Stakeholder Outreach on Potential Expansion of the Current NRC Policy for Addressing Digital Instrumentation and Controls Common Cause Failure

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

Outline

- Background
- Purpose of Expanding the Current DI&C CCF Policy
- SECY Development Milestones & Target Completion Date
- Terminology
- Guiding Principles
- Key Questions
- Open Discussion

Background

- Current DI&C CCF Policy
- DI&C CCF SRMs & SECYs
- Modernization of DI&C CCF Guidance
- Safety Concern

Background - Current DI&C CCF Policy

SRM-SECY-93-087 contains four NRC points on DI&C CCF Policy:

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."

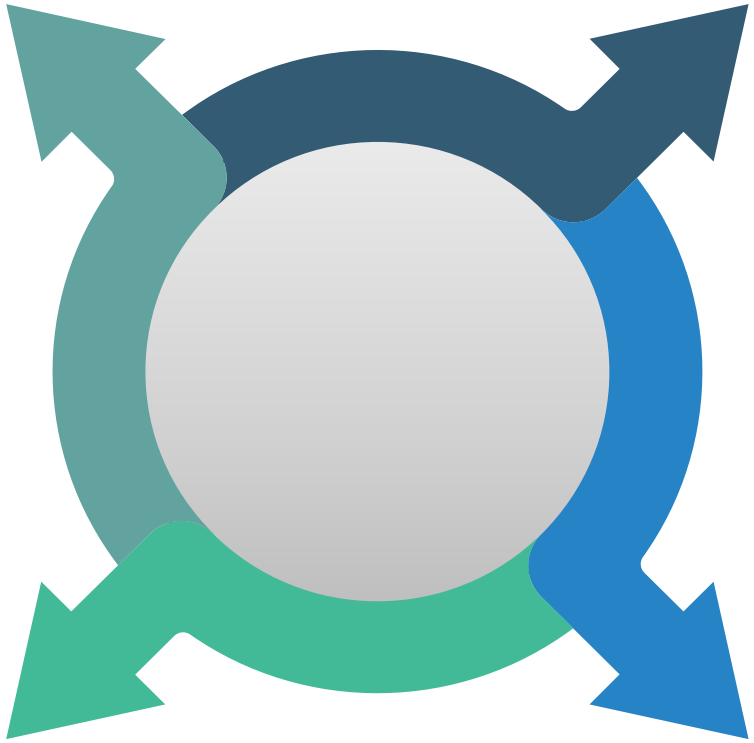
Point 2 – "… analyze each postulated common-mode failure for each event that is evaluated in the accident analysis section of the safety analysis report (SAR) using best estimate methods… demonstrate adequate diversity within the design for each of these events."

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…"

Background - Current DI&C CCF Policy (contd.)

Methods used under the current policy to address DI&C CCF:



Eliminate

e.g., Simple Design,
Internal DI&C System Diversity

Mitigate

e.g., Existing Equipment,
Manual Operator Action,
Diverse Actuation System

Limit

e.g., Design Measures

Accept

e.g., Consequence Calculation

Background - Current DI&C CCF Policy (contd.)

Examples of DI&C systems approved using the current policy:

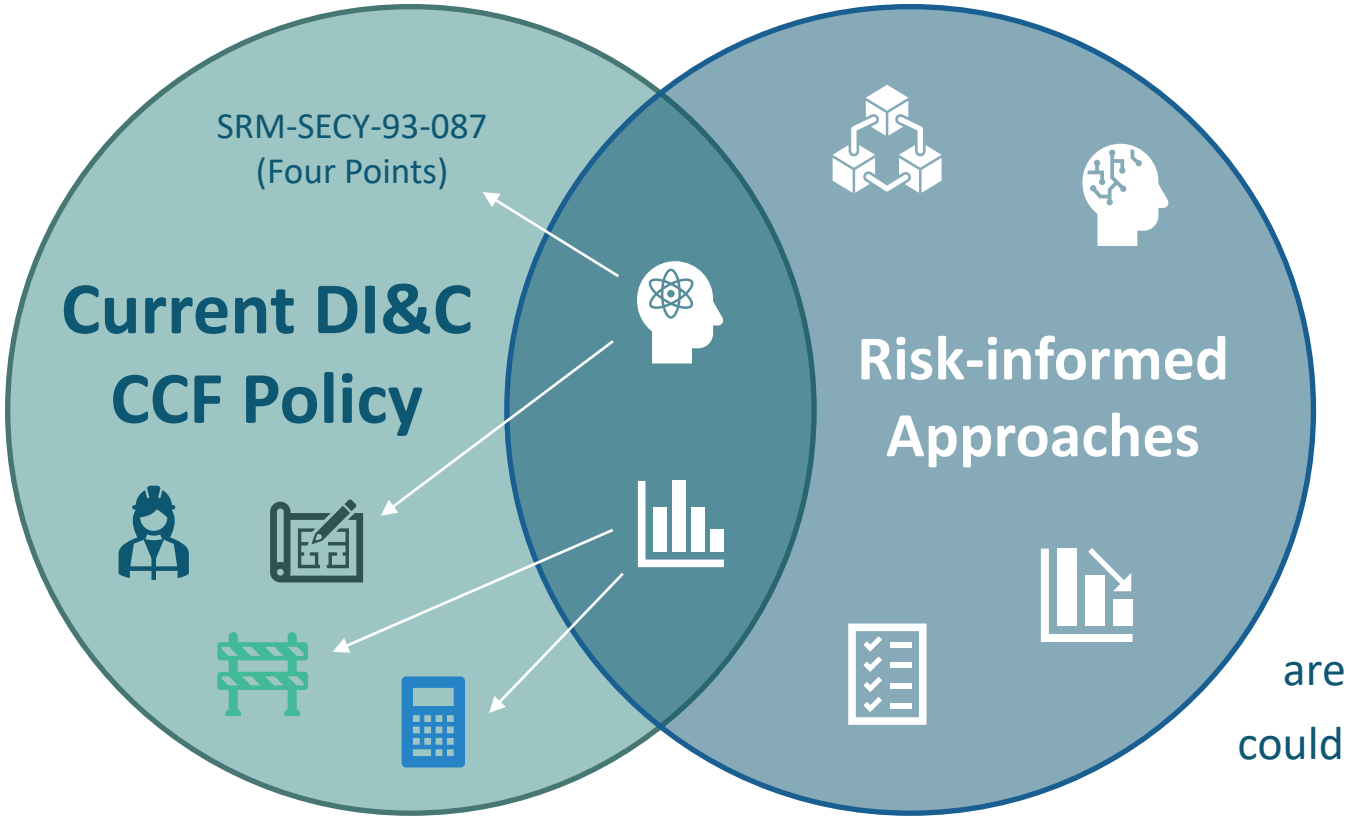
Reactor Trip System & Engineered Safety Features Actuation System	Main Steam and Feedwater Isolation System	Power Range Neutron Monitoring System	Integrated Control and Protection System
e.g., Oconee, Diablo Canyon & NuScale	e.g., Wolf Creek	e.g., Hope Creek & Browns Ferry	e.g., AP1000 & APR1400

The NRC staff developed a D3 comparison table that illustrates examples of NRC-approved methods licensees and applicants utilized to successfully address DI&C CCF among operating plants and new/advanced reactor licensing activities (ADAMS Accession Nos. ML20345A338 & ML19092A403).

Background - Current DI&C CCF Policy (contd.)

Use of risk information within the current policy vs risk-informed alternatives to the current policy.

There is some room in the current policy for risk information.



However, the current policy does not accommodate use of risk-informed **alternatives** to SRM-SECY-93-087 for addressing DI&C CCF (e.g., to determine whether diverse means are required if a postulated CCF could disable the safety function).

Background – DI&C CCF SRMs and SECYs

- **SECY-91-292** explained the staff concerns regarding the use of DI&C in evolutionary and advanced light water reactors.
- **SRM-SECY-93-087** identified the four points to address DI&C CCF.
- **SECY-09-0061** reaffirmed the SRM-SECY-93-087 policy in response to an industry White Paper on using risk information to eliminate the need for diverse actuation systems.
- **SRM-SECY-15-0106** directs the staff to develop an integrated strategy to modernize the NRC's DI&C regulatory infrastructure including "updates to the policy on common-cause failure in SRM-SECY-93-087."
- **SRM-SECY-16-0070** approved implementation of the staff's integrated action plan (IAP) to modernize the NRC's DI&C regulatory infrastructure, which included the evaluation of the current position to address CCF in DI&C systems.
- **SECY-18-0090** 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 DI&C systems but residual faults within digital systems may lead to CCFs
  - Provides guiding principles for updating the staff's guidance for addressing CCF

Background – Modernization of DI&C CCF Guidance: BTP 7-19, Rev. 8

As part of DI&C IAP Modernization Plan (MP) #1D, the staff revised BTP 7-19.

BTP 7-19, Rev. 8 was issued in January 2021, incorporating the following key changes:

- Incorporates the guiding principles from SECY-18-0090
- Clarifies D3 Assessment
  - Introduces graded approach
  - Incorporates qualitative assessment framework from Supplement 1 to RIS 2002-22 for non-RPS/ESFAS systems
  - Clarifies staff guidance on means to address CCF
- Refines guidance on spurious operation

Background – Safety Concern

- The safety concern to the NRC is that the introduction of DI&C may introduce new failure modes and behaviors (e.g., by introducing DI&C CCF) that could result in an unacceptable consequence (e.g., loss of safety function that leads to core damage).

- Diverse means, as described in SRM-SECY-93-087, may not be the only acceptable approach to address DI&C CCF.

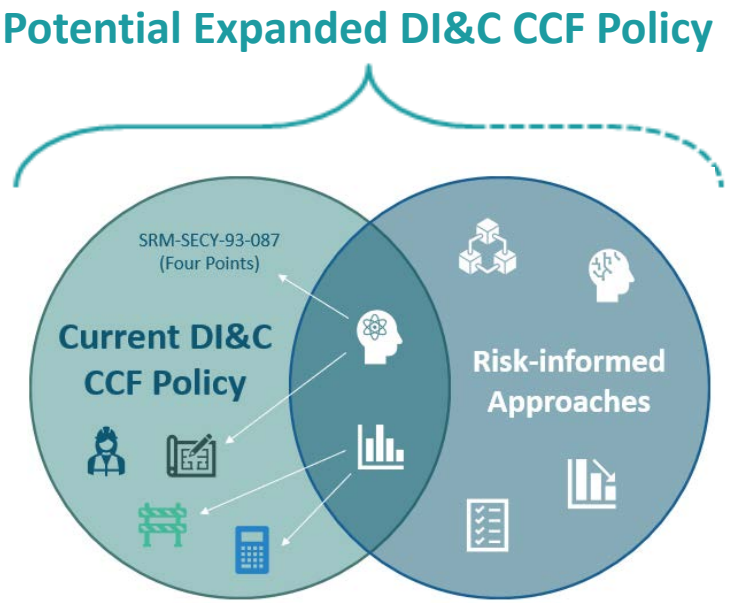
- Other stakeholders have expressed interest in alternative risk-informed methods for addressing DI&C CCF. For example, NEI submitted NEI 20-07, Draft D in September 2021. NEI states that NEI 20-07, Draft D does not "wholly conform to the four (4) positions" in SRM-SECY-93-087.

Purpose of Expanding the Current DI&C CCF Policy

- To allow consideration of risk-informed **alternatives** to SRM-SECY-93-087.
  - e.g., the staff is considering whether under some circumstances, the expanded policy might not require a diverse means for addressing DI&C CCF.

- Licensees/applicants will continue to have the option to meet the position in SRM-SECY-93-087.

- Goal is to provide more flexibility in addressing the DI&C CCF challenge while continuing to ensure safety.



SECY Development Milestones & Target Completion Date

First Public Meeting – February 2022

Research, Analysis, Developing Strategies, and Alignment – April 2022

Initial SECY Draft – May 2022

Public Meeting – June 2022

Send to OEDO for Review and Signature – August 2022

Terminology – Risk-Informed

The term “risk-informed” was originally presented in SECY-98-144 and modified by the Commission in SRM-SECY-98-144.

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 (although such analyses do not necessarily reflect all important sources of uncertainty), and

e) leading to better decision-making by providing a means to test the sensitivity of the results to key assumptions.

Terminology – Risk-Informed (contd.)

Where appropriate, a risk-informed regulatory approach can also be used to reduce unnecessary conservatism in purely deterministic approaches, or can be used to identify areas with insufficient conservatism in deterministic analyses and provide the bases for additional requirements or regulatory actions.

“Risk-informed” approaches lie between the “risk-based” and purely deterministic approaches. The details of the regulatory issue under consideration will determine where the risk-informed decision falls within the spectrum.

From SRM-SECY-98-144

Terminology – Diversity

Diversity per 10 CFR 50 Appendix A

- The introduction to the GDCs contemplates that applications may be required to consider “the possibility of systematic, nonrandom, concurrent failures of redundant elements in the design of protection systems and reactivity control systems. (See Criteria 22, 24, 26, and 29.)”

- Criterion 22—Protection system independence. The protection system shall be designed to assure that the effects of natural phenomena, and of normal operating, maintenance, testing, and postulated accident conditions on redundant channels do not result in loss of the protection function, or shall be demonstrated to be acceptable on some other defined basis. Design 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.”

Guiding Principles

- The new position shall not conflict with existing regulatory requirements (i.e., a rule change or exemption will not be required to implement it).
- Expanding the DI&C CCF policy should be consistent with the agency's PRA Policy Statement, SRM-SECY-98-144, 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 to evaluate DI&C failure modes during operation and maintenance, including inappropriate software behavior, is used.
- If a PRA is used for risk-informed approaches, it meets the guidance in RG 1.200 and includes an effective PRA configuration control and feedback mechanism.
- Risk Goal: Ensure the introduction of DI&C does not significantly increase the risk of operating the facility.

Key Questions

- Is it necessary to determine the risk worth of various defenses against CCF (e.g., architectural segmentation)?
  - If yes, how are they assessed in a clear and consistent manner?
- Can the risk of CCF in DI&C be assessed without determining software reliability with high confidence?
  - Are there practical bounding approaches?
  - How to address reliability and beta factors for DI&C?
- Should the expanded policy, consistent with the current practice, remain focused on architectural-level considerations or include focus on the building blocks such as software development tools?
  - Can the individual risks of specific building blocks be quantified?
  - Is the current focus on architectural-level considerations sufficient to implement risk-informed approaches?
- Is the consideration of low-probability and high-consequence initiators in expanded policy consistent with NRC's existing risk-informed approaches?
- How to determine the risk of CCF due to "system design aspects" vs risk of loss of function?

OPEN DISCUSSION

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

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

References

SECY-91-292, “Digital Computer Systems for Advanced Light-Water Reactors,” dated September 16, 1991 (ADAMS Accession No. ML12222A030)

SRM-SECY-93-087, “Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs,” dated July 21, 1993 (ADAMS Accession No. ML003708056).

SECY-09-0061, “Status of The Nuclear Regulatory Commission Staff Efforts to Improve the Predictability and Effectiveness of Digital Instrumentation and Control Reviews,” dated April 14, 2009 (ADAMS Accession No. ML090790409)

SRM-SECY-15-0106, “Rulemaking: Proposed Rule: Incorporation by Reference of Institute of Electrical and Electronics Engineers Standard 603-2009, “IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations”,” dated February 25, 2016 (ADAMS Accession No. ML16056A614)

SRM-SECY-16-0070, “Integrated Strategy to Modernize the Nuclear Regulatory Commission’s Digital Instrumentation and Control Regulatory Infrastructure,” Rev. 3, dated January 2019 (ADAMS Accession No. ML16126A137)

SECY-18-0090, “Plan for Addressing Potential Common Cause Failure in Digital Instrumentation and Control,” dated September 12, 2018 (ADAMS Accession No. ML18179A067)

References (contd.)

BTP 7-19, Rev. 8, "Guidance for Evaluation of Defense In Depth And Diversity To Address Common-Cause Failure Due to Latent Design Defects in Digital Safety Systems," dated January 2021 (ADAMS Accession No. ML20339A647)

Regulatory Issue Summary 2002-22, Supplement 1, "Clarification on Endorsement of Nuclear Energy Institute Guidance in Designing Digital Upgrades in Instrumentation and Control Systems," dated May 31, 2018 (ADAMS Accession No. ML18143B633)

NEI 20-07, Draft D, "Guidance for Addressing Common Cause Failure in High Safety-Significant Safety-Related DI&C Systems" (ADAMS Accession No. ML21278A471).

SRM-SECY-98-144, "White Paper on Risk-Informed and Performance-Based Regulation," dated March 1, 1999 (ADAMS Accession No. ML003753601)

RG 1.174, Rev. 3, "An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis," dated January 2018 (ADAMS Accession No. ML17317A256)

RG 1.200, Rev. 3, "Acceptability of Probabilistic Risk Assessment Results for Risk-Informed Activities," dated December 2020 (ADAMS Accession No. ML20238B871)

BACKUP SLIDES

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

Relevant Text from the SRM-SECY-93-087

18. II.Q. Defense Against Common-Mode Failures in Digital Instrumentation and Control Systems:

The Commission **approves**, in part, and **disapproves**, in part, the staff's recommendation.
The Commission has approved a revised position, as follows:

1. The applicant shall assess the defense-in-depth and diversity of the proposed instrumentation and control system to demonstrate that vulnerabilities to common mode failures have adequately been addressed.

2. In performing the assessment, the vendor or applicant shall 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. The vendor or applicant shall demonstrate adequate diversity within the design for each of these events.

3. If a postulated common-mode failure could disable a safety function, then a diverse means, with a documented basis that the diverse means is unlikely to be subject to the same common-mode failure, shall be required to perform either the same function or a different function. The diverse or different function may be performed by a non-safety system if the system is of sufficient quality to perform the necessary function under the associated event conditions.

4. A set of ~~safety grade~~ 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. The displays and controls shall be independent and diverse from the safety computer system identified in items 1 and 3 above.

Relevant Text from the SRM-SECY-93-087 (contd.)

The staff's position has been modified in essentially two respects:

First, inasmuch as common mode failures are beyond design-basis events, the analysis of such events should be on a best-estimate basis.

Second, the staff indicates in its discussion of the third part of its position that “The diverse or different function may be performed by a non-safety system if the system is of sufficient quality to perform the necessary function under the associated event conditions.” Therefore, this clarification has been added to the fourth part of the staff’s position (which refers to a subset of the safety functions referred to in the third part) by removing the safety grade requirement. Further, the remainder of the discussion under the fourth part of the staff position is highly prescriptive and detailed (e.g., “shall be evaluated,” “shall be sufficient,” “shall be hardwired,” etc.). The Commission approves only that such prescriptiveness be considered as general guidance, the practicality of which should be determined on a case-by-case basis.

Accepted Methods to Address CCF in DI&C Licensing Activities

Category	Method Name and Description
Eliminate	**Internal Diversity** If sufficient diversity exists within in the protection system, then vulnerabilities to Common Cause Failure (CCF) can be considered to be appropriately addressed without further action.
	Simple Design A system is sufficiently simple such that every possible combination of inputs and every possible sequence of device states are tested, and all outputs are verified for every case.
Limit	**Design Measures** Design measures are used to reduce the likelihood of a CCF (e.g., self-diagnostic, failure analysis, etc.).
Mitigate	**Existing Equipment** An existing system or equipment is used to perform the diverse or different function to mitigate the loss of the safety function performed by the digital I&C system during a Design Basis Event (DBE).
	Manual Operator Action (MOA) Actions that can be reasonably taken by operators to identify CCF failures and mitigate consequences within a realistic time frame during a DBE.
	Diverse Actuation System (DAS) Independent and diverse system that can activate protection systems if primary system fails during a DBE. Technology used can be analog or digital.
Accept	**Consequence Calculation** Consequence models, using best estimate methodologies, demonstrated that CCF failures concurrent with DBEs and Anticipated Operational Occurrences do not result in doses that exceed 10% of the applicable siting dose guideline values.

Examples of Licensing Successes

Examples	Methods Credited	Summary Description
Oconee (Reactor Protection System & Emergency Safety Features Actuation System)	**Existing Equipment** **Manual Operator Action** **Diverse Actuation System** **Consequence Calculation**	Anticipated Transient Without Scram (ATWS) equipment and MOA credited for most safety functions. Diverse Manual controls added to support MOAs Two automatic DAS added for High Pressure Injection and Low Pressure Injection. Use of analog was design choice by licensee.
NuScale & Diablo Canyon (Reactor Protection System & Emergency Safety Features Actuation System) **Wolf Creek** (Main Steam Isolation)	**Internal Diversity** **Design Measures** **Existing Equipment**	For NuScale, internal diversity was credited, where the Field Programmable Gate Arrays (FPGAs) used for two divisions were diverse from the FPGA in the other two divisions. For Diablo Canyon, existing diverse systems, including ATWS were credited. Design measures such as automatic self-testing, self-calibration and surveillance testing were also credited. For Wolf Creek, internal diversity among the different channels of the MSFIS were credited, where the software algorithms used to program two channels were different from the ones used for the other two channels.
Shearon Harris (Adoption of Westinghouse SSPS Topical Report)	**Simple Design**	Augmented approach using very high number of possible states were tested, and an analysis demonstrated that the remaining untested possible states were functionally irrelevant.
Hope Creek & Browns Ferry (Power Range Neutron Monitoring System)	**Manual Operator Action**	Existing MOAs Credited
AP1000 & APR1400 (Integrated Control and Protection System)	**Diverse Actuation System** **Manual Operator Action** **Consequence Calculation**	AP1000 – FPGA-based DAS with hardwired system-level manual controls on a separate panel. The MOA capability within the DAS is credited for a few safety functions such as initiating the automatic depressurizations system. APR1400 – FGPA-based Automatic Diverse Protection System that initiates three automatic functions. One manual reactor trip function is also credited. A FPGA-based diverse indication system is included to display plant parameters during a CCF of the safety-related displays. FPGA-based.

SECY-18-0090 – Five Guiding Principles

1. Applicants and licensees for Production and Utilization Facilities under 10 CFR Part 50, “Domestic Licensing of Productions and Utilization Facilities” or under 10 CFR Part 52, “Licensees, Certifications and Approvals for Nuclear Power Plants” should continue to assess and address CCFs due to software for DI&C systems and components.

2. A defense-in-depth and diversity analysis for reactor trip systems and engineered safety features should continue to be performed to demonstrate that vulnerabilities to a CCF have been identified and adequately addressed. In performing this analysis, the vendor, applicant, or licensee should analyze each postulated CCF for each event evaluated in the accident analysis section of the safety analysis report. This defense-in-depth and diversity analysis can be either a best estimate analysis or a design-basis analysis.

3. This analyses should also be commensurate with the safety significance of the system. An analysis may not be necessary for some low-significance I&C systems whose failure would not adversely affect a safety function or place a plant in a condition that cannot be reasonably mitigated.

SECY-18-0090 – Five Guiding Principles (contd.)

4. If a postulated CCF could disable a safety function, then a diverse means, with a documented basis that the diverse means is unlikely to be subject to the same CCF, should perform either the same function or a different function. The diverse or different function may be performed by either a safety or a non-safety system if the system is of sufficient quality to perform the necessary function under the associated event conditions in a reliable manner. Use of either automatic or manual actuation within an acceptable time frame is an acceptable means of diverse actuation. If the defense-in-depth and diversity analysis demonstrates that a CCF, when evaluated in the accident analysis section of the safety analysis report, can be reasonably mitigated through other means (such as with current systems), a diverse means that performs the same or a different function may not be needed.

5. The level of technical justification needed to demonstrate that defensive measures (i.e., prevention and mitigation measures) are adequate to address potential CCFs should be commensurate with the safety significance of the DI&C system. For the systems of higher safety significance, any defensive measures credited need technical justification that demonstrates that an effective alternative to internal diversity and testability has been implemented.