March 30, 2011

MEMORANDUM TO: Hossein G. Hamzehee, Chief
US-APWR Projects Branch
Division of New Reactor Licensing
Office of New Reactors

FROM: William R. Ward, Senior Project Manager ***/RA/***
US-APWR Projects Branch
Division of New Reactor Licensing
Office of New Reactors

SUBJECT: AUDIT REPORT FOR THE MITSUBISHI ELECTRIC TOTAL ADVANCED CONTROLLER SAFETY SYSTEM DIGITAL PLATFORM DATED MARCH 2 - 6, 2009

On March 2 - 6, 2009, the U.S. Nuclear Regulatory Commission (NRC) completed an audit of the Mitsubishi Electric Total Advanced Controller (MELTAC) digital platform at Mitsubishi Electric Corporation's (MELCO) Kobe, Japan facility. The MELTAC digital platform is described in Topical Report MUAP-07005-P, "Safety System Digital Platform -MELTAC-," Revision 3, which was submitted by Mitsubishi Heavy Industries, Ltd. (MHI). MELCO is the supplier of the MELTAC platform to MHI. The enclosed report documents the audit findings that were discussed on March 6, 2009, with Mr. Makoto Takashima of MHI, Mr. Katsumi Akagi of MELCO, and members of their staff. A non-proprietary version of the audit report is also being provided as Enclosure 1 with the information identified by MHI as proprietary redacted and replaced by the designation "[ ]". Enclosure 2 is the proprietary, non-public version of the report.

The audit examined activities associated with the submittal of Topical Report MUAP-07005-P, "Safety System Digital Platform -MELTAC-," Revision 3, as they relate to safety and compliance with the NRC's rules and regulations. The auditors reviewed selected procedures and records, observed activities, and interviewed personnel.

The NRC staff evaluated various aspects of the MELTAC platform. Specifically, the NRC staff audited aspects related to software quality assurance, configuration management, cyber security, and MELTAC components including their performance and quality. Overall, the NRC staff was able to verify the consistency of various aspects of the MELTAC platform as it is described in Topical Report MUAP-07005-P. However, there were issues identified by the NRC staff during the audit. These issues are discussed in the enclosed audit report. Appendix B contains a list of Open Items which have been or are being resolved. The resolution of these items may be reviewed during a future audit or inspection. Since this audit was performed MHI has committed to change the Topical Report MUAP-07005-P to a Technical Report applicable to only the US-APWR design.

CONTACT: William R. Ward, NRO/DNRL
301-415-7038

Audit Team:

Michael S. Magee, Project Manager for the US-APWR Projects Branch
Terry Jackson, Branch Chief for the Instrumentation and Controls Branch 1
Royce Beacom, Technical Reviewer for the Instrumentation and Controls Branch 1
Steve Wyman, Technical Reviewer for the Instrumentation and Controls Branch 1
Michael D. Muhlheim, NRC Contractor for the Oak Ridge National Laboratory
Thomas L. Wilson, NRC Contractor for the Oak Ridge National Laboratory

Docket No. 52-021

Enclosures:
As stated

cc w/encls: See next page

Audit Team:

Michael S. Magee, Project Manager for the US-APWR Projects Branch
Terry Jackson, Branch Chief for the Instrumentation and Controls Branch 1
Royce Beacom, Technical Reviewer for the Instrumentation and Controls Branch 1
Steve Wyman, Technical Reviewer for the Instrumentation and Controls Branch 1
Michael D. Muhlheim, NRC Contractor for the Oak Ridge National Laboratory
Thomas L. Wilson, NRC Contractor for the Oak Ridge National Laboratory

Docket No. 52-021

Enclosures:
As stated

cc w/encls: See next page

DISTRIBUTION:

PUBLIC	MMagee, NRO	RidsNroDeIce1	RidsAcrsAcnwMailCenter
NMIP R/F	JCiocco, NRO	RBeacom, NRO	RidsOgcMailCenter
D081	WKemper, NRR	RidsNroDnrlNmip	*via e-mail
	SWyman, NRR	RidsNroLACSmith	

ADAMS Accession Number: ML093010325; Pkg.: ML093240406 **NRO-002**

OFFICE	DNRL/NMIP: PM	DNRL/NMIP: LA	DNRL/NMIP: PM	DE/ICE1: BC	DE/EICB: PM
NAME	MMagee*	CSmith	JCiocco	RBeacom	SWyman
DATE	12/10/2010	12/1/2010	12/1/2010	3/28/2011	2/15/2011
OFFICE	DE/ICE1: BC	DE/EEEB: BC	DNRL/NMIP: BC	DNRL/NMIP: PM	
NAME	TJackson	GWilson	(JCiocco for) HHamzehee	WWard (signed)	
DATE	3/01/2011	2/24/2011	3/30/2011	3/30/2011	

OFFICIAL RECORD COPY

TABLE OF CONTENTS

March 2009 MELTAC Audit Report

SUMMARY OF FINDINGS

This report describes the audit activities performed by the U.S. Nuclear Regulatory Commission (NRC) staff at Mitsubishi Electric Corporation's (MELCO's) facility in Kobe, Japan from March 2 - 6, 2009. The audit was performed in association with Mitsubishi Heavy Industries, Ltd. (MHI) Topical Report MUAP-07005-P, "Safety System Digital Platform - MELTAC -," Revision 3 (ML083659338), which was submitted to the NRC staff for review and approval. MELCO is a sub-supplier of the Mitsubishi Electric Total Advanced Controller (MELTAC) platform to MHI. MHI requested NRC approval of the MELTAC platform for the application to the safety systems of the United States - Advanced Pressurized Water Reactor (US-APWR) and for replacement of current safety systems in the United States (U.S.) operating plants. The purpose of the audit was to verify specific aspects of the MELTAC platform, including its design, testing, manufacturing, modifying, inspecting, handling, and repairing activities. The auditors compared the processes and products associated with the MELTAC platform to the NRC regulations and guidance. Specifically, the auditors focused on activities that necessitated observations at the manufacturing facility. Other aspects of the MELTAC platform will be reviewed in later audits or office reviews. The following identifies the observations and findings associated with the audit activities.

- During the course of the audit, the NRC staff came upon several instances where an English version of the supporting documentation was not provided. In these cases, the NRC staff could not independently verify the content of the documents. During future audits, MELCO would need to provide English versions of the documents.

- The NRC staff observed some quality assurance (QA) aspects of the MELTAC platform. Specifically, the NRC staff observed the organizational structure of MELCO as it applies to the independence of development, verification and validation (V&V), and QA as described by the topical report. The NRC staff also discussed the error reporting and correction process, and observed some portions of the processes for material control. The NRC staff's activities should not be regarded as a QA inspection, and future NRC quality inspections may review the MELCO QA program in further detail.

- The NRC staff observed some of MELCO's practices and procedures regarding cyber security. Specifically, the NRC staff observed the archival system and the software development facility. Also, the NRC staff interviewed personnel associated with these two areas. [

]

- The NRC staff witnessed input power tests on a representative MELTAC system. [

  ]

- The NRC staff observed several demonstrations of the MELTAC self-diagnostic features. These demonstrations consisted of simulated communication and power failures. [

  ]

- The NRC staff observed response time calculations and actual time response measurements for the MELTAC system in clarification of the method described in the topical report.

- The NRC staff observed the various components of the MELTAC platform, including the cabinets, Central Processing Units (CPUs), communication networks, Input/Output (I/O) boards, Power Interface (PIF) modules, and video display units. The following issues were identified:

  - [

    ]

  - The synchronization between two CPUs in the redundant parallel configuration was not adequately described in the topical report.

  - [

    ]

  - [

    ]

  - [

    ]

  - Equipment labeling, technical manuals, and the engineering tool screen displays have not been translated into English.

- The NRC staff observed MELCO's equipment qualification facility. Only the official temperature/humidity testing was performed at the MELCO facility. The seismic and electromagnetic/radio-frequency testing was

performed at outside facilities. The NRC staff did observe the Electromagnetic Interference/Radio Frequency Interference (EMI/RFI) test data and will request the complete report to be submitted for review.

- MELCO personnel demonstrated the use of the application software development tools MELENS and RAPID. The NRC staff verified that the tools and test program were the latest or correct version, by observing MELCO personnel use of the archive system to verify the revision level.

- The NRC staff attempted to verify that key priority logic circuits housed in the PIF were not subject to common cause software failure by reviewing PIF schematics and assembly drawings against an actual unit. The NRC staff was able to identify, without language barrier, that the key priority circuits were, in fact, hard wired logic. However, MELCO was not able to provide English documentation to verify that component and drawing revision levels were not current nor the system interconnect documentation to verify that no soft logic was used outside the PIF. The NRC staff will request MHI/MELCO to provide a logic diagram of the priority logic in the topical report. Additionally, the NRC staff noted that field-programmable gate arrays (FPGAs) are used in parts of the MELTAC equipment. [

]

REPORT DETAILS

1. SOFTWARE QUALITY ASSURANCE

1.1 Software Development Organization

The NRC staff was presented information on the organizational structure of the MELCO facility and how it relates to software and hardware development. The NRC staff interviewed personnel to verify the organizational structure as it is presented in the topical report.

MELCO personnel discussed the organizational structure of MELCO at the start of the audit. [

]

[

]

1.2 Problem Reporting, Evaluation, and Correction

The NRC staff verified aspects of MELCO's problem reporting, evaluation, and correction action process through observation of appropriate plans, procedures and documented reports, and on-site personnel interviews. The NRC staff interviewed corrective action personnel and walked through a problem report to understand the process. The NRC staff also toured the MELCO facilities associated with failure analysis.

Most of the findings are limited because of the restrictions of the documentation that was available in English. The NRC staff interviewed MELCO corrective action personnel to understand the process for problem reporting, evaluation, and correction as it is described in the topical report. MELCO personnel used an example problem report, Error Report [ ], which was not in English, from [ ] to describe the process. In Japan, MELCO has onsite personnel at the [ ] nuclear sites that they provide parts and services. For U.S. sites, MELCO stated that they would need to ensure that the technical manuals supplied with the MELTAC platform contain information for reporting problems. At this time, the English technical manuals for MELTAC have not been developed so the NRC staff was unable to review them. For U.S. sites, error reporting may be through MHI, who would supply the platform to U.S. utilities. MELCO stated that interfacing personnel (i.e., marketing, sales, and service personnel) are directed to initiate an error report through their supervisor to the MELCO QA Manager. The NRC staff did not verify any procedures regarding this requirement. However, such procedures may be verified by a quality vendor inspection at a later date.

[

]

The NRC staff toured the failure analysis lab to understand how MELCO evaluates problems with MELTAC hardware. The failure analysis lab performs two functions: evaluation of parts prior to inclusion into a design and evaluation of parts failures. [

] MELCO demonstrated a commitment to doing a thorough failure analysis with the fully equipped lab co-located on the manufacturing floor and staffed by full-time, dedicated personnel.

1.3 Control of Materials and Manufacturing Processes

The NRC staff observed the staging and factory acceptance testing area for nuclear Instrumentation and Control (I&C) systems at the MELCO facility. Specifically, the NRC staff observed cabinets and main control room panels and components that completed factory acceptance testing and was currently staged in the area while shipping of equipment to the nuclear facility was in process. The NRC staff observed some of the material controls implemented by the applicant although none of the material or operations procedures were in English.

The NRC staff also observed the manufacturing process for printed circuit boards (PCB). The NRC staff interviewed the manager of the PCB manufacturing facility which included questions related to tracking mechanisms for materials and errors and the use of machinery and materials. Specific identification of MELTAC components to an English user would need to be addressed in a later audit.

During a tour of the staging facility, the NRC staff noted the access controls implemented by the applicant. [

]
The NRC staff also noted that for all areas involved in the manufacture or handling of electronic components, persons entering the facility were required to use anti-static footwear.

The NRC staff toured the portion of the MELCO facility that produces over [
] PCB assemblies per month for [ ] types of circuit boards for various electronic products, including those related to the MELTAC platform. After a presentation of the overall process, the NRC staff walked the floor to directly view the facility and workers. The Manufacturing Floor Manager explained that both commercial and high reliability products are assembled using a common process. The NRC staff questioned the difference between the PCB manufacturing processes for high reliability assemblies and those used in less critical applications.

MELCO explained that the process mostly differs in how much information is recorded. High reliability assemblies are better tracked and failure resolution is more thorough. The NRC staff questioned whether boards that fail inspection are reworked or discarded. MELCO both reworks and discards PCB, but the Floor Manager stated that many are reworked. The NRC staff observed a production report showing boards per month and failure rates. [

]

MELCO employs pick and place soldering equipment, some with automatic optical recognition quality control measures. They employ as much automation as possible since the machines have the capability to provide higher quality soldering and placement, as compared to manual soldering and placement. However, the NRC staff did not observe use of ground straps for manufacturing employees.

MELCO uses bar coding extensively to track components and board assemblies. The bar coding is located at every work station so that every part of the board's journey through the process is electronically recorded. The NRC staff inquired if the data was used to generate manufacturing reports and if they could see the manufacturing data. MELCO stated the information was proprietary, but agreed to show the NRC staff the reports on-site. The NRC staff interviewed MELCO personnel who interpreted and reviewed a number of manufacturing reports that are typical of good quality control and continuous improvement process. The NRC staff also observed workers utilizing the bar coding during the manufacturing process to track materials and aid in parts placement on the boards. The NRC staff raised the question of how the traceability of passive and mechanical components, those without specific barcodes as viewed by the NRC staff, is maintained for each circuit board. MELCO did not readily answer the question at the time. MELCO identified that only integrated circuits are tracked or traceable to a given circuit board.

Title 10 of the *Code of Federal Regulations*, Part 52.47(a)(22), requires applicants to incorporate operating experience into their plant designs. Information Notice 2005-25, describes an event at the Millstone Nuclear Power Plant where a tin whisker resulted in a reactor trip. Although the risks of tin whiskers increases with the use of lead-free solder material, the electronics industry is moving away from lead-based solder material due to the environmental concerns with such material. The NRC staff asked if MELCO used exclusively lead-free solder process. [

]

MELCO personnel were not able to readily answer the question at the time.

2. CYBER SECURITY

The NRC staff verified various cyber security aspects as they relate to basic software development for the MELTAC platform per Regulatory Guide (RG) 1.152, “Criteria for Digital Computers in Safety Systems of Nuclear Power Plants” in the topical report. The NRC staff observed the software development facilities and archival system. Specifically, the NRC staff verified practices employed by MELCO for prevention of cyber intrusion and introduction of malicious code. The NRC staff also interviewed software development personnel for their knowledge of information security practices and procedures, although none of the procedures or security guidelines were in English.

2.1. Software Archival System

The NRC staff observed the Mitsubishi Corporate Electronic Archive System (CEAS) facility. CEAS is the location where MELCO archives software development files including specifications, source code, executable code, test documentation, and manuals. The CEAS is maintained by a separate organization (Engineering, Manufacturing, and Information System department) within MELCO. [

]

[

] Control of official versions of software documents is performed through configuration sheets, which are discussed in Section 5 of this report.

MELCO stated that users of the CEAS system must enter a password [ ] Failure to enter a correct password after [ ] attempts would prevent access for that particular username. The system prompts users to update their password every [ ] days and will not allow entrance to the system if the password is expired. MELCO personnel stated that there is a firewall [ ] The NRC staff did not verify aspects of the firewalls. The NRC staff did observe that the CEAS facility contained physical security systems [

]

The NRC staff questioned MELCO personnel regarding cyber security procedures for the CEAS. [

]

2.2. Software Development Facility

The NRC staff visited the software development facility where MELTAC basic software is developed. Application software for the U.S. facilities would be performed through MHI, at their facilities. The NRC staff did not visit these facilities, as they involve the application-specific use of the MELTAC platform. [

]

The NRC staff observed the computers (laptops) used to develop software. The computers were physically secured and marked (as stated by MELCO employees) with notices stating, to not remove them from the room. The NRC staff verified that the development computers were not connected to an external network. The NRC staff also verified that the wireless network capability for the development computers was disabled. MELCO also stated that there were no wireless networks in the corporate area. MELCO personnel also stated that the development computers all possessed a password that only the software development personnel knew. The NRC staff questioned other cyber security aspects such as use of portable storage devices (e.g., thumb drives). MELCO personnel stated that there was a corporate policy regarding use of portable data storage devices at the facility.

The NRC staff requested MELCO personnel to demonstrate control of software tools in the development facility. As an example, the NRC staff requested MELCO to demonstrate control of the compiler used for MELTAC software development. [ ] Official copies of the compiler were maintained in CEAS. MELCO personnel were able to bring up the documentation and executable file for the compiler in CEAS. Additionally, MELCO personnel were able to demonstrate that the version in the configuration sheet for the software under development and the version in the computer were the same.

The NRC staff questioned the software development personnel whether there was a cyber security procedure for the software development facility. [

]

The NRC staff questioned whether a cyber security audit had been performed for the software development facility. [

]

3. POWER SUPPLIES

The NRC staff requested for MELCO to demonstrate the capability of the power supplies to function during faults as described in the topical report. MELCO set up a demonstration regarding MELTAC equipment performance for the range of power conditions (i.e., voltage, frequency, and harmonic distortion). The NRC staff observed the setup and reaction of the MELTAC equipment to the demonstrated conditions.

MELCO staff demonstrated the MELTAC components response to variations in voltage and frequency and a measurement of total harmonic distortion produced by MELTAC equipment. MELCO staff used a variable power supply to produce the variations in voltage and frequency. The NRC staff requested for MELCO to demonstrate the extreme end combinations for voltage and frequency. [

]

[

]

4. SELF DIAGNOSTICS AND FAULT TOLERANCE

The NRC staff witnessed a number of injected failures into the MELTAC demonstration system and the system's response primarily to observe actual tests in support of meeting Institute of Electrical and Electronics Engineers (IEEE) Standard (Std) 7-4.3.2 as stated by the topical report. The NRC staff verified the test setup and operation and response of the system as compared to the topical report. The NRC staff witnessed the following failure demonstrations:

- Power loss to one and both controllers in the standby controller configuration.
- Fail-off and fail-as-is capability of an I/O module.
- Loss of communication to an I/O rack.
- Break 4 to 20 mA output from an analog I/O card.
- Loss of power to an optical switch.
- Break in the control network rings.
- Break in a data link network.
- CPU fan failure.

- Loss of a power supply.
- Break in touch screen signal.

For the standby controller configuration, MELCO demonstrated the bumpless transfer from the primary to the standby controller. [

]

MELCO demonstrated the fail-off and the fail as-is configurations for a digital I/O module. [

]

The NRC staff observed the disconnection of the communication cable between the controller and one of its I/O racks. [

]

MELCO created a break in the 4 to 20 mA output line from an analog I/O board. [

]

To demonstrate the bypass feature of the optical switch, MELCO removed power to an optical switch. [

]

[

]

A demonstration of a break in the control network fiber optic cables was performed by unplugging the fiber optic cables from an optical switch. [

]

A break in a data link network was implemented by unplugging the data link cable from one CPU. [
]

A loss of CPU fan cooling was demonstrated by removing power to the fan. [

]

MELCO demonstrated the power supply failure alarm by removing the power to one of two redundant power supplies for an I/O rack. [

]

A break in the in touch screen cable between the Safety-Related Visual Display Unit (SVDU) and SVDU controller was disconnecting a cable. [

]

5. CONFIGURATION MANAGEMENT

The NRC staff interviewed MELCO personnel regarding configuration management practices. The NRC staff observed the configuration management process as described in the topical report against actual practice. MELCO personnel used Document [

] to aid in the discussion of the configuration management process.

MELCO personnel explained that configuration control of both hardware and software is controlled by a configuration sheet for discrete files, documents, drawings, etc. The NRC staff observed several configuration sheets during the audit, including those through the CEAS system. The configuration sheets remain with the design in the archive system.

The NRC staff had MELCO personnel step through an example basic software change (addition of a new Problem Oriented Language) and explain how configuration control is maintained. [

]

As an I&C system is developed from various parts, larger modules assembled from smaller components will have their own configuration sheets. The configuration sheets for the larger modules identify the versions of the smaller components that are to be used.

6. RESPONSE TIME

The NRC staff observed a demonstration of how the response time for a MELTAC application is calculated and verified. The NRC staff observed the demonstration setup, the calculation values, and the actual response time verification process and values.

MELCO demonstrated the calculation and measurement of response time testing on the MELTAC demonstration system. [

]

7. MELTAC EQUIPMENT

The NRC staff observed the MELTAC equipment in the demonstration system and compared the configuration, features, and capabilities of the equipment to the description in the topical report.

The NRC staff observed a demonstration facility for the MELTAC platform. The demonstration facility included [ ] cabinets that included the MELTAC CPUs, optical switches, electrical to optical isolators, power supplies, I/O boards, SVDU processors, PIF modules, fans, and the engineering tool. There was also a panel for the SVDU displays and a smaller rack for the MELTAC CPUs in the standby controller configuration. The demonstration facility included the [ ] MELTAC CPU configurations, including the single controller; redundant parallel controller; and standby controller configurations. The demonstration facility also demonstrated a control network, datalink network, and maintenance network.

7.1. SVDU Processor, Display Unit, and Cabling

Cabling between the SVDU processor and display units included Red, Green and Blue (RGB) analog cable from the processor to display units using coaxial cable, and use of fiber optic cable from the display units to the processor. The RGB cable provides graphic display information to the display units and is limited to a distance of approximately [ ] meters. Distance from the display units to the processor would need to be addressed on an application-by-application basis and will need to be in the technical/installation manuals supplied to a customer. The fiber optic cable transmits touch screen information from the display units to the processor [

]

[

]

7.2. I/O Boards

The NRC staff questioned the ability to hot-swap boards in the CPUs or other components. MELCO stated that the CPU boards could not be hot-swapped, but the I/O boards could be swapped while running. The NRC staff did observe the hot-swap capability of the I/O boards. MELCO also attempted to hot-swap a digital output board with a digital input board. [

]

7.3. CPUs

The NRC staff observed the markings on the front of the boards. The status alarms on the front of the CPU system status board only displayed Japanese labels. The NRC staff questioned whether an English version of the hardware, technical manuals, and engineering tool would be developed. MELCO stated that boards with English markings, English technical manuals, and English versions of the engineering tool will be developed in the future. The NRC staff stated that verification of English labels, manuals, and tools would be an application-specific action item.

The NRC staff observed [ ] toggle switches on the CPU system status board. [

]

The NRC staff observed that the CPU can be reset by cycling the power breaker feeding the CPU's power supplies or by pressing the reset button on the front of the CPU card. [

]

[

]

For the redundant parallel CPU configuration, the NRC staff observed a synchronization cable between the two CPUs. [

]

The NRC staff did not identify discussions in the topical report of the synchronization activities for the two CPUs in the redundant parallel configuration. [

]

7.4. Cabinet Alarms

The NRC staff observed that fan failures are indicated by a loss of fan rotation verses loss of power to the fan. [

]

7.5. Control Network and Optical Switches

The NRC staff observed the dual-ring control network in the demonstration facility. [

]

The NRC staff reviewed [ ], "The hours of operation and the observed failure rates of the MELTAC Platform." This document was provided as a result of a Request for Additional Information. [

]

[

]

7.6. Maintenance Network and Engineering Tool

The NRC staff observed the maintenance network and engineering tool connections to the MELTAC controllers. The engineering tool uses a Windows-based operating system running MELTAC Engineering Station (MELENS) software. The NRC staff observed the operation of the engineering tool for tracing through function blocks while the controllers were running. [

]

[

]

[

]

[

]

[

]

7.7. Datalink Network

The NRC staff observed the implementation of the data link between controllers. The data link is used to provide communication between controllers in separate divisions [

]

7.8. Identification of Hardware and Software Modules

MELCO provided a new document [ ], "MELTAC H/W and S/W Module List," which, listed the module types, descriptions and if each was safety or non-safety. [

]

8. HARDWARE QUALIFICATION

The NRC staff toured the environmental, electromagnetic/radio-frequency interference EMI/RFI, and seismic testing facilities at MELCO's Kobe, Japan facility. The NRC staff observed the operational condition of the equipment, interviewed personnel associated with the equipment, and observed operation of equipment.

[

]

MELCO also utilizes an un-qualified anechoic chamber to perform EMI/RFI pre-compliance testing. MELCO performs all official EMI/RFI testing at outside independent test houses, including the official testing for the MELTAC platform. MELCO provided a summary report of the EMI/RFI tests that were in English, at the audit. [

]

The NRC staff observed the vibration/seismic testing equipment at the MELCO Kobe, Japan facility. While MELCO possesses in-house testing equipment, the shaker tables are not capable of shaking a full cabinet. Therefore, the seismic qualification testing for the MELTAC platform was performed at an outside facility that could perform testing on an entire cabinet of equipment. MELCO stated that they do perform pre-confirmatory seismic/vibration table at their facilities at a component versus rack assembly. [

]

9. SOFTWARE TOOLS

The NRC staff observed the use of the application software development tools that are part of the MELTAC platform.

The NRC staff observed the use of two application software development tools that are used to develop application software for the MELTAC platform. Both tools run on the engineering tool workstation [ ] The first tool is RAPID, which is a computer-aided drafting software [

]

[

]

The second tool is MELENS which receives the RAPID function block diagram and translates it to a function block diagram format usable within the tool. MELENS compiles the function block diagram into a binary table that is downloaded to the controller. [

]

The NRC staff observed the transfer of the software from MELENS to the CPU. MELCO described the process by which the transfer was accomplished. [

]

[

]

RG 1.152, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," Revision 2, endorses IEEE Std. 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations." Clause 5.3.2 states, in part, that software tools used to support software development processes and V&V processes should be controlled under configuration management. The NRC staff verified that the RAPID and MELENS tools were under configuration management.

Specifically, MELCO personnel provided the development documents of the tools for the NRC staff to review at the audit. [

] The NRC staff also had MELCO personnel demonstrate retrieval of the tools and their documentation from the CEAS system. Clause 5.3.2 of IEEE Std. 7-4.3.2-2003 also states, in part, that one or both of the following methods should be used to confirm the software tools are suitable for use:

- A test tool validation program should be developed to provide confidence that the necessary features of the software tool function as required.

- The software tool should be used in a manner such that defects not detected by the software tool will be detected by V&V activities.

In Section 4.1.4.1, a), Creation of Application Software of the topical report, for application software development using the MELTAC platform, credit is not taken for the quality of the MELENS and RAPID tools for ensuring that no defects are introduced or omitted by the tools. Rather, MHI will take credit for the V&V activities for application software development to detect any errors introduced or omitted by the tools. However, MELCO was able to provide evidence that the tools had undergone a V&V program. The NRC staff viewed Document [ ], "Engineering Tool Test Manual and Test Report for MELTAC NPlus R3," Revision 4, dated January 28, 2004. The document outlined a testing program that was comparable in scope to the testing performed for the MELTAC basic software.

10. SOFTWARE VERIFICATION AND VALIDATION

10.1. Design Review Board or Comparable V&V for Category 2 Software

As a result of the audit of MHI documents in Arlington, VA, the NRC staff noted that a design review board, or comparable V&V, and should be considered in review of the Category 2 software at the next audit.

To this result, MELCO provided two "Program Creations Specification Checklists" documents; [

]

10.2. Further Information for the Assessment of the Sufficiency of Category-2 Software

At the January 22 - 23, 2009, public meeting with MHI, the NRC staff raised the concern with regards to the lack of independent V&V and the operating experience, with supportive conditions, of one fuel cycle or more as the basis for acceptance of Category 2 software units. MHI was to further justify their program for Category 2 software or propose additional U.S. Conformance Program (UCP) activities.

In a new document, [ ], "Category-2 S/W Validity Explanatory Material," MELCO presented additional information in the assessment of the Category-2 software. The main point of this document was to extrapolate the additional experience of the Category 2 software modules. Particularly, MELCO wished to present the additional operating experience that the Category 2 modules can be credited with since the UCP program began in 2006. At that time, the differentiation between Category 1 and Category 2 modules was one fuel cycle. Therefore, as of February 2009, the Category 2 software modules have a minimum of three years operating experience. Also, the document went on to state the anticipated experience that the Category 2 software will have by assuming the US-APWR initial startup, will be 2015.

10.3. Adherence of the topical report to Branch Technical Position (BTP) -14 - Guidance on Software Reviews

Also from the January 22 - 23, 2009, public meeting with MHI, the NRC staff raised a concern that the guidelines in BTP 7-14, "Guidance on Software Reviews," have not been addressed. MHI agreed to provide a cross reference between BTP 7-14 with the documents submitted or made available to the NRC staff at audits.

In a new document, [ ], "Correspondence Sheet Between BTP 7-14 and Topical Report," MELCO presented how the topical report met the guidelines of BTP 7-14. The document identifies, generally, where plans are addressed but does not provide any of the characteristics described in BTP 7-14.

The guidance in BTP 7-14 focuses on management, implementation and resource characteristics for each plan as well as review guidance that the NRC staff will specifically look for.

11. POWER INTERFACE MODULE

The NRC staff verified the technical aspects of the PIF module. The purpose of the verification was to ensure that the priority logic was non-software/non-firmware based. Additionally, the NRC staff attempted to verify the correctness of the logic. MELCO personnel provided an actual PIF module for observation as well as document [ ], "PIF Module Hardware Specification," Revision A, dated February 8, 2007, which was in Japanese.

[

]

[

]

[

]

[

]

12. THREAD AUDITS
None completed.

APPENDIX A: LIST OF DOCUMENTS REVIEWED

[ ], "The hours of operation and the observed failure rates of the MELTAC Platform."

[ ], "MELTAC H/W and S/W Module List."

[ ], "Release Note for MELENS," Revision BK, dated November 12, 2008 (in Japanese).

[ ], "Engineering Tool Test Manual and Test Report for MELTAC NPlus R3."

Loop Director C-DR Check Sheet

Flip-flop C-DR Check Sheet

[ ], "Category-2 S/W Validity Explanatory Material."

[ ], "Correspondence Sheet Between BTP 7-14 and Topical Report."

[ ], "PIF Module Hardware Specification," Rev. A, dated Feb. 8, 2007 (in Japanese).

Software Development Documents

[ ], "Standard POL Function and Structure Test Specification Test Report," Revision F

Error Reports

Error Report [ ]

APPENDIX B: LIST OF OPEN ITEMS

Open Item	Section of Audit Report	Description
1	1.3. Control of Materials and Manufacturing Processes	[ ]
2	1.3. Control of Materials and Manufacturing Processes	[ ]
3	3.0. Power Supplies	[ ]
4	4.0. Self Diagnostics and Fault Tolerance	[ ]
5	7.0. MELTAC Equipment - Input/Output Boards	[ ]

6	7.0. MELTAC Equipment - CPUs	[ ]
7	7.0. MELTAC Equipment - CPUs	[ ]
8	11. Power Interface Module	[ ]

APPENDIX C: LIST OF ACRONYMS

BTP	Branch Technical Position
CEAS	MELCO Corporate Electronic Archive System
CPU	Central Processing Unit
EEROM	Electrically Erasable Read-Only Memory
EMI	Electromagnetic Interference
FPGA	Field Programmable Gate Arrays
HDL	Hardware Description Language
Hz	Hertz
IEEE	Institute of Electrical and Electronics Engineers
I&C	Instrumentation and Control
I/O	Input/Output
ISG	Interim Staff Guidance
mA	Milliampheres
MELCO	Mitsubishi Electric Corporation
MELENS	Mitsubishi Electric Total Advanced Controller Engineering Station
MELTAC	Mitsubishi Electric Total Advanced Controller
MHI	Mitsubishi Heavy Industries, Ltd.
NRC	Nuclear Regulatory Commission
PCB	Printed Circuit Board
PIF	Power Interface Module
RAM	Random Access Memory
RAPID	Commercial Mitsubishi-made Computer-Aided Design (CAD) Software Package
RG	Regulatory Guide
RGB	Red, Green and Blue
RFI	Radio Frequency Interference
RS	Recommended Standard
SVDU	Safety-Related Visual Display Unit
S/W	Software
UCP	US Conformance Program
US-APWR	United States - Advanced Pressurized Water Reactor
V	Volts
V&V	Verification and Validation

DC Mitsubishi - US APWR Mailing List (Revised 02/15/2011)

cc:

Ms. Michele Boyd
Legislative Director
Energy Program
Public Citizens Critical Mass Energy
and Environmental Program
215 Pennsylvania Avenue, SE
Washington, DC 20003

Atsushi Kumaki
Mitsubishi Heavy Industries, Ltd.
APWR Promoting Department
Wadasaki-cho- 1-1-1, Hyogo-ku
Kobe 652-8585 JAPAN

Dr. Masanori Onozuka
Mitsubishi Nuclear Energy Systems, Inc.
1001 19th Street North, Suite 710
Arlington, VA 22201-5426

Dr. C. Keith Paulson
Mitsubishi Nuclear Energy Systems, Inc.
300 Oxford Drive, Suite 301
Monroeville, PA 15146

Mr. Tom Sliva
7207 IBM Drive
Charlotte, NC 28262

Mr. Robert E. Sweeney
IBEX ESI
4641 Montgomery Avenue
Suite 350
Bethesda, MD 20814

Mr. Ed Wallace
General Manager - Projects
PBMR Pty LTD
P. O. Box 9396
Centurion 0046
Republic of South Africa

Mr. Gary Wright, Director
Division of Nuclear Facility Safety
Illinois Emergency Management Agency
1035 Outer Park Drive
Springfield, IL 62704

DC Mitsubishi - US APWR Mailing List

Email

APH@NEI.org (Adrian Heymer)
atsushi_kumaki@mhi.co.jp (Atsushi Kumaki)
awc@nei.org (Anne W. Cottingham)
bgattoni@roe.com (William (Bill) Gattoni))
BrinkmCB@westinghouse.com (Charles Brinkman)
chris.maslak@ge.com (Chris Maslak)
ck_paulson@mnes-us.com (C Keith Paulson)
ckpaulson@aol.com (C.K. Paulson)
CumminWE@Westinghouse.com (Edward W. Cummins)
cwaltman@roe.com (C. Waltman)
david.hinds@ge.com (David Hinds)
david.lewis@pillsburylaw.com (David Lewis)
DeLaBarreR@state.gov (R. DeLaBarre)
Derlinda.Bailey@chguernsey.com (Derinda Bailey)
donald.woodlan@luminant.com (Donald Woodlan)
eliza.seedcoalition@gmail.com (Elza Brown)
erg-xl@cox.net (Eddie R. Grant)
f.tanaka@mnes-us.com
gcesare@enercon.com (Guy Cesare)
james.beard@gene.ge.com (James Beard)
jerald.head@ge.com (Jerald G. Head)
jim.riccio@wdc.greenpeace.org (James Riccio)
Joseph_Hegner@dom.com (Joseph Hegner)
jrund@morganlewis.com (Jonathan Rund)
KSutton@morganlewis.com (Kathryn M. Sutton)
kwaugh@impact-net.org (Kenneth O. Waugh)
lchandler@morganlewis.com (Lawrence J. Chandler)
lon.burnam@house.state.tx.us (Lon Burnam)
m.goto@mnes_us.com
Marc.Brooks@dhs.gov (Marc Brooks)
maria.webb@pillsburylaw.com (Maria Webb)
mark.beaumont@wsms.com (Mark Beaumont)
Mark.Crisp@chguernsey.com (Mark Crisp)
mark.vannoy@mnes-us.com
masahiko_kaneda@mhi.co.jp (Masahiko Kaneda)
masanori_onozuka@mnes-us.com (Masanori Onozuka)
masato.oba@mnes-us.com
masayuki_kambara@mhi.co.jp (Masayuki Kambara)
matias.travieso-diaz@pillsburylaw.com (Matias Travieso-Diaz)
mayorsouthern@granbury.org (Mayor David Southern)
media@nei.org (Scott Peterson)
mike_moran@fpl.com (Mike Moran)
MSF@nei.org (Marvin Fertel)
mutsumi_ishida@mnes-us.com (Mutsumi Ishida)

DC Mitsubishi - US APWR Mailing List

mwetterhahn@winston.com (M. Wetterhahn)
nan_sirirat@mnes-us.com (Sirirat Mongkolkam)
nirsnet@nirs.org (Michael Mariotte)
Nuclaw@mindspring.com (Robert Temple)
patriciaL.campbell@ge.com (Patricia L. Campbell)
paul.gaukler@pillsburylaw.com (Paul Gaukler)
Paul@beyondnuclear.org (Paul Gunter)
pbessette@morganlewis.com (Paul Bessette)
plarimore@talisman-intl.com (Patty Larimore)
pshastings@duke-energy.com (Peter Hastings)
RJB@NEI.org (Russell Bell)
Russell.Wells@Areva.com (Russell Wells)
ryan_sprengel@mnes-us.com (Ryan Sprengel)
sabinski@suddenlink.net (Steve A. Bennett)
sandra.sloan@areva.com (Sandra Sloan)
satoshi_hanada@mnes-us.com (Satoshi Hanada)
satoshi_watanabe@mnes-us.com (Satoshi Watanabe)
sfrantz@morganlewis.com (Stephen P. Frantz)
shinji_kawanago@mnes-us.com (Shinji Kawanago)
stephan.moen@ge.com (Stephan Moen)
steven.hucik@ge.com (Steven Hucik)
strambgb@westinghouse.com (George Stramback)
Tansel.Selekler@nuclear.energy.gov (Tansel Selekler)
tgilder1@luminant.com (Tim Gilder)
tmatthews@morganlewis.com (T. Matthews)
tom.miller@hq.doe.gov (Tom Miller)
trsmith@winston.com (Tyson Smith)
Vanessa.quinn@dhs.gov (Vanessa Quinn)
vijukrp@westinghouse.com (Ronald P. Vijuk)
Wanda.K.Marshall@dom.com (Wanda K. Marshall)
whorin@winston.com (W. Horin)
yoshiki_ogata@mhi.co.jp (Yoshiki Ogata)