TCIP: Trustworthy Cyber Infrastructure for Power

William H. Sanders

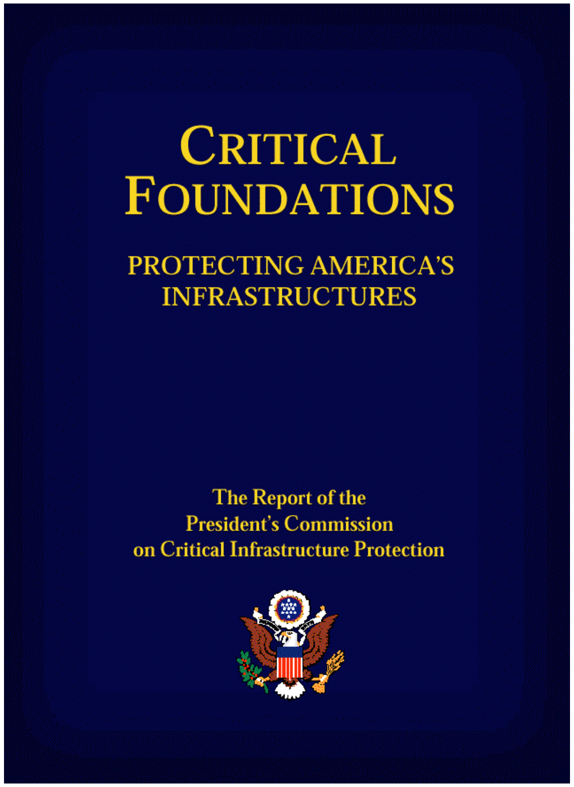
University of Illinois at Urbana-Champaign

IFIP 10.4 Winter Meeting, January 2006

The Nation's Power Cyber Infrastructure is at R

1997:

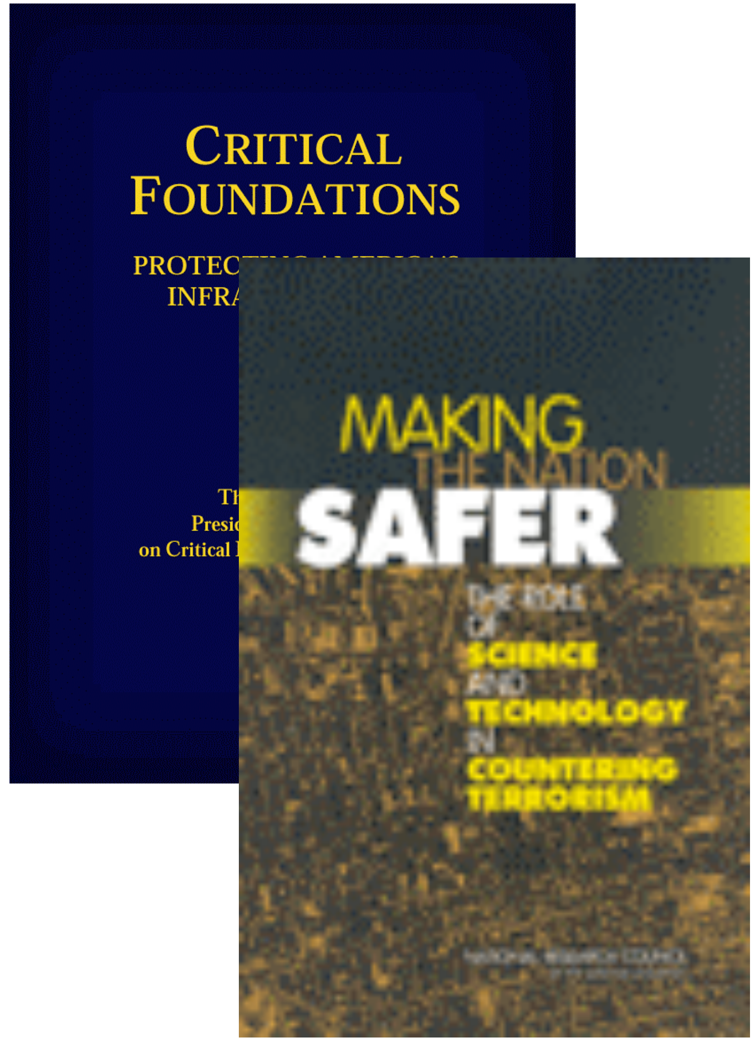
- "The widespread and increasing use of SCADA systems for control of energy systems provides increasing ability to cause serious damage and disruption by cyber means"



The Nation's Power Cyber Infrastructure is at R

2002:

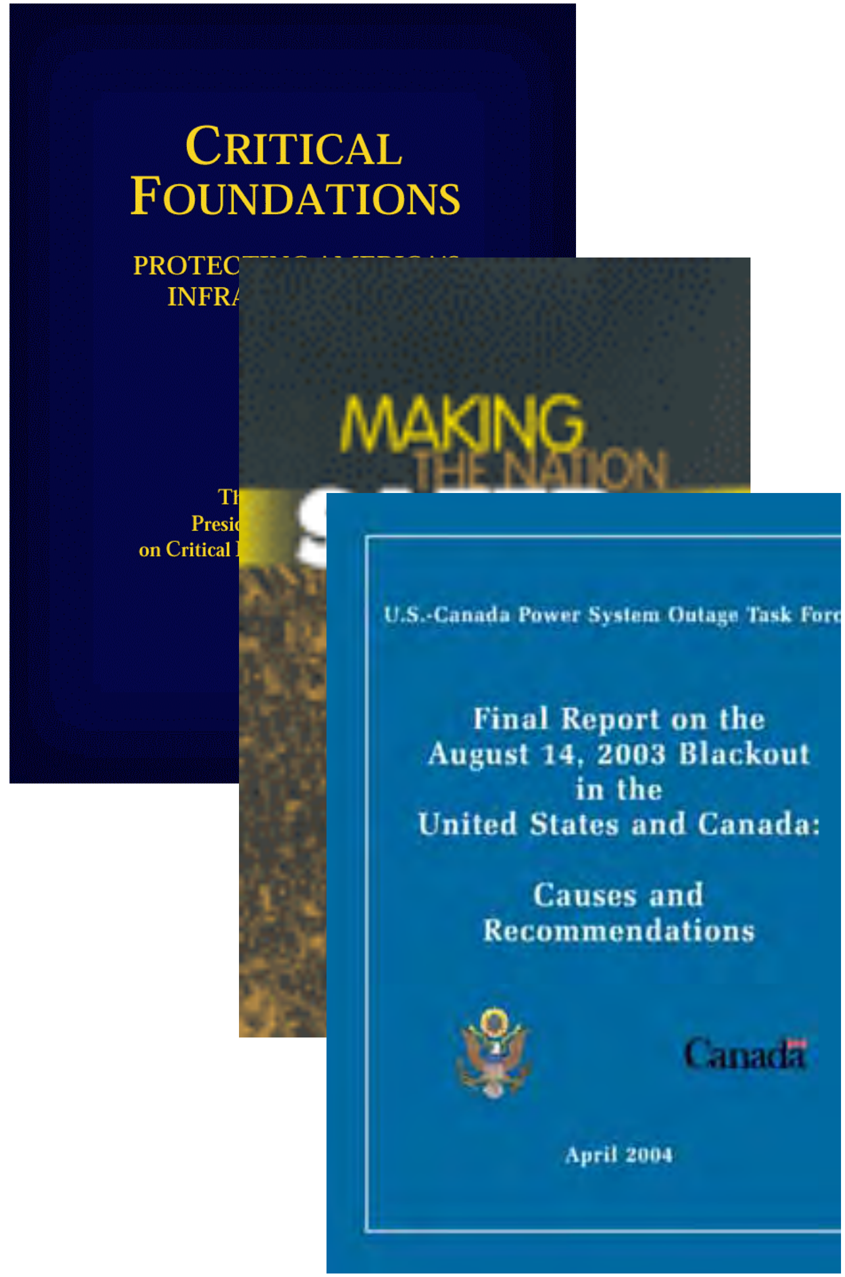
- "Simultaneous attacks on a few critical components of the grid could result in a widespread and extended blackout."
- "Conceivably, they could also cause the grid to collapse, with cascading failures in equipment far from the attacks, leading to an even larger, longer-term blackout."



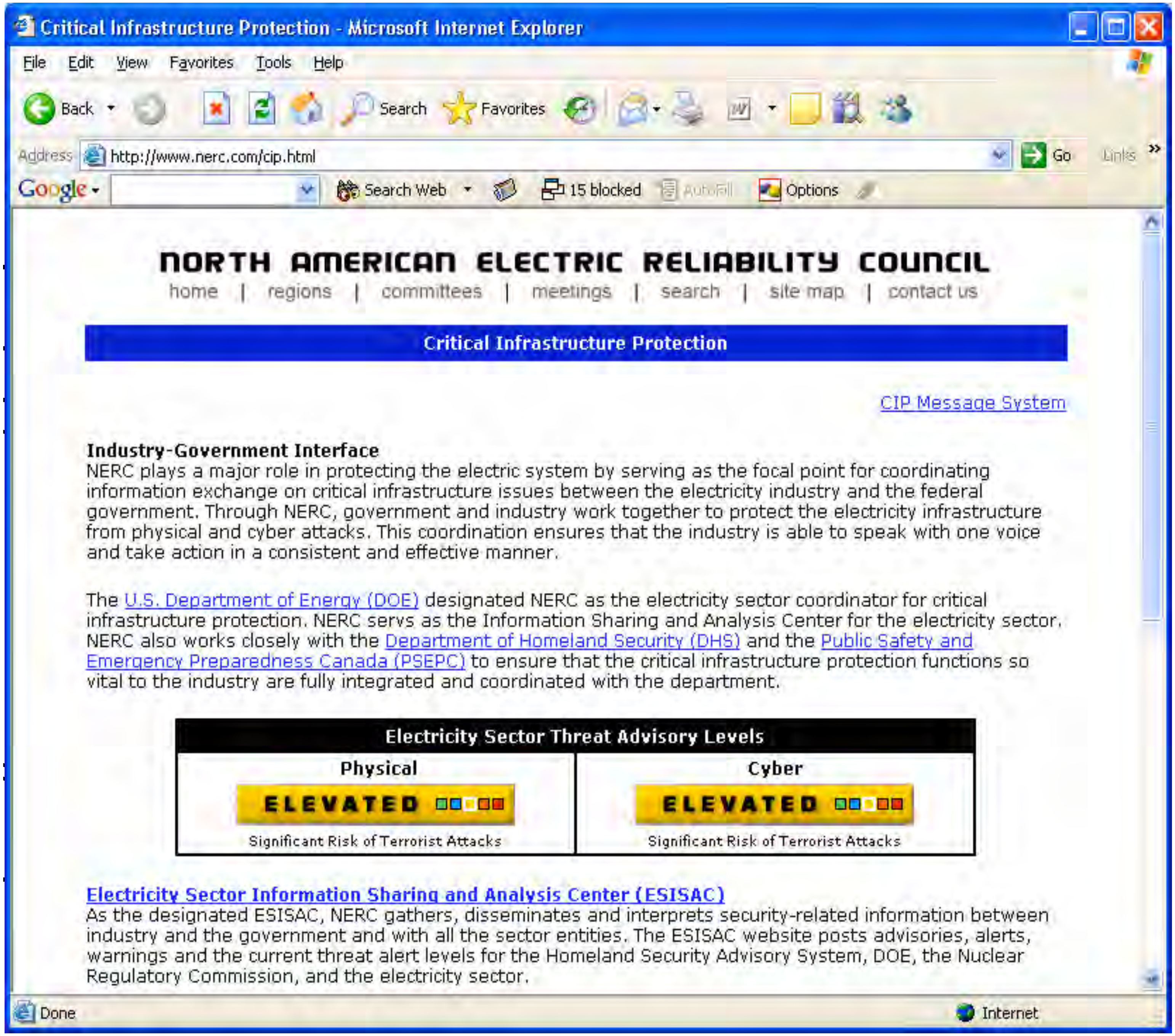
The Nation’s Power Cyber Infrastructure is at R

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.”



NERC is Concerned about such Attac



Critical Infrastructure Protection - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Search Favorites

Address http://www.nerc.com/cip.html Go Links

Google Search Web 15 blocked AutoFill Options

NORTH AMERICAN ELECTRIC RELIABILITY COUNCIL

home | regions | committees | meetings | search | site map | contact us

Critical Infrastructure Protection

CIP Message System

Industry-Government Interface

NERC plays a major role in protecting the electric system by serving as the focal point for coordinating information exchange on critical infrastructure issues between the electricity industry and the federal government. Through NERC, government and industry work together to protect the electricity infrastructure from physical and cyber attacks. This coordination ensures that the industry is able to speak with one voice and take action in a consistent and effective manner.

The U.S. Department of Energy (DOE) designated NERC as the electricity sector coordinator for critical infrastructure protection. NERC servs as the Information Sharing and Analysis Center for the electricity sector. NERC also works closely with the Department of Homeland Security (DHS) and the Public Safety and Emergency Preparedness Canada (PSEPC) to ensure that the critical infrastructure protection functions so vital to the industry are fully integrated and coordinated with the department.

Electricity Sector Threat Advisory Levels	
Physical	Cyber
ELEVATED	ELEVATED
Significant Risk of Terrorist Attacks	Significant Risk of Terrorist Attacks

Electricity Sector Information Sharing and Analysis Center (ESISAC)

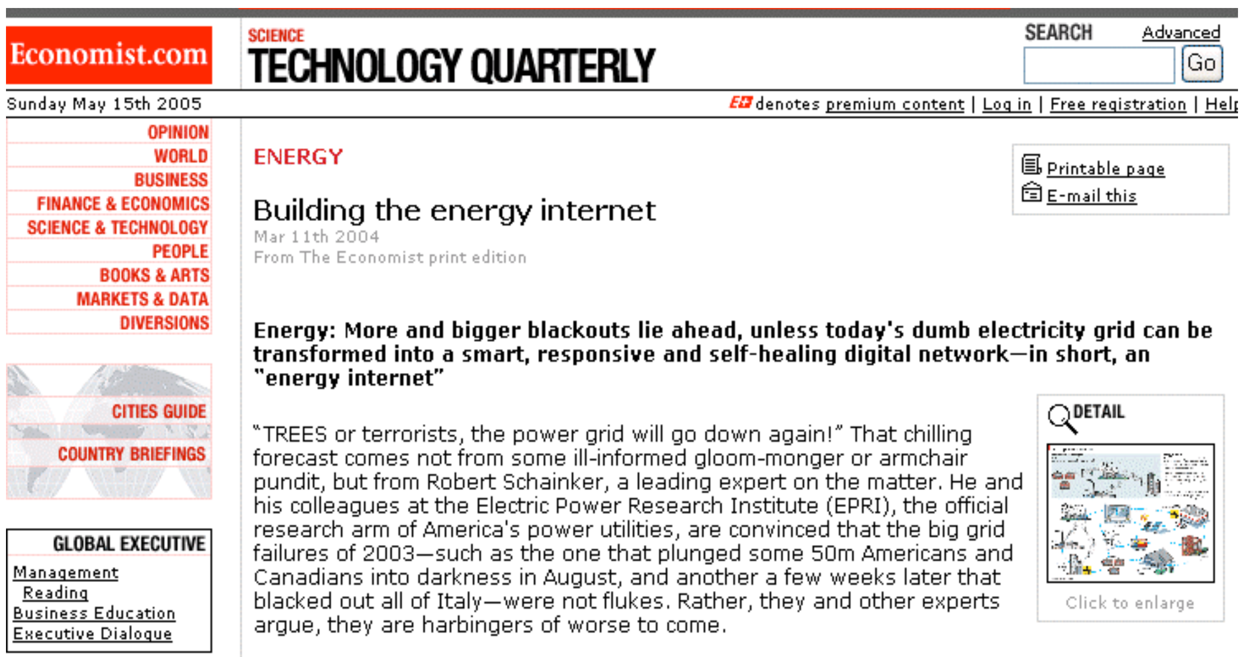
As the designated ESISAC, NERC gathers, disseminates and interprets security-related information between industry and the government and with all the sector entities. The ESISAC website posts advisories, alerts, warnings and the current threat alert levels for the Homeland Security Advisory System, DOE, the Nuclear Regulatory Commission, and the electricity sector.

Done Internet

A Smart, Responsive, a Self-Healing Grid is Need

"Building the Energy Internet," The Economist, March 11, 2004

More and bigger blackouts lie ahead, unless today's dumb electricity grid can be transforn into a smart, responsive and self-healing digi network …



Economist.com

SCIENCE

TECHNOLOGY QUARTERLY

SEARCH Advanced

Go

Sunday May 15th 2005

denotes premium content | Log in | Free registration | Help

OPINION
WORLD
BUSINESS
FINANCE & ECONOMICS
SCIENCE & TECHNOLOGY
PEOPLE
BOOKS & ARTS
MARKETS & DATA
DIVERSIONS

CITIES GUIDE
COUNTRY BRIEFINGS

GLOBAL EXECUTIVE
Management
Reading
Business Education
Executive Dialogue

ENERGY

Printable page
E-mail this

Building the energy internet

Mar 11th 2004
From The Economist print edition

Energy: More and bigger blackouts lie ahead, unless today's dumb electricity grid can be transformed into a smart, responsive and self-healing digital network—in short, an "energy internet"

"TREES or terrorists, the power grid will go down again!" That chilling forecast comes not from some ill-informed gloom-monger or armchair pundit, but from Robert Schainker, a leading expert on the matter. He and his colleagues at the Electric Power Research Institute (EPRI), the official research arm of America's power utilities, are convinced that the big grid failures of 2003—such as the one that plunged some 50m Americans and Canadians into darkness in August, and another a few weeks later that blacked out all of Italy—were not flukes. Rather, they and other experts argue, they are harbingers of worse to come.

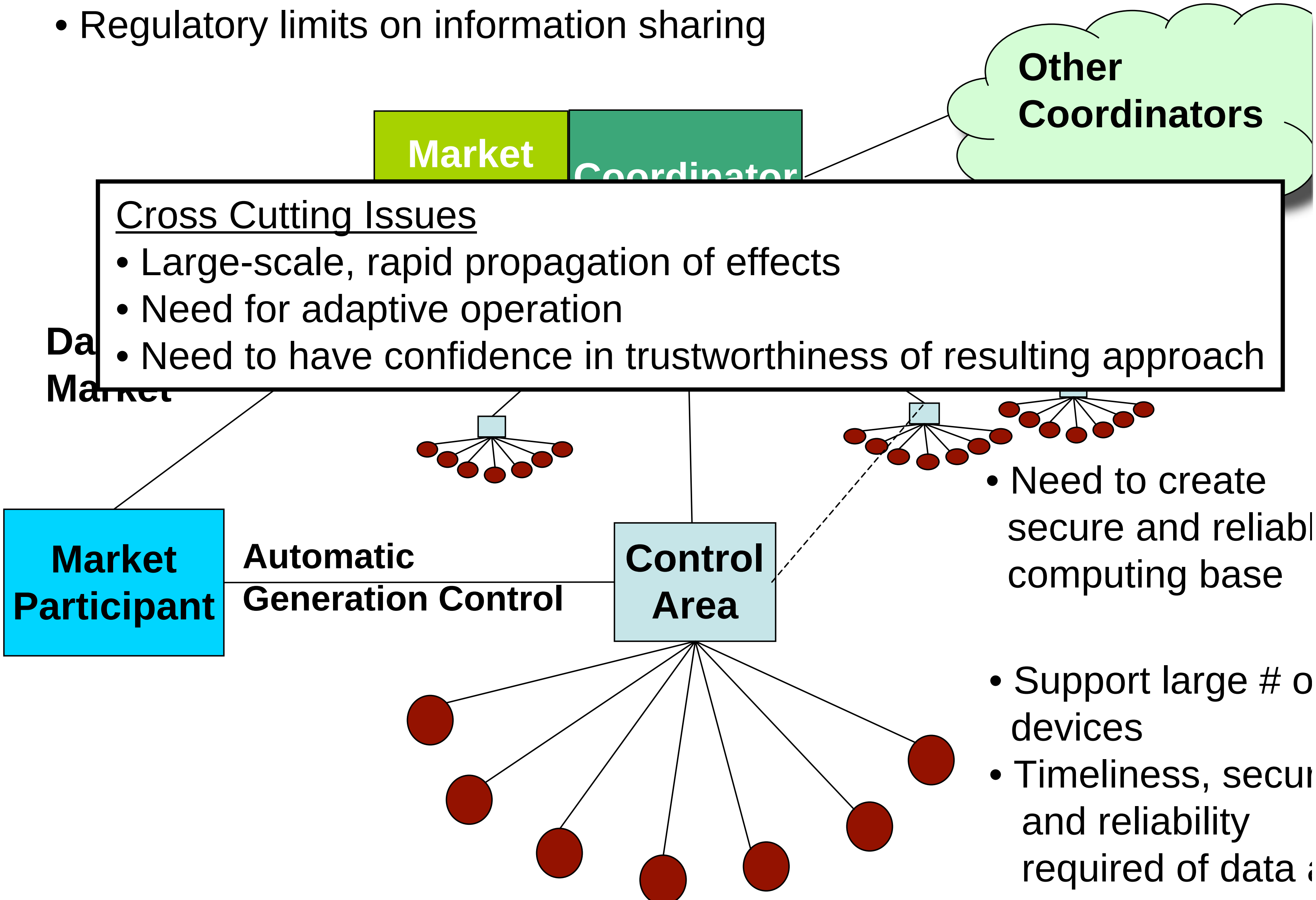
DETAIL

Click to enlarge

www.economist.com/displaystory.cfm?story_id=2476988

Next-Generation Power Grid Cy Infrastructure Challeng

- 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 reliabl computing base

- Support large # o devices
- Timeliness, secu and reliability required of data a control informatio

TCIP Vision and Strate

- Provide the fundamental science and technology to create *the cyber infrastructure for an adaptive, availabl and secure power grid* which
  - survives malicious adversaries and accidental failur
  - provides continuous delivery of power
  - supports dynamically varying trust requirements.
- By:
  - Creating the cyber building blocks and architecture
  - Creating simulation- and experimental testbeds to quantify the amount of trust provided by proposed approach

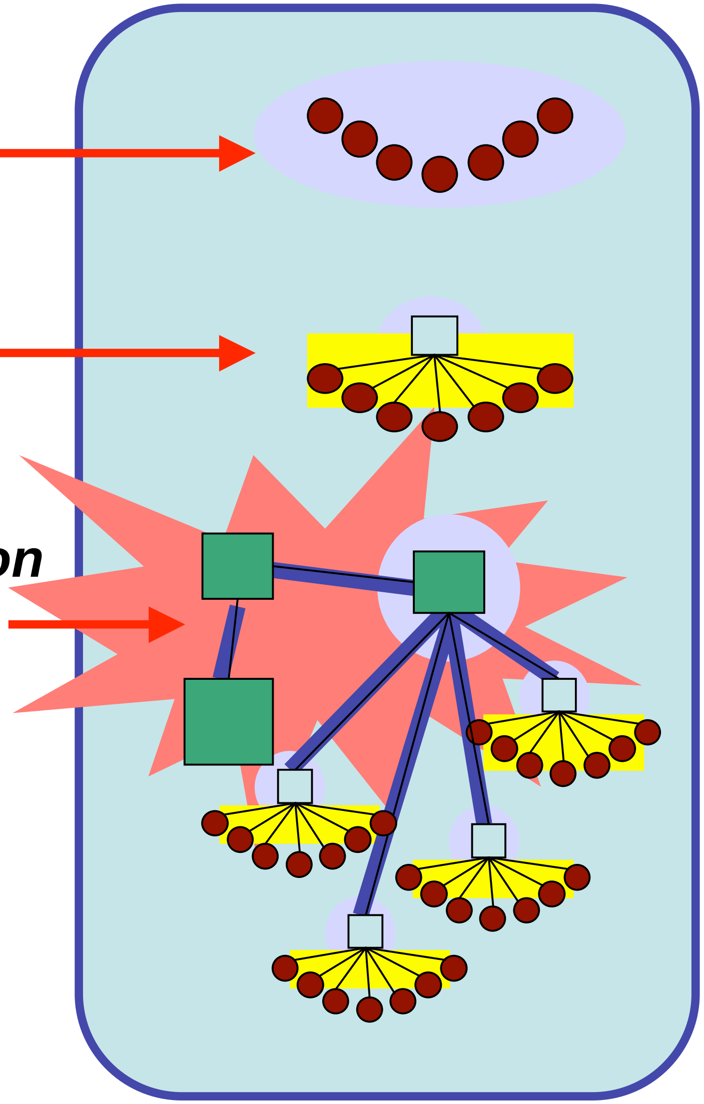
TCIP: Trustworthy Cyber Infrastructure for Pow

Address technical challenges motivated by power grid problems in

Ubiquitous exposed infrastructure

Real-time data monitoring and control

Wide area information coordination and information sharing



tcip.iti.uiuc.edu

By developing

Secure and Reliable Computing Base

Trustworthy Communication & Control Protocols

Quantitative & Qualitative Evaluatio

Education

Technical Approach & Challeng

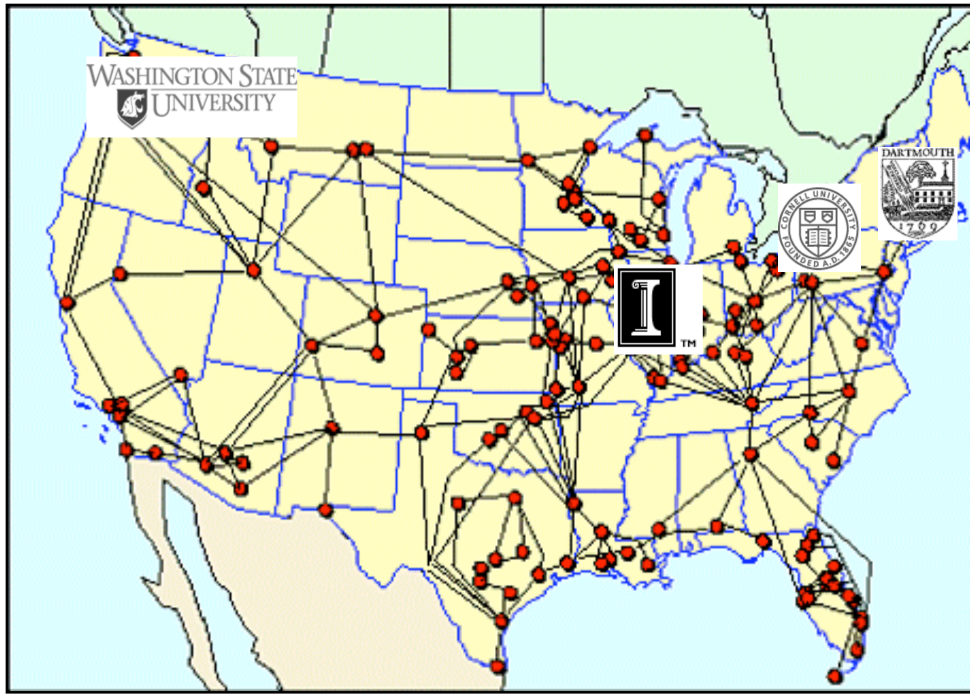
1. **Secure and Reliable Computing Base**: Make low-level devices and their communications trustworthy. Challenges:
   - Sheer number of devices to be secured
   - Cost of securing them
   - Performance impacts of security on the devices' functionality
2. **Communication and Control Protocols (1)**: Efficient, timely and secure measurement and aggregation mechanisms for edge device data.
   - Challenge: devising and implementing adaptable policies and mechanisms for trading off performance and security during
     - Normal conditions
     - Cyber-attacks
     - Power emergencies

Technical Challeng

3. **Communication & Control Protocols (2)**:
    - Mechanisms for scalable inter-domain authorization
    - Fundamental principles for security in emergency situations.
    - Approaches
        - Dynamic negotiation under normal, attack and emergency conditions
        - Mechanisms to exploit the trusted computing base.
4. **Quantitative & Qualitative Evaluation**: Validate the TCIP designs and implementations produced in the other areas.
    - create security metrics, multi-scale abstractions and attac models
    - emulation technology to allow quantitative analysis of rea power grid scenarios.

TCIP Senior Investigat

- 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



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

TCIP Graduate and Undergraduate Research

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.* (Dartmout
- Nathan Schubkegel (WSU)
- Evan Sparks* (Dartmouth)
- Erik Yeats* (WSU)

* Not funded by TCIP, but workin on TCIP

Area 1 Approa

- ***Focus*****:** Move from ***perimeter security*** to ***platform security*** in t 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 gc 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

Year 1 Accomplishments / Research Directio

- ***Hardening platforms***:
  - Demonstration of automatic tool to secure ***high-stakes ISO computation*** against dedicated insiders with physical access
  - Design and initial prototype of fast, novel crypto for ***control centers a substations***
  - Design and prototype of processor modules:
- ***Reconfigurable hardening***
  - Customize and implement, into an FPGA, Illinois Reliability and Secur Engine (RSE) for ***substations and control center*** applications of the power grid infrastructure
  - Incorporation of attack detectors and error detectors within RSE
  - Methodology and associated tools for generation of application-specif assertions for runtime detection of malicious and accidental errors in ***SCADA applications***
- ***Application Integration***
  - Applied *Trusted Computing (TC)* and *virtualization* technologies to develop an ***attested meter***
  - Analyzed security architecture requirements for ***relays*** in substations understand prospects for individually secured IEDs that can meet timi requirements

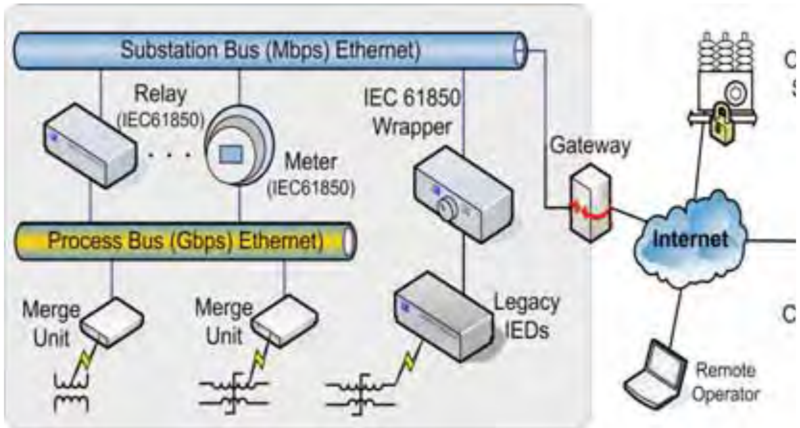
Trustworthy Communication & Control Protoc

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 relia monitoring, detection, alert, and control solutions in case of perturbations, vulnerabilities anc 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 communicati links among them



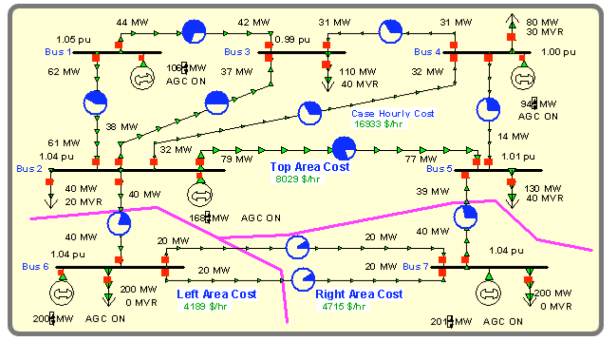
Communication & Control Protoc
Year 1 Accomplishments / Research Directio

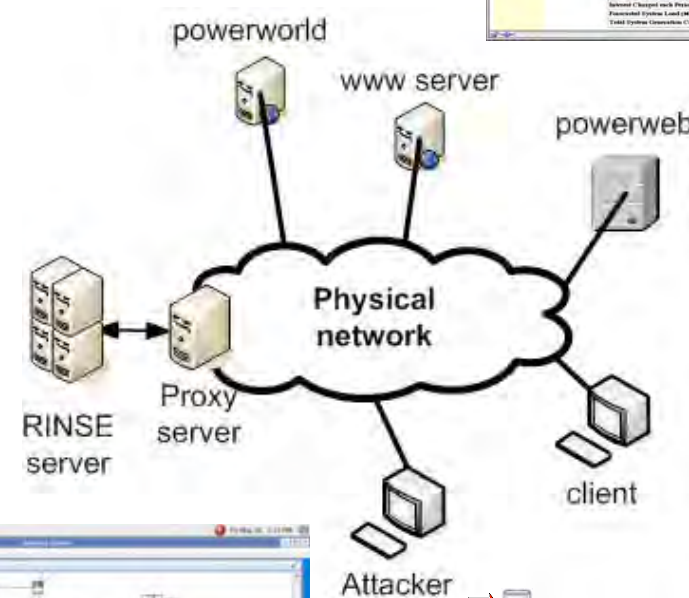
- Evaluated SCADA architectures and protocols for data transmiss and aggregation (IEC 61850)
- Identified security threats and attacks in SCADA networks
- Explored mathematical models for QoS/data/alarm aggregations
- Analyzed requirements for generalized trust in pub/sub systems
- Achieved rigorous reasoning about trust negotiation
- **Designed Architectural Innovations**
  - Exploration of selected aggregation functions and algorithms over wireless network technologies
  - Initial design of alert and attack containment to limit spread of unwanted updates
  - Deployment of Real-Time QoS mechanisms in standard IP-based network technologies for QoS-aware dissemination of TCIP information
  - Development of trust management for TCIP components
  - Design of Credentialing for Emergencies at ISO level

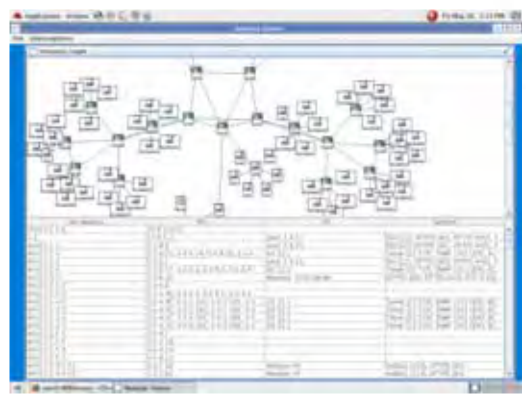
Quantitative & Qualitative Evaluati

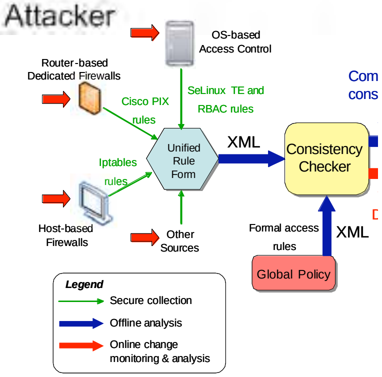
Approach:

- 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









Evaluation Year 1 Accomplishme / Research Directio

Simulation

- Emulation, transparent integration of IP devices {project,external} servers, rout clients
- Modbus speaking simulators of power grid, and SCADA control center
- Algorithms for high speed virtual background network traffic
- Cyber-attack models (algorithms/optimizations + implementation)
  - Random scanning worms, flash-worms, packet reflection, packet redirecti

Intruder client

- New man-in-middle code attack on Modbus timing
- Database of co-opted traffic

Power Markets

- Experimental design + technical support, co-opting auction information

System Evaluation

- Methodology for analyzing properties of system configuration vis a vis formaliz interpretation of best practices
- Tool (APT) for analyzing firewall configurations vis a vis formalized global polic

Integration

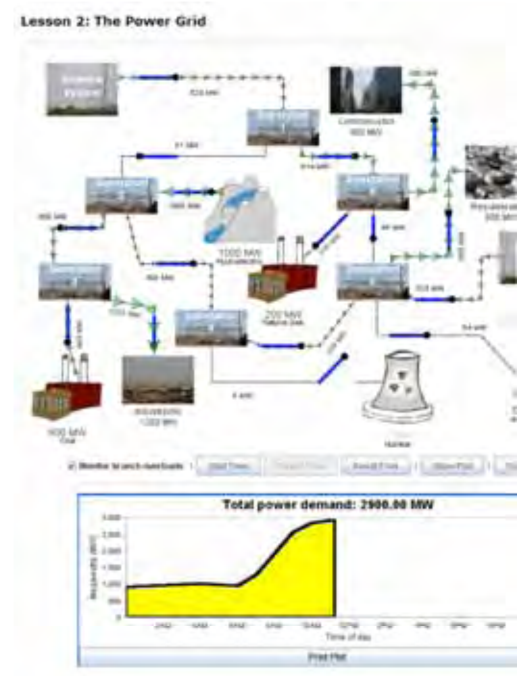
- Network simulation/emulation operationally integrated with
  - Simulated power grid and SCADA
  - Simulated power auction server
  - Intruder client
- Conceptually integrated with system evaluation

Education Go

- Facilitate the integration of research, education and knowledge transfer by linking researchers, educators and students
- Connect with K-12 teachers and students
- Share higher education courses and instructional modules across disciplines involved in the project (CE, EE, CS)
- Provide research experiences to undergraduate and graduate students
- Develop hands-on laboratories and tools

Education : Year 1 Accomplishme
/ Research Directio

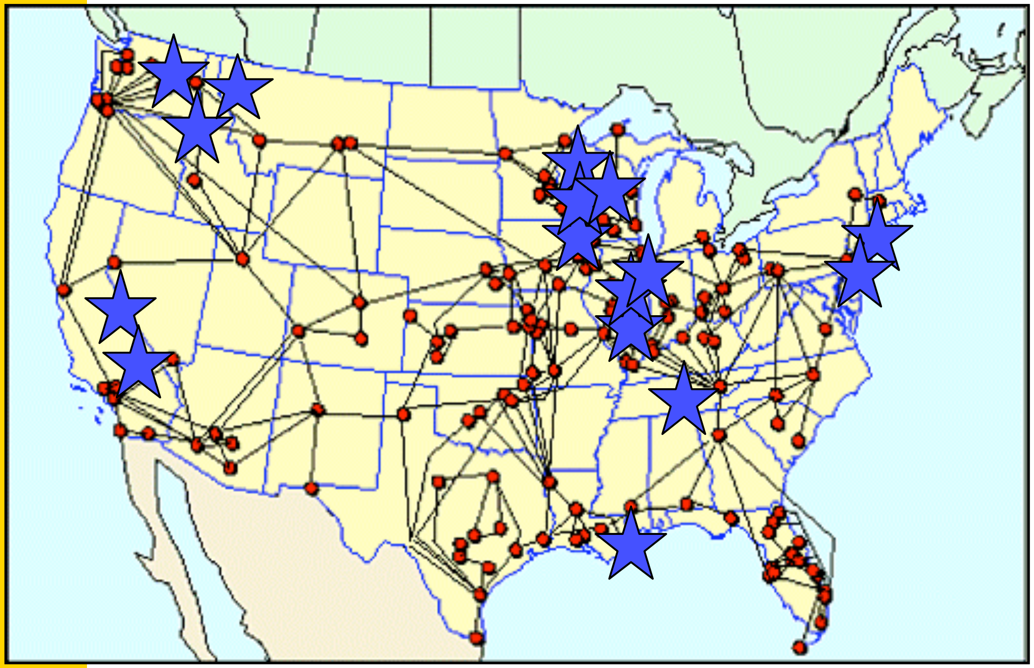
- TCIP Researchers, in partnership with math/science education specialists:



- Developed interactive and open-ended applets for middle-schoolers
- Produced printed activity materials and teacher guides coordinated with the applets
- Aligned lessons to content standards
- Started process of piloting and disseminating educational materials to students and educators in middle schools

5th grade student at Olympia North Elementary School using TCIP applet

Industrial Partnerships – Spanning Stakehold



Technology Providers/Research

ABB – Industrial manufacturer and supplier
Siemens – Industrial manufacturer and suppli
AREVA – Major SW vendor for utility EMS systems
Cisco Systems – CIP Researchers
Cyber Defense Agency – Security Assessm
EPRI – Electric Power Research Institute
GE Global Research – Research in communication and computing requirements f US power grid
Honeywell – Industrial control system provide 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 provid
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.

Year 1 Industry Interactio

- Comprehensive group of industrial advisors representing industries across the nation
- Industry seminars - ongoing
- Faculty visits and connections - ongoing
- Field trips for TCIP project team
  - MISO and Ameren IP during summer 2006
- Industry kickoff meeting – December 2005
- Industry workshop – December 2006
- Power systems infrastructure tutorial (in progress)
- Directory of industrial contacts (in progress)