TCIPG

Testbed Overview

Tim Yardley, David Nicol, William H. Sanders

Goals

- Provide provisioning for experimental support/integration of TCIPG projects.
- Provide a simulation and emulation environment with real hardware and software used in the power grid.
- Serve as a national resource for experimental work in research and analysis of trustworthy power grid systems.
- Span transmission, distribution & metering, distributed generation, and home automation and control, providing true end-to-end capabilities.

Fundamental Questions/Challenges

- How does one provide a large-scale, realistic, end-to-end power grid experimentation platform that is both repeatable and flexible to cover both legacy and emerging research?
- How does one leverage real equipment, simulation, and emulation to provide the necessary capabilities?
- How does one programmatically integrate, control, and interact with power grid equipment that was not designed with that in mind?

Research Plan

- Develop new modeling and evaluation technologies to enhance evaluation capabilities of the testbed.
- Continue to expand the equipment capabilities, features, and functionality through strategic integration of both software and hardware.
- Develop integration glue to seamlessly integrate power grid equipment and software into the testbed by combining simulation, emulation, and real equipment.
- Leverage existing and emerging research from other areas when it can benefit the goals of the testbed effort.

Impact and Interaction

- Enabling advanced research for smart grid efforts throughout the world.
- Flexible framework is being implemented and advancing towards tailored operating constraints.
- Will be open for collaborative research, facility-driven use, sponsored research, or technical testing.

Example Research Results

- Real-time Immersive Network Simulation Environment (RINSE) and Virtual Power System Testbed (VPST): large scale network and cyber-physical simulation.
- Network Access Policy Tool (NetAPT): policy tool to evaluate network access paths and verify compliance with a global policy.
- Security research on smart grid protocols, including AMI and SCADA protocols.

Capabilities

- Full end-to-end “smart grid” capabilities.
- Advanced Metering Infrastructure (AMI).
- Real, emulated, and simulated hardware/software.
- Real data from the grid, industry partners, etc.
- Power simulation, modeling, and optimization.
- Network simulation and modeling, visualization.
- Hardware-in-the-loop cyber-physical simulation.
- WAN/LAN/HAN integration and probes.
- Security and protocol assessment tools (static/dynamic analysis, test harnesses, fuzzing).

Hardware and Software

- RTDS, PowerWorld, PSSE, PSCAD, PSLF, DSAtools, DynRed.
- RINSE, tstBench, LabView, OSI PI, OSIi Monarch, SEL Suites.
- GPSs, substation computers, relays, PMUs, testing equipment, PLCs, security gateways, NI platforms.
- Power analysis tools, PDCs, data analytics.
- Full AMI deployment (meters, relays, MDMS), TCIPG smart meter research platform.
- RTUs, F-Net, inverters, oscilloscopes, firewalls, embedded devices, sensors, spectrum analyzers, SIEMs, IDSes.
- Home EMS, energy monitoring devices, Zigbee, automation.
- Display wall, visualization platforms (STI, RTDMS), training.
- Mu Dynamics, Fortify, security research tools.
- DETER integration and cyber-physical extension.

Use Cases

- Provide a multifaceted approach to security through testbeds, education and training, field testing, and tool creation.
- Facilitate collaboration among researchers and industry to work towards creation of more resilient critical infrastructure.
- Facilitate rapid transition and adoption of research in industry.
- Provide positive real-world impact through engagement.
- Allow for cutting-edge smart grid security research.