Common-Cause Failure (CCF) SECY Paper Outline
for ACRS DI&C Subcommittee Meeting
May 20, 2022

- **SUBJECT:** Consideration of Risk-Informed Alternatives to Address Potential Common-Cause Failures in Digital Instrumentation and Control Systems

- **PURPOSE:** The purpose of this paper is to provide the Commission with a recommendation on the expanded use of risk-informed alternatives to address digital instrumentation and control (I&C) common-cause failures (CCF). Specifically, this paper provides a recommendation for an expanded policy that encompasses the current deterministic position in SRM-SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs," and provides for the use of risk-informed alternatives to determine the appropriate level of defense-in-depth, which may or may not include diversity, to address systematic, nonrandom, concurrent failures of redundant elements in the design of digital I&C systems.

- **BACKGROUND:**
  - Early concerns with CCF
    - CCF has been an NRC concern since the mid-1960s
    - In the early 1990's the introduction of digital I&C became a concern as a new source for introducing CCF

  - SRM-SECY-93-087 as the means to address digital I&C CCF
    - The NRC's current digital I&C CCF policy is expressed in various documents, including SRM-SECY-93-087, SECY-18-0090, and BTP 7-19, Rev. 8.

  - Current state of digital I&C in the nuclear power industry
    - Evolution of development and quality assurance tools
    - The sources of digital I&C CCF concern today may not be the same as those considered in the early 1990's

  - Increased use of risk-informed decision making
    - PRA Policy Statement, SRM-SECY-98-144, and current agency focus to expand risk-informed decision making

  - SRM-SECY-16-0070, the digital I&C Integrated Action Plan to modernize the digital I&C regulatory infrastructure, and the opportunity to risk-inform the current policy to address digital I&C CCF
    - Issuance of NRC guidance on risk-informed, graded approaches to address digital I&C CCF (e.g., BTP 7-19 and RIS 2002-22, Supplement 1)

- External stakeholder involvement and industry efforts

- Guiding Principles
  - The expanded policy will not conflict with existing regulatory requirements (i.e., a rule change or exemption will not be required to implement it).
  - Expanding the digital I&C CCF policy should 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.
  - All five principles of risk-informed decision making, as listed in RG 1.174, need to be addressed satisfactorily.
  - A systematic approach is used to evaluate digital I&C failure causes during operation and maintenance, including inappropriate software behavior.
  - The PRA used for risk-informed approaches needs to be technically adequate (e.g., meets the guidance in RG 1.200) and include an effective PRA configuration control and feedback mechanism.
  - The expanded policy needs to ensure that the introduction of digital I&C does not significantly increase the risk of operating the facility.

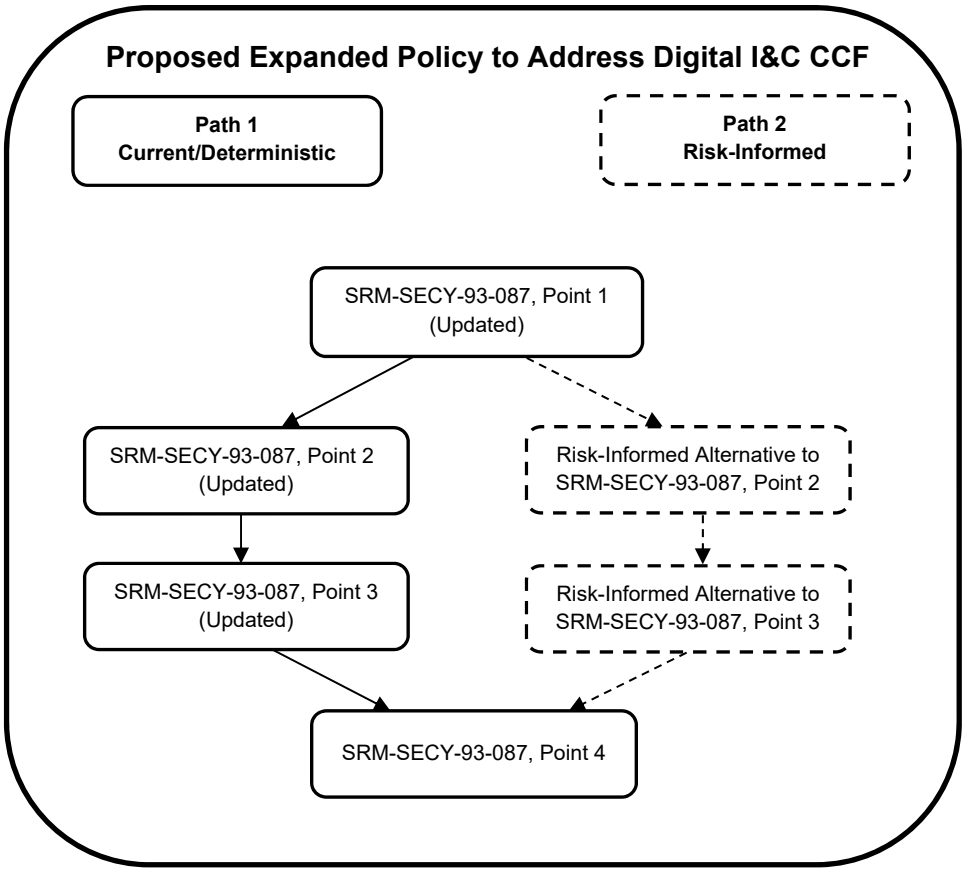
- **DISCUSSION:**
  - The current policy continues to be a viable option to address digital I&C CCF
    - The current four deterministic points in SRM-SECY-93-087 will remain as a viable path to licensees and applicants
      - Point 1 – "… assess the defense-in-depth and diversity of the proposed I&C 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

  - The use of risk-informed alternatives can provide flexibility to address digital I&C CCF and is consistent with recent Commission policy regarding application of risk-informed approaches
    - Current risk-informed approaches applied in other regulatory activities since SRM-SECY-93-087 will be described

- PRA models can be used to systematically compare the effectiveness (i.e., risk impact) of alternatives to the diversity stipulated in SRM-SECY-93-087
- Risk-informed alternatives can have different levels of PRA use, including a hybrid approach that uses PRA to identify the risk significance of sequences that may be challenging to address using currently acceptable means
- Risk-informed alternatives may be used to establish a graded approach in determining the degree of diversity that is needed

- Risk Informing the positions in SRM-SECY-93-087
  - SRM-SECY-93-087, Point 1:
    - 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 digital I&C system or component
    - Current application of Point 1 allows for the use of risk information
    - Note the current language in Point 1 can be misinterpreted (e.g., the use of the term common-mode failure when the intent is common-cause failure)
  - SRM-SECY-93-087, Point 2:
    - Current approach focuses on outcomes and doesn't consider the likelihood
    - This is considered an appropriate area for a risk-informed alternative to (i.e., instead of) demonstrating adequate diversity for each postulated CCF for each event evaluated in the accident analysis
  - SRM-SECY-93-087, Point 3:
    - Current approach only provides one way of addressing undesirable outcomes (i.e., diverse means)
    - This is considered an appropriate area for risk-informed alternative to (i.e., instead of) providing a diverse means of accomplishing the safety function(s) if the postulated CCF could disable the safety function(s)
  - SRM-SECY-93-087, Point 4:
    - Regulations appropriately require diverse and independent displays and controls
    - Not an appropriate area for a risk-informed alternative

- Proposed Expanded Policy to address Digital I&C CCF
  - A single policy that encompasses the current positions in SRM-SECY-93-087 and provides for risk-informed alternatives to address digital I&C CCF
  - This allows for:
    1) incorporating the language in Points 1, 2 and 3 of SRM-SECY-93-087 with appropriate clarifications and corrections (e.g., replace common-mode failure with common-cause failure),
    2) incorporating the existing language in Point 4 of SRM-SECY-93-087, and
    3) augmenting Points 2 and 3 of SRM-SECY-93-087 with risk-informed alternatives.



- Other options considered but not pursued
  - Staff developed options
  - Industry proposed options

- Summary and evaluation of stakeholder feedback (including ACRS)

- Differing views (if any)

- **COMMITMENT:**
  - If the Commission approves this SECY, the staff will proceed to update the implementation guidance in BTP 7-19, Rev. 8, and review industry proposed risk-informed approaches (e.g., NEI 20-07) for possible endorsement.

- **RECOMMENDATION:**
  - The staff recommends that the Commission approve the proposed expanded policy to allow for the use of risk-informed alternatives to address digital I&C CCF.