TCIPG

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

D. Chen, J. Zhang, K. Y. Tseng, Z. Kalbarczyk, R. Iyer

Goals

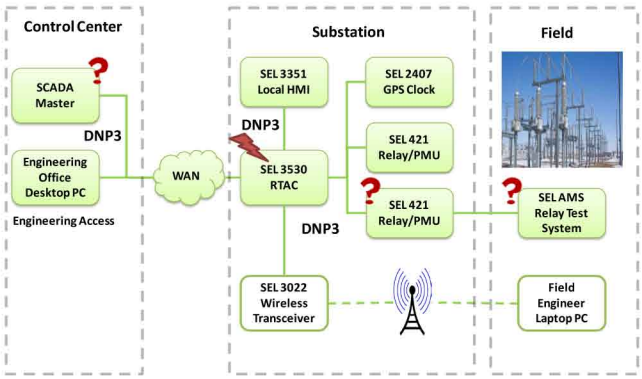
- Overall:
  - Develop methods and tools for evaluating security and reliability mechanisms for next-generation power grid.
  - Develop a framework for error diagnosis and experimental validation of system/application resiliency to errors and attacks.
- Specifically:
  - Experimentally study the impact of errors on next-generation micro-processor-based power grid equipment.
  - Experimentally validate bad data detection algorithm for PMU data.

Fundamental Questions/Challenges

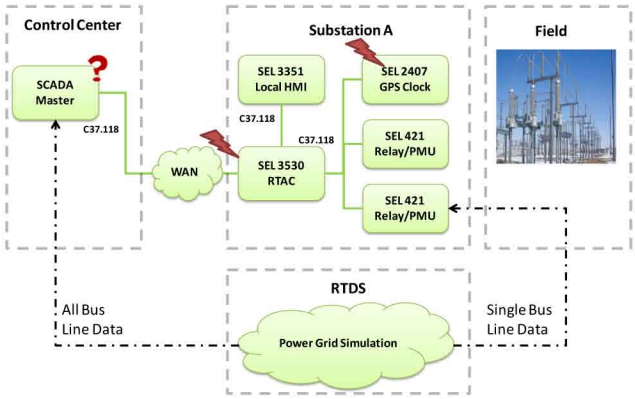
- New-generation power equipment more sensitive to accidental errors and malicious attacks:
  - micro-processor-based
  - increased network connectivity
  - synchronization between multiple devices
  - sophisticated remote control
- Crucial to understand failure modes and error/attack propagation patterns to enable improvements and deployment of protection mechanisms.

Research Plan

- Experimentally study the impact of errors on next-generation micro-processor-based power grid equipment:
  - Characterize error behavior and failure severity due to accidental and malicious errors in the power grid equipment.
  - Understand error impact and error propagation between the devices.
  - Develop and test error detection and recovery techniques to address the weaknesses discovered.



- Experimentally validate the bad data detection algorithm:
  - Study how PMU data can be corrupted.
  - Understand how to synchronize state estimation data and PMU data to utilize data redundancy.
  - Exploit the redundancy of state estimation data and PMU data for bad data detection.



Research Results

- Single-bit error in the DNP3 Client program could leave the DNP3 Master unable to pull the most current data from the Client, and the Client unable to receive control commands from the Master.
- Single-bit error in the codesys_rte program could cause the configuration of SEL-RTAC to reset, thus causing SCADA master to lose communication with the devices connected to the SEL-RTAC.

Broader Impact

- The testbed developed provides a platform to support a broad range of other experimental studies.
- The tools and methodology developed to assess error behavior could be applied to other power equipment.

Interaction with Other Projects

- Collaborate with a project on implementing appropriate and usable access control mechanisms for accessing power equipment configuration data.
- Collaborate and share the same testbed setup with projects on “Vulnerability Assessment Tool Using Model Checking” and “Quantifying the Impacts on Reliability of Coupling between Power System Cyber and Physical Components”

Future Efforts

- Develop error detection and recovery mechanism to increase the error resiliency of the power equipment.
- Explore other possible ways to corrupt and attack PMU data.