 of DCD Tier 2, revision 3, states "Signals transmitted from the PCMS to PSMS for interlocks and automatic control of safety components during normal operation. These signals are blocked by automatic safety signals and logic in the PSMS, which ensures priority of all safety functions. All safety components controlled by the PSMS have automated safety signals and priority logic." Interface from PCMS to PSMS for automatic control of safety-related components during normal operation is not credited in Chapter 15 and adds significant complexity to the interdivisional communication. This interface therefore should be avoided to make safety systems as simple as possible. The staff is unable to confirm that this PCMS to PSMS interface conforms to the ISG-04 guidance stated above to which MHI commits to conform. The staff requests MHI to fully address conformance to the stated guidance.