November 22, 2011

# AUDIT PLAN FOR DIGITAL INSTRUMENTATION AND CONTROLS DESIGN US-APWR DESIGN CERTIFICATION DOCUMENT CHAPTER 7

**December 12 - 16, 2011**

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

Location: 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 US-APWR digital instrumentation and controls (I&C) design is to examine and evaluate non-docketed details of the digital I&C systems, including development processes that support the staff's reasonable assurance of safety findings in the following areas:

1. Digital data communication independence:
   a. between safety and non-safety systems
   b. inter-divisional communication within safety systems

2. Deterministic performance of digital I&C systems

3. Implementation of watchdog timers

4. Digital I&C system application software development process

5. Integration of MELTAC basic software into the US-APWR application software for safety I&C systems

6. Follow-up on March 2009 US-APWR digital I&C system regulatory audit findings (ML093240406)

Additionally, the audit may be observed by other regulators such as the Japan Nuclear Energy Safety Organization (JNES). These observations foster the sharing of international experiences with digital I&C implementation, the construction of new reactors, and oversight of vendors consistent with the objectives of the Multinational Design Evaluation Program (MDEP).

Background:

Mitsubishi Heavy Industries, Ltd. (MHI) submitted the United States – Advanced Pressurized Water Reactor (US-APWR) standard design certification application on December 31, 2007. The staff of the U.S. Nuclear Regulatory Commission (NRC) is currently performing a detailed review of this application. The US-APWR Design Control Document (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 digital I&C systems design. The staff is in the process of finalizing the safety evaluation report (SER) with 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 open items.

Regulatory Audit 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. 10 Code of Federal Regulations (CFR) 50.55a(a)(1), "Quality Standards,"

2. 10 CFR 50.55a(h), "Protection and Safety Systems," which requires compliance with 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 52.79, "Contents of application; technical information in final safety analysis report,"

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.

Regulatory Audit Scope:

The primary focus of this audit will be in the areas that cannot be readily audited at the Mitsubishi Nuclear Energy Systems (MNES) offices located in the United States. The scope of the regulatory audit is to examine and evaluate 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 areas:

1. 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,
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,
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,
f. Perform thread audit of supporting documents referenced by Appendix E of 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,

2. 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,

3. 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 ,

4. 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,

5. 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,

6. Demonstration of Memory Integrity Check using Engineering Tool,

7. Follow-up on March 2009 US-APWR digital I&C system regulatory audit findings (ML093240406).

In addition, the audit team is planning to visit a Japanese nuclear power plant with MELTAC digital I&C platform that is similar in design to one being proposed for the US-APWR.

<u>Information and Other Material Necessary for the Regulatory Audit</u>:

Non-docketed US-APWR digital I&C design information that supports the docketed information provided in the referenced documents. MELTAC digital I&C system components in a laboratory environment for demonstration of the key digital I&C design features, such as, data communication independence, deterministic performance, fault detection and alarming schemes, etc.

Team Assignments:

Members of the audit team were selected based on their detailed knowledge of the US-APWR digital I&C system design and their thorough familiarity with the US-APWR DCD and supporting technical reports. This audit team is qualified and capable of adequately evaluating the critical aspects of this complex digital I&C system design and the US-APWR application software development process. All of the audit team members are currently involved in the review of the US-APWR design certification application focusing of the I&C system design.

**Dinesh Taneja**, Senior Electronics Engineer, NRO/DE, is a qualified technical reviewer and will lead the NRC audit team at MHI, Kobe, Japan. Mr. Taneja will also examine deterministic performance of the MELTAC controllers, implementation of watchdog timers, and will support the other audit areas as necessary.

**Ian Jung**, Branch Chief of the Instrumentation and Control Branch 2, NRO/DE, is the management representative and will interact with foreign regulators to gain a better understanding of the scope and practices used by other regulators such as the JNES to oversee vendors such as MHI providing nuclear power plant designs to the Japanese nuclear market. He will also engage the JNES on the plan for making use of the Multinational Design Evaluation Program Design-Specific Digital I&C Working Group Generic Common Positions as applied to the US-APWR in Japan. With his expertise on I&C systems and NRC regulatory knowledge, he will also provide support and insights to the team members on specific audit items.

**Khoi Nguyen**, Electronics Engineer, NRO/DE, is the lead technical reviewer of the US-APWR design certification application with respect to data communications system, which is one of the safety-critical design aspects for the proposed digital I&C design. Mr. Nguyen will participate in the audit to confirm the details of the data communications system design used to demonstrate the independence requirements such as the details on how communications both between redundant divisions and between safety and nonsafety divisions are implemented.

**Tung Truong**, Electronics Engineer, NRO/DE, is a technical specialist participating on the team audit at MHI, Kobe, Japan. Mr. Truong will audit design, systems integration, configuration management, and testing activities, including verification and validation, associated with the US-APWR Software Development Lifecycle, and will support other audit areas as necessary.

**Royce Beacom**, Electronics Engineer, NRO/DE, is a technical specialist participating on the team audit at MHI, Kobe, Japan. Mr. Beacom will follow the integration of MELTAC basic software into the US-APWR application software for safety I&C systems. He will provide insights and the necessary follow-up of the previous US-APWR digital I&C regulatory audit findings as well as supporting other audit areas as necessary.

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

Logistics:

The audit is planned for the week of December 12 – 16, 2011, at Mitsubishi Electric Corporation Energy Systems Center located in Kobe, Japan. Four members (Jung, Taneja, Beacom, Truong) of the audit team will be in Kobe, Japan for the week of December 4 – 9 to support a vendor inspection of MELCO, supplier of the MELTAC platform to the US-APWR design center. They will stay over the second week for the audit and are joined by the two additional team members (Nguyen, Ward). The inspection and audit have been planned together, but will be documented separately.

Special Requests:

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

Deliverables:

The NRC staff will conduct the US-APWR digital I&C design audit during the week of December 12 – 16, 2011 in Kobe, Japan. The NRC may request an ad-hoc extension of the audit to be continued at the applicant's US facilities, if findings during the ongoing audit reveal the need for additional time. Such an extension will be requested before the audit is adjourned on December 16, 2011, by the NRC staff responsible for the audit.

An audit report will be generated after completion of the audit. Objective of this audit is to verify that 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 Safety Evaluation Report with Open Items for the US-APWR Design Certification Document Chapter 7, Instrumentation and Controls. The audit outcome will be used to identify any additional information to be submitted for making regulatory decisions. If required, this audit will also assist the NRC staff in the preparation and issuance of further Requests for Additional Information for the licensing review of the digital I&C design submitted as a part of the US-APWR Design Certification Application.

References:


1. US-APWR DCD, Revision 3.

2. MUAP-07004-P, "Safety I&C System Description and Design Process," Revision 7, May 2011.

3. MUAP-07005-P, "Safety System Digital Platform –MELTAC-," Revision 8, July 2011.

4. MUAP-07017-P, "US-APWR Software Program Manual," Revision 4, May 2011.

5. MUAP-09021-P, "Response Time of Safety I&C System," Revision 2, April 2011.

6. JEXU-1012-1132, “MELTAC Platform Basic Software Program Manual,” Revision 3, January 2011

7. PQD-HD-19005, “The Quality Assurance Program (QAP) Description for Design Certification of the US-APWR,” Revision 4, April 2011

Docket No. 52-021

cc: See next page

5. MUAP-09021-P, “Response Time of Safety I&C System,” Revision 2, April 2011.

6. JEXU-1012-1132, “MELTAC Platform Basic Software Program Manual,” Revision 3, January 2011

7. PQD-HD-19005, “The Quality Assurance Program (QAP) Description for Design Certification of the US-APWR,” Revision 4, April 2011

Docket No. 52-021

cc: See next page

DISTRIBUTION:

| | | | |
|---|---|---|---|
| PUBLIC | JCiocco, NRO | RidsNroLACSmith | RidsOgcMailCenter |
| NMIP R/F | DTaneja, NRO | RBeacom, NRO | RidsAcrsAcnwMailCenter |
| D081 | IJung, NRO | TTruong, NRO | RidsNroDnrlNmip |
| WWard, NRO | KNguyen, NRO | TJackson, NRO | RidsNroLAKGoldstein |

**ADAMS Accession No.:ML113220196** **NRC-001**

| **OFFICE** | DNRL/NMIP: PM | DNRL/NMIP: LA | DNRL/NMIP: PM | DNRL/NMIP: BC |
|---|---|---|---|---|
| **NAME** | WWard(Paul Kallan for ) | KGoldstein for CSmith | JCiocco | HHamzehee |
| **DATE** | 11/22/2011 | 11/22/2011 | 11/22/2011 | 11/22/2011 |

**OFFICIAL RECORD COPY**

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. Tony Robinson
AREVA NP, Inc.
3315 Old Forest Road
Lynchburg, VA 24501

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

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)
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)
ewallace@nuscalepower.com (Ed Wallace)
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)
jrappe@nuscalepower.com (Jodi Rappe)
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.a.giles@dom.com (Mark Giles)
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)
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)
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)