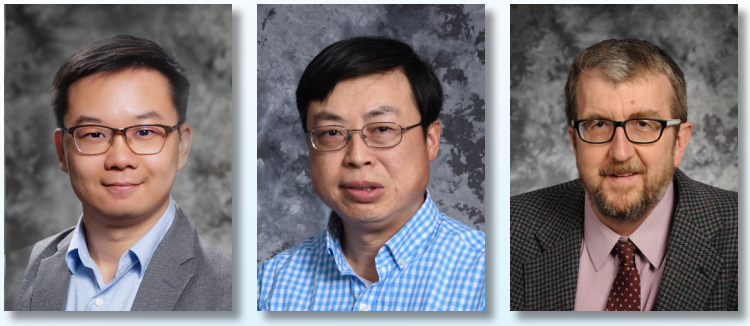
Integrated Risk Assessment for Digital Instrumentation and Control Systems



Han Bao, Hongbin Zhang, and Curtis Smith
Risk-Informed Systems Analysis Pathway

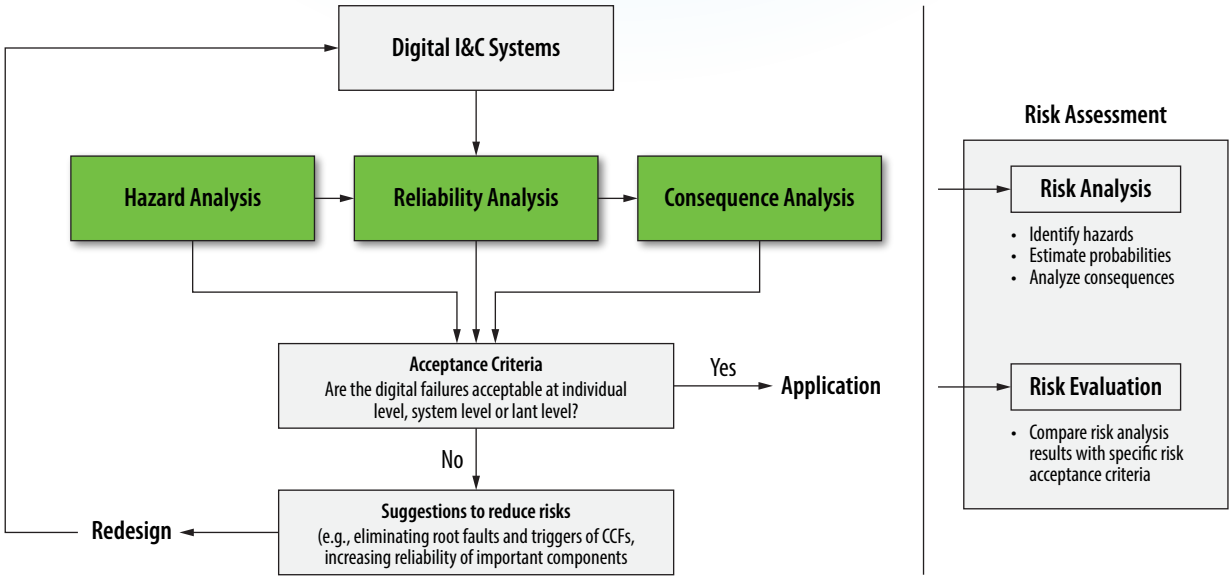
Risk-Informed Systems Analysis Pathway researchers, along with industry collaborators, are developing an integrated risk assessment approach to evaluate digital instrumentation and control (I&C) systems. This approach considers common cause failures (CCFs) and plant transient responses to provide the technical basis supporting effective, licensable, and secure digital I&C technologies for upgrades to existing nuclear power plants. This technical basis is instructive for nuclear vendors and utilities to effectively lower the costs associated with digital compliance and speed-up industry advances by: (1) defining an integrated risk-informed analysis approach for digital I&C upgrades including hazard analysis, reliability analysis, and consequence analysis; (2) applying systematic and risk-informed tools to address CCFs and quantify failure probabilities for digital I&C technologies; (3) evaluating the impact of digital failures at the component-level, system-level, and plant-level; and (4) providing insights and suggestions on designs to manage the risks to support the development, licensing, and deployment of digital I&C technologies to nuclear power plants.

Risk Assessment for Digital I&C Systems – An Integrated Approach

Digital I&C upgrades must be cost-effective and meet current licensing and qualification requirements for these systems. An integrated multi-disciplinary approach, defined as Risk Assessment for Digital I&C (RADIC), as displayed in Figure 3, supports this strategy. RADIC has three key parts—hazard analysis, reliability analysis, and consequence analysis.

Hazard analysis focuses on identifying both software and hardware failures and building models (i.e., fault trees).

Figure 3. Schematic of the Risk Assessment for Digital I&C (RADIC).



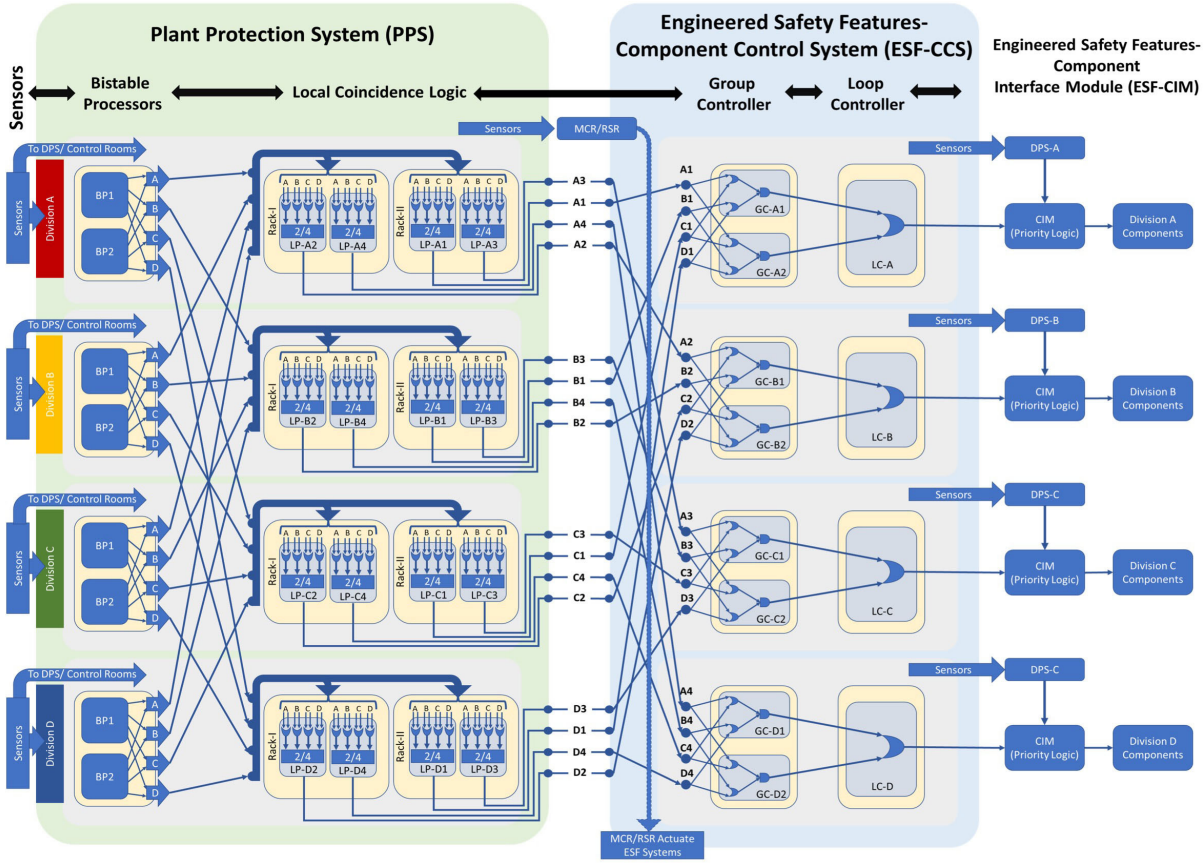


Figure 4. Detailed hardware representation of the digital ESFAS.

The acceptance criterion for hazard analysis is whether the individual digital failure leads to the loss of system function. In previous PRAs for analog systems, hardware failures were the focus. In this research, Nancy Leaveson, a researcher at Massachusetts Institute of Technology, used a Systems-Theoretic Process Analysis method, to identify potential software failures. The integration of software failures into the existing hardware fault tree in RADIC is further developed using the Hazard and Consequence Analysis for Digital Systems (HAZCADS) method jointly developed by the Electric Power Research Institute (EPRI) and Sandia National Laboratories (SNL). The reliability analysis quantifies the integrated fault trees and building event trees to represent the consequences of digital system failures.

A Case Study on a Representative Digital Safety System

Currently, the RADIC approach is being demonstrated on representative digital safety systems including the reactor trip system and Engineered Safety Features Actuation Systems (ESFASs). The key outcomes are an integrated fault tree that includes both hardware and software failures and ways to identify potential hazards that may make the digital system fail. To characterize this, a detailed hardware representation of the digital ESFAS was developed as shown in Figure 4. Next, a fault tree of hardware failures was developed for system failure, followed by using a modified systematic hazard analysis approach that includes software failures.

Researchers are using these models to characterize the strengths and weakness of the digital I&C system and provide recommendations to system designers and plant operators/owners to efficiently reduce system vulnerabilities. By integrating hazard analysis, reliability analysis, and consequence analysis together, this risk assessment strategy aims to: (1) help system designers and engineers to systematically address digital-based CCFs and quantitatively analyze their effects on digital-system vulnerability and key plant responses; (2) improve existing PRA models for the industry by identifying and evaluating the risk associated with digital I&C technologies; and (3) provide risk insights to address the licensing challenges facing digital I&C upgrades.