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

August 6, 2014

Mr. Mark A. Satorius
Executive Director for Operations
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

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

Dear Mr. Satorius:

During the 616th meeting of the Advisory Committee on Reactor Safeguards, July 9-11, 2014, we completed our review of Chapter 7, Instrumentation and Control Systems, of the Draft Final Design Specific Review Standard (DSRS) for the mPower integral pressurized water reactor (iPWR). Our Digital Instrumentation & Control (DI&C) Systems Subcommittee also reviewed this matter during a meeting on May 21, 2014. 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

1. The review process described in mPower iPWR DSRS Chapter 7, Instrumentation and Control Systems, should be piloted, subject to incorporation of our recommendations.

2. The DSRS should specify that safety importance Categories A1 (Safety-related risk-significant) and B1 (Non-safety-related risk-significant) should receive the most stringent review. The depth of review should be less stringent for Category A2 (Safety-related non-risk-significant) and least stringent for Category B2 (Non-safety-related non-risk-significant). This risk-significant/safety-related ordering should be applied in a consistent manner throughout all chapters of the DSRS.

3. Section 7.0, Instrumentation and Controls - Introduction and Overview of Review Process, Section 7.2.9 Control of Access, Identification, and Repair, and Section 7.2.13 Displays and Monitoring should be revised as indicated in the discussion.

BACKGROUND

Licensing reviews of I&C, and digital based I&C systems in particular, have been a significant challenge from the perspectives of both safety demonstration and schedule/resources for all new large light water reactor design centers. Industry has consistently expressed that DI&C licensing certainty is one of their highest priorities for new reactors. As a result, the staff has begun to develop a DSRS for iPWR designs beginning with mPower. Our December 18, 2012 letter report contains our first review of the draft Chapter 7, Instrumentation and Control Systems. We now provide our review of the updated version of that guidance, which has resolved industry and public comments.

DISCUSSION

The goal of the development of the design specific review standards was to apply the lessons learned during recent reviews of digital I&C systems and to develop a review standard for the mPower small modular reactor (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 DSRS Chapter 7:

- Reorganize the review guidance to emphasize the four fundamental design principles (i.e., redundancy, independence, determinism, diversity and defense-in-depth) plus the two implementing strategies of simplicity and control of access
- Provide guidance on fundamental design principles at the system level
- Remove redundant and non-applicable information
- Eliminate the use of design acceptance criteria
- 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 technical Appendices A, B, and C to address Hazard Analysis, System Architecture, and Simplicity, respectively. This organization accomplishes the following:

- Section 7.0 provides the reviewer with an overview of the process and maps I&C safety system regulatory requirements to the applicable DSRS section.
- Section 7.1 focuses the review guidance on how the applicant has addressed the fundamental design principles.
- Section 7.2 focuses the review guidance on the system characteristics and associated regulatory requirements for protection systems.
- Appendices A, B, and C contain review guidance for unique subjects that should be addressed in the application.

This construct essentially reorganizes the existing standard review plan 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. Design characteristics and regulatory requirements are then assessed within each system. Regulations not applicable to the new reactor I&C designs are deleted, which should streamline the review process.

Safety/Risk Importance Categories in Section 7.0

The DSRS defines four classifications for I&C systems according to their safety importance:

- Safety-related risk-significant (A1)
- Safety-related non-risk-significant (A2)
- Non-safety-related risk-significant (B1)
- Non-safety-related non-risk-significant (B2)

These classifications are directly analogous to similarly defined categories of structures, systems, and components (SSCs) in 10 CFR 50.69 (i.e., RISC-1 through RISC-4). While we understand that the staff wants to keep this safety importance review approach separate from the special treatment guidelines in 10 CFR 50.69, it is unnecessarily confusing to rename these identically defined categories that encompass the concepts of safety-related SSCs and their risk significance. Use of the RISC-1 through RISC-4 nomenclature in the standard review plan and the DSRS would preserve consistent understanding of these concepts throughout the regulations and staff guidance.

The DSRS specifies that the most stringent reviews will be performed for Categories A1 and A2, without any further differentiation between these categories. A less stringent level of review is specified for Category B1, involving more thorough scrutiny than is traditionally applied to non-safety-related SSCs. A traditional level of review is reserved for the SSCs in Category B2. In this context, all safety-related SSCs are subjected to the highest level of scrutiny, regardless of their risk importance. This guidance is not consistent with the risk–informed integrated SMR review framework that is described in NUREG-0800, "Introduction-Part 2, Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: Light-Water Small Modular Reactor Edition." The stated intent of that framework is to use design-specific risk information to focus review efforts on those SSCs that are most important to overall plant safety.

The specified DSRS priorities are inconsistent with the standard review plan guidance, other NRC regulations, and fundamental logic. The SSCs most important to plant safety are those that are determined to be risk-significant. Therefore, Categories A1 and B1 should receive the most stringent review.[1] While SSCs in Category A2 are classified as safety-related according to

[1] In this report, we are concerned primarily with the scope and depth of the technical design reviews. Other elements of the reviews for SSCs in Category B1 may be simplified, due to differing administrative and programmatic requirements for non-safety-related SSCs.

existing design-basis licensing criteria, their lower risk significance means that they are less important to plant safety, and their review effort can be correspondingly less stringent. Finally, the least detailed level of review should be reserved for SSCs in Category B2.

In a practical sense, we understand that the staff may anticipate that all digital I&C systems may need the same level of stringent review. However, that is a separate issue. The risk-significant/ safety-related ordering in the review guidance should make sense, and it should be applied in a consistent risk-informed manner throughout all chapters of the DSRS.

Control of Access in Section 7.2.9

In previous letter reports, 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, main control room, technical support center, emergency support center, or other support facilities from outside sources can be controlled administratively.

The staff understands our concern and position. However, they have stated that our recommendation entails a specific design implementation for control of access, that resolution of this recommendation has wider applicability than just for the mPower DSRS, and it involves policy level issues. The staff intends to develop a SECY paper regarding a number of DI&C technical issues which would address our recommendation.

Our recommendation is not intended to prescribe details of a specific design implementation. We simply stated that a solely one-way hardware-based design should be used to ensure control of access, rather than a potentially vulnerable software-controlled implementation. That function can be achieved through a variety of specific hardware designs.

We agree that our recommendation has wide applicability. It deals with communication access to the plant network from outside sources and thus needs consideration during the design phase of DI&C applications for both new reactors and modifications to existing reactors. However, we do not understand why policy level issues may conflict with our recommendation or why additional evaluation is required to proceed as we recommend. For example, Section 5.9 of IEEE Standard 603-1991, endorsed in 10 CFR 50.55a(h), states that control of access must be supported by the overall plant and system design. Thus, our recommendation is in consonance with the existing regulations.

Therefore, we continue to recommend that the Control of Access review section be revised to require the reviewer to assess the 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.

Inclusion of Licensed Operators in Section 7.2.13

Section 7.2.13 describes the review of displays and monitoring. It notes that the review of instrumentation and parameters that should be available for monitoring severe accidents is best accomplished by an interdisciplinary team. It is essential that licensed operators be included in that team. When the staff assembles any such interdisciplinary review team, they should ensure that the team includes members who have held licenses as senior reactor operators.

The review process described in mPower iPWR DSRS Chapter 7, Instrumentation and Control Systems, involves new concepts that must be addressed by both an applicant and the staff. It should be piloted after our recommendations have been resolved.

The staff has done an excellent job in developing this innovative approach to revising the standard review plan for future I&C designs and being proactive at incorporating lessons learned from recent new reactor DI&C design certifications.

Sincerely,

/RA/

John W. Stetkar
Chairman

REFERENCES

1. Final – Design-Specific Review Standard for B&W mPower SMR Design Section 7.1, Instrumentation of Controls – Fundamental Design Principles (ML14016A084).

2. Final – Design-Specific Review Standard for B&W mPower SMR Design Section 7.2, Instrumentation of Controls – System Characteristics (ML14016A179).

3. Final – Design-Specific Review Standard for B&W mPower SMR Design Section 7.0, Appendix B, Instrumentation of Controls – System Architecture (ML14016A084).

4. mPower Design-Specific Review Standard 7.1 Draft for Comment Rev 1.pdf (ML12236A232).

5. NUREG-0800, “Introduction-Part 2, Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: Light-Water Small Modular Reactor Edition,” Revision 0, January 2014, (ML 13207A315).

6. ACRS letter, Subject: “Draft Design Specific Review Standard for mPower iPWR Chapter 7 Instrumentation and Control Systems,” December 18, 2012 (ML12346A353)

7. NRO Memorandum, Subject: User Need Request, “Hazard Analysis- Development of Technical Basis and Recommendations for Review Guidance for Digital I&C Systems,” December 8, 2011 (ML11313A214)

8. RES Memorandum, Subject: Response to User Need Request, “Hazard Analysis-Development of Technical Basis and Recommendations for Review Guidance for Digital I&C Systems,” December 27, 2011 (NRO-2011- 009) (ML11355A038)

1. RES Memorandum, Subject: Response to User Need Request, "Hazard Analysis-Development of Technical Basis and Recommendations for Review Guidance for Digital I&C Systems," December 27, 2011 (NRO-2011- 009) (ML11355A038)

Accession No: **ML14196A141** **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 JWS
DATE	08/04/14	08/04/14	08/04/14	08/07/14	08/07/14

OFFICIAL RECORD COPY