NEI Common Cause Failure Policy Input

Alan Campbell
Technical Advisor
State of Digital I&C

- The Digital I&C Integrated Action Plan (IAP) has improved regulatory guidance clarity and consistency
  - RIS 2002-22 Supplement 1 provided criteria for qualitative assessments of Common Cause Failure (CCF) in low safety significant safety-related systems.
  - BTP 7-19 Revision 8 incorporated graded approach assessments into staff review guidance.
  - DI&C-ISG-06 Rev. 2 provided an Alternate Review Process to improve regulatory confidence for digital safety systems upgrades.
Why Digital Safety Systems?

- Existing systems are reaching (or have already reached) obsolescence
- Enhances safety via system diagnostic capabilities to identify and respond to issues
- Improves plant performance via improved accuracy, processing time, and automated capabilities
- Provides more data available to Operations, Maintenance and Engineering resulting in better real-time knowledge
- Reduces hardware inventory compared to existing systems

Supports long-term, safe operation of our plants
Today’s Digital Landscape

- Digital I&C technology has design features that provide for deterministic behaviors through the use modern standards
- International standards, such as IEC/IEEE, are widely accepted and have stable processes to reflect current understanding
- Hazard analysis techniques have matured and are used extensively in non-nuclear safety industries (such as aviation/aerospace, defense, automotive, and chemical industries)

NRC needs a modernized digital CCF policy that reflects today’s technology, experience, and understanding
Applicable Regulation

- 10 CFR 50.55a(h) – Codes and Standards, Protection and safety systems
  - Requires compliance with either IEEE 603-1991 or IEEE 279-1971
- IEEE requirements
  - Both IEEE standards require means to implement manual initiation of protection actions
  - Neither IEEE standard requires diversity
- RG 1.62 – Manual Initiation of Protective Actions
  - Provides guidance for manual initiation/control to meet IEEE requirements
  - Provides a staff position that diversity is required to meet BTP 7-19.

**Required codes and standards specify a means for manual initiation of protection actions, BUT do not specify diversity as a requirement.**
Applicable Regulation

- 10 CFR 50.62 – Anticipated Transient Without SCRAM (ATWS)
  - PWRs
    1) Must have diverse means of automatic Auxiliary (or Emergency) Feedwater Initiation and Turbine Trip
    2) Must have diverse SCRAM system (CE and B&W only)
  - BWRs
    3) Must have diverse Alternate Rod Injection system
    4) Must have standby liquid control system (no diversity requirement)
    5) Must have reactor coolant recirculation pump trip (no diversity requirement)

ATWS requirements for diversity are limited to specific functions and do NOT require manual, system-level actuation.
10 CFR 50 Appendix A, General Design Criteria 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. [emphasis added]

**Design techniques** are required to prevent loss of the protection function.
How Are We Addressing CCF Today?

- Branch Technical Position 7-19, Rev. 8
  - Eliminate
    - Diversity within system or component
    - Testing
    - Alternative Methods
  - Mitigate
    - Existing System
    - Manual Operator Action
    - New Diverse System
  - Acceptance
    - Bounding acceptance criteria
How Are We Addressing CCF Today?

- Branch Technical Position 7-19, Rev. 8
  - Eliminate
    - Diversity within system or component
  - Testing
  - Alternative Methods
  - Mitigate
    - Existing System – Requires “sufficient diversity”
    - Manual Operator Action – “SSCs used to support the manual operator action are diverse”
    - New Diverse System – Requires “sufficient diversity”
  - Acceptance
    - Bounding acceptance criteria
How Are We Addressing CCF Today?

- Branch Technical Position 7-19, Rev. 8
  - Eliminate
    - Diversity within system or component
  - Mitigate
    - Diversity using Existing System
    - Diversity using Manual Operator Action
    - Diversity using New Diverse System
  - Acceptance
    - Bounding acceptance criteria
How Are We Addressing CCF Today?

Primary System #1

NRC Digital Instrumentation & Control Training, Module 3.0
Regulatory Concerns, Figure 3-22
How Are We Addressing CCF Today?

Primary System #1

System Interactions (Controlled and Uncontrolled)

NRC Digital Instrumentation & Control Training, Module 3.0
Regulatory Concerns, Figure 3-22
How Are We Addressing CCF Today?

Based on the same understanding of system and interactions.

System Interactions (Controlled and Uncontrolled)
How Are We Addressing CCF Today?

- I&C OE (nuclear and non-nuclear) indicates that most systematic failures are a result of:
  - Latent design defects due to inadequate requirements
  - Uncontrolled system interactions
- An EPRI study on nuclear events¹ indicate that the primary contributing factor is requirements errors

Diversity MAY be useful in addressing hazards (e.g., CCF), BUT:

1. Diversity CAN increase plant complexity and errors.
2. Diversity MAY NOT address all sources of systematic failures.

¹ EPRI 3002005385
How Are We Addressing CCF Today?

- I&C OE (nuclear and non-nuclear) indicates that most systematic failures are a result of:
  - Latent design defects due to inadequate requirements
  - Uncontrolled system interactions
- An EPRI study on nuclear events\(^1\) indicate that the primary contributing factor is requirements errors

Industry solution to CCF is a diagnostic approach to addressing systematic failures proven effective in other industries and research.

1. EPRI 3002005385
Proposed Implementation Guidance

- NEI 20-07 Rev. D
  - Leverages EPRI Hazards and Consequence Analysis for Digital Systems\(^2\) and Digital Reliability Analysis Methodology\(^3\)
  - Provides a diagnostic approach to addressing systematic failure beginning during early stages of design process
    - Identifies missing, inadequate, or incorrect requirements
  - Diagnoses system architecture for unsafe control actions
  - Uses risk-insights to address hazards commensurate with plant risk

2. EPRI 3002016698
3. EPRI 3002018387
Research Basis

- EPRI investigated strengths and limitations of various hazard and failure analysis techniques\(^4\)
- EPRI HAZCADS and DRAM combines Fault Tree Analysis (FTA) and Systems Theoretic Process Analysis (STPA)
  - Complementary strengths
  - Reduces limitations of each method used on its own
Proposed Implementation Guidance

The applicant will:

- apply Systems Theoretic Process Analysis (STPA) to diagnose the system architecture and determine specific loss scenarios leading to hazards
- perform a Fault Tree Analysis (FTA) to determine the risk impact of loss scenarios
- map results of FTA to RG 1.174 Figures 4 and 5 regions (graded approach)
- apply control methods to address each loss scenario of STPA commensurate with results from FTA mapping
Systems Theoretic Process Analysis

- Diagnostic tool that iteratively analyzes requirements, design and system interactions

**STPA^5**

1) Define Losses and Hazards  
2) Model the Control Structure  
3) Identify Unsafe Control Actions  
Identify Loss Scenarios

Systems Theoretic Process Analysis

- Efficacy proven through blind studies
- Example blind study⁶
  - Real incident caused by digital I&C system analyzed
  - Participants were familiar with STPA and blind to the selected OE
  - Participants provided general description of the system as it existed prior to the incident
  - STPA results compared to actual flaws that led to OE

STPA anticipated exact flaw that led to OE.
STPA also identified ~9 other scenarios unaccounted for in the design.

⁶ EPRI 3002000509
Systems Theoretic Process Analysis

- Utilized in non-nuclear industries (automotive, aviation, chemical, defense, etc.)
  - Automotive Standards:
    - ISO/PAS 21448, SOTIF: Safety of the Intended Functionality
    - SAE J3187, Recommended Practice for STPA in Automotive Safety Critical Systems
  - Aviation Standards:
    - RTCA DO-356, Airworthiness Security Methods and Considerations
  - Cyber Security Standards:
  - Standards in Progress:
    - ASTM WK60748, Standard Guide for Application of STPA to Aircraft
    - SAE AIR6913, Using STPA during Development and Safety Assessment of Civil Aircraft
    - IET 978-1-83953-318-1, Code of Practice: Cyber Security and Safety
Systems Theoretic Process Analysis

- NuScale used STPA to perform a hazards analysis of I&C systems
  - DCA\(^7\) describes how STPA was used to analyze I&C systems
  - SER\(^8\) provides NRC acceptance of hazards analysis

*SER, Chapter 7 Section 7.1.8.6*

The NRC staff concludes that the application provides information sufficient to demonstrate that the proposed HA has identified the hazards of concern, as well as the system requirements and constraints to eliminate, prevent, or control the hazards. The NRC staff also concludes that the HA information includes the necessary controls for the various contributory hazards, including design and implementation constraints, and the associated commitments. The QA measures applicable to HA for developing the I&C system design conform to the QA guidance in RG 1.28 and RG 1.152. […] On this basis, the NRC staff concludes that the application provides information sufficient to demonstrate that the QA measures applied to the HA for I&C system and software life cycle meet the applicable QA requirements of GDC 1 of Appendix A to 10 CFR Part 50; Appendix B to 10 CFR Part 50; and Section 5.3 of IEEE Std. 603-1991. [Emphasis added]

Benefits of Risk

 Better system function allocation between components
 Better understanding of the impacts of system architectural decisions
 Inform the use of measures to address a potential common cause failure based upon risk significance
 Understand risk impact to specific loss scenarios
Proposed Risk Guiding Principles

- Common-Cause Failure (CCF) SECY Paper Outline, “Guiding Principles”
  - All five principles of risk-informed decision making, as listed in RG 1.174, need to be addressed satisfactorily.
  - 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.
Proposed Risk Guiding Principles

- Due to challenges modeling Digital I&C software reliability in PRA:
  - The absolute risk impact of software reliability cannot be quantitatively measured without substantial uncertainties
  - The effectiveness of applied design techniques cannot be quantitively measured without substantial uncertainties
  - There are no means of comparing design techniques to using diversity without substantial uncertainties
- NEI 20-07 Rev. D leverages concepts from RG 1.174; however, it is not completely applicable
  - This RG is used in the context of licensing basis changes, not design decisions
How Can We Use Risk Insights?

- NEI 20-07 utilizes Fault Tree Analysis to assess the risk sensitivity of each loss scenario.
- The result of the sensitivity analysis is mapped to the CDF/LERF regions and used in a graded approach to apply control measures.
Policy Considerations

- Allow for graded approaches based upon plant risk-insights to ensure applicants focus on the most risk-significant functions and to provide flexibility in meeting established system performance criteria.
- Consider the full plant defense-in-depth strategy to prevent (to the degree practicable), mitigate, or respond to a digital common cause failure.
- Allow for the use of modern hazards and/or reliability analysis techniques to examine the system for adverse conditions and identify appropriate system requirements to prevent systematic failures.
- Expand the ability to use design techniques, including diversity when applicable, to prevent (to the degree practicable), or mitigate a digital common cause failure in accordance with GDC 22.
Example Policy

1. The applicant shall assess the impact of the proposed digital instrumentation and control Reactor Protection System (RPS) and Engineered Safety Features Actuation System (ESFAS) on the plant’s defense-in-depth systems and procedures to demonstrate that vulnerabilities to digital common cause failures have been adequately addressed.

2. The applicant shall identify each digital common cause failure that could adversely impact a safety function using risk-insights, and hazards and/or reliability analysis techniques.
3. The applicant shall demonstrate commensurate with the risk significance of each identified digital common cause failure adequate measures to address the identified digital common cause failure that could adversely impact a safety function. The measures may include non-safety systems or components if they are of sufficient quality to reliably perform the necessary functions and with a documented basis that the measures are unlikely to be subject to the same common cause failure. The measures may also include monitoring and manual operator action to complete a function.