U.S.NRC

United States Nuclear Regulatory Commission

Protecting People and the Environment

Expansion of Current Policy to Address 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
- Industry Proposal
- Status of Draft SECY Paper and Next Steps

Introduction

- 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 CCF
- The SECY paper will provide recommended language for an expanded policy, which allows risk-informed approaches to address 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 need 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 CCF

- Early concerns with CCF
  - CCF has 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 CCF, 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 – Risk-Informing DI&C CCF

- 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 CCF for low safety significant safety 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 CCF to include the use of risk-informed approaches

SECY Paper Subject and Purpose

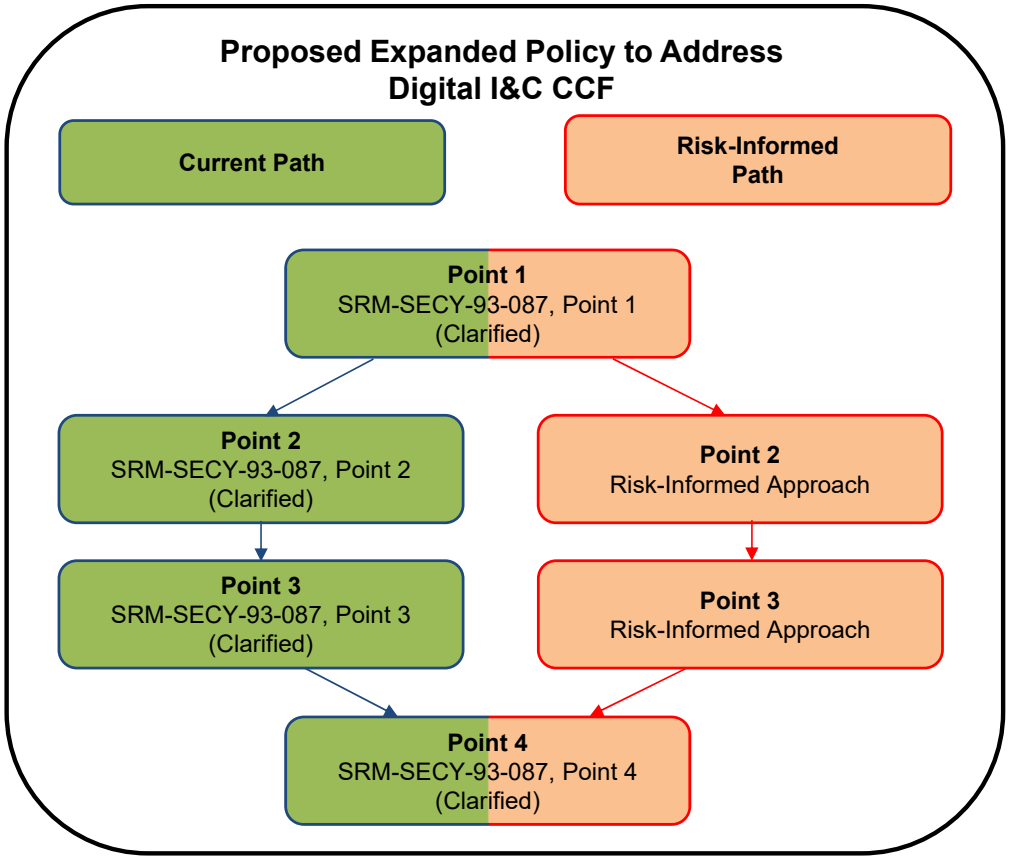
- **SUBJECT**
  - Expansion of Current Policy to Address Potential Common-Cause Failures in Digital Instrumentation and Control Systems
- **PURPOSE**
  - Provide the Commission a recommendation on expanding the current policy to include the use of risk-informed approaches for addressing DI&C CCFs
  - 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 CCF

Proposed Expanded Policy to Address DI&C CCF

- A **single expanded policy** that encompasses the current positions in SRM-SECY-93-087 and provides for risk-informed approaches to address DI&C CCF
- The expanded policy includes:
  1) Positions in points 1, 2, and 3 of SRM-SECY-93-087 with appropriate clarifications and corrections from SECY-18-0090
  2) Language 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 CCF

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 defensive measures other than diversity to address a potential DI&C CCF.

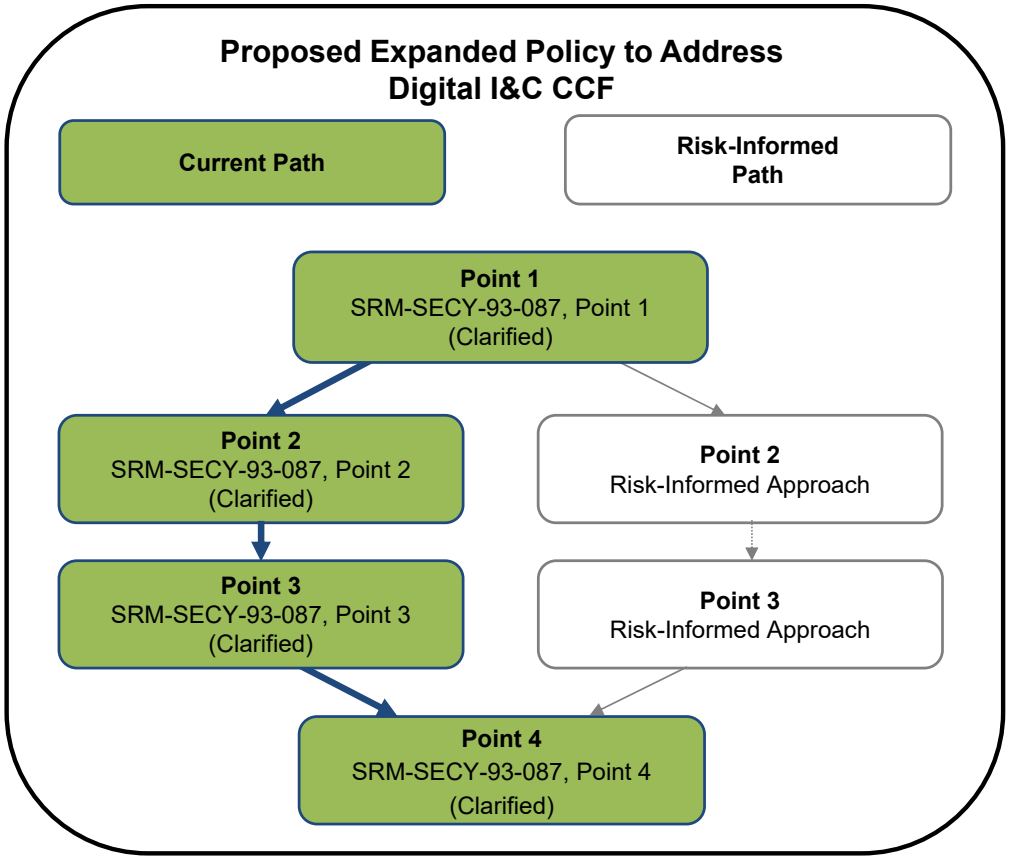
Current Path

Current Path

- The current policy continues to be a viable option to address DI&C CCF
- 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 clarifies the application of the four SRM-SECY-93-087 points and provides guiding principles that were used in the development of BTP 7-19, Rev. 8

Proposed Expanded Policy – Current Path

The 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

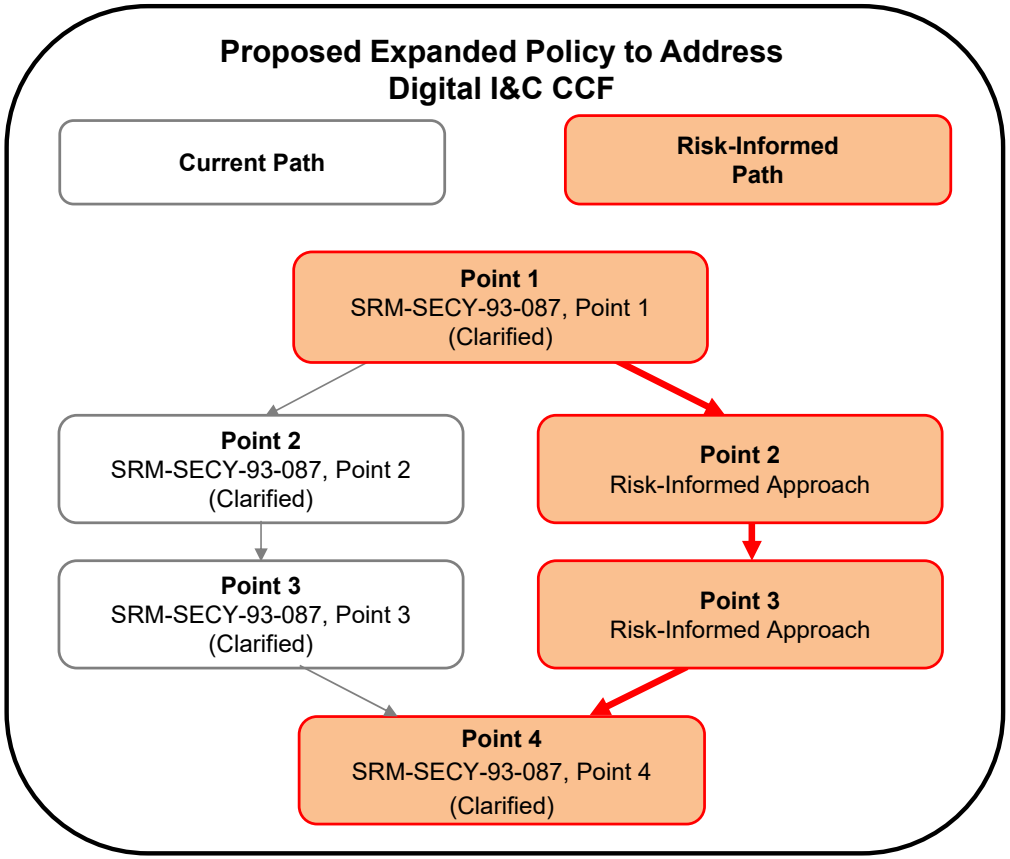
Guiding Principles for Implementation

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

Guiding Principles for Implementation (contd.)

- Applicants will need to address all five principles of risk-informed decision making, as listed in RG 1.174
- A systematic approach is used to evaluate DI&C failure causes during operation and maintenance, including inappropriate software behavior
- A PRA used for risk-informed approaches needs to be technically acceptable (e.g., meets the guidance in RG 1.200) and include an effective PRA configuration control and feedback mechanism

Proposed Expanded Policy – Risk-Informed Path



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

SRM-SECY-93-087, Points 1 and 4 in the Risk-Informed Path

- SRM-SECY-93-087, **Point 1**:
  - It does not preclude the use of risk-informed approach for the D3 evaluation
  - 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**:
  - Regulations effectively require diverse and independent displays and controls
  - Risk-informed approach to point 4 would not provide noticeable benefits

Risk-Informing the positions in SRM-SECY-93-087

Point 2

- Current approach focuses on consequences
- The staff considers this an appropriate area for risk-informing the evaluation of postulated DI&C CCFs
- A risk-informed approach can identify initiators or scenarios where lack of DI&C diversity does not compromise safety

Risk-Informing the Positions in SRM-SECY-93-087

Point 3

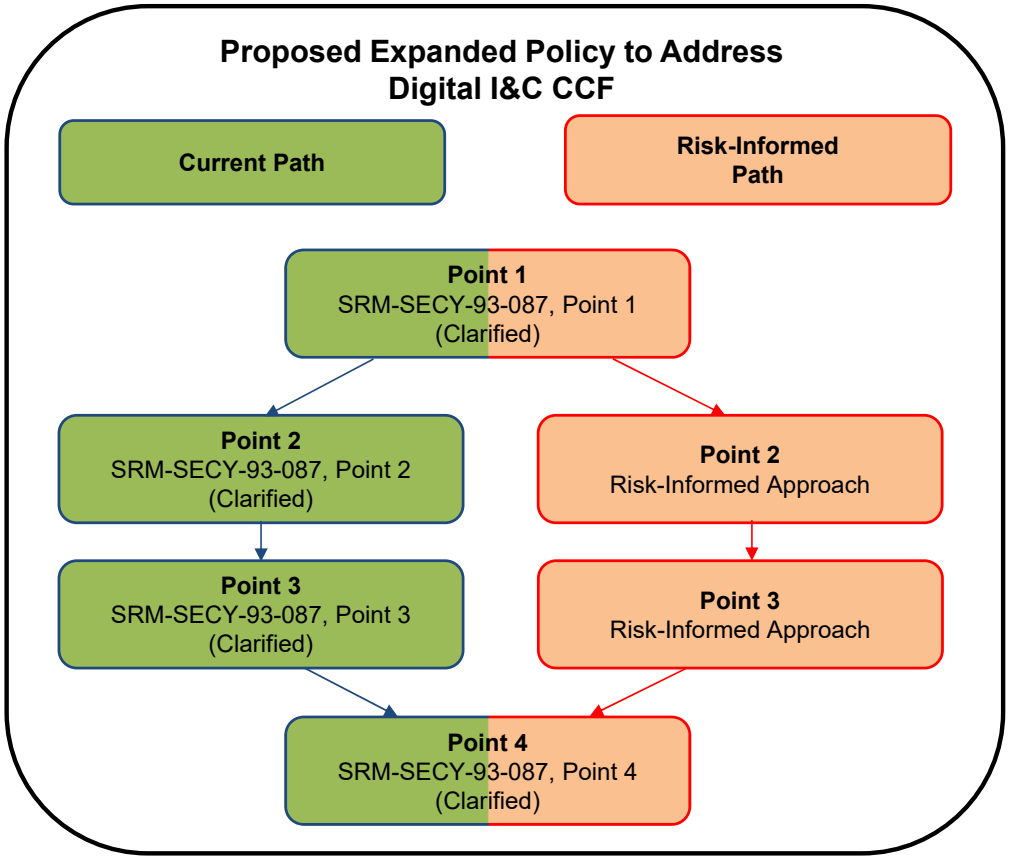
- Current approach only provides one way of addressing undesirable outcomes (i.e., diverse means)
- The staff considers this an appropriate area for evaluating design measures other than diversity to reduce the risk from a DI&C CCF

Benefits of Risk-Informed Approaches

- Risk-informed approaches can provide flexibility to address DI&C CCF and are consistent with the PRA Policy Statement
- Risk-informed approaches could support a graded approach in determining the degree of diversity that is needed
- PRA models could be used to systematically assess the need to reduce the risk introduced by the DI&C system
- Risk-informed approaches can have different levels of PRA use

Proposed Expanded Policy to Address DI&C CCF

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