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

August 5, 2014

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 616th meeting of the Advisory Committee on Reactor Safeguards, July 9-11, 2014, we completed our review of the proposed revision for 10 CFR 50.55a to incorporate by reference IEEE Standard (Std) 603-2009, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," and associated draft Revision 2 to Regulatory Guide (RG) 1.153, "Criteria for the Power, Instrumentation, and Control Systems for Nuclear Power Plants." Our Digital Instrumentation & Control (DI&C) Systems Subcommittee also reviewed this matter during a meeting on May 20, 2014. During these meetings, we had the benefit of discussions with representatives of the NRC staff. We also had the benefit of the documents referenced.

RECOMMENDATIONS

1. The proposed rule and draft Revision 2 of RG 1.153 should be published subsequent to incorporation of the following recommendations.

2. Section 10 CFR 50.55a(h)(5)i of the proposed rule should specify that for digital safety systems, if redundant portions must communicate with a functionally common processing unit in each redundant portion for coincidence voting for safety control device actuation, then the common processing units should be monitored by an independent hardware-based diverse means that produces a trip in the affected redundant portion if the common processing unit ceases operation or "locks-up" (ceases to respond). In addition, the trip should be produced independently of the monitored processing unit and executed by the hardware-based diverse means.

3. Section 10 CFR 50.55a(h)(4) of the proposed rule should be clarified to state that "both predictable and repeatable" means processing from sensor data input to safety control device actuation and independent of any redundant portions of the safety system or other external input.

4. Section 10 CFR 50.55a(h) of the proposed rule should specify an additional condition addressing Section 5.9 of IEEE Std 603-2009, Control of Access, that identifies communications external to the plant should be accomplished using one-way, hardware-based (transmit only) devices. These devices should neither be software configurable nor capable of alteration by external commands or any surreptitious means.

BACKGROUND

The purpose of the proposed rule revision is to update 10 CFR 50.55a to incorporate by reference the 2009 version of IEEE Std 603, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations." The revision is required because the previously incorporated IEEE Std 603-1991 is out of date:

- It does not address the introduction of digital technologies such as microprocessor or field programmable gate array (FPGA) based systems into instrumentation and control safety systems.

- It does not address certain design concepts possible with digital technologies such as data communications, system self diagnostics, integration of systems, and consolidation of functions.

In addition to incorporating by reference the 2009 version of IEEE Std 603, the proposed rule also:

- defines the conditions which would allow existing licensees to replace plant equipment while maintaining the existing licensing basis;

- defines the conditions for which existing permit, license, certificate, standard design, and standard design approvals would be required to address the new standard in modifications and applications; and most importantly;

- incorporates additional conditions upon the use of IEEE Std 603-2009 in the areas of system integrity, diversity and defense-in-depth analyses, independence, maintenance bypass, and maintenance of records.

Draft RG 1.153, Revision 2, provides guidance for the proposed rule.

DISCUSSION

Nuclear power plant safety system designs 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
- Control of access

These principles apply to digital instrumentation and control systems that use microprocessors or FPGAs, as well as analog systems.

Digital systems allow enhanced performance but:

- result in complex functional integration,
- have new design and failure issues (e.g., software complexity, need for verification and validation, lack of inherent inter-division communication independence, and lack of inherently deterministic processing), and
- networks may be used for communication between plant safety systems and control spaces to external site and corporate networks, resulting in potential compromised control of access from sources external to the plant.

The use of microprocessors or FPGAs in nuclear plant safety systems does not compromise the determination of the fundamental principles of redundancy, diversity and defense-in-depth, and simplicity. Their use does, however, introduce new vulnerabilities that potentially compromise division-to-division independence, determinant safety signal processing behavior, and control of access to plant safety systems from sources external to the plant.

Independence in digital applications is not inherently ensured by the existing rule requirement for electrical isolation. For example, a division computer that generates a trip must transmit its signal to the computer-based voting unit within its division and to other redundant divisions. Corruption of that data stream can result in lock-up of all voting units and failure to process a reactor trip or safeguards actuation. The proposed rule does not incorporate a condition that prevents this loss of independence.

Determinant behavior depends on program cycle design which can include operating system, operator, or other external interrupts. The proposed rule incorporates a condition for predictable and repeatable operation. The phrase “predictable and repeatable” in the rule is not clear in its application to real plant systems from sensor data inputs to control device actuation.

Connections between internal plant safety networks and networks external to the plant can enable remote access that is not under the control of the plant operators. This can compromise the control of reactor trip systems, safeguards systems, and critical plant normal control systems. Data may be transmitted from the systems via an internal plant network bus to the main control room, the technical support center, and the emergency support center, and can be transmitted through a firewall to an external network with access to the internet. These types of architectures compromise control of access, thus possibly compromising safety system information. The proposed rule does not contain any provision that prevents this loss of access control.

We have recommendations on two conditions in the proposed rule and the addition of a new condition as follows:

Independence - For independence between redundant portions of safety systems, the proposed rule [Section 10 CFR 50.55a(h)(5)i] includes the following conditions. The system architecture should be analyzed for 1) internal and external hazards, 2) the extent of connectivity, and 3) the impact of failures or degradation on the ability of the redundant portions to accomplish their safety functions.

The staff stated that the analysis of internal and external hazards would reveal whether processing unit lock-up could be a potential hazard and thus would determine whether an independent hardware means was required to monitor the processing units.

We disagree that a hazard analysis can identify all means by which a processor can lock-up. Digital system processing units are inherently subject to lock-up due to the nature and character of software-based data communications and cannot be adequately protected by operating system software or check algorithms. An analysis cannot provide positive assurance against the inherent nature of digital systems to lock-up. The conditions proposed in the rule for independence do not result in the same positive, inherent independence for digital safety systems as does the requirement for electrical isolation in analog safety systems. Thus, we recommend that Section 10 CFR 50.55a(h)(5)i of the proposed rule should incorporate the additional condition noted in Recommendation 2.

Determinance - The proposed rule [Section 10 CFR 50.55a(h)(4)] includes a condition that safety system functions "shall be demonstrated to be both repeatable and predictable." Draft RG 1.153, Revision 2, provides illumination on the intent as follows:

> "Predictable and repeatable operation of the system requires that the results of translating input signals to output signals are determined through known relationships among the controlled system states and required responses to those states, and in which a given set of input signals produce the same output signals for the full range of applicable conditions enumerated in the design basis."

This provides no context for application in real nuclear plant safety systems where the critical function is for the safety system processing to be both predictable and repeatable from sensor data input to safety control device actuation and independent of any redundant portions of the safety system or other external input. Thus, Section 10 CFR 50.55a(h)(4) of the proposed rule should be clarified as specified in Recommendation 3.

Control of Access - Section 5.9 of IEEE Std 603-2009 is identical to that in IEEE Std 603-1991. The application of digital safety systems and their associated networks compromises defense against external access. The proposed rule does not specify any condition that addresses external access to plant safety systems. The only way to prevent external access is through the use of a DI&C architecture that specifies hardware-based barriers that do not use software, allows only one-way outward data transmission, and blocks data transmission from

external sources. Software-based solutions can always be compromised either inadvertently or advertently. Therefore, an additional condition in Section 10 CFR 50.55a(h) addressing IEEE Std 603-2009, Section 5.9, Control of Access, should be specified as noted in Recommendation 4.

We commend the staff for a thorough, detailed evaluation and the development of the proposed rule to address vulnerabilities with the application of digital technologies to nuclear plant safety systems.

Sincerely,

/RA/

John W. Stetkar
Chairman

REFERENCES:

1. Federal Register Notice, Proposed Rule 10 CFR 50.55a (Incorporation by Reference of IEEE 603-2009), Provided on April 20, 2014 (ML113191306)

2. Regulatory Analysis for Proposed Rulemaking: "Incorporation by Reference of Institute of Electrical and Electronics Engineers Standard 603-2009," Provided on April 20, 2014 (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

external sources. Software-based solutions can always be compromised either inadvertently or advertently. Therefore, an additional condition in Section 10 CFR 50.55a(h) addressing IEEE Std 603-2009, Section 5.9, Control of Access, should be specified as noted in Recommendation 4.

We commend the staff for a thorough, detailed evaluation and the development of the proposed rule to address vulnerabilities with the application of digital technologies to nuclear plant safety systems.

Sincerely,

/RA/

John W. Stetkar
Chairman

REFERENCES:

1. Federal Register Notice, Proposed Rule 10 CFR 50.55a (Incorporation by Reference of IEEE 603-2009), Provided on April 20, 2014 (ML113191306)

2. Regulatory Analysis for Proposed Rulemaking: "Incorporation by Reference of Institute of Electrical and Electronics Engineers Standard 603-2009," Provided on April 20, 2014 (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

Accession No: ML14196A137 **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	08/04/14	08/04/14	08/04/14	08/07/14	08/07/14

OFFICIAL RECORD COPY