IAEA Technical Meeting on Common Cause Failures in Nuclear Power Plant Instrumentation and Control Systems
6-8 December 2022

Expansion of Policy for Addressing Potential Common Cause Failures in U.S. Nuclear Power Plant Digital Instrumentation and Control Systems

Samir Darbali
Electronics Engineer
Division of Engineering and External Hazards
Office of Nuclear Reactor Regulation
U.S. Nuclear Regulatory Commission
Email: Samir.Darbali@nrc.gov

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

Outline

- Key Messages
- Background
- Current NRC Policy for Addressing Digital I&C CCFs
- Proposed Expanded Policy for Addressing Digital I&C CCFs
- Status and Next Steps
- Closing Remarks/Key Messages

Key Messages

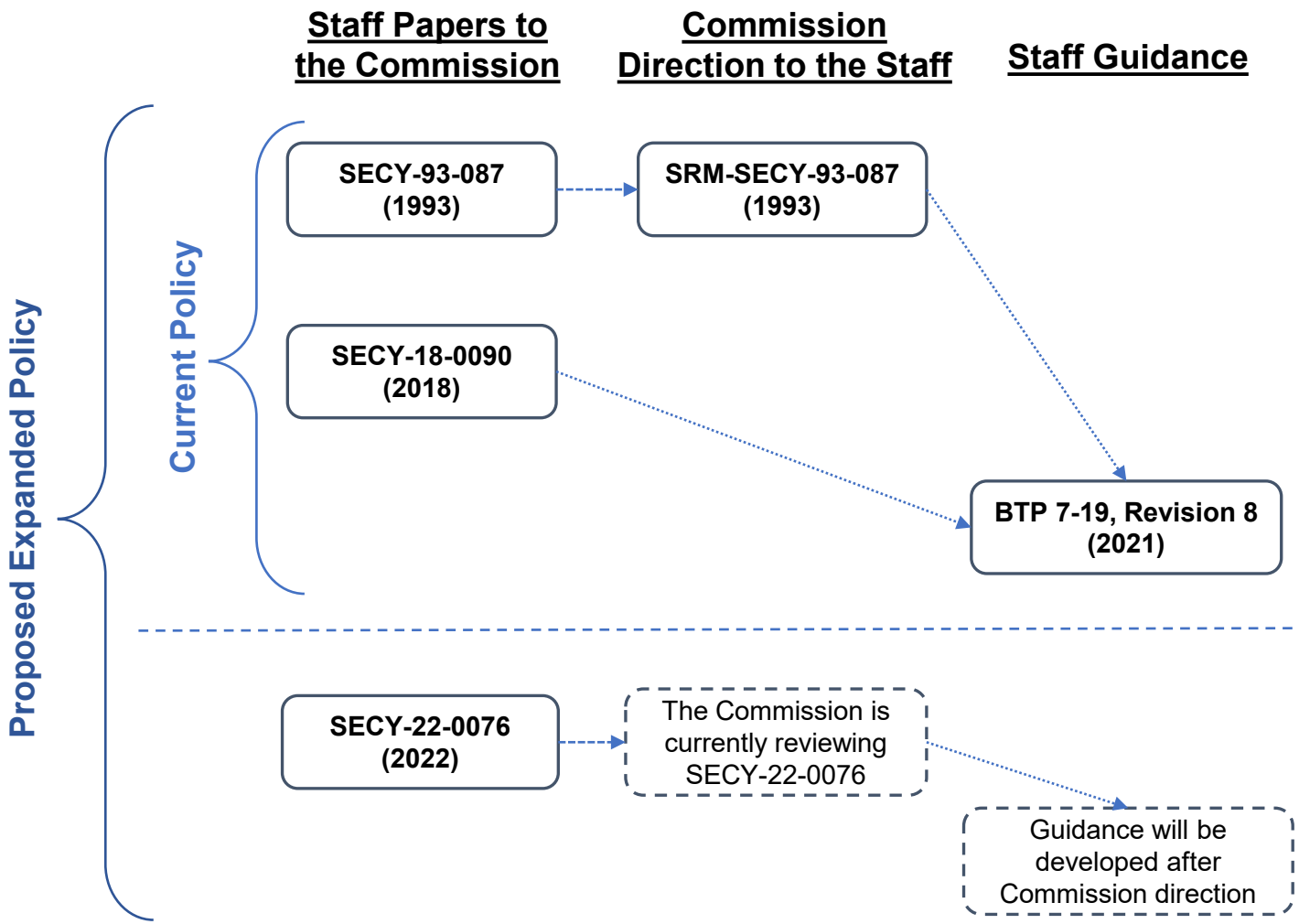
- The U.S. NRC's policy for addressing digital I&C CCFs goes back to 1993.
- The current policy has been effectively used to license digital I&C systems in nuclear power plants, but it requires a diverse means of actuation if a CCF could disable a safety function.
- The NRC staff requested the NRC Commission expand the current policy for digital I&C CCFs to allow the use of risk-informed approaches to demonstrate the appropriate level of defense-in-depth for high safety significance systems.
- The NRC staff's goal is that the acceptance criteria for risk-informed approaches for digital I&C CCFs will be consistent with established NRC practices and guidance for risk-informed decision making.
- The current policy will continue to remain a valid option for licensees and applicants.

Background

- Early Concerns with CCFs:
  - CCFs have been an NRC concern since the mid-1960s.
  - In the early 1990s, the introduction of digital I&C became a concern as a new source for introducing potential systematic, nonrandom, concurrent failures of redundant elements (i.e., CCFs).

- Current state of digital I&C in the nuclear power industry:
  - Design development practices and quality assurance tools have evolved.
  - Digital I&C CCFs remain a serious area of concern.
  - If not addressed, a digital I&C CCF can affect both the digital I&C system and manual controls and displays.

U.S. NRC's Policy to Address Digital I&C CCFs



SRM-SECY-93-087 identifies four points to address digital I&C CCFs.

SECY-18-0090 clarifies the application of the Commission's direction in the four points within SRM-SECY-93-087.

BTP 7-19 provides guidance to the staff for the evaluation of defense-in-depth and diversity to address digital I&C CCFs.

SECY-22-0076 requests the Commission expand the current policy for digital I&C CCFs to allow the use of risk-informed approaches to demonstrate the appropriate level of defense-in-depth.

U.S. NRC's Current Policy to Address Digital I&C CCFs

SRM-SECY-93-087 – "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs"

- The intent of the SRM is to address the possible negative consequences of a digital I&C CCF:
  - The loss of the safety functions performed by the digital I&C system
  - The loss of operators' ability to perform manual actions of critical safety functions (e.g., reactivity control, core heat removal, reactor coolant inventory, containment isolation, and containment integrity)

Source: https://www.nrc.gov/docs/ML0037/ML003708056.pdf

U.S. NRC's Current Policy to Address Digital I&C CCFs

SRM-SECY-93-087 (continued)

- Identifies four points to address digital I&C CCFs:
  - **Point 1** requires a defense-in-depth and diversity (D3) assessment to demonstrate that CCFs have adequately been addressed.
  - **Point 2** requires the D3 assessment analyze each postulated CCF for each event evaluated in the accident analysis using best estimate methods to demonstrate adequate diversity.
  - **Point 3** requires a diverse means of actuation (manual or automatic) if a CCF could disable a safety function.
  - **Point 4** requires diverse main control room displays and manual controls for actuation of critical safety functions.

Source: https://www.nrc.gov/docs/ML0037/ML003708056.pdf

U.S. NRC's Current Policy to Address Digital I&C CCFs

SECY-18-0090 – "Plan for Addressing Potential Common Cause Failure in Digital Instrumentation and Control"

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

Source: https://www.nrc.gov/docs/ML1817/ML18179A067.pdf

U.S. NRC's Current Policy to Address Digital I&C CCFs

Branch Technical Position (BTP) 7-19 – "Guidance for Evaluation of Defense in Depth and Diversity to Address Common-Cause Failure due to Latent Design Defects in Digital Safety Systems," Revision 8

- Provides guidance to the staff for the evaluation of defense-in-depth and diversity to address digital I&C CCFs:
  - Supports a risk-informed graded approach based on safety significance of the digital I&C system.
  - Incorporates lessons-learned from previous operating reactor and new reactor reviews.
  - Supports expanded use of defensive measures to address digital I&C CCFs.

Source: https://www.nrc.gov/docs/ML2033/ML20339A647.pdf

U.S. NRC's Approach to Risk-Informing the CCF Policy

- The current policy has been effectively used to license digital I&C systems in nuclear power plants, but it requires a diverse means of actuation if a CCF could disable a safety function.
- The NRC staff recognizes that there is an opportunity to risk-inform the current policy to address digital I&C CCFs for high safety significance systems.
- The proposed expanded policy for digital I&C CCF will not conflict with existing regulatory requirements (i.e., a rule change or exemption will not be required to implement the policy).
- Implementation of the proposed expanded policy will continue to provide reasonable assurance of adequate protection of public health and safety.

U.S. NRC's Approach to Risk-Informing the CCF Policy

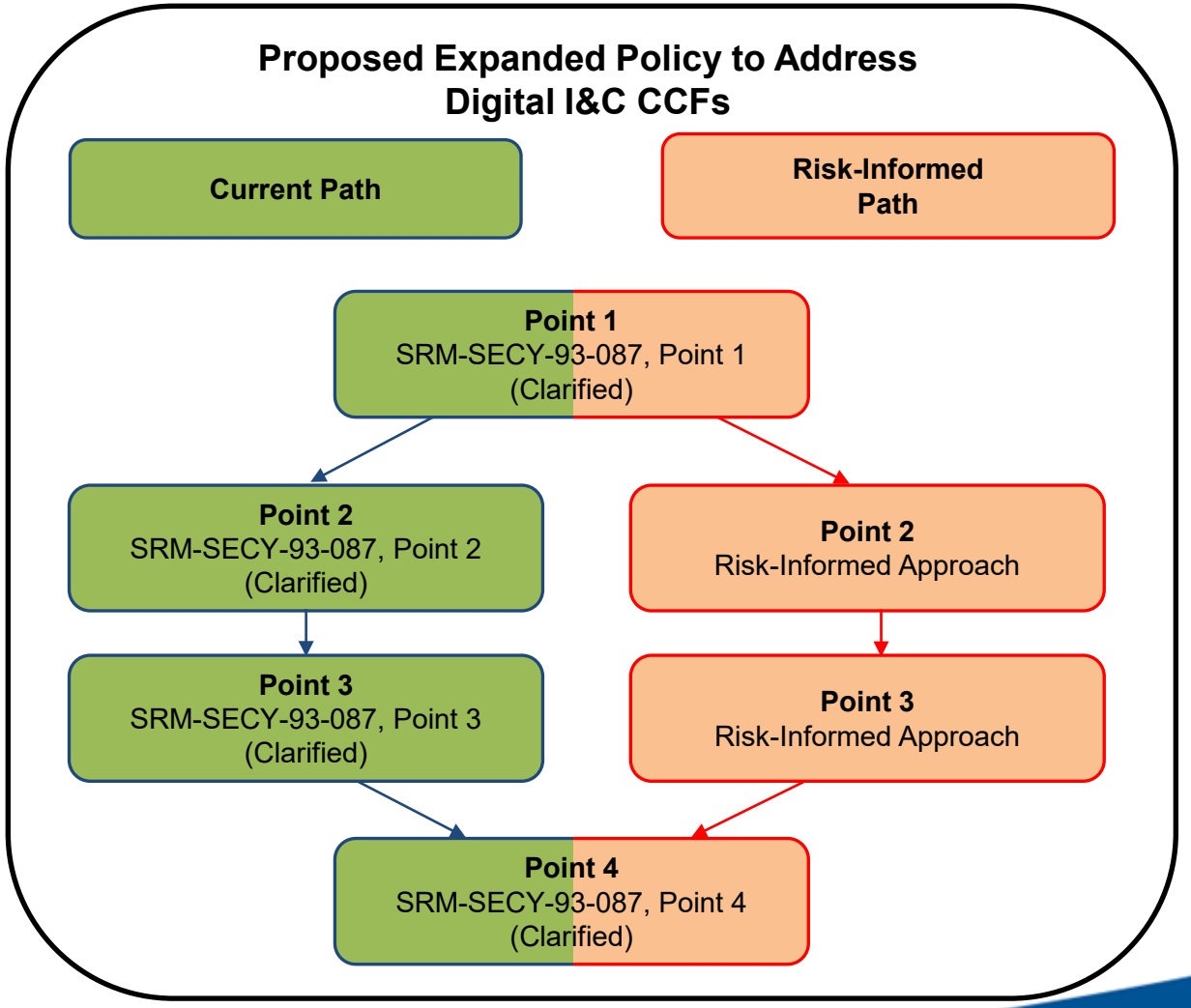
SECY-22-0076 – "Expansion of current policy on potential common-cause failures in digital instrumentation and control systems"

- This SECY was issued on August 2022 to request that the Commission expand the current policy for digital I&C CCFs to allow the use of risk-informed approaches to demonstrate the appropriate level of defense-in-depth, including not providing any diverse automatic actuation of safety functions.
- The proposed expanded policy encompasses the current points of SRM-SECY-93-087 (with clarifications) and expands the use of risk-informed approaches in points 2 and 3.
- The current policy will continue to remain a valid option for licensees and applicants.
- The staff's goal is to provide more flexibility in addressing the digital I&C CCF challenge while continuing to ensure safety.

Source: https://www.nrc.gov/docs/ML2219/ML22193A290.html

U.S. NRC's Approach to Risk-Informing the CCF Policy

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

U.S. NRC's Approach to Risk-Informing the CCF Policy

- The staff's goal is that the acceptance criteria for risk-informed approaches for digital I&C CCFs will be consistent with established NRC practices and guidance for risk-informed decision making.
- "Risk-informed" approaches lie between the "risk-based" and purely deterministic approaches.
- A risk-informed approach enhances the deterministic approach by:
  a) allowing explicit consideration of a broader set of potential challenges to safety,
  b) providing a logical means for prioritizing these challenges based on risk significance, operating experience, and/or engineering judgment,
  c) facilitating consideration of a broader set of resources to defend against these challenges,
  d) explicitly identifying and quantifying sources of uncertainty in the analysis, and
  e) leading to better decision-making by providing a means to test the sensitivity of the results to key assumptions.

Source: https://www.nrc.gov/docs/ML0037/ML003753601.pdf

Proposed Language to Risk-Inform Point 2

"In performing the D3 assessment, the applicant shall analyze each postulated CCF. This assessment may use either best-estimate methods or a risk informed approach.

When using best-estimate methods, the applicant shall demonstrate adequate defense in depth and diversity within the facility's design for each event evaluated in the accident analysis section of the safety analysis report.

When using a risk-informed approach, the applicant shall include an evaluation of the approach against the Commission's policy and guidance, including any applicable regulations, for risk-informed decision-making. The NRC staff will review applications that use risk-informed approaches for consistency with established NRC policy and guidance on risk-informed decision making (e.g., Regulatory Guide (RG) 1.174, 'An Approach for Using Probabilistic Risk Assessment in Risk Informed Decisions on Plant Specific Changes to the Licensing Basis')."

Source: https://www.nrc.gov/docs/ML1731/ML17317A256.pdf

Proposed Language to Risk-Inform Point 3

"The D3 assessment may demonstrate that a postulated CCF can be reasonably prevented or mitigated or is not risk significant. The applicant shall demonstrate the adequacy of any design techniques, prevention measures, or mitigation measures, other than diversity, that are credited in the assessment. The level of technical justification demonstrating the adequacy of these techniques or measures, other than diversity, to address potential CCFs shall be commensurate with the risk significance of each postulated CCF.

A diverse means that performs either the same function or a different function is acceptable to address a CCF, provided that the assessment includes a documented basis showing that the diverse means is unlikely to be subject to the same CCF. The diverse means may be performed by a system that is not safety-related if the system is of sufficient quality to reliably perform the necessary function under the associated event conditions. Either automatic or manual actuation within an acceptable timeframe is an acceptable means of diverse actuation.

If a postulated CCF is risk significant and the assessment does not demonstrate the adequacy of other design techniques, prevention measures, or mitigation measures, then a diverse means shall be provided."

Status and Next Steps

- The Commission is currently evaluating the proposed expanded policy in SECY-22-0076.
- If the Commission approves the expanded policy, the NRC staff will:
  - update the existing implementation guidance to address digital I&C CCFs and
  - continue to engage stakeholders and the public to seek comments on the staff's implementation of the expanded policy.

Closing Remarks/Key Messages

- The U.S. NRC's policy for addressing digital I&C CCFs goes back to 1993.
- The current policy has been effectively used to license digital I&C systems in nuclear power plants, but it requires a diverse means of actuation if a CCF could disable a safety function.
- The NRC staff requested the NRC Commission expand the current policy for digital I&C CCFs to allow the use of risk-informed approaches to demonstrate the appropriate level of defense-in-depth for high safety significance systems.
- The NRC staff's goal is that the acceptance criteria for risk-informed approaches for digital I&C CCFs will be consistent with established NRC practices and guidance for risk-informed decision making.
- The current policy will continue to remain a valid option for licensees and applicants.

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
I&C	Instrumentation and control
NRC	U.S. Nuclear Regulatory Commission
PRA	Probabilistic Risk Assessment
RG	Regulatory Guide
RPS	Reactor Protection System
SAR	Safety Analysis Report
SECY	Commission Paper
SRM	Staff Requirements Memorandum