TCIP: Trustworthy Cyber Infrastructure for Power

William H. Sanders

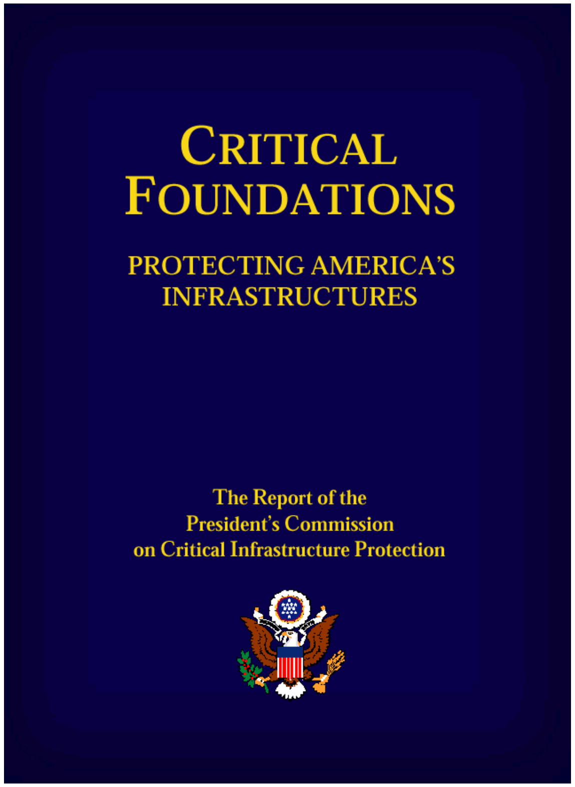
Information Trust Institute
University of Illinois at Urbana-Champaign

for the TCIP Project Team

The Nation’s Power Cyber Infrastructure is at Risk

1997:

- “The widespread and increasing use of SCADA systems for control of energy systems provides increasing ability to cause serious damage and disruption by cyber means”



CRITICAL FOUNDATIONS

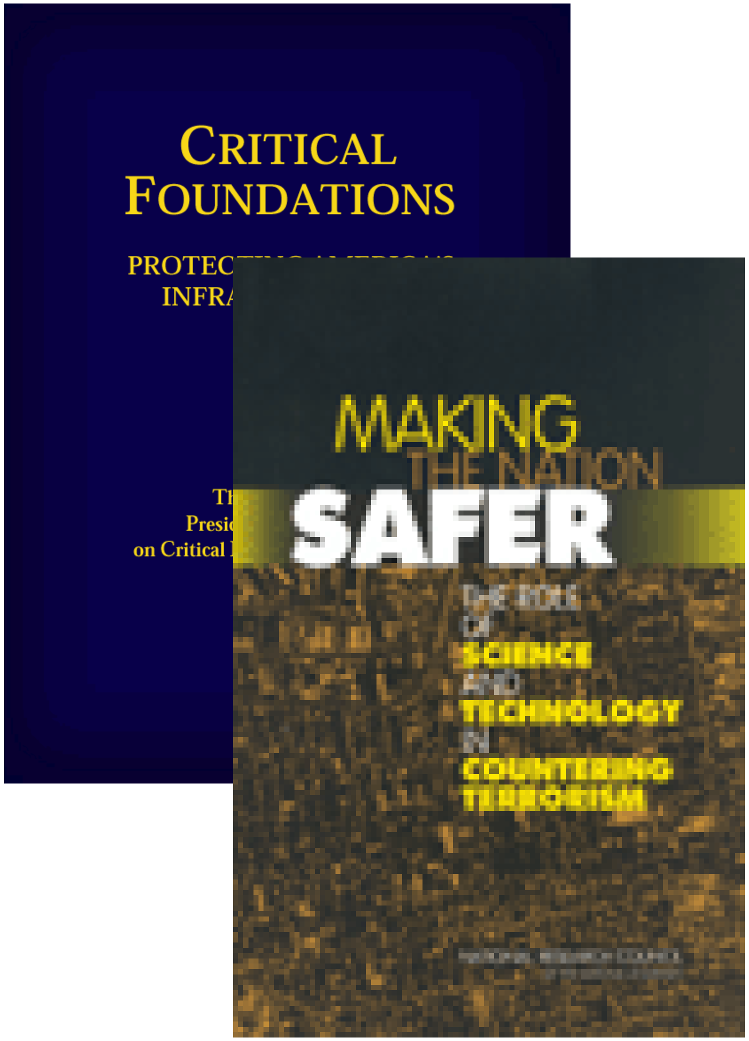
PROTECTING AMERICA’S INFRASTRUCTURES

The Report of the
President’s Commission
on Critical Infrastructure Protection

The Nation's Power Cyber Infrastructure is at Risk

2002:

- "Simultaneous attacks on a few critical components of the grid could result in a widespread and extended blackout."
- "Conceivably, they could also cause the grid to collapse, with cascading failures in equipment far from the attacks, leading to an even larger, longer-term blackout."



CRITICAL FOUNDATIONS

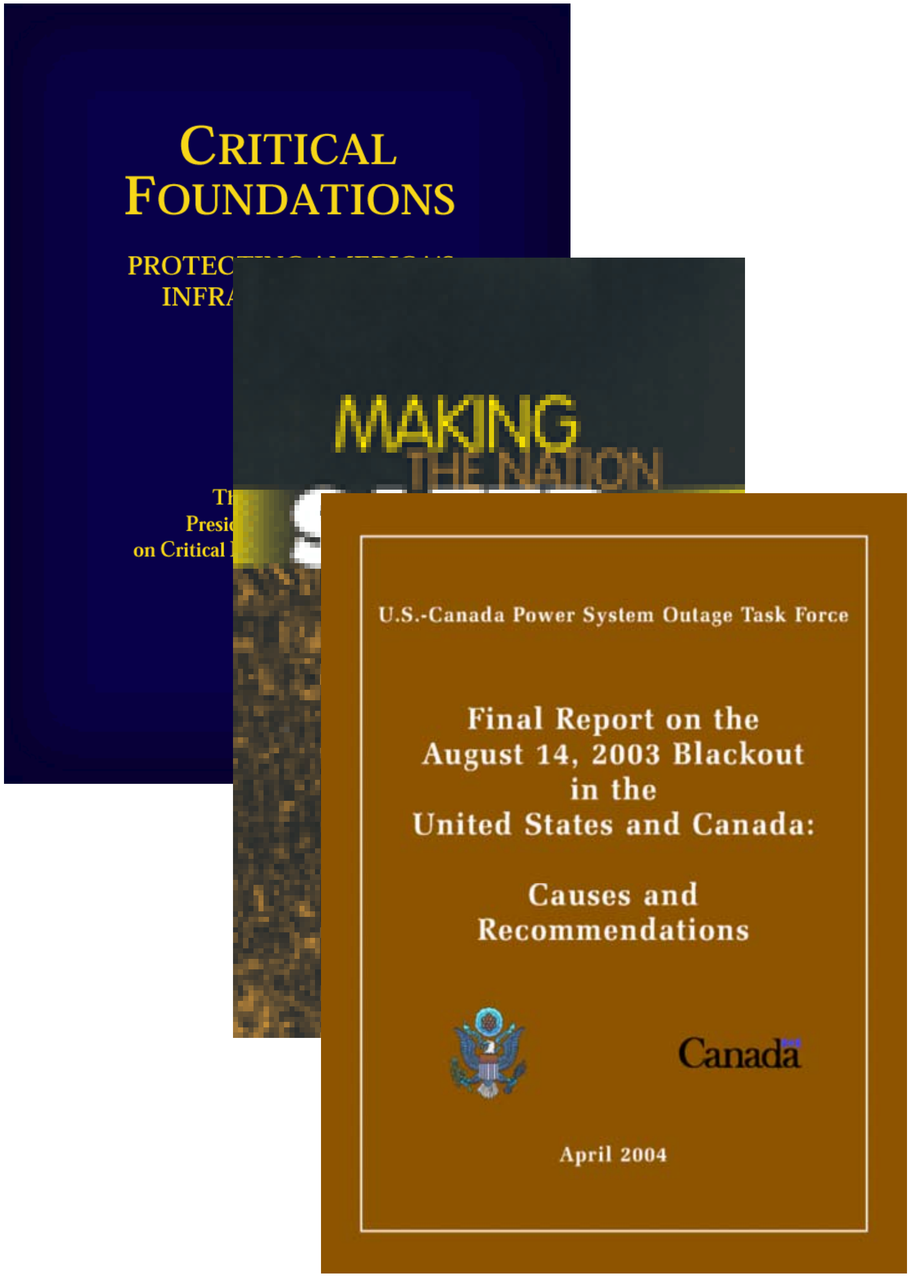
MAKING THE NATION SAFER

THE ROLE OF SCIENCE AND TECHNOLOGY IN COUNTERING TERRORISM

The Nation's Power Cyber Infrastructure is at Risk

2004:

- "A failure in a software program not linked to malicious activity may have significantly contributed to the power outage."
- "Control and Data Acquisition (SCADA) networks to other systems introduced vulnerabilities."
- "In some cases, Control Area (CA) and Reliability Coordinator (RC) visibility into the operations of surrounding areas was lacking."



U.S.-Canada Power System Outage Task Force

Final Report on the
August 14, 2003 Blackout
in the
United States and Canada:

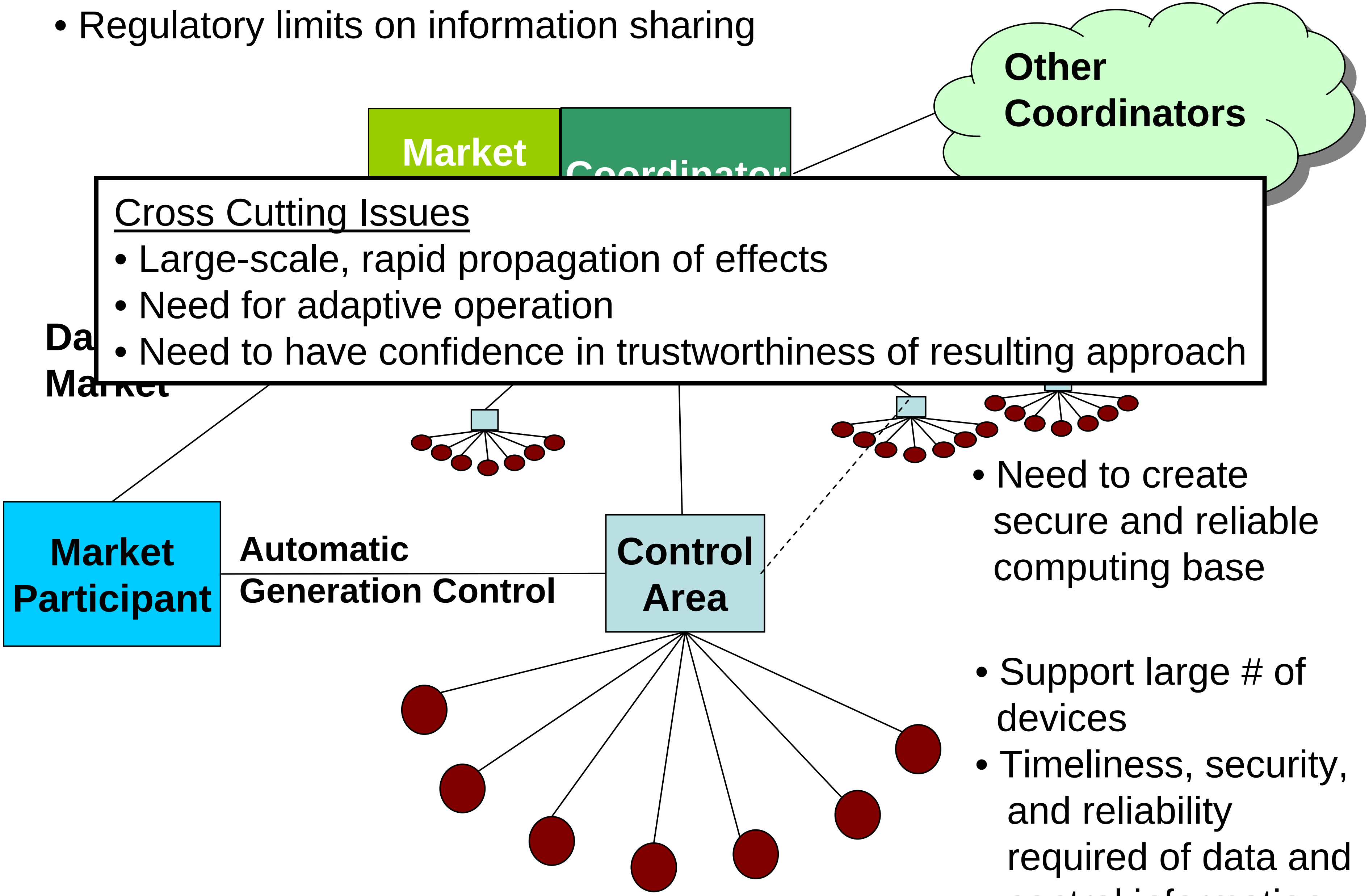
Causes and
Recommendations

Canada

April 2004

Next-Generation Power Grid Cyber Infrastructure Challenges

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



Other Coordinators

Market

Coordinator

Da

Market

Market Participant

Automatic Generation Control

Control Area

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

TCIP: Trustworthy Cyber Infrastructure for Power

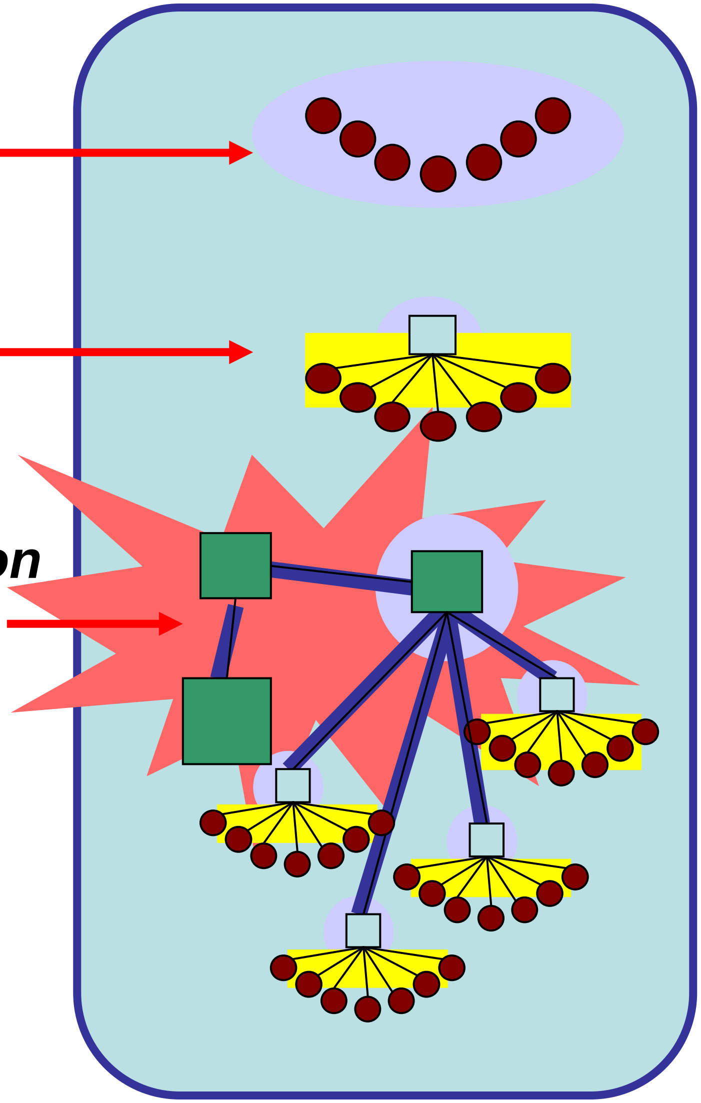
Address technical challenges motivated by power grid problems in

By developing

Ubiquitous exposed infrastructure

Real-time data monitoring and control

Wide area information coordination and information sharing



Secure and Reliable Computing Base

Trustworthy Communication & Control Protocols

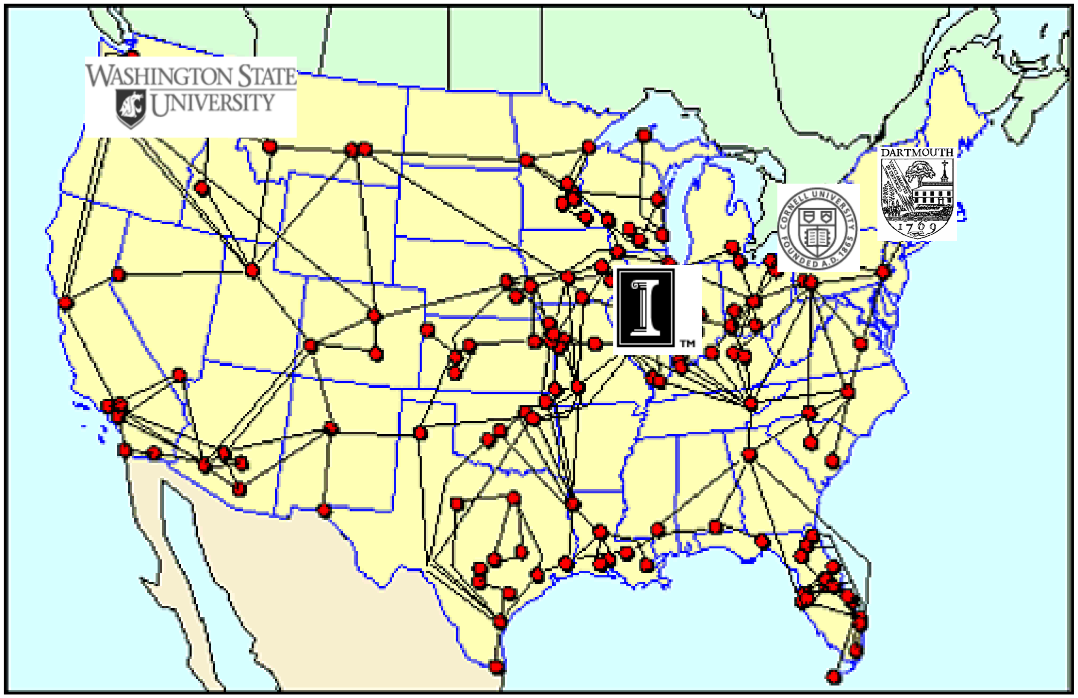
Quantitative & Qualitative Evaluation

Education

tcip.iti.uiuc.edu

TCIP Senior Investigators

- Secure & Reliable Base
  - Gross, Gunter, Iyer, Kalbarczyk, Sauer, and Smith
- Trustworthy Communication & Control Protocols
  - Bakken, Bose, Courtney, Fleury, Hauser, Khurana, Minami, Nahrstedt, Sanders, Scaglione, Welch, Winslett
- Quantitative & Qualitative Evaluation
  - Anderson, Campbell, Nicol, Overbye, Ranganathan, Thomas, Wang, Zimmerman
- Education
  - Kalbarczyk, Overbye, Reese, Sebestik, Tracy


WASHINGTON STATE UNIVERSITY
DARTMOUTH
1769
CORNELL UNIVERSITY FOUNDED A.D. 1865
I
TM

- Partner Institutions
  - Cornell
  - Dartmouth
  - University of Illinois
  - Washington State University

TCIP Graduate and Undergraduate Researchers

Graduate Students:

- Stian Abelsen (WSU)
- Angel Aquino-Lugo (UIUC)
- John Kwang-Hyun Baek* (Dartmouth)
- Scott Bai (UIUC)
- Nihal D’Cunha* (Dartmouth)
- Matt Davis (UIUC)
- Reza Farivar (UIUC)
- Chris Grier (UIUC)
- Joel Helkey (WSU)
- Alex Iliev* (Dartmouth)
- Sundeep Reddy Katasani (UIUC)
- Shrut Kirti (Cornell)
- Peter Klemperer (UIUC)
- Jim Kusznir (WSU)
- Adam Lee* (UIUC)
- Michael LeMay* (UIUC)
- Sunil Murthuswamy (WSU)
- Suvda Myagmar (UIUC)
- Hoang Nguyen (UIUC)
- Hamed Okhravi* (UIUC)
- Karthik Pattabiraman* (UIUC)
- Sankalp Singh* (UIUC)
- Erik Solum (WSU)
- Kim Swenson (WSU)
- Zeb Tate (UIUC)
- Patrick Tsang (Dartmouth)
- Erlend Viddal (WSU)
- Jianqing Zhang (UIUC)

Undergraduates:

- Katy Coles* (UIUC)
- Paul Dabrowski* (UIUC)
- Sanjam Garg (UIUC)
- Steve Hanna* (UIUC)
- Loren Hoffman (WSU)
- Allen G. Harvey, Jr.* (Dartmouth)
- Nathan Schubkegel (WSU)
- Evan Sparks* (Dartmouth)
- Erik Yeats* (WSU)

* Not funded by TCIP, but working on TCIP

Area 1 Approach

- ***Focus*****:** Move from ***perimeter security*** to ***platform security*** in the power grid cyber infrastructure

- ***Focus*****:** Secure power ***infrastructure by ensuring*** security of infrastructure ***applications***
  - Derive security ***requirements*** from ***application logic***
  - Derive ***hybrid solutions*** and ***constraints*** from application context
- ***Project Areas***:
  - Build ***new types of platforms*** to achieve specific security goals for power applications
  - Make these hardened platforms ***reconfigurable and customizable***, so one platform secures multiple power applications
  - Integrate hardened platforms into ***comprehensive security architectures*** for power grid scenarios

Trustworthy Communication & Control Protocols

The past

- Un-secure communication
- Slow communication links
- Lack of inclusion of networking and computing standard technologies

Trends

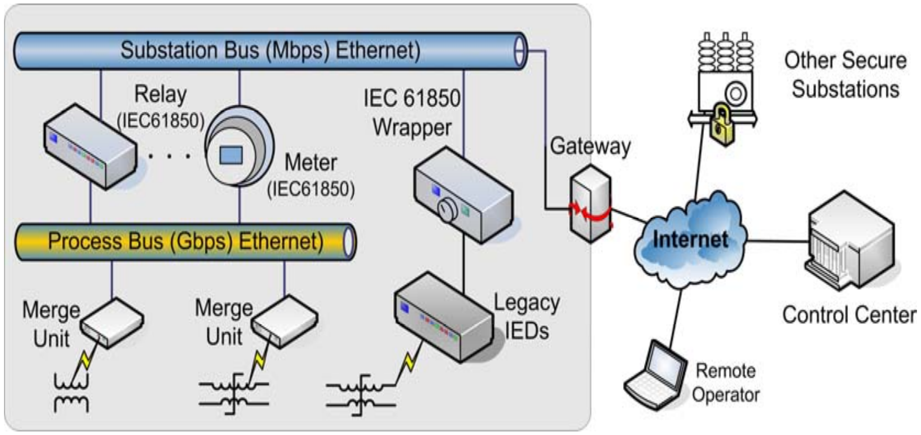
- Data collection at control areas
- High-speed wide area communication and computation solutions available (optical/SONET, multi-core devices, Linux)
- Standard wireless network technologies available
  - 802.11, 802.15, 802.16, Bluetooth
- IP-based protocol solutions available

Challenges

- End-to-end real-time, security, reliability, and QoS guarantees

Approach

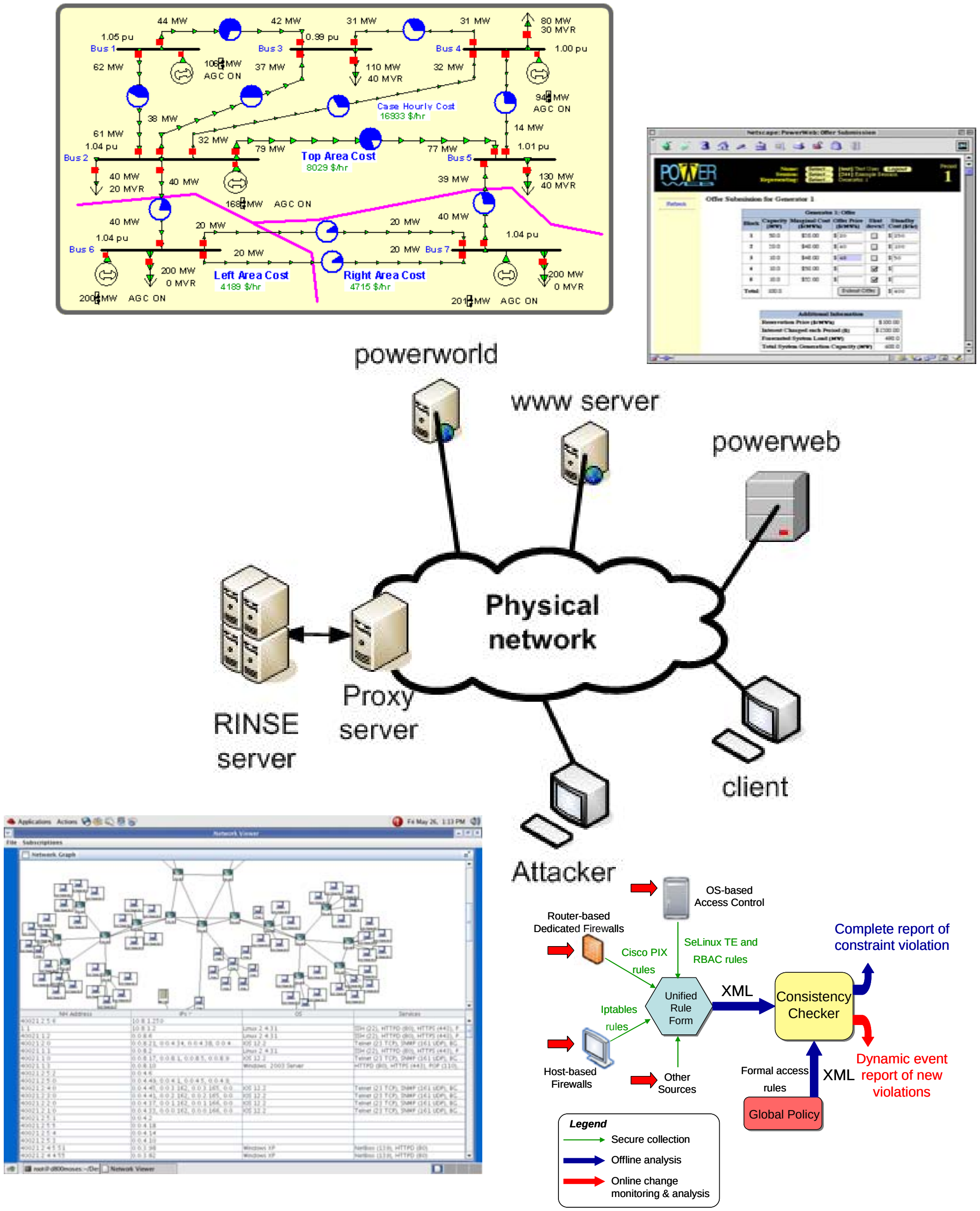
- Provision of real-time and reliable monitoring, detection, alert, and control solutions in case of perturbations, vulnerabilities and attacks
- Self-adaptation to new security needs due to long-lifetime installed base (RTUs)
- Handling of adversarial threats to end devices (IEDs), control centers, ISOs, and communication links among them



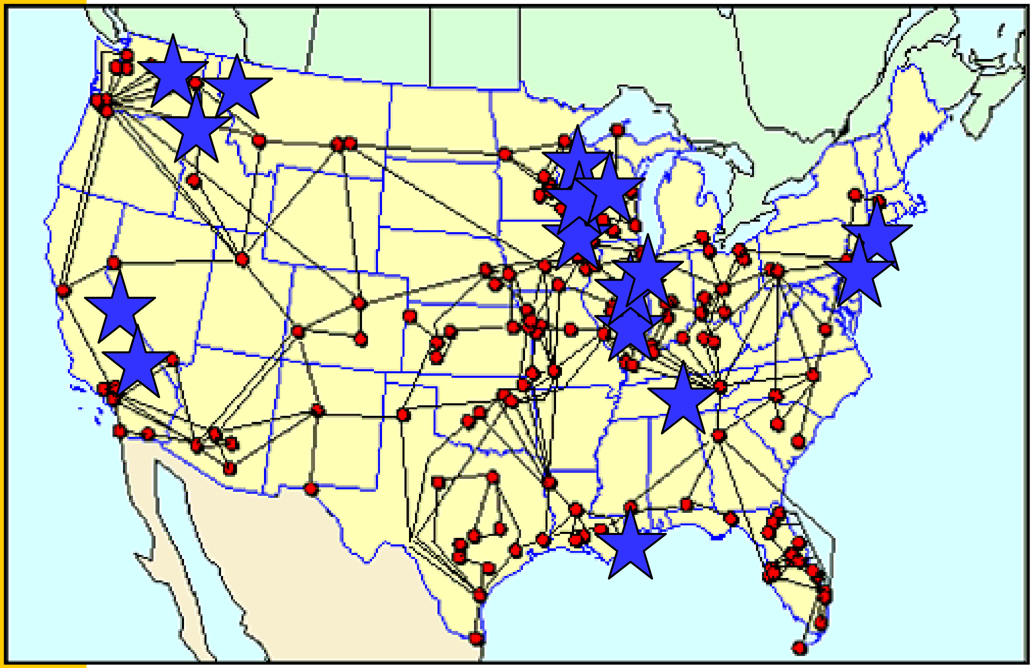
Quantitative & Qualitative Evaluation

Approach:

- Developing tools and methodologies for evaluating and validating next-generation power grid designs
- Developing tools and methodologies for evaluating existing system configurations with respect to best practice recommendations and global policies
- Studying the sensitivity of the power grid infrastructure to various kinds of cyber attacks



Industrial Partnerships – Spanning Stakeholders



Technology Providers/Researchers

ABB – Industrial manufacturer and supplier
Siemens – Industrial manufacturer and supplier
AREVA – Major SW vendor for utility EMS systems
Cisco Systems – CIP Researchers
Cyber Defense Agency – Security Assessment
EPRI – Electric Power Research Institute
GE Global Research – Research in communication and computing requirements for US power grid
Honeywell – Industrial control system provider and SCADA researcher
KEMA - Supports clients concerned with the supply and use of electrical power
OSII – Major SW vendor for utilities including SCADA and EMS systems
PNNL – National Lab doing SCADA research
PowerWorld Corp – System analysis and visualization tools
Sandia National Lab – SCADA research
Schweitzer – Industrial control system provider
Starthis – Automation Middleware

Electrical Power Generation, Delivery, and Management

Ameren – Major traditional utility in Mo. and IL
Entergy – Major traditional utility in South
Exelon – Major traditional Utility – Midwest & East
TVA – Largest public power company

CAISO – Independent system operator for CA
PJM – Regional transmission organization (RTO) for 7 states and D.C.

TCIP