DIGITAL INSTRUMENTATION AND CONTROLS DESIGN AUDIT REPORT

Audit Team:

The following U.S. Nuclear Regulatory Commission (NRC) staff members from Office of New Reactors participated in the audit (see Enclosure 2 for a complete list of audit participants):

- Dinesh Taneja (Audit Team Leader)
- Ian Jung (Instrumentation and Controls Branch (ICB) Chief, Supervisory Representative)
- Royce Beacom (Technical Reviewer)
- Tung Truong (Technical Reviewer)
- Khoi Nguyen (Technical Reviewer)
- William Ward (Senior Project Manager)

The following key individuals from Mitsubishi Electric Corporation (MELCO), Mitsubishi Heavy Industries Ltd. (MHI), and Mitsubishi Nuclear Energy Systems (MNES) participated in the audit:

- Masahiko Nambu, MELCO
- Masashi Kitamura, MELCO
- Hozumi Kadohara, MELCO
- Katsumi Akagi, MELCO (Deputy Manager, US-APWR Project)
- Toru Ito, MELCO (Manager, Nuclear Plant Engineering, Nuclear Power Dept.)
- Hiroyuki Fukumitsu, MELCO
- Yuzuru Yasui, MHI
- Katsuhisa Takaura, MHI (Deputy General Mgr., Nuclear Electrical and I&C Engineering Department)
- Takeshi Ikeuchi, MHI
- Makoto Takashima, MHI
- Tatsuhiko Goto, MHI (Engineering Manager, Project Group, APWR Promoting Department)
- Mamoru Tani, MHI (US-APWR Validation & Verification Team Manager, I&C Projecting Group, Nuclear Electrical and I&C Engineering Department)
- Amano Nobuo, MHI (Engineering Manager, I&C Projecting Group, Nuclear Electrical and I&C Engineering Department)
- Shinji Kiuchi, MNES (Mgr., I&C and Elec. Engineering Section)
- M. Vann Mitchell, MNES (General Mgr., Quality Assurance)
- Erin Wisler, MNES (DCD Licensing Engineer)

1.0 SUMMARY

MHI submitted to the NRC, Design Control Document (DCD) Revision 3 for its United States - Advanced Pressurized Water Reactor (US-APWR) application in March 2011. This included

Chapter 7, “Instrumentation and Controls.” MHI also submitted many supporting documents referenced in Chapter 7. These documents and technical reports are referenced by the DCD because they contain design details not provided in the DCD. Included among the technical reports were the details of the Mitsubishi Electric Total Advanced Controller (MELTAC) digital instrumentation and controls (I&C) platform to be used by MHI in the US-APWR design. The MELTAC platform is designed and built by MELCO. The NRC staff reviewed the information associated with Chapter 7 and issued multiple Requests for Additional Information (RAIs). Upon reviewing MHI’s responses to the RAIs, the NRC staff concluded that a review of the design details related to the MELTAC platform was needed to assist in making the determination that the US-APWR I&C systems design meets the regulatory requirements.

On December 12, 2011, MELCO/MHI arranged for the audit team to visit the Ohi Nuclear Power Station on the Ohshima peninsula. The station is operated by the Kansai Electric Power Company, Inc. The purpose of the visit was to observe the recent installation of the MELTAC digital I&C platform at Units 3 and 4. The staff was given a tour of the units and the MELTAC related equipment. The staff was able to take a detailed look at the equipment and have their questions answered by knowledgeable MELCO and station personnel.

The audit was conducted at the MELCO facilities in Kobe, Japan from December 13, 2011, to December 16, 2011. The NRC staff conducted the audit in accordance with the NRC Office of New Reactors (NRO) Office Instruction NRO-REG-108. The plan for this audit is documented and can be found in the Agencywide Document Access and Management System (ADAMS) under accession number ML113220196, dated November 22, 2011. Daily during the audit, the NRC team and MHI met to discuss issues identified by the NRC team.

The audit focused on the areas that cannot be readily audited at the MNES offices located in the United States. The staff examined and evaluated non-docketed details of the US-APWR digital I&C design that support the staff’s findings of reasonable assurance of safety in a number of areas as described below:

1. Observed a demonstration of the MELTAC controller operations and reviewed un-docketed documentations to verify the critical aspects that support independence in the US-APWR data communications,

2. Observed sample projects that are similar to the US-APWR digital I&C systems, and reviewed un-docketed documentations to verify the US-APWR digital I&C system application software development process,

3. Observed sample projects that are similar to the US-APWR digital I&C systems, and reviewed un-docketed documentations to verify integration of the MELTAC basic software into the US-APWR application software for safety I&C systems,

4. Observed a demonstration of the Memory Integrity Check using Engineering Tool, and

5. Verified closure of the March 2009, US-APWR digital I&C system regulatory audit findings (ML093240406).

The audit commenced with an entrance briefing. At this briefing, MELCO and MHI provided the schedule of activities for the audit, initial documents for review, and introduced its key staff. Daily briefings were held by the NRC audit team to discuss observations. The audit and the briefings were attended by representatives from MHI, MELCO, MNES, and Luminant Generation Company, LLC (a MHI customer). The Japan Nuclear Energy Safety Organization (JNES) was invited to observe the audit but declined due to other commitments. The audit and the briefings were attended by interpreters to facilitate translations.

At the final exit briefing, the NRC audit team stated that all of its objectives as stated in the audit plan had been met and there are no outstanding issues resulting from this audit.

2.0 BASIS

- Title 10 of the *Code of Federal Regulations* (10 CFR), Part 52 – "Licenses, Certifications, and Approvals for Nuclear Power Plants," provides the requirements regarding an application for a new reactor design certification. Subpart B – Standard Design Certifications, Section 52.48 – Standards for review of applications, states, "Applications filed under this subpart will be reviewed for compliance with the standards set out in 10 CFR parts 20, 50 and its appendices, 51, 73, and 100."

- Part 10 CFR 50.55a, "Codes and standards," Section (h), "Protection and safety systems," provides additional requirements regarding the standard codes and standards related to instrumentation and controls which are incorporated by reference into the regulations and must be met in the application.

- General Design Criterion (GDC) 13 of 10 CFR 50, Appendix A, "Instrumentation and control," requires that, "Instrumentation shall be provided to monitor variables and systems over their anticipated ranges for normal operation, for anticipated operational occurrences, and for accident conditions as appropriate to assure adequate safety, including those variables and systems that can affect the fission process, the integrity of the reactor core, the reactor coolant pressure boundary, and the containment and its associated systems. Appropriate controls shall be provided to maintain these variables and systems within prescribed operating ranges."

- GDC 20, "Protection system functions"; GDC 21, "Protection system reliability and testability"; GDC 22, "Protection system independence"; GDC 23, "Protection system failure modes"; and GDC 24, "Separation of protection and control systems" provide additional regulatory requirements regarding the instrumentation and controls systems.

- Regulatory Guide (RG) 1.206, "Combined License Applications for Nuclear Power Plants (LWR Edition)," Section C.III, Chapter 7, provides additional guidance regarding the information to be provided by the applicant.

- Instrumentation and Controls Applications are evaluated following the guidance provided in NUREG-0800, Chapter 7, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition – Instrumentation and Controls."

3.0 OBSERVATIONS AND RESULTS

MHI and MELCO invested a significant amount of effort in preparations and for facilitating this audit. A large amount of non-docketed information was made available in a well-organized manner, especially; the handout material that addressed all of the audit items identified in the NRC audit plan, and also included some of the key open items associated with the US-APWR DCD. Table 1, "Audit Plan for US-APWR Digital I&C Design," contained in the audit handout material and adapted below was followed for performing the NRC audit activities.

Table 1: Audit Plan for US-APWR Digital I&C Design

No.	Item	NRC request {NRC audit plan}	Demonstration*	Document Review*
1	Digital data communication independence	Observation of the MELTAC controller operations and review of un-docketed documentations will be conducted to verify the critical aspects that support the US-APWR data communication independence. The following are some of the key activities that are intended for the audit of the MELTAC data communication design:	---	---
		a. Verify nonsafety signals are rejected by priority module upon the presence of a safety signal	YES	YES
		b. Verify a failure or communication fault of a single sending train does not affect the receiving bus master module's ability to receive data from the other two trains		
		c. Verify the safety signals do not depend on the bypass status signals		
		d. Verify only predefined data are processed	YES	YES
		e. Verify data check to detect: data corruption, unintended repetition, incorrect sequence, data loss, unacceptable delay, unexpected data insertion, invalid data "masquerade" as valid ones, incorrect address/wrong destination, over length messages, high rate messages, commission fault, inconsistency fault, excessive jitter, data collision, out of range data, incorrect data location, out of sync, incorrect encoding or decoding, and interruption.	NO	
		f. Perform thread audit of Hardware Specification JEMJ-04CC07-J5 as referenced	NO	YES

No.	Item	NRC request {NRC audit plan}	Demonstration*	Document Review*
		by technical report MUAP-07005-P, "Safety System Digital Platform," Revision 8. The audit focuses on error correcting code		
		g. Perform thread audit of the MELTAC controllers' failure data records	NO	YES
2	Deterministic performance of digital I&C systems	Observation of the MELTAC controller operations and review of un-docketed documentations will be conducted to verify deterministic performance of integrated digital I&C systems	YES	YES
3	Implementation of watchdog timer	Implementation of the watchdog timers as described in DCD and related technical reports will be verified by observation the MELTAC controller operations and review of un-docketed documentations	YES	YES
4	Digital I&C system application software development	Observation of sample projects that are similar to the US-APWR digital I&C systems, and review of un-docketed documentations will be conducted to verify the US-APWR digital I&C system application software development process	YES	YES
5	Integration of MELTAC basic software into the US-APWR safety I&C systems	Observation of sample projects that are similar to the US-APWR digital I&C systems, and review of un-docketed documentations will be conducted to verify integration of the MELTAC basic software into the US-APWR application software for safety I&C systems	NO	YES
6	Demonstration of memory integrity check using engineering tool	Demonstration of Memory Integrity Check using Engineering Tool	YES	YES
7	Demonstration of other manual testing	N/A	YES	YES
8	Self-diagnostic features of the PSMS	N/A	YES	YES
9	PSMS software change	N/A	YES	YES
10	Diverse actuation system	N/A	YES	YES
11	Follow-up March 2009 audit findings	Follow-up on March 2009 US-APWR digital I&C system regulatory audit findings (ML093240406)	NO	YES

*Details in the Demonstration and Document Review columns referred to proprietary information and have been changed to a simple yes or no to indicate the type of review performed.

In summary, the audit accomplished all of the intended objectives. The staff had the opportunity to review a number of documents, and witness demonstrations that provided additional technical details regarding the US-APWR digital I&C design. All of the audit items outlined in

the audit plan and Table 1 were successfully evaluated and as a result there are no outstanding issues.

The NRC staff made the following observations:

Ohi Nuclear Power Plant Visit

MELCO/MHI made all the needed arrangements for a visit to the Ohi Nuclear Power Station located at the tip of Ohshima peninsula on December 12, 2011. The site contains four PWR units. Units 1 and 2 were supplied by Westinghouse. Units 3 and 4 were supplied by MHI. Our visit was limited to Ohi, Unit 4, a four-loop pressurized water reactor, which began commercial operation on February 02, 1993. The plant visit began with a brief overview of the Ohi Nuclear Power Station by Kansai Electric Power Company (KEPCo) management. MELCO representatives then provided an overview of the Ohi-4 I&C system architecture and compared it to the US-APWR I&C architecture. The Ohi-4 Reactor Protection System (RPS) is similar in design to the US-APWR RPS and employs the MELTAC platform. Also, the Ohi-4 plant control and monitoring system is configured with digital platforms, including MELTAC.

The plant tour included I&C equipment rooms, main control room (MCR), main turbine area observation deck, and refueling pool area. The staff was allowed to look into each of the safety and non-safety related I&C cabinets containing MELTAC controllers and analog electronic components. However, plant policies do not allow the taking any photographs in the plant. MELCO representatives, who are responsible for the maintenance of I&C components, explained the Ohi-4 I&C system at board-level detail. The Ohi-4 MCR utilizes traditional hardwired controls. Upgrade of the MCR to an advanced design using visual display units (VDUs) is in the planning stages.

This plant visit provided evidence and additional assurance of the MELTAC platform's capabilities for performing safety related controls. Parts of the US-APWR I&C architecture are similar to the Ohi-4 data communication features and therefore utilize the maturity in design gained from operating experience of the MELTAC platform.

Digital Data Communication Independence (Table 1, Item No. 1)

Critical aspects of the US-APWR data communication independence were evaluated by witnessing lab demonstrations and document reviews outlined below:

- Demonstrations

  Per the staff requests, MHI successfully performed demonstrations of several operations on the actual MELTAC controllers. The demonstration setup includes two cabinets, one safety VDU (S-VDU), one operational VDU (O-VDU), three monitors, and input devices. Cabinet #1 (Central Processing Unit {CPU} 1) consists of RPS and communication controllers. Cabinet #2 (CPU 2) consists of

engineered safety features actuation system (ESFAS) and safety logic system (SLS) controllers. Each demonstration was preceded with a detail explanation of the circuitry. The demonstrations include the following:

1. Demonstration for Interdivisional Communication of RPS

   The following were successfully demonstrated:
   - Voting logic: Functionality of two-out-of-four voting logic via Data Link.
   - Bypass control: Functionality of bypass control logic.
   - Communication error:
     - Communication error of data link in three or more trains results in tripped condition.
     - Data link communication maintains operational in the event of one train in bypass condition.

2. Verify non-safety signals are rejected by priority module upon the presence of a safety signal

   The demonstrations showed safety signals were given higher priority over non-safety signals as follows:

   - Safety signal from S-VDU was given higher priority over non-safety signal from O-VDU.
   - Safety automatic signal was given higher priority over non-safety automatic signal.
   - Safety automatic signal was given higher priority over non-safety manual signal.
   - Safe state signal was given higher priority over non-safe state signal.

3. Manual tests on the following were successfully performed:
   - Channel calibration
   - Trip actuation device operational testing

4. Failure Detection Testing

   The following were successfully performed:

   - The CPU generated alarms when the control network cable was disconnected.
   - The CPU generated alarms when the data link cable was disconnected.
   - The CPU generated alarms when the input/output (I/O) module was removed.

5. Power interface module (PIF) testing

   The bit-by-bit tests with different inputs were successfully performed on the PIF module.

6. Bus master module testing

   Tests were successfully performed to verify that a failure or communication fault of a single sending train does not affect the receiving bus master module's ability to receive data from the other two trains (trip signals were processed through).

- Interviews and Document Review

1. The following documents were reviewed to verify that the data check function existed to detect data corruption, unintended repetition, incorrect sequence, data loss, unacceptable delay, unexpected data insertion, invalid data "masquerade" as valid ones, incorrect address/wrong destination, over length messages, high rate messages, commission fault, inconsistency fault, excessive jitter, data collision, out of range data, incorrect data location, out of sync, incorrect encoding or decoding, and interruption (See Enclosure 3 for a complete list of documents and titles).

   - **[**
   -
   -
   -
   -
   -
   -
   -
   -
   -
   ]

   The review has shown that the above documents contain information that is consistent with the US-APWR DCD.

2. A thread audit of the following documents was performed to verify that the error correcting code (ECC) is used consistently across docketed and non-docketed documents.

   - **[**
     ]
   - **[**
     ]
   - **[** **]**

   The document reviews and interviews with MHI engineers showed that the ECC is used consistently across all applicable documents.

3. A summary of a thread audit of the MELTAC Controllers' Failure Data Record is as follows:

   Since the delivery of the first system in 2001, the MELTAC platform has been applied to Japanese plants. In the facilities where the current MELTAC platform has been applied, **[**

   ]

   Further interviews with MHI and MELCO engineers revealed that these failures had been studied and corrected, and monitored by MHI and MELCO and have not impacted the safe operation of the Japanese plants.

MELTAC Basic & Application Software (Table 1, Item No. 4 through 9)

Observation of sample projects that are similar to the US-APWR digital I&C systems was conducted to verify the application software development process and integration of MELTAC basic software by witnessing lab demonstrations and document reviews outlined below:

- **Demonstrations**

  (1) Application Software Development Process and Software Integration

  The staff had requested to observe sample implementation of the US-APWR digital I&C system application software development process. MHI provided a demonstration on the application software generation flow based on Figure 3.2-2, "Development Process of the Application Software," of MUAP-07017-P-SRI,

Revision 4, “US-APWR Software Program Manual.” The first part of the demonstration involves using the RAPID software tool to create a Function Block Diagram (FBD) for a particular PSMS function based on Plant and Basic Requirements. The FBD data is copied to a CD-R media which is used to import it into the MELTAC engineering tool (MELENS) laptop. **[**

] Then MELENS compiles the three imported items into an application executable module. Finally, MELENS loads the executable module onto the MELTAC controller.

(2) Memory Integrity Check

The Memory Integrity Check (MIC) feature compares the application executable module that resides on MELENS laptop and the application execution module that resides on the controller’s F-ROM. The MIC feature does a bit-by-bit check of both data, and outputs an error (displays yellow text) if there is a mismatch. Examples of both matched and mismatched application modules were demonstrated.

The staff understands that MELCO is also developing a MIC feature for the basic software. It may be helpful to the staff to have design and implementation information.

(3) PSMS Software Change

MHI demonstrated the procedure for PSMS Software Change. Changes are allowed by following the re-writing method and through a dedicated re-programming chassis, **[**

] MELTAC memory integrity check feature is used to verify correct software download version on the CPU Module.

The staff observed that these demonstrations reflect the high-level procedures described in the US-APWR Software Program Manual. The demonstrations also clarify some software process related issues raised in pending RAIs. In summary, the audit objectives were met, and any potential changes to the US-APWR DCDs will be handled through resolution of these pending RAIs.

- **Interview**

(1) Presentations were provided by the Verification and Validation (V&V) team of the Plant Requirement and System Requirement phases with regards to the

identification of the input requirements and documents. Additionally the overall planning schedule was provided for these phases showing MHI is currently in the System Requirements phase V&V for US-APWR. Also provided was the Task Manual (procedure) for the System Requirements phase V&V activities.

(2) The staff interviewed several MHI V&V team members. The V&V Team had worked on a similar I&C project at the Tomari 3 Nuclear Power Plant in Japan. The team went over the V&V Task Manual which described V&V activities for various development phases like plant requirements, systems requirement, and design phase. The documentation also included a table of anomalies found during development phases and software installation plans with checklists to verify software between the factory and plant environment. Overall, MHI provide helpful examples of the V&V activities undertaken for Tomari 3 which are similar to that of the US-APWR.

(3) Based on the interviews, the staff believes MHI delegates to MELCO these tasks: Developing Application Software (D-4A) and Acceptance Testing. It would be helpful if MHI describes any tasks that are delegated to MELCO in the US-APWR Software Program Manual.

(4) Referenced demonstration documents:

[
]
[**]**

Deterministic Performance (Table 1, Item No. 2)

Deterministic performance of the US-APWR digital I&C system, as described in the DCD and related technical reports, was verified by observation of the MELTAC lab demonstrations and review of un-docketed documentation. MELCO provided the following documents that demonstrate the constant cycle (deterministic) processing of MELTAC:

- **[**
]
- **[**
]

In general, the deterministic performance requirements specified in these documents confirm the design information provided in the DCD. From review of these documents the following items of interest were noted:

- Constant cycle operation with a single task is applied.

- CPU cycle time contains “Execution Time” and “Remaining Time Diagnostics.”
- **[**
-
-
    - o
    - o
    - o
    - o
    - o
    - o
-

]

Initially, MELCO had not planned on any lab demonstrations related to the MELTAC deterministic performance design feature. Upon the staff’s request, MELCO set up a test to measure the execution time data from CPU memory. In the lab setup, the CPU-1 cycle time was set at 100 mSec. The results of this test are as follows:

- **[**
-
-
- **]**

In this test example, a remaining cycle time of **[** **]** would be available for the remaining time diagnostics.

Interviews conducted with MELCO staff members provided additional clarifications on the deterministic performance of the MELTAC platform.

Watchdog Timer (Table 1, Item No. 3)

Implementation of the watchdog timers (WDT) as described in the DCD and related technical reports was verified by observation of the MELTAC lab demonstrations and review of un-docketed documentation. MELCO provided the following documents that provide the details of the watchdog timer implementation in the MELTAC CPU module:

- **[**
  ]
- **[**
  ]

A hardware based watchdog timer is installed on the MELTAC CPU module. The watchdog timer is typically set at approximately **[**

] It was also noted that if the constant cycle time is exceeded (greater than fixed cycle time), an alarm is generated.

Constant cycle main infinite loop processing flow in the MELTAC CPU module is a part of the MELTAC basic software and is outlined below:

[

]

During the lab demonstrations, reset of the watchdog timer on CPU1 was prevented which resulted in a CPU halt.

Interviews conducted with MELCO staff members provided additional clarifications on implementation of the watchdog timers on all three modules; namely 1) CPU Module, 2) Intelligent I/O Bus Master module, and 3) System Management Module.

Diverse Actuation System (Table 1, Item No. 10)

Review of the Diverse Actuation System (DAS) was not a part of the NRC audit plan. However, as a part of an RAI response, MHI/MELCO wanted to demonstrate the capabilities for 100 percent testing of the priority logic on the PIF module. The following design features of the PIF module's priority logic were demonstrated in the lab:

- The priority logic is composed of discrete AND/OR/NOT gates, and does not contain any software.
- Outputs don't depend on the timing or sequence of the inputs.
- When inputs are determined, the outputs are uniquely fixed regardless of the previous state of the device.
- All possible combinations of inputs and outputs of the priority logic can be defined and 100 percent tested. Priority logic on the lab demonstration PIF module had 6 inputs that resulted in 64 test cases.
- Testing does not involve use of the design tool. During testing, different combination of inputs simulated and output states verified based on the truth table for each test case.

March 2009 Audit Findings Follow-up (Table 1, Item No. 11)

In March 2009, the NRC had conducted a regulatory audit of the US-APWR digital I&C system in Kobe, Japan. The audit report, including the resulting findings is available in ADAMS under accession number ML093010325. MHI/MELCO was asked to provide a status on the findings reported. A proprietary internal document, JEXU-1034-1037, contained a list of eight Open Items from the NRC's March 2009, regulatory audit findings. This list was part of the audit documentation handout provided to staff at the start of this audit. During the course of the audit, MELCO demonstrated or described their resolution of the Open Items. The staff found these demonstrations or discussions acceptable and the Open Items are considered closed.

4.0 CONCLUSION

The observations and results identified in Section 3.0 above were reviewed and resolved. MELCO's MELTAC platform design as presented in the US-APWR DCD and referenced technical reports was verified through lab demonstrations of key design features and the review of un-docketed design documents. The MELTAC platform's basic and application software development process, as explained in the DCD was verified by reviewing the MELTAC process and procedures, and by reviewing the software development documents of a Japanese nuclear power plant. The audit accomplished all of the intended objectives. All of the audit items outlined in Table 1 were successfully evaluated and as a result there are no outstanding issues.