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

December 21, 2022

Mr. Daniel H. Dorman
Executive Director for Operations
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

SUBJECT: PROPOSED DRAFT REGULATORY GUIDE 1.152, REVISION 4, "CRITERIA FOR PROGRAMMABLE DIGITAL DEVICES IN SAFETY-RELATED SYSTEMS OF NUCLEAR POWER PLANTS"

Dear Mr. Dorman:

During the 701st meeting of the Advisory Committee on Reactor Safeguards (ACRS), November 29 - December 2, 2022, we reviewed proposed draft Regulatory Guide (RG) 1.152, Revision 4, "Criteria for Programmable Digital Devices in Safety-Related Systems of Nuclear Power Plants." Our Digital Instrumentation and Control (DI&C) Systems Subcommittee also reviewed this matter on November 17, 2022. During this review, we had the benefit of discussions with representatives of the United States Nuclear Regulatory Commission (NRC). We also had the benefit of the documents referenced.

RECOMMENDATIONS

1. Proposed draft RG 1.152, Revision 4, should be issued for public comment after incorporation of our recommendations 2, 3, and 4.

2. The RG introduction should include a brief discussion highlighting that a robust safety-related system architecture and its fundamental design principles are key elements for developing sound safety-related protection and safeguards systems.

3. To comply with Commission direction, the RG should be revised to provide an example of use of RG 5.71 guidance during the design phase by noting the use of hardware-based, uni-directional communication is an approach the staff considers acceptable.

4. The RG should incorporate a new Clarification that strongly discourages the use of any active virus detection features that interact with and can prevent the normal execution of safety-related system software.

INTRODUCTION

Title 10 of the *Code of Federal Regulations* (10 CFR) Sections 50.55a(h)(2) and (h)(3) mandate compliance with the requirements stated in Institute of Electrical and Electronics Engineers (IEEE) Standard (Std) 279, various dates, or IEEE Std 603-1991, "IEEE Criteria for Safety Systems for Nuclear Power Generating Stations," for post-1991 safety system applications and development. These standards were written and applied for analog type systems.

Several versions of RG 1.152, endorsing IEEE Standard 7-4.3.2 "IEEE Standard Criteria for Programmable Digital Devices in Safety Systems of Nuclear Power Generating Stations," were developed for applications of computer-based systems. These versions of this IEEE standard use the term "safety system," consistent with the NRC's definition of safety-related systems in 10 CFR Section 50.2, "Definitions." This RG uses the term "safety-related system" in lieu of the term "safety system."

BACKGROUND

Proposed draft Revision 4 of RG 1.152 endorses IEEE Std 7-4.3.2-2016 with exceptions and clarifications. Specifically, this revision:

- Removes the previous secure development and operational environment (SDOE) guidance from this guide and instead endorses, with clarifications, a similar SDOE criteria within IEEE Std 7-4.3.2-2016,

- Includes additional guidance for fault detection and self-diagnostics in DI&C systems,

- Endorses Annex D, "Identification and control of hazards," of IEEE Std 7-4.3.2-2016,

- Clarifies the applicability of control of access guidance for safety-related programmable digital devices (PDDs),

- Includes applicable guidance on independence from interim staff guidance (ISG)-04 that has not been incorporated into IEEE Std 7-4.3.2-2016,

- Identifies that NRC uses branch technical position (BTP) 7-19 guidance to evaluate the applicant's defense-in-depth and diversity assessment to address common-cause failures (CCFs), and

- Implements the Commission's direction to address our concern pertaining to uni-directional communications from high-safety to low-safety significant systems and internal plant to external systems connected to the internet. The proposed RG revision references RG 5.71 to inform applicants of cybersecurity requirements and how these requirements could be considered during the design phase.

DISCUSSION

RG 1.152, BTP 7-19, and RG 5.71 are the primary guidance documents for the development of safety-related systems using PDDs. Additional information should be incorporated into RG 1.152 to address the following issues:

1. Safety-Related System Architecture

The use of software-based systems for the reactor protection system (RPS) and engineered safety feature actuation system (ESFAS) introduces new modes of CCF such as: unused, unintended, or prohibited functions, silent failures due to processor lockup, and failure to complete processing all safety functions within a software operating system timing cycle. Additionally, it introduces a new vulnerability from external source electronic access.

The primary protection against these types of CCFs is an overall robust multi-division architecture for RPS and ESFAS that meets the fundamental principles of DI&C design: redundancy; redundant division independence; deterministic operating system processing; defense-in-depth and diversity; and control of physical and external source electronic access. An additional important principle is providing a means of manual backup to initiate critical reactor shutdown and safeguards actuation that are not dependent on software.

A brief discussion highlighting the importance of a robust safety-related system architecture and its fundamental design principles, as the key elements for developing sound safety-related protection and safeguards systems, should be incorporated in the RG introduction.

2. Control of Access

During our November 17, 2022, DI&C Systems Subcommittee meeting, the staff indicated that they implemented the above noted Commission's direction by incorporating a new Clarification 1.b.(3), 3.3 stating that this RG is not intended to address protective features to prevent malicious cyberattacks. The Clarification further states that if cybersecurity design features are included, the extent of the staff's review is limited to ensuring that these features do not adversely affect a system's capability to perform its safety functions. The RG Clarification also highlights that licensees can consider the cybersecurity guidance in RG 5.71 in preparing a design certification under 10 CFR Part 52.

We commented that, while this calls attention to the use of RG 5.71 during the design phase, it does not provide an example of any method(s) that would be acceptable to the staff. During our Full Committee meeting on November 29, 2022, staff stated that they would revise proposed draft Revision 4 of RG 1.152 to provide an example indicating the use of hardware-based uni-directional communication is an approach the staff considers acceptable. We agree with the proposed resolution.

3. IEEE 7-4.3.2, Clause 5.9.3 - Interaction between Cybersecurity Features and Safety Functions

This clause provides guidance on the incorporation of cybersecurity features (e.g., various types of virus protection software) into safety-related systems. It states initially that inclusion of cybersecurity features directly into safety-related systems should be avoided. However, it then goes on to say when incorporation of cybersecurity features into DI&C safety-related systems is necessary, then a number of specific issues must be addressed.

Cybersecurity protection may take many forms including: hardware-based (e.g., uni-directional communications); system design (e.g., factory-burned field programmable arrays); operating system (e.g., secure boot, avoiding the use of vulnerability-prone languages); and the use of active virus detection software that depends on up-to-date virus definition files. RG 1.152 should incorporate a new Clarification that strongly discourages the use of any active virus

detection features that interact with and can prevent the normal execution of safety-related system software.

SUMMARY

Proposed draft RG 1.152, Revision 4 should be issued for public comment after incorporation of our recommendations 2, 3 and 4.

Sincerely,

Signed by Rempe, Joy
on 12/21/22

Joy L. Rempe
Chairman

REFERENCES

1. U.S. Nuclear Regulatory Commission (NRC), Draft Guide (DG)-1374, Proposed Regulatory Guide (RG) 1.152, “Criteria for Programmable Digital Devices in Safety-Related Systems of Nuclear Power Plants,” Revision 4, September 2022, Washington, DC (ML22244A199)

2. Institute of Electrical and Electronics Engineers (IEEE) Standard (Std) 7-4.3.2-2016, “IEEE Standard Criteria for Programmable Digital Devices in Safety Systems of Nuclear Power Generating Stations,” Piscataway, NJ, August 25, 2016

3. IEEE Std 603-1991, “IEEE Criteria for Safety Systems for Nuclear Power Generating Stations,” and the correction sheet dated January 30, 1995, Piscataway, NJ

4. NRC, NUREG-0800, Branch Technical Position 7-19, “Guidance for Evaluation of Defense-in-Depth and Diversity to Address Common-Cause Failure due to Latent Design Defects in Digital Safety Systems,” Revision 8,” January 25, 2021 (ML20339A647)

5. NRC, DG-1402, Proposed New RG 1.250, “Dedication of Commercial-Grade Digital Instrumentation and Control Items for Use in Nuclear Power Plants,” Revision 0, March 2022, Washington, DC (ML22003A180)

6. NRC, Interim Staff Guidance-04 “Highly-Integrated Control Rooms - Communications Issues (HICRc),” Revision 1, March 6, 2009 (ML083310185)

December 21, 2022

SUBJECT: PROPOSED DRAFT REGULATORY GUIDE 1.152, REVISION 4, "CRITERIA FOR PROGRAMMABLE DIGITAL DEVICES IN SAFETY-RELATED SYSTEMS OF NUCLEAR POWER PLANTS"

Accession No: ML22342B268 **Publicly Available (Y/N):** Y **Sensitive (Y/N):** N
If Sensitive, which category?
Viewing Rights: ☒ NRC Users or ☐ ACRS only or ☐ See restricted distribution

OFFICE	ACRS*	SUNSI Review*	ACRS*	ACRS*	ACRS*
NAME	CAntonescu	CAntonescu	LBurkhart	SMoore	JRempe
DATE	12/9/22	12/9/22	12/12/22	12/19/22	12/21/22

OFFICIAL RECORD COPY