DIGITAL INSTRUMENTATION AND CONTROLS DESIGN AUDIT REPORT

NRC Audit Team:

The following U.S. Nuclear Regulatory Commission (NRC) staff members from the Office of New Reactors (NRO) participated in the audit:

- Dinesh Taneja (Audit Team Leader)
- Deanna Zhang (Senior Electronics Engineer)
- Ian Jung (ICE2 Branch Chief, Supervisory Representative)
- William Ward (Senior Project Manager)

The following entities supporting the digital instrumentation and controls (DI&C) design portion of the United States - Advanced Pressurized Water Reactor (US-APWR) Design Certification application provided staff to answer questions during the audit: Mitsubishi Electric Corporation (MELCO), Mitsubishi Heavy Industries Ltd. (MHI), and Mitsubishi Nuclear Energy Systems (MNES). A complete listing of attendees by day is provided in Enclosure 2.

1.0 SUMMARY

In December 2008, MHI applied to NRC for certification of its US-APWR reactor design under Title 10 of the *Code of Federal Regulations* (CFR) Part 52. As part of the application MHI submitted the US-APWR Design Control Document (DCD), Revision 0. 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) DI&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 RAIs were either closed, left open as confirmatory items awaiting revisions to documents to close them, or left open and described as open items (OIs) in the Phase 2, Safety Evaluation Report (SER) with OIs. In September 2013, MHI submitted Revision 4 of the US-APWR DCD to NRC (see Agencywide Document Access and Management System (ADAMS) Accession No. ML13262A471). DCD Revision 4, as well as the revisions to the many supporting technical reports, allowed staff to close the confirmatory items. The Chapter 7 SER with OIs was reviewed by a subcommittee of the Advisory Committee on Reactor Safeguards (ACRS) in April 2013 and by the full committee in December 2013. The full committee issued its letter on December 24, 2013 (see ADAMS Accession No. ML13346A732). In the letter, the ACRS stated that the staff should ensure that sufficient design details are available to provide assurance that the watchdog timers (WDTs) will produce the desired reactor protection system and engineered safety feature actuation system failure state signals independently from the MELTAC platform software.

Staff continued its review of the remaining OIs and their associated RAI responses and issued a new RAI regarding the WDTs. After receiving the response to the last RAI, the NRC staff decided that an audit of the non-docketed design details related to the MELTAC platform was

needed to assist in making the determination that the US-APWR instrument and controls (I&C) systems design meets the regulatory requirements.

The audit was conducted at the MHI and MELCO facilities in Kobe, Japan from November 17 to November 21, 2014. The NRC staff conducted the audit in accordance with the NRC NRO Office Instruction NRO-REG-108. The plan for this audit, dated November 10, 2014, is documented and can be found in ADAMS Accession No. ML14310A834. 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. Staff examined and evaluated non-docketed details of the US-APWR DI&C design that support the staff's findings of reasonable assurance of safety in the following OIs (publicly available RAI response accession number listed first):

1. Correlation of Probabilistic Risk Analysis (PRA) information provided in DCD Chapter 7, Technical Report MUAP-07004-P, and DCD Chapter 19 (RAI 1091-7447, Questions 07-1 and 07-2 (ML14100A340 and ML14100A339)).

2. Details of WDTs to clarify their operation and independence from MELTAC platform software (RAI 1094-7466, Question 07.01-46 (ML14119A193 and ML14119A192)).

3. Details that demonstrate plant control and monitoring system (PCMS) failures are bounded by the Chapter 15 analysis, and design details that provide basis for segmentation of the US-APWR control functions. (RAI 1093-7366, Question 07.07-34 (ML14118A169 and ML14118A170)).

4. Details regarding the design-basis data communication faults, and information that demonstrates data communications independence between safety and non-safety I&C systems, including adequate testing for normal and abnormal data transmission conditions for the interfaces between non-safety and safety systems. (RAI 1076-7368, Question 07.09-27 (ML14059A163 and ML14059A164)). In addition, details of the following items related to data communications independence features were examined:

    a. Details regarding bounding constraints for the operational commands that are allowed from the Operational - Video Display Unit (O-VDU). [

    ]

    b. [

    ]

c. Details regarding how the priority logic ensures that the functional independence between the O-VDU and the safety system is validated. [

]

d. Details regarding how the lock function operates. [

]

e. [

]

f. Details of the detection and mitigation features of communications errors in the MELTAC platform. [

]

g. Details regarding the operation of the hardware arbitration interlock. [

]

h. Details that support the claims in Technical Report MUAP-07004, Table G.2-2, “Failure Modes and Effects Analysis for ESF Actuation in PSMS” (Sheet 25), regarding spurious signals from the O-VDU.

[

]

i. Details that support and verify the design features regarding the detection and mitigation strategies for identified failures in the Communication Error Patterns (Safety System Digital Platform MELTAC Technical Report (MUAP-07005), Appendix H, Table H.1, "Communication Error Patterns Identified."). [

] Staff interviewed technical experts who described the operation of these features. In addition, MUAP-13018 contains a table regarding how communication architecture and faults detectability are addressed for each communications fault (W-NET). Information that shows how communication failures are addressed for those with an action required identified in the evaluation table was examined.

j. Details that provide a complete list of interfaces between safety and non-safety systems, including both communications are hardwired interfaces.

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 their 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 Mitsubishi Electric Power Products, Inc. MELCO provided interpreters to translate between English and Japanese during the audit and the briefings. Lists of the docketed (Enclosure 3, ML15078A454) and non-docketed (Enclosures 4 - 6) documents available for this audit are provided as enclosures. Enclosure 4 is publicly available (ML15078A456). Enclosures 5 and 6 have been determined contain proprietary information and not available to the public.

At the final exit briefing, the NRC audit team stated that its original objective as stated in the audit plan had been met. Generally, the resolution of these OIs requires MHI to amend the associated RAI responses. MHI agreed to amend their responses to the RAIs discussed during the audit in order to clarify the responses. In addition, during the audit, other issues were identified which require revisions to the RAI responses, DCD, or other supporting documentation. These issues are identified as action items in Enclosure 7. They are referenced by the Action Item numbers in the detailed discussion in Section 3.0, Observations and Results, of this report. The audit team stated that this audit report would be prepared per NRO-REG-108. The team also stated that final resolution of the OIs would not occur until the amended RAI responses and revised documents were received and evaluated and the team completed evaluating the information obtained during the audit and the resolution of the action items.

2.0 BASIS

For the I&C area of review, the relevant regulatory requirements are identified, and the associated acceptance criteria are given, in NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition (SRP)," Section 7.1 and Appendix 7.1-A. The key regulations are identified below:

1. Title 10 of the *Code of Federal Regulations* (10 CFR) 50.55a(a)(1), "Quality Standards;"

2. 10 CFR 50.55a, "Codes and standards," 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;

3. 10 CFR 50.55a, "Codes and standards," Section (h), "Protection and safety systems," which requires compliance with Institute of Electrical and Electronics Engineers (IEEE) Std. 603-1991 and the correction sheet dated January 30, 1995;

4. 10 CFR Part 50, Appendix A, "General Design Criteria for Nuclear Power Plants," General Design Criteria (GDC) 1, 2, 4, 10, 16, 19, 25, 28, 29, 33, 34, 35, 38, 41, and 44;

5. 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;"

6. 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;

7. 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;"

8. 10 CFR 52.47, "Contents of applications; technical information;"

9. NUREG-0800, SRP, Appendix 7.1-D provides review guidance for evaluation of the digital system compliance with regulation [§50.55a(h)] by following IEEE Std. 7-4.3.2 criteria;

10. DI&C-ISG-04, "Digital Instrumentation and Controls, Highly-Integrated Control Rooms - Communications Issues," provides review guidance for evaluation of DI&C data communication independence; and

11. Regulatory Guide 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.

3.0 OBSERVATIONS AND RESULTS

The NRC staff has the following observations based on information reviewed; demonstrations provided by MHI and MELCO; and discussions with MHI and MELCO staff at the audit:

Correlation of PRA and I&C systems (Audit Scope Item 1):

MHI's response to RAI 1091-7447, Questions 07-1 and 07-2 dated April 9, 2014 (ML14100A340), was discussed with the MHI engineers cognizant of the response during the audit. The NRC staff informed MHI that in general, the RAI response, which removes unnecessary PRA references from DCD Chapter 7 and associated technical reports, is acceptable. However, an issue with the I&C reliability values provided in Chapter 19 for the PRA model is still an open item and will be evaluated as a part Chapter 19 review. MHI should confirm that the US-APWR I&C design safety analysis is addressed deterministically without any reliance on the PRA. MHI is asked to revise its response to RAI 1091-7447 to delete unnecessary PRA references in relation to I&C systems from the DCD and related technical reports. In addition, correct a typographical error in Section A.4.9 of MUAP-07004. (Audit Action Item No. 1-1)

Watchdog timer (Audit Scope Item 2):

The NRC staff examined the operation of the WDTs to verify the information provided in the response to RAI 1094-7466, Question 07.01-46, dated April 25, 2014 (ML14119A193). Specifically, the NRC staff examined information and held discussions with MHI and MELCO staff to verify that the WDTs' operation is independent from MELTAC platform software. [

]

[

] MHI agreed to address this issue. (Audit Action Item No. 2-3)

Plant Control and Monitoring System Failures Bounded by Chapter 15 Analyses (Audit Scope Item 3):

In its response to RAI 1093-7366, Question 07.07-34, dated April 23, 2014 (ML14118A169), MHI explained their bases for plant control and monitoring system (PCMS) failures analyses, PCMS segmentation design principles, and walked through the contents of the PCMS failure analyses presented in Sections J.1, J.2, and J.3 of MUAP-07004. MHI also responded to staff's request for additional details needed to evaluate Table J.1-1, Failure Modes and Effects Analysis of PCMS for Single Control Group Failure. Table J.1-1 contains conclusions stating a single PCMS group failure is bounded by the Chapter 15 anticipated operational occurrences (AOOs). [

]

NRC staff responsible for reviewing Chapter 15 provided the following feedback to MHI's response to RAI 1093-7366, which was shared with the MHI engineers cognizant of the response during the audit:

> In response to RAI 1093-7366, MHI changed only the first item (control group 1-1) in Table J.1-1. Whereas, MHI was asked to review all the control group failures [control groups (1-1) through (1-6), and (2-26)] and re-evaluate if all failure modes within a group are bounded by chapter 15 AOOs. Below are some of the specific issues:
>
> 1. [
>
>]
>
> 2. [
>
>]

[

]

3. [

]

4. [

]

5. [

]

The staff has not reviewed control group 20, operational VDU failures to see if they are bounded by DCD Chapter 15 postulated accidents, and needs to complete this review. NRC committed to providing any additional feedback that may result while reviewing control group 20. (Audit Action Item No. 1-4)

MHI understood the issues identified by the NRC staff during the audit and provided a draft amended RAI response after the audit. NRC staff plans to complete its review of this amended RAI response and provide any additional feedback to MHI. (Audit Action Item No. 1-4)

Digital Data Communications Independence (Audit Scope Item 4):

1. The NRC staff reviewed documentation to verify the abnormal data testing commitments described in MHI's response to RAI 1076-7368, Question 07.09-27, dated February 25, 2014 (ML14059A163). [

]

   a. Non-predefined data packets are not processed by the safety functional processor. The NRC staff observed that the full set of tests to ensure that this type of abnormal data transmission can be adequately addressed by the design has not been completed. [

] In addition, MHI staff agreed to map the abnormal transmission test cases to the communication faults identified in DI&C-ISG-04. (Audit Action Item Nos. 5-1, 5-2, and 5-3)

b. [

]

2. The NRC staff also observed a demonstration by MHI and MELCO to illustrate the following abnormal data communications are identified and mitigated by the MELCO platform.

a. Sequence error-Messages may be sent in the incorrect sequence: MHI and MELCO staff provided a demonstration to illustrate that out of sequence data packets sent from the O-VDU (or other non-safety controllers) will be detected by the MELCO communications system (COMS). [

] Based on the demonstration, the NRC staff observed that the simulated data transmission error was not a sequence error, but an overflow error. The NRC staff informed MHI and MELCO staff of this observation. MHI and MELCO staff acknowledged that the simulation represented their interpretation of a sequence error and this may not conform to the NRC staff's definition of a sequence error as identified in ISG-04. The NRC staff held discussions with MHI and MELCO staff to understand the response of the COMS to a sequence error (as defined by DI&C-ISG-04). [

] The NRC staff agreed with MHI and MELCO staff's assessment; however, the NRC staff noted that the analysis of why this type of transmission error is not possible per design needed to be described in the US-APWR DCD. MHI agreed to include this analysis in the US-APWR DCD. (Audit Action Item No. 3-2)

b. Communication Message Error/Error with improper format-Incorrect location of data: MHI and MELCO staff provided a demonstration to illustrate that a message with improper format sent from the O-VDU will be detected by the COMS. [

] During the demonstration, the NRC staff noted that it was not possible to observe the specific data packet error, nor the response by the safety CPU to this error because the demonstration was at the graphical level of the logical connections and did not show the actual data fields. To enable the NRC staff to view the communications process at the data field level, MHI and MELCO staff displayed the contents of the random access memory (RAM) in order for the staff to view the data in the different locations within the RAM. As such, the NRC staff was able to observe that a message

with data located in an improper data field would be detected by the COMS, and therefore would not be processed by the safety CPU.

c. Network error/Network Cable Error - Abnormal network connections: MHI and MELCO staff provided a demonstration to illustrate that when one of the two redundant network cables between the O-VDU and the safety controller is disconnected, data can still be transmitted from the O-VDU to the safety controllers through the redundant network cable; however, when both redundant network cables are disconnected, data cannot be transmitted to the safety controllers and therefore an alarm is generated. During the demonstration, the NRC staff was able to observe the intended response of the safety controllers when a single network cable was disconnected and when the two redundant network cables were disconnected.

During the demonstration of the above abnormal data communications between the safety controller and the O-VDU, the NRC staff observed that the MELTAC platform was used for both the safety VDU and the O-VDU. The NRC staff requested MHI to verify that the MELTAC platform is also used for the O-VDU in the US-APWR design. The MHI staff stated that the O-VDU is implemented on the MR computer which is not part of the MELTAC platform. [

] In addition, the staff noted that the US-APWR DCD indicates that the O-VDU platform is MELTAC. [

] In addition, MHI staff agreed to clarify within the US-APWR DCD that the O-VDU will be implemented using the MR computer and that the development process of the O-VDU using this MR computer conforms to the development process for items of augmented quality as described in the DCD. (Audit Action Item No. 2-2)

3. [

]

[

]

The NRC staff was not able to find specific requirements in the MELTAC design and requirements specifications to verify this design constraint. MHI needs to demonstrate that a requirement exists in the MELTAC requirements specifications that specifies that the number of commands is predetermined and fixed for every communication cycle (Audit Action Item No. 3-4)

4. The NRC staff reviewed the bounding list of predefined and acceptable commands from the O-VDU to safety systems for the US-APWR design. Specifically, this list represents the bounding list of allowable predefined commands from the O-VDU that can be written to the data table and therefore processed by safety CPU. The NRC staff observed that several of the commands within this list did not appear to have been documented in the US-APWR DCD. Specifically, the NRC staff noted that there are commands to initiate and terminate a maintenance trip and these functions have not been identified in the DCD nor was there an analysis provided in the DCD to analyze and assess whether these commands conform to the guidance of DI&C-ISG-04. [

] MHI staff also agreed to include the list of all predefined commands from the O-VDU in the US-APWR DCD. (Audit Action Item No. 4-2)

5. The NRC staff discussed with MHI staff on how the priority scheme between the O-VDU and the safety system is validated. [

]

6. The NRC staff examined details and held discussions with MHI and MELCO staff on the operation of the manual permissive logic that allows the O-VDU to bypass the safety function. The NRC staff requested MHI staff provide specific descriptions on how the signal for the permissive is generated (e.g., default settings, signal latching, set and reset block configuration). [

] This description should include default configuration settings for the permissive and the set/reset logic. MHI staff should also verify that the different symbols representing the latch function are included in the legend. MHI staff agreed. (Audit Action Item No. 1-2)

In addition, the NRC staff held a discussion with MHI staff to understand the justification for having the capability to bypass safety functions using the O-VDU enhances the performance of the safety function, as stated in DI&C-ISG-04, Section 1, "Interdivisional Communications," Position 3, given that the operator needs to set the permissive on the safety VDU. [

] MHI staff agreed to provide information to justify how the capability to perform these maintenance functions from the O-VDU supports or enhances the performance of safety functions to support demonstration of conformance to DI&C-ISG-04. (Audit Action Item No. 1-3)

7. The NRC staff requested that MHI and MELCO staff provided a description of how the lock function operates. [

]

[ ] The NRC staff requested that MHI staff verify that the description of the lock function, including how components are unlocked, is adequate in the US-APWR DCD. MHI agreed to verify this information in the US-APWR DCD. (Audit Action Item No. 1-3)

8. The NRC staff observed the operation of the bypass and lock function on the Japanese APWR simulator. MHI and MELCO staff demonstrated that performance of bypass and lock functions using the O-VDU on the simulator. The NRC staff requested MHI staff to show which alarms are generated when a function is bypassed or a component is locked out. [

] (Audit Action Item No. 6-1)

9. The NRC staff requested MHI staff to describe the bounding limits of the non-safety unit-bus configuration and the number of actions allowed per data packet for the US-APWR design-specific application. [

]

(Audit Action Item No. 2-1)

10. The NRC staff examined details regarding the operation of the hardware arbitration interlock. To demonstrate conformance to DI&C-ISG-04, Section 1, Position 4, MUAP-13018, Section 3.1.4, "ISG-04 1.4," specifies that various techniques are used to minimize the potential for simultaneous memory access while allowing each device to operate asynchronously. One of the key features is a hardware arbitration interlock. [

] (Audit Action Item No. 6-2)

11. The NRC staff requested MHI staff to clarify how the safety system priority logic addresses non-concurrent demands between the safety system and the O-VDU.

[

] (Audit Action Item No. 6-3)

12. The NRC staff requested that MHI and MELCO staff describe the operation of design features used to detect and mitigate failures identified in the Communication Error Patterns (MUAP-07005, Table H.1). [

] The NRC staff requested MHI and MELCO staff to verify that the description of these features in the US-APWR DCD is adequate and consistent with the information provided during the audit. MHI staff agreed. (Audit Action Item No. 5-1)

[

] The staff informed MHI staff that non-safety failures do not count as single failures. Therefore, MHI staff needs to perform additional analysis to evaluate the possible faults caused by multiple failures in the non-safety system. MHI staff agreed. (Audit Action Item No. 3-5)

13. [

] This technical report stated that an action is required to address several of the faults identified. The staff requested that MHI staff identify where the resolution to these action items is located in the US-APWR DCD. MHI staff clarified that the resolution to these action items was not included in the US-APWR DCD and agreed to modify this technical report to include the resolution to these action items. (Audit Action Item No. 5-1)

14. The NRC staff examined details that provide a complete list of interfaces between safety and non-safety systems, including both communications and hardwired interfaces. The

NRC staff requested MHI staff to verify that these interfaces are described in the US-APWR DCD. MHI staff stated that these interfaces are described in the US-APWR DCD.

15. Inspections, Tests, Analyses, and Acceptance Criteria (ITAAC) Item 6 in Table 2.5.6-1, "Data Communication Systems Inspections, Tests, Analyses, and Acceptance Criteria," in Tier 1 of the US-APWR DCD states that "Digital comunications independence is achieved by communication processors that are independent of RT and ESF actuation processing functions of the redundant divisions of the PSMS and also between non-safety systems and the PSMS." The NRC staff requested that MHI staff clarify whether the reference to communication processor within this ITAAC is the Control Network I/F module or both the Control Network I/F module and the CPU module. MHI staff clarified that the communication processor referenced includes both the Control Network I/F module and the CPU module. The staff requested that MHI clarify this in the US-APWR DCD. MHI staff agreed. (Audit Action Item No. 4-1)

4.0 CONCLUSION

MELCO's MELTAC platform design as presented in the US-APWR design certification documents was verified through lab demonstrations of key design features and review of un-docketed detail design documents. 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.

The purpose of the audit was to examine and evaluate non-docketed documents that may assist in resolving the OIs, in particular, data communications independence, identified in the US-APWR Chapter 7 SER with OIs. The audit accomplished this objective. Generally, the resolution of the OIs requires MHI to amend the associated RAI responses. MHI agreed to amend their responses to the RAIs as discussed during the audit in order to clarify the responses. During the audit, additional, related, issues were identified which are to be resolved post-audit. These issues are identified in Enclosure 7 as action items. Resolution of these issues will require revisions to the RAI responses, DCD, or other supporting documentation. Closing these new issues will lead to closure of the OIs. The final resolution of the OIs will not occur until the amended RAI responses and revised documents are received and evaluated and the team completes its evaluation of the information obtained during the audit and the resolution of the action items.