Reliability Study of Digital Instrumentation and Control Systems in Nuclear Power Plants: Insights from Operating Experience Data

Tao Liu[a], Zhegang Ma[b], and John Lane[c]

[a]Idaho National Laboratory, Idaho Falls, ID, USA, Tao.Liu@inl.gov
[b]Idaho National Laboratory, Idaho Falls, ID, USA, Zhegang.Ma@inl.gov
[c]Nuclear Regulatory Commission, Washington, DC, USA, John.Lane@nrc.gov

Abstract: Digital instrumentation and control (DI&C) systems are increasingly used in nuclear power plants (NPPs), but their reliability and risk contribution remain difficult to quantify because operating experience is limited, failure modes are not consistently classified, and hardware-software dependencies are not well represented in conventional probabilistic risk assessment (PRA) models. Idaho National Laboratory (INL), under sponsorship from the U.S. Nuclear Regulatory Commission (NRC), reviewed operating experience from the NRC Licensee Event Report (LER) database and the Institute of Nuclear Power Operations (INPO) Industry Reporting and Information System (IRIS). The LER review identified safety-significant DI&C events reported from 2016 through 2023, while the IRIS review screened broader operating experience from 1997 through 2023. This paper summarizes the data screening approach, key LER and IRIS findings, dominant affected systems and components, common failure modes and causes, and the implications for DI&C reliability estimation, common-cause failure (CCF) treatment, and PRA modeling. The results show that the available data support structured event classification and risk-informed screening, but improved device identification, demand or run-hour data, and failure-cause documentation are needed before routine DI&C component reliability estimation can be performed in the same manner as existing hardware reliability studies.

1. INTRODUCTION

DI&C systems are used in NPP monitoring, control, actuation, diagnostics, and operator information functions. Compared with analog instrumentation and control (I&C) systems, digital systems rely on processors, programmable logic controllers (PLCs), software, digital communications, and human-system interfaces. These features can add self-diagnostics, data processing, display functions, and flexible control logic, but they also introduce failure mechanisms that are not always represented by traditional hardware-centered reliability models.

Reliability and risk assessment for DI&C systems must address failure-mode classification, software and configuration errors, hardware-software interdependence, and CCF. These issues affect how DI&C failures are screened, coded, quantified, and modeled in PRA. The available operating experience data also limit the analysis because many digital failures are described at a functional level rather than with the diagnostic detail needed for component reliability estimation.

Recently, the NRC initiated an INL study to evaluate the feasibility of estimating DI&C component and system reliability parameters, including CCF parameters, from existing nuclear industry operating experience. The study reviewed LERs and INPO IRIS events to identify DI&C-related failures, classify affected systems and components, characterize failure modes and causes, and evaluate how the data could support the Integrated Data Collection and Coding System (IDCCS), the Reliability and Availability Data System (RADS), and PRA applications. A detailed report for this NRC-sponsored study has been prepared as NUREG/CR-7313 and is currently under NRC review [1].

This paper reviews prior DI&C reliability studies, describes the operating experience screening methodology, presents LER and IRIS results, and identifies data limitations relevant to DI&C reliability estimation and risk assessment. The scope is U.S. operating experience. Cybersecurity events are considered only when they appear in the operating experience coding used for screening.

2. DI&C OVERVIEW

I&C systems monitor plant conditions and provide control or actuation signals. They include sensors, signal processors, actuators, and human-system interfaces used to monitor and regulate plant parameters such as temperature, pressure, and flow. As shown in Figure 1, sensors measure process parameters, and signal conditioning and data acquisition convert the raw sensor outputs into a form that can be processed and compared with setpoints or operating thresholds. Signal-processing logic evaluates deviations from desired values and generates commands to actuators, such as valves or motors. The objective is to maintain plant conditions within design and operating limits [2].

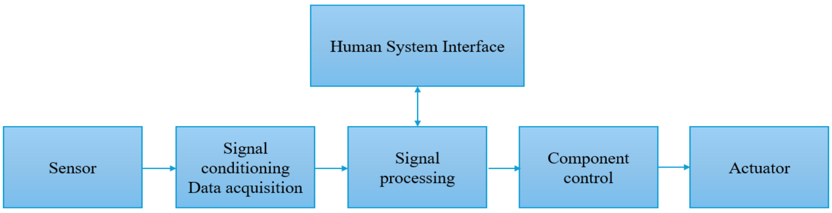

Figure 1: Typical I&C function (adapted from Reference [2]).

The Nuclear Energy Institute [3] defines a digital asset as "a programmable device (e.g., Erasable Programmable Read Only Memory (EPROM), microprocessor, etc.) that uses any combination of hardware, firmware, and/or software to execute internally stored programs and algorithms, including numerous arithmetic or logic operations, without operator action." Analog systems use continuous voltages or currents to represent measured parameters. These signals are processed using analog electronics, such as amplifiers and filters, and can directly control actuators. Digital systems convert analog signals into binary values using analog-to-digital converters (A/D). Processors then execute control algorithms and generate output signals, which may be converted back to analog form through digital-to-analog converters (D/A) to drive actuators [2].

For reliability analysis, the practical DI&C boundary includes the digital processing equipment, input/output (I/O) modules, communication modules, power supplies, displays, software, firmware, and configuration data that support the monitored or controlled plant function. Failures may appear as loss of function, incorrect output, delayed response, loss of communication, processor lockup, spurious actuation, or degraded monitoring. For this reason, PRA models often need to represent the affected plant function as well as the failed digital device.

3. PRIOR STUDIES AND DATA BASIS FOR DI&C RELIABILITY ASSESSMENT

3.1. PRA Modeling Challenges for DI&C Systems

Several NRC-sponsored studies describe limitations in applying conventional PRA methods to DI&C systems. NUREG/CR-6962 identified limitations in traditional PRA treatment of software, digital dependencies, and CCF, and recommended additional modeling and expert-elicitation approaches where operating data are sparse [4]. NUREG/CR-6997 used a digital feedwater control system case study to examine how digital control failures could be represented in fault trees and event logic [5]. NUREG/CR-6942 reviewed dynamic reliability methods for digital systems, including approaches that capture timing, state dependence, and hardware-software interactions [6].

These NRC contractor studies indicate that DI&C PRA modeling cannot rely only on the static hardware-centered treatment used for many analog systems. NUREG/CR-6962 identified software reliability, digital CCF, and component interdependence as areas where conventional fault-tree treatment is limited [4]. NUREG/CR-6997 showed that Markov modeling and failure modes and effects analysis can represent some digital feedwater control system behavior, but also noted practical limits related to model size, transition probabilities, and software-failure data [5]. NUREG/CR-6942 further showed that timing, sequence, and state-dependent behavior may require dynamic reliability methods when digital system behavior affects accident sequence progression [6]. These findings indicate a need for operating experience data that link DI&C components, software or configuration mechanisms, failure modes, and credited plant functions.

3.2. Operating Experience Studies and CCF Insights

Prior operating experience studies provide context for the LER and IRIS review in this paper. The Brookhaven National Laboratory (BNL) LER study of 2005-2015 events identified 97 relevant digital I&C events out of 618 reviewed LERs, including 18 potential or confirmed CCF events [7]. An earlier NRC Analysis and Evaluation of Operational Data (AEOD) review of computer-based digital system failures identified software, human-system interface, electromagnetic interference, and random component failures, with software and human-system interface issues accounting for a large fraction of the reviewed events [8].

Electric Power Research Institute (EPRI) studies of digital CCF found that safety-related systems were more often affected by hardware failures, human errors, and procedure issues, while non-safety systems showed more design-related hardware and software vulnerabilities [9, 10]. The European Clearinghouse review found recurring issues involving smart devices, configuration management, and digital communications [11]. These results indicate that operating experience coding must preserve system, component, failure-mode, cause, and dependency information.

3.3. Reliability Data Sources for Quantification

Existing reliability data sources provide reference information but are not sufficient for direct DI&C reliability estimation. Nuclear industry-average component reliability studies, including NUREG/CR-6928, provide benchmarks for demands, operating hours, and observed failures, but much of that experience is based on analog reactor protection system components rather than modern DI&C equipment [12]. Other reviews of DI&C reliability data discuss aerospace and broader risk-informed data practices, but also note that reporting systems, mission profiles, and operating environments differ from nuclear plant applications [13].

Non-nuclear safety-system data and standards provide concepts and target measures, but they cannot be transferred directly into nuclear DI&C PRA without qualification. Offshore oil and gas data, such as the PDS Data Handbook, provide failure-rate information for programmable safety systems and control logic units [14]. International Electrotechnical Commission (IEC) 61508 defines safety integrity levels and target failure measures for electrical, electronic, and programmable electronic safety-related systems [15]. Nordic digital I&C studies discuss digital CCF modeling and practical modeling issues [16, 17]. These sources also show why nuclear operating experience data need device identifiers, demand or run-hour data, failure counts, and consistent event coding.

3.4. Failure-Mode Taxonomies for Event Coding

This study also reviewed DI&C failure-mode taxonomies to support consistent event coding. Existing sources do not provide a single consensus taxonomy, but they identify recurring categories for operating experience analysis: task-level failures such as crash, hang, late response, incorrect response, and no response; processor or system-level failures such as processor crash, corrupted input, output failure, and communication loss; and component-level failures for processors, I/O modules, PLCs, communication modules, power supplies, and software. This paper uses failure-mode classification to link event reporting with PRA modeling, drawing on NUREG/CR-6579 [18], NRC interim guidance [19], Oak Ridge National Laboratory (ORNL) failure-mode work [20], and the OECD Nuclear Energy Agency (NEA) taxonomy [21].

4. INL DI&C OPERATING EXPERIENCE STUDY

The operating experience review used two data sources with different reporting bases. LERs provide regulatory information on safety-significant events and often include more complete event narratives, causes, and consequences. IRIS provides broader industry operating experience and captures many events that do not meet LER reporting thresholds. The two datasets provide complementary information on DI&C failures, but they also show the limits of current data for direct reliability quantification.

4.1. Operating Experience Database

The LER database documents events and conditions reported under Title 10 of the Code of Federal Regulations (10 CFR) 50.73, including equipment failures, safety system malfunctions, and human errors. The LER review focused on events from 2016 through 2023 and used keyword screening followed by manual review to identify DI&C-related events. Because LERs are safety-significant reports, they are useful for identifying operational consequences such as reactor trips and safety system impacts.

The IRIS review used a broader operating experience dataset. The study analyzed 2,104 IRIS-reported events from 1997 through 2023 with the cause category value "Digital/Cyber/Instrumentation Condition." Of these, 636 events were identified as potentially DI&C-related and were categorized by affected system, component, failure mode, and failure cause. This dataset complements the LER review by capturing routine equipment and operational issues that may not become reportable LERs.

4.2. Methodology

The LER review used keywords including "digital," "software," "computer," "microprocessor," "central processing unit (CPU)," "memory," "PLC," "field-programmable gate array (FPGA)," "program," and "digital feedwater control." The search identified 206 candidate LERs, and manual screening confirmed 43 DI&C-related events. These events were classified by hardware or software relationship, affected system and component, failure mode, failure cause, operational impact, plant operating mode, and detection method.

For IRIS, the screening started from the Digital/Cyber/Instrumentation cause-category field and then used structured review to remove events that were not related to DI&C failures. The remaining 636 events were coded using a framework aligned with the LER review so the two data sources could be compared at the level of systems, components, failure modes, and causes.

Manual screening limits reproducibility because event narratives vary in detail and borderline cases require analyst judgment. The keyword list, cause-category screen, and coding fields define the review basis, but a formal inter-reviewer agreement statistic is not reported here. Screening judgment should therefore be treated as a source of uncertainty.

The analysis has several limitations. Keyword and cause-code searches can miss events that do not use the selected terms. Event narratives vary in detail, and many IRIS records do not identify a specific failure mechanism. The available databases also do not consistently provide the device identifiers, demand counts, operating hours, or population data needed for direct component reliability estimation.

4.3. Preliminary Results

The LER review identified 43 DI&C-related events from 2016 through 2023 out of 1,580 total LERs. These included 23 hardware-related and 20 software-related events. The annual count of DI&C-related LERs varied, but their share of all LERs increased from 1.37% in 2016 to 5.56% in 2023. The study also identified 19 unexpected reactor trips attributed to DI&C failures, representing about 5.6% of unexpected trips reported during the same period. Figure 2 summarizes the LER reporting trend and hardware- and software-related classification. Preliminary results from this LER review were previously reported in [22].

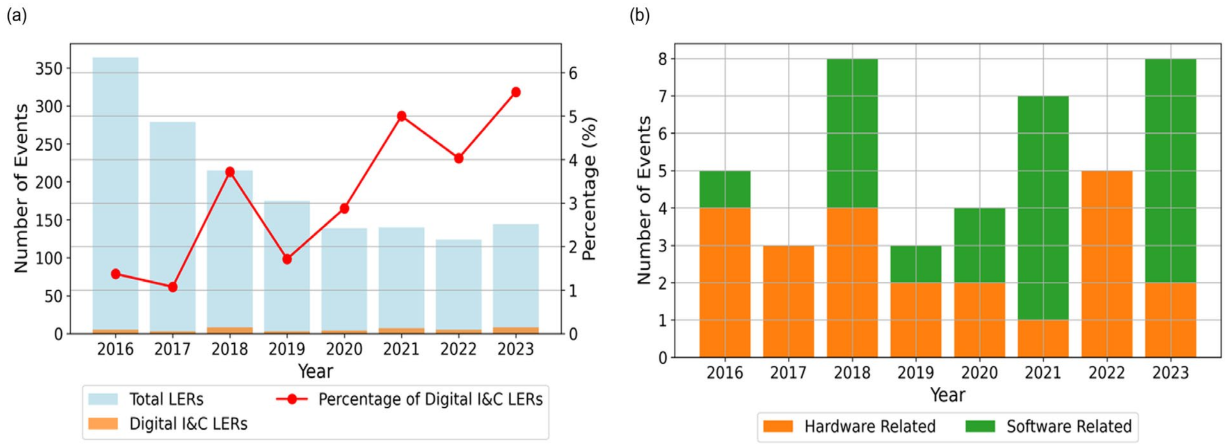

Figure 2: LER-based DI&C operating experience: (a) total LERs and DI&C-related LERs from 2016 to 2023; (b) hardware- and software-related DI&C LERs.

The most frequently involved LER systems included the digital electrohydraulic control system, digital feedwater control system, core monitoring system, radiation monitoring system, and reactor protection system. Figure 3 summarizes the affected systems and the hardware- and software-related cause categories. Hardware-related LER causes were grouped using existing component failure-cause categories; software-related causes were grouped separately to account for logic, configuration, setpoint, and design issues. The dominant LER failure modes were fail to operate or loss of function and output errors.

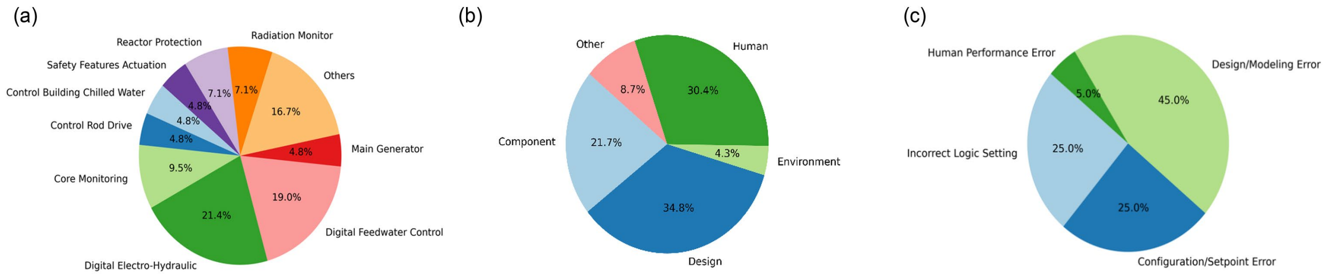

Figure 3: LER event characteristics: (a) affected DI&C systems; (b) hardware-related failure causes; (c) software-related failure causes.

The IRIS review identified 636 potential DI&C-related failures over the 1997-2023 period. The number of events increased from 1997 to 2001, peaking at 57 events in 2001, and then generally stabilized, with annual counts often between 19 and 37 events. Hardware-related failures accounted for 489 events (76.9%), while software-related failures accounted for 178 events (28.0%). These categories overlap: 31 events involved both hardware and software and are counted in both totals. Figure 4 summarizes the IRIS event trend and hardware- and software-related classification.

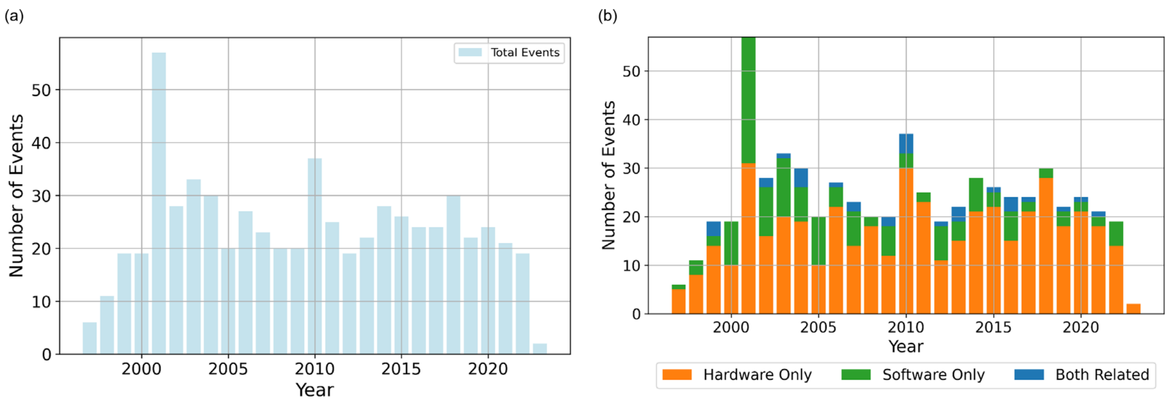

Figure 4: IRIS-based DI&C operating experience: (a) DI&C-related failures from 1997 to 2023; (b) hardware- and software-related failure classification.

Figure 5 and Table 1 show the most frequently affected systems in the IRIS review. The listed systems account for 430 of the 636 DI&C-related IRIS events (67.61%); the remaining events are distributed across lower-frequency systems and are not shown in the table. Radiation monitoring and plant process computer events were frequent, with 171 events (26.89%) and 167 events (26.26%), respectively. Frequency should not be interpreted as risk significance: many of these functions are monitoring or support functions, so PRA relevance depends on whether the event affected a credited safety function, operator information, or an accident sequence.

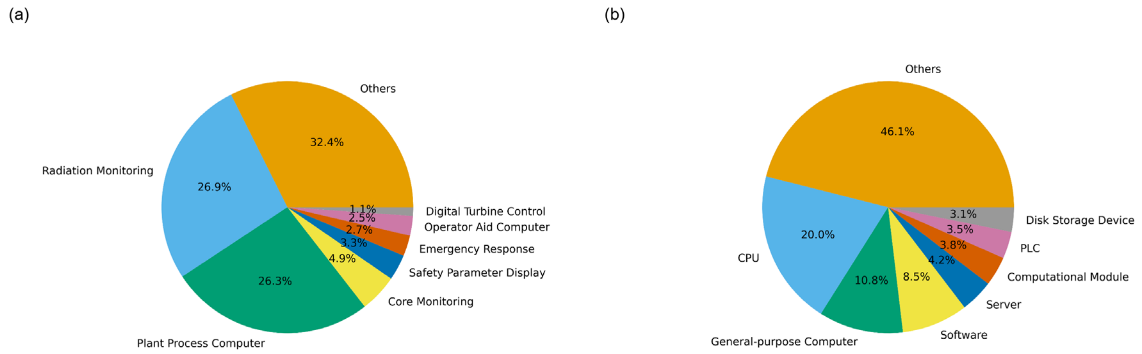

Figure 5: IRIS event distributions: (a) affected systems; (b) failed components.

Table 1: Most frequently affected systems in IRIS DI&C failure events.

System	Number of Failures	Percentage
Radiation monitoring system	171	26.89%
Plant process computer system	167	26.26%
Core monitoring system	31	4.87%
Safety parameter display system	21	3.30%
Emergency response system	17	2.67%
Operator aid computer system	16	2.52%
Digital turbine control system	7	1.10%

Figure 5 and Table 2 show the most frequently identified components. The listed components account for 343 of the 636 DI&C-related IRIS events (53.93%); the remaining events involve lower-frequency components and are not shown in the table. CPUs were the most frequently identified components, followed by general-purpose computers and software. The affected component list also included servers, computational modules, PLCs, and disk storage devices. PRA data collection would therefore need to capture both conventional electronic hardware records and software-related failure records.

Table 2: Most frequently identified components in IRIS DI&C failure events.

Component	Number of Failures	Percentage
CPU	127	19.97%
General-purpose computers	69	10.85%
Software	54	8.49%
Server	27	4.25%
Computational module	24	3.77%
PLC	22	3.46%
Disk storage device	20	3.14%

Table 3 summarizes recurring failure modes across key DI&C components. The dominant modes include fail to operate, loss of communication, lockup, incorrect output, output failure, spurious operation, and loss of network. These modes are useful for PRA screening because they connect the failed digital device to the plant function or credited operator information that may be affected.

Table 3: Key DI&C component failure modes.

Component	**Failure Modes**	**Description**
CPU	Fail to operate, lockup, loss of communication, loss of signal, output failure, spurious operation	CPU failures caused complete shutdowns (fail to operate), temporary freezes (lockup), and disrupted data flow (loss of communication). Output errors and spurious operations introduced instability and unsafe conditions.
Computer	Fail to operate, loss of communication, lockup, incorrect output	Failures in general-purpose computers impacted real-time processing, leading to unavailability (fail to operate), freezes (lockup), and data inaccuracies (incorrect output).
Software	Fail to operate, loss of communication, incorrect output, lockup	Software-related failures disrupted system logic, with fail to operate affecting critical operations. Incorrect output and loss of communication often propagated errors across subsystems.
Server	Fail to operate, loss of communication, spurious operation	Server failures impaired centralized data processing and communication, with fail to operate and loss of communication causing significant operational disruptions. Spurious operation introduced unpredictable behavior.
Computational module	Fail to operate, loss of communication	Failures in computational modules, which handle specialized tasks, were primarily related to complete loss of functionality or communication breakdowns.

Component	Failure Modes	Description
PLC	Fail to operate, output failure, loss of communication, lockup	PLC failures disrupted real-time control processes, with fail to operate and loss of communication being the most frequent. Output failures and lockups introduced delays and control instability.
Disk storage	Fail to operate	Disk storage failures often resulted in data retrieval issues, affecting logging, archival, and operational analytics.
Communication module	Fail to operate, loss of communication	Failures in communication modules primarily affected network reliability, with loss of communication interrupting data flow between subsystems.
Multiplexer	Loss of network	Multiplexer failures led to network interruptions, affecting data routing and system connectivity.

The high fraction of unknown causes limits cause-based interpretation of the IRIS results. System and component attributions remain useful for screening because the affected system or failed item can often be identified even when the failure mechanism is not. In contrast, cause distributions should be interpreted as conditional on the subset of events with sufficient cause information and may not represent all DI&C-related IRIS events.

Among the 489 hardware-related events, 433 (88.5%) had unknown cause; among the 178 software-related events, 109 (61.2%) had unknown cause. Within the remaining known-cause subset, aging was the most frequent identified hardware cause, and software, programming, configuration, or setpoint issues were recurring identified software-related causes. These results are better suited for screening candidate review areas than for estimating cause probabilities.

4.4. Implications for PRA Modeling

The operating experience results affect PRA model scope and screening. The LER data provide fewer events but richer causal and consequence information, while the IRIS data provide broader coverage of recurring systems, components, and failure modes. The datasets support identification of candidate DI&C failure modes for fault trees and event trees, especially fail to operate, loss of communication, lockup, incorrect output, output failure, and spurious operation. Hardware-related events also indicate that aging, CPU or module failures, and communication faults should be considered when developing time-dependent or system-specific reliability models.

The results also show that DI&C failures should not be treated only as independent hardware component failures. Software-related events involve configuration, setpoint, logic, programming, and design issues that do not correspond directly to classical hardware failure rates. Events involving both hardware and software indicate dependencies in which a CPU, communication module, interface, or other digital device can affect software execution, operator information, or credited control functions. These dependencies need to be represented in PRA models where they can affect accident sequence progression, operator response, or common-cause screening. The high fraction of unknown causes in IRIS also limits direct parameter estimation and indicates the need for more detailed DI&C event coding, diagnostics, and denominator data before the operating experience can be used for routine quantification.

5. DI&C RELIABILITY AND RISK ASSESSMENT - NEXT STEPS

These modeling implications suggest a staged approach for DI&C reliability and risk assessment. DI&C events need a stable coding structure so the data can be collected consistently. IDCCS and RADS would need DI&C-specific fields to support reliability calculations. PRA models also need to represent functional dependencies, software-related failures, and common-cause mechanisms that differ from classical hardware CCF treatment.

5.1. Potential Incorporation of DI&C Failures into IDCCS

A DI&C failure database should be distinct from the existing hardware failure and CCF studies, but compatible with them. Each event should identify the event date, plant, DI&C system and component, affected plant system or component, DI&C failure mode, affected component failure mode, failure cause, detection method, operating mode, and the evidence supporting the classification. For PRA use, the coding must also identify whether the DI&C failure directly affects a modeled component, operator information, an automatic actuation function, or a broader plant function.

5.2. Estimating DI&C Reliability Using Operating Experience

RADS, the NRC/INL PRA data calculation website [23], could estimate DI&C component reliability in a manner similar to existing hardware reliability calculations only if the underlying database contains the necessary denominator information. For each DI&C component or device family, the data would need to identify the component population, operating time or demand count, failure count, and the credited function affected by the failure. Current IRIS and LER data support event characterization, but they do not consistently provide device identifiers, run hours, demands, or population counts.

For CCF treatment, this study distinguishes between two categories that should not be modeled the same way:

- DI&C internal CCF refers to a shared-cause failure of redundant DI&C trains or components, such as redundant software or processors that fail to perform the same credited function.
- DI&C external CCF refers to a DI&C failure that affects multiple plant components, systems, functions, or operator actions. This is not the traditional CCF of redundant hardware components; it is usually a dependency that should be modeled explicitly in the PRA logic.

This distinction affects the PRA treatment because defense-in-depth and diversity requirements primarily address the risk that a single DI&C vulnerability could affect multiple functions. For PRA, those dependencies may be better represented through explicit functional modeling, surrogate events, or bounding sensitivity cases rather than by directly applying classical hardware CCF parameter models.

5.3. PRA Modeling and Implementation Considerations

The operating experience data indicate several PRA modeling needs. Hardware-related trends, including aging-related events, support consideration of time-dependent reliability for digital hardware. Software-related events involve configuration, setpoint, programming, and design errors that do not behave like age-driven hardware degradation. Events involving both hardware and software indicate that coupled failures and cascading effects should be considered when a processor, communication module, or software fault can affect downstream plant functions.

A graded PRA modeling approach should be used so that modeling detail is commensurate with the risk significance of the DI&C application. Important modeling elements include DI&C equipment unavailability, DI&C-related human actions, fault-tolerant and self-monitoring features, function integration across multiple plant systems, and uncertainty in failure probability estimates.

Implementation would require a DI&C event coding guideline, pilot population of historical LER and IRIS events in IDCCS, RADS updates for DI&C reliability calculations, and coordination with INPO and industry stakeholders to improve DI&C device identification, demand or run-hour data, and reporting of software and configuration-related causes [23].

6. CONCLUSIONS

This paper summarizes an INL review of DI&C operating experience data for reliability and risk assessment. The LER review provides a smaller set of safety-significant and better documented events, including 43 confirmed DI&C-related LERs from 2016 through 2023 and 19 unexpected reactor trips attributed to DI&C failures. The IRIS review provides a broader view of operating experience, identifying 636 potential DI&C-related events from 1997 through 2023, with hardware-related events more frequent than software-related events and 31 events involving both categories.

The main technical finding is that existing operating experience can support DI&C event screening, taxonomy development, and identification of affected systems, components, failure modes, and causes. The data are not yet sufficient for routine DI&C component reliability estimation without improved device identifiers, operating times or demands, component population data, and failure-cause documentation.

For PRA, DI&C failures should be treated through explicit functional modeling where possible. Internal DI&C CCF, external functional dependencies, software-related failures, hardware-software coupling, fault tolerance, human actions, and uncertainty should be considered separately rather than forced into a single hardware CCF parameter model. Recommended follow-on work includes consistent DI&C event coding in IDCCS and RADS updates so that future operating experience can be used more directly for DI&C reliability estimation and risk-informed decision-making.

Acknowledgements

This paper was authored by Battelle Energy Alliance, LLC, under Contract No. DE-AC07-05ID14517 with the U.S. Department of Energy (DOE), and Agreement Number 31310019N0006, Task Order Number 31310019F0022 with the NRC. References herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise do not necessarily constitute or imply endorsement, recommendation, or favoring by the U.S. Government or any agency thereof. The views and opinions of the authors expressed herein do not necessarily state or reflect those of the U.S. Government or any agency thereof.

References

[1] T. Liu and Z. Ma, "Operating Experience Data Analysis for Digital Instrumentation and Control System Reliability and Risk Assessment," Idaho National Laboratory, prepared for the Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, Washington, DC, NUREG/CR-7313, manuscript under NRC review.

[2] Core knowledge on instrumentation and control systems in nuclear power plants (IAEA Nuclear Energy Series No. NP-T-3.12). Vienna: International Atomic Energy Agency, 2011.

[3] "Identifying systems and assets subject to the cyber security rule," NEI, Washington D.C, NEI 10-04, 2012.

[4] T. Chu, G. Martinez-Guridi, M. Yue, J. Lehner, and P. Samanta, "Traditional probabilistic risk assessment methods for digital systems," U.S. NRC, Washington D.C, NUREG/CR-6962, 2008.

[5] T. Chu, M. Yue, G. Martinez-Guridi, K. Mernick, J. Lehner, and A. Kuritzky, "Modeling of digital feedwater control system using traditional probabilistic risk assessment methods," U.S. NRC, Washington D.C, NUREG/CR-6997, 2009.

[6] T. Aldemir et al., "Dynamic reliability modeling of digital instrumentation and control systems for nuclear reactor probabilistic risk assessments," U.S. NRC, Washington D.C, NUREG/CR-6942, 2007.

[7] BNL, "An LER search of digital I&C failure events at NPPs during 2005 and 2015," Upton, NY, 2016.

[8] E. Lee, "Computer-based digital system failures," U.S. NRC, Washington, D.C, AEOD/T94-03, 1994.

[9] EPRI, "Operating experience insights on common-cause failures in digital instrumentation and control systems," Palo Alto, CA, 1016731, 2008.

[10] EPRI, "Digital common-cause failure susceptibility: 2014 project status," Palo Alto, CA, 3002002990, 2014.

[11] M. Peinador, "Operating experience with digital I&C systems at nuclear power plants. A summary report from European Clearinghouse," Luxemburg, 2019.

[12] S. A. Eide, T. E. Wierman, C. D. Gentillon, D. M. Rasmuson, and C. L. Atwood, "Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants," U.S. NRC, Washington, D.C., NUREG/CR-6928, 2007.
[13] M. A. Azarm and S. Khericha, "Assessment of Technical Feasibility of Risk-Informed Approaches and Gaps Associated with Further Integrating Risk Insights into Regulatory Reviews for Digital I&C Systems and Components," U.S. Nuclear Regulatory Commission, Washington, D.C., 2020.
[14] S. Hauge and T. Onshus, "Reliability Data for Safety Instrumented Systems, PDS Data Handbook, 2010 Edition," SINTEF, Norway, 2009.
[15] IEC, "Functional Safety of Electric/Electronic/Programmable Electronic Safety-Related Systems," IEC 61508, 2010.
[16] T. Tyrväinen, "Probabilistic Modelling of Common Cause Failures in Digital I&C Systems - Literature Review," VTT Technical Research Centre, Finland, VTT-R-00728-21, 2021.
[17] S. Authén, O. Bäckström, J.-E. Holmberg, M. Porthin, and T. Tyrväinen, "Modelling of Digital I&C, MODIG: Interim report 2015," Nordic Nuclear Safety Research NKS, 2016.
[18] M. Hassan and W. E. Vesely, "Digital I&C Systems in Nuclear Power Plants: Risk-Screening of Environmental Stressors and a Comparison of Hardware Unavailability With an Existing Analog System," U.S. NRC, Washington, D.C., NUREG/CR-6579, 1998.
[19] U.S. Nuclear Regulatory Commission, "Digital Instrumentation and Control Systems Interim Staff Guidance," Washington, D.C., 2008.
[20] K. Korsah, S. M. Cetiner, M. D. Muhlheim, and W. P. Poore III, "An Investigation of Digital Instrumentation and Control System Failure Modes," Oak Ridge National Laboratory, Oak Ridge, TN, ORNL/TM-2010/32, 2010.
[21] NEA, "Failure Modes Taxonomy for Reliability Assessment of Digital Instrumentation and Control Systems for Probabilistic Risk Analysis," OECD Nuclear Energy Agency, NEA/CSNI/R(2014)16, Paris, 2015.
[22] T. Liu and Z. Ma, "A preliminary review of digital instrumentation and control failure events in U.S. nuclear power plants," presented at the ANS Winter Conference, Orlando, FL, 2024.
[23] U.S. Nuclear Regulatory Commission and Idaho National Laboratory, "RADS - PRA Data Calculations Web Site," Reliability and Availability Data System, Version 1.7.2024.295, 2024. [Online]. Available: https://rads.inl.gov/.