U.S.NRC

United States Nuclear Regulatory Commission

Protecting People and the Environment

SECY-22-0076
"Expansion of Current Policy on Potential Common-Cause Failures in Digital Instrumentation and Control Systems"

Public Meeting
October 20, 2022

Presentation Outline

- Recent Activities and Current Status
- Purpose of Today's Meeting
- Staff Key Messages
- Summary of Proposed Expanded Policy
- Staff Position on ACRS Questions
- Point 4 Applicability and Clarifications
- Open Dialogue with Stakeholders

Recent Activities and Current Status

- The staff issued SECY-22-0076 on August 10, 2022, proposing an expansion to the digital instrumentation and control (DI&C) common cause failure (CCF) policy contained in the Staff Requirements Memorandum (SRM) to SECY-93-087
- The Nuclear Energy Institute (NEI) provided a letter to the NRC on August 26, 2022, providing comments on the staff's position contained in the SECY on diverse and independent main control room displays and manual controls
- The staff and NEI briefed the Advisory Committee on Reactor Safeguards (ACRS) DI&C Subcommittee on September 23, 2022, and the staff is scheduled to brief the full ACRS on November 1, 2022
- The SECY is currently under Commission review and the Commission will provide its direction to the staff through a Staff Requirements Memorandum

Purpose of Today's Meeting

The staff will use today's meeting to:

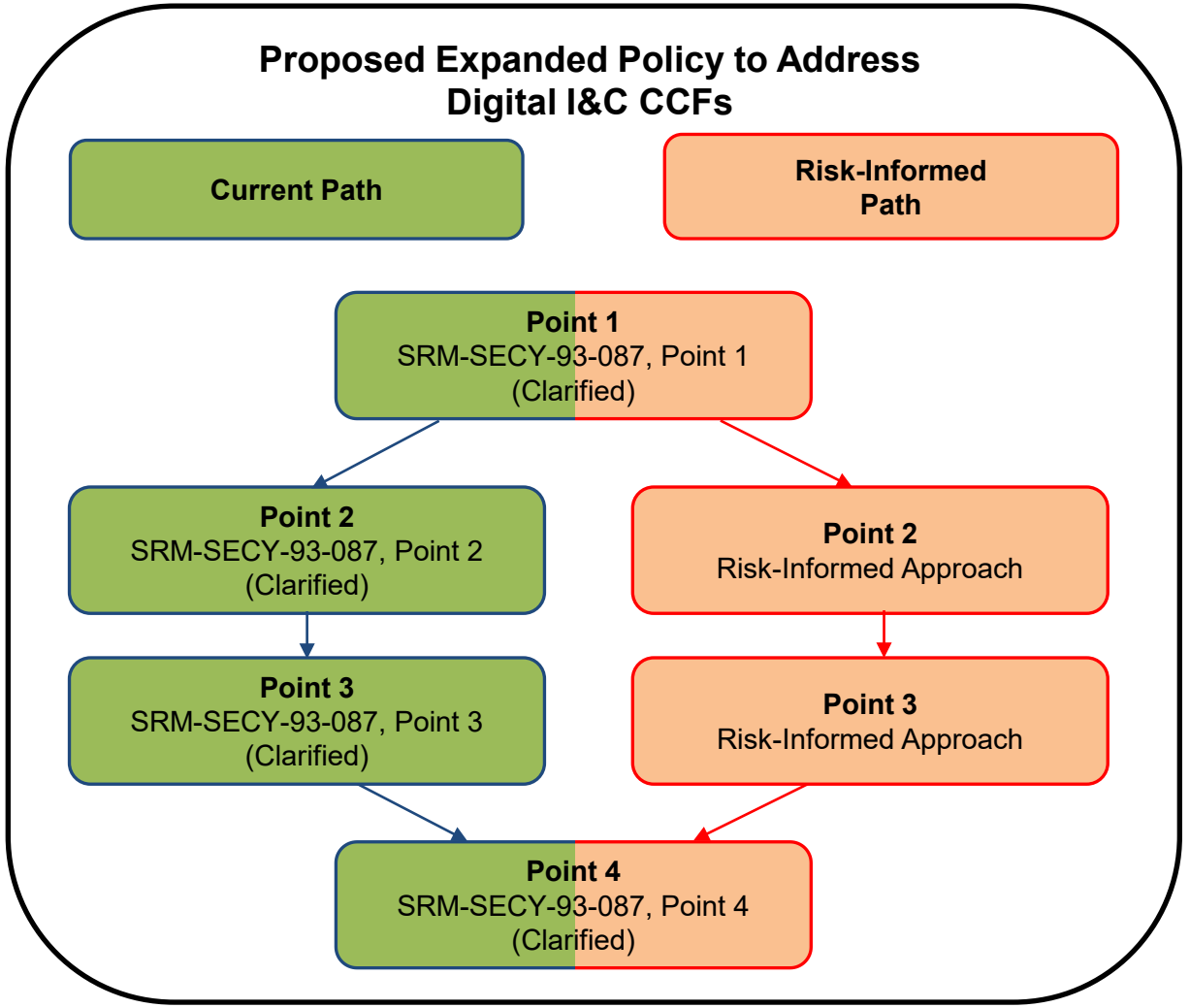
1) Summarize the expanded policy contained in SECY-22-0076
2) Share the staff's position on questions received from the ACRS
3) Share the staff's position on diverse and independent main control room displays and manual controls, i.e., "Point 4"
4) Conduct an open dialogue with stakeholders to hear their perspectives

Staff Key Messages

- The proposed expanded policy in SECY-22-0076 encompasses the current four points of SRM-SECY-93-087 (with clarifications) and expands the use of risk-informed approaches in points 2 and 3.
- Points 1-3 and Point 4 of the policy address two facets needed to ensure safe operation of the plant:
  - Points 1-3 ensure DI&C systems are sufficiently robust to adequately cope with CCF
  - Point 4 ensures operators can manually control critical safety functions even in the event of a DI&C CCF
- Point 4 incorporates an implicit element of risk-informing as it focuses only on those critical safety functions needed to ensure the safety of the facility.
- The expanded policy is intended to be technology neutral and applies to any reactors (including non-light-water reactors) licensed under 10 CFR Parts 50 and 52.
- The staff acknowledges that the critical safety functions listed in SRM-SECY-93-087, SECY-22-0076 and Branch Technical Position (BTP) 7-19 (i.e., reactivity control, core heat removal, reactor coolant inventory, containment isolation, and containment integrity) may not be the appropriate set for all reactor designs
- The SECY provides for existing regulatory tools (exemptions and alternatives), if necessary, to accommodate for reactor designs with different critical safety functions
- If the staff encounters a reactor design where the policy would not be applicable, the staff will engage the Commission as appropriate.

Summary of Proposed Expanded Policy

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

Staff Positions on ACRS Questions

ACRS Question 1: *Would the revised policy be applicable to advanced reactors?*
Answer: The proposed expanded policy would apply to requests all nuclear power plant types licensed under 10 CFR Part 50 and 10 CFR Part 52, including advanced reactors.

ACRS Question 2: *Do aspects of the policy for which the staff did not request a change carry forward unaltered?*
Answer: Yes

ACRS Question 3: *Might different reactor types warrant consideration of different critical safety functions?*
Answer: While the expansion of the policy is intended to be technology neutral it relies on the staff's licensing experience to date and assumptions about the design of the facility, such as the presence of a main control room. The staff acknowledges that the critical safety functions listed in the SECY and BTP 7-19 (reactivity control, core heat removal, reactor coolant inventory, containment isolation, and containment integrity) may not be the appropriate set for all reactor designs. The staff has existing regulatory tools (exemptions and alternatives), if necessary, to accommodate designs with different critical safety functions and, if the staff encounters a reactor design where the policy would not be applicable, the staff will engage the Commission as appropriate.

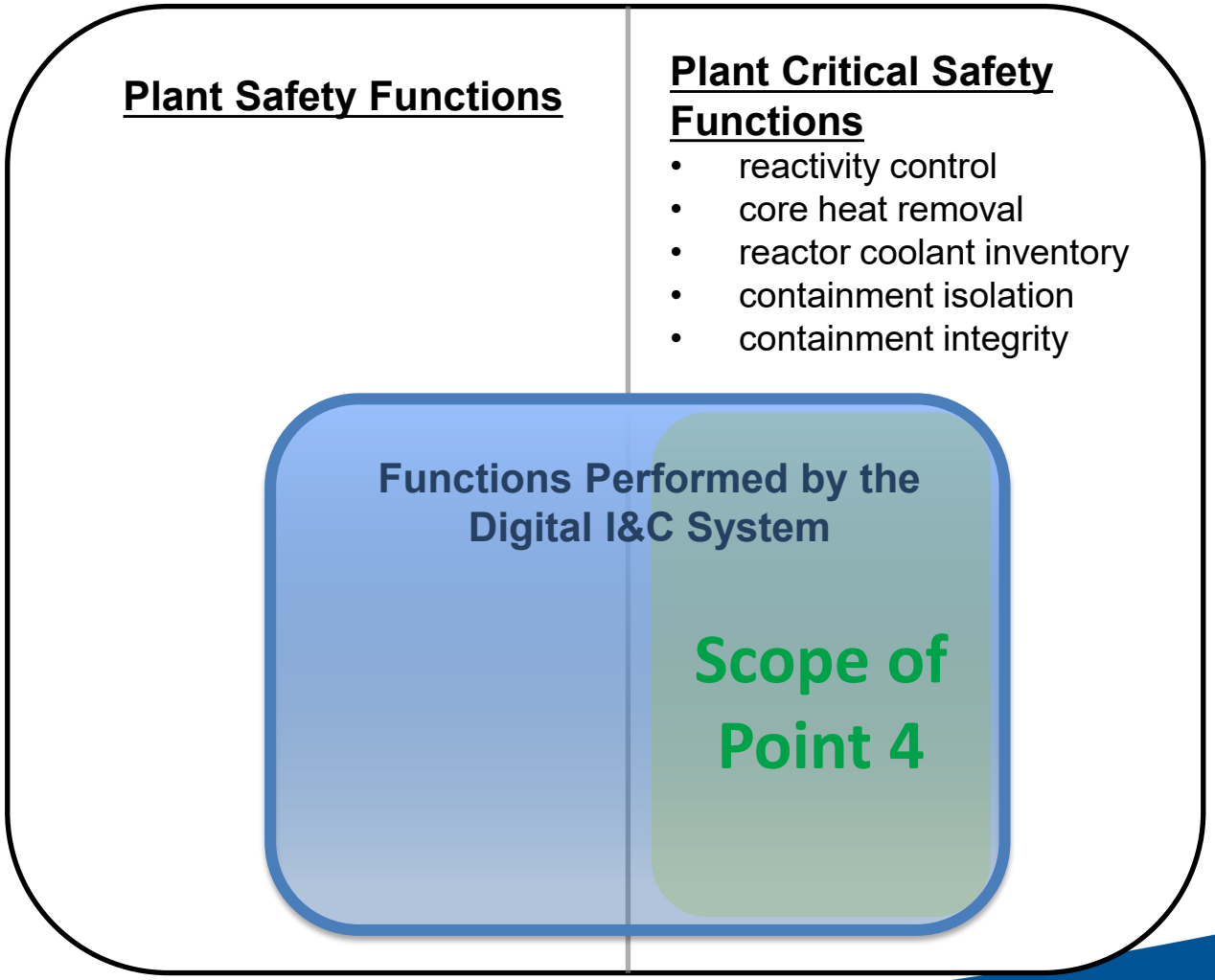
Applicability of Point 4

Point 4 only applies to:

- The critical safety functions performed by the digital I&C system.

Point 4 does not apply to:

- All safety functions performed by the digital I&C system.
- Critical safety functions not performed by the digital I&C system.



The diverse manual controls and displays for critical safety functions ensure the safety of the facility.

Staff's Position on Diverse and Independent Main Control Room Displays and Manual Controls

- In SECY-93-087, the staff recommended that safety-grade displays and controls located in the main control room and hardwired to the lowest level of the safety computer system architecture, be provided for manual, system-level actuation of critical safety functions and monitoring of parameters that support the safety functions and that the displays and controls should be independent and diverse from the safety computer system identified in Points 1 and 3 of the policy.
- The staff recommended this because such controls and displays provide the plant operators with unambiguous information and control capabilities to enable the operators to expeditiously mitigate the effects of the postulated common-cause software failure of the digital safety I&C system. The control room would be the center of activities to safely cope with the event, which could also involve the initiation and implementation of the plant emergency plan. The design of the plant should not require operators to leave the control room for such an event.

Staff's Position on Diverse and Independent Main Control Room Displays and Manual Controls (contd.)

- While the Commission's Staff Requirements Memorandum to SECY-93-087 modified the policy to permit non-safety grade displays and controls and more flexible architectural implementation, the Commission supported the staff's recommendation on diverse displays and controls, and the staff continues to believe this position remains appropriate for critical safety functions to provide reasonable assurance of adequate protection.
- Point 4 incorporates an implicit element of risk-informing as it focuses only on those critical safety functions needed to ensure the safety of the facility.
- Requests for exemptions (under 10 CFR 50.12 or 52.7) or alternatives (under 10 CFR 50.55a(z)) provide avenues for applicants to request a deviation from the regulations based on risk information on a case-by-case basis.
- If the staff encounters a reactor design where the policy would not be applicable, the staff will engage the Commission as appropriate.

SECY-22-0076: Addressing DI&C CCFs & Ensuring the Ability to Perform Manual Actions

Points 1-3 and Point 4 address two facets needed to ensure the safe operation of the plant

Protection against DI&C CCFs
to cope with the loss of a safety function

- Point 1 – Perform a D3 Assessment
- Point 2 – Ways of performing the assessment
- Point 3 – Ways of addressing a postulated DI&C CCF

Allow operators to take manual actions
when needed, after a DI&C CCF

- Point 4 – Diverse displays and manual controls for critical safety functions

- If not addressed, a DI&C CCF can affect both the DI&C system and manual controls and displays

- The four points when taken together provide criteria for the assessment of diversity and defense in depth against CCF, and ensure DI&C CCFs do not:
  - Defeat safety functions (Points 1-3)
  - Impede operators' ability to take manual actions when needed (Point 4)

Open Dialogue with Stakeholders

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
NEI	Nuclear Energy Institute
NRC	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