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

November 21, 2022

The Honorable Christopher T. Hanson
Chair
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

SUBJECT: SECY-22-0076, "EXPANSION OF CURRENT POLICY ON POTENTIAL COMMON-CAUSE FAILURES IN DIGITAL INSTRUMENTATION AND CONTROL SYSTEMS"

Dear Chair Hanson:

During the 700th meeting of the Advisory Committee on Reactor Safeguards (ACRS), November 1-4, 2022, we reviewed SECY-22-0076, "Expansion of Current Policy on Potential Common-Cause Failures in Digital Instrumentation and Control Systems" (Notation Vote). Our Digital Instrumentation and Control (DI&C) Systems Subcommittee also reviewed this matter on May 20, 2022, and September 23, 2022. During our reviews, we had the benefit of discussions with representatives of the United States Nuclear Regulatory Commission (U.S. NRC) and Nuclear Energy Institute staffs. We also had the benefit of the documents referenced.

CONCLUSION AND RECOMMENDATION

1. SECY-22-0076 provides a reasonable approach to a risk-informed evaluation of the need for diversity in DI&C systems to address common-cause failures (CCFs).

2. Prior to implementation, the Commission should reinforce that positions in SECY-93-087 and the SRM-SECY-93-087, that are not explicitly addressed or modified by SECY-22-0076, are still applicable.

BACKGROUND

In SECY-93-087, dated April 2, 1993, the staff recommended an approach for demonstrating an adequate level of defense-in-depth and diversity to protect against potential common-mode failures of DI&C systems. [1] In SRM-SECY-93-087, the Commission approved in part and modified in part the staff's recommendations. In general, the Commission actions were:

---

1 Although SECY-93-087 and its associated SRM often refer to "common-mode failures," we use the term common-cause failure (CCF) as a broader term encompassing common-mode failures because it better characterizes the type of failures in question.

Approved Position 1: Applicants shall assess the "defense-in-depth and diversity" of the proposed DI&C systems to demonstrate that vulnerabilities to common-mode failures have been addressed adequately.

Modified Position 2: Applicants shall analyze each postulated common-mode failure for events evaluated in the accident analysis section of the safety analysis report. The Commission stated that in as much as common-mode failures are beyond design-basis events, the Position 2 analysis of such events should be on a best-estimate basis.

Approved Position 3: If a postulated common-mode failure could disable a safety function, then a diverse means, with a documented basis that the diverse means is unlikely to be subject to the same common-mode failure, shall be required to perform either the same function or a different function. The diverse or different function may be performed by a non-safety system if the system is of sufficient quality to perform the necessary function under the associated event conditions.

Modified Position 4: SECY Position 4 requires a set of safety-grade displays and controls be in the main control room, independent and diverse from the safety computer system identified in Positions 1 and 3 above for manual, system-level actuation of critical safety functions and monitoring of parameters that support the safety functions. The Commission modified this position, stating that because the staff indicates in Position 3 that "The diverse or different function may be performed by a non-safety system…", the words "safety-grade" should be deleted from Position 4.

Also addressing Position 4, the Commission further stated, that "…the remainder of the discussion under the fourth part of the staff position is highly prescriptive and detailed (e.g., 'shall be evaluated', 'shall be sufficient', 'shall be hardwired', etc.). The Commission approves only that such prescriptiveness be considered as general guidance, the practicality of which should be determined on a case-by-case basis."

In SECY-18-0090, "Plan for Addressing Potential Common-Cause Failure in Digital Instrumentation and Controls," dated September 12, 2018, the staff reaffirmed the Commission's direction in SRM-SECY-93-087. This direction remained appropriate and established guiding principles for implementing the policy.

INTRODUCTION

SECY-22-0076 requests that the Commission expand the current policy for DI&C CCFs to allow the use of risk-informed approaches to demonstrate the appropriate level of defense-in-depth. This includes evaluation of whether diverse automatic actuation of safety functions is required. This expanded policy would apply to requests for new or amended licenses and design approvals, for all nuclear power plant types, under Title 10 of the *Code of Federal Regulations* (10 CFR) Part 50, "Domestic Licensing of Production and Utilization Facilities," and 10 CFR Part 52, "Licenses, Certifications, and Approvals for Nuclear Power Plants."

The current approach, outlined in SRM-SECY-93-087 and reaffirmed in SECY-18-0090, will remain acceptable to address CCFs in DI&C systems. The current DI&C CCF policy has been used successfully but does not accommodate the use of risk-informed approaches to determine whether diverse automatic actuation functions are required to address postulated CCFs for structures, systems, and components (SSCs) of high safety-significance.

The staff recognizes there is now an opportunity to risk-inform the current policy to address DI&C CCFs for SSCs of high safety-significance. This opportunity arises because of the maturity of: (1) DI&C design processes, (2) risk-informed decision-making guidance, and (3) processes that are in place to ensure the acceptability of probabilistic risk assessment (PRA) models.

The staff is proposing an expanded DI&C CCF policy that encompasses and augments the current positions in SRM-SECY-93-087. It incorporates the use of risk-informed approaches in performing the defense-in-depth and diversity assessment and in determining the adequacy of design techniques, prevention measures, and mitigation measures, to address postulated DI&C CCFs without any diverse automatic actuation functions for SSCs of high safety-significance.

SECY-22-0076 is written to provide two parallel paths for evaluating diversity and defense-in-depth to address CCFs in DI&C safety systems based on the position guidance provided by the Commission in SRM-SECY-93-087. Staff reworded Positions 1 and 4 for clarity using the term “common cause failure” in place of “common mode failure”. Positions 2 and 3 are revised to incorporate two paths, one for using risk-informed techniques, and one for the traditional defense-in-depth and diversity assessment.

If the Commission approves the expanded policy described in SECY-22-0076, the staff will update existing implementation guidance to address DI&C CCFs. The following guiding principles will be applied to ensure that implementation of the expanded policy for DI&C CCF is consistent with the NRC’s policies on risk-informed decision-making:

- no conflict with existing regulatory requirements (i.e., a rule change or exemption will not be required),
- maintain consistency with existing PRA policies,
- maintain reasonable assurance of adequate protection of public health and safety,
- risk-informed approaches will be consistent with established principles of risk-informed decision-making.

DISCUSSION

In SECY-22-0076, staff states that the proposed revised Positions 1 through 4, incorporating the risk-informed approach for DI&C CCF, encompass and augment the current positions in SRM-SECY-93-087 rather than replacing them. SECY-22-0076 provides a reasonable approach to a risk-informed evaluation of the need for diversity in DI&C systems to address CCFs.

The revised Positions 1 through 3 reasonably replicate those in SRM-SECY-93-087, with Positions 2 and 3 incorporating the risk-informed approach in concert with the defense-in-depth and diversity approach. However, revised Position 4, while consistent, in part, with SRM-SECY-93-087, results in ambiguity since it did not incorporate paragraphs 2 through 4 of Position 4. These three paragraphs included extensive discussion on the character of manual displays and controls stating that they “shall be evaluated”; “shall be sufficient”; and “shall be hardwired”; etc., for actuation at the lowest level in the safety computer system.

The Commission commented that this level of specificity in the staff position is highly prescriptive and detailed. Thus, they approved only that such prescriptiveness be considered as general guidance, the practicality of which should be determined on a case-by-case basis.

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.

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 manual backup means to initiate critical reactor shutdown and safeguards actuation that are not dependent on software.

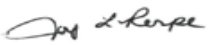
SECY-93-087 and SRM-SECY-93-087 make clear that hardwired backups are to be considered on a case-by-case basis where needed for safety critical systems. We have followed Commission guidance in our review of RPS and ESFAS in recent design applications for actuation at the lowest level in the safety computer system architecture.

The SECY-93-087 terms “shall be hardwired” and “for actuation at the lowest level in the safety computer system” would be particularly relevant if SECY-22-0076 abrogated (or nullified) the SECY-93-087, Position 4, paragraphs 2 through 4 discussion and Commission SRM guidance. Thus, we asked the staff during our subcommittee meeting on September 23, 2022, if the position in SECY-22-0076, which does not specifically address the above stated position paragraphs from SRM-SECY-93-087, would cause the SRM requirements to no longer be applicable.

Subsequent to our subcommittee meeting on September 23, 2022, staff followed up on the ACRS question and confirmed that if SECY-22-0076 did not request a change, then positions in SRM-SECY-93-087 not addressed explicitly are still the Commission’s requirements and need not be restated.

Because there is substantial comingling of positions amongst SECY-93-087, SRM-SECY-93-087, and SECY-22-0076, it would help prevent future misunderstandings to explicitly state this position in SECY-22-0076. Thus, we recommend that prior to implementation, the Commission should reinforce that positions in SECY-93-087 and SRM-SECY-93-087, that are not explicitly addressed or modified by SECY-22-0076, are still applicable.

Sincerely,


Signed by Rempe, Joy
on 11/21/22

Joy L. Rempe
Chairman

REFERENCES

1. U.S. Nuclear Regulatory Commission, SECY-22-0076, “Expansion of Current Policy on Potential Common-Cause Failures in Digital Instrumentation and Control Systems,” August 10, 2022 (Notation Vote) (ML22164B003)

2. U.S. Nuclear Regulatory Commission, SECY-93-087, “Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs,” April 2, 1993 (ML003708021)

3. U.S. Nuclear Regulatory Commission, Staff Requirements Memorandum-SECY-93-087, “Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs,” July 21, 1993 (ML003708056)

4. U.S. Nuclear Regulatory Commission, SECY-18-0090, “Plan for Addressing Potential Common Cause Failure in Digital Instrumentation and Controls,” September 12, 2018 (ML18179A067)

November 21, 2022

SUBJECT: SECY-22-0076, “EXPANSION OF CURRENT POLICY ON POTENTIAL COMMON-CAUSE FAILURES IN DIGITAL INSTRUMENTATION AND CONTROL SYSTEMS”

Accession No: ML22313A101 **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	11/10/22	11/10/22	11/10/22	11/17/22	11/21/22

OFFICIAL RECORD COPY