



U.S. Department of Energy

Office of Electricity Delivery and Energy Reliability

Activities to Secure Control Systems in the Energy Sector

November 2008

Hank Kenchington – Program Manager

Office of Electricity of Delivery and Energy Reliability

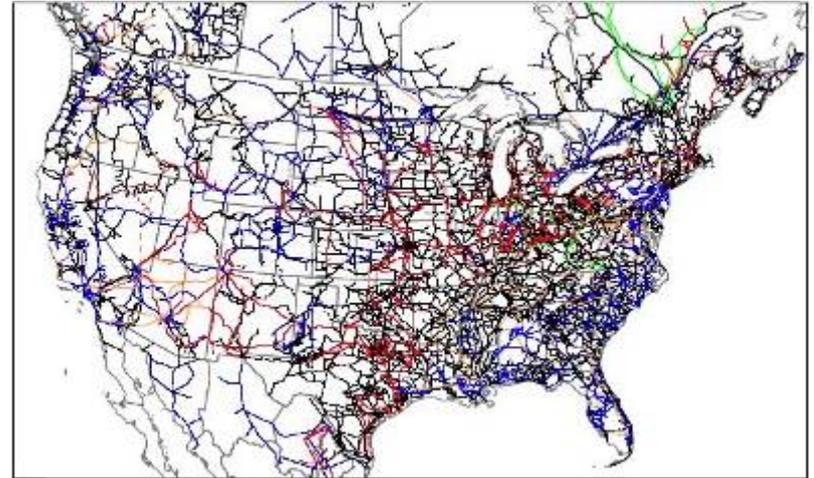
U.S. Department of Energy

NSTB

Enhancing control systems security in the energy sector

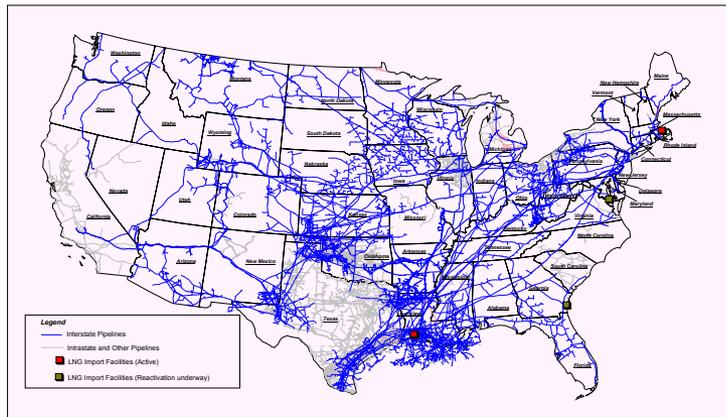
North American Energy Infrastructure: vast, complex, interconnected

- 160,000 Miles of Electrical Transmission lines
- ~17,000 Generators; 985,000 Megawatts (net summer capacity)
- Over 3,100 Electric Utilities, with 131 million customers



U.S. Electric Power Grid

Refinery Locations, Crude and Product Pipelines



Source: Energy Information Administration, Office of Oil & Gas

- 2,000,000 Miles of Oil Pipelines
- 1,300,000 Miles of Gas Pipelines
- 2,000 Petroleum Terminals
- ~1,000,000 Wells
- Extensive Ports, Refineries, Transportation, and LNG Facilities

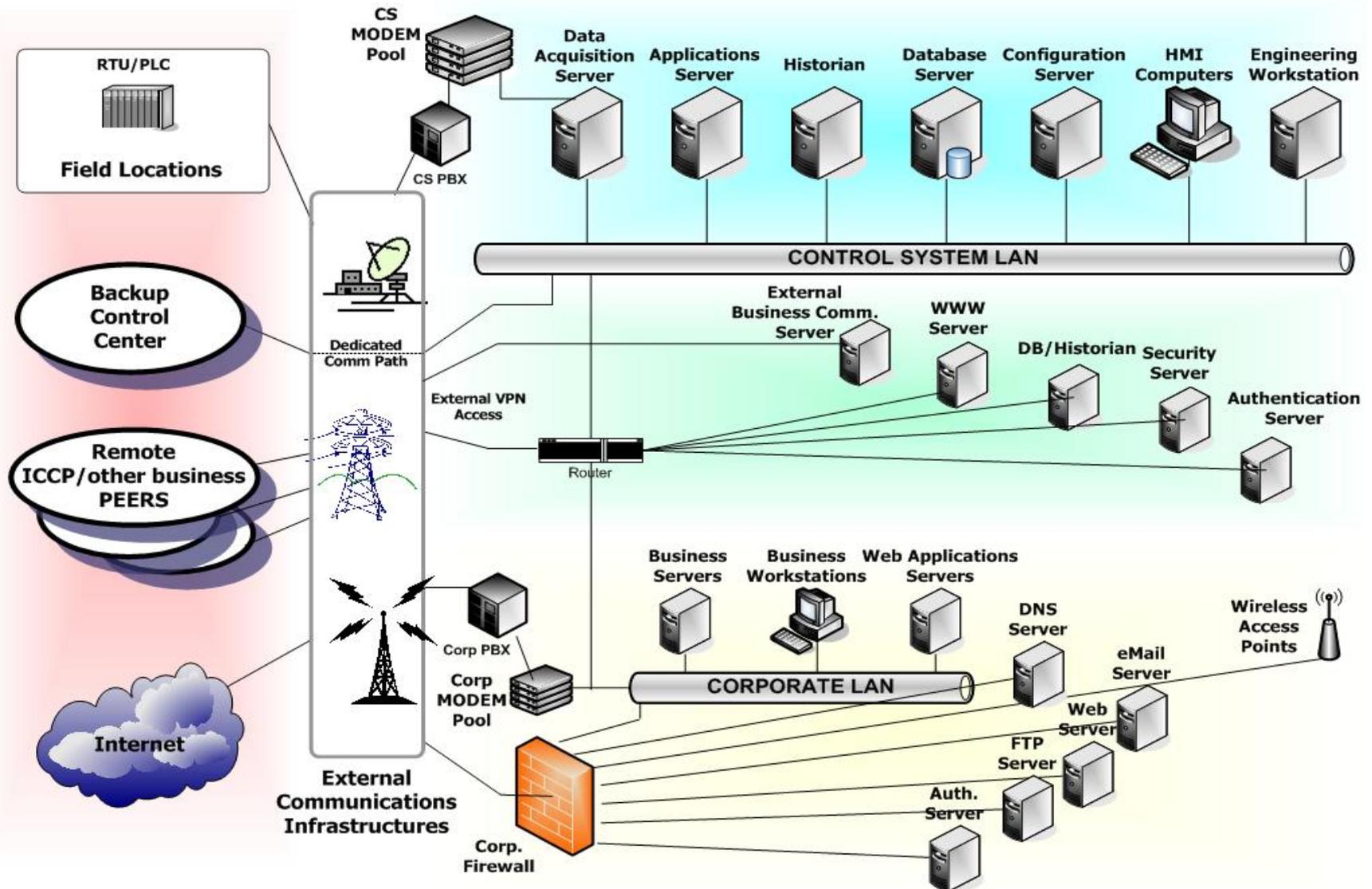
DOE Office of Electricity Delivery and Energy Reliability

Leads national efforts to:

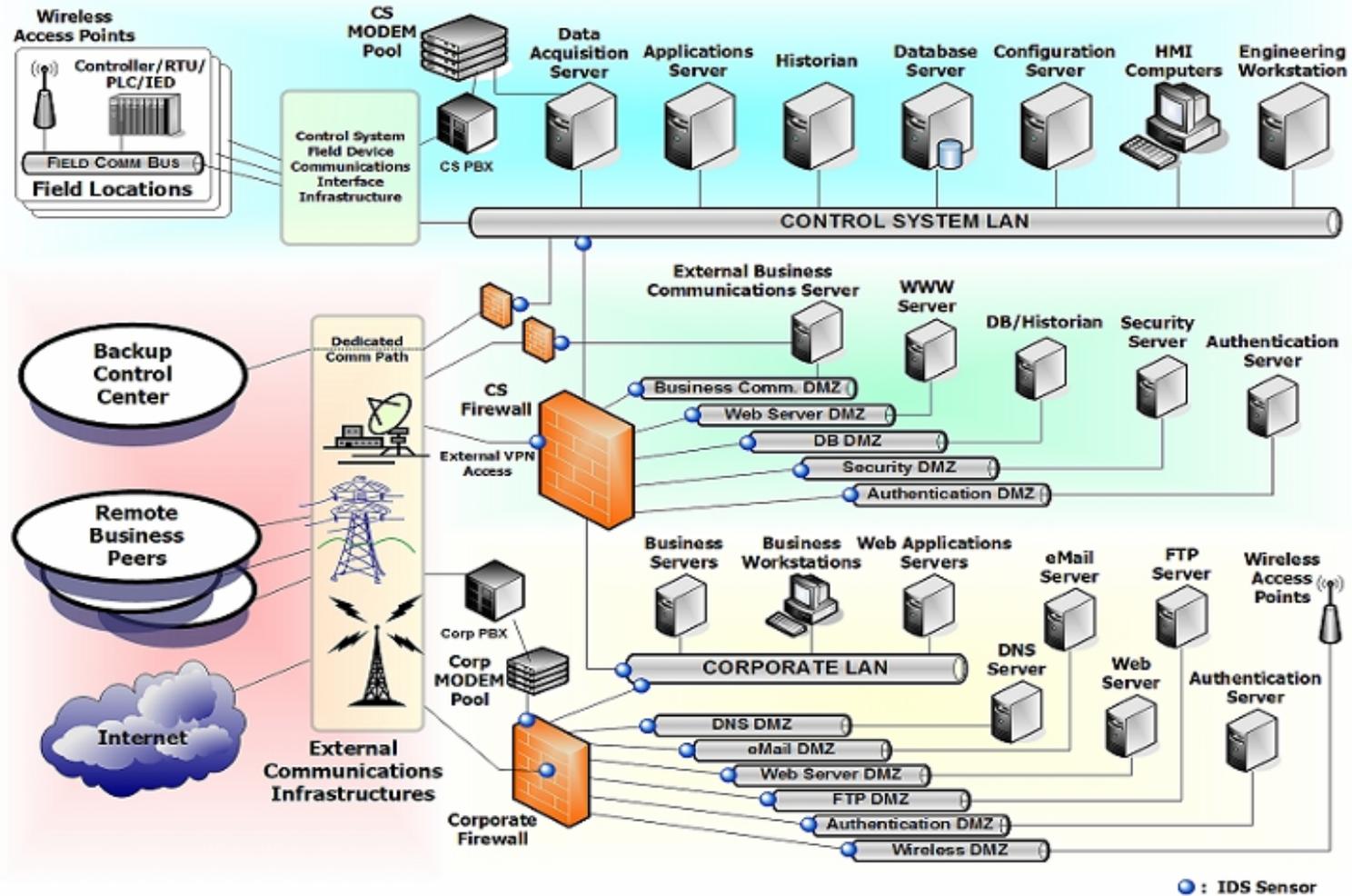
- *modernize the electric grid,*
- *enhance security and reliability of the energy infrastructure, and*
- *facilitate recovery from disruptions to energy supply.*

Developing highly robust and secure Control Systems is a cornerstone for a resilient and robust energy infrastructure

Example SCADA Architecture

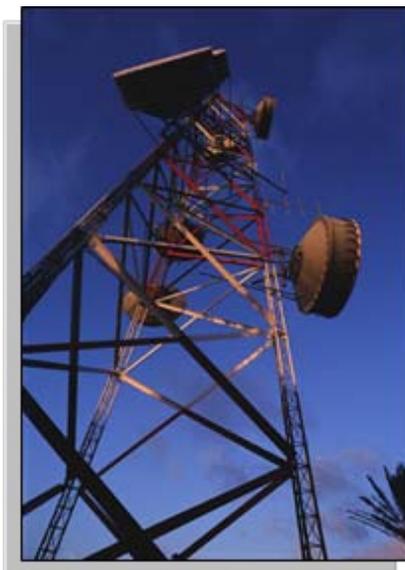


Recommended Architecture

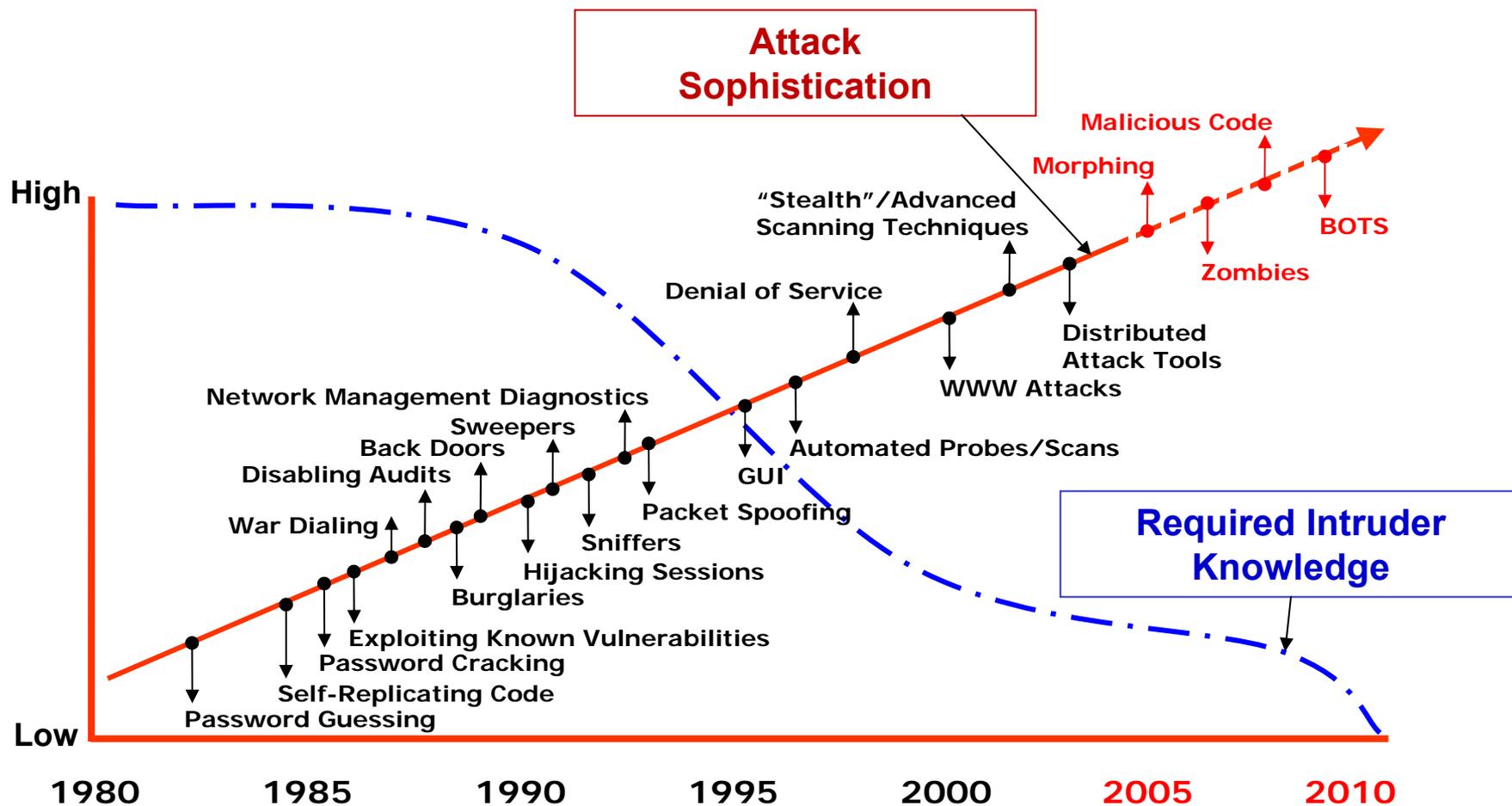


Trends Impacting Control System Security

- **Open Protocols**
 - Open industry standard protocols are replacing vendor-specific proprietary communication protocols
- **Common Operating Systems**
 - Standardized computational platforms increasingly used to support control system applications
- **Interconnected to Other Systems**
 - Connections with enterprise networks to obtain productivity improvements and information sharing
- **Reliance on External Communications**
 - Increasing use of public telecommunication systems, the Internet, and wireless for control system communications
- **Increased Capability of Field Equipment**
 - “Smart” sensors and controls with enhanced capability and functionality



Cyber Threat Trends



Source: Carnegie-Mellon University

Threat is Real and Targeted

“Our information infrastructure—including the internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries—increasingly is being targeted for exploitation and potentially for disruption or destruction, by a growing array of state and non-state adversaries.”



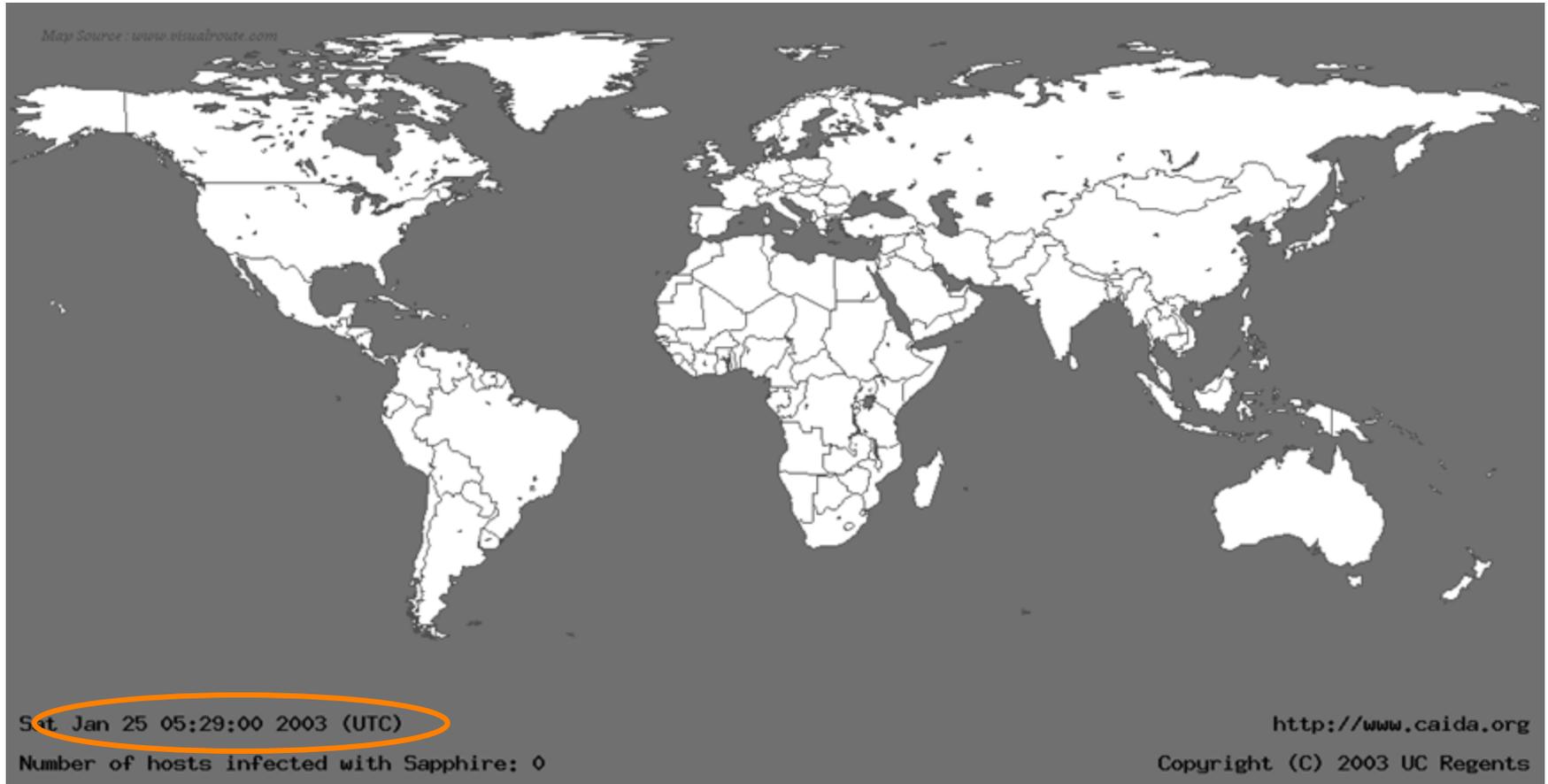
Annual Threat Assessment of the Intelligence Community

7 February 2008

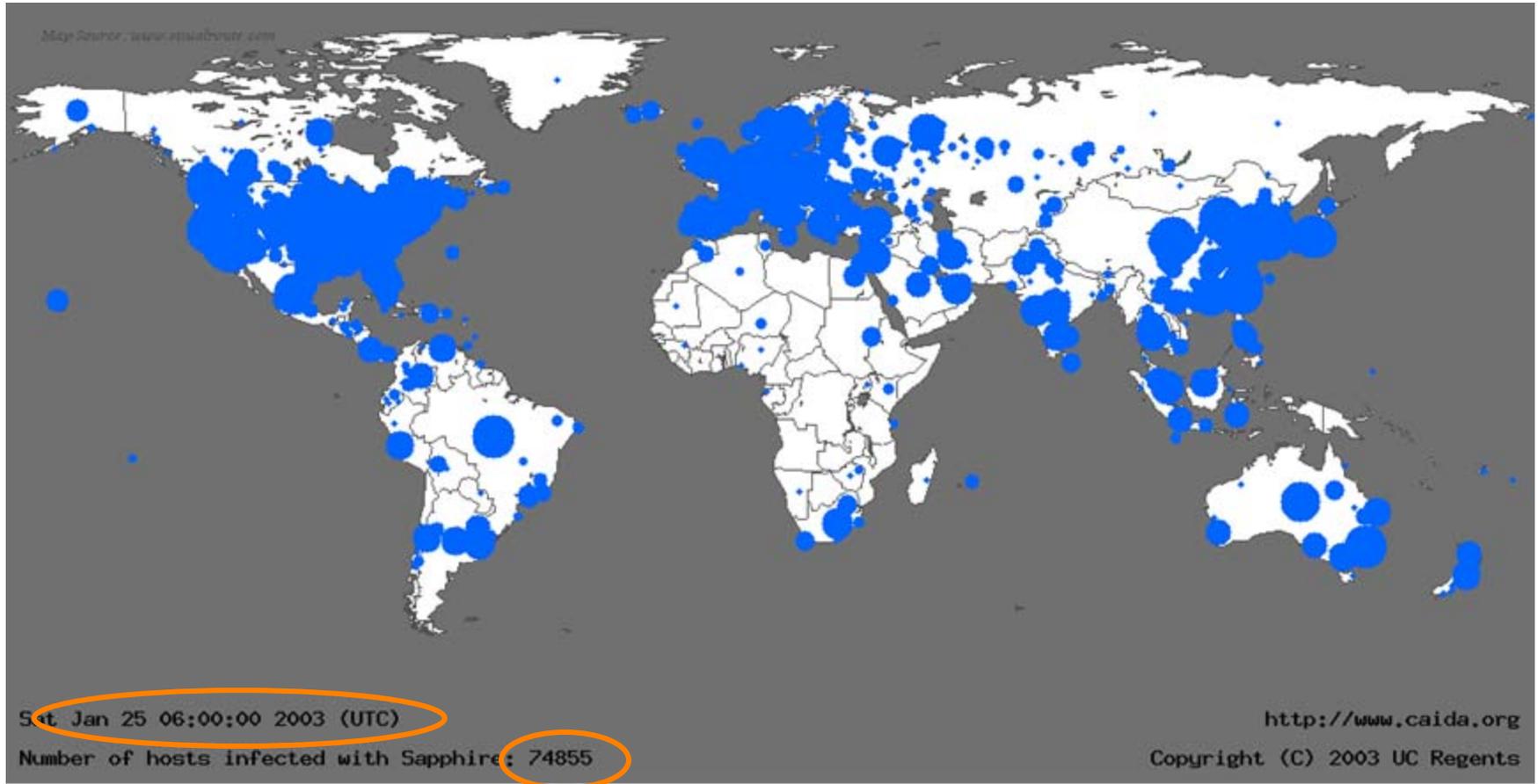
J. Michael McConnell

Director of National Intelligence

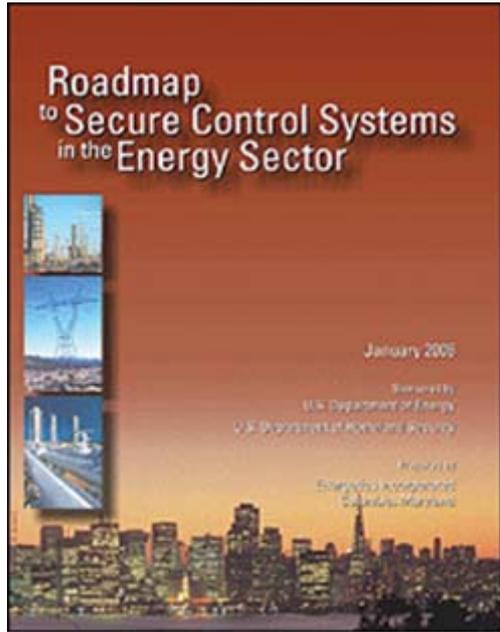
Life Just Before Slammer



Life Just After Slammer



Roadmap – Framework for Public-Private Collaboration



- Published in January 2006
- *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

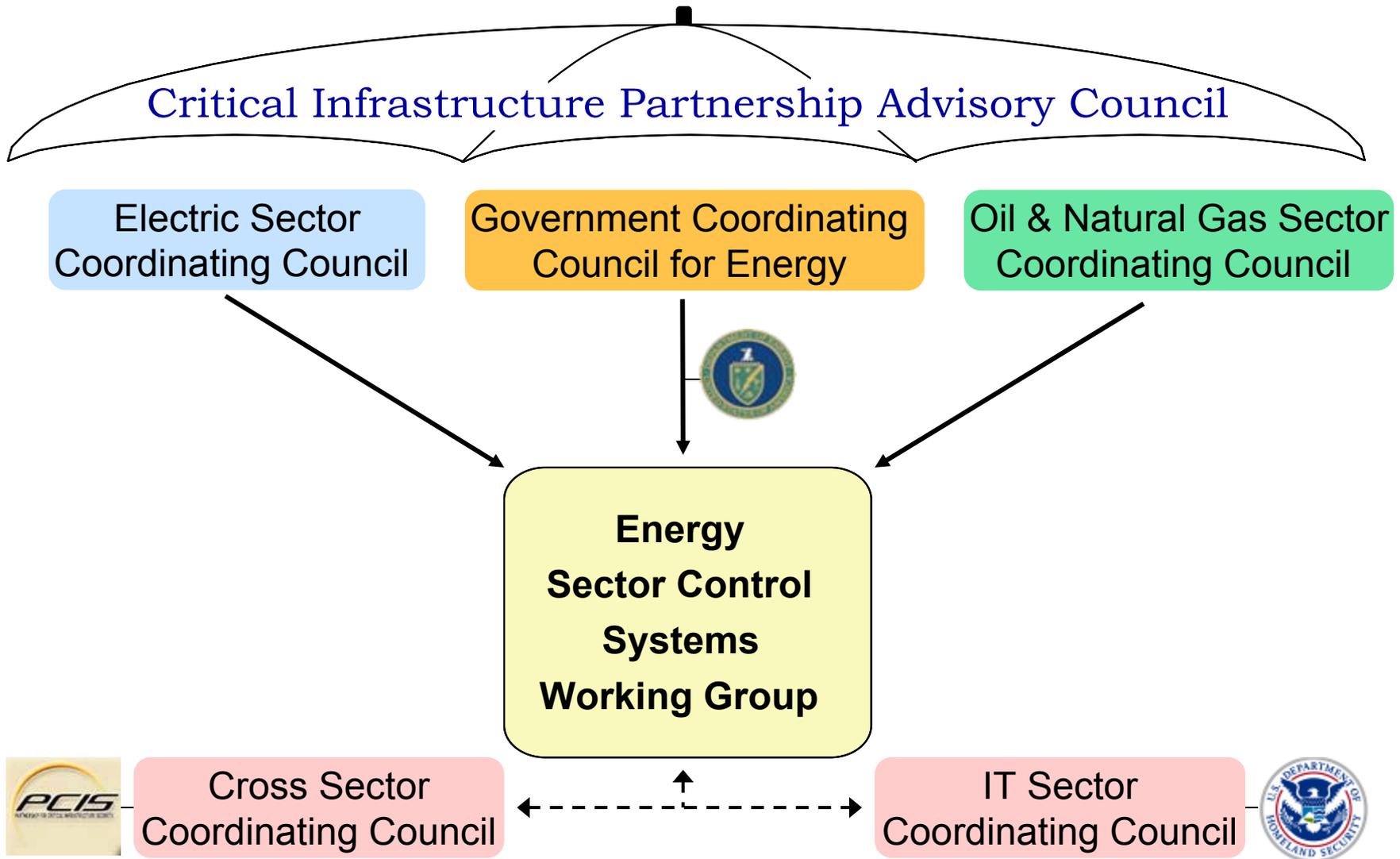
Roadmap Vision

In 10 years, control systems for critical applications will be designed, installed, operated, and maintained to **survive an intentional cyber assault with no loss of critical function.**

Key Roadmap Strategies and Selected Milestones

Measure and Assess Security Posture	Develop and Integrate Protective Measures	Detect Intrusion & Implement Response Strategies	Sustain Security Improvements
Milestones	Milestones	Milestones	Milestones
<p>50% of asset owners & operators performing self-assessments of their control systems using consistent criteria (2008)</p> <p>Fully automated security state and common response of control system networks (2015)</p>	<p>Secure connectivity between business systems and control systems within corporate network (2009)</p> <p>Secure control system architectures produced with built-in, end-to-end security (2015)</p>	<p>Cyber incident response is part of emergency operating plans at 30% of control systems (2008)</p> <p>Self-configuring control system network architectures are in production (2015)</p>	<p>Compelling, evidence-based business case to increase private investment in control system security (2007)</p> <p>Cyber security awareness, outreach, and education programs integrated into energy sector operations (2015)</p>

Working Group Oversees Roadmap Implementation



Energy Sector Control Systems Working Group

Members

- Dave Batz, Alliant Energy (NERC, AGA, EEI, InfraGard)
- Stuart Brindley, IESO Ontario (NERC, PCIS, CSCSWG)
- Page Clark, El Paso Corporation (INGAA)
- Steve Elwart, Ergon Refining Inc. (NPRA, I3P, CI/KR RAMP)
- Eric Fletcher, NiSource
- Tom Flowers, CenterPoint Energy, Inc. (NERC)
- Ed Goff, Progressive Energy (NERC, EEI)
- Morgan Henrie, Alyeska Pipeline (API)
- Hank Kenchington, DOE (PCSF, CSCSWG)
- Doug Maughan, DHS S&T
- Seán McGurk, DHS NCSD (PCSF, CSCSWG)
- Dave Norton, Entergy Corporation (NERC, PCSF, IEEEA, InfraGard)
- Dave Scheulen, BP (API)

ieRoadmap – “weapon of mass collaboration”¹

Facilitates collaboration and measures progress



www.pcsforum.org/roadmap

- On-line Roadmap Mapping Tool
- Hosted by Process Control Systems Forum (PCSF)
- Total 102 projects mapped by 21 organizations

¹“Wikinomics, How Mass Collaboration Changes Everything”, Tapscott and Williams

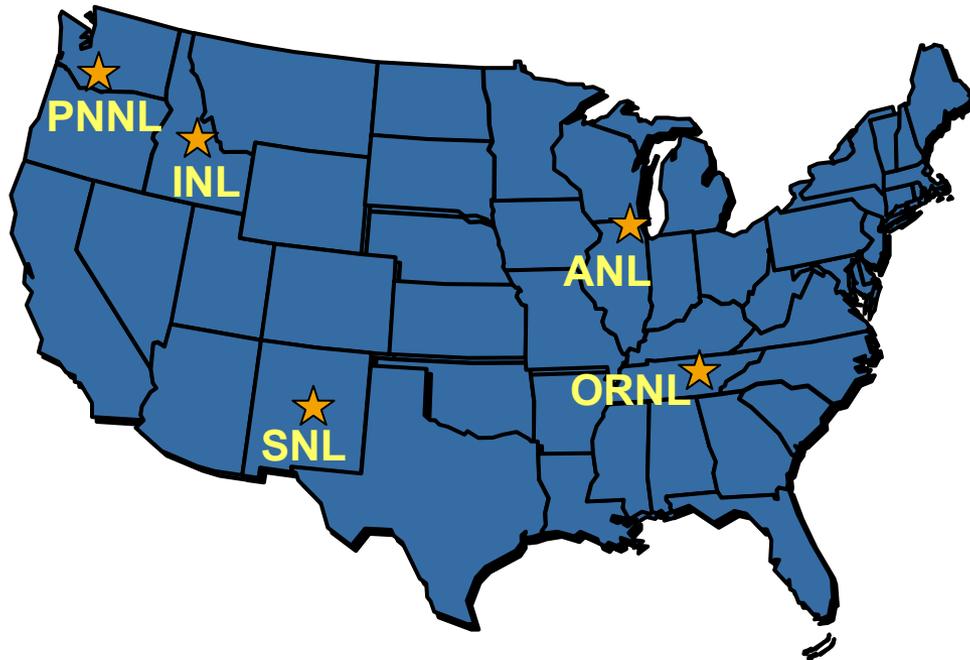
ieRoadmap – Progress to Date

Since 2006 Total 102 projects mapped by 21 organizations		62 projects	Measure and Assess Security Posture
		59 projects	Develop and Integrate Protective Measures
		45 projects	Detect Intrusion and Implement Response Strategies
		49 projects	Sustain Security Improvements

DOE National SCADA Test Bed (NSTB) Program

DOE multi-laboratory program ...established 2003

Supports industry and government efforts to enhance cyber security of control systems in energy sector



Key Program Elements

- Cyber security assessments and recommended mitigations for energy control systems
- Integrated risk analysis
- Secure next generation control systems technology R&D
- Public-private partnership, outreach, and awareness

“..the only reliable way to measure security is to examine how it fails”

Bruce Schneier, Beyond Fear

17 NSTB Facilities From 5 National Labs

IDAHO Critical Infrastructure Test Range

- SCADA/Control System Test Bed
- Cyber Security Test Bed
- Wireless Test Bed
- Powergrid Test Bed
- Modeling and Simulation Test Bed NEW
- Control Systems Analysis Center NEW

SANDIA Center for SCADA Security

- Distributed Energy Technology Laboratory (DETL)
- Network Laboratory
- Cryptographic Research Facility
- Red Team Facility
- Advanced Information Systems Laboratory



PACIFIC NORTHWEST Electricity Infrastructure Operations Center

- SCADA Laboratory
- National Visualization and Analytics Center
- Critical Infrastructure Protection Analysis Laboratory



OAK RIDGE Cyber Security Program

- Large-Scale Cyber Security and Network Test Bed
- Extreme Measurement Communications Center

ARGONNE Infrastructure Assurance Center

Selected NISTB FY08 Activities

1. System Vulnerability Assessments and Mitigation

- Test bed and On-site SCADA/EMS Vulnerability Assessments:
Completed: ABB, AREVA, GE, Siemens
In process/planned: Telvent, OSI, Siemens, ABB Consortium, Teltone Gauntlet Dial-up Gateway

2. Public-Private Partnership, Outreach, and Awareness

- Vendor User Groups, training courses - over 1,700 end-users trained to date
- Red/Blue Team Training
- Coordinate with Industry groups (electric, oil, and gas)

3. Integrated Risk Analysis

- Modelling/simulation capability to better evaluate RISK of various cyber threats

4. Next Generation Technology Development

- Secure SCADA Communications Protocol for serial-based data communications
- Open architecture for secure, interoperable IP-based communications
- Advanced Network Toolkit for Advanced Remote Mapping (ANTFARM)
- 5 new industry-led projects – over \$8MM in federal funding plus private cost-share

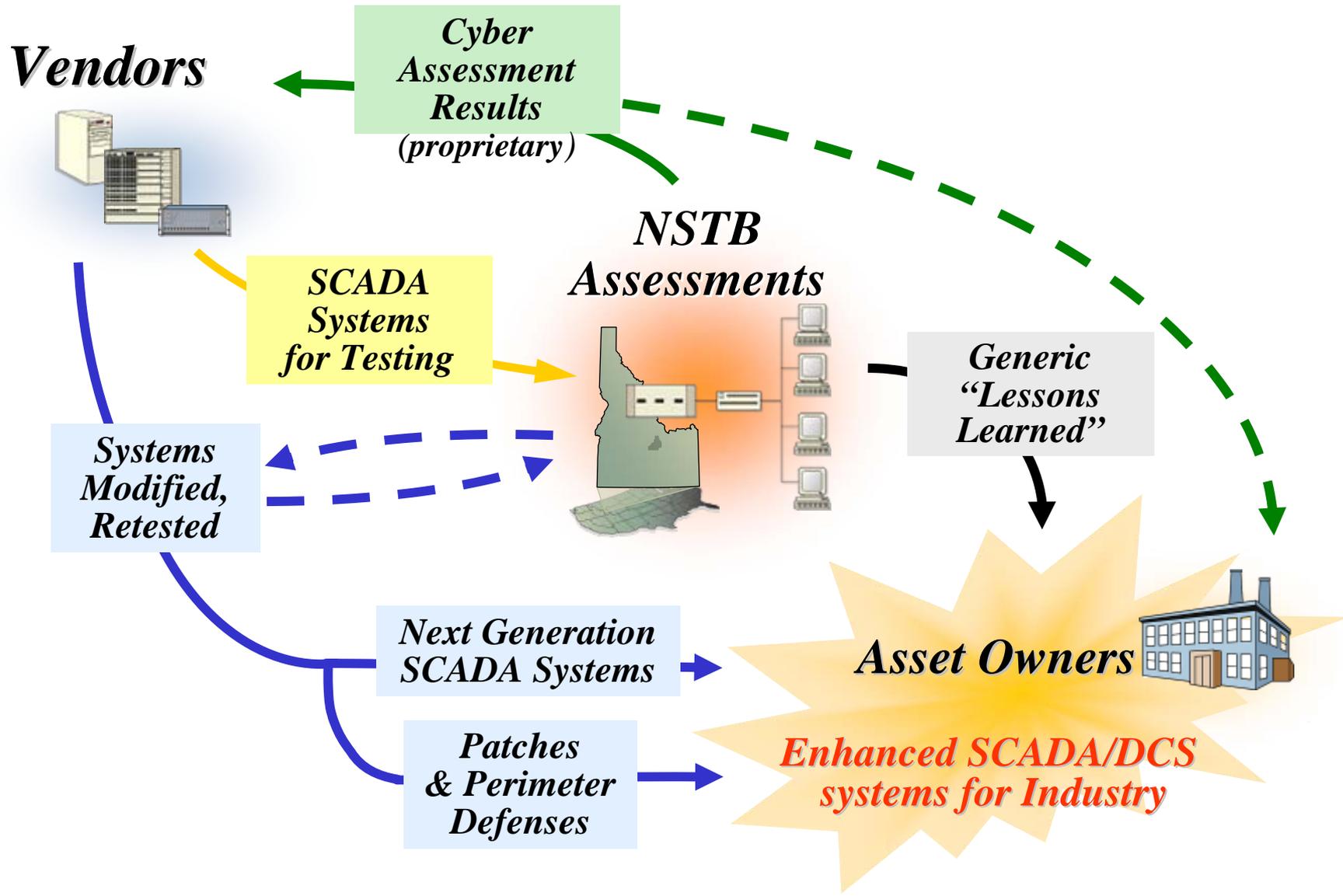
NSTB Assessments Summary

Assessments	Completed	In Process	Planned
Test Bed - Systems	11	4	2
Test Bed - Components	4	1	2
On-Site	4	3	1

MARKET OUTCOMES:

- 7 Enhanced Systems**
- 4 Enhanced Systems in development**
- 5 Patches (addressing 5 issues)**
- 2 New Perimeter Architectures**
- 21 Installations of One Vendor's Upgraded Systems**
- 45 Asset Owner Requests for Proprietary Assessment Reports**
- 82 System Applications Using Downloaded Software Patches**

Enhanced SCADA Systems in Market **TODAY!**



“Common Vulnerabilities” Report

Preliminary Results

Communications:

Control System Protocols 8/8
Communications with External Systems 7/7
Direction of Communications Weaknesses 2/2
Network Addressing Weaknesses 12/12
Bypassed Communications 3/4
Perimeter Protection 4/4

Applications:

Authentication Weakness 9/10
Network Protocol Overflow 8/8
Other Coding Weaknesses 10/10

System:

Vulnerable Component/Service 8/10
Unused Services Weaknesses 9/11

Web Interfaces:

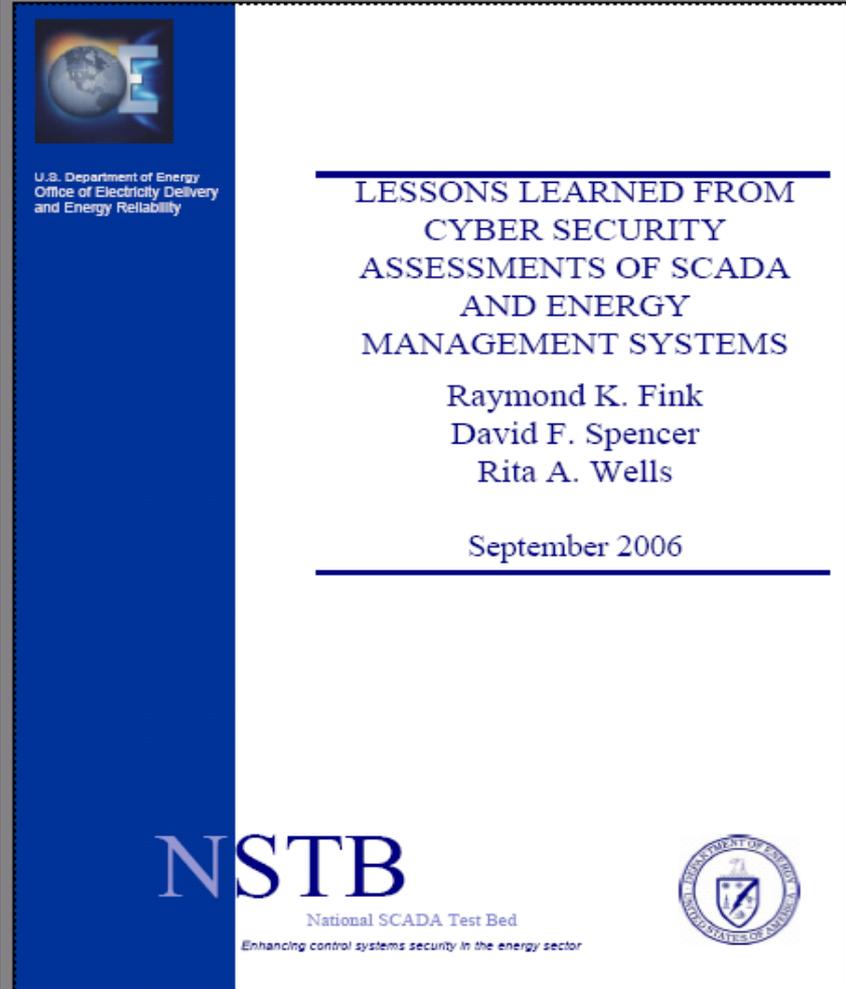
Web Directory Traversal/Browsing Weaknesses 4/4
Web Application Weaknesses 6/6
Web Authentication Weaknesses 2/2

Account:

Clear Text Login 10/12
Password Weakness 7/10
Default Account Weaknesses 3/4
Session Management 5/6

Information Disclosure:

Account Information Disclosure 3/3
Application Version Disclosure 5/5
Configuration Vulnerability Disclosure 4/4



The image shows the front cover of a report. The left side has a blue vertical bar with a globe icon and the text 'U.S. Department of Energy Office of Electricity Delivery and Energy Reliability'. The main title is 'LESSONS LEARNED FROM CYBER SECURITY ASSESSMENTS OF SCADA AND ENERGY MANAGEMENT SYSTEMS'. Below the title are the authors: Raymond K. Fink, David F. Spencer, and Rita A. Wells. The date is 'September 2006'. At the bottom, there is the NSTB logo (National SCADA Test Bed) and the Department of Energy seal.

U.S. Department of Energy
Office of Electricity Delivery
and Energy Reliability

LESSONS LEARNED FROM
CYBER SECURITY
ASSESSMENTS OF SCADA
AND ENERGY
MANAGEMENT SYSTEMS

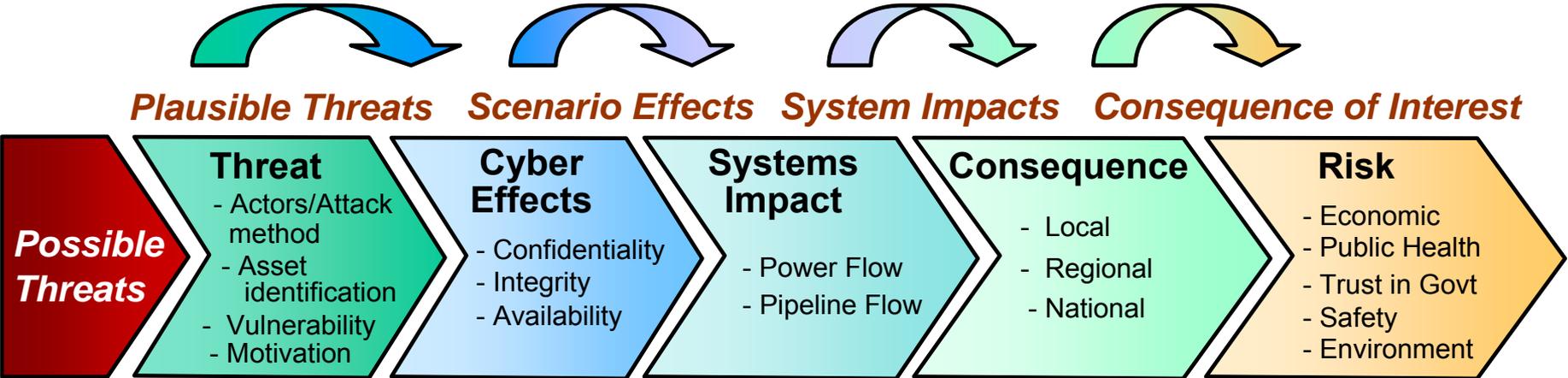
Raymond K. Fink
David F. Spencer
Rita A. Wells

September 2006

NSTB
National SCADA Test Bed
Enhancing control systems security in the energy sector



End-to-End Risk Analysis

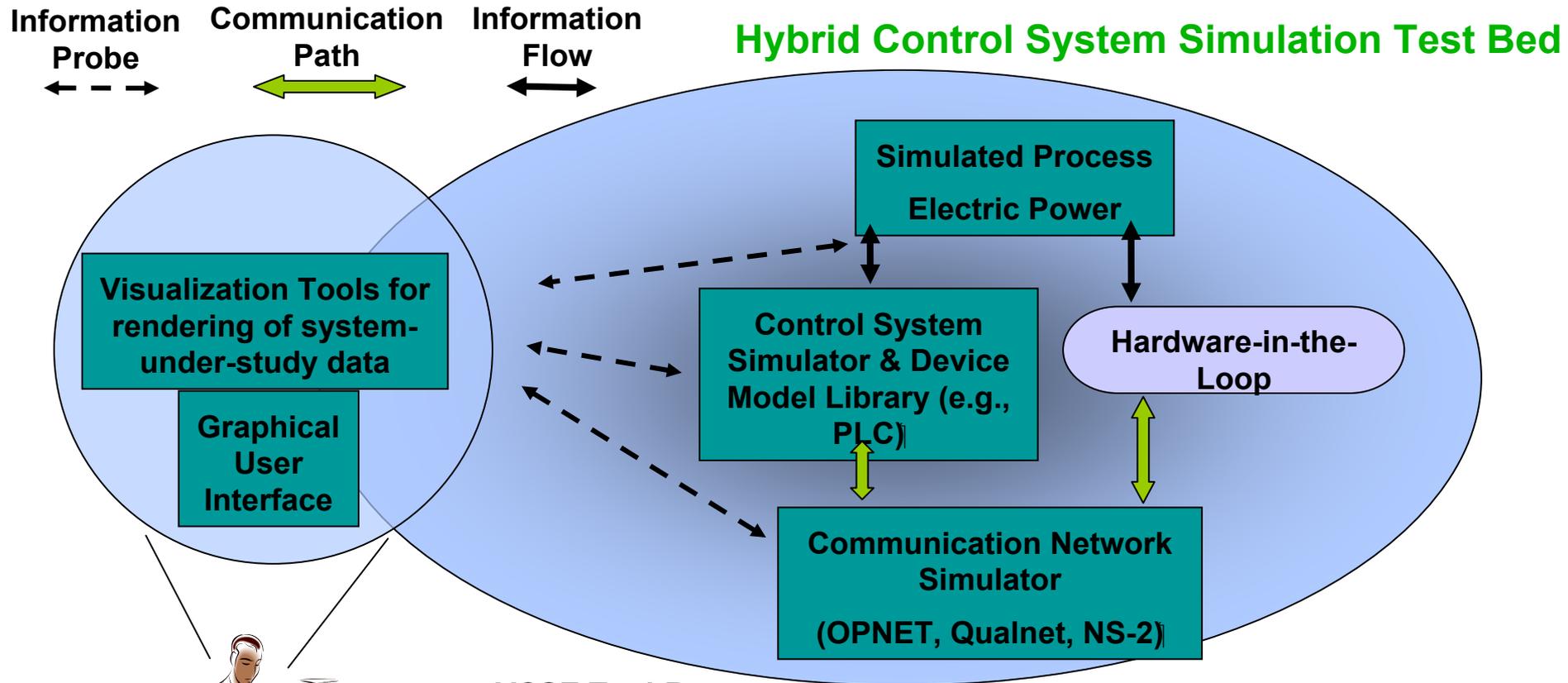


Threat-to-Consequence Risk Model



Provides a Framework for Conducting Risk Analysis

Virtual Control Systems Environment



VCSE Tool-Box

Software Library: Visual simulation tools; PCS devices and network models

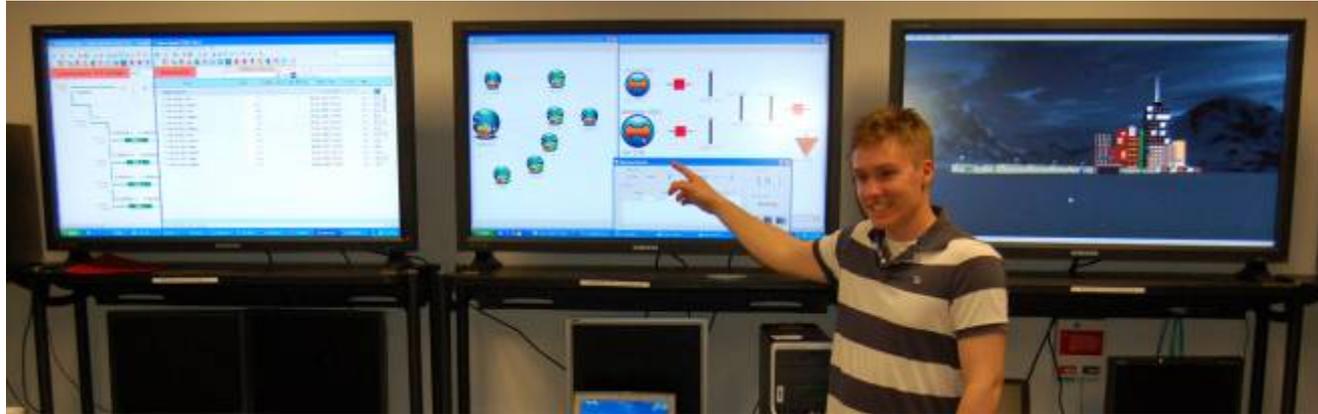
Hybrid Simulation Library: hardware component interfaces; emulated devices

Analysis Library: Analysis and result visualization tools

Power Simulation Library: static and dynamic power models

NSTB Risk Analysis Workshop

Sandia National Laboratories



- More than 40 industry researchers and asset owners
- Engaged in a plausible scenario – **WHAT IS YOUR RISK?**
- “Test drove” risk analysis tools being developed by the National SCADA Test Bed at Sandia National Laboratories such as:
 - Threat Discovery Tool, Virtual Control Systems Environment Impact Analysis, and Consequence Modeling
- Exchanged valuable insight to ensure tools are practical and applicable to meet energy sector cyber risk analysis needs

Red Team/Blue Team Advanced Training

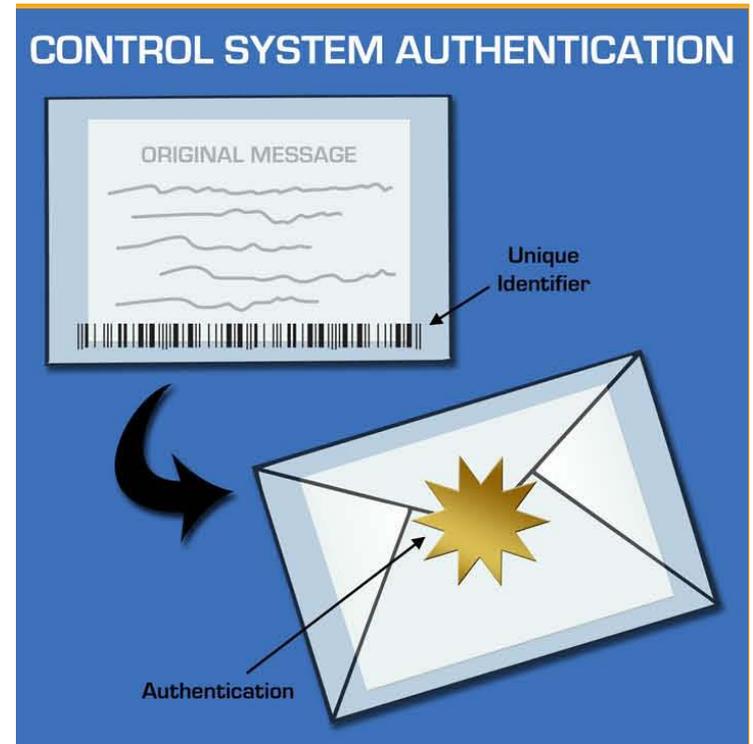
November 3-6, 2008 at Idaho National Laboratory

- Intensive, hands-on training for asset owners and operators
- Participants divided into red team and blue team to attack or defend a simulated electrical control center
- Will demonstrate control system network exploits
- Users can learn and showcase skills in an actual control systems environment
- Owners learn how control system attacks could be launched, why they work, and potential mitigation strategies
- Booked at 42 attendees with more on waiting list



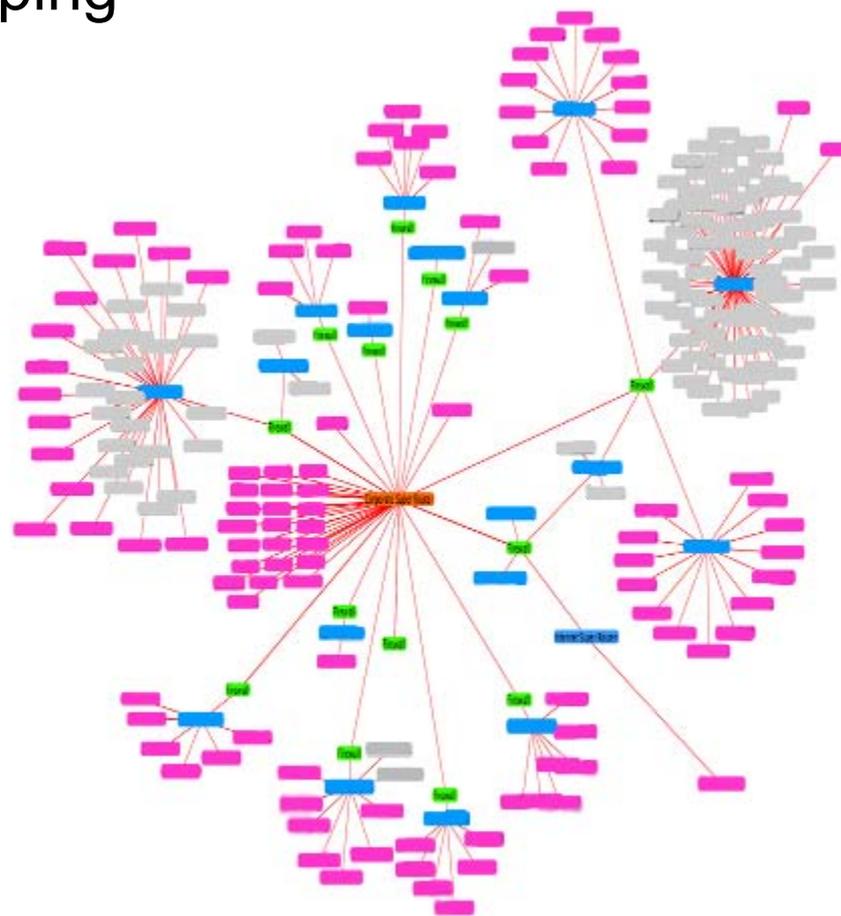
Secure SCADA Communications Protocol

- Trusted communications between remote serial devices and control center
- Embedded solution provides better performance than bump in the wire encryption devices
- Allows operators to continue to read and interpret telemetry data for troubleshooting purposes
- Supports both low and high-bandwidth environments



Advanced Network Toolkit For Assessments and Remote Mapping

- PASSIVE network discovery tool
- Input – various network databases (firewall tables)
- Output – graphical depiction of the network topology
- Benefits - network asset identification; supports implementation of industry standards
- Developed by Sandia National Laboratories



DOE-awarded industry projects to support Energy Roadmap

- 1. Hallmark Project** - commercialize Secure SCADA Communications Protocol (SSCP) - Schweitzer Engineering Laboratories, Pacific Northwest National Laboratory, CenterPoint Energy
- 2. Detection and Analysis of Threats to the Energy Sector (DATES)** – IDS (network, host, and device level), event correlation framework, and a sector-wide, distributed, privacy-preserving repository of security events for participants to automatically contribute *without attribution* - SRI International, ArcSight, Sandia National Laboratories, ERCOT
- 3. Audit and Attack Detection Toolkit** - extend capability of existing vulnerability scanning tools (e.g., Nessus et al) to evaluate SCADA security configuration (supports compliance with standards); develop templates for a security event monitoring system by mining data in PI Systems - Digital Bond, Tenable Network Security, OSIssoft, Constellation Energy, PacifiCorp, TVA
- 4. Lemnos Interoperable Security Program** - conduct testing, validation, and outreach to increase the availability of cost-effective, interoperable security solutions for IP-based communications - EnerNex Corp., Schweitzer Engineering Laboratories, TVA, Sandia National Laboratories
- 5. Protecting Intelligent Distributed Power Grids against Cyber Attacks** - develop risk-based critical asset identification system; an integrated and distributed security systems with optimization to establish the best topology for networking the security components - Siemens Corporate Research, Idaho National Laboratory, Rutgers Center for Advanced Energy Systems

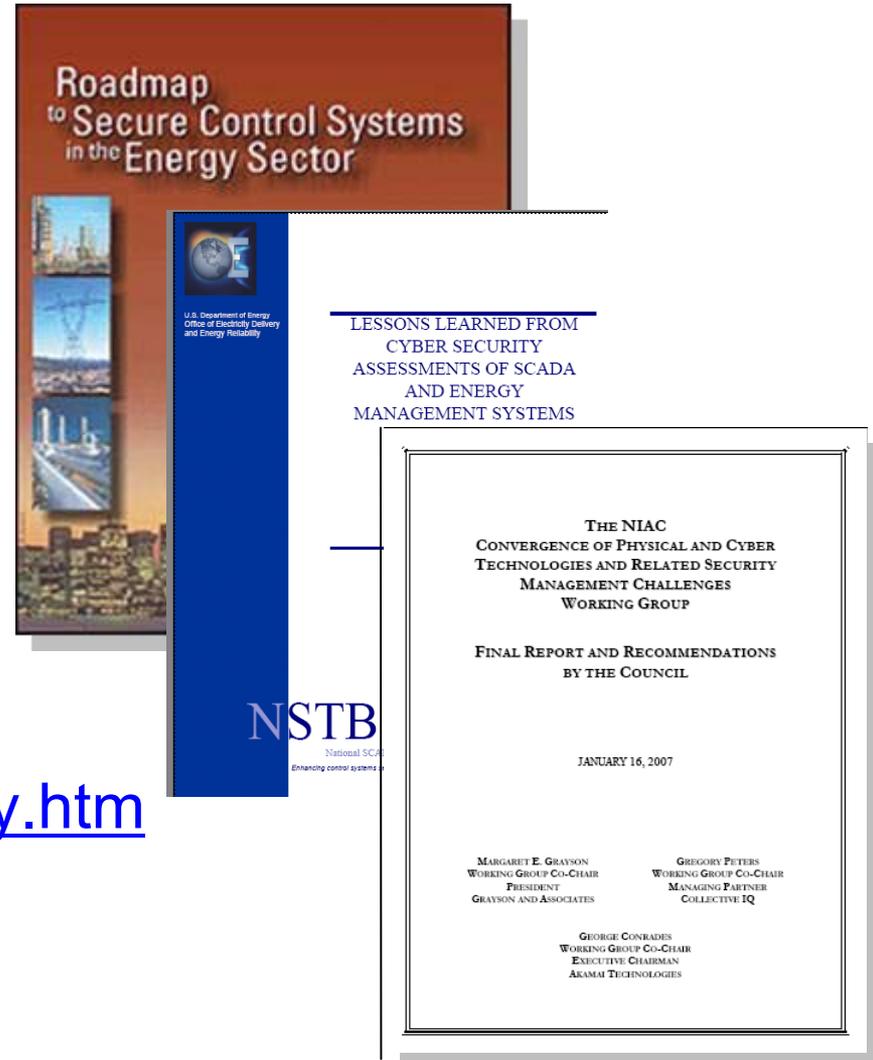
For more info ...

Contact:

Hank Kenchington
US Department of Energy
henry.kenchington@hq.doe.gov
202-586-1878

Visit:

www.oe.energy.gov/controlsecurity.htm





Backup Slides