POLICY ISSUE
(Information)

September 12, 2018 SECY-18-0090

FOR: The Commissioners

FROM: Margaret M. Doane
Executive Director for Operations

SUBJECT: PLAN FOR ADDRESSING POTENTIAL COMMON CAUSE FAILURE IN DIGITAL INSTRUMENTATION AND CONTROLS

PURPOSE:

The purpose of this paper is to inform the Commission about the staff's plan to clarify guidance associated with evaluating and addressing potential common cause failure (CCF) of digital instrumentation and control (DI&C) systems. The proposed plan is consistent with the Commission's direction in the staff requirements memorandum (SRM) for SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs," dated July 21, 1993, reproduced in Enclosure 1 (Agencywide Documents Access and Management System (ADAMS) Accession No.: ML003708056). Specifically, this paper describes how the staff of the U.S. Nuclear Regulatory Commission (NRC) will ensure that the direction in the SRM continues to be applied consistently as the staff updates licensing guidance for evaluating a potential CCF in current DI&C technologies.

BACKGROUND:

The nuclear power industry continues to replace aging instrumentation and control (I&C) systems with modern DI&C systems. DI&C technologies provide increased reliability and safety benefits, but can also introduce new types of potential CCF hazards. For example, software design errors, programming errors, or hardware design errors could result in a CCF of redundant trains with identical DI&C systems.

CONTACTS: Mauricio Gutierrez, RES/DE
301-415-1925

Rossnyev Alvarado, NRR/DE
301-415-6808

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[1] of DI&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 assess the "defense-in-depth and diversity" of the proposed I&C systems to demonstrate that vulnerabilities to CCF have been addressed adequately, but allowed applicants to do so using best-estimate methods. The Commission also approved the use of a diverse means to address a CCF that could disable a safety function, as identified by the licensee 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. The SRM also addressed displays and controls in the main control room, but they are not a subject of this SECY paper.

The staff developed review procedures and acceptance criteria to incorporate the Commission direction in the Branch Technical Position (BTP) 7-19, "Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems," of NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants: LWR Edition," (ADAMS Accession No.: ML16019A344). The staff has updated BTP 7-19 several times based on experience with DI&C technologies and industry standards.[2]

Industry stakeholders have identified CCF as the highest technical priority to address in support of their DI&C deployment plans. Stakeholder comments have focused on three areas: (1) methods for addressing a potential CCF in upgrades performed under Title 10 of the *Code of Federal Regulations* (10 CFR) 50.59, "Changes, Tests, and Experiments," (2) evaluation scope and methods for addressing potential CCF in upgrades approved under NRC licensing actions; and (3) crediting the use of defensive measures to mitigate or eliminate CCF hazards.[3]

In SRM-SECY-16-0070, "Integrated Strategy to Modernize the Nuclear Regulatory Commission's Digital Instrumentation and Control Regulatory Infrastructure," dated October 25, 2016 (ADAMS Accession No.: ML16299A157), the Commission approved the staff's proposed Integrated Action Plan (IAP) to modernize the NRC's DI&C regulatory infrastructure. IAP Modernization Plan (MP#1) was developed to allow for near term activities (i.e., "tactical activities") that could begin addressing CCF in DI&C systems. Pursuant to SRM-SECY-16-0070, the Commission is periodically briefed and updated on the status of all IAP activities.[4] IAP Modernization Plan 4B (MP#4B) will broadly evaluate the current overall I&C regulatory infrastructure and the supporting technical bases. MP#4B will consider other important areas beyond those identified in the tactical activities, such as past review experiences, ongoing licensing review and research efforts, lessons learned from operating experience, insights from other industries that use DI&C technologies for safety critical

---

[1] Although SECY-93-087 and the SRM associated with it often refer to "common-mode failures," this paper uses the term CCF as a broader term encompassing common-mode failures.

[2] The current version of BTP 7-19 is revision 7. Revision 4 was the first revision of BTP 7-19 to address and reference Commission direction in SRM-SECY-93-087. Hardware design errors are not addressed in BTP 7-19 because they are not unique to DI&C systems and are adequately addressed in other parts of the NRC's regulatory infrastructure.

[3] Examples of industry proposed defensive measures now under NRC staff consideration can be found in NEI 16-16 (Draft 2), "Guidance for Addressing Digital Common Cause Failure" (ADAMS Accession No.: ML17135A253).

[4] See SECY-17-0105, "Update to the Integrated Strategy to Modernize the NRC's Digital Instrumentation and Control Regulatory Infrastructure" (ADAMS Accession No.: ML17277B542) and Draft IAP Revision 2, "Integrated Action Plan to Modernize Digital Instrumentation and Controls and Regulatory Infrastructure," Jan. 31, 2018 (ADAMS Accession No.: ML17277B643).

applications, and international perspectives. MP#4B focuses on identifying and prioritizing the improvements to modernize the regulatory infrastructure over the longer term in light of evolving approaches to I&C. As part of its implementation of MP#4B, the staff is reviewing requirements in other industries and countries to determine whether more effective and efficient methods to ensure safety can be implemented by the U.S. nuclear industry. Although these regulatory structures differ, as do the methods and depth of oversight, there is a universal recognition that defense-in-depth and diversity provisions are needed to protect against potential CCF hazards that could challenge plant safety.

DISCUSSION:

The staff continues to believe that the Commission's direction in SRM-SECY-93-087 addresses CCF in digital I&C systems and provides adequate flexibility for regulatory modernization activities that support near-term DI&C implementation. Although significant effort has been applied to the development of highly reliable DI&C systems, the staff believes that some residual faults might remain undetected within a system and could result in hazards that can challenge plant safety. To address these potential hazards, applicants and licensees (1) identify potential hazards unique to the specific DI&C technology and associated impacts to the intended safety functions and (2) evaluate the ability of the design to sufficiently perform its intended safety functions assuming a CCF in the DI&C system.

The staff will ensure consistent application of the direction provided in SRM-SECY-93-087 and address stakeholder comments by applying the following guiding principles, which are intended to reduce regulatory uncertainty:

(1) Applicants and licensees for Production and Utilization Facilities under 10 CFR Part 50, "Domestic Licensing of Production and Utilization Facilities or under 10 CFR Part 52, "Licenses, Certifications, and Approvals for Nuclear Power Plants" should continue to assess and address CCFs due to software for DI&C systems and components.

(2) A defense-in-depth and diversity analysis for reactor trip systems and engineered safety features should continue to be performed to demonstrate that vulnerabilities to a CCF have been identified and adequately addressed. In performing this analysis, the vendor, applicant, or licensee should analyze each postulated CCF for each event evaluated in the accident analysis section of the safety analysis report. This defense-in-depth and diversity analysis can be either a best estimate analysis or a design-basis analysis.

(3) This analyses should also be commensurate with the safety significance of the system. An analysis may not be necessary for some low-safety-significance I&C systems whose failure would not adversely affect a safety function or place a plant in a condition that cannot be reasonably mitigated.

(4) If a postulated CCF 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 CCF, should perform either the same function or a different function. The diverse or different function may be performed by either a safety or a non-safety system if the system is of sufficient quality to perform the necessary function under the associated event conditions in a reliable manner. Use of either automatic or manual actuation within an acceptable time frame is an acceptable means of diverse actuation. If the defense-in-depth and diversity analysis demonstrates that a CCF, when evaluated in the accident analysis section of the safety analysis report, can be reasonably mitigated though other

means (such as with current systems), a diverse means that performs the same or a different function may not be needed.

(5) The level of technical justification needed to demonstrate that defensive measures (i.e., prevention and mitigation measures) are adequate to address potential CCFs should be commensurate with the safety significance of the DI&C system. For the systems of higher safety significance, any defensive measures credited need technical justification that demonstrates that an effective alternative to internal diversity and testability has been implemented.

The staff applied these guiding principles in Regulatory Issue Summary (RIS) 2002-22, Supplement 1, "Clarification on Endorsement of Nuclear Energy Institute Guidance in Designing Digital Upgrades in Instrumentation and Control Systems" (ADAMS Accession No.: ML18143B633). The RIS supplement clarifies guidance on the use of a qualitative assessment that considers design attributes, quality of design process, and operating experience, and supports failure and defense-in-depth and diversity analyses for licensees to address CCF likelihood in low-safety-significance applications when performing 10 CFR 50.59 evaluations.

The staff intends to revise BTP 7-19, which describes an acceptable approach for a defense-in-depth and diversity analysis. Industry stakeholders have questioned the necessity of applying guidance on a defense-in-depth and diversity analysis to safety-related auxiliary support systems and non-safety systems. The staff has affirmed that potential CCF hazards due to software should be considered and addressed for all types of DI&C systems for which their malfunction could adversely affect safety function(s) or plant conditions. Specifically, an appropriate defense-in-depth and diversity analysis is necessary when implementing digital technology so that failures due to software or failures propagated through connectivity cannot result in a failure to perform safety functions or adverse plant conditions that cannot be reasonably mitigated. As stated above in principle 3, the staff believes that the level—rigor and detail— of the defense-in-depth and diversity analysis should be commensurate with the safety significance of the system or consequence of potential system failure. More details on systems for which a defense-in-depth and diversity analysis is or is not necessary will be provided in the revised BTP 7-19.

The staff will also update BTP 7-19 to be consistent with the use of design attributes, quality of design process, and operating experience in accordance with RIS 2002-22, Supplement 1, for systems of lower safety significance that may require specific licensing approval. The staff is evaluating the methods available to determine the safety significance and potential consequences of a DI&C system CCF and the associated uncertainties. BTP 7-19 currently notes that either of two design attributes is sufficient to eliminate software CCF from further consideration: (1) demonstration of diversity; or (2) assurance (through testing of systems that are sufficiently simple) that all possible software states and failure paths have been eliminated. Industry representatives have asked the staff to consider "defensive measures" as additional alternatives to reduce the likelihood of CCF. A defense-in-depth and diversity analysis can currently credit defensive measures if they provide the assurance that faults are unlikely to propagate and impact plant safety. Similar to the defense-in-depth and diversity analysis, as stated above in principle 5, the staff believes that the level of technical justification necessary to demonstrate that the design measures are effective in addressing potential CCFs should be commensurate with the safety significance of the system or consequence of potential failure. The staff will evaluate how to incorporate the Commission's direction into the broader regulatory infrastructure as part of MP#4B.

In developing this SECY, the staff has engaged with stakeholders on the technical subject matter and has presented a draft version of the guiding principles previously noted, which will be used to update the licensing guidance. The staff has made public presentations to the Advisory Committee on Reactor Safeguards Digital I&C Subcommittee on May 17, 2018 (ADAMS Accession No: ML18171A325), and June 20, 2018 (ADAMS Accession No: ML18177A382). In addition, the staff discussed a draft form of these principles with stakeholders at public meetings held on May 24, 2018 (ADAMS Accession No: ML18122A134), and July 25, 2018 (ADAMS Accession No: ML18204A313). The staff will continue to engage industry and seek comments on the next revision of BTP 7-19.

CONCLUSION:

The Commission's direction in SRM-SECY-93-087 addresses CCF in digital I&C systems and provides adequate flexibility for regulatory modernization activities that support near-term DI&C implementation. To ensure consistent application of the NRC's position on defense against CCF in current and future DI&C system designs, the staff will update and clarify licensing guidance by using the guiding principles described in this paper. Updated licensing guidance will support the near-term licensing needs identified by stakeholders. The staff will evaluate how to address CCF in broader regulatory infrastructure activities described in MP#4B of the IAP.

RESOURCES:

No additional resources beyond those currently identified in the IAP are anticipated. Work on the next revision of BTP 7-19 will be performed in-house. The staff continues to assess the resources associated with these activities as part of the normal budget development process.

COORDINATION:

The Office of the General Counsel has reviewed this paper and has no legal objections. The Office of the Chief Financial Officer has reviewed this paper for resource implications and has no objections.

Margaret M. Doane
Executive Director
for Operations

Enclosure:
Relevant Text from the Staff Requirements Memorandum to SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light Water Reactor (ALWR) Designs"

SUBJECT: PLAN FOR ADDRESSING POTENTIAL COMMON CAUSE FAILURE IN DIGITAL INSTRUMENTATION AND CONTROLS

ADAMS Package Accession No.: ML18179A066 ***via-email**

OFFICE	RES/DE	NRR/DEI	NRO/DEI	Tech Ed	NRR/DE
NAME	M. Gutierrez	*R. Alvarado	*D. Taneja	*QTE	*S. Arndt
DATE	06/28/18	07/02/18	07/02/18	06/29/18	07/03/18

OFFICE	NRO/DEI	RES/DE	NRR/DE	NRO/DEI	RES/DE
NAME	*I. Garcia	R. Jenkins	*R. Alvarado for D. Rahn	*D. Taneja for L. Betancourt	B. Thomas
DATE	07/03/18	07/03/18	07/02/18	07/02/18	07/11/18

OFFICE	NRO/DEI	NRR/DE	*OGC	RES	NRO
NAME	*R. Caldwell	*E. Benner	R. Weisman	*R. Furstenau	*F. Brown
DATE	07/05/18	07/03/18	08/07/18	07/23/18	07/19/18

OFFICE	NRR	OCFO	EDO		
NAME	L. Dudes for B. Holian	*R. Allwein for M. Wylie	M. Doane		
DATE	07/20/18	07/23/18	09/12/18		

OFFICIAL RECORD COPY