TCIPG

ANNUAL INDUSTRY WORKSHOP
NOVEMBER 12-13, 2014

CLUSTER:
TRUST ASSESSMENT

NOVEMBER 12, 2014

ZBIGNIEW KALBARCZYK

UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

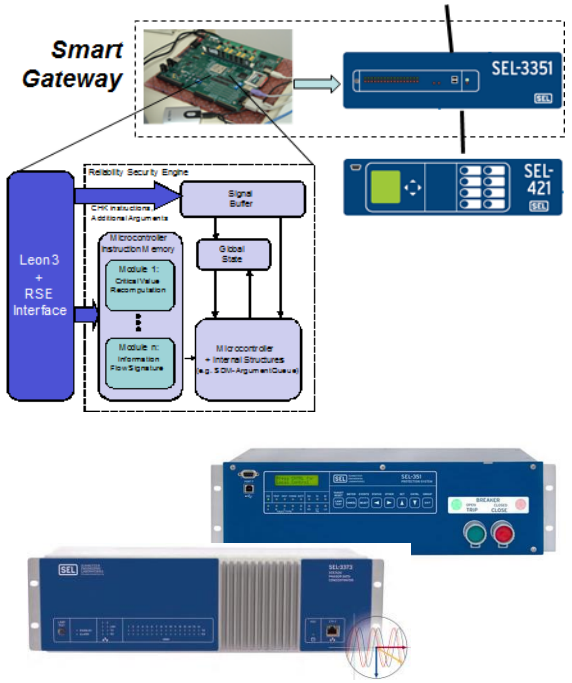
FUNDING SUPPORT PROVIDED BY DOE-OE AND DHS S&T

CLUSTER THEMES

- Create methods and tools that use simulation, modeling, and experimentation to support quantitative trust assessment of
  - power grid devices, hardware/software architectures, protocols, and applications
  - measurement data representing power system state
  - monitoring and protection mechanisms/algorithms used to provide power grid resiliency
  - emerging computing technologies, e.g., cloud computing infrastructure to support Smart Power Grid

TCIPG ACCOMPLISHMENTS IN THIS CLUSTER (1)

- *Back in 2005 work focused on:*
  - Providing evidence of security threats in Power Grid
  - Develop methods for hardening hardware/software computing base
  - Develop new validation (simulation and experimental based) methods applicable to cyber physical system such as power grid
  - PMUs were “few and far between”

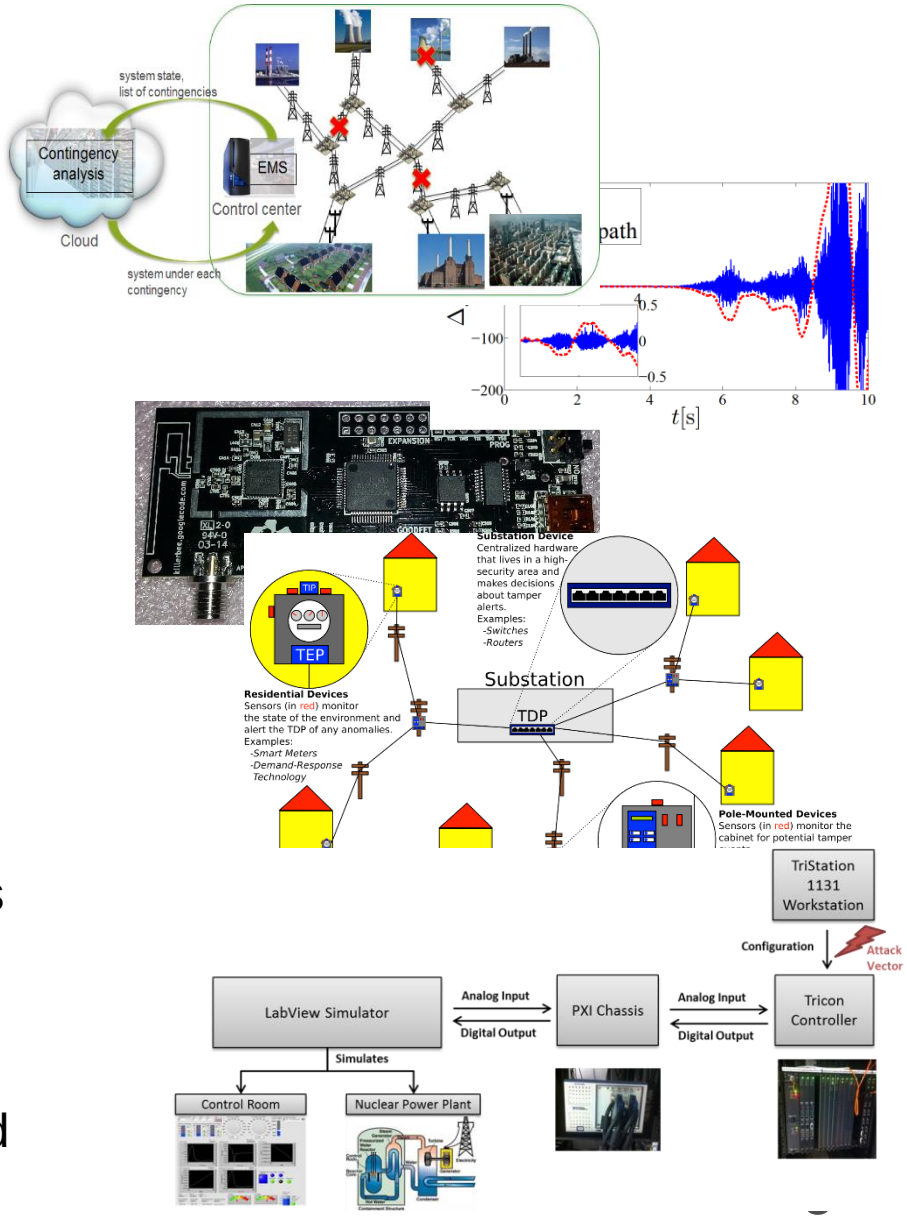


TCIPG ACCOMPLISHMENTS IN THIS CLUSTER (2)

- *Today (recent years):*
  - New tools for automated analysis and identification of configuration inadequacies in power grid environment (NetAPT -> NP-View)
  - High-fidelity highly-scalable simulation and emulation platform for security evaluation in power grid control networks
  - Analysis of vulnerabilities associated with measurement and collection of PMU data
  - *Api-mote* toolset to facilitate assessment of ZigBee Networks security
  - Tools for experimental (fault injection based) evaluation of the impact of data corruption in power substation on the health of the power network

ACTIVITIES

1. Quantifying the Impacts on Reliability of Coupling between Power System Cyber and Physical Components
2. Security and Robustness Evaluation and Enhancement of Power System Apps
3. Synchrophasor Data Quality
4. Testbed-Driven Assessment: Experimental Validation of System Security and Reliability
5. Trustworthiness Enhancement Tools for SCADA Software and Platforms
6. Understanding and Mitigating the Impacts of GPS/GNSS Vulnerabilities
7. 802.15.4/ZigBee Security Tools
8. Tamper Event Detection Using Distributed SCADA Hardware

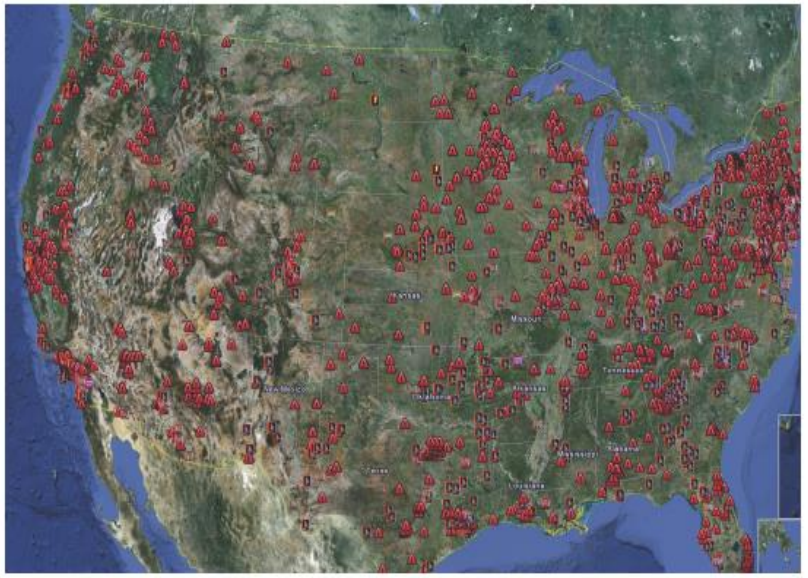


CURRENT CHALLENGES

- ***Model-based assessment***
  - Create scalable modeling and simulation infrastructure for evaluation of power grid architectures and applications
  - Create stochastic models for power system to study reliability impact of uncertainties introduced by cyber and physical components
  - Create tools for automated analysis of integrity of security policies
- ***Experiment-based assessment***
  - Create experimental environment to test and evaluate security of power grid devices, protocols, and applications under realistic use cases
  - Assure trustworthiness of PMU data and their use for detection of malicious attacks and accidental failures
  - Use of cloud computing for power grid, including applications, grid management, and tools for security assessment

EMERGING OPPORTUNITIES AND CHALLENGES (1)

- *Challenge:* Control system devices on the Internet
  - Many critical infrastructure assets are directly facing the Internet
  - About 7,200 Internet facing control system devices in US
  - These devices once accessed can provide an entry point to the control network (ICS-CERT 2012)



- *Need*
  - Methods to identify and remove the direct access of control system devices to the Internet
  - Intelligent methods to monitor and detect intruders preemptively, i.e., before the damage to the system
  - Validation

EMERGING OPPORTUNITIES AND CHALLENGES (2)

- *Challenge:* Broad spectrum of vulnerabilities to handle
  - 181 vulnerability reports from researchers and ICS vendors in 2013
  - 87% exploitable remotely; 13% required local access (ICS-CERT 2013)

Need

- Adapt and assess techniques and strategies used in other application domains to provide ICS resiliency