REQUEST FOR ADDITIONAL INFORMATION 727-5662 REVISION 2

4/6/2011

US-APWR Design Certification

Mitsubishi Heavy Industries

Docket No. 52-021

SRP Section: 07.02 - Reactor Trip System
Application Section: 7.2.3.1

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

07.02-5

Background:

Conformance to IEEE 603-1991, Section 4.11
MUAP-07004, Rev. 5, Appendix A, Section A.4.11 “Equipment Protective Provisions” provides the following list:

“The equipment protective features are designed to place the safety systems in a safety state, or into a state that has been demonstrated to be acceptable, if the safety equipment fails or the equipment protective device operates. Each protection function has different characteristics and therefore different techniques are used to achieve a fail-safe design.
Examples of protective features for selected functions include:

- Reactor trip circuits are designed to fail in the tripped state.

- Engineered safety features actuated components are designed to fail into a de-energized state or fail as-is. The de-energized state applies to failures that result in complete loss of component control. The as-is state is selected for failures that impair control but do not result in complete loss of component control. These states ~~has~~ (have) been demonstrated to be acceptable if conditions such as disconnection, loss of power source, or postulated adverse environments are experienced.

- Sensor circuits are designed, where possible, so that a loss of power will produce a safe signal or will produce an off-scale value or a signal that can be identified by the protection system as bad. Digital protective equipment input circuits are designed to recognize off-scale or bad values and take appropriate action (alarm, actuate or use redundant signal or equipment where available, etc.)

- Actuation signals from multiple PSMS trains are provided for selected actuated equipment to improve the reliability of the protection system and minimize the impact of equipment protective provisions.”

Conformance to IEEE 603-1991, Section 5.1
DCD Tier 2, Rev. 2, Section 7.2.3.1, in regards to the discussion of FMEA lists:

"The FMEA for reactor trip in PSMS is described in Table 7.2-8 and Figure 7.2-8. The FMEA demonstrates that:

- All credible PSMS failures are detectable (through self-diagnosis or manual surveillance tests).
- No credible single failure will prevent PSMS actuation.
- No credible single failure will result in spurious PSMS actuation, which results in a RT.
- The PSMS will fail to the safe state for all credible failures. The safe state for the RPS is trip. The safe state for the ESFAS/SLS is as-is."

Demonstrate: MUAP-07004, Section 6.5.1, "FMEA Method," in regards to the discussion of FMEA lists:

"The Failure Modes and Effects Analyses (FMEA) demonstrates that:

- All credible PSMS failures are detectable (through self-diagnosis or manual surveillance tests).
- No credible single failure will prevent PSMS actuation.
- No credible single failure will result in spurious PSMS actuation.
- The PSMS will fail to the safe state for all credible failures. The safe state for the RPS is trip. The safe state for the ESFAS/SLS is as-is."

1. The NRC staff requests MHI to provide clear explanations for the inconsistencies between the lists as well as inconsistencies in the terms. An example of inconsistent terms is "fail as-is" versus "as-is."

2. The NRC staff requests MHI to document which ESF signals fail into a de-energized state and which ESF signals fail as-is, and explain how failing into a de-energized state achieves the fail-safe design requirement.

07.02-6

MUAP-07004, Appendix A, Section A.4.11 states "Sensor circuits are designed, where possible, so that a loss of power will produce a safe signal or will produce an off-scale value or a signal that can be identified by the protection system as bad. Digital protective equipment input circuits are designed to recognize off-scale or bad values and take appropriate action (alarm, actuate or use redundant signal or equipment where available, etc.)"

The NRC staff requests MHI to:

1. Describe how, why, and where the sensor circuits generate three different signals on loss of power:
   a. a safe signal,
   b. an off-scale value, or
   c. a signal identified by the protection system as bad

2. Describe how, why, and where the digital protective system recognizes the following signals and describe what the appropriate actions are:

a. off-scale
b. bad values

3. Explain why the digital protective system does not recognize the sensor circuit generated signal for “a safe signal.”

4. Describe how these signals are accounted for in the Sections 7.2 and 7.3 FMEAs.

07.02-7

MUAP-07004, Section 6.5.1, states:
“Fault Classification
Failures that are undetectable or result in effects that violate the system design basis are specifically highlighted. These failures are specifically justified or the system design is modified.”

Table 6.5-1, "Typical FMEA Table," includes a column for Fault Classification; however, DCD Tier 2, Tables 7.2-8 and 7.3-7 do not have a column for Fault Classification. The NRC staff requests MHI to:

1. Explain why DCD Tier 2, Tables 7.2-8 and 7.3-7 do not follow the methodology as defined in MUAP-07004, Section 6.5.1.
2. Fault Classification: Identify failures that were undetectable or resulted in effects that violate the system design basis.
3. Explain why conclusions made in MUAP-07004, Table 6.5-1 are different from conclusions in DCD Tier 2, Section 7.2.3.1.
4. Document the ESF conclusion in DCD Tier 2, Section 7.3.3.1, "FMEA."