October 16, 2014

Mr. John W. Stetkar, Chairman
Advisory Committee on Reactor Safeguards
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555-0001

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 ELECTRONICS ENGINEERS (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 August 5, 2014, regarding the ACRS review and recommendations associated with 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," to incorporate by reference the Institute of Electrical and Electronics Engineers (IEEE) Standard 603-2009, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations."

The ACRS letter contains a summary of ACRS concerns with the draft proposed rule language and several recommendations. The NRC staff appreciates the ACRS interest in this rulemaking effort and has carefully reviewed the ACRS recommendations. Please see the staff's response to the ACRS recommendations, below.

Recommendation 1

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

Response:

The NRC staff is completing its management review of the draft proposed rulemaking. Staff has incorporated one of the ACRS recommendations, as discussed below. Staff will also include discussions of the ACRS recommendations in its interactions during the public comment resolution process.

Recommendation 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.

Response:

The NRC staff has reviewed and approved safety system designs that conform to the proposed additional requirements in this recommendation and is therefore familiar with the design concepts being recommended. Though the staff agrees that a system which satisfies the proposed additional requirements would provide adequate protection, the staff also recognizes other design solutions are possible that could provide adequate protection.

10 CFR 50 Appendix A, General Design Criteria (GDC), 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 if conditions such as disconnection of the system, loss of energy, or postulated adverse environments are experienced." The NRC staff considers the scenario of a processing unit lock-up to be a postulated adverse environment as described in GDC 23. If the acceptable fail state is determined to be the non-actuated state for a given function, then there should not be a regulatory requirement that opposes the condition.

There are cases in which a trip or actuated state results in a plant condition that is less safe than a non-trip state (e.g., high pressure safety injection system actuation during normal rated thermal power conditions). The generally accepted practice for engineered safety features is for these safety functions to be designed in an "energize-to-actuate" configuration such that a system failure such as a loss of electrical power would not cause a safety function to actuate.

For reactor trip functions, the current regulation, 10 CFR 50.62, "Requirements for reduction of risk from anticipated transients without scram (ATWS) events for light-water-cooled nuclear power plants," already addresses the scenario of a common processing unit ceasing operation or locking-up. This regulation requires diverse equipment from the reactor trip system to automatically initiate the auxiliary (or emergency) feedwater system and initiate a turbine trip under conditions indicative of an ATWS. The ATWS rule also has design-specific requirements

for diverse scram and reactivity control systems. The scenario described in the ACRS letter of a voter processing unit lock-up in the context of a reactor trip system falls within the regulatory definition of an ATWS event. It is a failure of the reactor trip portion of the protection system specified in GDC 20, Appendix A; of 10 CFR Part 50.

Consideration must also be given to the potential for an independent hardware-based device to cause spurious safety function actuations during normal plant operations. The results of such actuations can, in some cases, be severe and must be considered in a plant accident analysis. Revision 6 of Branch Technical Position 7-19, Section 3.1, contains guidance for minimizing the potential for spurious actuation of protective systems caused by diverse means.

Currently, the NRC requires licensees and applicants to assess diversity and defense-in-depth when using digital safety systems as stipulated by the Commission in staff requirements memorandum to SECY 93-087. Any such diversity and defense-in-depth analysis requires postulation of digital system failures or malfunctions, including a system lock-up, which would impair a safety function. For such scenarios, the analysis is required to identify diverse means of maintaining plant safety through either manual operator actions or through diverse automatic actuation systems. The NRC staff agrees that a design function (i.e., an independent, hardware-based design with diverse means that produces a safety function actuation signal in the affected redundant portion (of the safety system)) could be an acceptable means of addressing existing diversity and defense-in-depth requirements. However, other means such as manual operator actions, or automatic actuation by a diverse system, can also ensure that the safety function is accomplished when the primary protection system is not functioning properly.

Based upon the considerations described above, the NRC staff has concluded that existing regulatory requirements address the scenario described in ACRS Recommendation 2; and, therefore, 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.

Recommendation 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.

Response:

ACRS Recommendation 3 proposes a clarification to the rule to add a new definition for "both predictable and repeatable" as "processing from sensor data input to safety control device actuation and independent of any redundant portions of the safety system or other external input." The NRC staff agrees (in part) with this clarification and supplemental definition. The staff notes that Section III of the preliminary draft proposed rule *Federal Register* notice includes the following individual definitions for the terms predictable and repeatable:

Predictable - the ability to determine the output of a system at any time through known relationships among the controlled system states and required responses to those states, such that a given set of input signals will always produce the same output signals.

Repeatable - the output of a system being consistently achieved given the same input and system properties (including internal and external conditions).

Additionally, the proposed rule statements of consideration provide the following clarification statement for clause 50.55a(h)(4):

Proposed § 50.55a(h)(4) would be added to amplify the requirements stated in IEEE Std 603-2009, section 5.5, "System Integrity." Proposed § 50.55a(h)(4) would require that in order to assure the integrity and reliable operation of safety systems, safety functions shall be designed to operate in a predictable and repeatable manner. 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.

Predictable and repeatable systems, in general, do not provide the capability for unscheduled event-based interrupts or operator-based system interrupts to meet system safety requirements. Systems that operate in a predictable and repeatable manner, in general, should not be designed with the capability for unscheduled event-based disruptions or operator-based system functions that would inhibit or prevent the system from meeting its safety requirements. Any analysis used to demonstrate system predictability and repeatability should be based on analysis of system characteristics (e.g., definitive design and performance criteria) as opposed to probabilistic analysis.

In response to the ACRS recommendation to improve clarity, the NRC staff will add the following statement to the *Federal Register* notice statements of consideration:

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.

This additional clarification, in conjunction with the definitions provided and the existing statements of consideration, should address the concerns expressed by the ACRS.

Recommendation 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.

Response:

The NRC staff acknowledges the ACRS recommendation and notes that the ACRS made a similar recommendation on Chapter 7 of the mPower Design-Specific Review Standard as outlined in letters dated December 18, 2012 (Agencywide Documents Access & Management System (ADAMS) Accession No. ML12362A173), March 19, 2013 (ADAMS Accession No. ML13084A057), and August 6, 2014 (ADAMS Accession No. ML14196A141). In NRC staff response letters (ADAMS Accession Nos. ML13010A110, ML13101A264, and ML14071A121), the staff agreed that the ACRS's recommended approach would provide high assurance against malicious events and reasonable assurance against nonmalicious events originating from outside a nuclear power plant's protected area. Furthermore, the staff noted that it intends to develop a Commission policy (SECY) paper regarding a number of issues specific to highly integrated instrumentation and control systems. This SECY paper would 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 staff is also developing a specific response to the ACRS letter dated August 6, 2014, regarding the control of access recommendation that was identified in that letter. This staff response will provide additional details on the basis for the proposed SECY paper.

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

Sincerely,

/RA Darren Ash for/

Mark A. Satorius
Executive Director
for Operations

cc: Chairman Macfarlane
Commissioner Svinicki
Commissioner Ostendorff
Commissioner Baran
SECY

Response:

The NRC staff acknowledges the ACRS recommendation and notes that the ACRS made a similar recommendation on Chapter 7 of the mPower Design-Specific Review Standard as outlined in letters dated December 18, 2012 (Agencywide Documents Access & Management System (ADAMS) Accession No. ML12362A173), March 19, 2013 (ADAMS Accession No. ML13084A057), and August 6, 2014 (ADAMS Accession No. ML14196A141). In NRC staff response letters (ADAMS Accession Nos. ML13010A110, ML13101A264, and ML14071A121), the staff agreed that the ACRS's recommended approach would provide high assurance against malicious events and reasonable assurance against nonmalicious events originating from outside a nuclear power plant's protected area. Furthermore, the staff noted that it intends to develop a Commission policy (SECY) paper regarding a number of issues specific to highly integrated instrumentation and control systems. This SECY paper would 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 staff is also developing a specific response to the ACRS letter dated August 6, 2014, regarding the control of access recommendation that was identified in that letter. This staff response will provide additional details on the basis for the proposed SECY paper.

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

Sincerely,

/RA Darren Ash for/

Mark A. Satorius
Executive Director
for Operations

cc: Chairman Macfarlane
Commissioner Svinicki
Commissioner Ostendorff
Commissioner Baran
SECY

DISTRIBUTION: OEDO-14-00555
RidsAcrsAcnw_MailCTR
OGC
OCA
OPA
CFO
RidsNrrOd Resource RidsNrrMailCenter Resource RidsNrrDpr Resource
RidsResDE Resource RidsNroDe Resource

ADAMS ACCESSION NUMBERS:
Package ML14223A681
Incoming ML14223A680
Rulemaking Draft ML14196A137
Response ML14260A342 ***via email**

OFFICE	NRR/DE/ECIB	NRR/DE	Tech Editor*	NRR/DPR*
NAME	RStattel	SArndt	CHsu	LKokajko (MKhanna for)
DATE	09/17/2014	09/17/2019	09/12/2014	9/19/2014
OFFICE	NRR/DE/ECIB	NRR/DE	RES/DE*	NRO/DE*
NAME	JThorp	PHiland (MJRoss for)	BThomas	JTappert
DATE	09/19/2014	09/22/2014	09/22/2014	09/24/2014
OFFICE	NRR	EDO		
NAME	DDorman	Dash for MSatorious		
DATE	09/29/2014	10 /16 /2014		

OFFICIAL RECORD COPY