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

Daniel Chen, Yongkyu An, Calogero Sollima, Zbigniew Kalbarczyk, and Ravishankar Iyer

GOALS

- Overall goal: Experimental evaluation of the security, reliability, and risk assessment of digital I&C systems in a nuclear power plant (NPP).
- Build a test-bed with real-time simulation of the 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 digital I&C systems.
- Develop fault injection and attack simulation tools to simulate various failures and attacks on the test-bed to demonstrate their potential impacts.
- Develop logics to analyze and report the impact of failures and attacks on the safety-critical digital I&C components of the NPP.

FUNDAMENTAL QUESTIONS/CHALLENGES

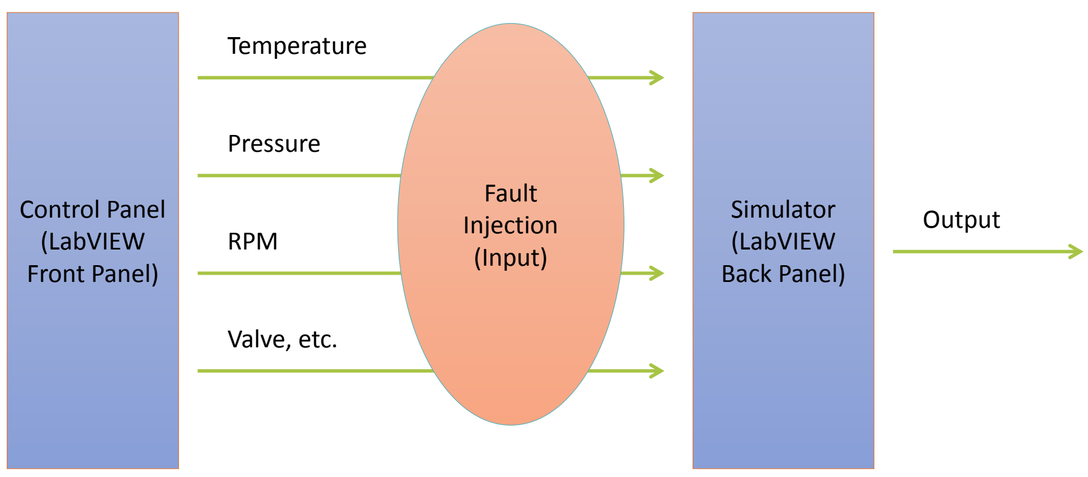
Analog

Digital

- Analog I&C systems:
  - Most were built in the 1970s and 1980s, with a life of 40 years.
  - Many original analog parts are no longer available.
  - Complex; require frequent maintenance.
  - High manpower to maintain.
- Digital I&C systems:
  - Can process and execute complex computation and control functions.
  - Provide more precise and accurate measurements.
  - Detect and respond faster and provide more accurate warning signals.
  - Require less manpower to operate.
- Gap
  - Modeling of digital I&C systems in NPP.
  - Relationship between cyber and physical element functionalities.
  - Safety and cyber-security assessment.

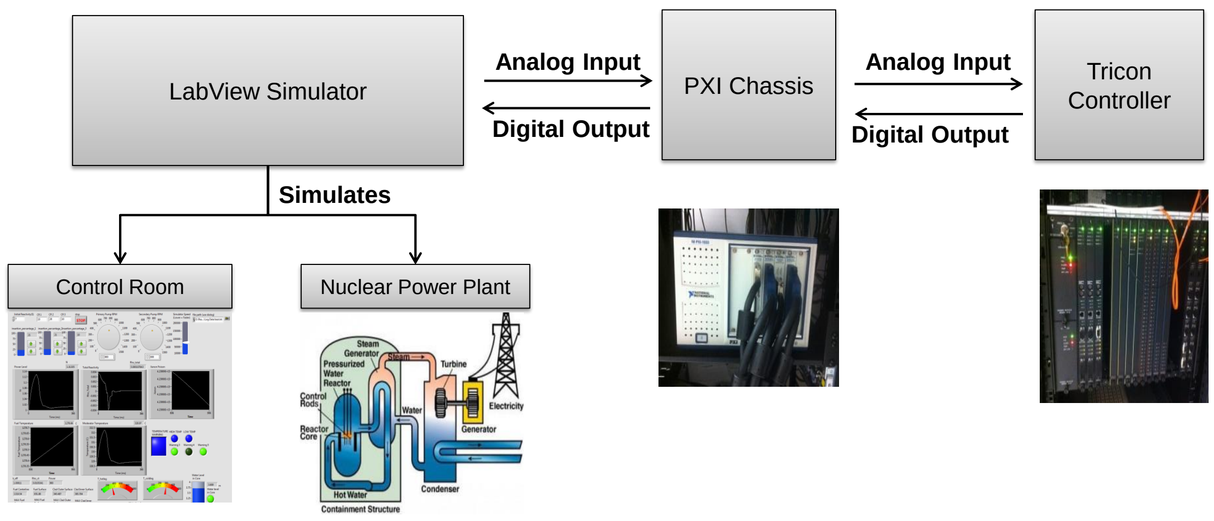
RESEARCH PLAN

- Build a test-bed for the purpose of security and resiliency evaluation of the digital I&C systems for the NPP.
- Develop a real-time simulation of the NPP in LabView.
- Connect the NPP simulation with a real digital I&C control system to simulate realistic NPP operation.
- Develop fault injection and attack simulation tools to simulate realistic failures and attack scenarios.
- Study the impact of simulated faults and attacks to help develop safety and security assessment procedures.



RESEARCH RESULTS

- A test-bed is being developed. It consists of a reactor model, a digital controller, and associated communication links.
- The digital controller (Tricon) has a Triple-Modular Redundant (TMR) architecture to ensure continuous availability of the controller.
- A real-time NPP simulator has been developed in LabVIEW using the point kinetics equation for the core, and models for a pressurizer and a pump.
- The NPP simulator and the TMR controller, with its associated application program, have been assembled, and communications between them have been established.



- A fault injection module has been 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).
- 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 FIM, which injects faults into the system.
- The Result Analyzer module analyzes and records the impact of injected faults on the system.
- The state of the NPP corresponding to the operation on the faulty data is compared with the simulated output data to determine the impact of the injected fault.
- The preliminary fault injection parameters and result are provided in the table below.

Table 1. Fault Injection Parameters

Core	Pressurizer	Pump
Fuel Temperature	Pressure	Pressure
Coolant Temperature	Temperature	Temperature
Neutron Power Density	Spray	Spray
Control Rods	Heater	Heater

Table 2. Results of Detecting Faulty System by RA

Total Experiments	30
Detected	29
Not Detected	1

BROADER IMPACT

- Other potential uses of the test-bed include compliance tests of digital I&C systems for NPPs, stability analysis of the NPP test-bed connected to a simulator of the electric grid, and human machine interface and human factor engineering studies of newly developed control rooms for NPPs.

INTERACTION WITH OTHER PROJECTS

- This project is being done in collaboration with faculty and students from the Nuclear, Plasma, and Radiological Engineering department, and the test-bed is incorporated within the TCIPG test-bed.

FUTURE EFFORTS

- The next step is to focus on potential cyber-attacks on the digital I&C systems.
- Currently, we are reverse-engineering the communication protocol between the configuration software and the Tricon controller.
- If the communication is compromised, it could be used as an entry to create a common mode failure of the triple-modular redundant digital controller.

FUNDING SUPPORT PROVIDED BY DOE-OE AND DHS S&T