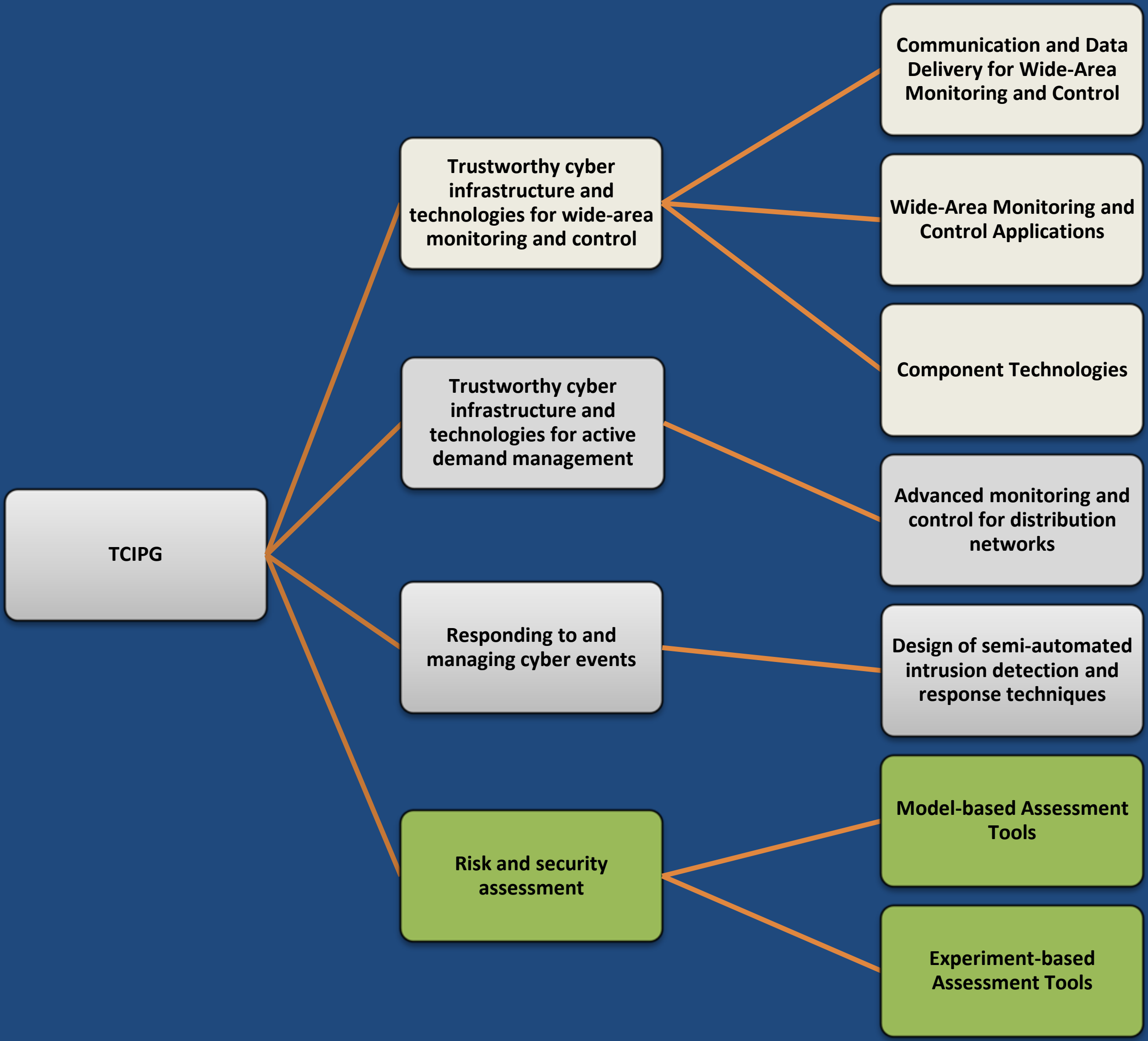
Risk and Security Assessment

Zbigniew Kalbarczyk

TCIPG Cluster Arrangement


TCIPG
Trustworthy cyber infrastructure and technologies for wide-area monitoring and control
Communication and Data Delivery for Wide-Area Monitoring and Control
Wide-Area Monitoring and Control Applications
Component Technologies
Trustworthy cyber infrastructure and technologies for active demand management
Advanced monitoring and control for distribution networks
Responding to and managing cyber events
Design of semi-automated intrusion detection and response techniques
Risk and security assessment
Model-based Assessment Tools
Experiment-based Assessment Tools

Cluster Overview

- Cyber infrastructure for power grid constitutes a large-scale heterogeneous system that provides critical services on the continuous basis
  - Many players contribute to robustness of the infrastructure: energy producers and providers, users, equipment manufacturers, standardization bodies …

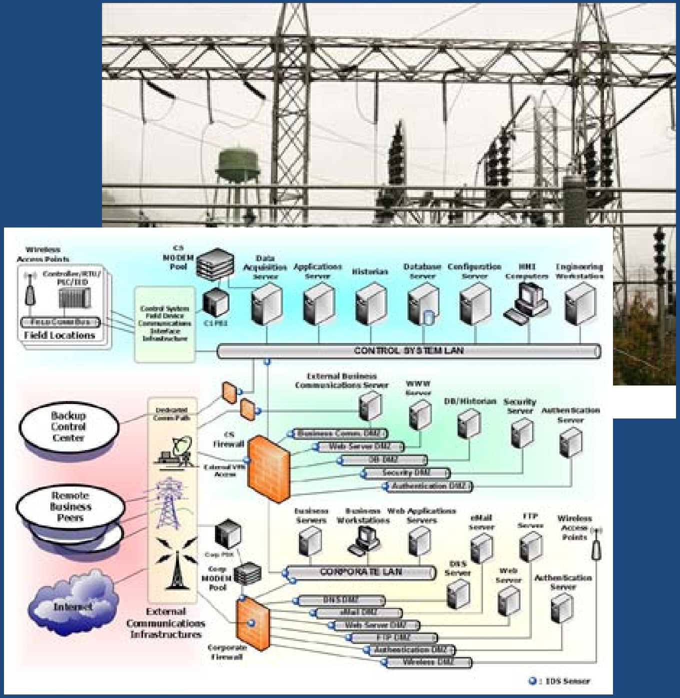
- This cluster builds methods and associated tools to support design and quantitative assessment of devices, hardware/software architectures, protocols, applications, and monitoring and protection mechanisms/algorithms used to provide security and reliability in the context of power grid

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:
  - Designing, 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
  - Analyzing reliability and economics in smart grid settings

Cluster Objectives

- Provide methods and tools that use simulation, modeling and experimentation to
  - Characterize system resiliency in presence of malicious attacks and accidental errors
  - Measure and quantify the system security/reliability
  - Evaluate effectiveness and performance of novel mechanisms for continuous monitoring and defense against potential intruders and failures
  - Analyze and assess interplay between economics, renewable energy sources and demand response

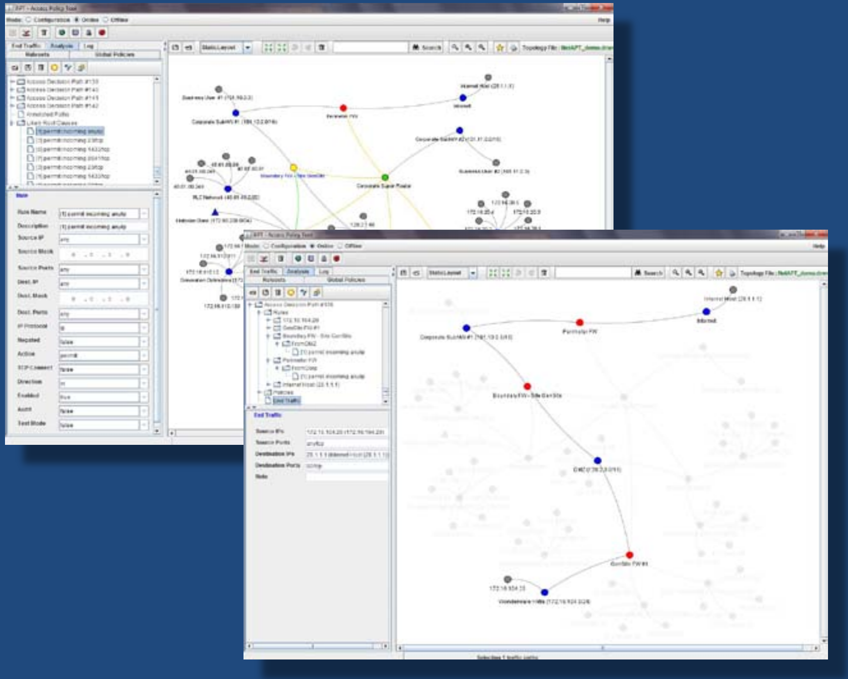


Cluster Activities (with more details in posters)

- Ongoing
  - Automatic verification of network access control policy implementations
  - Modeling methodologies for power grid control system evaluation
  - Quantifying the impacts on reliability of coupling between power system cyber and physical components
  - Analysis of impacts of smart grid resources on economics and reliability of electricity supply
  - Test-bed driven assessment: experimental validation of system security and reliability
  - Trustworthiness enhancement tools for SCADA software and platforms
  - Tools for assessment and self-assessment of ZigBee networks
  - Fuzz-testing of proprietary SCADA/control network protocols
- New Starts
  - Security and robustness evaluation and enhancement of power system applications
- Completed
  - Vulnerability assessment tool using model checking

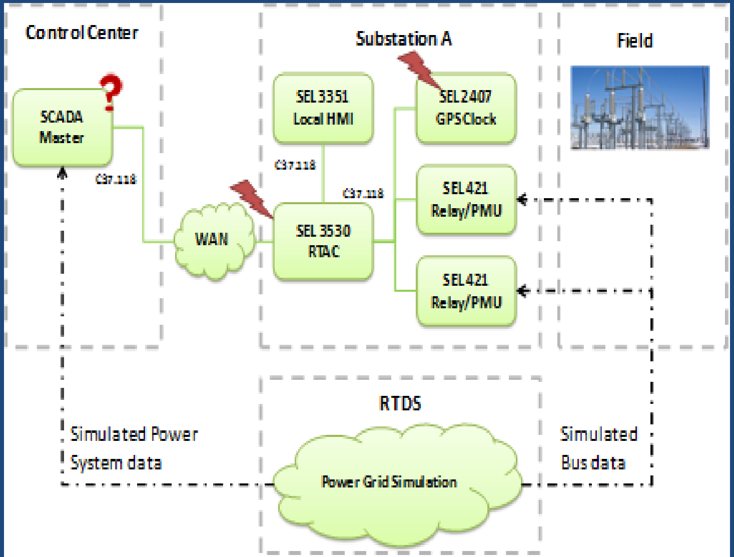
Cluster Accomplishments and Impacts

- Developed software tool (NetAPT) to analyze security policy implementation for conformance with global security policy specification for industrial control networks
  - NetAPT has been released to select industry partners for evaluation
  - NetAPT was used for an internal audit and vulnerability assessment at a major utility, for a network with nearly 100 firewalls and several thousand hosts
  - Close interaction with utility partners and NERC CIP auditors



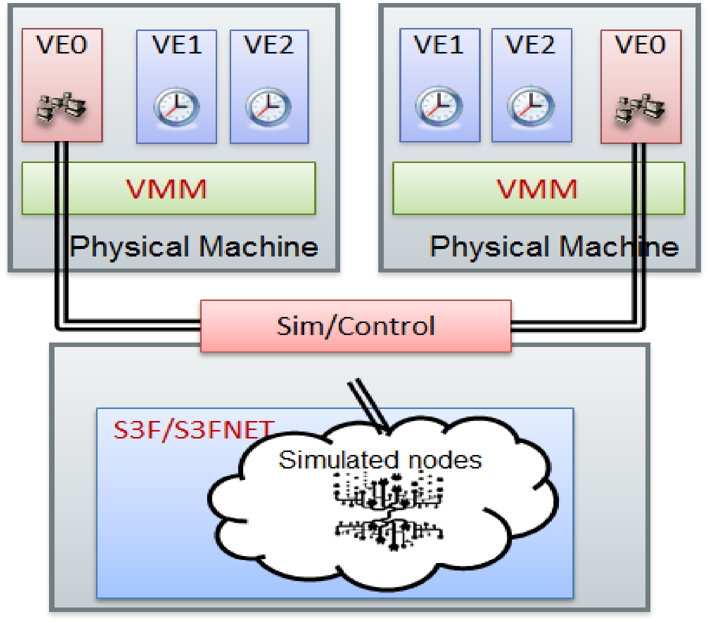
Cluster Accomplishments and Impacts, cont.

- Developed generic tools (software and hardware) for on-line system assessment
  - Hot-patching tool (Katana)
  - Lightweight in-kernel intrusion-detection system (Autoscopy Jr.)
  - First generation tools for 802.15.4/ZigBee Networks assessment
- Developed methods and tools for experimental assessment of power grid applications & hardware configurations using testbed
  - Built experimental setup to mimic current generation substation/SCADA
  - Created fault/error injection tool to simulate impact of malicious errors



Cluster Accomplishments and Impacts, cont.

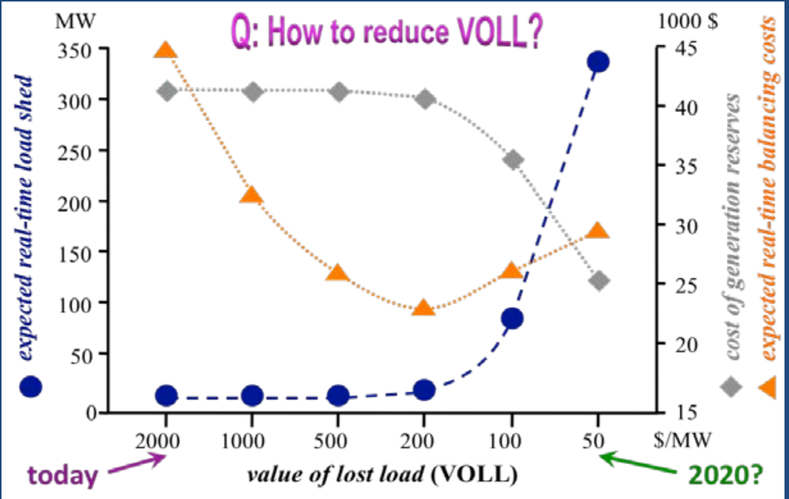
- Developed high fidelity simulation engine
  - Virtual machine (OpenVZ) based high functional & temporal fidelity network simulation with good scalability
  - Parallel network simulator that enables
    - interactive communication with emulation
    - analysis of various application scenarios in a large-scale setting



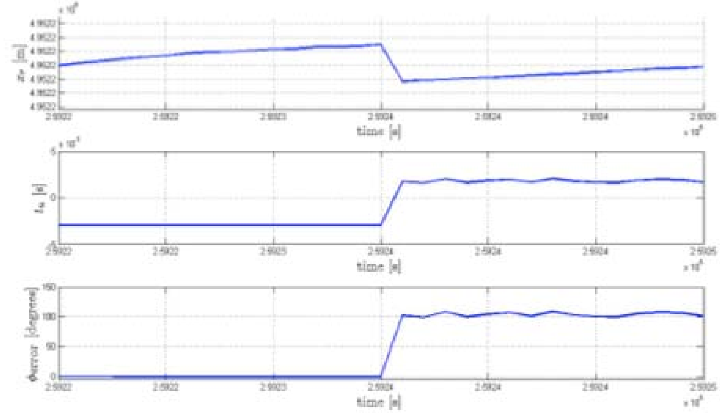
- Developed formal tools for vulnerability assessment
    - A technique and a tool to discover vulnerabilities in an application using symbolic execution and model checking

Cluster Accomplishments and Impacts, cont.

- Developed simulation to analyze impact of smart grid resources on economics and reliability of electricity supply
    - Evaluated impact of renewable generation, energy storage, and demand response on markets and energy delivery
- Developed simulation (MATLAB based) to characterize the impact of GPS clock spoofing attack on phase shift error on PMU data



Load shedding can be cheaper than purchasing reserve generation capacity



4 Satellite spoofing

Cluster Directions for Coming Year

- Release of NetAPT to SERC for use in audits
- Work with INL to interface NetAPT with Sophia
- Design of electricity contracts viewing electricity as a service or product with multi-attributes rather than a commodity
- Full characterization of the impact of attacks as a function of the number of spoofed satellites
- Characterization of transient error and attack propagation and impact on power equipment and applications in substation and SCADA
- Experimental validation of bad data (due to GPS clock spoofing) detection algorithm
- Work on transitioning Autoscopy Jr. (an intrusion detection system) into real devices used in power grid settings
- Work on integration of the simulation capabilities with the test bed environment for experimental system evaluation

Questions and Discussion