TCIPG

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

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

Goals

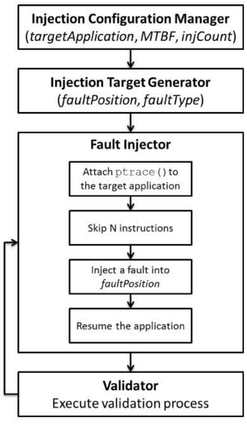
- Design a framework for error diagnosis and experimental validation of system/application resiliency to transient errors and malicious attacks for the next-generation power grid.
- Experimentally study the impact of errors/attacks on next-generation micro-processor-based power grid equipment.
- Develop detection and recovery mechanisms to protect power grid devices from transient errors and malicious attacks.

Fundamental Questions/Challenges

- New-generation power equipment is more sensitive to accidental errors and malicious attacks:
  - Microprocessor-based
  - Increased network connectivity
  - Synchronization between multiple devices
  - Sophisticated remote control
- It is crucial to understand failure modes and error propagation patterns to enable improvements and deployment of attack and error protection mechanisms.

Research Plan

- **Software-implemented Fault Injection (SWIFI)** is used to evaluate and characterize the behavior of power grid equipment.
- This technique can mimic the impact/consequences of transient errors and malicious attacks on the substation.
- Different devices in the TCIPG Testbed Laboratory are coordinated to mimic the working scenario of a power grid (as shown in Figure 2).
- A fault injection framework based on `ptrace()` is being developed to automate the fault injections to the critical applications (see Figure 1).
- *DNP3 Client, DNP3 Server, Monitor App* running on the Data Aggregator have been chosen as targets for fault injections.



Injection Configuration Manager
(*targetApplication*, *MTBF*, *injCount*)

Injection Target Generator
(*faultPosition*, *faultType*)

Fault Injector

Attach `ptrace()` to the target application

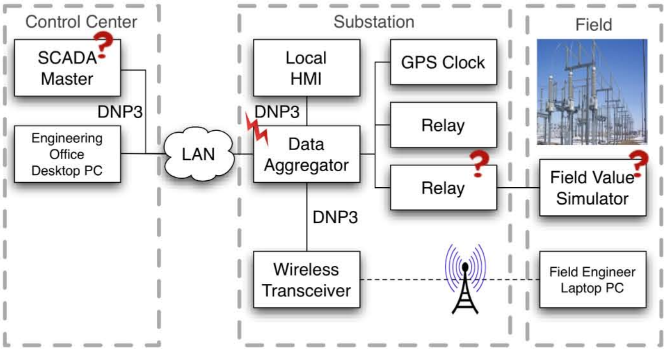
Skip N instructions

Inject a fault into *faultPosition*

Resume the application

Validator
Execute validation process

Figure 1. Fault Injection Process



Control Center

SCADA Master

Engineering Office Desktop PC

DNP3

LAN

Substation

Local HMI

DNP3

Data Aggregator

DNP3

Wireless Transceiver

GPS Clock

Relay

Relay

Field

Field Value Simulator

Field Engineer Laptop PC

Figure 2. Testbed Setup

Research Results

Silent Data Corruption (SDC) is the most severe outcome, which may cause the operator in the control center to lose control over the equipment in the substation.

- E.g., there are 13% and 7% chances that the DNP3 Client and DNP3 Server will exhibit silent data corruption (as shown in Figure 3).
- Lost control over the substation may result in a blackout or damage of equipment.

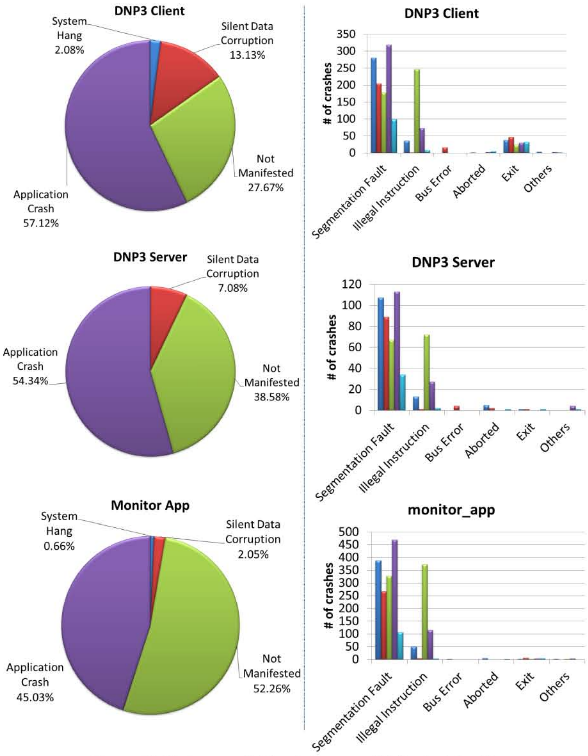


Figure 3. Outcome & Crash Cause of Injected Faults

Broader Impact

- The developed testbed provides a platform to support a broad range of other experimental studies.
- Experimental study provides important feedback to the power grid equipment manufacturers, to address potential reliability and security vulnerabilities.

Interaction with Other Projects

- Collaborate and share the testbed setup with the activity on "Specification-based IDS for the DNP3 Protocol" to study issues related to DNP3 security.

Future Efforts

- Experimentally validate and test the error detection and recovery techniques to address the weaknesses discovered.