U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Branch Technical Position 7-19 Draft Revision 8

Advisory Committee on Reactor Safeguards

Subcommittee Meeting

NRC Staff Presentation

November 21, 2019

Agenda

- Background on Commission's Common Cause Failure (CCF) Policy
- Objective of Branch Technical Position (BTP) 7-19 Modifications
- Key Changes:
  - Categorization Scheme and Graded Approach
  - Defense-in-Depth and Diversity (D3) Assessment
  - Means to Eliminate CCF from Further Consideration
  - Qualitative Assessment
  - Spurious Operation Assessment
  - Re-structuring of BTP

Objective

- Present the modifications proposed for the next draft of BTP 7-19 regarding the review of license applications and amendments addressing CCFs due to latent software defects
- Obtain ACRS Subcommittee feedback for draft BTP-19, Revision 8

Background: Commission's Policy on CCF

- SRM-SECY-93-087 presents the Commission's policy on how potential CCFs should be addressed in DI&C systems
- Provides four positions for addressing potential CCFs
  - Perform D3 assessment to demonstrate that vulnerabilities to CCF have been adequately addressed
  - Analyze each postulated CCF for each event evaluated in the SAR accident analysis using best estimate methods
  - If the assessment shows a CCF could disable a safety function, provide a diverse means with a documented basis that the diverse means is unlikely to be subject to the same CCF
  - Provide a set of diverse displays and controls located in the main control room for manual, system-level actuation of critical safety functions and monitoring of critical plant parameters to support the performance of these safety functions

Background: SECY-18-0090

- SECY-18-0090 clarifies the application of the Commission's direction in the four positions within SRM-SECY-93-087
  - Recognizes significant effort has been applied to the development of highly reliable DI&C systems but residual faults within digital systems may lead to CCFs
  - Provides five guiding principles for updating the staff's guidance for addressing CCF

Summary of Draft BTP 7-19 Changes

- Incorporates the guiding principles from SECY 18-0090 Alignment
- Clarifies the applicability of the D3 assessment to safety-related systems with high safety significance
- Incorporates qualitative assessment criteria from Supplement 1 to RIS 2002-22 for non-RPS/ESFAS
- Clarifies staff positions on means to address CCF
- Provides additional guidance on spurious operation assessment
- Improves the structure of the BTP to enhance ease of use

Key Changes: Categorization Scheme and Graded Approach

	Safety-Related	NSR
Safety Significant—Significant contributor to plant safety	**A1** Perform D3 Assessment	**B1** Perform Qualitative Assessment
Not Safety Significant—Not a significant contributor to plant safety	**A2** Perform Qualitative Assessment	**B2**

Deterministic Criteria for Categorization of DI&C Systems (1)

- A1: safety-related DI&C system that:
  - Is relied upon to initiate and complete control actions essential to maintain plant parameters within acceptable limits established for a DBE, or
  - Whose failure could directly lead to accident conditions that may cause unacceptable consequences if not mitigated by other A1 systems
- A2: safety-related DI&C system that:
  - Provides an auxiliary or indirect function in the achievement or maintenance of plant safety, or
  - Maintains the plant in a safe shutdown state after the plant has reached initial safe shutdown state

Deterministic Criteria for Categorization of DI&C Systems (2)

- B1: NSR DI&C that:
  - Directly controls the reactivity or power level of the reactor, or
  - Whose failure may result in unacceptable consequences to plant safety due to integration of multiple control functions into a single system
- B2: NSR DI&C system that:
  - Does not have direct affect on reactivity or power level of the reactor, or
  - Whose failure does not have consequences to plant safety or whose failure can be detected and mitigated with significant safety margin

Use of Risk Insights to Support Categorization

- Risk insights can be used to support the safety-significance determination in categorizing the DI&C system in terms of safety consequences from site-specific PRAs
- Use of risk insights should be an input to an integrated decision-making process for categorizing the proposed DI&C system

Key Changes: D3 Assessment

- D3 assessment should be performed for A1 systems
- D3 assessment includes determination of whether:
  - CCF vulnerability is eliminated from further consideration by use of design attributes, testing, or defensive measures;
  - A diverse means can be used to perform the same or different function than the safety function disabled by the postulated CCF; or
  - Consequence of a DBE concurrent with a CCF of the A1 system is acceptable
- For systems that are not A1 but are integrated with A1 systems, the D3 assessment should be performed on the integrated system unless it can be shown that the non-A1 system will not adversely impact the A1 system upon a postulated CCF

Key Changes: Means to Eliminate CCF from Further Consideration (1)

- Use of design attribute: diversity within the DI&C system or component
  - Provides guidance to use diversity within each safety division or among redundant divisions to address CCF
  - Calls for an analysis to demonstrate sufficient diversity exists in the design, so it is not subject to the same CCF
  - Provides acceptance criteria for use of this attribute

Key Changes: Means to Eliminate CCF from Further Consideration (2)

- Use of testing to demonstrate latent defects are not present
  - Clarifies criteria and terminology associated with use of testing to eliminate CCF from further consideration
  - Emphasizes the limitations on use of testing
  - Provides guidance to establish test methods
  - Provides acceptance criteria

Key Changes: Means to Eliminate CCF from Further Consideration (3)

- Use of defensive measures
  - Provides guidance to use defensive measures to prevent, limit, or mitigate the effects of a potential CCF to eliminate CCF from consideration
  - Provides criteria to use defensive measures based on an NRC-approved methodology
  - Provides criteria for use of other methodologies with the provision of a technical basis and acceptance criteria

Key Changes: Diverse Means (1)

- Clarifies guidance on the use of diverse means to perform the same or different function as the safety function disabled by the postulated CCF
- Clarifies the types of diverse means that can be credited
  - Existing systems
  - Manual operator actions
  - Diverse system
- Identifies acceptance criteria

Key Changes: Diverse Means (2)

- Provides guidance on the use of equipment outside the main control room for the performance of manual operator actions
  - Applies only for use of diverse means to address Position 3 in the SRM-SECY-93-087
- Clarifies guidance to address Position 4 in SRM-SECY-93-087, which calls for manual controls and indications located in the MCR to perform manual system level actuation of critical safety functions

Key Changes: Qualitative Assessment

- Provides guidance for performing a qualitative assessment to evaluate potential CCFs and their effects in A2 and B1 systems
- Identifies three factors can be used to show that the likelihood of CCF is sufficiently low, including:
  - Design attributes
  - Design quality
  - Operating experience
- Provides guidance on the performance of a qualitative assessment on a B2 system that could place the plant in an unanalyzed condition
  - Basis for not performing an assessment should be documented

Key Changes: Spurious Operation Assessment

- Provides bifurcated criteria for addressing spurious operation of SSCs due to a CCF in a DI&C system
- Provides guidance for operating reactors for performing an assessment to demonstrate that the safety analysis of spurious operations is not invalidated by the proposed digital modification
- Provides guidance for new and advanced reactors for performing an assessment to demonstrate that potential spurious operation of SSCs is bounded by events analyzed in the safety analysis
- Clarifies scope and methods for performing the assessment, including use of design attributes, testing, and defensive measures to eliminate CCF from further consideration

Key Changes: Re-Structuring of BTP 7-19

- Simplifies background and incorporates new guidance on CCF
  - SECY-18-0090
  - NUREG/CR 7007
  - RIS 2002-22, Supplement 1
- Maps criteria to four positions in the SRM-SECY-93-087
- Consolidates CCF guidance and corresponding acceptance criteria

Next Steps

- Public comment period ends in February 2020
- Potential public meeting during public comment period to facilitate comments
- Potential second ACRS Subcommittee meeting in Spring 2020 if changes resulting from public comment period are significant
- ACRS Full Committee meeting in Spring 2020
- OMB review and publication of final BTP 7-19, Revision 8 anticipated in 3rd Quarter 2020

Questions

Questions

Acronyms

BTP	Branch Technical Position	NSR	Not safety related
CCF	Common Cause Failure	PRA	Probabilistic Risk Assessment
CFR	Code of Federal Regulations	RIS	Regulatory Issue Summary
D3	Defense-in-Depth and Diversity	RPS	Reactor Protection System
DI&C	Digital Instrumentation and Control	SAR	Safety Analysis Report
ESFAS	Engineered Safety Feature Actuation System	SRM	Staff Requirements Memorandum
MCR	Main Control Room	SSC	Structure, System and component
MP	Modernization Project		

Background Information

Modernization Plans (MPs)

- Developed in accordance with Staff Requirements Memorandum (SRM) to SECY-16-0070
- MP#1 – Common Cause Failure
  - MP#1A: Supplement 1 to RIS 2002-22
  - MP#1D: Update to BTP 7-19
- MP#2 – 10 CFR 50.59 Guidance
- MP#3 – Commercial Grade Dedication
- MP#4A – ISG-06 Revision
- MP#4B – Broader Modernization Activities

SECY-18-0090 – Five Guiding Principles

1. Applicants and licensees for Production and Utilization Facilities under 10 CFR Part 50, “Domestic Licensing of Productions and Utilization Facilities” or under 10 CFR Part 52, “Licensees, 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-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.

Five Guiding Principles continued

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 through 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.

SRM to SECY-93-087

1. The applicant shall assess the defense-in-depth and diversity of the proposed instrumentation and control system to demonstrate that vulnerabilities to common-mode failures have adequately been addressed.
2. In performing the assessment, 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 (SAR) using best-estimate methods. The vendor or applicant shall demonstrate adequate diversity within the design for each of these events.
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 nonsafety system if the system is of sufficient quality to perform the necessary function under the associated event conditions.
4. A set of displays and controls located in the main control room shall be provided for manual, system-level actuation of critical safety functions and monitoring of parameters that support the safety functions. The displays and controls shall be independent and diverse from the safety computer system identified in Items 1 and 3 above.

Graded Approach for Systems Categorization Concept

	Safety-Related	Non-Safety Related
Safety Significant	A1 (e.g. Protection System, Safety Control Systems*, Load Sequencers*)	B1 (e.g. Rod Control System, Feedwater Control system, Certain BOP Control Systems)
Not Safety Significant	A2 (e.g. Safety Chillers, Safety Control Systems*, Load Sequencers*)	B2 (e.g. Plant Computer, Service Water System Controls)

*The staff recognizes actual categorization may be driven by specific plant system configurations, the exact nature in which systems may be interconnected by digital equipment, and the plant's licensing basis. Systems that depend on the overall plant design may be safety significant or non-safety significant.