Assuring the Trustworthiness of the Smarter Electric Grid

Bill Sanders

University of Illinois at Urbana-Champaign
www.tcipg.org
whs@illinois.edu

ICPE 2012

Coordinated Science Laboratory

Building Interdisciplinary Excellence with Societal Impact

- **Excellence in:**
  - Computing and Networks
  - Circuits, Electronics & Surface Science
  - Communications & Signal Processing
  - Decision & Control
  - Remote Sensing

- **Initiatives:**
  - Computer Vision
  - SRC Focus Center Research Program
  - Neuroengineering IGERT
  - Human-Machine Adversarial Network MURI

- **Statistics:**
  - 60 years as a premier national interdisciplinary research facility
  - 550 Researchers: 110 professors, 330 graduate students, 60 undergraduate students, & 50 professionals
  - Over $300M in active research projects as of Jan. 2011

- **Affiliated Institutes:**
  - ITI: Information Trust Institute
  - ADSC: Advanced Digital Sciences Center (Singapore)
  - PCI: Parallel Computing Institute

- **Major Centers:**
  - Illinois Center for Wireless Systems
  - NSF National Center for Professional and Research Ethics
  - NSF Science of Information Science and Technology Center
  - DOE/DHS Trustworthy Cyber Infrastructure for the Power Grid (TCIPG) Center
  - Boeing Trusted Software Center
  - HHS SHARPS Health Care IT Security Center
  - NSA Science of Security Center
  - Illinois Center for a Smarter Electric Grid

Outline

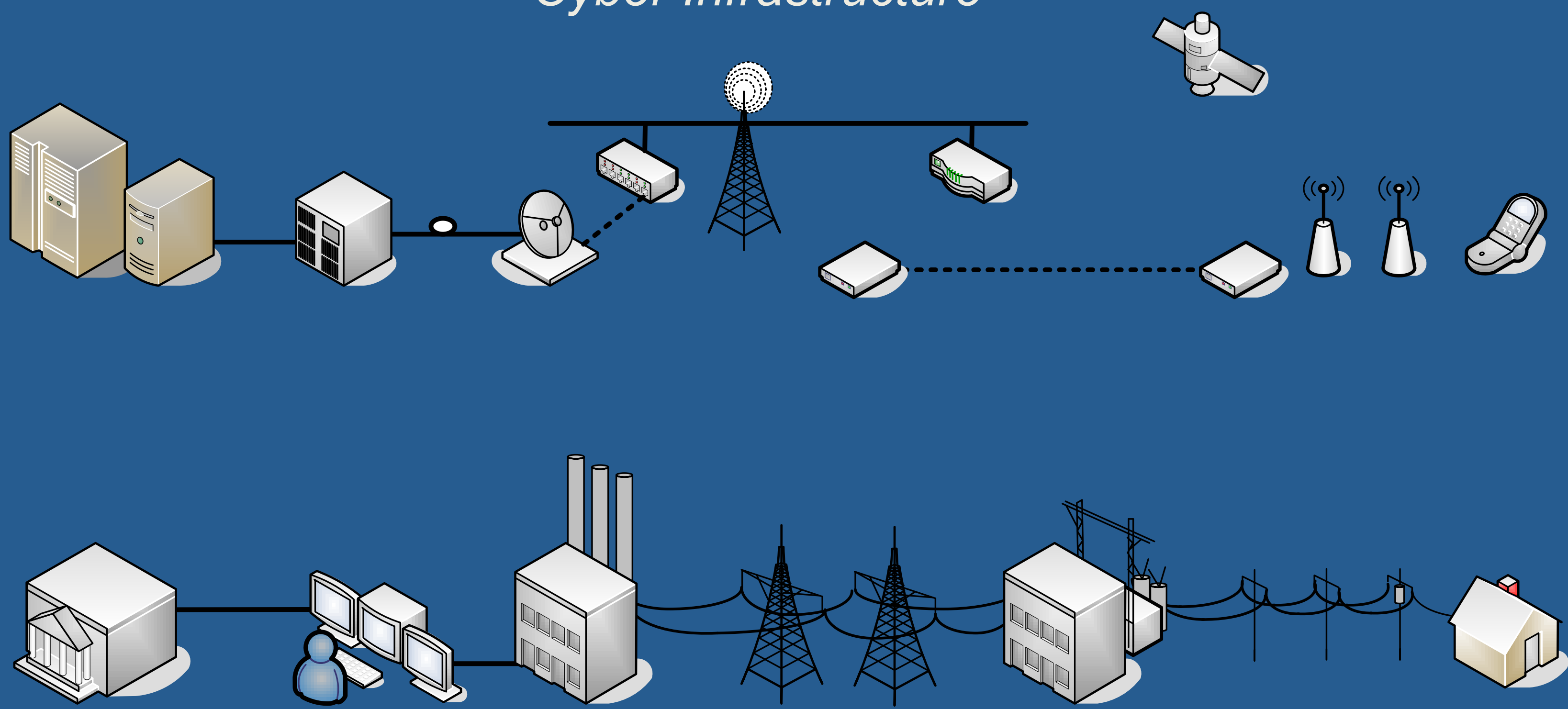
- A Quick Primer on the Modern Electric Grid
- Vulnerabilities and Threats
- Challenges to Achieving Trustworthy Operation
- TCIPG's Research Mission and Results

Outline

- A Quick Primer on the Modern Electric Grid
- Vulnerabilities and Threats
- Challenges to Achieving Trustworthy Operation
- TCIPG's Research Mission and Results

Power Grid Trust Dynamics
Span Two Interdependent Infrastructures

Cyber Infrastructure



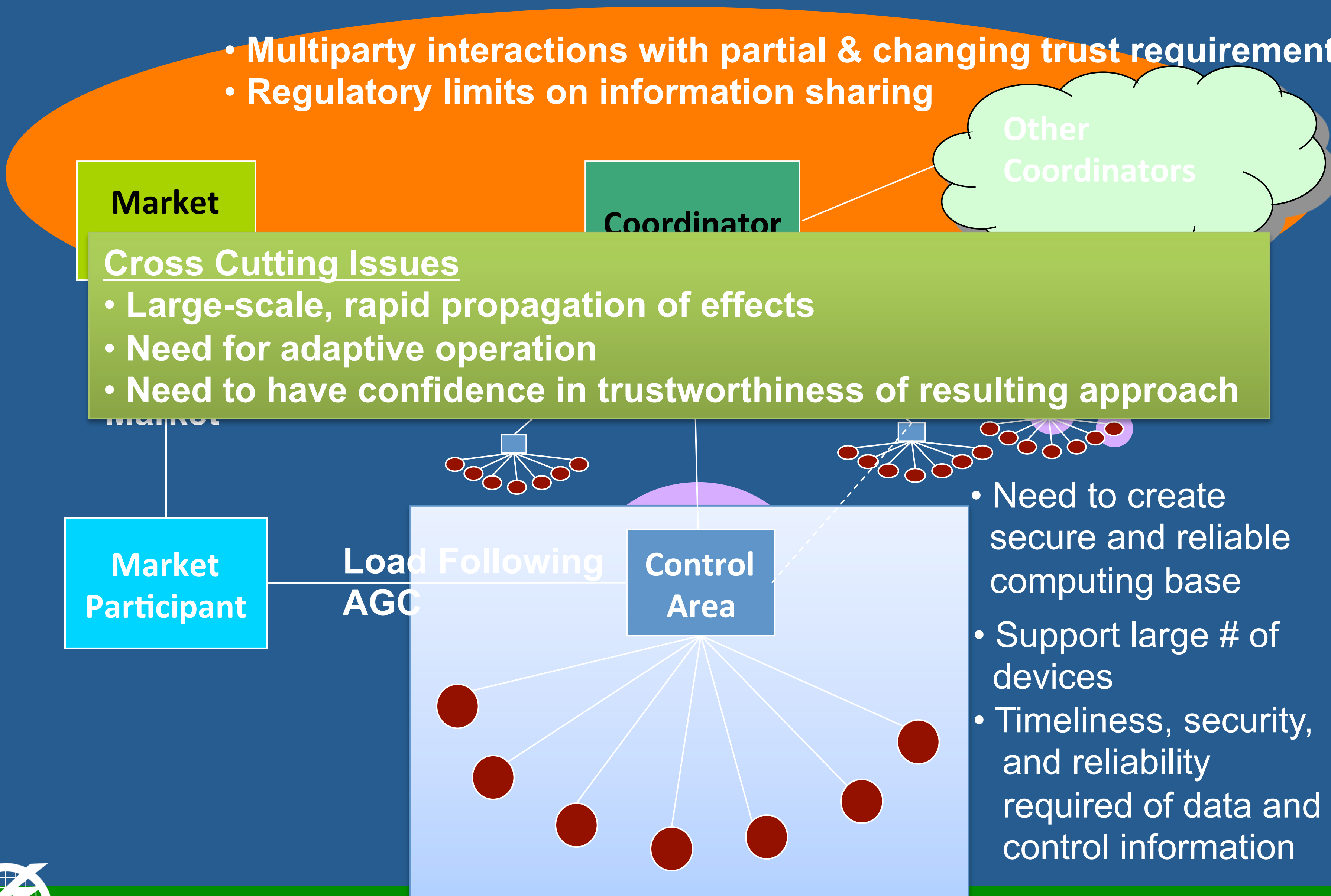
Electrical (Physical) Infrastructure

The Challenge: Providing Trustworthy Smart Grid Operation in Possibly Hostile Environments

- Trustworthy
  - A system which does what is supposed to do, and nothing else
  - Availability, Security, Safety, …
- Hostile Environment
  - Accidental Failures
  - Design Flaws
  - Malicious Attacks
- Cyber Physical
  - Must make the whole system trustworthy, including both physical & cyber components, and their interaction.

Next-Generation Power Grid Cyber Infrastructure Challenges

- Multiparty interactions with partial & changing trust requirements
- Regulatory limits on information sharing



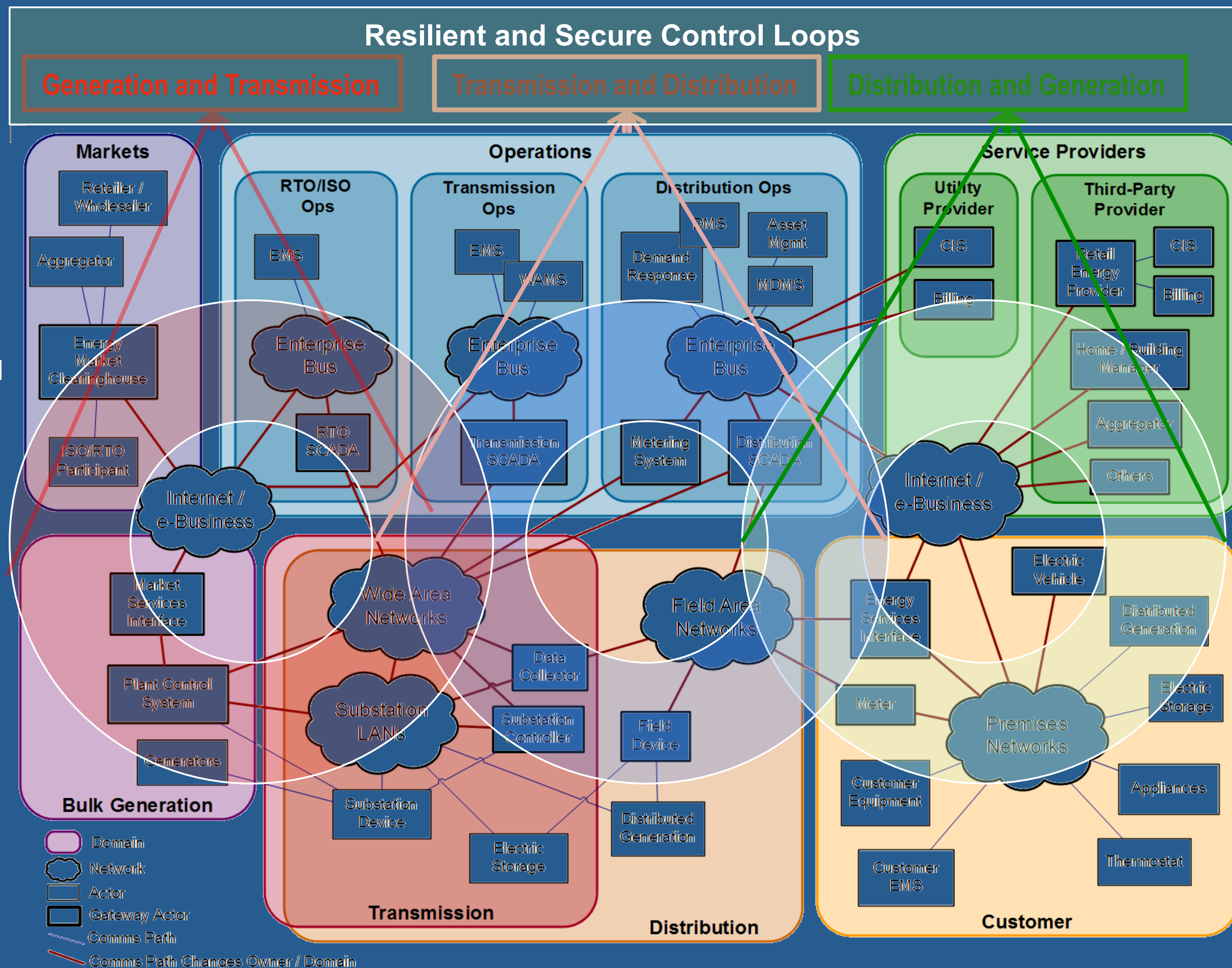
Cross Cutting Issues

- Large-scale, rapid propagation of effects
- Need for adaptive operation
- Need to have confidence in trustworthiness of resulting approach

- Need to create secure and reliable computing base
- Support large # of devices
- Timeliness, security, and reliability required of data and control information

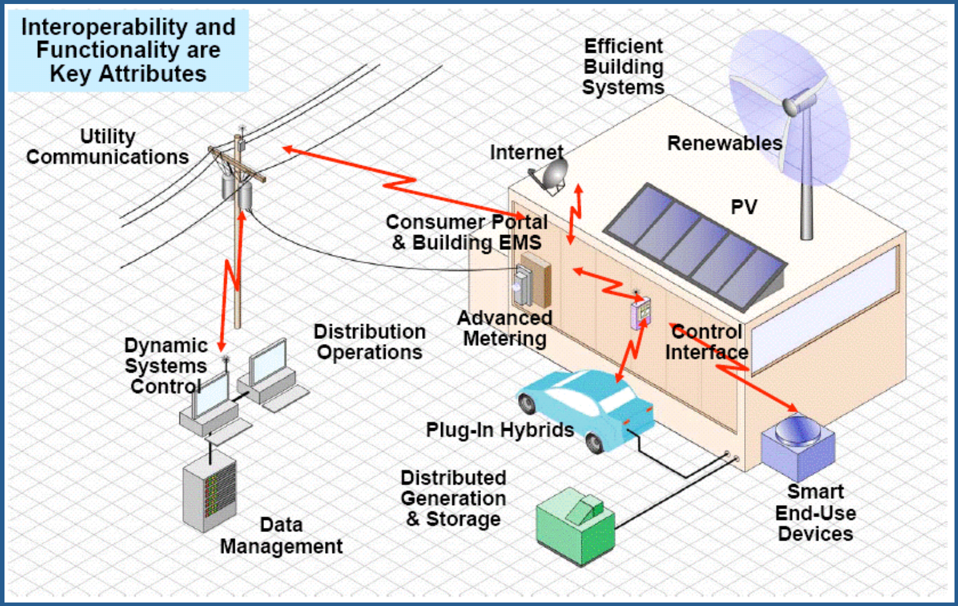
Infrastructure must provide control at multiple levels

- ✧**Multi-layer Control Loops**
- ✧*Multi-domain Control Loops*
  - ✧ Demand Response
  - ✧ Wide-area Real-time control
  - ✧ Distributed Electric Storage
  - ✧ Distributed Generation
- ✧ *Intra-domain Control Loops*
  - ✧ Home controls for smart heating, cooling, appliances
  - ✧ Home controls for distributed generation
  - ✧ Utility distribution Automation
- ✧ **Resilient and Secure Control**
  - ✧ *Secure and real-time communication substrate*
  - ✧ Integrity, authentication, confidentiality
  - ✧ Trust and key management
  - ✧ End-to-end Quality of Service
  - ✧ *Automated attack response systems*
  - ✧ *Risk and security assessment*
  - ✧ Model-based, quantitative validation tools



Note: the underlying Smart Grid Architecture has been developed by EPRI/NIST.

The Power Grid of Tomorrow: Smart Control of Electrical Equipment and an Open Grid



Consumer Portal:

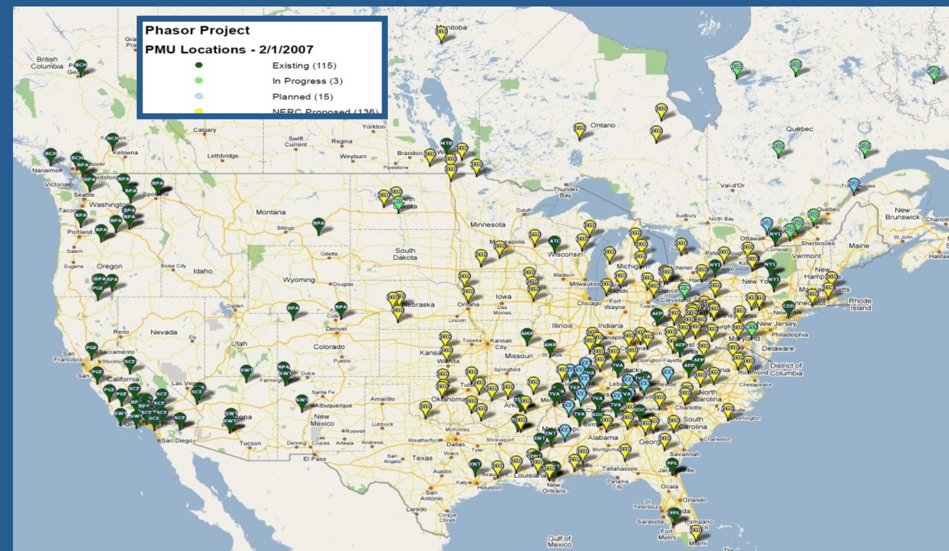
- Security issues are huge
  - Privacy, Billing integrity, Mischief, vandalism, intrusion, Consumer manipulation of system
- Customer education
  - Understanding impact of choices, Home user technical abilities, Home user security knowledge

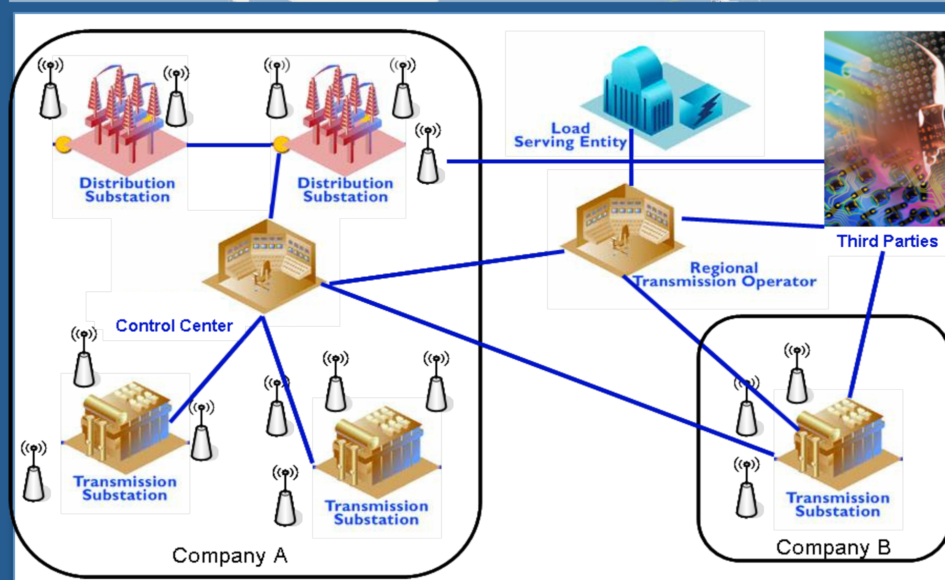
Who is responsible for security?

- Consumer? Utility?
  - Who would accept responsibility?
- Will be decided by regulators
  - Political decision, but may be influenced by technology

Power Grid of Tomorrow: North American SynchroPhasor Initiative

- Initiative, funded by DOE and industry, to investigate putting Phasor Measurement Units (PMUs) throughout physical power infrastructure
- Need significant changes in power cyber infrastructure to support PMUs.
- “Class A” service requires low latency, data integrity & availability (“no gaps”)





Trustworthiness through Cyber-Physical Resiliency

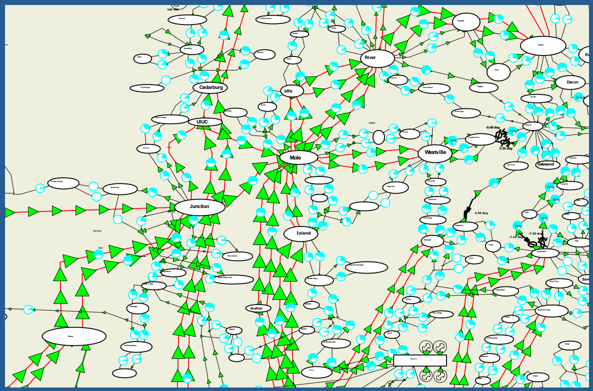
- Physical infrastructure has been engineered for resiliency ("n-1"), *but*
- Cyber infrastructure must also be made resilient:
  - Protect the best you can (using classical cyber security methods optimized for grid characteristics), but
  - Detect and Respond when intrusions succeed
- *Resiliency of overall infrastructure dependent on both cyber and physical components*
- Approaches must be developed that make use of sound mathematical techniques whose quality can be proven (need a *science* of cyber-physical resilience)

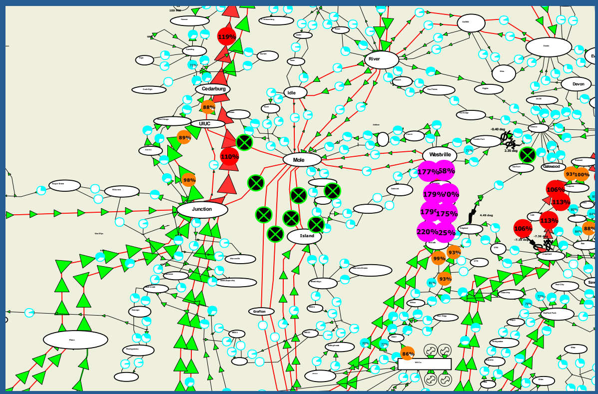
Outline

- A Quick Primer on the Modern Electric Grid
- Vulnerabilities and Threats
- Challenges to Achieving Trustworthy Operation
- TCIPG's Research Mission and Results

Vulnerabilities in Current Power Systems

- Systems are designed to be robust in the face of single failures but are at risk for certain kinds of multiple failures
  - While secure against single points of failure, analysis may reveal combinations of faults that would have severe consequences
- The tools to find such combinations are not difficult to construct
- In a couple hours, using a commercially available Power simulator, and publicly available power flow data, TCIP researchers found a small set of breakers who’s tripping would lead to a blackout almost the scale of the August 2003 blackout





Classical (Physical) Attack Approaches

- Physical attacks on lines, buses and other equipment can also be effective:
  - "low tech" attacks may be easy, and are also difficult to defend against
  - Requires physical proximity of attacker
  - Particularly effective if multiple facilities are attacked in a coordinated manner
- But coordination may be much easier in a cyber attack

J.D. Konopka (a.k.a. Dr. Chaos) Alleged to have caused $800K in damage in disrupting power in 13 Wisconsin counties, directing teenaged accomplices to throw barbed wire into power stations. (From Milwaukee Journal Sentinel) http://www.jsonline.com/news/Metro/may02/41693.asp

Intelligent Electronic Devices

- Intelligent Electronic Devices (IEDs) monitor and control devices, relays, and breakers
- IEDs may be subject to cyber tampering given access to the substation network and knowledge of a password.
  - Publicly accessible information contains the default passwords for some IEDs

PASSWORD Shows or sets passwords. Command pulses ALARM contacts closed momentarily after password entry. PAS 1 OTTER sets Level 1 password to OTTER. PAS 2 TAIL sets Level 2 password to TAIL.

- Attacks on multiple grid locations, whether physical or cyber, would need to be well synchronized to be effective (<10 minutes)

Potential Cyber Attack Strategies

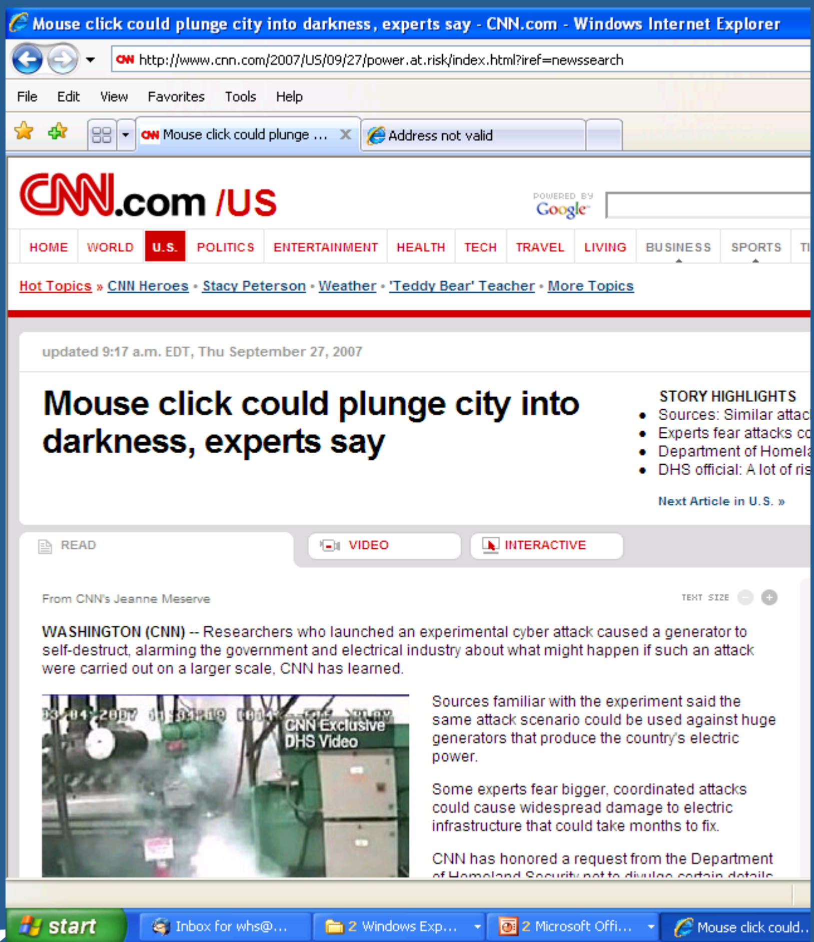
- Tripping Breakers
- Changing Values Breaker Settings
  - Lower settings can destabilize a system by inducing a large number of false trips
  - Lowering trip settings can cause extraneous other breakers, causing overloading of other transmission lines and/or loss of system stability
- Fuzzing of Power System Components
- Life Cycle Attacks
- Insider Threats

Combined Cyber-Physical Attack

- The physical element could be aimed at destabilizing the system and inflicting some lasting damage
- The cyber element could:
  - Focus on blinding the operator to the true nature of the problem, inhibiting defensive responses, and spreading the extent of an outage
  - Be the cause of the physical damage
    - INL Generator Demonstration
    - Stuxnet computer worm

Potential for Long-Term (Physical) Damage

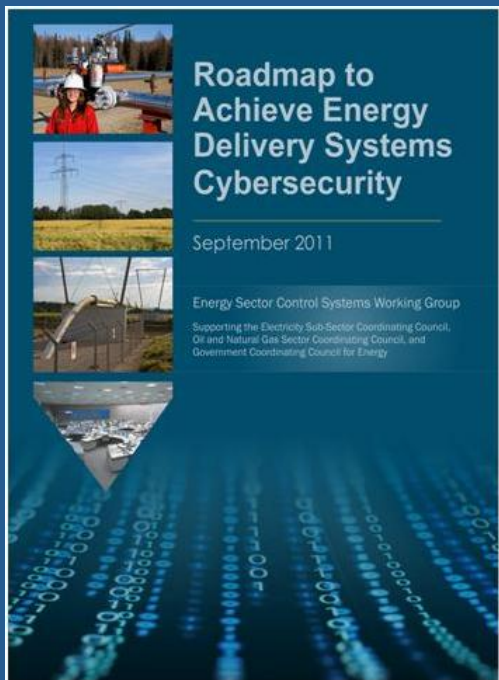
- Unclear how likely it could be achieved in practice, but researchers at Idaho National Labs have shown physical damage by cyber means



Outline

- A Quick Primer on the Modern Electric Grid
- Vulnerabilities and Threats
- Challenges to Achieving Trustworthy Operation
- TCIPG's Research Mission and Research Results

Roadmap – A Framework for Public-Private Collaboration



- Published in January 2006/updated 2011
- *Energy Sector's* synthesis of critical control system security challenges, R&D needs, and implementation milestones
- Provides strategic framework to
  - align activities to sector needs
  - coordinate public and private programs
  - stimulate investments in control systems security

Roadmap Vision

By 2020, resilient energy delivery systems are designed, installed, operated, and maintained to survive a cyber incident while sustaining critical functions.

American Recovery and Reinvestment Act of 2009

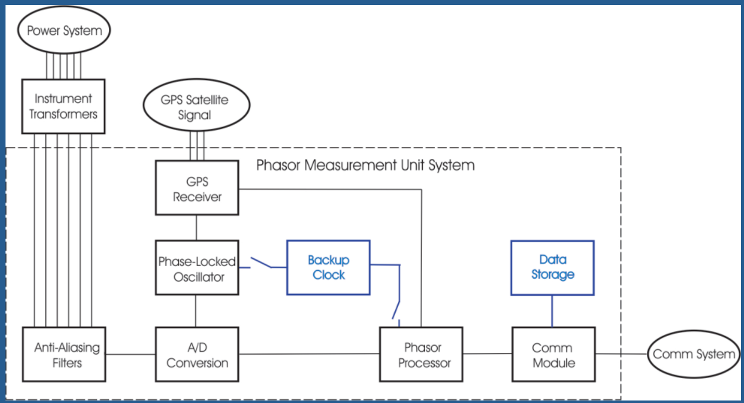
- DOE-OE ($4.5B)
  - Smart Grid Investment Grants ($3400M)
  - Smart Grid Demonstrations ($615M)
  - State Electricity Regulators Assistance ($46M)
  - Enhancing State Government Energy Assurance Capabilities and Planning for Smart Grid Resiliency ($39.5M)
  - Local Energy Assurance Planning Initiative ($10.5M)
  - Resource Assessment and Interconnection-Level Transmission Analysis and Planning ($60 M)
  - Workforce Training for the Electric Power Sector ($100M)

Summary of Smart Grid Investment Grant Awards

Topic Area	Number of Applications Selected/ Conforming	Federal Funding ($)	Applicant Funding ($)	Applicant Cost Share (%)
Equipment Manufacturing	2/14	25,786,501	25,807,502	50.02
Customer Systems	5/27	32,402,210	34,933,413	51.88
Advanced Metering Infrastructure	31/138	818,245,749	1,194,272,137	59.34
Electric Distribution	13/39	254,260,753	254,738,977	50.05
Electric Transmission	10/28	147,990,985	150,454,793	50.41
Integrated and Crosscutting	39/143	2,150,505,323	3,082,366,420	59.09
Total	100/389	3,429,191,521	4,742,573,246	58.04

Challenge 1: Trustworthy technologies for wide-area monitoring and control

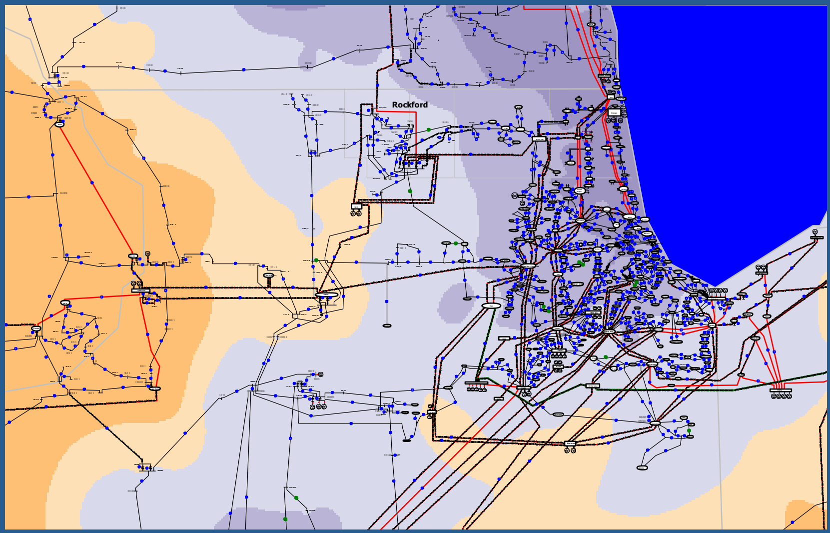
- Smart Grid vision for the wide area (primarily transmission) is:
  - Vastly more sensing at high, synchronous rates (example: PMUs)
  - New applications that use these data to improve
    - Reliability
    - Efficiency
    - Ability to integrate renewables



- Achieving the vision requires secure and reliable communications between sensors, control devices, and monitoring and control applications all owned and operated by the many entities that make up the grid

Challenge 1 Problem Areas

- Smart grid technologies bring new vulnerabilities along with benefits
  - Need improvements in security of wide-area communication technologies
  - Need ways to understand and mitigate the impacts of vulnerabilities

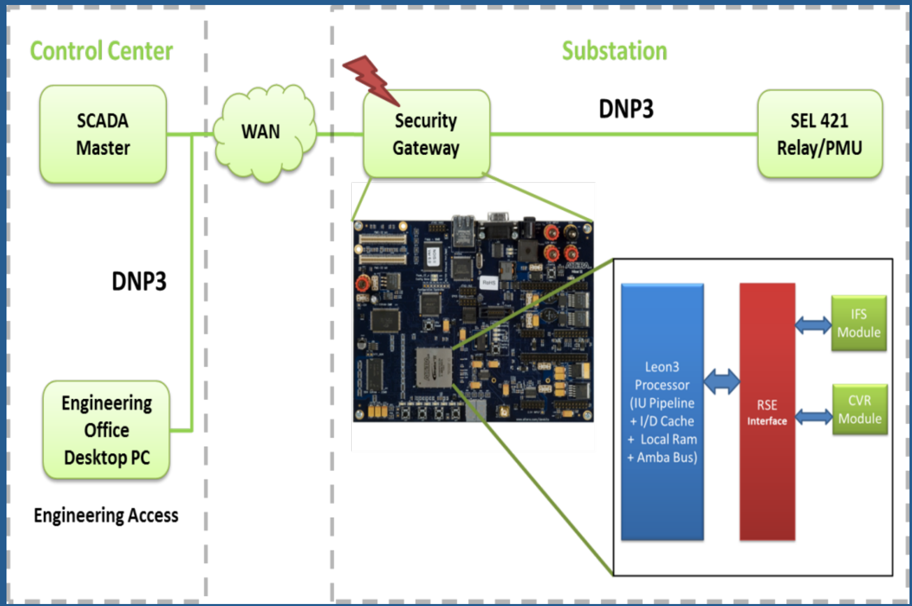


- What data delivery infrastructure design will provide the *integrity*, *confidentiality, availability*, and *real-time performance* needed for wide-area smart grid operations?

Challenge Area 1 Problem Areas, cont'd

- What is the relationship between security (or lack of security) of communications for wide-area monitoring and control and the power-system's behavior?

- What kinds of hardware and software components will provide a better foundation on which to build the wide-area monitoring and control infrastructure?



Specific Area 1 Research Challenges

- Secure wide-area data and communication networks for PMU-based power system applications
  – Hierarchical gateway-based architecture
- Cooperative congestion avoidance and end-to-end real-time scheduling to achieve real time information delivery
- Real-time, secure, and converged power grid cyber-physical networks
- Algorithm-based intrusion-tolerant energy applications

Challenge 2: Trustworthy technologies for local area management, monitoring, and control

- Electric grid can be divided into three groups: the generation, the wires (T&D), and the demand. This challenge focuses on the demand and the nearby distribution
  - Generation must track load

- For a grid with more renewable, but less controllable generation (e.g., wind and solar PV), more load control will be needed
  - Distributed generation may be embedded in "demand"
  - New loads (electric vehicles) could drastically change demand profile

Motivation: PV Output Variation with Clouds

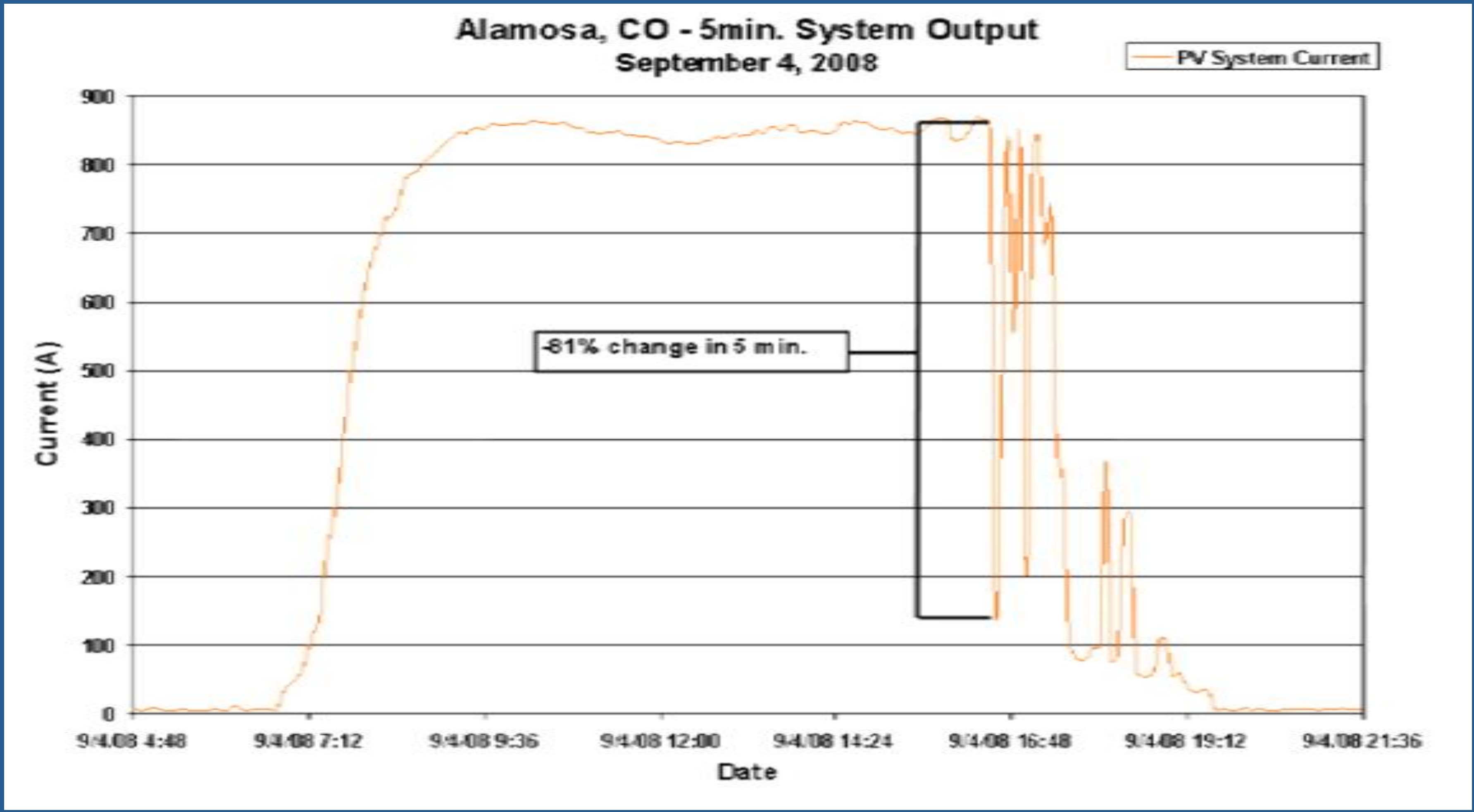
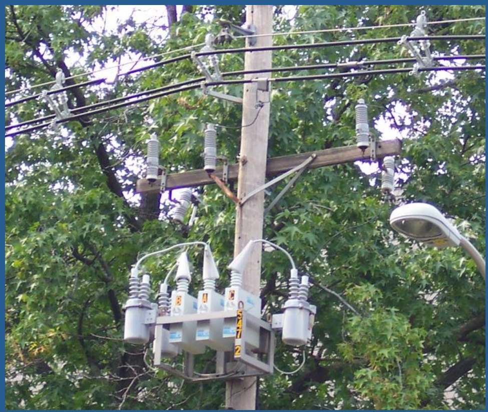


Image Source: Secretary Chu, "Investing in our Energy Future" GridWeek Presentation, Sept. 21, 2009

Challenge 2 Problem Areas

- This challenge focuses on making the demand more known and/or controllable
- Must address many of the Smart Grid core issues

  - Great advances over years in generation and T&D, but end user has been mostly left out
  - Customers require targeted information to help them optimize their electricity usage
  - Making a smarter distribution system and more "active" load could greatly enhance system operations and control, but adds cyber issues



Specific Area 2 Research Challenges

- Cyber-Enabled management of distribution (physical) infrastructure
  - Smart-grid-enabled distributed voltage support
  - Agent technologies for active control applications in the grid
- Trustworthy integration of new distribution side technologies, e.g., vehicle-to-grid (V2G)
- Non-intrusive, privacy-preserving, practical demand-response management

Challenge 3: Responding to and managing cyber events

- Combined cyber and physical attack detection, response to detected attacks, and recovery from attack consequences is essential to providing resilience
- Existing detection and response methods are *ad hoc*, at best, and rely on assumptions that may not hold
- Aim to detect and respond to cyber and physical events, providing resilience to partially successful attacks that may occur:
  - Making use of cyber and physical state information to detect attacks
  - Determine appropriate response actions in order to maintain continuous operation
  - Minimize recovery time when disruptions do occur

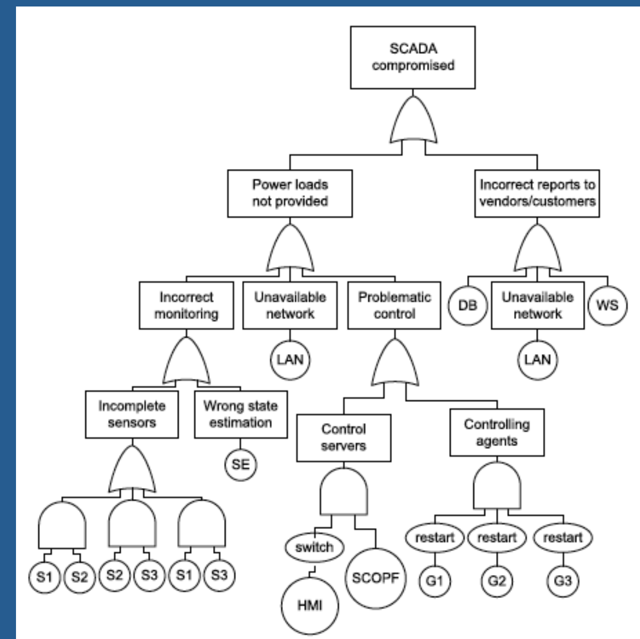
Challenge 3 Scope

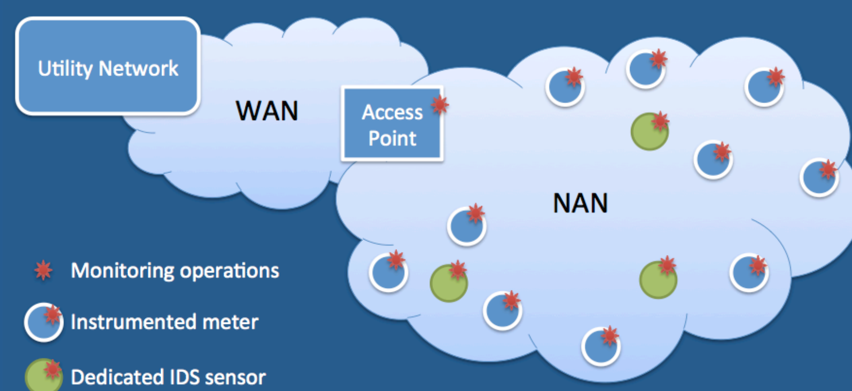
- Sensors
  - Monitor both physical and cyber state
  - Make use of application characteristics improve sensing
- Actuators
  - Not just in generation, transmission, and distribution, but in every outlet, car, parking garage, DER
- Response algorithms and engines that are:
  - Have provable bounds on the quality of decisions that they recommend
  - Cannot cause harm in the hands of an adversary
  - Are scalable (and almost surely) hierarchical
  - Are wide in their end-to-end scope

Challenge 3 Problem Areas

Create complete detection, response, and recovery environment, at all necessary levels of abstraction:

- Physical level
  - Taking into account noise and malicious manipulation of values
- Hardware level
  - Respecting embedded and cost sensitive nature of power system components
- OS / Platform level
  - Dealing with lack of source code other observability limitations
- Computer network level
  - Accommodating observability limitations due to encryption and protocols



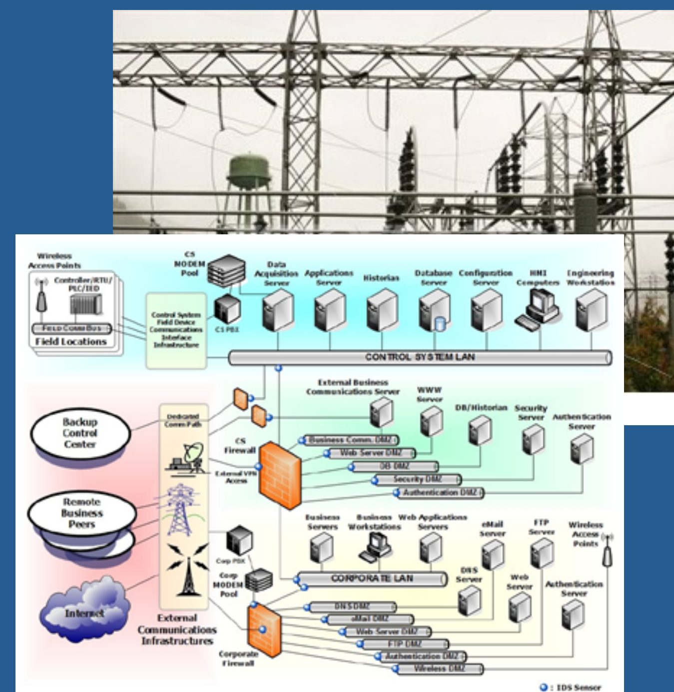


Challenge 4: Trust and Risk Assessment

- Define appropriate security metrics
  - Integrated at multiple levels
  - Applied throughout system lifecycle
  - Be both “process” and “product” oriented
- Determine methods for estimating metrics
  - To choose appropriate architectural configuration
  - To test implementation flaws, e.g., fuzzing, firewall rule analysis
  - Can be applied in cost effective manner *before* an audit
- Which link technical and business concerns

Example Challenge 4 Research Topics

- 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



Outline

- A Quick Primer of the Modern Electric Grid
- Vulnerabilities and Threats
- Challenges to Achieving Trustworthy Operation
- TCIPG's Research Mission and Results

TCIPG Vision & Research Focus

Vision: Drive the design of an adaptive, resilient, and trustworthy cyber infrastructure for transmission & distribution of electric power, which operates through attacks

Research focus: Resilient and Secure Smart Grid Systems

- Protecting the cyber infrastructure
- Making use of cyber and physical state information to detect, respond, and recover from attacks
- Supporting greatly increased throughput and timeliness requirements for next generation energy applications
- Quantifying security and resilience

TCIPG Statistics

- Builds upon $7.5M NSF TCIP CyberTrust Center 2005-2010
- $18.8M over 5 years, starting Oct 1, 2009 (including 20% cost share from partner schools)
- Funded by Department of Energy, Office of Electricity and Department of Homeland Security
- 5 Universities
  - University of Illinois at Urbana-Champaign
  - Washington State University
  - University of California at Davis
  - Dartmouth College
  - Cornell University
- 20 Faculty, 20 Senior Technical Staff, 37 Graduate Students, 5 Undergraduate Students, and 1 Admin

Industry Interaction: Vendors and Utilities that have participated in TCIPG Events

Adventium Enterprises
archimatica
Alcatel·Lucent
ALSTOM
Ameren
at&t
Black & Veatch
Boeing
BT
Cisco
ComEd
Electric Power Group
DTE Energy
Emerging Threats Pro
Encari
Grid Protection Alliance
Entergy – The Power of People
Fujitsu
GE – imagination at work
General Dynamics – Strength On Your Side
GVEA – Golden Valley Electric Association
Harris
Honeywell
IBM
Integrated Architecture
intel
Itron
IXIA
JCE – JD Carroll Energy
Landis+Gyr
Lockheed Martin
Luminant
McAfee
Mehta Tech Inc.
nationalgrid – The Power of Action
n-dimension solutions
NiSource
Northrop Grumman
OSIsoft
OSI – opening your world
Patrick
PG&E
pjm
NIPSCO
Quanta Technology
SAIC – From Science to Solutions
SEL – Schweitzer Engineering Laboratories
Siemens
SISCO
PowerWorld Corporation
Space•Time•Insight
Symantec
Telcordia
Veracode
ViaSat
Westar Energy

Industry Interaction: Other organizations that have participated in TCIPG Events

Association of Illinois Electric Cooperatives
Your Touchstone Energy® Partner
CLEAN ENERGY TRUST
ENERGETICS
A Subsidiary of VSE Corporation
ETRI Electronics and Telecommunications Research Institute
Department of Energy – United States of America
U.S. Department of Homeland Security
EPRI ELECTRIC POWER RESEARCH INSTITUTE
EnergySec
National Electric Sector Cybersecurity Organization
FERC
ILLINOIS SCIENCE & TECHNOLOGY COALITION
Illinois VENTURES
IEIA FORUM
I3P
Institute for Information Infrastructure Protection
NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION
INL
Idaho National Laboratory
OAK RIDGE
National Laboratory
Pacific Northwest
NATIONAL LABORATORY
Sterne Kessler Goldstein Fox
ATTORNEYS AT LAW
UL
U.S. ARMY
THINK SMARTGRID
UtiliSec
Electric Utility Cyber Security

TCIPG Impacts all aspects of the *2011 Roadmap to Achieve Energy Delivery Systems Cybersecurity*

TCIPG Efforts

Build a Culture of Security

- Conduct summer schools for industry
- Develop K-12 power/cyber curriculum
- Develop public energy literacy
- Directly interact with industry
- Educate next-generation cyber-power aware workforce

Assess and Monitor Risk

- Analyze security of protocols (e.g. DNP3, Zigbee, ICCP, C12.22)
- Create tools for assessing security of devices, systems, & use cases
- Create integrated scalable cyber/ physical modeling infrastructure
- Distribute NetAPT for use by utilities and auditors
- Create fuzzing tools for SCADA protocols

Protective Measures/Risk Reduction

- Build secure, real-time, & flexible communication mechanisms for WAMS
- Design secure information layer for V2G
- Provide malicious power system data detection and protection
- Participate in industry-led CEDS projects

Manage Incidents

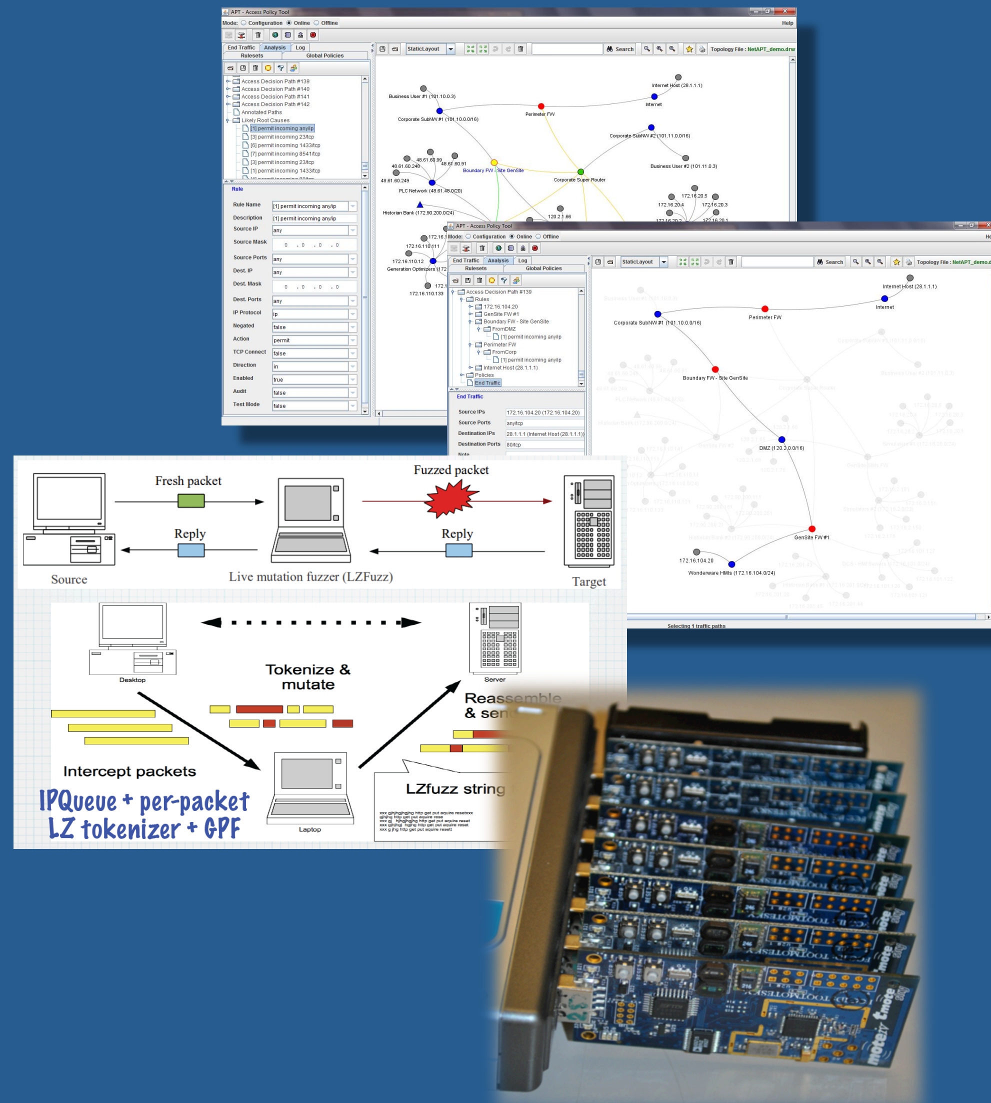
- Build game-theoretic Response and recovery engine
- Develop forensic data analysis to support response
- Create effective Intrusion detection approach for AMI

Sustain Security Improvements

- Offer Testbed and Expertise as a Service to Industry
- Anticipate/address issues of scale: PKI, data avalanche, PMU data compression
- Act as repository for cyber-security-related power system data

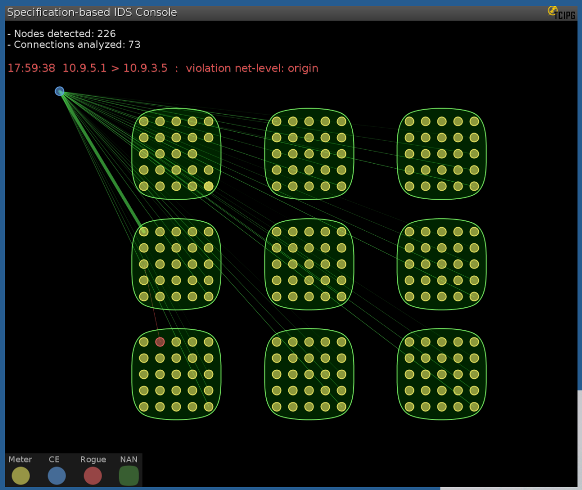
Selected TCIPG Activities: Practical Vulnerability Assessment Tools for Industry

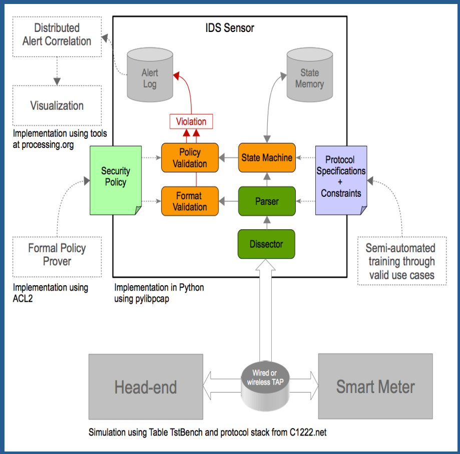
- NetAPT
  - In evaluation by SERC as an audit tool
  - Used in pilot assessments by utilities
- LZ-Fuzz has been used in a power environment to test ICCP connections
- Api-DO ZigBee Self-assessment framework
  - More than 50% of KillerBee code base is now contributed by TCIPG Dartmouth team

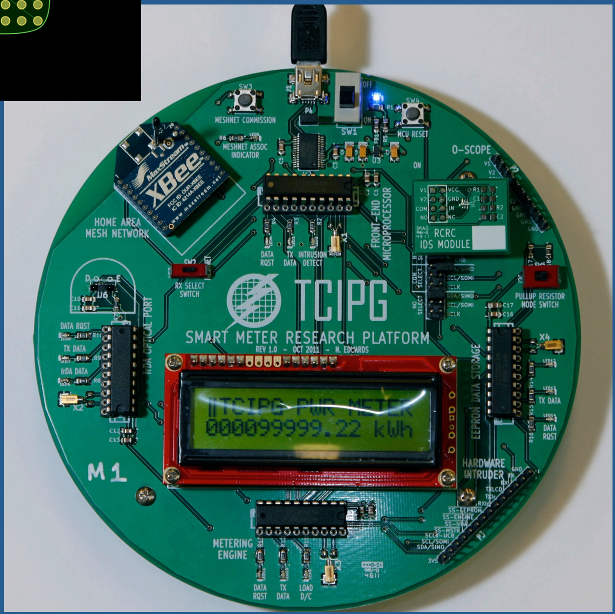


Selected TCIPG Activities: Embedded System and AMI Security

- Autoscopy Jr.: Lightweight kernel-based intrusion detection system
  - Ongoing Discussions with SE
- Specification-based IDS for AMI
  - Discussions with Itron, Fujitsu, EPRI
- Hardware-based IDS for meters
  - Signal-level IDS detects meter tampering
- Security specification development and review for industry

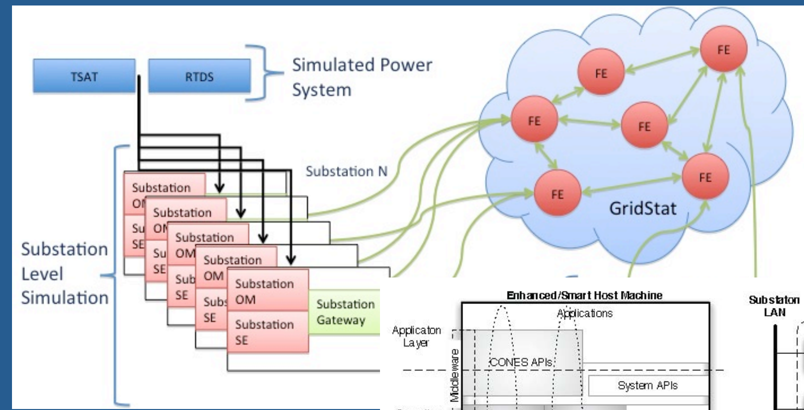


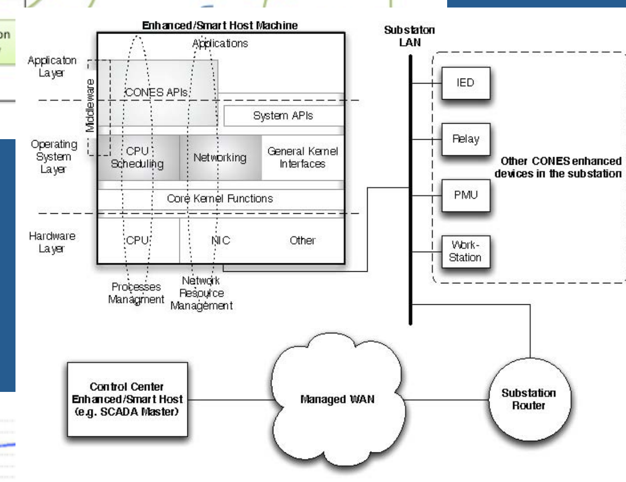


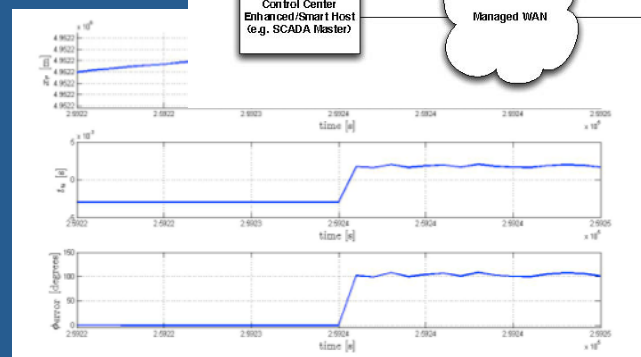


Selected TCIPG Activities: Efforts to Secure Wide-Area Measurement Infrastructures

- GridStat Secure Middleware Communication Framework
  - Used in test with INL
- CONES: Converged Networks for SCADA
  - Algorithms formed basis of DOE-funded SIEGate (System Information Gateway) appliance
- Analysis of GPS spoofing attacks against PMU synchronization
  - Demonstrated, using MatLab simulation, spoofing attack on GPS







4 Satellite spoofing

To Learn More

- www.tcipg.org
- Bill Sanders whs@illinois.edu

- Request to be on our mailing list
- Attend Monthly Public Webinars
- Attend our Industry/Govt. workshop Oct. 30-31, 2012