Key Technical Issues

Issue 1:

Compliance with the U.S. Nuclear Regulatory Commission (NRC) regulatory requirements in General Design Criterion 24 and Title 10 of the *Code of Federal Regulations* (10 CFR), Part 50.55a(h) (i.e., Section 5.6 of Institute of Electrical and Electronics Engineers (IEEE) 603-1991) since safety functions could be adversely affected by non-safety systems.

1. The bi-directional communication aspects of the design are not necessary to provide the required safety functions, and the resulting increased complexity will require substantially more information to be submitted by Mitsubishi Heavy Industries, Ltd. (MHI) and reviewed by the NRC staff.

2. MHI has not demonstrated the safety divisions need to receive any communication from outside their own safety division. These bi-directional data communication flows have not been adequately justified to enhance or support a safety function.

3. MHI has not demonstrated the safety system or operator, by backup safety commands, has sufficient time or indications of communications failures to take appropriate actions and, if necessary, disable the non-safety display unit.

4. MHI has not adequately defined the additional failure modes associated with bi-directional communication. Software errors from a non-safety device, producing the valid but conflicting command, are one type of failure that is still considered credible.

5. MHI has not demonstrated how their priority logic cannot be altered in the field. The NRC staff guidance provides that the contents, such as priority logic, of nonvolatile memory should be changeable only through removal and replacement of the memory device.

6. MHI has not shown the how the Engineering Tool connection to the safety systems meets the NRC staff guidance nor demonstrates how the continuous connection between the non-safety related Engineering Tool and Safety Systems is necessary.

Issue 2:

Compliance with the NRC regulatory requirements regarding quality assurance (QA) and quality standards. The current set of information does not conform to the NRC regulatory guidance on QA and quality standards nor does it provide an acceptable alternative with sufficient evidence and justification to meet the NRC's regulations. The related NRC regulatory requirements are included in 10 CFR 50 Appendix A General Design Criteria 1 and 21, 10 CFR 50.55a(h) (i.e., Section 5.3 of IEEE 603-1991), 10 CFR 21, 10 CFR 50.55a(a)(1), and Appendix B of 10 CFR 50.

1. Demonstration of the compliance with Appendix B of 10 CFR Part 50 and 10 CFR 21 for the development of the Mitsubishi Electric Total Advanced Controller (MELTAC) platform.

    a. MELTAC has not been developed under 10 CFR 50 Appendix B, and MHI's audits of Mitsubishi Electric Company (MELCO), the developer of MELTAC, have found many deficiencies associated with 10 CFR 50 Appendix B and 10 CFR 21 implementation. The NRC staff is not aware of whether the deficiencies have been corrected and if subsequent revisions have been made to the MELCO QA program and applied to the MELTAC.

    b. The feasibility and process for commercial grade dedication (CGD) of MELTAC has been a major concern iterated by the NRC staff on several public interactions. The existing scope of the CGD plan, as verbalized, has been insufficient with regards to the current regulatory guidance (including applicable Electric Power Research Institute (EPRI) reports) being acceptable to the NRC staff.

    c. Deviations of the original MELTAC QA process from the Appendix B criteria have not been adequately justified for requirements in multiple areas such as verification, testing, and configuration control. A specific example of this is the failed test results not retained in the original development phase. Therefore, failed test results and record of the reconciliation could not be reconstructed.

2. Demonstration of the quality of the software and its development process used in safety systems - software program manuals.

    a. In the design certification application, MHI identifies no exceptions to the NRC staff guidance on safety software reviews. However, the docketed software program manuals have shown that there are a significant number of exceptions as the NRC staff stated at public meetings and requests for additional information.

    b. 10 CFR 50 Appendix B criteria, as identified in various Regulatory Guides (RG) for software design elements, are not met for criteria such as design control, audits, testing, test documentation, and configuration management.

    c. The software development processes described does not include activities or provide justification for differences in terminology of recognized software engineering practices referenced by regulatory guidance. Examples include types of testing such as acceptance and system as well as audits such as walkthroughs, management reviews or software inspections. In addition, key documents such as software design descriptions and software requirements specifications.

3. Demonstration of the quality of programmable logic technologies, such as Field Programmable Gate Arrays (FPGAs), used in safety systems.

    a. MHI did not identify the use of FPGAs in the design certification application nor in the MELTAC topical report submittals. The NRC staff identified this technology during an audit in Kobe, Japan.

    b. Because a software (versus hardware) development process should have been used to implement FPGAs, MHI has not adequately demonstrated how its use of the technology meet applicable NRC regulations.

    c. MHI has not provided sufficient documentation on the quality development of FPGAs in their safety system design.

4. Demonstration of a secure development and operational environment for the software development process as described in RG 1.152.

    a. MHI has not addressed potential security vulnerabilities in each phase of the lifecycle development process in accordance with the NRC staff guidance.

    b. MHI has not addressed security self-assessments and audits in accordance with the NRC staff guidance.