November 10, 2014

AUDIT PLAN FOR US-APWR INSTRUMENTATION AND CONTROLS DESIGN

November 17 - 21, 2014

US-APWR DESIGN CERTIFICATION
Mitsubishi Heavy Industries, Ltd.
Docket No. 52-021

Locations: Mitsubishi Heavy Industries, Ltd.
Kobe, Japan

Mitsubishi Electric Corporation
Energy Systems Center
1-1-2, Wadasaki-cho, Hyogo-ku
Kobe, 652-8555, Japan

Purpose:

The purpose of this regulatory audit of the United States - Advanced Pressurized Water Reactor (US-APWR) instrumentation and controls (I&C) design is to examine and evaluate non-docketed documents that may assist in resolving the open items identified in the U.S. Nuclear Regulatory Commission's (NRC's) safety evaluation report (SER) with open items, and other areas associated with data communications independence for the US-APWR Design Control Document (DCD) Chapter 7. In addition, documents related to the MELTAC watchdog timers will be examined which support Mitsubishi Heavy Industries, Ltd. (MHI) response to the Advisory Committee on Reactor Safeguards (ACRS) action item regarding this topic.

Background:

MHI submitted the US-APWR design certification application on December 31, 2007. The NRC staff has been performing a detailed review of this application. The US-APWR DCD, Chapter 7, provides the design details of the I&C systems. A number of referenced technical reports provide supplemental and proprietary information related to the I&C systems design. The staff is in the process of finalizing the SER with no open items for DCD Chapter 7. This audit of the non-docketed I&C design details will be used to verify the staff's findings of reasonable assurance of safety as documented in the SER with no open items.

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(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;

3. 10 CFR Part 50, Appendix A, “General Design Criteria for Nuclear Power Plants,” General Design Criterion (GDC) 1, 2, 4, 10, 13, 16, 19, 20, 21, 22, 23, 24, 25, 28, 29, 33, 34, 35, 38, 41, and 44;

4. 10 CFR 52.47, “Contents of applications; technical information;” and

5. 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.

Scope:

The scope of the regulatory audit is to examine non-docketed details of the US-APWR digital I&C system design that support the staff’s findings of reasonable assurance of safety in the following open items (publicly available request for additional information (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, ML14100A339)).

2. Details of watchdog timers to clarify their operation and independence from MELTAC platform software (RAI 1094-7466, Question 07.01-46 (ML14119A193, ML14119A192)).
3. Details that demonstrate 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, 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, ML14059A164)). In addition, details of the following items related to data communications independence features will be examined:

    a. Details regarding bounding constraints for the operational commands that are allowed from the O-VDU. MUAP-07004, Section E1, Staff Position 1.7 states that the size of the communication message from the non-safety O-VDU is variable and application-dependent based on the number of commands sent by the operator. This is because each data packet can contain multiple commands as shown on Figure 4.3-11 in MUAP-07005. Details that describe the bounding set of control functions allowed by the operational VDU for the US-APWR application to support the failure modes analysis will be examined. In addition, the need and rationale for multiple concurrent commands per data packet will be examined.

b. Rationale that sets the bounding list of predefined and acceptable messages from the O-VDU to safety systems for the US-APWR design. Specifically, the data table with the bounding list of allowable predefined data from the O-VDU should be provided for audit.

c. Details regarding how the priority logic that ensures functional independence between the O-VDU and the safety system is validated. MUAP-07004, Section 5.1.13 discusses the priority logic scheme for actuation, lock, and bypass signals from the safety I&C system, the O-VDU, and the diverse actuation system (DAS). This priority logic scheme is implemented at three priority levels. Details that demonstrate how the priority logic scheme is validated for all safety functions will be examined. In addition, details on the manual permissive logic will be examined that allows the operational VDU to bypass the safety function, with specific descriptions how the signal for the permissive is generated (e.g. default settings, signal latching, set and reset block configuration), including the justification for why the capability to bypass safety functions using the O-VDU enhances the performance of the safety function given that the operator needs to set the permissive on the safety VDU. From a human factors perspective, it appears that the operator would need to operate two screens to accomplish this function.

d. Details regarding how the lock function operates. Specifically, design information regarding how the safety VDU generates the permissive for allowing the O-VDU to lock out a component or function will be examined. Information regarding how a component is unlocked after the safety VDU removes the permissive and regarding the relationship between the lock function and technical specifications will be examined.

e. Details that 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.

f. Details regarding the detection and mitigation features of communications errors in the MELTAC platfrom. The MELTAC Platform ISG-04 Conformance Analysis Technical Report (MUAP-13018 (R0)), Section 3, Analysis Results states: "…if detection and mitigation were done by software, its implementation was confirmed through verification of specification document and source code." Documentation supporting these confirmations will be examined, including portions of the source code that the verification of these features are based on. Technical experts to explain how the source code effectively implements these features will be interviewed.

g. Details regarding the operation of the hardware arbitration interlock. Section 3 of MUAP-13018, 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. Details of the hardware arbitration

interlock that prevents modules from reading and writing simultaneously and its operation will be examined.

h. Details that support the claims in Technical Report MUAP-7004, Table G.2-2, "Failure Modes and Effects Analysis for ESF Actuation in PSMS" (Sheet 25), regarding spurious signals from the O-VDU. Specifically, details regarding how the safety system priority logic addresses non-concurrent demands between the safety system and the O-VDU will be examined.

i. Details that support and verify the design features regarding the detection and mitigation strategies for identified failures in the Communication Error Patterns (MUAP-07005, Table H.1). For example, information on how the queue index is an effective feature to address sequence errors in incoming messages from the O-VDU will be examined. Technical experts to describe the operation of these features will be interviewed. In addition, MUAP-13018 contains a table regarding how communication architecture and faults detectability are addressed for each communications fault (WNET). Information that shows how communication failures are addressed for those with an action required identified in the evaluation table will be examined.

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

Audit Team:

Members of the audit team were selected based on their detailed knowledge of the US-APWR design and their thorough familiarity with the US-APWR DCD and supporting technical reports. All of the audit team members are currently involved in the review of the US-APWR design certification application.

- Dinesh Taneja, Senior Electronics Engineer, NRO/DE/ICE2, is a qualified technical reviewer and will lead the NRC audit team.

- Deanna Zhang, Senior Electronics Engineer, NRO/DE/ICE1, is a qualified technical reviewer and will conduct the communications independence portion of the audit.

- Ian Jung, Branch Chief of the Instrumentation, Controls, and Electronics Engineering Branch 2, NRO/DE/ICE2, is the management representative.

- William Ward, Senior Project Manager, NRO/DNRL, is the lead project manager for the US-APWR review, including Chapter 7 and digital I&C systems. He will provide general support and assist with coordination and documentation of the audit.

Information and Other Material Necessary for the Regulatory Audit:

Non-docketed US-APWR digital I&C design information that supports the docketed information provided in the referenced documents. MELTAC platform development and implementation test reports.

Logistics:

The audit is planned for November 17 - 21, 2014, at MHI located in Kobe, Japan. The audit team members will conduct an exit briefing with MHI on the last day.

Special Requests:

Appropriate handling and protection of proprietary information shall be acknowledged and observed throughout the audit.

Schedule and Deliverable:

The NRC may request an ad-hoc extension of the audit if findings during the ongoing audit reveal the need for additional time. Such an extension will be requested before the audit is adjourned on November 21, 2014, by the NRC staff responsible for the audit.

An audit report will be generated within ninety days after completion of the audit. The objective of this audit is to verify that the non-docketed details of the US-APWR digital I&C system design, support the staff's findings of reasonable assurance of safety as documented in the SER with no open items and other areas associated with data communications independence for the US-APWR DCD Chapter 7. The audit outcome will be used to identify any additional information to be submitted for making regulatory decisions.

References:

1. Design Control Document for the US-APWR, Chapters 1-18.

2. MUAP-07004, Safety I&C System Description and Design Process, Revision 8.

3. MUAP-07005, Safety System Digital Platform -MELTAC-, Revision 9.

4. MUAP-07017, Software Program Manual, Revision 5.

5. MUAP-09020, Functional Assignment Analysis for Safety Logic System, Revision 2.

6. MUAP-09021, Response Time of Safety I&C System, Revision 3.

7. MUAP-09022, Instrument Setpoint Methodology, Revision 3.

8. MUAP-13018, MELTAC Platform ISG-04 Conformance Analysis, Revision 0.

9. Letter from ACRS [Ch 7 Full Committee], dated December 24, 2013 (ML13365A063).

10. Response letter to ACRS, dated February 24, 2014 (ML13365A056).

11. RAIs and responses

    a. RAI 1091-7447, MHI response dated April 9, 2014 (ML14100A339, ML14100A340).

    b. RAI 1094-7466, MHI response dated April 25, 2014 (ML14119A193, ML14119A192).

    c. RAI 995-7024, MHI response dated November 11, 2013 (ML13324A960).

    d. RAI 568-4588, MHI response dated September 11, 2013 (ML13270A236).

    e. RAI 1093-7366, MHI response dated April 23, 2014 (ML14118A169, ML14118A170).

    f. RAI 1076-7368, MHI response dated February 25, 2014 (ML14059A163, ML14059A164).

Docket No. 52-021

cc: See next page

11. RAIs and responses

    a. RAI 1091-7447, MHI response dated April 9, 2014 (ML14100A339, ML14100A340).

    b. RAI 1094-7466, MHI response dated April 25, 2014 (ML14119A193, ML14119A192).

    c. RAI 995-7024, MHI response dated November 11, 2013 (ML13324A960).

    d. RAI 568-4588, MHI response dated September 11, 2013 (ML13270A236).

    e. RAI 1093-7366, MHI response dated April 23, 2014 (ML14118A169, ML14118A170).

    f. RAI 1076-7368, MHI response dated February 25, 2014 (ML14059A163, ML14059A164).

Docket No. 52-021

cc: See next page

DISTRIBUTION:

PUBLIC	SLee, NRO	RidsNroLACSmith	RidsOgcMailCenter
LB2 R/F	DTaneja, NRO	RBeacom, NRO	RidsAcrsAcnwMailCenter
D081	IJung, NRO	DSantos, NRO	RidsNroDnrlLB2
WWard, NRO	DZhang, NRO	TJackson, NRO	CMurphy, NRO

ADAMS Accession No.: ML14310A834 **NRO-002**

OFFICE	DNRL/LB2: PM	DNRL/LB2: LA	DNRL/LB2: PM
NAME	WWard	CMurphy	WWard
DATE	11/07/2014	11/10/2014	11/10/2014

OFFICIAL RECORD COPY

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

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
acpasswater@aol.com (Al Passwater)
APH@NEI.org (Adrian Heymer)
atsushi_kumaki@mhi.co.jp (Atsushi Kumaki)
awc@nei.org (Anne W. Cottingham)
bgattoni@roe.com (William (Bill) Gattoni))
Carl.Corbin@luminant.com (Carol Corbin)
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)
donald.woodlan@luminant.com (Donald Woodlan)
eliza.seedcoalition@gmail.com (Elza Brown)
erg-xl@cox.net (Eddie R. Grant)
ewallace@nuscalepower.com (Ed Wallace)
Fred.Madden@luminant.com (Fred Madden)
George_Stramback@Charter.net (George Stramback)
james1.beard@ge.com (James Beard)
jerald.head@ge.com (Jerald G. Head)
Joseph_Hegner@dom.com (Joseph Hegner)
joseph_tapia@mnes-us.com (Joseph Tapia)
jrappe@nuscalepower.com (Jodi Rappe)
jrund@morganlewis.com (Jonathan Rund)
karlg@att.net (Karl Gross)
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)
maria.webb@pillsburylaw.com (Maria Webb)
mark.a.giles@dom.com (Mark Giles)
media@nei.org (Scott Peterson)
MSF@nei.org (Marvin Fertel)
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)
rdbirdjr@gmail.com (Bobby Bird)
RJB@NEI.org (Russell Bell)
ryan_sprengel@mnes-us.com (Ryan Sprengel)

DC Mitsubishi - US APWR Mailing List

sabinski@suddenlink.net (Steve A. Bennett)
sfrantz@morganlewis.com (Stephen P. Frantz)
stephan.moen@ge.com (Stephan Moen)
takayuki_mori@mhi.co.jp (Takayuki Mori)
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)