February 10, 2012

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

February 13 - 15, 2012

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

Location: Mitsubishi Nuclear Energy Systems, Inc.
1001 19th Street North
7th Floor
Arlington, VA 22209

Purpose:

The purpose of this regulatory audit of the United States – Advanced Pressurized Water Reactor (US-APWR) digital instrumentation and controls (I&C) design is to examine and evaluate non-docketed documents used for developing the list of Post Accident Monitoring (PAM) instrumentation for Type A, B, and C variables contained in DCD Chapters 7 and 16. In addition, staff will examine existing MELTAC test reports that support the staff's reasonable assurance of safety findings in the following key digital I&C design areas:

1. Redundancy;
2. Physical, electrical, and data communication independence;
3. Deterministic performance;
4. Diversity;
5. Simplicity.

Background:

Mitsubishi Heavy Industries, Ltd. (MHI) submitted the 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. Included in the staff's instrumentation evaluation is the adequacy of the applicant's alternative method for categorizing variables associated with PAM instrumentation, based on the category definitions of Regulatory Guide (RG) 1.97, Revision 4, and the selection of instrumentation for Type A, B, and C variables for inclusion in the PAM limiting condition for operation's list of PAM instrumentation functions in the generic technical specifications.

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, Appendix 7.1-A, and Section 16.0. The key regulations are identified below:

1. 10 Code of Federal Regulations (CFR) 50.55a(a), "Quality Standards, ASME Codes and IEEE standards, and alternatives";

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 52.47, "Contents of application; technical information";

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;

6. 10 CFR 50.36, "Technical specifications."

Regulatory Audit Scope:

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. A review of un-docketed documentation will be conducted to verify adequacy of the bounding list of PAM variables identified in Table 7.5-3 of the US-APWR DCD. This list of PAM variables was developed using performance-based criteria of RG 1.97 Rev. 4.

The DCD refers to the US-APWR Functional Restoration Guidelines (FRGs), which establish redefined function-related restoration strategies for responding to emergency transients. The focus of this audit will be the US-APWR FRGs and associated documents as they relate to development of the bounding PAM variables list.

2. The MELTAC platform has been implemented in existing Japanese nuclear power plants for various digital I&C applications and is now being designed and developed for the US-APWR application. In support of these MELTAC implementation and development activities, MELCO has conducted a number of tests. The objective of this audit is to review these un-docketed test reports to confirm the staff's findings of reasonable assurance of safety related to key digital I&C design features, namely; 1) redundancy; 2) independence; 3) determinism; 4) diversity; and 5) simplicity.

3. The review of un-docketed test reports will also focus on confirming 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. All basic and application software of the protection and safety monitoring system (PSMS) is stored in nonvolatile devices. These devices cannot be altered without withdrawal from the chassis in the PSMS. Safety software cannot be altered online;

   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. Communication failures do not impact reactor protection system (RPS), engineered safety features (ESF), and safety logic system (SLS) functions. The desired reactor trip and ESF logics are maintained in the event of processing failures; communication failures, or bypass;

   d. Safety signals do not depend on bypass status signals;

   e. Non-safety signals are rejected upon the presence of a safety signal;

   f. The voting logic within each safety train ensures that a failure that results in loss of data from any one train does not affect the safety functions;

   g. Only predefined data are processed;

   h. The safety function processors of the PSMS perform no communication handshaking and do not accept interrupts from outside their own safety trains;

   i. The logic within power interface module (PIF) gives priority to the predefined safe state of the component;

   j. Multidivisional safety visual display units (VDUs) have no control capability.

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.

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/ICB, is a qualified technical reviewer and will lead the NRC audit team at MNES Arlington, VA.

Ian Jung, Branch Chief of the Instrumentation and Control Branch, NRO/DE/ICB, is the management representative.

Hulbert Li, Senior Electronics Engineer, NRO/DE/ICB, is a technical specialist reviewing the US-APWR design certification application digital instrumentation and controls.

Joe Ashcraft, Electronics Engineer, NRO/DE/ICB, is a technical specialist reviewing the US-APWR design certification application digital instrumentation and controls.

Khoi Nguyen, Electronics Engineer, NRO/DE/ICB, is the lead technical reviewer of the US-APWR design certification application with respect to the data communications system.

Erick Martinez, Electronics Engineer, NRO/DE/ICB, is a technical specialist reviewing the US-APWR design certification application diverse actuation system.

Paul Pieringer, Reactor Operations Engineer, NRO/DCIP/COLP, is the lead technical specialist reviewing the human factors engineering and human-system interface design portions of the US-APWR design certification application.

Craig Harbuck, Senior Reactor Engineer, NRO/DSRA/BPTS, is a technical specialist reviewing the US-APWR design certification application generic technical specifications.

Michelle Hayes, Reactor Systems Engineer, NRO/DSRA/SRSB, is a technical specialist reviewing the US-APWR design certification application reactor systems and severe accident analysis.

William Ward, Senior Project Manager, NRO/DNRL/LB2, is the project manager for the US-APWR Chapter 7 and digital I&C systems review.

Logistics:

The audit is planned for the three days of February 13 - 15, 2012, at Mitsubishi Nuclear Energy Systems, Inc. located in Arlington, Virginia. Participating individuals will meet at the audit location. The audit team members will conduct an exit briefing with MHI and MNES on the last day.

Special Requests:

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

The NRC staff will conduct the US-APWR digital I&C design audit during the week of February 13 - 15, 2012 in Arlington, Virginia. 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 February 15, 2012, by the NRC staff responsible for the audit.

Deliverables:

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

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	CSmith, NRO

ADAMS Accession No.: ML120330634 **NRO-002**

OFFICE	DNRL/NMIP: PM	DNRL/NMIP: LA	DNRL/NMIP: PM	DNRL/NMIP: BC
NAME	WWard	CSmith **(R. Butler for)**	JCiocco **(W. Ward for)**	HHamzehee **(D. Galvin for)**
DATE	02/2/2012	02/10/2012	02/10/2012	02/10/2012

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

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))
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)
hiroki_nishio@mhi.co.jp (Hiroki Nishio)
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)
masahiko_kaneda@mhi.co.jp (Masahiko Kaneda)
masanori_onozuka@mnes-us.com (Masanori Onozuka)
masayuki_kambara@mhi.co.jp (Masayuki Kambara)
matias.travieso-diaz@pillsburylaw.com (Matias Travieso-Diaz)
media@nei.org (Scott Peterson)
mike_moran@fpl.com (Mike Moran)
MSF@nei.org (Marvin Fertel)

mutsumi_ishida@mnes-us.com (Mutsumi Ishida)
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)
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)