Testbed-Driven Assessment: Experimental Validation of System Security and Reliability

Overview and Problem Statement

Efforts are underway to switch existing nuclear power plants (NPPs) based on analog control systems to digital control systems. It is expected that digital Instrumentation and Control (I&C) systems will be used in all future NPPs, and they are expected to solve the obsolescence problem of analog components and to improve safety and performance. However, before analog systems can be switched to digital, much work needs to be done to ensure the safety of the new systems to the level required by the nuclear sector. The goal of this research project is to identify and experimentally evaluate possible faults and attacks against the safety-critical digital I&C systems destined for use in NPPs. In pursuit of that goal, the project is developing tools and methods and building a testbed to study and validate the failure/attack behavior of the safety-critical digital I&C systems.

Research Objectives

- Experimentally evaluate the resiliency and security of the digital I&C system.
- Build a testbed with real-time simulation of an NPP in conjunction with physical digital I&C components for realistic NPP operation simulation.
- Identify potential attack vectors, single points of failure, and common mode failures in the future digital I&C systems.
- Develop fault injection and attack simulation tools to simulate various failures and attacks on the testbed to demonstrate their potential impacts.
- Develop logics to analyze and report on the impact of failures and attacks on the safety-critical digital I&C components of an NPP.
- **Smart Grid Application Area:** Develop tools to enable experimental evaluation of the resiliency and security of the safety-critical digital I&C systems to be used in NPPs in the future.

Technical Description and Solution Approach

- A testbed is being developed for the purpose of security and resiliency evaluation of the digital I&C systems for NPPs. It consists of a reactor model, a digital controller, and associated communication links. The digital controller has a Triple-Modular Redundant (TMR) architecture to ensure continuous availability of the controller. (Figure 1 shows the NPP testbed setup.)
- A real-time NPP simulator has been developed in LabVIEW; the point kinetics equation is being used for the core and models of a pressurizer and a pump. The model for the primary loop is fairly complete; the secondary loop is still in progress.
- The NPP simulator and the TMR controller, with its associated application program, have been assembled, and communications between them have been established. The testbed also includes a set of specialized fault/error injectors to inject different types of faults/errors, both transient and permanent.
- A fault injection module is being developed in LabVIEW in order to simulate hardware failures. The module contains a fault list manager (FLM), a fault injection manager (FIM), and a result analyzer (RA). The FLM picks a fault type and fault location at random from the pre-generated list of fault locations and types, and communicates this information to the FIM, which injects faults into the system.
- Since the digital controller has a TMR architecture, common-mode failures, in which a failure or attack would impact all three redundant modules, are of the greatest concern. One potential common mode failure would be corruption of the communication channel during configuration of the digital controller. Since the same configuration is applied to all three modules in the controller, a corruption or attack on the communication channel could result in a common mode failure, as shown in Figure 1.

Results and Benefits

- The testbed provides the ability to simulate the operation of an NPP with real-time control feedback from the digital controller.
- Potential future uses of the testbed include cyber security tests of digital I&C systems for NPPs, stability analysis of the NPP testbed connected to a simulator of the electric grid, and human machine interface and human factor engineering studies of newly developed control rooms for NPPs.
- **Technology Readiness Level:** Ongoing development of the testbed and experimental evaluation tools.

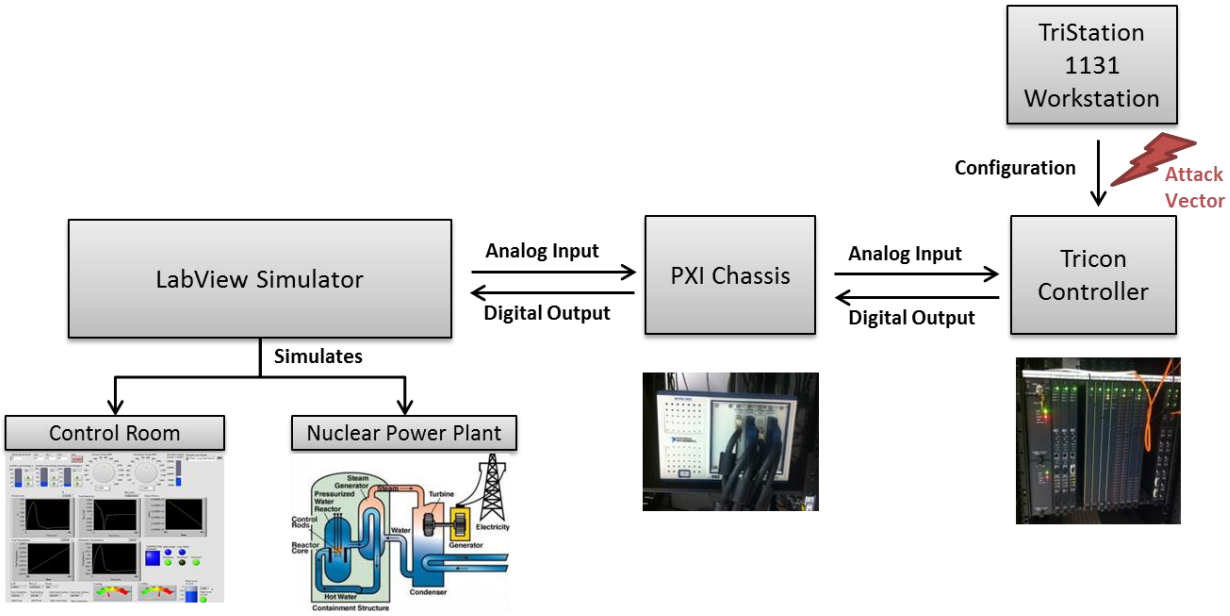

Figure 1. NPP Testbed Setup

Researchers

- Daniel Chen, dchen8@illinois.edu
- Yongkyu An, an24@illinois.edu
- Calogero Sollima, csollima@illinois.edu
- Zbigniew Kalbarczyk, kalbarcz@illinois.edu
- Ravishankar Iyer, rkiyer@illinois.edu

funded by the U.S. Department of Energy and the U.S. Department of Homeland Security