January 5, 2009

MEMORANDUM TO: Michael A. Norato, Branch Chief
US-APWR Projects Branch (NMIP)
Division of New Reactor Licensing
Office of New Reactors

FROM: Terry Jackson, Branch Chief ***/RA/***
Instrumentation, Controls and Electrical Engineering Branch 1
Division of Engineering
Office of New Reactors

SUBJECT: Audit of MHI Documents in support of the MELTAC platform safety evaluation

The purpose of this memorandum is to provide you with the input from the Office of New Reactors on the information audited in support of the MELTAC safety evaluation. A non-proprietary version of the Audit is also being provided with the information identified by MHI as proprietary redacted and replaced by the designation "[ ]". The attachment documents the efforts of the team that reviewed the documents related to the life cycle process and, in particularly, the verification and validation activities associated with the MELTAC digital electronics platform. The review of the documents related to this life cycle process was conducted between September 2 through 4, 2008.

The team consisted of:

Team Leader:	Royce D. Beacom	Electronics Engineer, Instrumentation, Controls & Electrical Engineering Branch 1, Division of Engineering (DE)
Team Members:	Michael D. Muhlheim	NRC Contract Specialist Oak Ridge National Laboratories
	Thomas L. Wilson	NRC Contract Specialist Oak Ridge National Laboratories
	Stephen R. Monarque	Project Manager, USAPWR Projects Branch, Division of New Reactor Licensing (DNRL)
	Michael S. Magee	Project Manager, USAPWR Projects Branch, Division of New Reactor Licensing (DNRL)

January 5, 2009

MEMORANDUM TO: Michael A. Norato, Branch Chief
US-APWR Projects Branch (NMIP)
Division of New Reactor Licensing
Office of New Reactors

FROM: Terry Jackson, Branch Chief ***/RA/***
Instrumentation, Controls and Electrical Engineering Branch 1
Division of Engineering
Office of New Reactors

SUBJECT: Audit of MHI Documents in support of the MELTAC platform safety evaluation

The purpose of this memorandum is to provide you with the input from the Office of New Reactors on the information audited in support of the MELTAC safety evaluation. A non-proprietary version of the Audit is also being provided with the information identified by MHI as proprietary redacted and replaced by the designation "[ ]". The attachment documents the efforts of the team that reviewed the documents related to the life cycle process and, in particularly, the verification and validation activities associated with the MELTAC digital electronics platform. The review of the documents related to this life cycle process was conducted between September 2 through 4, 2008.

The team consisted of:

Team Leader:	Royce D. Beacom	Electronics Engineer, Instrumentation, Controls & Electrical Engineering Branch 1, Division of Engineering (DE)
Team Members:	Michael D. Muhlheim	NRC Contract Specialist Oak Ridge National Laboratories
	Thomas L. Wilson	NRC Contract Specialist Oak Ridge National Laboratories
	Stephen R. Monarque	Project Manager, USAPWR Projects Branch, Division of New Reactor Licensing (DNRL)
	Michael S. Magee	Project Manager, USAPWR Projects Branch, Division of New Reactor Licensing (DNRL)

DISTRIBUTION: NRO/DE ICE1 RF MMagee MMayfield LDudes WKemper PLoeser

ADAMS Accession Number: ML

OFFICE	NRO/DE/ICE1	NRO/DE/ICE1
NAME	RBeacom	TJackson
DATE	1/5/2009	1/5/2009

OFFICIAL RECORD COPY

MELTAC Safety System Digital Electronics Platform
Software Life Cycle and Quality Assurance Process
Mitsubishi Nuclear Energy Systems, Inc.

Background

Mitsubishi Heavy Industries (MHI) seeks NRC approval of Mitsubishi Electric Total Advanced Controller (MELTAC) Platform for application to the safety systems of the US-APWR and for replacement of current safety systems in U.S. operating plants. The MELTAC digital platform was developed by MHI and Mitsubishi Electric Corporation (MELCO) for nuclear power plants in Japan. The MELTAC Platform includes of Basic Software and Application Software. The application software, which includes setpoints and constants, will be developed uniquely for each application. For the US-APWR application, this is defined in various sections of MUAP-07004-P, Safety System Description and Design Process, and the plant licensing documentation. The basic software which includes the operating system for the MELTAC platform is the same for all applications. The process by which it was developed, the focal point of this audit, is discussed in Topical Report MUAP-07005, Safety System Digital Platform-MELTAC.

The original quality assurance program (referred to as Original QAP) used for the MELTAC Platform development was based on the Japanese Standard JEAG4101 and IS09001. Since MELCO now plans to apply the platform to safety systems in US nuclear facilities, a new quality assurance program has been adopted, entitled "NPD Procedure Q-4102: Safety System Platform Quality Assurance Program", hence forth referred to as Q-4102. It is MELCO's contention that Q-4102 addresses all requirements of 10CFR Part 50 Appendix B and IEEE Std. 7-4.3.2-2003, including the applicable Regulatory Guides and IEEE software standards. All new MELTAC development or revisions to current platform components will be in accordance with Q-4102. Platform components (hardware or software) developed prior to Q-4102 (referred to as Existing Platform) will be reused for US nuclear applications. The Original QAP and records of the Existing Platform have been assessed by MELCO against Q-4102, to ensure suitable quality of the Existing Platform. MELCO then developed the MELTAC US Conformance Program (UCP), which is the combination of the corrective actions taken to compensate for differences between the Original QAP and Q-4102 and the assessment of the developed software by the independent V&V Team.

Objective

By letter dated May 21, 2008, MHI has been requested to provide the English version of documentation listed in Topical Report MUAP-07005, Safety System Digital Platform-MELTAC, at their Arlington, VA office for the NRC staff to facilitate the review in a timely review. This information would also support the claim made in the Topical Report that the platform components developed under the Existing Platform, as well as the Original QAP, will be acceptable for use in US nuclear applications. Of particular interest in the NRC staff's review is MELCO's assessments performed (including the US Conformance Program) on the original MELTAC system software development process against the current MELTAC Safety System Digital Platform Quality Assurance Program. Section 6.1 "Life Cycle Process," of MUAP-07005-P, discusses the original quality assurance program, the new quality assurance program and assessments done on the differences between the programs. The conformance of the MELTAC

electronics platform quality assurance program to the high quality requirements identified by the NRC for use in I&C safety system applications has not yet been determined.

The review was conducted at the Mitsubishi's offices in Arlington, VA. The MELCO engineering and programming staffs from Japan who did the work and approved the work were present at the audit. The resources provided by MHI/MELCO included a complete set of engineering documents for the MELTAC safety platform software in Japanese, plus a subset of those documents that had been translated into English. The main Japanese set included ~30 two ring binders of information. The English set consisted of eight volumes. In the English set, all the documents requested to be translated to English identified in the letter dated 5/21/2008 where provided.

Regulatory Basis

A determination by the staff that the safety system software development process produces high quality software is required under the Standard Review Plan. The specifics for the review are detailed in Branch Technical Position 7-14, "Guidance On Software Reviews For Digital Computer-Based Instrumentation and Control Systems." The BTP summarizes the regulatory basis, provides specific guidance for the review, and references appropriate industry standards for the software development process.

The staff's acceptance of software for safety system functions is based upon (1) confirmation that acceptable plans were prepared to control software development activities, (2) evidence that the plans were followed in an acceptable software life cycle, and (3) evidence that the process produced acceptable design outputs.

Method of Review

The staff initially reviewed the documents identified in the letter dated May 21, 2008 which were requested to be interpreted from Japanese to English. The letter identified these following subject areas:

I. Quality Assurance Program
II. Configuration Management
III. Equipment Qualification

The method of the review was determining the completeness of the information in these areas with the focus on the assessments done in evaluating the Existing platform to meeting the requirements defined by the NRC. And in doing so, the staff could better define the path forward in the approval process of the MELTAC platform for US nuclear applications.

The staff brought to the attention of MHI 11 issues which were discussed at the audit. MHI provided proposed resolutions for each one. All 11 issues are identified in the attached; "Table 1 Issues Discussed during the 08 Sept MHI Audit."

The staff discusses post audit observations in Section II.a, "Software Life Cycle & Thread Path Audit Observations."

I. Quality Assurance Program

The original QA program used for MELTAC Platform was based on JEAG-4101-1990 (Guide for Quality Assurance of Nuclear Power Plants) and ISO9001. The "Comparison between NRC and Japanese Life Cycle Process Requirements and Guidance" provided in No. 1-1 (Folder E2-01, Index 08) provides the relationship between 10CFR50, Appendix B and JEAG-4101 (E2-01, Index 04).

- The titles show that the scopes of the documents are comparable. A sampling comparison of the text also shows favorable agreement. Almost all of the original QA Program for the existing platform meets the requirements of Appendix B. This confirms the information provided by MHI in letter (ML070670452) dated March 7, 2007, which compared U.S. and Japanese Quality Requirements for Nuclear Facilities.

- The exception in the original QA Program is that Appendix B, Criterion I-4, requires that "persons and organizations performing quality assurance functions shall report to a management level so that the required authority and organizational freedom, including sufficient independence from cost and schedule when opposed to safety considerations, are provided." In addition, IEEE 7-4.3.2, requires independence in three parameters; technical, managerial and financial. The review did confirm the software deficiency specification for independent V&V.

a. Quality Assurance Program Observation

Section 6.1.2 of MUAP-07005 states that the US conformance program (UCP) compensates for this inadequacy. UCP is the umbrella for corrective actions taken to compensate for differences between the Original QAP and Q-4102 and the assessment of the developed software by the independent V&V Team. A more thorough review should be performed regarding the UCP with respect to compensating for the inadequacy of the independence of the V&V team.

II. Configuration Management

Software Configuration

The MELTAC platform basic software consists of the modules that are needed to assemble a protection system, not an assembled system with an identifiable safety function. The modules perform the operations necessary for processing input signals, communicating, processing logic, and driving output devices. The Safety Software is based on pre-existing software that was originally developed by MELCO for non-safety control applications. The Existing Platform software was originally developed under Japanese standards. A comparison of the Japanese standard and the US program for compliance with the BTP 7-14 was conducted by MELCO. The main difference was the lack of an independent verification and validation at the conclusion of each step of the design process. (V&V of requirements, V&V of program specification, V&V of coding specification, V&V of source code, V&V of unit test plan and V&V of integral tests.) The US software development standards require that the V&V step be a formal and documented process with a planning document and a V&V report for each review. The Japanese standard allows for a design review board that is less structured and is not necessarily an independent review. The software underwent a review: the difference is that the reviewers were not necessarily from an organization that was administratively independent of the developers.

The MELCO US compliance review also identified that a Requirements Traceability Matrix was not part of the Japanese software development documentation.

Thread Audit

A thread audit is a technique of reviewing the documentation for a single component or function from the requirements through each phase of development to final qualified product. The thread can be traced as a horizontal line in the Requirements Traceability Matrix (RTM). This type of audit gives the reviewer a chance to understand one particular feature or function sufficiently well to assess the quality of the development process. The intent of the RTM is to show, at a minimum, each requirement, the source of the requirement, the life cycle phases that are utilized by this project, and an associated requirement item identification. The MHI/MELCO staff assisted the thread audit by laying out a series of all the development documents for a Category 1 module in chronological order from functional specification through the software development process.

A thread audit of a Category 2 module was also conducted. This review was of Japanese documents. The documents could be seen to have similar format and page length. Graphics and programming elements were similar to the documents in English provided for Category 1. The MHI/MELCO staff indicated that there was no difference in the level of information in Safety Platform documentation versus Existing Platform documentation. There is no documentation of the design review board process that constituted the closest approximation to a V&V of the Existing Platform. The MHI/MELCO staff indicated that there might be meeting minutes of the review in Japanese but these documents were not part of the information collected for the audit.

a. Software Life Cycle & Thread Path Audit Observations

1)

(Change management for System Specification, Software Specification, and Programming Specification. JEXU-1014-4001, JEXU-1014-4002, JEXU-1014-4003)

2) The Safety Platform software documentation is very similar to the original Existing Platform software. The main changes are renumbering the sections and making the deletions that are necessary.

3) The software documentation is of high quality. The text provides meaningful description of the function and the process for implementing it. The requirements progress from a high level descriptive text in the requirements document in increments through the stages of specification toward perfectly precise but less readable a source code that accomplishes the function. The process can be followed by a knowledgeable lay person which is a primary test of documentation.

4) The determination of software qualifying for Category 2 was more rigorous and better documented than indicated in the topical report. The determination for modules to be included in this category involved these three checks:

(JEXU-1015-6342, Previously Developed Software Evaluation Report).

5) The V&V reports did not find any major anomalies. The types of anomalies that were reported in the items reviewed were mainly consistency between the specifications. A feature that was needed had not been adequately described in a higher level topical report. The V&V process added value by making the documents more consistent.

6) The testing documentation was sparse but sufficient for review. Raw data consisted mainly of strip charts. These were recorded when the test included timing or output response. The test documentation for configuration and test method would allow the test to be reconstructed.

7) The English versions of the V&V reports were in some instances incomplete in recording resolution of anomalies. The Japanese versions of the same documents showed items as being resolved.

8) The Category 2 software also appears to be very high quality software. Review by a design review board or comparable V&V should be considered before accepting the Category 2 software.

9) The System Specification V&V review report, JEXU-1015-6351, identified 11 matters related to these external requirement documents; 5 to IEEE 7-4.3.2, 1 to RG 1.152 and 4 to IEEE 1012. The System Specification was revised by the Design Team accordingly. Example: one of which referenced criteria 5.6 of IEEE 7-4.3.2 with the comment "Separation of communication is defined as a requirement for the specification." This confirms external requirements are used for the basic platform which should be reflected in the Requirements Traceability Matrix.

Self-Diagnostics

The types of hardware based self-diagnostics employed in the MELTAC platform are watchdog timer, parity error, timeout and analog input check. These are specifically identified in Section 4.1.5 a) of the MELTAC topical report, MUAP-07005.

Diagnosis is covered in the design documents, V&V, and V&V input (Category 1). Because none of these documents were translated, the diagnosis review picked I/O processing for review because Safety System Digital Platform MELTAC Nplus S I/O Processing Program Specification is translated (Folder E4-01, Index 7).

Safety System Digital Platform MELTAC Nplus S I/O Processing Program Specification (Folder E4-01, Index 7) indicates that failure detection and self-diagnostics follows IEEE 7-4.3.2. Section 5.5.3 Quality (NQA-1) and 5.10.1 and .2 of Safety System Digital Platform MELTAC-Nplus S System Specification (Folder E2-01, Index 19) describes where the diagnosis program checks occurred. Attachment 3 of this document describes what is diagnosed and what type of failure notification will be issued. Section 5.10 also describes the failure mode classification, performance when a fault is detected, and the summary of indication of display. Section 5.10.1 is a figure showing self-diagnosis points. Section 5.10.2 is a figure showing the scope of self-diagnosis. Upon initialization, self-diagnosis includes RAM read/write, ROM sum check, CPU command health check. Operating function has self-diagnosis of CPU, memory, I/O, etc.

Equipment Qualification

The Environmental Test Summary Report for MELTAC Platform (Folder E2-04, Index 38), states that "For MELTAC Platform, the Environmental Test has been performed based on Industry standard in Japan."

Before, during, and after each test it was confirmed that there were not any equipment failures or abnormal functions.

The Seismic Test Summary Report for MELTAC Platform (Folder E2-04, Index 39), states that "For MELTAC Platform the seismic test has been performed based on Japanese Standard . . . this method is considered equivalent to … OBE, which is required by IEEE Std-344. . . Seismic qualification for the SSE conformed to IEEE Std-344." The test confirmed the physical integrity and functional integrity of the modules before, during, and after excitation.

The Isolation Test Summary Report for MELTAC Platform (Folder E2-04, Index 40), states that "the isolation test was performed with the purpose of verifying that the functional separation is established between the safety system and the non-safety system. . . For MELTAC Platform, the Isolation test has been performed based on IEEE Std 384-1992." Both analog and digital isolation devices passed the test.

The EMC qualification test summary report for MELTAC platform (Folder E2-04, Index 41), indicates that EMI/RFI emission and susceptibility test, surge withstand capability tests, and electrostatic discharge tests for the MELTAC Platform were performed. These tests are based on the methods and acceptance criteria of RG 1.180. All tests were successfully passed.

Summary

The staff requests MHI/MELCO maintain the documents for potential further discussions and selected review by the staff. Also, the staff will identify documents translated in this audit, or any additional documents pertaining to the MELTAC platform and the US-APWR application, which may required to be put on the docket, via request for additional information.

Table 1
Issues Discussed during the 08 Sept MHI Audit

Issue or Question No. 1	Document No. JEXU-1015-1009	Date:
NRC issue or question statement: The Software Safety Analysis does not address MELTAC communications functions • Network • Datalink • Safety VDU Interface		
MHI Proposed Resolution: MELCO will revise the Software Safety Analysis for basic software, JEXU-1015-1009, to address detection of communication interface failures. DI&C-ISG-04 Task Working Group #4: Highly-Integrated Control Rooms- Communications Issues will be used as a basis for this analysis. The response to detected failures for specific applications will be documented in the application level safety analysis. The application level safety analysis for the US-APWR will be in accordance with Section 3.9 of MUAP-07017		
Issue or Question No. 2	Document No.	Date:
NRC issue or question statement: It is not clear how the RTM has been used to track system specification requirements through each phase of the software development process.		
MHI Proposed Resolution: MELCO V&V team member walked NRC through a specific system requirement example to explain the use of the RTM. The example selected was for the MELTAC communication network.		

Table 1
Issues Discussed during the 08 Sept MHI Audit

Issue or Question No. 3	Document No.	Date:
NRC issue or question statement: The RTM starts from the MELTAC System Specification, which only includes internal platform requirements, such as redundancy configurations, I/O capacity, cycle time, etc. Where are the requirements that originate from industry standards, such as IEEE 603?		
MHI Proposed Resolution: Requirements from industry standards, such as IEEE 603, pertain to functions implemented at eh application level, not performance requirements applicable to the basic platform. For example IEEE 603 requirements for single failure compliance, operating bypasses, maintenance bypasses, bypassed and inoperable status monitoring, etc. are all implemented through the configuration of the system (e.g. Multiple controllers in separate divisions with interconnected data links) and the application software. Therefore, the System Specification and RTM required by the Software Program Manual for the application software (e.g. MUAP-0717 for the US-APWR) will address compliance to the industry standards.		
Issue or Question No. 4	Document No.	Date:
NRC issue or question statement: ( )		
MHI Proposed Resolution: ( )		

Table 1
Issues Discussed during the 08 Sept MHI Audit

Issue or Question No. 5	Document No.	Date:
NRC issue or question statement: MELTAC documentation goes from the System Specification to Program Specification for each software module. These Program Specifications appear to be meta-code. There should be a Software Specification that is in functional narrative format. The Software Specification should tie together the program specifications for all modules.		
MHI Proposed Resolution: Document JSX3D634 is the Controller Software Specification. This document is the high level narrative specification which ties together the Program Specifications for all software modules. This document is listed in the System Specification section of the document spreadsheet.		
Issue or Question No. 6	Document No.	Date:
NRC issue or question statement: What evidence is available to justify that the original hardware design process and the hardware specifications conform to US standards		
MHI Proposed Resolution: MELCO conducted an assessment of their original QA process to 10CFR50 Appendix B. That assessment is summarized in Section 6.1.2 of the topical report. Evidence of that assessment is available in the audit documentation. No deficiencies were identified; therefore there were no deficiencies in the hardware design process. Conformance to US technical requirements for hardware has been confirmed by the equipment qualification program, which included qualification to US standards for: Seismic qualification (IEEE 344) Environmental qualification (IEEE 323) EMI qualification (RG1.180) Fault isolation qualification (IEEE 384) All qualification results are available in the audit documentation: JEXU-3300-2160 (Environmental) JEXU-3300-2160 (Seismic) JEXU-3300-2160 (isolation) JEXU-3300-2160 (EMI) There are no additional industry standards that impose hardware technical requirements. Other hardware requirements are self-imposed by the System Specification.		

Table 1
Issues Discussed during the 08 Sept MHI Audit

Issue or Question No. 7	Document No.	Date:
NRC issue or question statement: NRC is having difficulty accepting this response since configuration management of test results is indicative of a high quality software development program; lack of this configuration management is indicative of a quality problem.		
MHI Proposed Resolution: The test procedures and test results are under configuration control (see documents in Spreadsheet “Document List” labeled “Unit Test Specification (with test report) NRC note; The TR will be revised to clarify		
Issue or Question No. 8	Document No.	Date:
NRC issue or question statement: MELCO is relying primarily on the quality of their original software development process to allow acceptance of software modules that are in Category 2. These are the modules that did not undergo additional independent V & V through US Conformance Program (UCP). What evidence is available to demonstrate the quality of the original software development program?		
MHI Proposed Resolution: All of the documentation generated during the original software development program is available to the NRC for audit within the “J” binders. Since this documentation is in Japanese, MELCO experts will walk the NRC through these documents. MELCO is willing to translate a thread through these documents (e.g. One software module beginning to end) if the NRC believes this is necessary after this audit.		

Table 1
Issues Discussed during the 08 Sept MHI Audit

Issue or Question No. 9	Document No.	Date:
NRC issue or question statement: ( )		
MHI Proposed Resolution: Annex C of IEEE 7-4.3.2 2003 and Annex D of IEEE 7-4.3.2 1993 state the following: Lack of documentation or performance of some development process steps may be compensated for by either of the following: a) Documented operating experience that is similar to the manner in which the computer will be used in the nuclear power generating station ( )		

Table 1
Issues Discussed during the 08 Sept MHI Audit

Issue or Question No. 10	Document No.	Date:
NRC issue or question statement: ( )		
MHI Proposed Resolution: ( )		
Issue or Question No. 11	Document No.	Date:
NRC issue or question statement: What process is used to ensure components that are replaced due to obsolescence conform to the original hardware performance requirements?		
The process used for component replacement due to obsolescence is described in Section 6.2.3 of the MELTAC Topical Report. ( ) To date, the MELTAC platform uses the same CPU and communication controllers as in the original product release (i.e. There have been no substitutions for major components).		