POLICY ISSUE
(Notation Vote)

August 10, 2022 SECY-22-0076

FOR: The Commissioners

FROM: Daniel H. Dorman
Executive Director for Operations

SUBJECT: EXPANSION OF CURRENT POLICY ON POTENTIAL COMMON-CAUSE FAILURES IN DIGITAL INSTRUMENTATION AND CONTROL SYSTEMS

PURPOSE:

To request that the Commission expand the current policy for digital instrumentation and control (I&C) common-cause failures (CCFs) to allow the use of risk-informed approaches to demonstrate the appropriate level of defense-in-depth, including not providing any diverse automatic actuation of safety functions. 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."

CONTACTS: Samir Darbali, NRR/DEX
301-415-1360

Steven M. Alferink, NRR/DRA
817-200-1548

Bhagwat P. Jain, NRR/DORL
301-415-6303

SUMMARY:

The staff recommends the Commission adopt an expanded policy for digital I&C CCF. The recommended policy builds upon the current policy from Staff Requirements Memorandum (SRM)-SECY-93-087, "SECY-93-087–Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs," dated July 21, 1993 (Agencywide Documents Access and Management System (ADAMS) Accession No. ML003708056), (relevant text reproduced in Enclosure 1), and provides for the expanded use of risk-informed approaches. The expanded policy would allow consideration of whether design techniques and prevention and mitigation measures are adequate to address potential CCFs without any diverse automatic actuation functions for high safety significance structures, systems, or components (SSCs).

BACKGROUND:

The nuclear power industry is implementing modern digital I&C technologies. While these technologies increase reliability and provide safety benefits, they can also introduce new types of potential systematic, nonrandom, concurrent failures of redundant elements, also known as CCFs, in the design of protection systems.[1] For example, software design errors, programming errors, or hardware design errors could result in a CCF of redundant trains controlled by identical digital I&C systems. These kinds of failures are less of a concern with analog I&C systems because they do not rely on software and are not capable of the same degree of integration of functions as modern digital technologies.

The possibility of CCFs in protection systems has been a concern since the mid-1960s. The U.S. Nuclear Regulatory Commission (NRC) started receiving applications that included digital I&C technology in protection systems in the 1970s, and the use of digital I&C technologies continued to expand in the 1980s. In the early 1990s, the NRC staff described the major regulatory issues associated with the use of digital I&C in evolutionary and ALWRs to the Commission in SECY-91-292, "Digital Computer Systems for Advanced Light-Water Reactors," dated September 16, 1991 (ADAMS Accession No. ML12222A030).

NRC regulations for independence and diversity of I&C systems are contained in 10 CFR Part 50. Specifically, 10 CFR 50.55a(h) incorporates by reference Institute of Electrical and Electronics Engineers (IEEE) Std 279, "IEEE Standard: Criteria for Protection Systems for Nuclear Power Generating Stations," and IEEE Std 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," which are mandatory for nuclear power plants licensed since 1971. IEEE Std 279, clauses 4.1, 4.17, and 4.20, and IEEE Std 603-1991, clauses 4.10, 5.6.1, 6.2.1, 6.2.2, and 6.2.3, contain requirements related to automatically initiated protective actions, manual controls, and information displays. Furthermore, the introduction to 10 CFR Part 50, Appendix A, "General Design Criteria for Nuclear Power Plants," calls for applicants to consider the possibility of systematic, nonrandom, concurrent failures of redundant elements (i.e., CCFs) in the design of protection systems and reactivity control systems and points to General Design Criteria 22, 24, 26, and 29. General Design Criterion 22, "Protection system independence," states, "[d]esign techniques, such as functional diversity or diversity in component design and principles of operation, shall be used to the extent practical to prevent loss of the protection function."

---

[1] Although SECY-93-087 and its associated SRM often refer to "common-mode failures," this paper uses the term CCF as a broader term encompassing common-mode failures because it better characterizes the type of failures in question.

In SECY-93-087, dated April 2, 1993 (ADAMS Accession No. ML003708021), the staff recommended an approach for demonstrating an adequate level of diversity and defense in depth to protect against potential CCFs of digital I&C systems. In SRM-SECY-93-087, the Commission approved in part and modified in part the staff's recommendations. In general, the Commission approved the position that an applicant assesses the "defense-in-depth and diversity" of the proposed I&C systems to demonstrate that vulnerabilities to CCF have been addressed adequately, but the Commission modified the staff's proposal to specify that best-estimate methods can be used. The Commission also approved the use of a diverse means to address a CCF that could disable a safety function, as identified by the applicant's assessment, provided the diverse means is unlikely to be subject to the same CCF. The Commission indicated that the diverse means need not be safety-related, but the system must be "of sufficient quality to perform the necessary function under the associated event conditions." The SRM also states that displays and controls, independent and diverse from the safety system, shall be provided in the main control room for manual, system-level actuation of critical safety functions. In SECY-18-0090, "Plan for Addressing Potential Common Cause Failure in Digital Instrumentation and Controls," dated September 12, 2018 (ADAMS Accession No. ML18179A067), the staff reaffirmed that the Commission's direction in SRM-SECY-93-087 remained appropriate and established guiding principles for implementing the policy as the staff was updating a significant amount of related staff guidance at the time.

In response to SRM-SECY-93-087, the staff developed review procedures and acceptance criteria, which were initially contained in Branch Technical Position (BTP) 7-19, Revision 4, "Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems," (ADAMS Accession No. ML052500555) of NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition."[2] The staff continues to update BTP 7-19 to reflect experience with digital I&C technologies, licensing reviews, stakeholder feedback, and industry standards. The current revision of BTP 7-19, Revision 8, (ADAMS Accession No. ML20339A647) provides guidance for staff review of applications using a graded approach based on safety significance of the digital I&C system.

DISCUSSION:

The current approach, outlined in SRM-SECY-93-087 and the guiding principles in SECY-18-0090, remains acceptable to address CCF in digital I&C systems in applications for new or amended licenses and design approvals, for all nuclear power plant types, under 10 CFR Part 50 and 10 CFR Part 52. The current digital I&C CCF policy has been used successfully, but does not accommodate the use of risk-informed approaches to determine whether diverse automatic functions are required to address postulated CCFs for high safety significance SSCs.[3] Specifically, Item 18 in SRM-SECY-93-087 states, in part, "the vendor or applicant shall analyze each postulated common-mode failure for each event that is evaluated in the accident analysis section of the safety analysis report using best-estimate methods," and "[i]f a postulated common-mode failure could disable a safety function, then a diverse means … shall be required to perform either the same function or a different function." (Emphasis added).

The staff recognizes that there is an opportunity to risk-inform the current digital I&C CCF policy to address digital I&C CCFs for high safety significance SSCs. This opportunity arises because

[2] https://www.nrc.gov/reading-rm/doc-collections/nuregs/staff/sr0800/index.html

[3] BTP 7-19, Revision 8, defines high safety significance SSCs as safety-related SSCs that perform safety-significant functions.

of the maturity of (1) digital I&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. This paper addresses the use of PRA in the evaluation of potential digital I&C CCFs. In its 1995 PRA Policy Statement, the Commission presented its policy on the use of PRA methods in regulatory matters (60 FR 42622; August 16, 1995). SRM-SECY-98-144, "White Paper on Risk-Informed and Performance-Based Regulation," revised March 1, 1999 (ADAMS Accession No. ML003753601), provides direction to the staff and definitions of key terms for risk-informed and performance-based regulation. The use of risk-informed approaches can provide flexibility to address digital I&C CCF while maintaining safety and is consistent with the PRA Policy Statement.

The staff's latest review guidance in BTP 7-19, Revision 8, incorporates consideration of risk-informed safety significance using a graded approach in determining whether: (1) the proposed digital I&C system is of such low safety significance that CCF need not be evaluated or (2) a less rigorous method can be used to address CCF. However, BTP 7-19, Revision 8, represents the limits of the staff's ability to accept new, risk-informed approaches without additional Commission direction.

To allow the staff to evaluate expanded risk-informed approaches for digital I&C CCF in applications for new or amended licenses or design approvals, the staff proposes, as illustrated in enclosure 2, an expanded policy for digital I&C CCF that augments, rather than replaces, the current policy for digital I&C CCF. The staff is proposing an expanded digital I&C CCF policy that encompasses the current position in SRM-SECY-93-087 and provides for 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, other than diversity, to address a postulated digital I&C CCF. In particular, the expanded policy would provide flexibility to the staff to approve approaches that do not rely on a diverse means of performing a safety function to address a postulated CCF for high safety significance SSCs. The staff's recommendation would expand the current policy as follows:

- Incorporate the language in point 1 of SRM-SECY-93-087, Item 18, with appropriate clarifications and corrections (e.g., replace "common-mode failure" with "common-cause failure").

- Incorporate the language in points 2 and 3 of SRM-SECY-93-087, Item 18, with the flexibility to use risk-informed approaches.

- Incorporate the existing language in point 4 of SRM-SECY-93-087, Item 18, with appropriate clarifications.

Specifically, the staff recommends that the Commission approve the following four points in the expanded policy for staff review of applications involving digital I&C systems:[4]

(1) The applicant shall assess the defense in depth and diversity of the facility incorporating the proposed digital I&C system to demonstrate that vulnerabilities to digital CCFs have been adequately identified and addressed.

---

[4] Consistent with the direction in SRM-SECY-93-087, standard design certifications must meet these points. Deviations in other applications from the recommended policy described in this paper would need to be approved by the Commission.

The defense-in-depth and diversity assessment shall be commensurate with the risk significance of the proposed digital I&C system.

(2) In performing the defense-in-depth and diversity assessment, the applicant shall analyze each postulated CCF. This assessment may use either best-estimate methods or a risk-informed approach.

When using best-estimate methods, the applicant shall demonstrate adequate defense in depth and diversity within the facility's design for each event evaluated in the accident analysis section of the safety analysis report.

When using a risk-informed approach, the applicant shall include an evaluation of the approach against the Commission's policy and guidance, including any applicable regulations, for risk-informed decision-making. The NRC staff will review applications that use risk-informed approaches for consistency with established NRC policy and guidance on risk-informed decision-making (e.g., Regulatory Guide (RG) 1.174, "An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis").

(3) The defense-in-depth and diversity assessment may demonstrate that a postulated CCF can be reasonably prevented or mitigated or is not risk significant. The applicant shall demonstrate the adequacy of any design techniques, prevention measures, or mitigation measures, other than diversity, that are credited in the assessment. The level of technical justification demonstrating the adequacy of these techniques or measures, other than diversity, to address potential CCFs shall be commensurate with the risk significance of each postulated CCF.

A diverse means that performs either the same function or a different function is acceptable to address a CCF, provided that the assessment includes a documented basis showing that the diverse means is unlikely to be subject to the same CCF. The diverse means may be performed by a system that is not safety-related if the system is of sufficient quality to reliably perform the necessary function under the associated event conditions. Either automatic or manual actuation within an acceptable timeframe is an acceptable means of diverse actuation.

If a postulated CCF is risk significant and the assessment does not demonstrate the adequacy of other design techniques, prevention measures, or mitigation measures, then a diverse means shall be provided.

(4) Main control room displays and controls that are independent and diverse from the proposed digital I&C system (i.e., unlikely to be subject to the same CCF) shall be provided for manual, system-level actuation of critical safety functions and monitoring of parameters that support the safety functions. These main control room displays and controls may be used to address point 3, above.

The recommended expanded policy for digital I&C CCFs would apply to requests for new or amended licenses and design approvals, for all nuclear power plant types, under 10 CFR Part 50 and 10 CFR Part 52. The expansion of the policy is intended to be technology neutral but relies on assumptions about the design of the facility, such as the presence of a main control room. Therefore, if the staff encounters a design where the policy would not be applicable, the staff will engage the Commission as appropriate.

Points 1 and 3 of the proposed expanded policy both allow for consideration of the risk significance of the digital I&C system and the postulated CCF. Specifically, point 1 would explicitly allow the defense-in-depth and diversity assessment to be commensurate with the risk significance of the proposed digital I&C system. This clarifying aspect of point 1 would be implemented consistent with the review guidance for graded approaches to digital I&C CCF in BTP 7-19, Revision 8.

The recommended expanded digital I&C CCF position in point 3 refers to the risk significance of CCFs whereas point 1 refers to the risk significance of the proposed system. For example, the staff expects that for a license amendment request, the risk significance of CCFs will be determined by any increase in risk to the facility (e.g., increase in core damage frequency or large early release frequency) from a postulated digital I&C CCF and that this risk increase would be determined using a quantitative bounding assessment.[5] Bounding assessments are conservative approaches that have been used in other areas, and the staff has confidence in their ability to account for the uncertainties in quantifying the probability of occurrence of digital I&C CCFs. In contrast, current experience is insufficient to establish confidence in quantifying the probability of occurrence of digital I&C CCFs.[6] Therefore, the NRC staff will not be able to approve risk-informed quantitative approaches based on reducing the probability of occurrence of digital I&C CCFs through design techniques for high safety significance SSCs.[7] If future experience establishes confidence in quantifying the probability of occurrence of a digital I&C CCF, the staff will inform the Commission before approving approaches based on reducing the probability of occurrence through design techniques.

Point 3 of the recommended expanded policy would allow for a system that is not safety-related to perform the diverse means if the system is of sufficient quality to reliably perform the necessary function under the associated event conditions. In addition, this point states that diverse means can be performed by either automatic or manual actuation within an acceptable timeframe. The current guidance in BTP 7-19, Revision 8, provides the staff guidance for determining if a non-safety-related system credited to perform the diverse means is of sufficient quality and if automatic and manual actuations can the performed within an acceptable timeframe.

Regarding point 2 of the recommended expanded policy for digital I&C CCF, the NRC staff's goal is that the acceptance criteria for risk-informed approaches for digital I&C CCFs will be consistent with the NRC's broader (i.e., not specific to digital I&C) practices and guidance for risk-informed decision-making. For example, the NRC staff will review license amendment requests for conformance to the guidance in RG 1.174 for applications employing risk-informed approaches.

The position in point 4 of SRM-SECY-93-087, Item 18, is maintained in point 4 of the recommended expanded policy because (1) it clarifies the implementation of existing regulatory requirements (e.g., IEEE Std 279, clauses 4.1, 4.17, and 4.20, and IEEE Std 603-1991, clauses 4.10, 5.6.1, 6.2.1, 6.2.2, and 6.2.3) for addressing digital I&C CCFs and (2) the lack of

---

5 Current PRA models can assess the risk increase associated with digital I&C CCFs by using bounding values for the probability of occurrence of digital I&C CCFs. These bounding values can be justified through quantitative or qualitative analyses

6 Current PRA models do not include details of various hardware or software components of digital I&C systems and cannot compare the risk reduction between different digital I&C design techniques.

7 BTP 7-19, Revision 8, allows a qualitative assessment and failure analysis that the likelihood of failure is sufficiently low to be used to eliminate a CCF from further consideration for SSCs with low safety significance.

independent and diverse displays and controls in the control room would prevent the manual operation of critical safety functions in the event that a CCF disables the digital I&C system. The displays and controls credited for point 4 must provide for effective manual control of the following critical safety functions: reactivity control, core heat removal, reactor coolant inventory, containment isolation, and containment integrity. Point 4 of the recommended expanded policy clarifies that it is intended to be addressed in the same assessment as the first three points. Point 4 implements existing regulatory requirements, from which licensees may request exemptions (under 10 CFR 50.12 or 52.7) or alternatives (under 10 CFR 50.55a(z)). However, to implement the proposed expanded Commission policy for digital I&C CCF, the staff would inform the Commission before approving or denying exemptions and alternatives that deviate from point 4.

The staff maintains awareness of how digital I&C CCFs are treated in other countries and in nonnuclear safety-critical applications.[8] The staff factored these considerations into the development of this paper and performed significant stakeholder engagement while developing this paper through: (1) holding public meetings to discuss the proposed approach on February 15, 2022 (ADAMS Accession No. ML22054A002), and June 8, 2022 (ADAMS Accession No. ML22167A159); (2) considering proposals from the Nuclear Energy Institute (NEI) for a revised policy for digital I&C CCF in letters dated April 8, 2022 (ADAMS Accession No. ML22098A218), and June 1, 2022 (ADAMS Accession No. ML22152A271); and (3) presenting the approach to the Advisory Committee on Reactor Safeguards (ACRS) Digital I&C Subcommittee on May 20, 2022 (ADAMS Accession No. ML22130A727). At the ACRS Subcommittee meeting, it was discussed that the ACRS would have an opportunity to review any guidance that might be developed to implement the expanded policy, if approved. The Subcommittee decided not to send a letter to the Commission regarding the staff's proposed expanded policy at this time.

During the public meetings, stakeholders, including NEI, expressed that clarification was needed in the application of point 4 of SRM-SECY-93-087, specifically as it relates to the assessment performed for the first three points. The staff agrees that clarification of point 4 is warranted and incorporated this feedback into the proposed point 4 of the expanded policy. NEI also expressed the desire to risk-inform point 4. The staff does not believe that risk-informing point 4 is practical because, as mentioned above, it clarifies the implementation of existing regulatory requirements, and a lack of independent and diverse displays and controls in the control room would prevent the manual operation of critical safety functions in the event that a CCF disables the digital I&C system. However, requests for alternatives or exemptions provide an avenue for applicants to request a deviation from point 4 based on risk information on a case-by-case basis.

If approved, the staff will apply the following guiding principles to ensure that implementation of the expanded policy for digital I&C CCF is consistent with the NRC's policies on risk-informed decision-making:

- The expanded policy for digital I&C CCF will not conflict with existing regulatory requirements (i.e., a rule change or exemption will not be required to implement the policy).

---

[8] See, for example, the report for the House and Senate Committees on Appropriations, "Approaches to Permitting the Use of Digital Instrumentation and Controls in Safety Applications," dated December 27, 2018 (ADAMS Accession No. ML18309A327).

- The expanded policy for digital I&C CCF will be implemented consistent with the Commission's 1995 PRA Policy Statement and SRM-SECY-98-144.

- Implementation of the expanded policy for digital I&C CCF will continue to provide reasonable assurance of adequate protection of public health and safety.

- The use of risk-informed approaches will be consistent with established principles of risk-informed decision-making. For example, RG 1.174, Revision 3 (ADAMS Accession No. ML17317A256), provides five principles that should be considered in the risk-informed integrated decision-making process.

- The underlying PRAs used for the bounding assessment as part of risk-informed approaches will be technically acceptable and will be supported by an effective PRA configuration control and feedback mechanism. For example, RG 1.200, Revision 3, "Acceptability of Probabilistic Risk Assessment Results for Risk-Informed Activities," (ADAMS Accession No. ML20238B871) and interim staff guidance DC/COL-ISG-028, "Assessing the Technical Adequacy of the Advanced Light-Water Reactor Probabilistic Risk Assessment for the Design Certification Application and Combined License Application," (ADAMS Accession No. ML16130A468) provide guidance for determining the acceptability of PRA models.

COMMITMENT:

If the Commission approves the expanded policy described in this paper, the staff will update the existing implementation guidance to address digital I&C CCFs. The staff also will continue to engage stakeholders and the public to seek comments on the staff's implementation of the expanded policy.

RECOMMENDATION:

The staff recommends that the Commission approve the proposed expanded policy for digital I&C CCF.

RESOURCES:

Staff estimate 2 full-time equivalent in fiscal year (FY) 2023 to implement its recommendation and expect to use resources currently included in the FY 2023 President's Budget. Resources for FY 2024, and if needed beyond FY 2024, will be addressed during the planning, budgeting, and performance management process

COORDINATION:

The Office of the General Counsel reviewed this package and has no legal objection.
The Office of the Chief Financial Officer reviewed this package and determined that it has no additional financial impact.

Daniel H. Dorman Digitally signed by Daniel H. Dorman
Date: 2022.08.10 07:34:26 -04'00'

Daniel H. Dorman
Executive Director
for Operations

Enclosures:
1. Relevant Text from SRM-SECY-93-087
2. Proposed Expanded Policy Flowchart

SUBJECT: EXPANSION OF CURRENT POLICY ON POTENTIAL COMMON-CAUSE FAILURES IN DIGITAL INSTRUMENTATION AND CONTROL SYSTEMS DATED August 10, 2022

ADAMS Accession Numbers: Pkg. - ML22193A290, SECY - ML22164B003, Encl1 - ML22193A293m Encl 2 - ML22193A294 **SECY-012**

OFFICE	NRR/DORL/PM	NRR/DORL/LA	NRR/DEX/ELTB/BC	NRR/DEX/EICB/BC
NAME	BJain	PBlechman (KGoldstein for)	SWyman	MWaters
DATE	06/13/2022	06/14/2022	06/14/2022	06/13/2022
OFFICE	NRR/DEX/D	NRR/DRA/D	QTE	CFO
NAME	EBenner	MFranovich (MKhanna for)	JDougherty	RAllwein
DATE	06/24/2022	06/13/2022	06/15/2022	07/07/2022
OFFICE	OGC	NRR/D	EDO	
NAME	SClark	AVeil	DDorman	
DATE	07/08/2022	07/12/2022	08/10/22	

OFFICIAL RECORD COPY