Trust Assessment

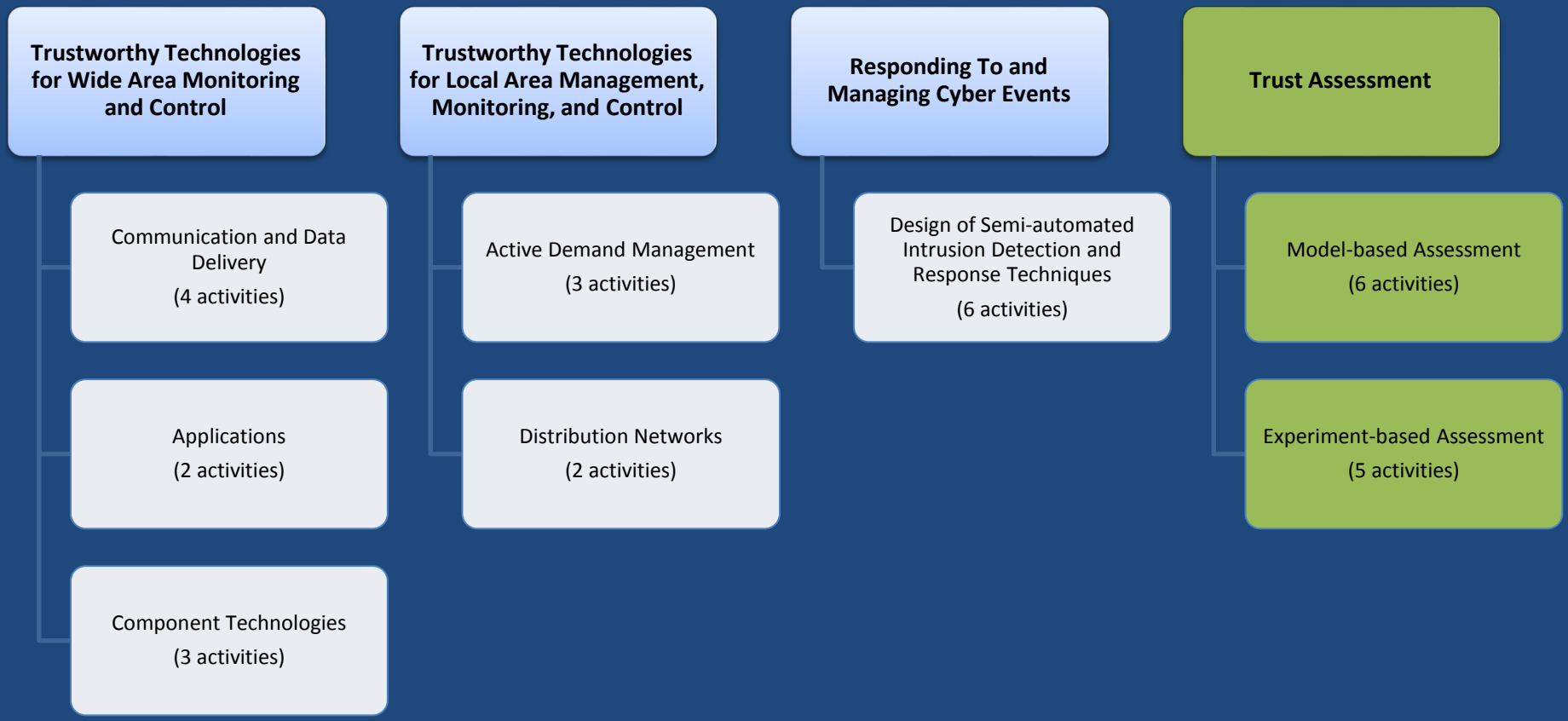
Zbigniew Kalbarczyk

Number of Activities: 11

2012 Industry Workshop

October 30, 2012

TCIPG Technical Clusters and Threads



Cluster Overview

- This cluster builds methods and associated tools to support quantitative trust assessment of
  - devices, hardware/software architectures, protocols, and applications
  - quality of measurement data representing system state
  - monitoring and protection mechanisms/algorithms used to provide resiliency in the context of the power grid

Cluster Problem Areas

- The cluster focuses on issues associated with providing techniques to analyze and measure power grid resiliency to
  - malicious attacks and accidental errors
  - potential volatility of energy sources
- Cluster directly addresses technical issues in
  - Testing and evaluating applications, protocols, and devices employed to permit uninterrupted energy delivery
  - Analyzing integrity of security policies
  - Reasoning about vulnerabilities being in applications or security policies
  - Assessing resiliency of different system configurations
  - Assessing quality of measurement data reflecting system state
  - Analyzing reliability and economics in Smart Grid settings

Cluster Approach

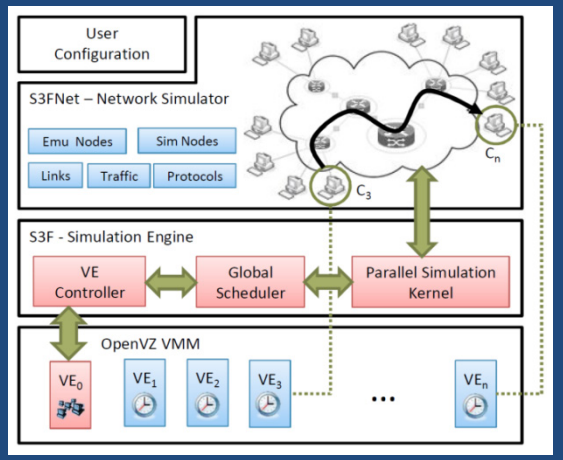
- Create methods and tools that use simulation, modeling and experimentation to characterize resiliency of power grid devices, subsystems and applications in presence of malicious attacks and accidental errors
- *Model-based Assessment Thread*
  - Use modeling, formal methods (including model checking) and high fidelity simulation to build tools for supporting a broad range of analysis and evaluation studies
- *Experiment-based Assessment Thread*
  - Use real physical devices to create system/application configurations that mimic power grid settings (e.g., power substation)
  - Create tools to support experimental assessment of: (i) error resiliency of systems and applications and (ii) efficiency of error/attack protection mechanisms

Cluster Impact

- NetAPT (Network Access Policy Tool) fully implemented and ready for commercialization
- High-fidelity highly-scalable simulation and emulation platform for security evaluation in power grid control networks
- Contingency analysis framework for the power grid that takes into account characteristics of the underlying cyber infrastructure
- Established NDA with ATC to facilitate synchrophasor data exchange
- A prototype of *Api-mote* to facilitate assessment of ZigBee Networks security
- Demonstrated experimentally that undetected data corruption in substation devices can cause the Control Center to temporarily operate on invalid information on the system state

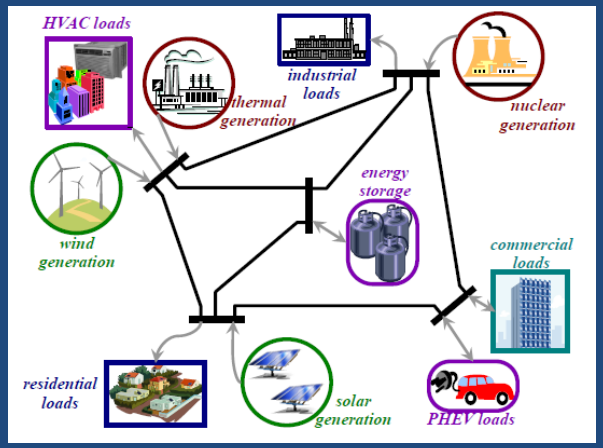
Activity Highlights

- *Automatic Verification of Network Access Control Policy Implementations*
  - Software tool (NetAPT) to analyze security policy implementation for conformance with global security policy specification. Fully implemented and used to aid in vulnerability assessments and compliance audits at our industry partners.
- *Modeling Methodologies for Power Grid Control System Evaluation*
  - Large-scale, high-fidelity simulation testbed (parallel network simulator and OpenVZ emulation with virtual time system).
- *Quantifying the Impacts on Reliability of Coupling between Power System Cyber and Physical Components*
  - Modeling framework for quantifying the effect of cyber events on system performance measures, e.g., increase in noise in feedback AGC (Automatic Generation Control) communication channels



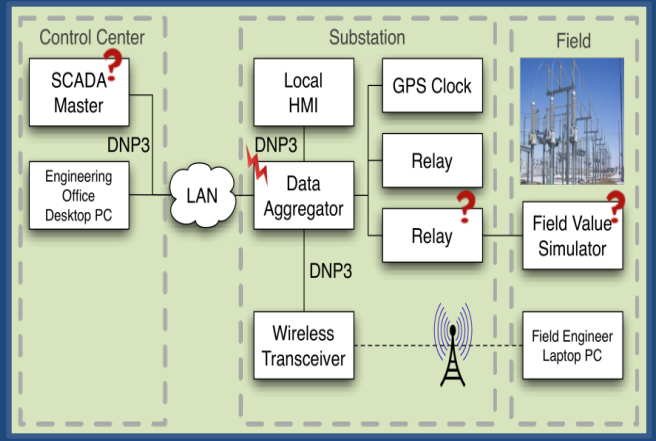
Activity Highlights

- *Security and Robustness Evaluation and Enhancement of Power System Applications*
  - Impact of malicious sensor data manipulation in power systems, and analyzed mitigation and defense strategies based on the state of the underlying cyber infrastructure and power system operations.
- *Smart Grid: Economics and Reliability*
  - Control strategies for power grids with renewable generation, energy storage and demand response resources. Study HVAC loads of commercial buildings to extract ancillary services (e.g., manipulating the fan speed) from these loads without discomfort to building occupants.
- *Synchrophasor Data Quality*
  - Study the sources, effects, and implications of absent or erroneous synchrophasor data and remedies for defective synchrophasor data.



Activity Highlights

- *Testbed-Driven Assessment: Experimental Validation of System Security and Reliability*
  - Error injection methods for evaluating impact of an attack or an accidental error on power grid equipment (including SCADA). Assess impact on system robustness of data corruption in substation devices.
- *Tools for Assessment and Self-assessment of ZigBee Networks*
  - Low-cost commodity tools for characterizing security of ZIgBee networks.



- *Trustworthiness Enhancement Tools for SCADA Software and Platforms*
  - Tools to maintain trustworthiness of embedded systems in smart grid. Leverage already developed (e.g., YASIR, Katana, and Autoscopy Jr.) and build new lightweight security support that can live at different levels inside a device (e.g., at the process-level or at the low-level network support).

Planned Research for Coming Year

- Interfacing NetAPT with their Sophia (INL) tool to enhance the topology discovery and firewall maintenance, and refine global policies
- Enhance simulation/emulation testbed, e.g., develop distributed simulation control and support more virtualization platforms, e.g. Xen, QEMU
- Simulation study of the control algorithms develop to manage resources in a constrained power network with focus on flexible resources, e.g., HVAC
- Assessment of synchrophasor data quality and understanding of the impact on power system performance, of cyber attacks that affect accuracy and validity of the PMU data
- Design, prototype, and evaluate mechanisms/algorithms for rapid detection of data corruption in SCADA environment (e.g., data aggregator in a substation)
- Light-weight trustworthiness enhancement tools for SCADA software and platforms, e.g., ELFBac, an instrumentation system for isolating security critical pieces of a binary without the need to rewrite the original program

Questions?