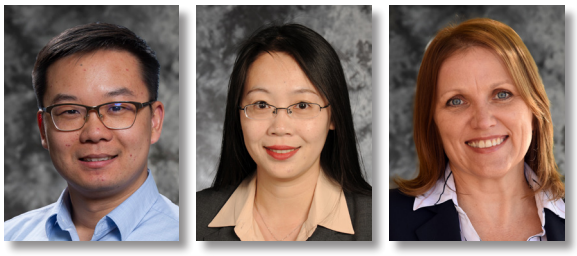
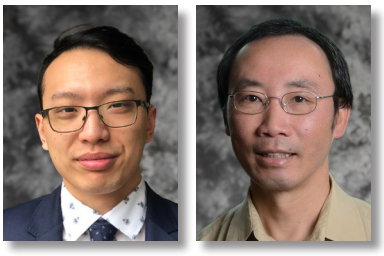
Identification of Software Common-Cause Failures in Digital I&C Systems at Nuclear Reactors



Han Bao, Sai Zhang, Svetlana Lawrence
Risk-Informed Systems Analysis Pathway



Edward Chen, Nam Dinh
North Carolina State University

Tate Shorthill
University of Pittsburgh

Most existing nuclear power plants in the U.S. were designed in the 1970s and 1980s using analog and relay components, as well as limited digital technology for monitoring, control, and protection functions. As the industrial base moves to digital systems for monitoring and control, the maintenance of analog systems at nuclear power plants has become challenging due to the lack of spare parts, increasing replacement costs, and limited vendor support. Compared with existing analog instrumentation and control (I&C) systems, digital I&C systems have significant functional advantages, such as reliable system performance in terms of accuracy and computational capability and high-capacity data-handling and storage capabilities to fully measure and display operating conditions. Therefore, in the last few years, the U.S. nuclear power industry has initiated the replacement of existing aging analog systems with digital I&C technology.

A key challenge faced in the transition from legacy analog systems to digital I&C systems is the need to address and mitigate possible common-cause failures (CCFs). A CCF is the occurrence of two or more failure events due to the simultaneous occurrence of a shared failure cause and a coupling factor (or mechanism). Today, most safety-grade I&C systems at a nuclear power plant are designed with redundancy and/or various diversity types (e.g., design and functional diversity) to provide several ways of detecting and responding to a significant event, so that no common part and no single failure mechanism can result in a failure to detect or actuate a safety function when needed. But with a digital I&C system, the software could be employed in both primary functional areas, as well as the backup. Certain CCFs cannot be readily detected, as failures from analog systems are not directly transferable to digital systems, which impedes the licensing of advanced control systems. Existing failure identification approaches in conventional probabilistic risk assessment (PRA) lack the capability to assess why and how digital I&C systems can fail. Digital I&C systems can integrate previously separate analog systems [1], which makes it difficult to identify the source and evaluate potential consequences of CCFs. This has resulted in a disconnect between PRA model predictions and operational environments, where software failures may occur because the causes could not be anticipated and modeled.

The LWRS Program Risk-Informed Systems Analysis (RISA) team is developing a framework for digital I&C risk assessment that provides a technical basis to identity and evaluate software CCFs in digital I&C systems due to unintended design or implementation defects [2]. The framework assesses such systems by considering the following: (1) in what ways can the system fail; (2) how likely is a failure event to occur; and (3) how does it impact stakeholder goals and ultimately the safe operation of a nuclear power plant. To assess how the system can fail, the framework focuses on the identification of failures and mechanisms leading to these failures, both when nuclear plant operators provide inputs to their controls (actuation pathway) and when the information is transmitted (information feedback pathway). Two types of software failure modes are possible. The first type of failure results in an errant controller action and is defined as an unsafe control action (UCA). The second type of failure is due to corrupted or counterfactual information from intermediate digital processors (e.g., analog-to-digital converters). This type of failure mode is defined as an unsafe information flow (UIF) [2]. In Figure 2, a model control loop is provided to show where UCA and UIF can be produced, as well as the flow of data.

The introduction of UIF allows digital I&C designers and software engineers to describe how errant data can lead

to undesirable behavior by controllers or human operators of the system. While both UCAs and UIFs are considered independent software failure events, they can also be used to identify errant CCF events within redundant digital I&C systems. This novel approach has been demonstrated in the qualitative assessment of the human system interfaces in nuclear power plant digital I&C systems. The areas of concern associated with these digital components can be mitigated by eliminating causal factors for independent and CCF events. Detailed findings can be found in [2]. In essence, by tracing relevant failures, this approach aims to: (1) systematically isolate areas of potential risk; and (2) provide targets for future risk quantification for reliability assessment. The latest research accomplishments were presented at the Pressurized Water Reactor Owners Group (PWROG) meeting in August 2022. In addition, the LWRS Program RISA team is currently collaborating on a PWROG project to identify and quantify potential CCF events.

References:

1. NRC, 2021, Guidance for Evaluation of Defense in Depth and Diversity to Address Common-Cause Failure due to Latent Design Defects in Digital Safety Systems, Branch Technical Position 7-19, U.S. Nuclear Regulatory Commission, Washington, D.C., USA.
2. Bao, H., S. Lawrence, J. Park, H. Ban, E. Chen, N. Dinh, A. V. Jayakumar, C. Elks, H. Zhang, E. Quinn, S. Zhang, and T. Shorthill, 2022, An Integrated Framework for Risk Assessment of High Safety-significant Safety-related Digital Instrumentation and Control Systems in Nuclear Power Plants: Methodology and Demonstration, INL/RPT-22-68656, August 2022, Idaho National Laboratory, Idaho Falls, ID, USA.

Figure 2. Information pathways in a digital I&C system.