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

November 23, 2020

Ms. Margaret M. Doane
Executive Director for Operations
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

SUBJECT: FINAL DRAFT REVISION 8 OF STANDARD REVIEW PLAN BRANCH TECHNICAL POSITION 7-19, “GUIDANCE FOR EVALUATION OF DEFENSE-IN-DEPTH AND DIVERSITY TO ADDRESS COMMON CAUSE FAILURE DUE TO LATENT DEFECTS IN DIGITAL SAFETY SYSTEMS”

Dear Ms Doane:

During the 680th meeting of the Advisory Committee on Reactor Safeguards, November 4-6, 2020, we completed our review of Final Draft Revision 8 of Standard Review Plan (SRP)(NUREG-0800), Branch Technical Position (BTP) 7-19, "Guidance for Evaluation of Defense-in-Depth and Diversity to Address Common Cause Failure Due to Latent Defects in Digital Safety Systems," dated October 2020. Our Digital Instrumentation & Control (DI&C) Systems Subcommittee also reviewed this matter during meetings on November 21, 2019, June 2, 2020, and September 8, 2020. During these reviews, we had the benefit of discussions with representatives of the United States Nuclear Regulatory Commission (U.S. NRC) staff and comments from industry representatives. We also had the benefit of the documents referenced.

RECOMMENDATIONS

1. BTP 7-19, Revision 8 should be issued subsequent to incorporation of Recommendations 2 and 3.

2. Sections A and B.2.1 discuss the combining or integrating of the Reactor Trip System (RTS) and Engineered Safety Features Actuation System (ESFAS) and associated communications architectures into a single protection system. This approach challenges two critical defense-in-depth and diversity (D3) elements, redundancy and independence. The BTP should ensure that reviewers verify these fundamental architecture principles are maintained.

3. Section B.2.1 should ensure that interconnections between High Safety-Significance systems and those of Lower Safety-Significance are one-way, uni-directional digital communication devices rather than bi-directional communication devices (which reduce independence and defense-in-depth) to preclude compromise of High Safety-Significance Systems.

BACKGROUND

Digital technology offers significant operational and maintenance benefits for instrumentation and control systems in nuclear power plants (NPPs). DI&C systems are composed of both hardware components and logic elements (e.g., software). DI&C systems or components are vulnerable to common cause failures (CCFs) similar to those considered for analog systems due to latent design defects in active hardware components, software, or software-based logic. A CCF occurs when multiple (usually identical) systems or components fail due to a shared cause. CCFs can result in two different effects: (1) a loss of the capability to perform a safety function or initiate a plant transient, or (2) initiate the operation of a function without a valid demand or result in erroneous (i.e., spurious) system actions.

Staff Requirements Memorandum (SRM) to SECY-93-087 provided the Commission's policy on how potential CCFs should be addressed in DI&C systems and the following four staff positions for their evaluation:

1. Perform a D3 assessment to demonstrate vulnerabilities were addressed.

2. Analyze each CCF for each event in the safety analysis report using best estimate methods.

3. Provide a diverse means if assessment shows a CCF could disable a safety 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.

4. Provide diverse displays and controls in the main control room for manual, system-level actuation of critical safety functions.

SECY-18-0090 clarifies the staff application of the Commission's direction in the four positions within SRM-SECY-93-087. The BTP focusses the staff review guidance to satisfy the above Commission direction.

The BTP provides guidance for evaluating any diversity and defense-in-depth means credited to address vulnerabilities to CCF caused by latent defects in system hardware, software or software-based logic, as well as, the effects of any unmitigated CCF outcomes on plant safety.

Specifically, the BTP provides guidance for reviewing (1) proposed design attributes, such as the use of diverse equipment, testing, or U.S. NRC-approved alternative methods, including defensive measures within the design of a system or component to eliminate the potential for CCF from further consideration, (2) diverse external equipment, including manual controls and displays to limit or mitigate a potential CCF, and (3) other measures to ensure conformance with the U.S. NRC's position on addressing potential CCFs in DI&C systems.

The guidance of this BTP is intended for staff reviews of DI&C safety systems with (1) proposed modifications that require implementation of a license amendment, and (2) applications for construction permits, operating licenses, combined licenses, design certifications, standard design approvals, and manufacturing licenses. This BTP is not applicable to proposed modifications performed under the change process in 10 CFR 50.59, "Changes, tests and experiments." Review criteria for single random failures and cascading failures from shared resources (i.e., not due to latent design defects in DI&C Structures, Systems and Components (SSCs)) are not covered in this BTP.

To accomplish the D3 evaluation, the proposed revision:

1. maintains the guiding principles from SRM-SECY-93-087,

2. incorporates the use of safety significance determination assessments with three specific categories:

    a. High Safety-Significance: Safety-Related SSCs that perform Safety-Significant Functions,

    b. Lower Safety-Significance: Safety-Related SSCs that do not Perform Safety-Significant Functions and Non-Safety-Related SSCs that do perform Safety-Significant Functions, and

    c. Lowest Safety-Significance: Non-Safety-Related SSCs that do not perform Safety-Significant Functions

3. incorporates qualitative assessment criteria from Supplement 1 to RIS 2002-22 for non-reactor protection systems/ESFAS and concepts of alternative measures,

4. provides guidance on spurious operation assessments,

5. identifies means to eliminate CCF from further consideration, to mitigate CCFs, and also defines the need to demonstrate that consequences of CCF vulnerabilities that have not been eliminated or mitigated are acceptable,

6. provides guidance for manual actions as diverse means for mitigation of CCFs, and

7. improves the structure of the BTP to enhance ease of use and readability.

DISCUSSION

A fundamental precept for developing the CCF D3 assessment is to have a defined and detailed one-line block diagram architecture that meets the fundamental design principles for the structure of DI&C system designs. An architecture that meets the fundamental design principles already embodies multiple layers of D3. Thus, the detailed architecture provides the basic framework for identifying the need for and type of additional D3 to mitigate any remaining vulnerabilities. This fundamental precept is incorporated and emphasized in the background preamble of the BTP and meeting the fundamental design principles is also emphasized. Without this framework, the D3 assessment will devolve back into a piecemeal approach.

Revision 8 incorporates expanded discussion on the philosophy of defense-in-depth and diversity. A discussion of implementing approaches follows:

1. descriptions of the means to eliminate CCF from further consideration, including the use of diversity, the use of testing, and the use of alternative measures, including defensive measures or qualitative assessments.

2. descriptions of the means to mitigate CCF failures, including use of diverse means, crediting existing systems, crediting manual operator actions including protective actions initiated by manual actions, and crediting a new diverse system.

3. a discussion on how the consequences of the occurrence of a CCF may be acceptable with no action at all.

We agree that the reorganized structure and expanded content of the BTP have made it much easier to understand and use. However, there are two areas that are of significant concern.

1. Of particular interest, Revision 8 notes in Sections A. "Background," and B.2.1, "System Integration and Interconnectivity," that DI&C systems can integrate design functions that were previously located in separate and dedicated analog systems. For example, it states that formerly discrete systems (e.g., the RTS and the ESFAS) can be combined into a single DI&C protection system. Also, DI&C systems can share resources, such as communications, networks, controllers, power supplies, or multifunction display and control stations. The BTP concludes that the integrability of DI&C systems makes the identification and evaluation of potential consequences of a postulated CCF more challenging.

   Integration of these two major safety systems challenges redundancy and independence, two of the main elements of defense-in-depth, and potentially degrades reliability and fail-safe operation. In addition, integrating communications significantly compromises independence and the assurance that critical data are not put in a priority chain thus compromising transmission to critical safety features. NUREG/CR-6303, "Method for Performing Diversity and Defense in Depth Analyses of Reactor Protection Systems," issued December 1994, describes defense-in-depth for NPPs and identifies the normal reactor control systems, the RTS, the ESFAS, and the reactor monitoring and indication systems as individual echelons of defense. The BTP sections discussing the combining or integrating of the RTS and ESFAS and associated communications architectures into a single protection system should ensure that reviewers verify their redundant and independent architectures are maintained.

2. In the November 2019 version of the draft BTP, Section B.2.2, emphasized that interconnections between High Safety-Significance systems and those of Lower Safety-Significance should be accomplished through the use of one-way digital communication devices rather than bi-directional communication devices which reduce independence and defense-in-depth to ensure that failures in lower significance systems do not compromise High Safety-Significance systems. This emphasis has been deleted in all later versions of the draft BTP. Instead, the BTP states that per SECY-18-0090, "Plan for Addressing Potential Common Cause Failure in Digital Instrumentation and Controls," a D3 assessment is used to demonstrate "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." The SECY makes no mention of communication other than the single vague word "connectivity." The October 2020 version of the draft BTP, Section B.2.1, "System Integration and Interconnectivity," should ensure that interconnections between High Safety-Significance systems and those of Lower Safety-Significance are one-way, uni-directional digital communication devices rather than bi-directional communication devices. One-way

digital communications between High Safety-Significance systems and Lower Safety-Significance systems is key to maintaining redundancy and independence and is a critical defense-in-depth attribute and defensive measure to mitigate CCFs.

SUMMARY

Revision 8 incorporates expanded discussion on the philosophy of D3. The reorganized structure and expanded content of the BTP makes it much easier to understand and use. It describes means to eliminate or mitigate the consequences of CCF from further consideration. It also defines the need to demonstrate that consequences of CCF vulnerabilities that have not been eliminated or mitigated are acceptable. However, there are several concerns as noted above and reflected in our recommendations that should be incorporated to ensure the critical defense-in-depth defensive measures of redundancy and independence to eliminate and mitigate CCFs are not compromised.

Sincerely,

Matthew W. Sunseri

Digitally signed by Matthew W. Sunseri
Date: 2020.11.23 22:06:47 -05'00'

Matthew W. Sunseri
Chairman

REFERENCES

1. NUREG-0800 Standard Review Plan (SRP) - Chapter 7, Branch Technical Position (BTP) 7-19, Rev. 8, “Guidance for Evaluation of Diversity and Defense in Depth in Digital Computer-Based Instrumentation and Control System,” October 2020 (ML20293A299)

2. NUREG-0800 Standard Review Plan (SRP) - Chapter 7, Branch Technical Position (BTP) 7-19, Rev. 8, “Guidance for Evaluation of Diversity and Defense in Depth in Digital Computer-Based Instrumentation and Control System,” August 2020 (ML20237F570)

3. SRM on SECY-93-087, “Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced LWR Designs,” July 21, 1993 (ML003708056)

4. SECY-18-0090, “Plan for Addressing Potential Common Cause Failure in Digital Instrumentation and Controls,” September 12, 2018 (ML18179A066)

5. NUREG/CR – 6303, “Method for Performing Diversity and Defense - in - Depth Analyses for Reactor Protection Systems,” December 1994 (ML071790509)

6. U.S. Nuclear Regulatory Commission, Regulatory Issue Summary (RIS) 2002-22, Supplement 1, “Clarification on Endorsement of NEI Guidance in Designing Digital Upgrades in I&C Systems,” Revision 1, May 31, 2018 (ML18143B633)

7. U.S. Code of Federal Regulations (CFR), “Domestic Licensing of Production and Utilization Facilities,” Part 50, Chapter 1, Title 10, “Energy” (10 CFR Part 50), Section 59, “Changes, tests and experiments”

November 23, 2020

SUBJECT: FINAL DRAFT REVISION 8 OF STANDARD REVIEW PLAN BRANCH TECHNICAL POSITION 7-19, “GUIDANCE FOR EVALUATION OF DEFENSE-IN-DEPTH AND DIVERSITY TO ADDRESS COMMON CAUSE FAILURE DUE TO LATENT DEFECTS IN DIGITAL SAFETY SYSTEMS”

Accession No: **ML20328A157** **Publicly Available Y** **Sensitive N**
Viewing Rights: ☒ NRC Users or □ ACRS Only or □ See Restricted distribution *via email

OFFICE	**ACRS/TSB**	**SUNSI Review**	**ACRS/TSB**	**ACRS**	**ACRS**
NAME	CAntonescu (LB for)	CAntonescu (LB for)	LBurkhart	SMoore (SWM)	MSunseri
DATE	11/18/2020	11/18/2020	11/18/2020	11/19/2020	11/23/2020

OFFICIAL RECORD COPY