UNITED STATES
NUCLEAR REGULATORY COMMISSION
ADVISORY COMMITTEE ON REACTOR SAFEGUARDS
WASHINGTON, DC 20555 - 0001

December 18, 2012

Mr. R.W. Borchardt
Executive Director for Operations
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

SUBJECT: DRAFT DESIGN SPECIFIC REVIEW STANDARD FOR mPOWER iPWR CHAPTER 7 INSTRUMENTATION AND CONTROL SYSTEMS

Dear Mr. Borchardt:

During the 600th meeting of the Advisory Committee on Reactor Safeguards, December 6-8, 2012, we reviewed the Draft Design Specific Review Standard (DSRS) for the mPower integral pressurized water reactor (iPWR), Chapter 7, Instrumentation and Control (I&C) Systems. Our Digital Instrumentation & Control (DI&C) Systems Subcommittee also reviewed this matter during a meeting on November 16, 2012. During these reviews, we had the benefit of discussions with representatives of the NRC staff and comments from industry representatives. We also had the benefit of the documents referenced.

RECOMMENDATIONS AND CONCLUSIONS

1. The Draft Design Specific Review Standard (DSRS) for mPower iPWR Chapter 7 Instrumentation and Control (I&C) Systems should be issued for industry and public comment.

2. The mPower I&C DSRS provides a review standard that is likely to be applicable to large reactor designs, as well as other small modular reactors (SMRs).

3. Section 7.0, Instrumentation and Controls - Introduction and Overview of Review Process, Acceptance Criteria and Review Process, and Section 7.2.9 - Control of Access Review, should be revised as indicated in the discussion.

4. The diagrams of the overall architecture, as called for in Appendix B, Item 3, should be expanded to provide examples of the desired level of detail as was done for defense-in-depth in Item 4.

BACKGROUND

Licensing reviews of I&C, and digital-based I&C systems in particular, have been a significant challenge from the perspective of both safety demonstration and schedule/resources for all design centers for new large light water reactors. Industry has consistently expressed licensing certainty of I&C to be one of their highest priorities for new reactors. As a result, the Office of New Reactors, Division of Advanced Reactors and Rulemaking has begun to develop DSRS for the iPWR designs starting with mPower. This draft presented by the staff will be issued for interim use and comment by the industry and the public with a goal of completing and issuing the mPower DSRS by the end of 2013.

DISCUSSION

The goal of the development of the DSRS was to apply the lessons learned during recent reviews of digital I&C systems and develop a review standard for the mPower SMR design that:

- Enhances the safety focus of staff reviews, and
- Improves the staff's review efficiency.

The staff established the following framework and guidelines for the DSRS:

- Reorganize the review guidance to separate Fundamental Design Principles from specific system requirements
- Provide guidance on Fundamental Design Principles at the system level
- Remove redundant and non-applicable information
- Eliminate the use of Design Acceptance Criteria (DAC)
- Introduce the concepts of Simplicity in design and Hazard Analysis into the review
- Ensure adequate coverage of regulatory requirements and applicable guidance

The use of the above framework resulted in a Chapter 7 organization consisting of Section 7.0 Overview, 7.1 Fundamental Design Principles, 7.2 System Characteristics, and three Appendices A, B, and C to address Hazard Analysis, I&C Architecture, and Simplicity, respectively. This organization accomplishes the following:

- Section 7.0 provides the reviewer with an overview of the process and a table, which includes all I&C safety system regulatory requirements, and maps them to the applicable DSRS section.

- Section 7.1 focuses the review guidance on how the applicant has addressed the Fundamental Design Principles of Independence, Redundancy, Determinism, and Diversity and Defense-in-Depth (D3), plus Simplicity which is discussed in Appendix C.

- Section 7.2 focuses the review guidance on the system characteristics and associated regulatory requirements for protection systems which includes the reactor trip system (RTS) and engineered safety features actuation system (ESFAS).

- Appendices A, B, and C address unique subjects that the applicant should address in its application.

The DSRS essentially reorganizes the existing standard review plan (SRP) from a bottom-up system-by-system approach, where regulatory requirements and principles are repeated multiple times, to a top-down approach which focuses on ensuring the basic architecture of the I&C systems meets the Fundamental Design Principles. Then design characteristics and regulatory requirements are assessed within each system. In addition, regulations not applicable to the new reactor plant I&C designs are deleted. As a result, the DSRS significantly simplifies understanding of the review goals and should streamline the review process.

Although the DSRS was developed as a pilot initiative for the mPower design, it appears to us that it may be applicable to large reactor designs as well as other SMRs.

The DSRS focus on the Fundamental Design Principles and functional design characteristics should permit applicants to provide information adequate to allow the staff to make an I&C safety licensing determination without requiring them to make detailed-hardware specifications that could soon become obsolete. This may well minimize or eliminate DAC.

To emphasize this point, the guidance should state that the level of detail necessary for this review should be sufficient to ensure that enough information on the functional I&C System Architecture is provided to establish a satisfactory and complete licensing/safety basis at the time of license approval.

Section 7.2.9, Control of Access, Identification, and Repair, Sub-section Control of Access states that the reviewer should evaluate how access to I&C safety systems will be controlled and how the requirements of Section 5.9 of IEEE 603-1991 are satisfied. Section 5.9 states that "administrative controls shall be supported by provisions within the safety system, by provision in the generating station design, or by a combination of both."

For digital-based systems, data may be transmitted from the systems via a network bus to the Main Control Room (MCR), the Technical Support Center (TSC), and the Emergency Support Center (ESC), and in some cases is shown as being transmitted through a firewall to a corporate network with access to the internet. These types of architecture configurations that have access to the internet can compromise control of access, thus possibly compromising the safety system information being sent to or control signals emanating from the MCR, TSC, and ESC.

Item 2, under the Control of Access review section, should be expanded to require the reviewer to assess architecture and the firewall to ensure that it is a hardware-based, one-way firewall with no software involved in either its operation or setup such that no access is possible to plant systems, the control station, or support centers via this connection, if it is present. This assures that all interface access with the plant, MCR, TSC, and ESC or other support facilities from outside sources can be controlled by administrative controls under the supervision of licensed operators.

Appendix B addresses review requirements for the I&C System Architecture. Page 2 includes a list of information the staff should review and that the applicant should include. Item 3 states "Diagrams of the overall architecture." This statement is at too high of a level and does not provide the level of detail the reviewer should expect to see to reach a safety finding. Item 3 should be expanded similar to what was done for Item 4, Defense-in-Depth, to give examples of the desired level of detail. For example (not inclusive), the list should include channel/division functional block diagrams showing sensor-to-control device actuation, including intermediate processing of data for producing a reactor trip, followed by the voting unit processing, and then outputs to the actuators. For software-based digital systems, the functional diagrams should illustrate how each channel/division will produce a trip if the data processing and voting units lockup. The diagrams should also show how the function that is used to ensure a trip (for reactor trip functions) or an alarm in the MCR and other appropriate locations (for fail-as-is systems such as the ESFAS) on lockup, is completely independent of the main processing path, is not software-based and is independent of any external software-based systems inputs.

During the November 16, 2012 Subcommittee meeting, there were substantive and productive discussions with and observations and suggestions provided to the staff to clarify and improve numerous sections of the DSRS. These suggestions will be evaluated by the staff along with the industry and public comments received during the comment period.

The Draft DSRS for the mPower iPWR, Chapter 7, I&C Systems should be issued for industry and public comment. We look forward to reviewing a revised version of the DSRS after resolution of the public comments.

We commend the staff for their efforts in developing this innovative approach to revising the SRP for future I&C designs and being proactive at incorporating lessons learned from recent new reactor DI&C design certifications.

Sincerely,

/RA/

J. Sam Armijo
Chairman

REFERENCES:

1. Design-Specific Review Standard for mPower, iPWR Design, Section 7.0 "Instrumentation and Controls – Introduction and Overview of Review Process," dated September 19, 2012 (Draft for Comment)(ML12108A272)

2. Design-Specific Review Standard for mPower, iPWR Design, Section 7.1 "Fundamental Design Principles," Revision 1, dated September 19, 2012 (Draft for Comment) (ML12236A232)

3. Design-Specific Review Standard for mPower, iPWR Design, Section 7.2 "System Characteristics," dated September 19, 2012 (Draft for Comment) (ML12179A151)

4. Design-Specific Review Standard for mPower, iPWR Design, Section 7.0 "Instrumentation and Controls, Appendix A - Hazard Analysis," dated September 19, 2012 (Draft for Comment) (ML12249A448)

5. Design-Specific Review Standard for mPower, iPWR Design, Section 7.0 "Instrumentation and Controls, Appendix B – I&C System Architecture," Revision 1, dated September 19, 2012 (Draft for Comment) (ML12255A178)

6. Design-Specific Review Standard for mPower, iPWR Design, Section 7.0 "Instrumentation and Controls, Appendix C - Simplicity," Revision 1 (Draft for Comment) (ML12255A178)

7. Design-Specific Review Standard for mPower, iPWR Design, Section 7.0 "Instrumentation and Controls, Appendix D - References," Revision 1(Draft for Comment) (ML12255A192)

8. Regulatory Guide 1.152, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," Rev. 3, 07/31/2011 (ML102870022)

4 Design-Specific Review Standard for mPower, iPWR Design, Section 7.0 "Instrumentation and Controls, Appendix A - Hazard Analysis," dated September 19, 2012 (Draft for Comment) (ML12249A448)

5. Design-Specific Review Standard for mPower, iPWR Design, Section 7.0 "Instrumentation and Controls, Appendix B – I&C System Architecture," Revision 1, dated September 19, 2012 (Draft for Comment) (ML12255A178)

6. Design-Specific Review Standard for mPower, iPWR Design, Section 7.0 "Instrumentation and Controls, Appendix C - Simplicity," Revision 1 (Draft for Comment) (ML12255A178)

7. Design-Specific Review Standard for mPower, iPWR Design, Section 7.0 "Instrumentation and Controls, Appendix D - References," Revision 1(Draft for Comment) (ML12255A192)

8. Regulatory Guide 1.152, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," Rev. 3, 07/31/2011 (ML102870022)

Accession No: **ML12346A353** **Publicly Available** **Y** **Sensitive** **N**
Viewing Rights: ☒ NRC Users or ☐ ACRS Only or ☐ See Restricted distribution

OFFICE	ACRS	SUNSI Review	ACRS	ACRS	ACRS
NAME	CAntonescu	CAntonescu	HGonzalez	EMHackett	EMH for JSA
DATE	12/18/12	12/18/12	12/20/12	12/20/12	12/20/12

OFFICIAL RECORD COPY