Draft Request for Additional Information Based on the Review of US-APWR Topical Report MUAP-07005-P, Rev.1 "Safety System Digital Platform-MELTAC"

Number	Description
Section I.0 Purpose	
RAI-01	Identify the specific differences in the MELTAC equipment applied for non-safety applications vs. the equipment applied to safety applications. Section 1.0 briefly mentions this as differences "in Quality Assurance methods for design and other software life cycle processes." This difference is also described in compliance to Branch Technical Position 7-19, "Guidance on Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems."
Section 3.0 Applicable Code, Standards And Regulatory Guidance	
RAI-02	With respect to the Anticipated Transient Without Scram Rule, Item 6 indicates that the Diverse Actuation System (DAS) is described briefly in this topical report but no information on the system is found in the topical. Please discuss. In addition, the item mentions a "common module" as the final device in common between the primary and the diverse actuation system and indicates that it is described in the topical—if this is the Power Interface Module, item 6 should refer to this; if not, please clarify.
RAI-03	Item 16 indicates that environmental qualification for temperature, humidity and radiation is by analysis. The description in Section 5.1.2.2, Module Environmental Test, describes a test in a thermostatic chamber. This is not consistent. Please clarify.
RAI-04	Item 53 indicates compliance with IEEE 7-4.3.2, "2003 Criteria for Programmable Digital Computer Systems in Safety Systems of Nuclear Power Generating Stations," yet exceptions on Verification and Validation (V&V) have been taken due to the development of the system under Japanese standards. Please clarify. Has the code remained in Japanese or has it been translated into English? If the code has been translated, please discuss the traceability, V&V, testing, and management of the translation.
RAI-05	Identify how the MELCO internal design documents are marked for the safety and non-safety MELTAC systems. Section 3.0, Applicable Code, Standards and Regulatory Guidance, (item 62), referencing IEEE 494 1974 (this is also required by IEEE Std 603-1991, Criterion 5.11) states that documents used for internal use do not contain the "Nuclear Safety Related" designation. Also discuss how documents for the non-safety MELTAC system are differentiated from the safety related system.

Number	Description
RAI-06	Some items listed in Ch. 3 indicate compliance but do not cite the documentation that supports the claim. The following item numbers give the instances in which some citation of a MELCO submittal should be provided to support the claim of compliance: 16, 53-57, 59, 61, 64-74, 76, and 77. If it is necessary to reference the Environmental Qualification Program Technical Report, then please address this issue.
RAI-07	Item 44—Branch Technical Position HICB-16, "Guidance on Self-Test and Surveillance Test Provisions" has been withdrawn by the NRC on February 2007. A reference for this level of detail required for design certification applications under 10 CFR Part 52 would be Regulatory Guide (RG) 1.206, "Combined License Applications for Nuclear Power Plants." MHI is requested to identify if it plans to conform to this RG.
Section 4.0	**Meltac Platform Description**
RAI-08	Section 4.1.1.1, Concept of Configuration, discusses the three different kinds of configurations for the MELTAC Platform. Although the reliability of the switchover module is not presented, presumably the reliabilities of the additional device for switching between subsystems and the algorithm for self detection of failure are higher than the single channel reliability such that the net reliability of the system is greatly improved. This seems likely but a review of the switchover reliability should be a part of any system installation that employs the redundant standby configuration. The topical report does not indicate what protection system applications, if any, will use the redundant parallel, redundant standby or the single channel configurations. Identify at what point in the process this decision is made. Also, the criteria used to determine which of these configurations is used is only identified as "based on configuration requirements.". Please clarify.
RAI-09	Can individual Engineering Tools have read or write capability for more than one division at a time? If so, how is this controlled to maintain minimum redundancy requirements? In Section 4.1.4.2, Network for Engineering Tool, the feature that "the same Engineering Tool and personal computer (PC) used for all divisions (i.e. one division at a time)" was removed in Revision 0. In Revision 1, the statement "There is a separate PC for each division" was added with no discussion of the number of simultaneity.
RAI-10	In Section 4.1.5, Self-Diagnosis, the self-diagnosis of errors and failures are categorized as (1) failure, (2) alarm, and (3) Input/Output alarm. The listing of tests that follows does not indicate the category of a failure of each test. Please indicate the error categories for each test and reasoning for categorizing failure types.
RAI-11	In Section 4.3.1, General Description, the design basis is discussed. The communications link is not protected against common mode failures in hardware or software; however, self-testing and diagnostics are in place to detect a failure if it occurs. Please discuss.

Number	Description
RAI-12	In section 4.3.2, Control Network, item (b), the discussion indicates that the communication network has the capability of communicating with other divisions or non-safety system. DI&C-ISG-04, "Task Working Group #4: Highly Integrated Control Room – Communications Issues (HICR)" describes approximately 20 NRC staff positions on interdivisional and safety to non-safety communication. Please discuss any of these positions for which the MELTAC platform may not be in full compliance.
RAI-13	Data Link communication is discussed in Section 4.3.3.1, Configuration. The various interconnections for the communication systems are listed and named in the topical report. The information describes the network connections but does not give a graphical representation. No information is provided that would substantiate the claim that the communications network design provides physical, electrical or functional isolation of the interconnections at any level of the communications stack. There is no discussion of the failure modes that addresses the main concerns of communication independence. Provide a graphical representation of the network connections, along with information that would substantiate the claim that the communications networks provide physical, electrical, or functional isolation of the interconnected systems. Also, list the failure modes of the communications systems and address the independence of the communication systems.
Section 5.0	**Environmental, Seismic And Electromagnetic Qualification**
RAI-14	Chapter 5 of the topical report describes the qualification program for environmental, seismic and electromagnetic compatibility. The range of test conditions and descriptions are given. These tests have been compared in detail to the requirements of RG 1.89 (IEEE 323) for environmental tests, RG 1.100 (IEEE 344) for seismic and RG 1.180 (MIL-STD 461E, IEC 6100, IEEE Std C62.41-1991, IEEE Std C62.45-1992, IEEE Std 1050-1996, EPRI TR-102323) for qualification regarding electromagnetic and radio frequency interference. The module environment test conditions and test methods are based on industry standards in Japan [p. 98]. No discrepancy between those methods and procedures and the US standards is noted in the topical report, although an analysis was probably done. An audit of the test procedures and reports identifying the results and any corrective action is needed to complete acceptance of the MELTAC equipment qualification. Will the Environmental Qualification Program, to be submitted in December 2008, include those test procedures and reports or does MHI plan to submit these documents on the docket?
RAI-15	In Section 5.2.2.2, Module Seismic Resistance Test, seismic testing mentioned a minor exception on the duration and profile of seismic aging events applied to the equipment under test. Please explain the equivalence of the aging technique more fully.
Section 6.0	**Life Cycle**

Number	Description
RAI-16	Section 6.1.5.7, Reviews, indicates that while the test data and test programs have not been under configuration control, they can be reconstructed. Have these documents been reconstructed and placed under configuration control for both pre-existing software and newly developed software? Configuration management of the lifecycle documents is a requirement under Appendix B of 10 CFR, Part 50.
RAI-17	
RAI-18	In the process described shown in Figure 6.1-5 and the description in Section 6.1.8, it is not clear that the hardware has any feature to identify itself automatically in the installation or that any external labeling is used that would allow an installer and verifier to determine that the software and hardware match. IEEE 7-4.3.2 [p. 14] states that software and firmware identification should be used to assure that the correct software is installed on the correct hardware. Please clarify how the installation process ensures that the proper software is installed on a particular hardware module.
Section 7.0 Equipment Reliability	
RAI-19	What are the calculated failure rates which are described in Section 7.2, Mean Time between Failures (MTBF) Analysis? What are the observed failure rates? What components comprise a module? What are the number of observed failures and hours of powered service by component and module type? These data needed to help determine the quality of the platform on the basis of operation.
RAI-20	What is the meaning of the junction upstream of the output line in Figure 7.3-1, Reliability Model? Did the reliability models and fault trees consider common mode failures? Will (did) the Failure Mode and Effect Analysis follow the guidance of any standard?
RAI-21	According to Section 7.1, History of Operation, "no plant system has ever suffered shutdown due to software or hardware related problems." The collection of data need to be audited to ensure that all failures are entered into the system and that the number of demands and hours of operation are accurately tallied to compute the failure per demand and failure per operating year rates. The actual quotation is not exactly clear on the types of failures that have occurred, only that no shutdown has occurred. The statement does not preclude the occurrence of failures with lesser consequences than a shutdown. The data on all failures and failure rates of all types are needed to establish the system quality. Please provide a summary of the test procedures and the results of those tests.
RAI-22	With regards to Equipment Reliability, Section 7.0, use of the reliability record in substantiating quality, the failure rates and methods of collecting failure rate data should be made available for audit. Please identify how the operating history, summary of the test procedures and the results of those tests can be made available to the staff during the audit scheduled for August 2008.