

## GOALS

- Span transmission, distribution & metering, distributed generation, and home automation and control, providing true end-to-end capabilities.
- Provide foundational research support for TCIPG projects.
- Validate research across varying fidelities and scales.
- Leverage advanced testbed capabilities to train the next generation of secure power systems professionals.
- Develop and share open models of cyber and power systems to facilitate reproducible experimentation in this sector.
- Serve as a national resource for experimental work in research and analysis of trustworthy power grid systems.

## FUNDAMENTAL QUESTIONS / CHALLENGES

- How does one provide a scalable and flexible framework that can operate at varying fidelities to facilitate emerging research?
- What is the right mix of simulation, emulation, and real equipment to accomplish the stated research goals, and how does one set up an experiment to achieve those goals?
- How does one programmatically set up, integrate, control, and interact with the equipment, and how can this be done to support both research and education/training?

## RESEARCH PLAN

- Develop and share new cyber-physical and experimentation models and technologies to enhance experimentation capabilities.
- Continue to expand the testbed capabilities, features, and functionality through strategic integration of equipment.
- Develop and share integration glue that provides unique capabilities in the testbed environment.
- Leverage existing and emerging research from other areas when it can advance the goals of the testbed effort.
- Develop and share an open, modular, and exercise-based training curriculum for cyber security in the smart grid.

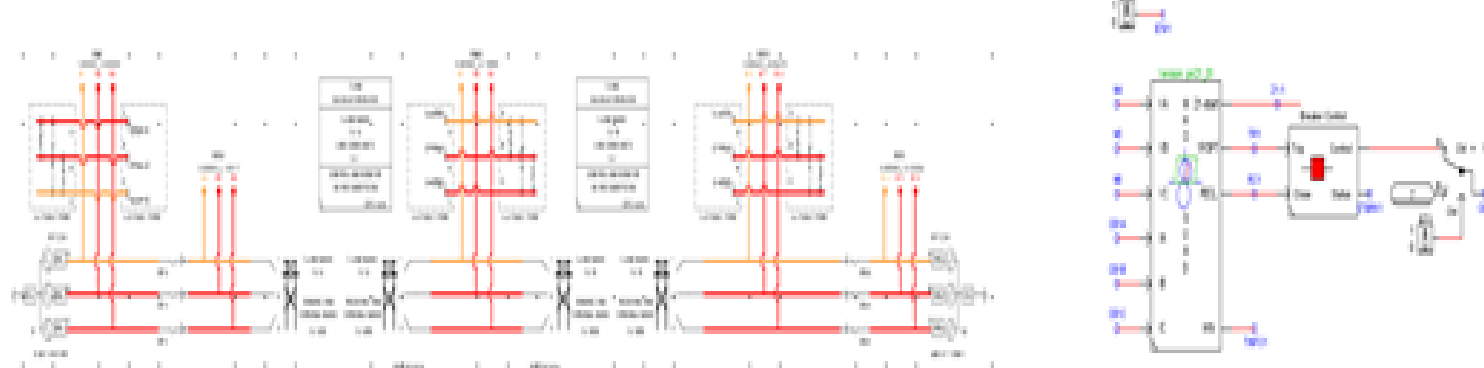
## HIGHLIGHTED RESEARCH RESULTS

- Virtual Power System Testbed (VPST and RINSE/S3F): large-scale cyber-physical simulation.
- Network Access Policy Tool (NetAPT/NP-View): policy tool to evaluate network access paths and verify compliance with a global policy.
- Tools and analysis of smart grid protocols: Amilyzer, protocol parsers and test harnesses, and scalable environment.
- Quantum key distribution: validation of external quantum computing research through application to smart grid systems.
- Released various IEEE bus models in several simulator formats.
- Five student-created protection relay models demonstrating protection functions in a connected simulation environment.

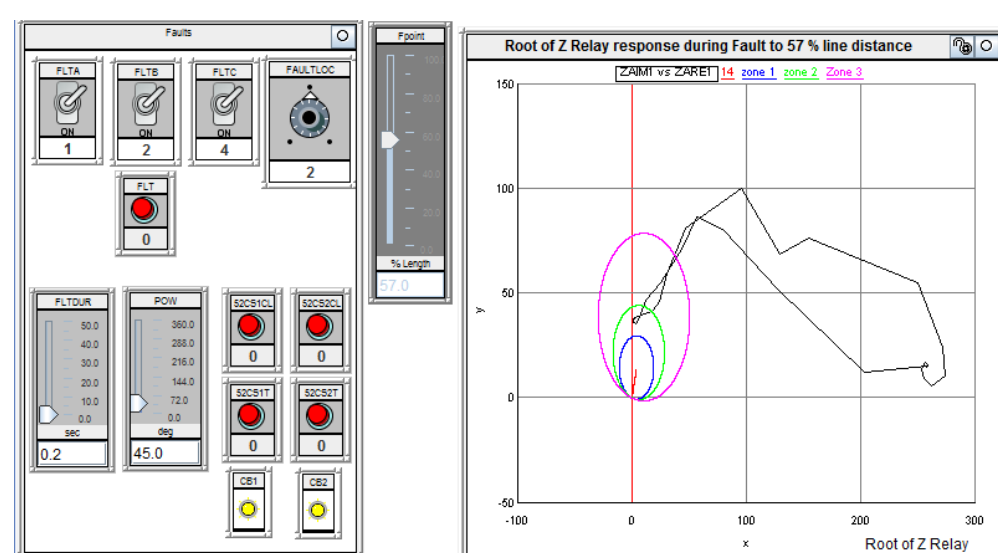
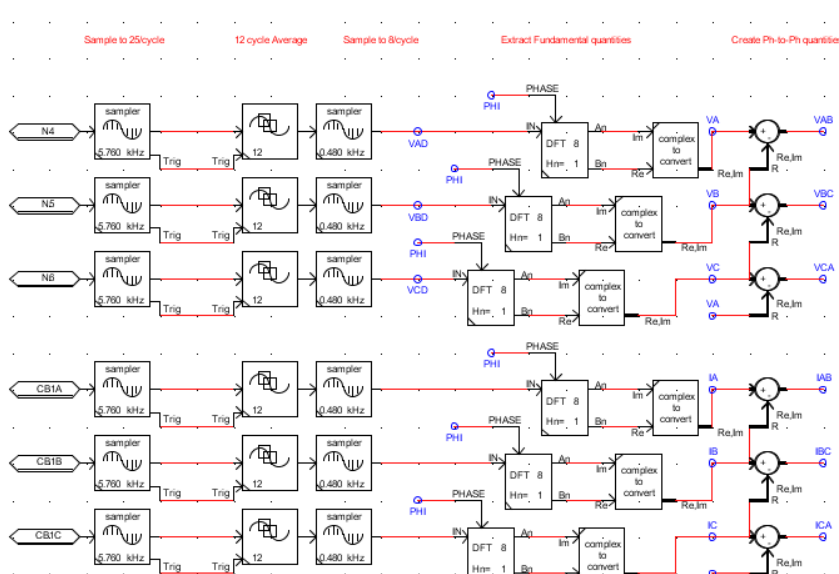
SEL-421 Directional Impedance Relay



Case Modeling



Run Mode



## BROADER IMPACT

- Enabling advanced research for smart grid efforts throughout the world via federation and collaboration.
- Flexible framework leverages tailored operating constraints to use resources efficiently for research, education, and training.
- Open for collaborative research, facility-driven use, sponsored research, education and training, and technical testing.

## CAPABILITIES

- Full end-to-end smart grid capabilities.
- On-grid 12kV/69kV testing capabilities via Ameren TAC facility (with fiberoptic interconnects to the TCIPG testbed).
- Deployed advanced metering infrastructure (AMI).
- Solar research platforms.
- Real, emulated, and simulated hardware/software for scalability.
- Real data from the grid, industry partners, etc.
- Power simulation, modeling, and optimization of various forms.
- Network simulation, modeling, and visualization of various forms.
- Advanced hardware-in-the-loop cyber-physical simulation.
- WAN/LAN/HAN integration and probes.
- Security & protocol assessment tools (static/dynamic analysis, test harnesses, fuzzing).

## ASSETS

- RTDS, PowerWorld, PSSE, PSCAD, PSLF, DSAtools, DynRed.
- RINSE, tstBench, LabView, OSI PI, OSII Monarch, SEL suites, PGDA.
- Full range of open-source power grid tools (openDNP3, openPDC, openPG, openXDA/openFLE, openHistorian, SIEGate, GridLAB-D).
- Substation computers, relays, PMUs, testing equipment, PLCs, security gateways, NI platforms.
- Power analysis tools, PDCs, data analytics.
- Full AMI deployment, TCIPG Smart Meter Research Platform.
- RTUs, F-Nets, 4-quad amps, oscilloscopes, firewalls, embedded devices, sensors, spectrum analyzers, SIEMs, IDSes, RF capture, GPS signal generation, GPS clocks.
- Home EMS, energy and environmental monitoring devices, ZigBee, automation, building automation controls.
- Display wall, visualization platforms (STI, RTDMS), training platforms.
- Mu Dynamics, Fortify, security research tools, IBM Tivoli suite.
- DETER integration and cyber-physical extension via federation.

## 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.

