INL/MIS-23-75814-Revision-0

Digital Instrumentation & Controls Study with Operating Experience Data

November 2023

Zhegang Ma, Tao Liu

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

DISCLAIMER

This information was prepared as an account of work sponsored by an agency of the U.S. Government. Neither the U.S. Government nor any agency thereof, nor any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness, of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the U.S. Government or any agency thereof.

INL/MIS-23-75814-Revision-0

Digital Instrumentation & Controls Study with Operating Experience Data

Zhegang Ma, Tao Liu

November 2023

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

November 2023

Zhegang Ma, Ph.D., P.E.

Tao Liu, Ph.D.

INL/MIS-23-75814

Digital Instrumentation & Controls Study with Operating Experience Data

Idaho National Laboratory

Background – Digital I&C Implementation Status in U.S. NPPs

- **Regulatory Advancements:**
  - The NRC has updated policies and guidelines to facilitate the implementation of digital instrumentation and control (I&C) systems in nuclear power plants (NPPs)[1]
- **Industry Transition:**
  - Dozens of small modular reactor and advanced reactor designs are in development, incorporating digital I&C systems from inception[2]
- **Plant Modernization:**
  - Duke Energy's Oconee Nuclear Station: $250 million upgrade for the first integrated digital Reactor Protection System (RPS) and Engineered Safety Protection System (ESPS) I&C system[3]
  - Broader Adoption: Numerous utilities have transitioned to digital control systems in non-safety-related applications; additionally, a select few have pioneered the replacement of small safety-related systems with digital technology[4]

[1] U.S. NRC, "Modernizing the Regulatory Infrastructure for Digital I&C."
[2] ANS, "Nuclear I&C Modernization: The Future is Digital."
[3] Nuclear Engineering International, "USA's first fully digital station."
[4] Kelley, S, & Bolian, T W. "Plant Modernization with Digital Reactor Protection System Safety System Upgrades at US Nuclear Power Stations."

Background – Comparing Analogue and Digital I&C Systems

Feature	Analogue I&C	Digital I&C
Signal Representation	Continuous signals	Discrete (binary) signals
Technology	Mechanical or electrical systems	Microprocessors and software
Accuracy and Precision	May have less precision	Higher precision
Data Processing	Real-time, direct processing	Requires conversion, then processing
Maintenance	May require more physical maintenance	Software updates and cybersecurity measures
Upgradability	Challenging to upgrade	Easier to upgrade with software updates
Integration with Other Systems	May have limited integration capabilities	Easier integration with other digital systems
Diagnostic Capabilities	Limited diagnostic capabilities	Enhanced diagnostic capabilities
Cost	Higher operating and maintenance costs	Higher initial cost but potentially lower maintenance costs
Cybersecurity	Less susceptible to cybersecurity threats	Requires robust cybersecurity measures
Regulatory Approval	Established approval processes	Rigorous, evolving approval processes

DI&C OpE Study – Purposes

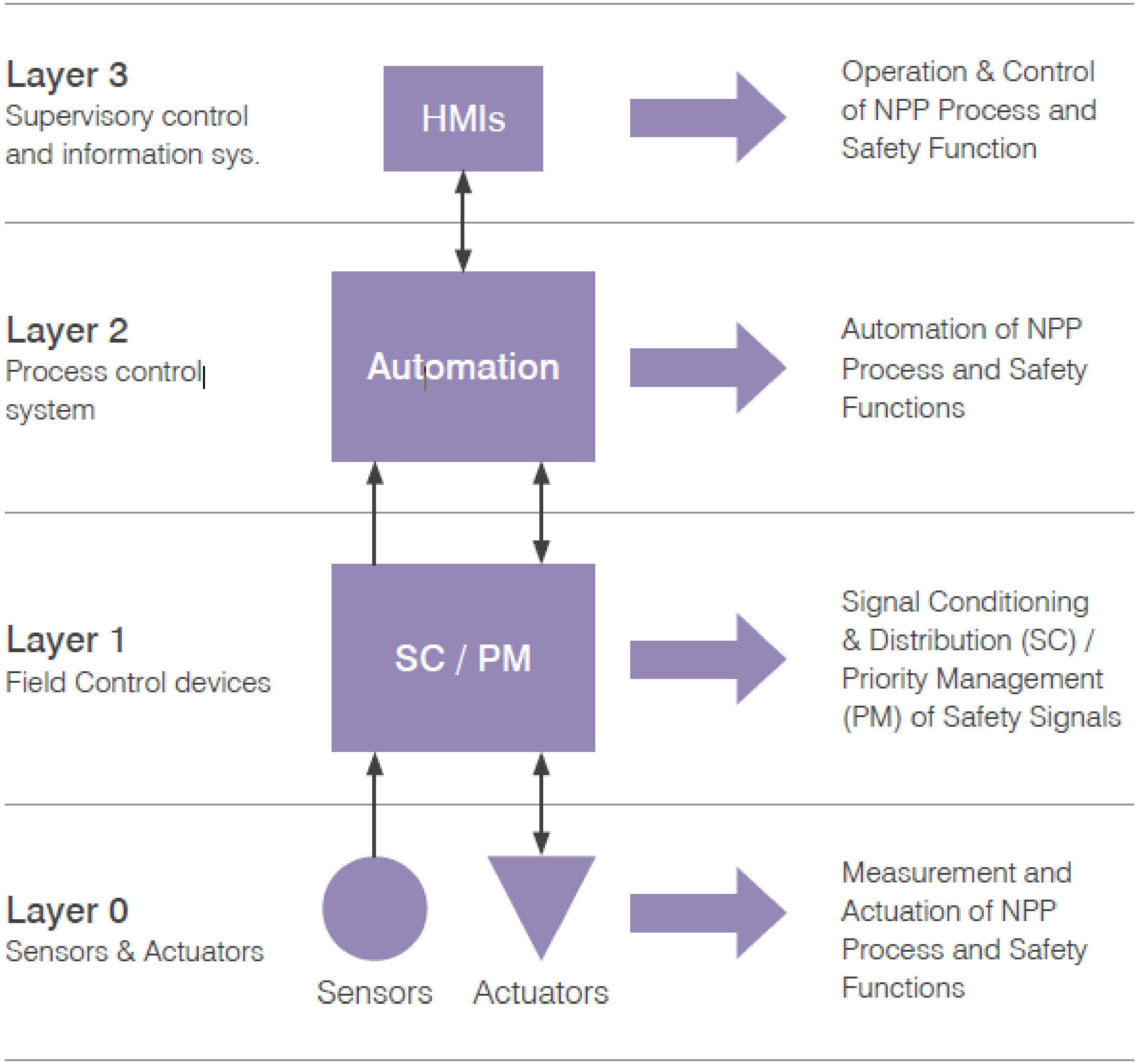
1. Provide Data Analysis Support for Digital I&C (DI&C) Risk Assessment using Nuclear Industry Operating Experience (OpE) Data
2. Estimate Reliability Parameters for DI&C Equipment (Including Software) as Supported by OpE Data
3. Estimate Common-Cause Failure (CCF) Parameters for DI&C Equipment (Including Software) as Supported by OpE Data
4. If Needed, Provide DI&C System Level Reliability Estimate for Specific DI&C Applications

DI&C OpE Study – Literature Review

- 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

BNL:	Brookhaven National Laboratory
EPRI:	Electric Power Research Institute
IAEA:	International Atomic Energy Agency
IEC:	International Electrotechnical Commission
IEEE:	Institute of Electrical and Electronics Engineers
INL:	Idaho National Laboratory
ORNL:	Oak Ridge National Laboratory

Literature Review – IAEA, I&C Architectures



Layer 3
Supervisory control and information sys.
HMIs
Operation & Control of NPP Process and Safety Function
Layer 2
Process control system
Automation
Automation of NPP Process and Safety Functions
Layer 1
Field Control devices
SC / PM
Signal Conditioning & Distribution (SC) / Priority Management (PM) of Safety Signals
Layer 0
Sensors & Actuators
Sensors
Actuators
Measurement and Actuation of NPP Process and Safety Functions

Figure 5. I&C Layer Concept (according to IAEA NP-T-2.11 [13])

Literature Review – IEEE, I&C Failure Mode

Failure Mode Categorization	Failure Mode
Catastrophic	Zero or maximum output No change of output with change of input Functioned without signal No function with signal
Degraded	Erratic output, high output, low output Functioned at improper signal level Intermittent operation
Incipient	Has not failed (yet)

Source: Adapted from (IEEE) Std. 500, "IEEE Guide to the Collection and Presentation of Electrical, Electronic, Sensing Components, and Mechanical Equipment Reliability and Mechanical Equipment Reliability Data for Nuclear Power Generating Stations."

Literature Review – Dunn Study, Computer Hardware Failures

Digital Component	Failure Mechanisms	Failure Modes
CPU (microprocessor) integrated circuits	Die attachment failure Metallization failure Contamination Cracked/fractured Oxide defects	High leakage current Output stuck low Shorted
Memory (MOS integrated circuit)	Mechanical failure	Data bit loss Short Open Slow transfer of data
Digital integrated circuit (general)	Die attachment failure Metallization failure Contamination Oxide defects Wire bond failure Package-related failure	Open Shorted Output stuck high Output stuck low Supply open

Source: Adapted from W. Dunn, *Practical Design of Safety-Critical Computer Systems*, Reliability Press, 2002.

Literature Review – IEC, Digital Data Communication Failure Mode

Failure Modes	Description
Data corruption	Message corruption due to errors or interference
Unintended repetition	Old messages repeated at incorrect times due to errors
Incorrect sequence	Messages from a source in the wrong sequence due to errors
Data loss	Messages not received or acknowledged due to errors
Unacceptable delay	Excessive message delays due to various factors
Insertion	Unexpected messages inserted due to faults or interference
Masquerade	Invalid messages appear legitimate due to interference
Addressing	Messages sent to the wrong recipient due to faults

Source: Adapted from IEC 61784-3, "Digital Data Communications for Measurement and Control—Profiles for Functional Safety Communications in Industrial Networks."

Literature Review – Digital I&C Failure Parameters in NPP

Source: Adapted from ORNL/TM-2006-626, “Industry Survey of Digital I&C Failures,” 2007.

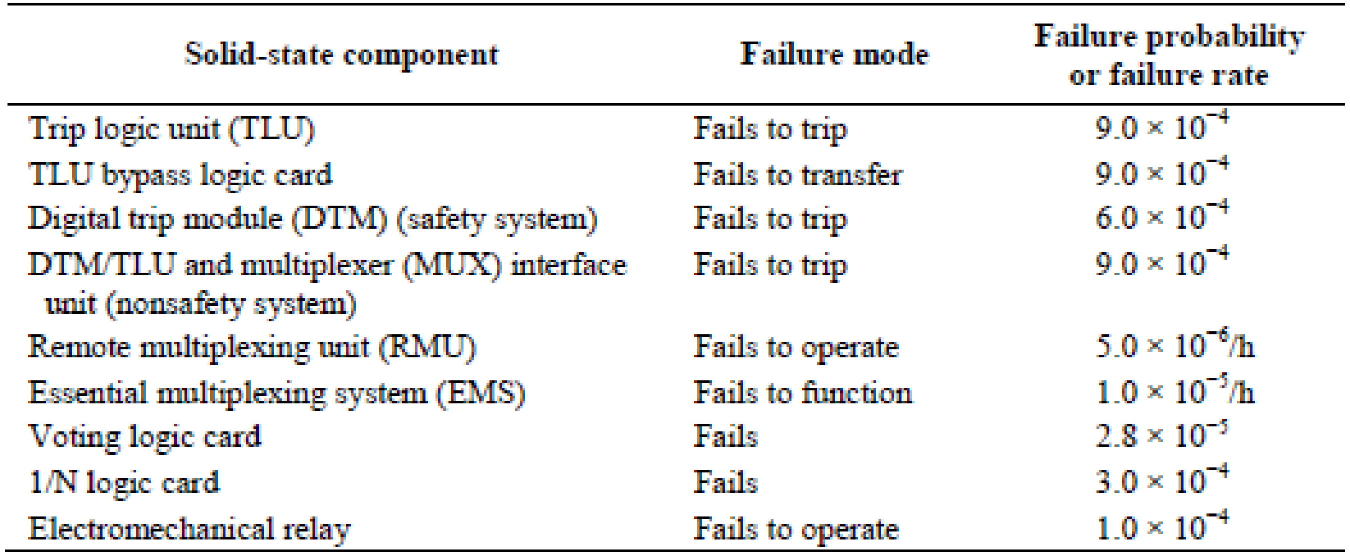
- Lungmen, GE ABWR

Solid-state component failure modes and failure probabilities used in the Lungmen PRA

Solid-state component	Failure mode	Failure probability
Digital trip module	Fails to trip	1.2×10^{-4}
Digital trip multiplexer	Fails to trip	1.66×10^{-3}
Remote multiplexing unit (RMU)	Fails to operate	2.40×10^{-4}
System logic units	Fails to function	1.2×10^{-5}

- GE ESBWR

Solid-state component failure modes and failure probabilities used in the GE ESBWR PRA

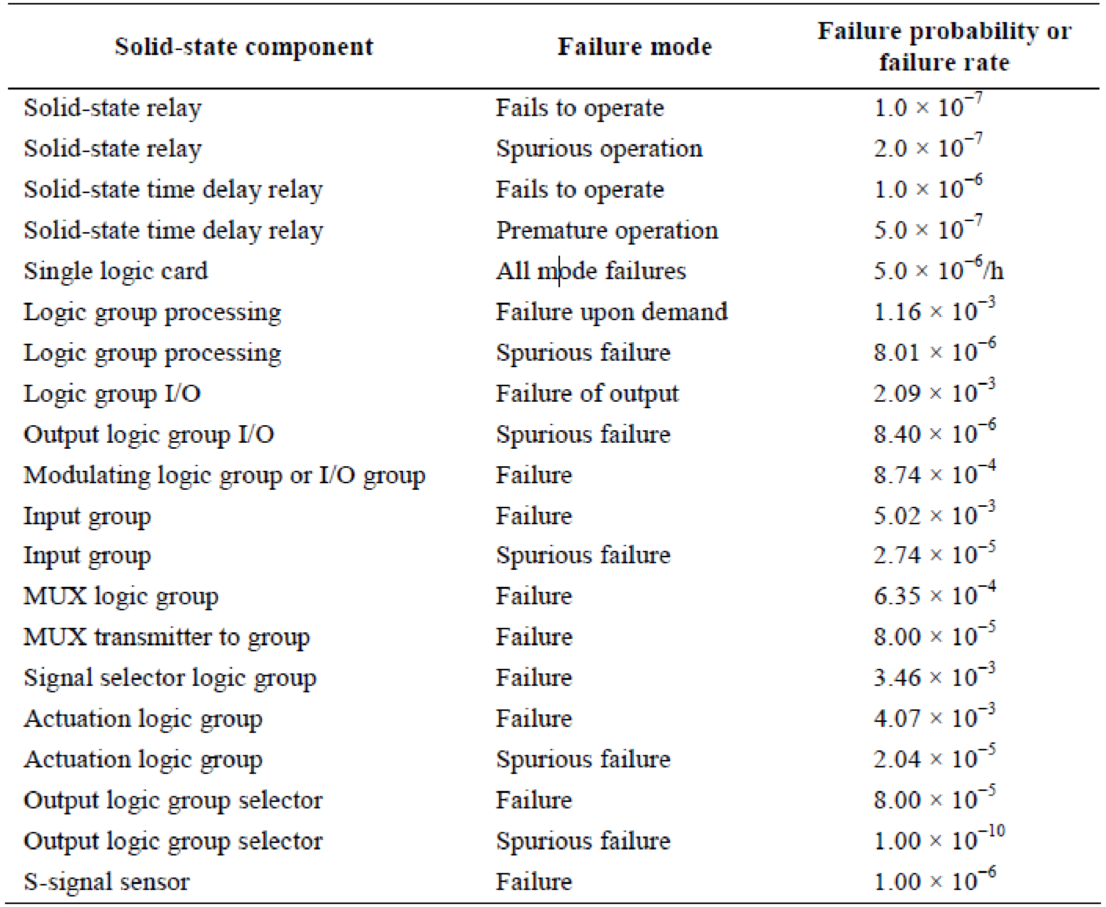


Solid-state component	Failure mode	Failure probability or failure rate
Trip logic unit (TLU)	Fails to trip	9.0×10^{-4}
TLU bypass logic card	Fails to transfer	9.0×10^{-4}
Digital trip module (DTM) (safety system)	Fails to trip	6.0×10^{-4}
DTM/TLU and multiplexer (MUX) interface unit (nonsafety system)	Fails to trip	9.0×10^{-4}
Remote multiplexing unit (RMU)	Fails to operate	5.0×10^{-6}/h
Essential multiplexing system (EMS)	Fails to function	1.0×10^{-5}/h
Voting logic card	Fails	2.8×10^{-5}
1/N logic card	Fails	3.0×10^{-4}
Electromechanical relay	Fails to operate	1.0×10^{-4}

Literature Review – Digital I&C Failure Parameters in NPP (Cont.)

- AP600 and AP1000

Solid-state component failure modes and failure probabilities used in the AP600 and AP1000 PRAs



Solid-state component	Failure mode	Failure probability or failure rate
Solid-state relay	Fails to operate	1.0×10^{-7}
Solid-state relay	Spurious operation	2.0×10^{-7}
Solid-state time delay relay	Fails to operate	1.0×10^{-6}
Solid-state time delay relay	Premature operation	5.0×10^{-7}
Single logic card	All mode failures	5.0×10^{-6}/h
Logic group processing	Failure upon demand	1.16×10^{-3}
Logic group processing	Spurious failure	8.01×10^{-6}
Logic group I/O	Failure of output	2.09×10^{-3}
Output logic group I/O	Spurious failure	8.40×10^{-6}
Modulating logic group or I/O group	Failure	8.74×10^{-4}
Input group	Failure	5.02×10^{-3}
Input group	Spurious failure	2.74×10^{-5}
MUX logic group	Failure	6.35×10^{-4}
MUX transmitter to group	Failure	8.00×10^{-5}
Signal selector logic group	Failure	3.46×10^{-3}
Actuation logic group	Failure	4.07×10^{-3}
Actuation logic group	Spurious failure	2.04×10^{-5}
Output logic group selector	Failure	8.00×10^{-5}
Output logic group selector	Spurious failure	1.00×10^{-10}
S-signal sensor	Failure	1.00×10^{-6}

Source: Adapted from ORNL/TM-2006-626, “Industry Survey of Digital I&C Failures,” 2007.

DI&C OpE Study – Data Sources

- Industry Reporting and Information System (IRIS) Database from Institute of Nuclear Power Operations (INPO)
- Licensee Event Reports (LERs)

DI&C OpE Study – IRIS Database

- INPO proposed and added a set of event codes for digital systems and equipment in 2011 in its efforts to track DI&C performance
- One Cause Category - Digital/Cyber/Instrumentation Condition
- Four Cause Factors
  - Digital Hardware Deficiency
  - Erratic/Intermittent/Erroneous Performance
  - Misalignment/Incorrect Setpoints or Gain
  - Software/Firmware Deficiency
- About 2,000 IRIS failures with the above Digital Cause Category/Factors
- Range from 1997 to 2023
- *INL is reviewing these IRIS events and trying to incorporate DI&C into INL's Integrated Data Collection and Coding System (IDCCS)*

DI&C OpE Study – Examples of Existing Coding

- IRIS Component Type
  - Instrument Controllers, Integration/Computation Module, Control Board/Panel, Software
- RADS Subcomponent and Piecepart
  - Control Switch, Controller, I&C, Limit Switch, Logic Circuit, Relay
  - Control Module, Sensors, Voltage Regulating Module, Wires
- RADS Failure Mode
  - Automatic Close or Open, Fail to Close or Open, Fail to Control, Fail to Run, Fail to Start, Spurious Operation

RADS: Reliability and Availability Data System

DI&C OpE Study – LERs

- BNL conducted an LER search of DI&C failure events from 2005 to 2015 for the NRC in 2016
- 97 potential DI&C-related events were identified
- 18 of the events were believed to be CCF
- *The above study could be continued by reviewing LERs from 2016 to 2023*
- *INL routine LER reviews for initiating event (IE) and loss-of-offsite-power (LOOP) study could be expanded to include DI&C study*

DI&C OpE Study – IDCCS Coding

- The original thought was to integrate DI&C coding into the existing failure data study
  - **Key Components** would still be generator (GEN), motor-drive pump (MDP), motor-operated valve (MOV), turbine-driven pump (TDP), etc.
  - DI&C could be added to the list of **Subcomponent** which currently includes items such as actuator, breaker, driver, governor, I&C, logic circuit, miscellaneous, motor, pump, relay, sequencer, various, and wires-connectors-board, etc.
  - Then the DI&C equipment (software, controller, etc.) could be added to the list of **Piecepart** which currently includes items such as alarm module, bearing, body, I&C, instrumentation, limit switch, logic circuit, relay, piping, plug, switch, tank, etc.

DI&C OpE Study – IDCCS Coding (cont.)

- However, the integration with the failure database approach may not be sufficient or suitable for the purposes of DI&C study
  - The existing failure database is focused on the PRA components such as MDPs, TDPs, and MOVs
  - The failure modes are related to the PRA components, e.g., fail to start (FTS), fail to run (FTR), fail to operate (FTOP), fail to open (FTO), and spurious operation (SOP)
  - On the other hand, DI&C studies should look at DI&C systems/equipment and their unique failure modes
  - For example, we could define software failure mode as FTOP, but a software FTOP could lead to a valve FTO or SOP
  - In the current failure database, we are not concerned with the failure modes of a subcomponent or piecepart, since the key system components and their failure modes are what is modeled in PRAs
  - This is not the case for DI&C because the failure impact may be more pervasive across systems

DI&C OpE Study – IDCCS Coding (cont.)

- The basic data fields for the new DI&C coding system would include

- Same as Current Failure Database **for DI&C Equipment**
  - Device ID
  - System
  - Component Type
  - Failure Mode
  - P Value
  - Failure Cause
  - Detection
  - Recovery
  - Number of Failures
  - Notes

- New Failures for DI&C Study **for Impacted Key Component**
  - Device ID
  - System
  - Component Type
  - Failure Mode
  - P Value
  - Failure Cause

DI&C OpE Study – DI&C CCF

- 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

DI&C OpE Study – DI&C CCF (cont.)

- BNL 2016 DI&C LER Report indicates that “*Non-safety-related systems (i.e., control systems) may not have redundancy and CCF may not be of too much concern,*” which seems to refer to the DI&C “Internal” CCF
- Example OpE event – Ginna, 2/16/2005

  “Failure of redundant I/O power supplies for the Advanced Digital Feedwater Control System (ADFCS) resulted in a loss of main feedwater and an automatic reactor trip Subject: OE20089 - Failure of redundant I/O power supplies for the Advanced Digital Feedwater Control System (ADFCS) resulted in the loss of ADFCS system which caused the ***main feedwater valves*** *to close. This failure initiated a feedwater transient which resulted in a plant trip.”*

DI&C OpE Study – DI&C CCF (cont.)

- EPRI 3002002990 presents an example that a DI&C single failure could trigger a loss of multiple functions:

  "A single controller controls both feedwater regulating valves (FRV) and both feedwater pumps (FWP), so a single controller misbehavior could cause simultaneous overfeed of both steam generators (S/G), leading to a reactor trip."

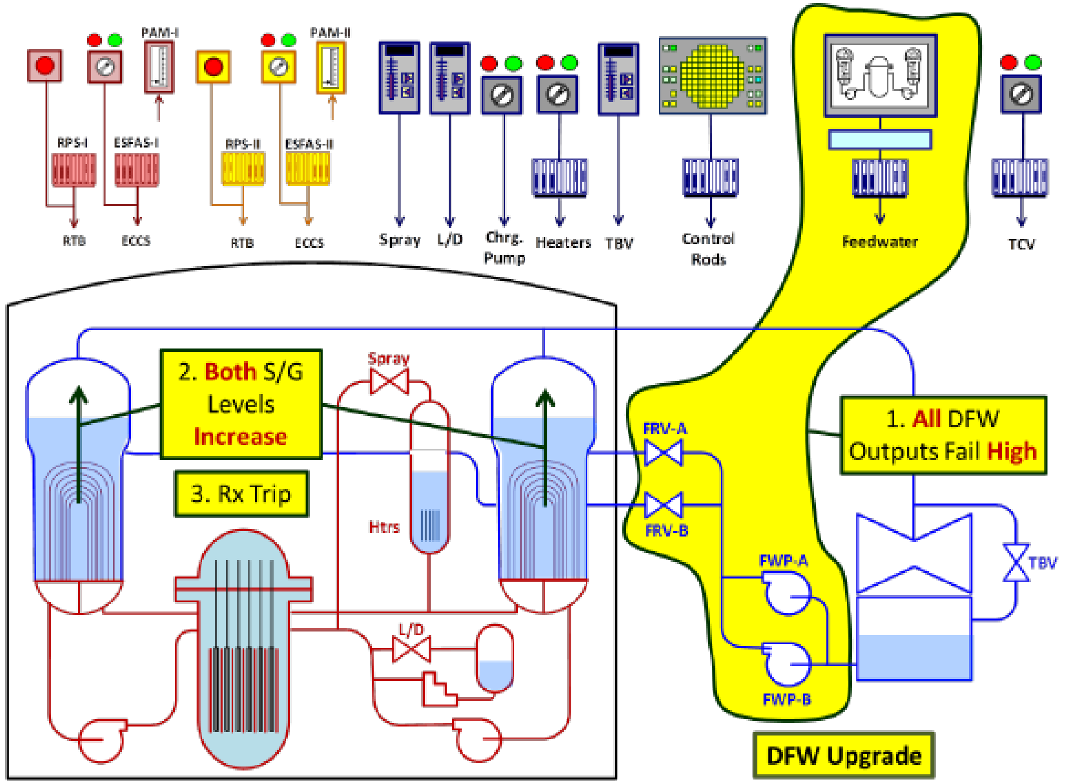


Figure 2-2
Analog Plant with a Digital Feedwater Control (DFW) Upgrade

DI&C OpE Study – DI&C CCF for IDCCS

- Similar with Current CCF Database 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

- New 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

DI&C OpE Study – Issues/Challenges

- Do we have sufficient OpE data to support the data-driven DI&C analysis?
  - Of the 2000 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?
  - New methodology for DI&C “External” CCF?
- For the next phase of DI&C System Reliability analysis, we may need to select the representative DI&C systems and their descriptions

DI&C OpE Study – Other Discussions

- In general, I&C is within the PRA key component (e.g., MDP, TDP) boundary (and so should DI&C) → the key component's failure probability estimates should have already entailed the contributions from I&C (and DI&C, if applicable)
- However, inter-system component failures due to the common cause of DI&C are most likely not considered or included in the current SPAR (and 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 are worrying about in DI&C as they are not calculated and included in PRA
- This is the so called "external" DI&C CCF in this presentation, which is a term used in DI&C OpE data collection and characterization distinguished from the "internal" CCF that would occur within the DI&C redundant trains

INL

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.

WWW.INL.GOV