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

March 19, 2013

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 602nd meeting of the Advisory Committee on Reactor Safeguards (ACRS), March 7, 2013, we reviewed your letter dated February 6, 2013, regarding disposition of the ACRS recommendations contained in our letter of December 18, 2012, on the draft Design Specific Review Standard (DSRS) for mPower iPWR Chapter 7, Instrumentation and Control Systems.

RECOMMENDATION AND CONCLUSION

1. The staff's disposition of the recommendations in our December 18, 2012 letter is satisfactory except for an essential element of recommendation 3.

2. The staff should incorporate the revision to the mPower DSRS Chapter 7, Section 7.2.9 Item 2 discussed in our December 18, 2012 letter.

DISCUSSION

In digital-based I&C systems, data may be transmitted from the plant systems via a network bus to the Main Control Room (MCR), the Technical Support Center (TSC), and the Emergency Support Center (ESC). In some cases, this bus is connected through a firewall to a corporate network with communication to the internet. This configuration can compromise control of access. This could make safety system information being sent to the MCR, TSC, and ESC or control signals emanating from the MCR vulnerable to unauthorized access or corruption. We recommended that the Control of Access review section of the DSRS be expanded to require the reviewer to assess the architecture and the firewall to ensure that it is a hardware-based, one-way firewall. No software should be involved in either its operation or setup. These design features and architecture are necessary to assure that all interface access with the plant, MCR, TSC, and ESC or other support facilities from outside sources can be controlled administratively.

We have identified three points in your response with which we disagree.

First, IEEE 603-1991, Section 5.9, Control of Access, states: "The design shall permit the administrative control of access to safety system equipment. These administrative controls shall be supported by provisions within the safety systems, by provision in the generating station design, or by a combination thereof." In other words, Section 5.9 not only addresses administrative controls but also a design and architecture that support the application of administrative controls.

Second, our concern was not about communication links between the MCR, TSC, and ESC but communication from a common network bus which passes plant data from safety systems to these three locations and that also passes plant control signals back to safety systems. The network bus itself is a critical link between the safety systems and the locations noted above.

Third, control of access to the network bus is not controlled by the cyber security rules in 10 CFR Part 73.54, but by IEEE 603-1991, Section 5.9 as part of the overall licensed design certification. IEEE Standard 603 is the primary reference in the licensing basis, as required by 10 CFR 50.55a(h), Protection and Safety Systems, for the design of I&C systems.

The staff should incorporate the revision to the mPower DSRS Chapter 7, Section 7.2.9 Item 2 discussed in our December 18, 2012 letter.

Sincerely,

/RA/

J. Sam Armijo
Chairman

REFERENCES:

1. EDO letter, dated February 6, 2013, "Response to Advisory Committee on Reactor Safeguards Recommendations on Chapter 7, 'Instrumentation and Controls,' of the Draft Design Specific Review Standard for the mPower ™ Integral Pressurized-Water Reactor" (ML13004A385)

2. ACRS letter, dated December 18, 2012, "Draft Design Specific Review Standard for mPower iPWR Chapter 7 Instrumentation and Control" (ML12346A252)

3. 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)

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

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

6. 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)

7. 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)

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

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

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

11. IEEE Std. 603 1991, “Criteria for Safety Systems for Nuclear Power Generating Stations,” and the correction sheet dated January 30, 1995, Institute of Electrical and Electronics Engineers, Piscataway, NJ

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

6. 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)

7. 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)

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

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

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

11. IEEE Std. 603 1991, "Criteria for Safety Systems for Nuclear Power Generating Stations," and the correction sheet dated January 30, 1995, Institute of Electrical and Electronics Engineers, Piscataway, NJ

Accession No: **ML13067A273** **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	CSantos	EMHackett	EMH for JSA
DATE	03/20/13	03/20/13	03/20/13	03/21/13	03/21/13

OFFICIAL RECORD COPY