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

February 26, 2015

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

SUBJECT: PROPOSED REVISION FOR 10 CFR 50.55a TO INCORPORATE BY REFERENCE IEEE STANDARD 603-2009, "IEEE STANDARD CRITERIA FOR SAFETY SYSTEMS FOR NUCLEAR POWER GENERATING STATIONS"

Dear Mr. Satorius:

During the 621st meeting of the Advisory Committee on Reactor Safeguards (ACRS), February 5-7, 2015, we reviewed your October 16, 2014 response to the recommendations in our August 5, 2014 letter, titled, "Proposed Revision for 10 CFR 50.55a to Incorporate by Reference IEEE Standard 603-2009, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations"."

As we noted in our letter, nuclear power plant safety systems, whether analog or digital, rely on the following fundamental principles and implementing strategies to compensate for failures that could degrade safety system reliability: redundancy, independence, determinance, defense-in-depth and diversity, simplicity, and control of access. Only the principles of independence, determinance, and control of access are potentially compromised by the use of computer-based systems. Our recommendations are meant to ensure that these principles are maintained for digital-based systems critical to reactor safety. We request that the staff reconsider our recommendations based on the following clarifications:

ACRS Recommendation 2 - The staff states that, although our recommendation for the use of a hardware monitor for voting units in safety systems would provide adequate protection, other design solutions are possible that could do the same. However, the staff did not identify any other design solutions that would provide the independence that is needed for adequate protection.

The staff goes on to contend that we are suggesting a reactor shutdown or safeguards actuation be required if a processor locks up (ceases to respond). That is not true. We only suggest that the hardware monitor should produce a trip signal from any redundant voting unit that locks up.

A requirement for a hardware monitor should be incorporated in the rule.

ACRS Recommendation 3 - To address our concern to improve clarity regarding the independence of input-to-output response from redundant divisions or external systems, the staff proposes the following language: "All signal processing between sensor data input and safety control device actuation must be accomplished in a manner such that required safety functionality remains assured regardless of responses by redundant portions of the safety system or other external systems." We agree with this language. The staff intends to include it in the Federal Register Notice statements of consideration. We prefer to see this language incorporated also in proposed Revision 2 of Regulatory Guide (RG) 1.153, "Criteria for the Power, Instrumentation, and Control Portions of Safety Systems for NPPs," because that guidance is most at-hand to designers, licensee engineers, and NRC staff. We are concerned that requirements presented in the statements of consideration can become ephemeral over time.

ACRS Recommendation 4 - The staff agreed that our recommended approach to specify a hardware one-way transmission device would provide high assurance against malicious events and reasonable assurance against non-malicious events originating from outside a nuclear power plant's protected area. The staff stated they are planning to address the issue of control of access at the architecture boundary with a Commission policy (SECY) paper including an option for rulemaking. We are not persuaded that this requires a Commission policy determination. However, if they must seek Commission advice, we urge that the staff proceed expeditiously, setting a high priority for this issue and not entangle it with other instrumentation and control topics. The effects of losing control of access, either by intent or by accident, can be severe and have occurred in other industries. Neither NRC nor any licensee wants to see this issue driven by operating experience; i.e., an actual failure to maintain control of access.

Sincerely,

/RA/

John W. Stetkar
Chairman

REFERENCES

1. Draft Federal Register Notice, Proposed Rule 10 CFR 50.55a (Incorporation by Reference of IEEE 603-2009), November 15, 2011 (ML113191306)

2. Regulatory Analysis for Proposed Rulemaking: "Incorporation by Reference of Institute of Electrical and Electronics Engineers Standard 603-2009," January 31, 2012 (ML120310194)

3. Draft Regulatory Guide, DG-1251 (Proposed Revision 2 of RG 1.153), "Criteria for the Power, Instrumentation, and Control Portions of Safety Systems for NPPs," May 2014 (ML112160394)

4. IEEE 603-1991, "IEEE Standard - Criteria for Safety Systems for Nuclear Power Generating Stations," June 27, 1991

5. IEEE 603-2009, “IEEE Standard - Criteria for Safety Systems for Nuclear Power Generating Stations,” November 5, 2009

6. ACRS Letter, Subject: “Proposed Revision for 10 CFR 50.55a to incorporate by Reference IEEE Standard 603-2009,”IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations,” August 5, 2014 (ML14196A137)

7. EDO Letter, Subject: ”Proposed Revision of Title 10 of the Code of Federal Regulations Section 50.55a,”Codes and Standards,” to incorporate by Reference Institute of electrical and electronic engineers (IEEE) Standard 603-2009, “IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations,” October 16, 2014 (ML14260A342)

5. IEEE 603-2009, “IEEE Standard - Criteria for Safety Systems for Nuclear Power Generating Stations,” November 5, 2009

6. ACRS Letter, Subject: “Proposed Revision for 10 CFR 50.55a to incorporate by Reference IEEE Standard 603-2009,”IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations,” August 5, 2014 (ML14196A137)

7. EDO Letter, Subject: ”Proposed Revision of Title 10 of the Code of Federal Regulations Section 50.55a,”Codes and Standards,” to incorporate by Reference Institute of electrical and electronic engineers (IEEE) Standard 603-2009, “IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations,” October 16, 2014 (ML14260A342)

Accession No: **ML15039A003** **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	MLBanks	EMHackett	EMH for JWS
DATE	02/26/15	02/26/15	02/26/15	02/26/15	02/26/15

OFFICIAL RECORD COPY