



Expansion of Current Policy Regarding Potential Common-Cause Failures in Digital Instrumentation and Control Systems

**Advisory Committee on Reactor Safeguards
Digital Instrumentation & Controls Subcommittee Briefing
May 20, 2022**

Technical Staff Presenters

- **Samir Darbali** – Electronics Engineer, NRR/DEX
- **Norbert Carte** – Senior Electronics Engineer, NRR/DEX
- **Steven Alferink** – Reliability and Risk Analyst, NRR/DRA

Digital I&C Project Managers

- **Bhagwat Jain** – Senior Project Manager, NRR/DORL
- **Michael Marshall** – Senior Project Manager, NRR/DORL

Working Group Members

- **NRR/DEX**
 - Norbert Carte
 - Samir Darbali
- **NRR/DRA**
 - Steven Alferink
 - Shilp Vasavada
 - Sunil Weerakkody
- **NRR/DSS**
 - Charley Peabody
- **NRR/DORL**
 - Bhagwat Jain
- **OGC**
 - Sheldon Clark
- **RES/DE**
 - Sergiu Basturescu
- **Additional NRR/DEX and DORL Support**
 - Wendell Morton
 - Ming Li
 - Michael Marshall
 - Khoi Nguyen
 - David Rahn
 - Richard Stattel
 - Michael Waters
 - Steve Wyman

Presentation Outline

- Introduction and Key Messages
- Background
- Subject and Purpose
- Proposed Expanded Policy
 - Current Path
 - Risk-Informed Path
- Status of Draft SECY Paper and Next Steps

Introduction

- Nuclear power plants continue to install digital I&C technology
 - Increased reliability and safety benefits
 - Can introduce new types of types of potential systematic, nonrandom, concurrent failures of redundant elements (i.e., CCFs)
- SRM-SECY-93-087 directs that, if the D3 assessment shows that a postulated CCF could disable a safety function, then a diverse means be provided to perform that safety function or a different function
 - Diverse means may include manual actions
 - The current policy does not allow for the use of a risk-informed approach to determine specific circumstances that would not require a diverse means for addressing DI&C CCFs
- The staff is developing a SECY paper that will provide recommended language for an expanded policy, which allows greater use of risk-informed approaches to address DI&C CCFs

Key Messages

- The expanded policy will encompass the current points of SRM-SECY-93-087 (with clarifications) and expand the use of risk-informed approaches
- Any use of risk-informed approaches will be expected to be consistent with the Safety Goal Policy Statement, PRA Policy Statement, and SRM-SECY-98-0144
- The current DI&C CCF policy will continue to remain a valid option for licensees and applicants

Background – Early Concerns with CCFs

- Early concerns with CCFs
 - CCFs have been an NRC concern since the mid-1960s
 - In the early 1990s, the introduction of DI&C became a concern as a new source for introducing CCFs, as explained in SECY-91-292
- Current DI&C CCF policy
 - The NRC’s current DI&C CCF policy is expressed in various documents, including SRM-SECY-93-087; SECY-18-0090; and BTP 7-19, Revision 8
- Current state of DI&C in the nuclear power industry
 - Design development practices and quality assurance tools have evolved
 - DI&C CCFs remains a serious area of concern

Background – Use of Risk-Information

- Increased use of risk-informed decision making
 - The staff is following the PRA Policy Statement and SRM-SECY-98-144 to expand risk-informed decision making
- Modernizing the DI&C regulatory infrastructure
 - SRM-SECY-16-0070 approved implementation of the staff’s integrated action plan to modernize the NRC’s DI&C regulatory infrastructure
 - The staff issued guidance on risk-informed, graded approaches to address DI&C CCFs for low safety significant systems (e.g., BTP 7-19 and RIS 2002-22, Supplement 1)
 - The staff believes this is an appropriate time to expand the current policy on DI&C CCFs to include the use of risk-informed approaches

SECY Paper Subject and Purpose

- **SUBJECT**

- Expansion of Current Policy Regarding Potential CCFs in DI&C Systems

- **PURPOSE**

- Provide the Commission a recommendation on expanding the current policy to include the use of risk-informed approaches for addressing DI&C CCFs

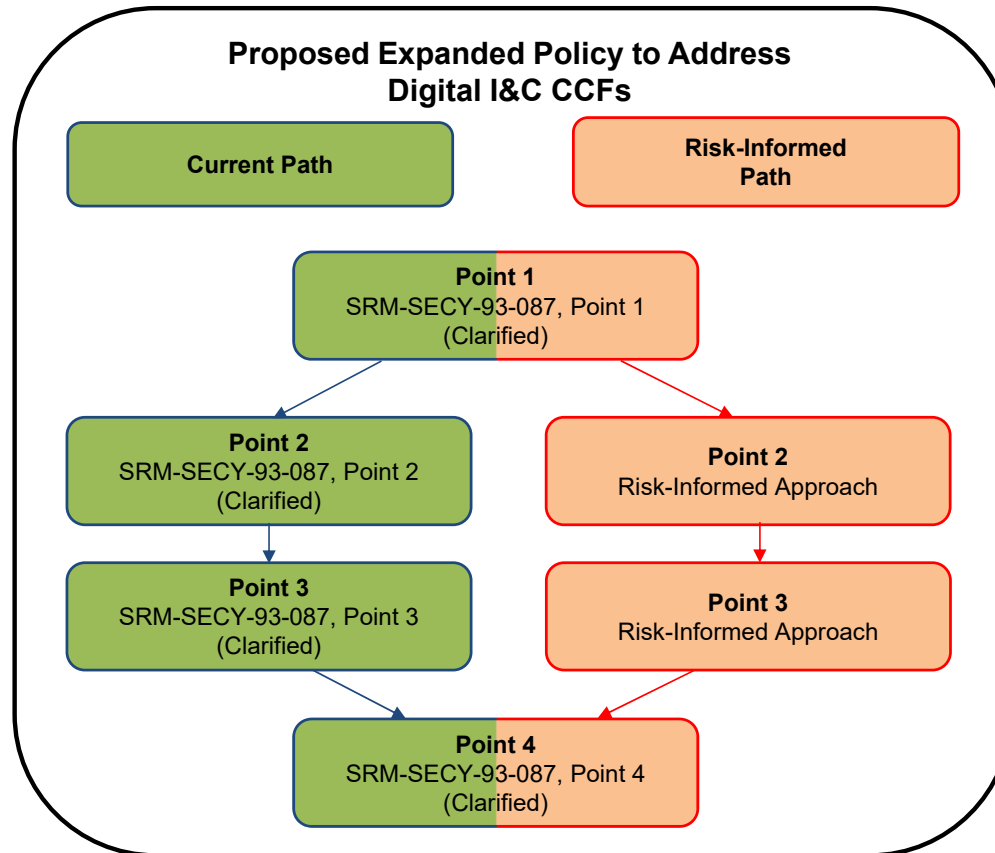
- The recommended expanded policy will encompass the current positions in SRM-SECY-93-087 and the use of risk-informed approaches to determine the appropriate level of defense-in-depth and diversity to address DI&C CCFs

Proposed Expanded Policy to Address DI&C CCFs

- A **single expanded policy** that encompasses the current position in SRM-SECY-93-087 and provides for risk-informed approaches to address DI&C CCFs
- The expanded policy includes:
 - 1) Position in points 1, 2, and 3 of SRM-SECY-93-087 with appropriate clarifications and corrections from SECY-18-0090
 - 2) Position in point 4 of SRM-SECY-93-087 with appropriate clarifications
 - 3) The addition of risk-informed approaches to points 2 and 3 of SRM-SECY-93-087
- The expanded policy provides for:
 - 1) The deterministic demonstration of adequate diversity
 - 2) Risk-informed approaches

Proposed Expanded Policy to Address DI&C CCFs

The Current Path allows for the use of best estimate analysis and diverse means to address a potential DI&C CCF



The Risk-Informed Path allows for the use of risk-informed approaches and other design techniques or measures other than diversity to address a potential DI&C CCF

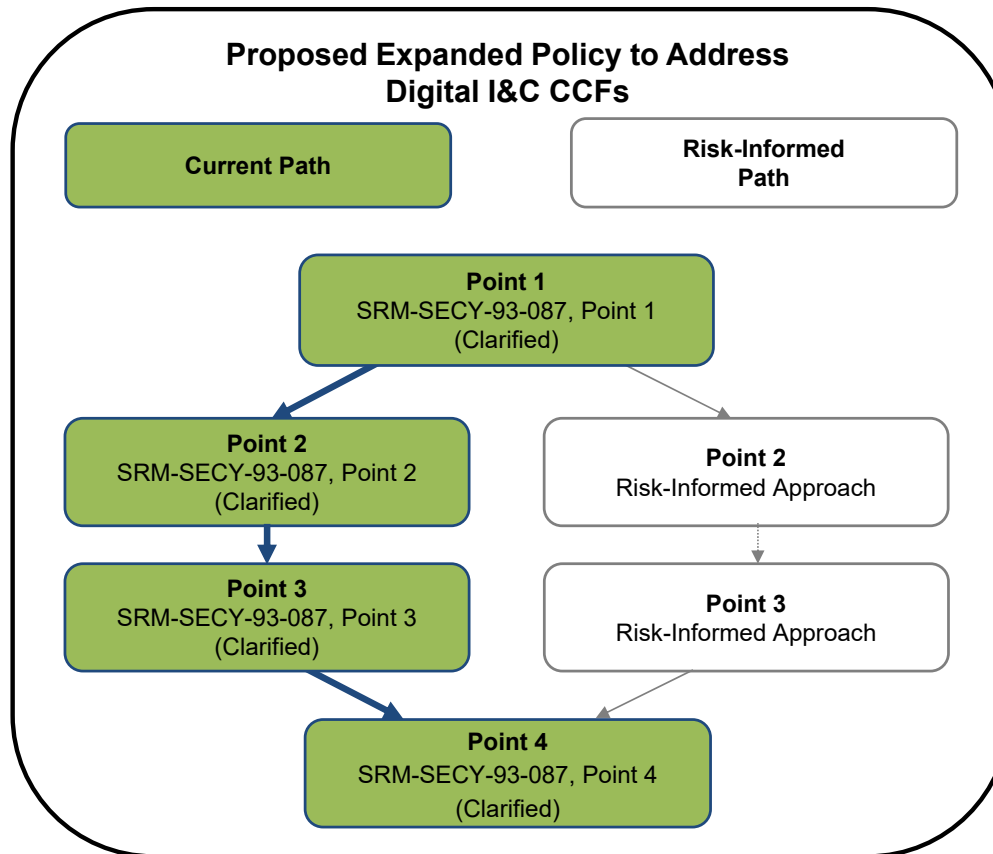
Current Path

Current Path

- The current policy continues to be a viable option to address DI&C CCFs
- The current four points in SRM-SECY-93-087 will remain as a viable path to licensees and applicants:
 - **Point 1** – “... assess the defense-in-depth and diversity of the proposed I&C system to demonstrate that vulnerabilities to common-mode failures have adequately been addressed.”
 - **Point 2** – “... 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... demonstrate adequate diversity within the design for each of these events.”
 - **Point 3** – “If 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.”
 - **Point 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...”
- SECY-18-0090 provides guiding principles for the application of policy, which were used in the development of BTP 7-19, Revision 8

Proposed Expanded Policy – Current Path

The Current Path allows for the use of best estimate analysis and diverse means to address a potential DI&C CCF

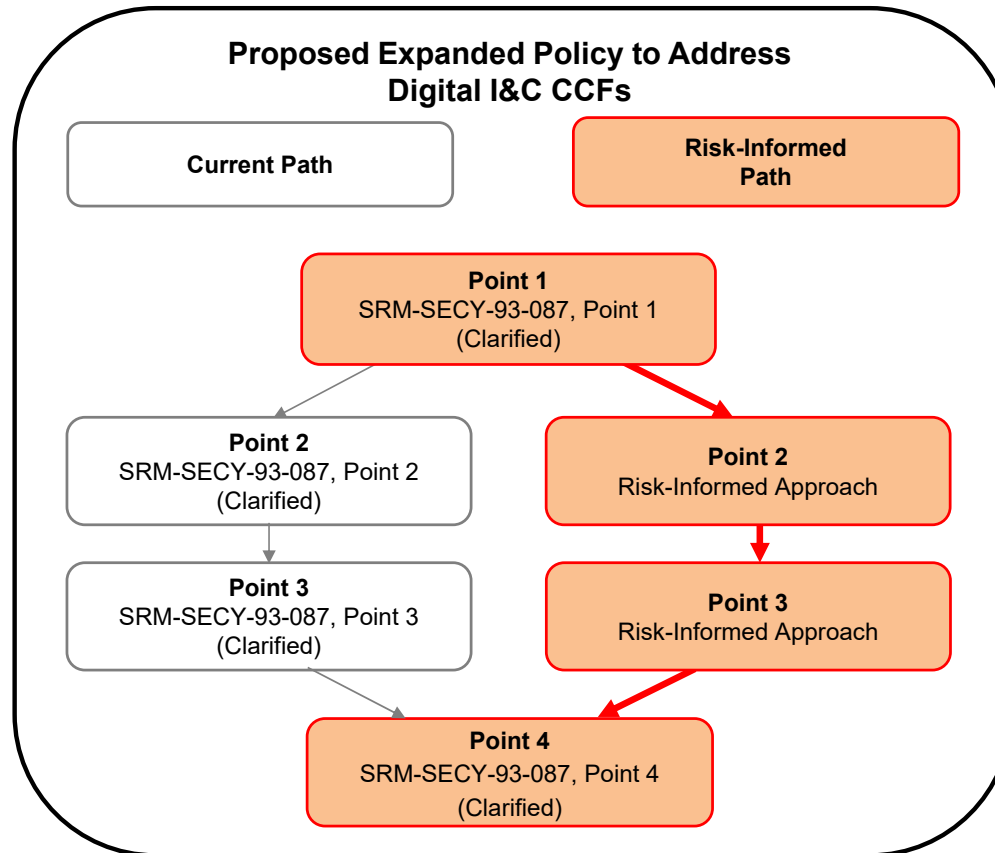


Clarifying the Current Policy Language

- Replacing “common-mode failure” with “common-cause failure”
 - The current language in SRM-SECY-93-087 points 1, 2, and 3 uses the term “common-mode failure” when the intent and implementation is “common-cause failure”
- Adding “facility” where appropriate
 - The current language in SRM-SECY-93-087 points 1 and 2 focuses on the proposed I&C system, when the NRC’s concern is on the defense-in-depth and diversity of the facility incorporating the DI&C system
- Adding “defense-in-depth” where appropriate
 - The current language in SRM-SECY-93-087 point 2 focuses on demonstrating adequate diversity, when the intent and implementation includes defense-in-depth

Risk-Informed Path

Proposed Expanded Policy – Risk-Informed Path



The Risk-Informed Path allows for the use of risk-informed approaches and other design techniques or measures other than diversity to address a potential DI&C CCF

SRM-SECY-93-087, Point 1 in the Risk-Informed Path

- Point 1 does not preclude the use of risk-informed approaches for the D3 assessment
- Existing policy and guidance support a graded approach and applying a level of rigor for the D3 assessment commensurate with the safety significance of the proposed DI&C system or component

SRM-SECY-93-087, Point 4 in the Risk-Informed Path

- Point 4 is consistent with current regulations that effectively require diverse and independent displays and controls
 - 10 CFR 50.55a(h) incorporates by reference IEEE Std 279 and IEEE Std 603-1991, 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
 - 10 CFR Part 50, Appendix A, General Design Criterion 22 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.”
- Risk-informed approach to point 4 would not provide appreciable benefits

SRM-SECY-93-087, Point 2 in the Risk-Informed Path

- Current approach focuses on consequences
- The staff considers this an appropriate area for risk-informing the evaluation of postulated DI&C CCFs
- The staff's goal is that risk-informed approaches will be consistent with all five principles of risk-informed decision making, as listed in RG 1.174

SRM-SECY-93-087, Point 3 in the Risk-Informed Path

- Current approach only provides one way of addressing undesirable outcomes (i.e., diverse means)
- The staff considers this an appropriate area for evaluating design measures other than diversity to reduce the risk from a DI&C CCF
- The staff's goal is to apply a graded approach for the level of justification needed for design techniques or measures other than diversity
- Diverse means will continue to be acceptable

Benefits of Risk-Informed Approaches

- Risk-informed approaches can provide flexibility to address DI&C CCFs and are consistent with the PRA Policy Statement
- Risk-informed approaches can have different levels of PRA use
- Risk-informed approaches could support a graded approach for addressing DI&C CCFs in high safety significant systems
- PRA models could be used to systematically assess the need to reduce the risk introduced by the DI&C system
- Risk-informed approaches can identify initiators or scenarios where lack of DI&C diversity does not compromise safety

Guiding Principles for Implementation

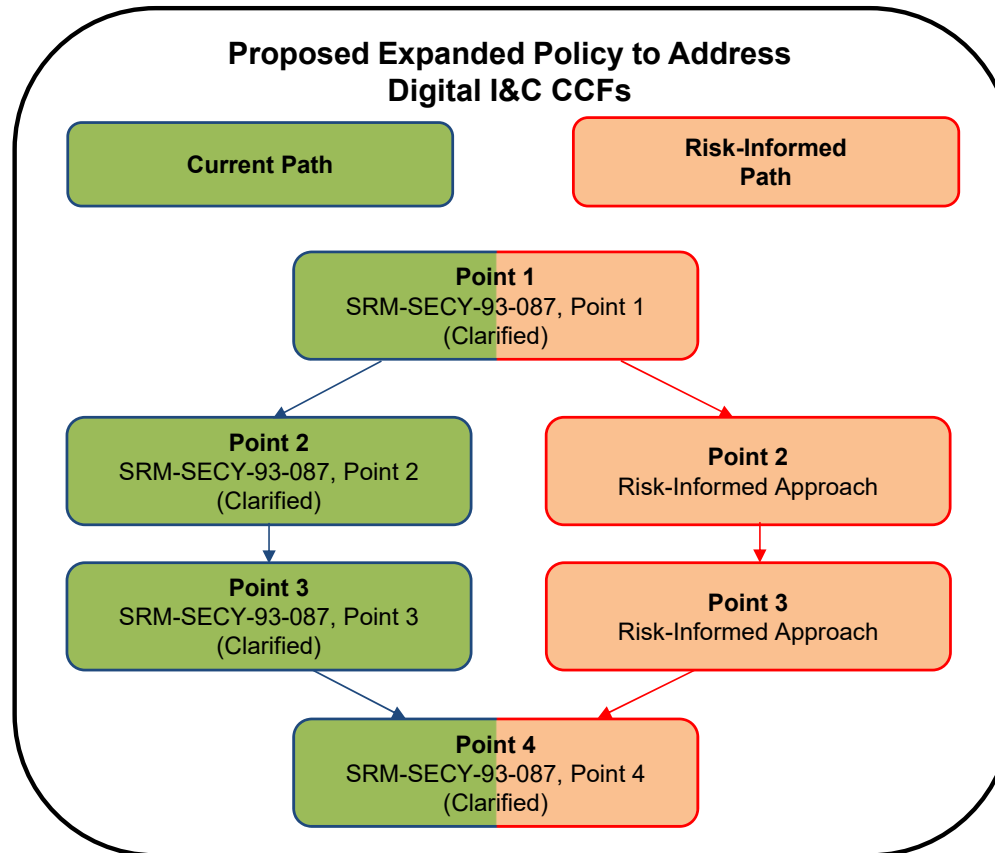
- The expanded policy will not conflict with existing regulatory requirements
 - A rule change or exemption will not be required to implement it
- The expanded DI&C CCF policy will be implemented consistent with the Commission's 1995 PRA Policy Statement, SRM-SECY-98-0144, and the current agency focus on expanding risk-informed decision making
- Implementation of the expanded DI&C CCF policy will continue to provide reasonable assurance of adequate protection of public health and safety

Guiding Principles for Implementation (contd.)

- The use of risk-informed approaches will be consistent with all five principles of risk-informed decision making, as listed in RG 1.174
- PRAs used for risk-informed approaches will be technically acceptable (e.g., meet the guidance in RG 1.200) and include an effective PRA configuration control and feedback mechanism

Proposed Expanded Policy to Address DI&C CCFs

The Current Path allows for the use of best estimate analysis and diverse means to address a potential DI&C CCF



The Risk-Informed Path allows for the use of risk-informed approaches and other design techniques or measures other than diversity to address a potential DI&C CCF

Key Messages

- The expanded policy will encompass the current points of SRM-SECY-93-087 (with clarifications) and expand the use of risk-informed approaches
- Any use of risk-informed approaches will be expected to be consistent with the Safety Goal Policy Statement, PRA Policy Statement, and SRM-SECY-98-0144
- The current DI&C CCF policy will continue to remain a valid option for licensees and applicants

Status of Draft SECY Paper and Next Steps

- The draft SECY is currently being developed
- A public outreach meeting is planned for June 2022
- The staff plans to send the SECY paper to the Commission in 2022
- Upon approval of an expanded policy, the staff will proceed to update the implementation guidance in BTP 7-19

Questions?

Acronyms

BTP	Branch Technical Position	NRC	Nuclear Regulatory Commission
CCF	Common Cause Failure	OEDO	Office of the Executive Director for Operations
D3	Defense-in-Depth and Diversity	PRA	Probabilistic Risk Assessment
DI&C	Digital Instrumentation and Control	RG	Regulatory Guide
ESFAS	Engineered Safety Features Actuation System	RIS	Regulatory Issue Summary
GDC	General Design Criteria	RPS	Reactor Protection System
IAP	Integrated Action Plan	SAR	Safety Analysis Report
I&C	Instrumentation and control	SECY	Commission Paper
MP	Modernization Plan	SRM	Staff Requirements Memorandum
NEI	Nuclear Energy Institute		