INL/MIS-24-76449-Revision-0

Common Cause Failure Analysis for Nuclear Power Plant Instrumentation and Control Systems

February 2024

Zhegang Ma

Changing the World's Energy Future

INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance, LLC

INL/MIS-24-76449-Revision-0

Common Cause Failure Analysis for Nuclear Power Plant Instrumentation and Control Systems

Zhegang Ma

February 2024

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

February 5, 2024

INL/MIS-24-76449

Zhegang Ma, Ph.D., P.E.
Zhegang.Ma@inl.gov

Common Cause Failure Analysis for Nuclear Power Plant Instrumentation and Control Systems

IAEA Virtual Consultancy Meeting on I&C CCF Research Project, 5–8 February 2024

IAEA International Atomic Energy Agency

Idaho National Laboratory

Acronyms

- BNL Brookhaven National Laboratory
- CCF common cause failure
- DI&C digital instrumentation and control
- DOE Department of Energy
- EPRI Electric Power Research Institute
- FTA fault tree analysis
- HAZCADS hazards and consequences analysis for digital systems
- HRA human reliability analysis
- I&C instrumentation and control
- IAEA International Atomic Energy Agency
- IDCCS integrated data collection and coding system
- IEC International Electrotechnical Commission
- IEEE Institute of Electrical and Electronics Engineers
- INL Idaho National Laboratory
- INPO Institute of Nuclear Power Operations
- IRIS Industry Reporting and Information System
- LER licensee event report
- LWRS light water reactor sustainability
- NRC Nuclear Regulatory Commission
- OpE operating experience
- ORNL Oak Ridge National Laboratory
- PRA probabilistic risk assessment
- RISA risk-informed systems analysis
- SPAR standardized plant analysis risk
- STPA systems-theoretic process analysis

Content

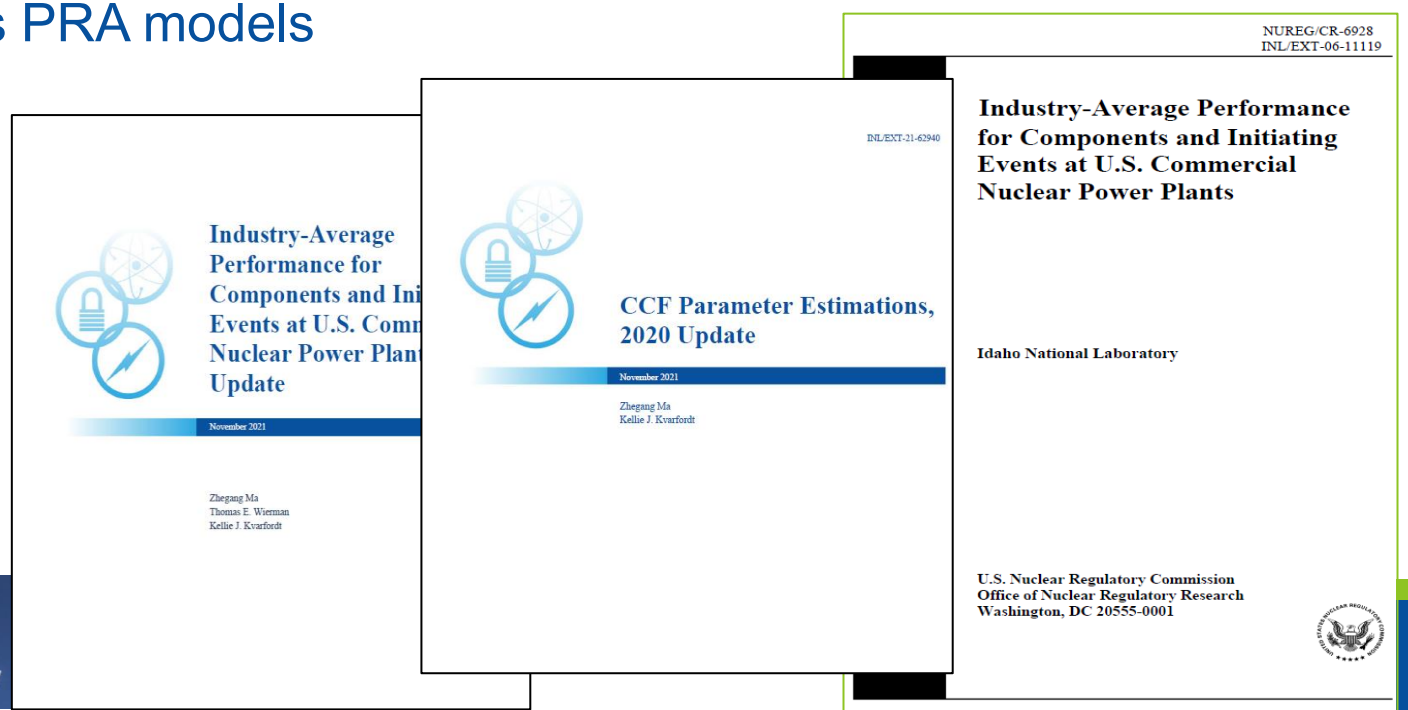
- Introduction
- INL Activities – U.S. NRC
  - Classical CCF Analysis
  - Digital I&C OpE Study
- Thoughts, Issues, and Challenges
- INL Activities – U.S. DOE LWRS
- Q&A

Introduction

- INL has provided technical assistance to the U.S. NRC in reliability and risk analysis including the OpE program since the 1980s
- The U.S. nuclear OpE data sources include
  - INPO IRIS Database
  - Licensee Event Reports
  - Event Notification Reports
  - Monthly Operating Reports
- In early 2000s, INL developed the Integrated Data Collection and Coding System to capture and characterize nuclear industry OpE data

Introduction (cont.)

- OpE data are characterized for different studies
  - **Component Failure**: system, component type, failure mode, p-value, failure cause…
  - **Initiating Event**: loss-of-offsite power, general transients, LOCAs…
  - **CCF**: failure cause, coupling factor, shared cause factor, time delay factor…
- These studies provide input parameters to the NRC's SPAR models as well as the industry's PRA models



INL Activities – U.S. NRC: Classical CCF Analysis

- NUREG/CR-4780 and NUREG/CR-5485 provide guidelines and procedures on modeling CCFs in PRA
  - **Alpha Factor Model**
  - Impact vector and mapping methods
- NUREG/CR-6268 provides the guidance for collecting, classifying, and coding CCF events and describes the **CCF database and software system** that is used to estimate CCF parameters
- NUREG/CR-5497 estimates CCF parameters for the majority of the **risk important safety systems and components** in commercial NPPs based on the CCF data collection effort from 1980–1995
- INL/EXT-21-62940 was published in 2022 updating CCF parameter estimates with data from 2006–2020

INL Activities – U.S. NRC: Classical CCF Analysis (cont.)

- Classical CCF analysis is focused on the PRA components
  - Motor-driven pumps
  - Diesel generators
  - Motor-operated valves
  - Breakers
- The failure modes are related to the PRA components
  - Fail to start
  - Fail to run
  - Fail to operate
  - Fail to open
  - Spurious operation

INL Activities – U.S. NRC: Digital I&C OpE Study

- To support the NRC's DI&C Study, INL conducted a limited DI&C literature review focusing on OpE and reliability analysis
  - NRC studies in NUREG and contractor (ORNL, BNL, etc.) reports
  - Industry studies including EPRI reports
  - IAEA reports
  - IEEE and IEC standards
- INL is currently reviewing about 2,000 INPO IRIS events that are coded with the cause category of *Digital/Cyber/Instrumentation Condition*
- The objective is to incorporate DI&C failure events into the IDCCS database and conduct DI&C reliability and CCF analysis

INL Activities – U.S. NRC: Digital I&C OpE Study (cont.)

- The new DI&C coding system would include fields for both DI&C component and the PRA component it impacted

For DI&C Equipment

- Device ID
- System
- Component Type
- Failure Mode
- P Value
- Failure Cause
- Detection
- Recovery
- Number of Failures

- **For Impacted PRA Component**
  - Device ID
  - System
  - Component Type
  - Failure Mode
  - P Value
  - Failure Cause

INL Activities – U.S. NRC: Digital I&C OpE Study (cont.)

- Two Different Kinds of DI&C CCF
  - DI&C "Internal" CCF: CCF among redundant DI&C equipment in different trains of the DI&C system
    - Can be treated with current CCF analysis process
  - DI&C "External" CCF: DI&C failures that impact and trigger multiple outside-of-DI&C-system key component failures
    - New area for CCF study
    - The impacted "external" key components could be
      - Redundant within the same system → same function
      - In the same system but not redundant → multiple functions
      - In different systems → multiple functions
- DI&C "Internal" CCF analysis would be needed for DI&C system reliability analysis
- DI&C "External" CCFs would need more focus as they are new and can lead to unanalyzed risks that are not included in the existing models

INL Activities – U.S. NRC: Digital I&C OpE Study (cont.)

For DI&C "Internal" CCF

- CCCG
- Event Type => CCF Type = Internal?
- Event Level
- Cause Code
- Coupling Factor
- Coupling Strength
- Defense Mechanism
- Shock Type
- Time Delay Factor
- Failure Mode App

For DI&C "External" CCF

- No CCCG?
- CCF Type = External
- DCCG – Digital Cause Component Group?
- Coupling Factor
- Coupling Strength
- Defense Mechanism
- Shock Type
- Time Delay Factor

Thoughts, Issues, and Challenges

- In general, I&C (including DI&C) is within the PRA key component boundary →
  - The key component's failure probability estimates have included the contributions from I&C
- However, intersystem component failures due to the common cause of DI&C are not included in the current SPAR or industry PRA models
  - Existing CCF database and parameter estimates are limited to the redundant components in the same system
- This is likely the biggest CCF concern and the largest risk contributor that we should work on

Thoughts, Issues, and Challenges (cont.)

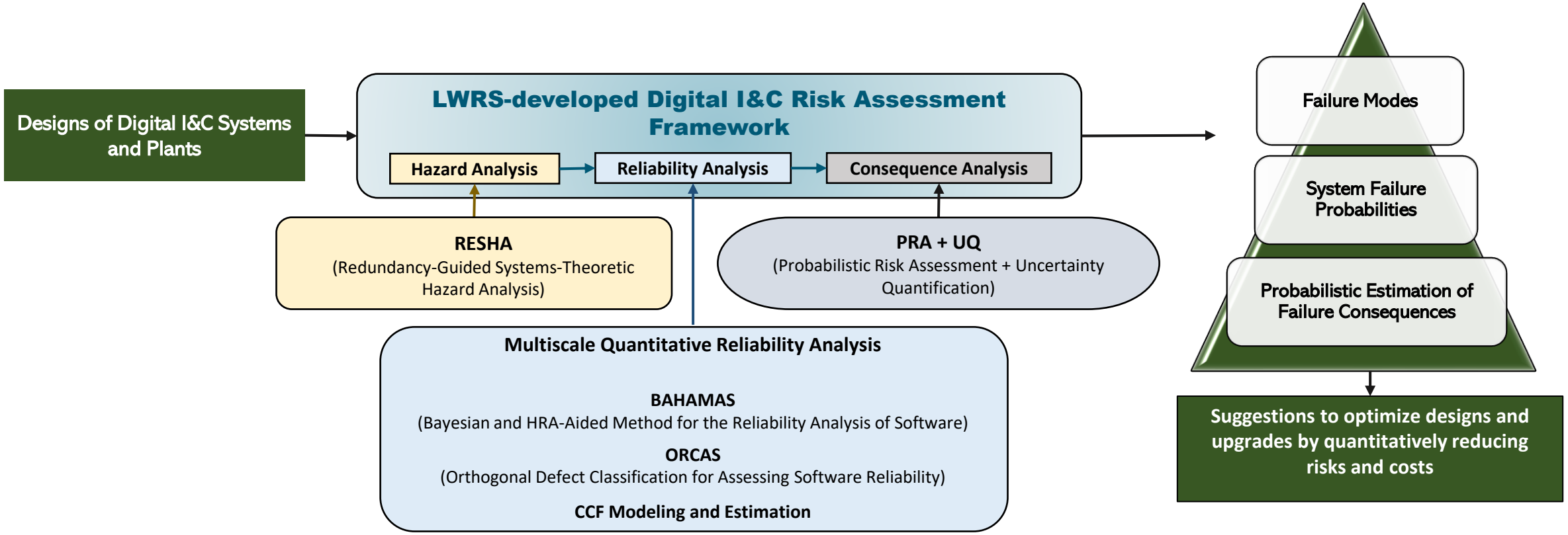
- Do we have sufficient OpE data to support the data-driven DI&C analysis?
  - Of the 2,000 IRIS failures events with the digital cause category, how many were actual DI&C failures?
  - What about LERs?
  - If we can obtain the number of DI&C failures, can we get their demands or run hours?
- Can we find a good DI&C coding system that meets most of needs?
- How to assess the impacted multiple components and functions that are outside of the scope of classical CCF analysis?
  - New methodology for DI&C "External" CCF?
- Representative DI&C systems and their descriptions will be needed for specific digital I&C study

INL Activities – U.S. DOE LWRS

- The U.S. DOE LWRS Program RISA Pathway supports plant owner-operator decisions with the aim to improve the economics, reliability, and maintain the high levels of safety of current nuclear power plants over periods of extended plant operations
- The goals of the LWRS DI&C Risk Assessment project:
  - Evaluate the design architecture of various DI&C systems to support system design decisions on diversity and redundancy applications
  - Develop approaches to address CCFs and estimate corresponding risk for DI&C technologies
  - Support existing risk-informed DI&C design guides by providing quantitative risk-informed evidence

INL Activities – U.S. DOE LWRS (cont.)

The LWRS DI&C Risk Assessment Framework



INL Activities – U.S. DOE LWRS (cont.)

- **Hazard Analysis**
  - Incorporates the concept of combining FTA and STPA from HAZCADS
  - Reframes STPA in a redundancy-guided way to identify various CCFs in highly redundant DI&C systems
  - Identifies and traces failures in both the actuation and information feedback pathway of DI&C systems due to unintended latent design or implementation defects or intended cyberattacks

INL Activities – U.S. DOE LWRS (cont.)

- **Reliability Analysis**
  - Bayesian and HRA-Aided Method for the Reliability Analysis of Software
    - Developed for the conditions with limited testing/operational data or for reliability estimations of software in early development stage
    - Provide an estimation of failure probabilities to support the design of software and target DI&C systems
  - Orthogonal Defect Classification for Assessing Software Reliability
    - Developed for the conditions with sufficient testing/operational data
    - A more refined estimation of software failure probabilities can be provided

INL Activities – U.S. DOE LWRS (cont.)

- **Reliability Analysis**
  - Bayesian and HRA-Aided Method for the Reliability Analysis of Software
    - Developed for the conditions with limited testing/operational data or for reliability estimations of software in early development stage
    - Provide an estimation of failure probabilities to support the design of software and target DI&C systems
  - Orthogonal Defect Classification for Assessing Software Reliability
    - Developed for the conditions with sufficient testing/operational data
    - A more refined estimation of software failure probabilities can be provided

Questions?

Idaho National Laboratory

Battelle Energy Alliance manages INL for the U.S. Department of Energy's Office of Nuclear Energy. INL is the nation's center for nuclear energy research and development, and also performs research in each of DOE's strategic goal areas: energy, national security, science and the environment.