April 17, 2015

Mr. John W. Stetkar, Chairman
Advisory Committee on Reactor Safeguards
U.S. Nuclear Regulatory Commission
Washington, D.C. 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. Stetkar:

I am responding to the Advisory Committee on Reactor Safeguards (ACRS) letter dated February 26, 2015. It provided the ACRS's review and recommendations on the U.S. Nuclear Regulatory Commission (NRC) staff's draft proposed revision of Title 10 of the *Code of Federal Regulations* (10 CFR) Section 50.55a, "Codes and Standards." The staff plans to revise this regulation by incorporating by reference the Institute of Electrical and Electronics Engineers (IEEE) Standard 603-2009, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations."

In addition to new comments, the ACRS letter also requested that the staff reconsider recommendations from an earlier ACRS letter on the subject, dated August 5, 2014. On October 16, 2014, the staff responded to the ACRS's August recommendations. The NRC staff appreciates the ACRS interest in this rulemaking effort. Below are the staff's responses to the ACRS's comments and recommendations from the February 26, 2015, letter.

Clarification to 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 a 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.

Response:

The NRC staff has completed several safety evaluations for instrumentation and controls (I&C) platform designs that use various methods to ensure deterministic processor performance of voter modules. Some of these methods differ from the specific external hardware monitoring solution that the ACRS recommends for inclusion in regulation. During its safety evaluations, the staff learned that technical means of establishing independence between system divisions as well as deterministic system performance may vary greatly due to the fundamental design differences between the individual I&C platforms.

The Westinghouse Common Q platform is a good example of these fundamental design differences. The Common Q platform is currently used for safety-related functions in several operating nuclear power plants, and the staff has also evaluated and approved it for use in the AP1000 new reactor design. The Common Q platform includes a hardware-based watchdog timer that is integral with the processor module which initiates a reactor trip when a voter processor locks up. However, engineered safety feature functions are designed to fail as-is on voter processor lock-up. During its evaluation of the Common Q platform, the staff reviewed the design of these features and evaluated the independence characteristics established against all applicable regulatory criteria. This safety evaluation concluded the Common Q platform provides adequate independence between divisions and it ensures predictable deterministic performance of safety functions.

The staff recognizes the ACRS recommendation for the hardware monitor is to produce a trip signal from any redundant voting unit that locks up. However, with respect to engineered safety features actuation systems (ESFAS) and those associated safety functions, this recommendation remains contrary to existing regulatory guidance on the matter. In applications where redundant dual-voter processors are used for ESFAS systems, voters are configured such that either voter will initiate the actuation signal independently from the other. This one-of-two actuation configuration is necessary so the required safety functions remain operable even when one of the two redundant voters becomes inoperable. As such, a regulatory requirement for a hardware monitoring device to cause a divisional actuation signal would also require activation of the associated ESFAS functions during processor lock-up conditions. Appendix A, “General Design Criteria,” of 10 CFR Part 50, Criterion 23, “Protection System Failure Modes,” states, “The protection system shall be designed to fail into a safe state or into a state demonstrated to be acceptable on some other defined basis.” The staff considers the scenario and effect of a processing unit lock-up to be a failure as described in General Design Criterion 23. If the acceptable fail state is determined to be the nonactuated state for a given function, then there should not be a regulatory requirement that opposes this condition.

The following guidance on a hardware watchdog timer already exists in Standard Review Plan 7.1D (Conformance to IEEE Std. 7-4.3.2) which states the following:

> A non-software watchdog timer is critical in the overall diagnostic scheme. A software watchdog will fail to operate if the processor freezes and no instructions are processed. The reviewer should look for a hardware watchdog timer whose only software input is reset after the safety processor completes its function. Even then, the reviewer should look to ensure that there is no possibility of a software failure causing a jump to the reset function, thereby nullifying the effectiveness of the watchdog timer.

The staff finds that this guidance is sufficient and does not believe it needs to be a regulatory requirement because the staff has reviewed and approved alternative cases as discussed above.

Based upon the considerations described above, the NRC staff has concluded that existing regulatory requirements address the scenario described in ACRS Recommendation 2. Therefore, the staff does not plan to modify the proposed criteria outlined in 10 CFR 50.55a(h)(5)(i). However, the staff will consider inclusion of this recommendation in regulatory guidance as an acceptable means to meet the regulatory requirements for diversity and defense-in-depth when implementing digital safety systems in nuclear power plants.

Clarification to 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 proposed 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 requirement presented in the statements of consideration can become ephemeral over time.

Response:

As stated in the NRC's October 16, 2014, response letter, the staff will add the reference statement to the *Federal Register* notice statements of consideration. The staff will also add this statement to the proposed revision of RG 1.153, "Criteria for Safety Systems." This additional clarification, in conjunction with the definitions provided in the existing statements of consideration and the RG, should address the ACRS's concerns.

Clarification to 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.

Response:

The NRC staff acknowledged this ACRS recommendation in the NRC's October 16, 2014, response letter. The staff is currently developing a Commission (SECY) paper that is scheduled to be complete this fiscal year regarding the issue of control of access and what, if any, changes to Commission policy and regulation should be made to better address it.

This SECY paper will provide the Commission with options, including an option for rulemaking concerning control of access at the defensive architecture boundary that the ACRS has communicated as a specific issue of concern.

The NRC staff appreciates the comments and clarification provided by the ACRS. The staff looks forward to continuing discussions with the Committee as the staff completes this rulemaking.

Sincerely,

/RA/

Mark A. Satorius
Executive Director
for Operations

cc: Chairman Burns
Commissioner Svinicki
Commissioner Ostendorff
Commissioner Baran
SECY

Response:

The NRC staff acknowledged this ACRS recommendation in the NRC's October 16, 2014, response letter. The staff is currently developing a Commission (SECY) paper that is scheduled to be complete this fiscal year regarding the issue of control of access and what, if any, changes to Commission policy and regulation should be made to better address it.

This SECY paper will provide the Commission with options, including an option for rulemaking concerning control of access at the defensive architecture boundary that the ACRS has communicated as a specific issue of concern.

The NRC staff appreciates the comments and clarification provided by the ACRS. The staff looks forward to continuing discussions with the Committee as the staff completes this rulemaking.

Sincerely,

/RA/

Mark A. Satorius
Executive Director
for Operations

cc: Chairman Burns
Commissioner Svinicki
Commissioner Ostendorff
Commissioner Baran
SECY

ADAMS Accession Number: ML15064A121 *via email EDO-002

OFFICE	NRR/DE*	Tech Editor*	NRR/DE*	NRR/DPR
NAME	SArndt	CHsu	JThorp	LKokajko
DATE	03/23/2015	03/27/2015	03/31/2015	04/01/2015
OFFICE	NRR/DE*	RES/DE*	NRO/DE*	NRR
NAME	JLubinski (MJ Ross-Lee for)	BThomas	JTappert	WDean (JUhle for)
DATE	04/02/2015	04/07/2015	04/03/2015	04/08/2015
OFFICE	EDO			
NAME	MSatorius			
DATE	04/17/15			

OFFICIAL RECORD COPY

Letter to John W. Stetkar from Mark A. Satorius dated April 17, 2015

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”

DISTRIBUTION: OEDO-15-00194
PUBLIC
SArndt
RidsAcrsAcnw_MailCTR\
RidsOcfoMailCenter
RidsNrrDpr
RidsOgcMailCenter
RidsNrrOd
RidsResDe
RidsOcaMailCenter
RidsNrrMailCenter
RidsOpaMailCenter