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

November 20, 2013

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

SUBJECT: DRAFT FINAL REVISIONS OF REGULATORY GUIDES 1.168 THROUGH 1.173, SOFTWARE PROCESSES FOR DIGITAL COMPUTERS IN SAFETY SYSTEMS OF NUCLEAR POWER PLANTS

Dear Mr. Satorius:

During the 609th meeting of the Advisory Committee on Reactor Safeguards, November 7-8, 2013, we reviewed your August 29, 2013, response to the recommendations in our June 18, 2013, letter report on Draft Regulatory Guides (RGs) 1.68 through 1.73, Software Processes for Digital Computers in Safety Systems of Nuclear Power Plants.

Our letter noted that a footnote in each of these draft RGs stated:

> *The term "safety systems" is synonymous with "safety-related systems." The scope of the GDC includes structures, systems, and components "important to safety." However, the scope of this regulatory guide is limited to "safety systems," which are a subset of "systems important to safety."*

We noted that the current regulatory framework for reactors licensed under 10 CFR Part 50 and for new designs licensed under 10 CFR Part 52 contains provisions for enhanced design, quality, reliability, and regulatory oversight for non-safety-related structures, systems, and components (SSCs) that are "important to safety." These enhanced programs generally apply criteria that are less stringent than the requirements for safety-related SSCs, but are more restrictive than the criteria for other non-safety-related SSCs. We recommended that the staff expedite the development of consistent regulatory guidance for enhanced design, development, operation, and maintenance of digital hardware and software which controls non-safety-related equipment that is "important to safety."

The staff agreed that the footnote was overly restrictive and revised it by adding the following clarification:

> *Although not specifically scoped to include non-safety-related but "important to safety systems" this regulatory guide provides methods that the staff finds appropriate for the design, development and implementation of all important to safety systems. The NRC may apply this guidance in licensing reviews of non-safety but important to safety digital software and may tailor it to account for the safety significance of the system software.*

The staff stated that the revised footnote aligns well with existing guidance in Chapter 7 of NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants," and with the criteria for regulatory treatment of non-safety systems in RG 1.206, "Combined License Applications for Nuclear Power Plants."

The revised footnote appropriately clarifies the scope and context of the subject RGs. It also informs licensees and applicants that the staff intends to use similar guidance in their reviews of non-safety digital systems, which support functions that are important to plant safety. This is an excellent start. However, it is evident that additional guidance is needed for those reviews, tailored to the safety significance of those systems and their functions.

The IEEE standards that are referenced in these RGs define four levels of integrity for software. Level 4 is the most stringent, and the subject RGs recommend its use for safety-related systems. Complementary regulatory guidance is needed to clarify the intent and the degree to which the most appropriate software integrity levels should be applied for reviews of non-safety-related systems that are "important to safety." This is a challenging effort, but vital for common understanding of staff expectations. We encourage the staff to begin the development of formal regulatory guidance to support those reviews.

We look forward to future interactions with the staff on this important matter.

Sincerely,

/RA/

J. Sam Armijo
Chairman

REFERENCES

1. EDO Letter, Subject: "Draft Final Revisions of Regulatory Guides 1.168 Through 1.173, Software Processes for Digital Computers in Safety Systems of Nuclear Power Plants," August 29, 2013 (ML13219A062)

2. ACRS Letter, Subject: "Draft Final Revisions of Regulatory Guides 1.168 Through 1.173, Software Processes for Digital Computers in Safety Systems of Nuclear Power Plants," June 18, 2013 (ML13161A243)

3. NUREG-0800 Standard Review Plan (SRP) - Chapter 7, Instrumentation and Controls," Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition ," (ML110550791)

4. Regulatory Guide 1.206,"Combined License Applications for Nuclear Power Plants," June 2007 (ML 07072184)

3. NUREG-0800 Standard Review Plan (SRP) - Chapter 7, Instrumentation and Controls," Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition ," (ML110550791)

4. Regulatory Guide 1.206,"Combined License Applications for Nuclear Power Plants," June 2007 (ML 07072184)

Accession No: **ML13318A217** **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	11/19/13	11/19/13	11/19/13	11/20/13	11/20/13

OFFICIAL RECORD COPY