Experimental Validation of Digital Instrument & Control System Security and Reliability

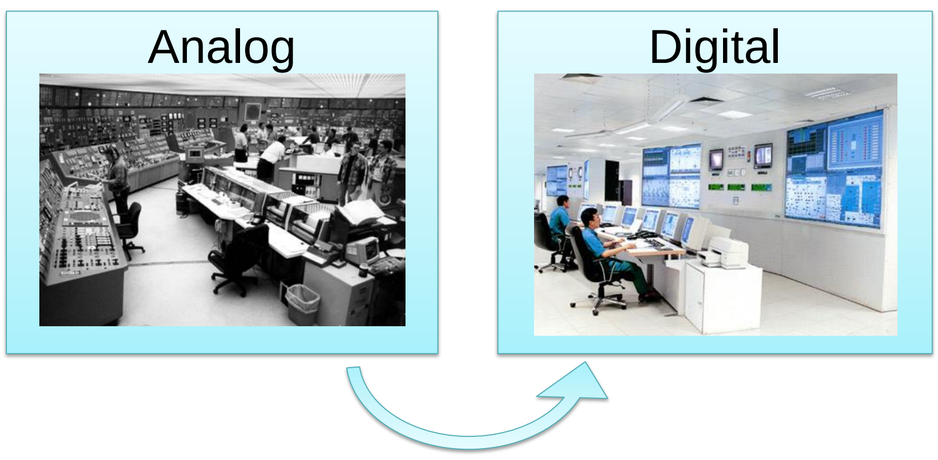
Bernard Lim, Daniel Chen, Yongkyu An, Zbigniew Kalbarczyk, and Ravishankar Iyer

GOALS

- Experimental evaluation of the security, reliability, and risk assessment of digital instrument & control (I&C) systems.
- Build a testbed with real-time simulation of an industrial control system (ICS) in conjunction with physical digital I&C components for realistic 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 testbed.
- Develop logics to analyze and report on the impact of failures and attacks on the safety-critical digital I&C components.

FUNDAMENTAL QUESTIONS/CHALLENGES

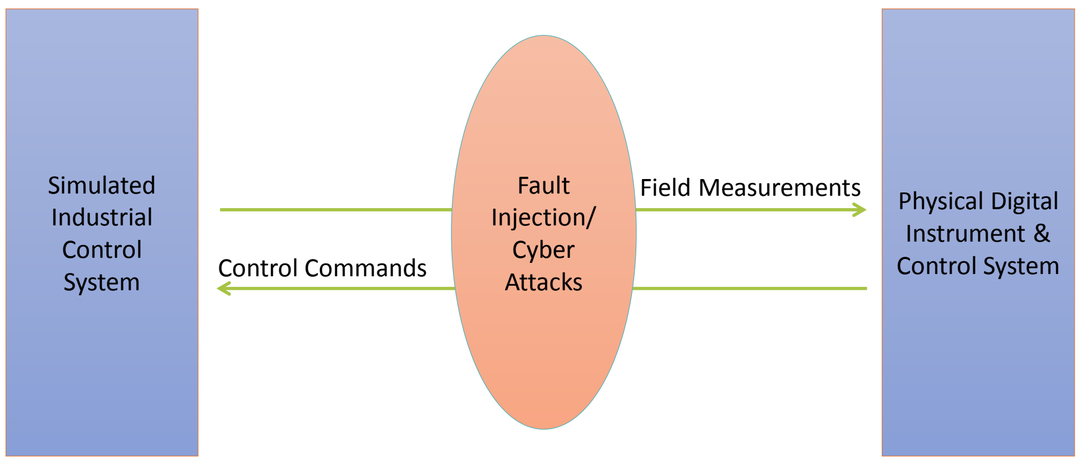
- Develop methods and tools for resiliency assessment of digital instrument & control systems; utilize protection and control in a nuclear power plant as a case study.



- Analog I&C systems:
  - Most were built in the 1970s and 80s, with a lifespan of 40 years.
  - Many original analog parts are no longer available.
  - Complex and 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 measurement.
  - Detect and respond faster and provide more accurate warning signals.
  - Require less manpower to operate.
- Gap:
  - Modeling of hardware-in-the-loop digital I&C systems.
  - Relationship between cyber and physical element functionalities.
  - Safety and cyber-security assessment.

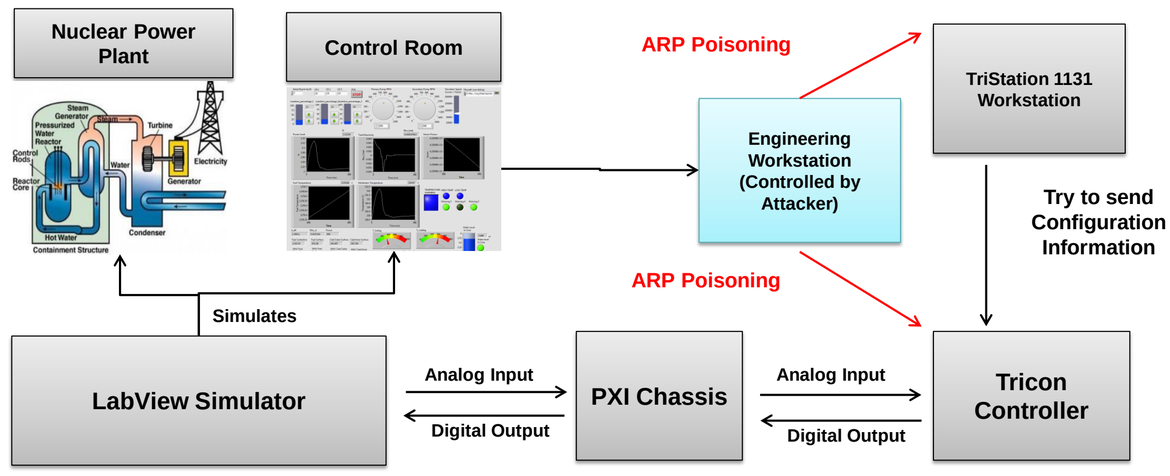
RESEARCH PLAN

- Build a testbed for the purpose of security and resiliency evaluation of digital I&C systems that can be applied to various industrial control systems.
- Develop a real-time simulation of the ICS (e.g., in LabView).
- Connect the ICS simulation with a real digital I&C control system to simulate realistic industrial process 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.

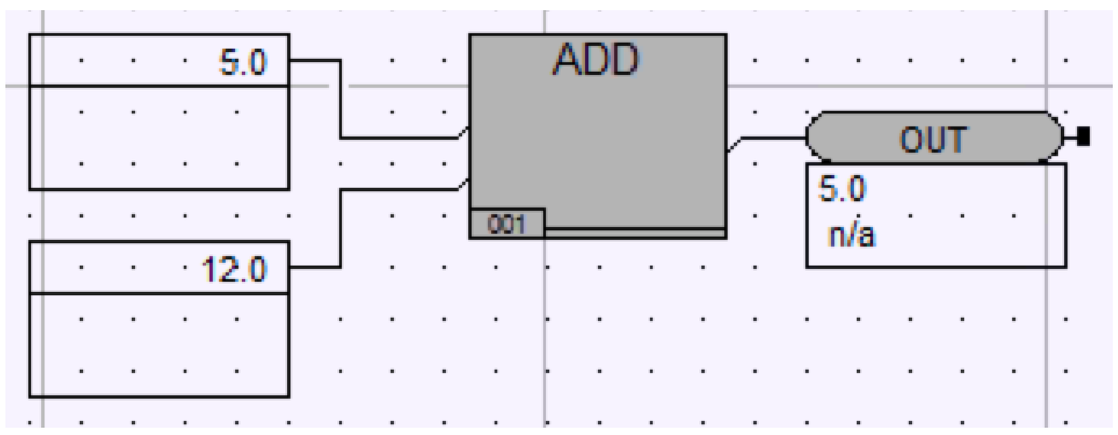


RESEARCH RESULTS

- Development of a testbed, which consists of a nuclear power plant 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 man-in-the-middle (MitM) attack has been developed and deployed between the TriStation workstation, Tricon controller, and control room to demonstrate the potential impact of a cyber attack.



- The MitM attack malware compromises an engineering station and uses it to intercept and modify the configuration settings sent from the TriStation software to the Tricon digital controller, effectively embedding a common-mode-failure logic in the controller.
- The MitM attack is developed by reverse-engineering the digital I&C configuration protocol, identifying key fields, and modifying the packets.
- The MitM attack malware modifies data packets, re-computes UDP, IP, and protocol-specific checksums, and updates other metadata before forwarding to the digital controller. The forwarded packets are accepted as legitimate.
- The malware successfully modifies configuration packets sent from TriStation to Tricon, causing the Tricon to behave differently from the original program.
- The below figure shows an example logic, downloaded to the Tricon, that has been modified by the MitM malware, resulting in an incorrect value produced by the ADD logic (e.g., 5 +12 should be 17, but the result shows 5.)



BROADER IMPACT

- The MitM module, combined with a testbed, can be used to test a variety of other digital I&C systems and industrial control systems (e.g., for oil & gas or water treatment), and evaluate their resiliency against accidental errors and malicious cyber attacks.

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 testbed being developed is being incorporated with the CREDC testbed.

FUTURE EFFORTS

- The next step is to create finer control in modifying packets to explore the possibility of more sophisticated MitM attacks.
- We want to integrate the MitM module with the fault injector module and observe how the simulated ICS reacts to different types of MitM attacks.

FUNDING SUPPORT PROVIDED BY THE DEPARTMENT OF ENERGY, OFFICE OF ELECTRICITY DELIVERY & ENERGY RELIABILITY