U.S. Department of Energy

Office of Electricity Delivery and Energy Reliability

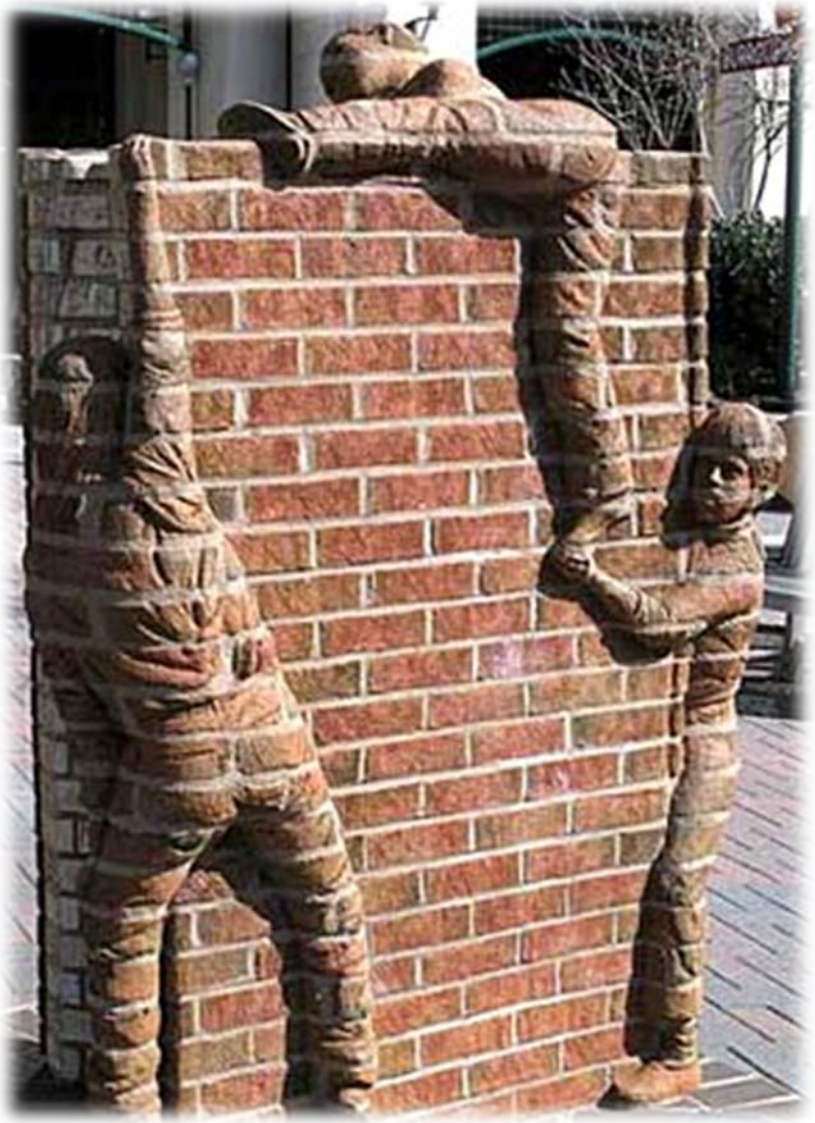
Working to Achieve Cybersecurity in the Energy Sector

"Cybersecurity for Energy Delivery Systems (CEDS)"

Carol Hawk, Ph.D.
Department of Energy

Energy Sector Cybersecurity Challenges

- **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, demand response communication networks



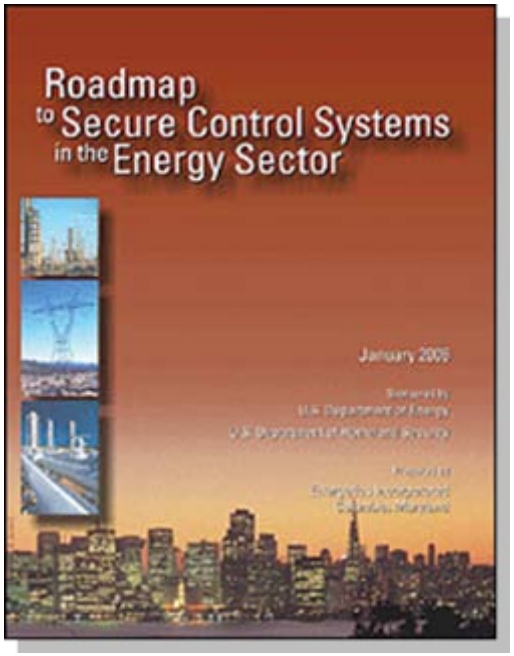
Business/IT Cybersecurity Solutions Can **Break** Energy Delivery Control Systems

Different Priorities

Energy Delivery Control Systems ≠ ***Business/IT Systems***

- **Power systems must operate 24/7 with high reliability and high availability, no down time for patching/upgrades**
- **Energy delivery control system components may not have enough computing resources (e.g., memory, CPU, communication bandwidth) to support the addition of cybersecurity capabilities that are not tailored to the energy delivery system operational environment**
- **Energy delivery control system components are widely dispersed over wide geographical regions, and located in publicly accessible areas where they are subject to physical tampering**
- **Real-time operations are imperative, latency is unacceptable**
- **Real-time emergency response capability is mandatory**

Roadmap – Framework for Public-Private Collaboration

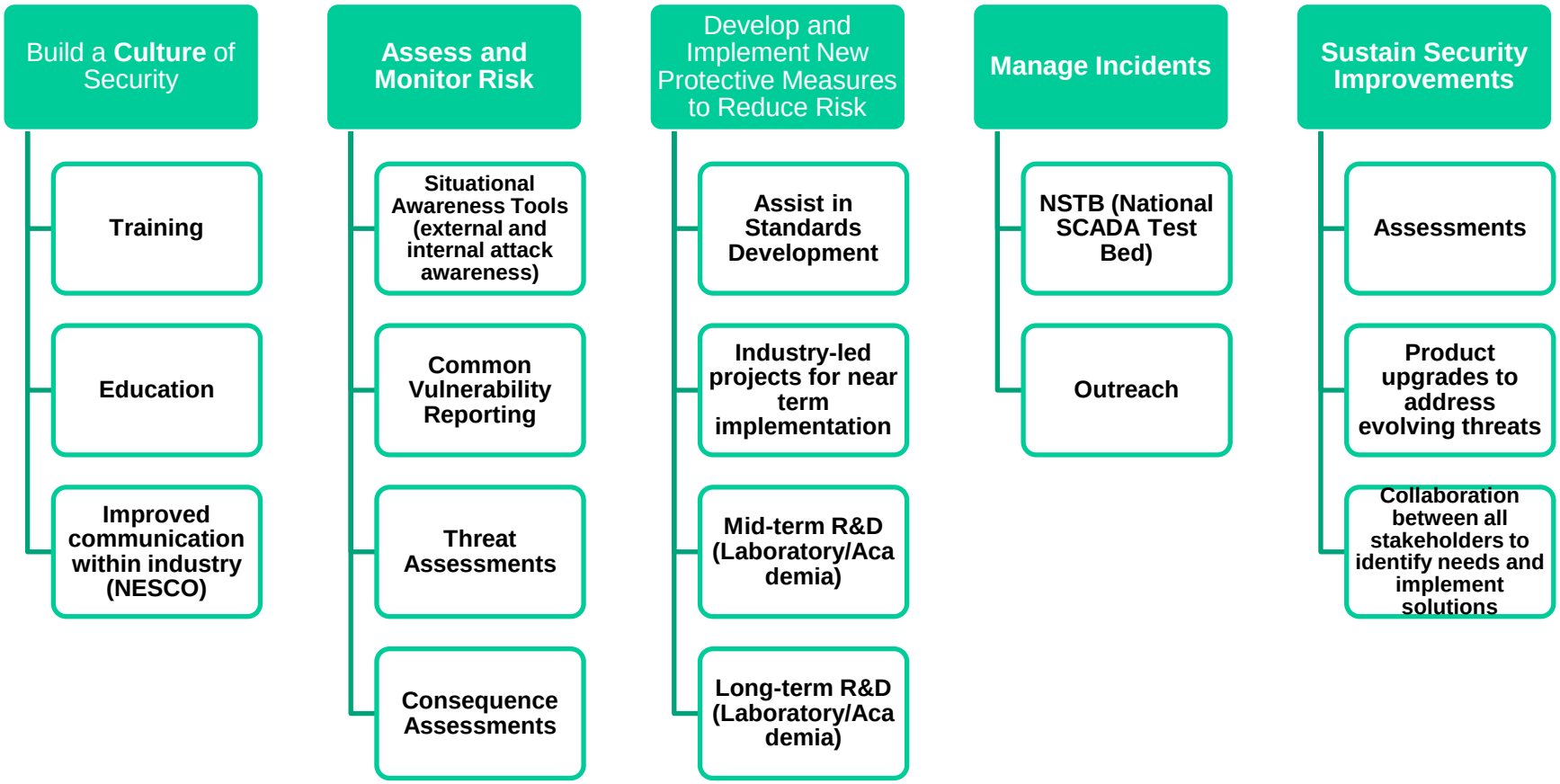


- Published in January 2006/updated 2011
- *Energy Sector's* synthesis of critical control system security challenges, R&D needs, and implementation milestones
- Provides strategic framework to
  - align activities to sector needs
  - coordinate public and private programs
  - stimulate investments in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

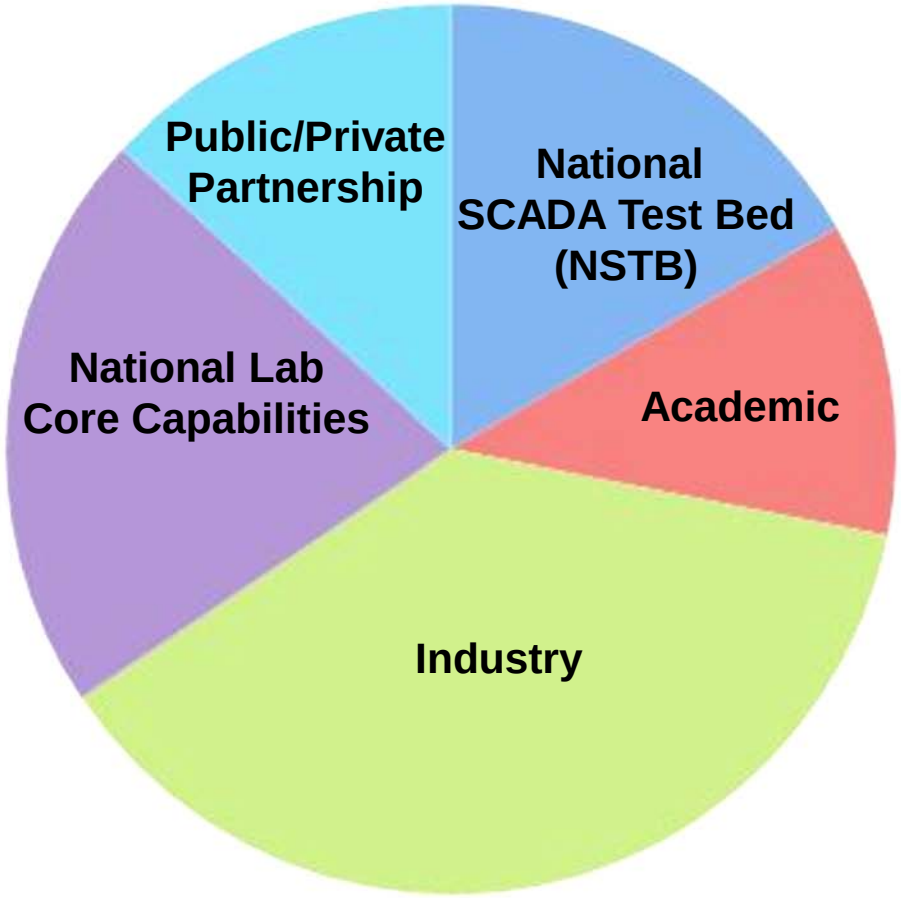
Roadmap Vision

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.

Strategic Framework



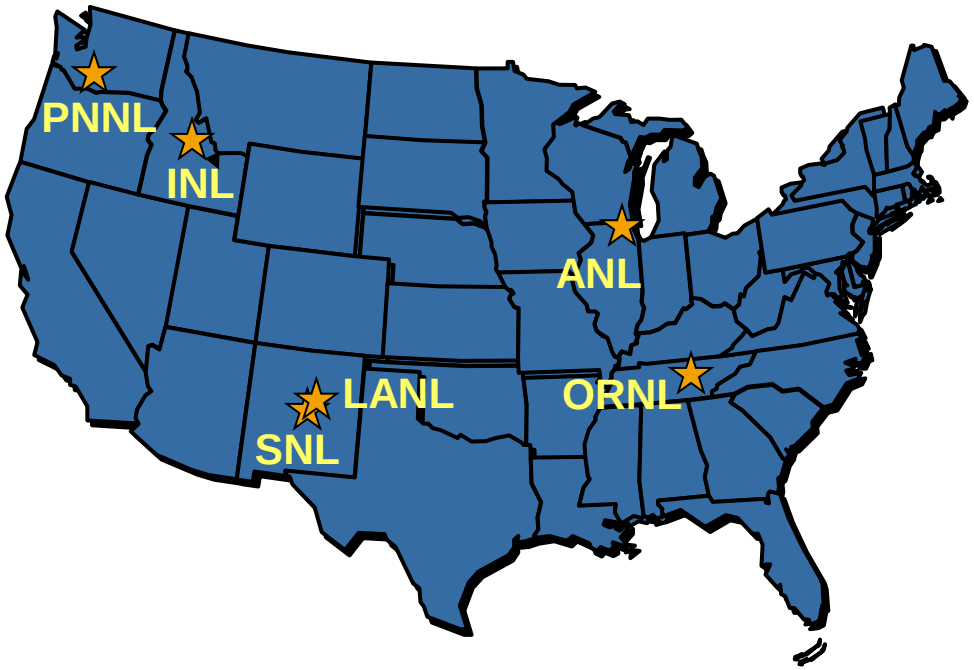
Cybersecurity for Energy Delivery Systems (CEDS) Program—5 Key Areas



DOE National SCADA Test Bed (NSTB)

DOE multi-laboratory program . . . established 2003

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



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

Bruce Schneier, Beyond Fear

DOE National SCADA Test Bed (NSTB)
System Vulnerability Assessments - SCADA/EMS

- **Completed assessments of 38 vendor control systems and associated components on-site at utility field installations and at the INL SCADA Test Bed facility**

Detroit Edison
A DTE Energy Company

AREVA

SIEMENS

TELVENT

GE Energy

TELTONE®

ABB

AMERICAN TRANSMISSION COMPANY®

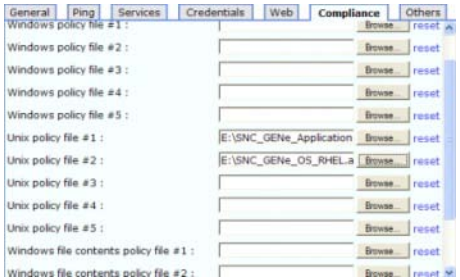
OSIsoft.

OSI
opening your world

CEDS—Industry Accomplishments

- Hallmark Cryptographic Serial Communication
  - → Commercialized technologies that provide secure communications between remote devices and control centers

- Bandolier Security Audit Files
  - → Enables asset owners using the Nessus vulnerability scanner to optimize security configurations of their control systems



- Lemnos Interoperable Security
  - → Developed and demonstrated an interoperability configuration profile for creating a secure communications channel between two control system networks operated by different vendors

CEDS—Academia Accomplishments

Trustworthy Cyber Infrastructure for the Power Grid (TCIPG)

Architecture for End-to-End Resilient, Trustworthy & Real-time Power Grid Cyber Infrastructure

Recent Papers

Smart-Grid –Enabled Load and Distributed Generation as a Reactive Resource

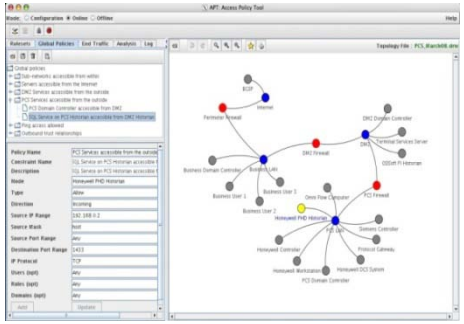
Katherine M. Rogers, *Student Member, IEEE*, Ray Klump, *Member, IEEE*, Hemanshu Khurana, *Senior Member, IEEE*, Thomas J. Overbye, *Fellow, IEEE*

Building Security In

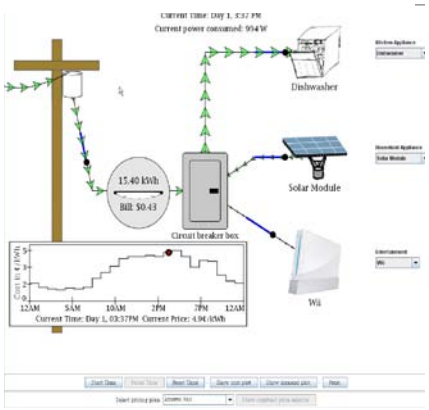
Editors: John Steven, jsteven@cigital.com
Gunnar Peterson, gunnar@arctecgroup.net
Deborah A. Frincke, deborah.frincke@pnl.gov

Smart-Grid Security Issues

TCIPG NetAPT Network Access Policy Tool (adopted by utility in Spring 2010)



Applets for Schools



Facilities

Test bed combining power grid hardware and software with sophisticated simulation and analysis tools

University of Illinois • Dartmouth College • University of California at Davis• Washington State • University Cornell University

NEW CEDS Activities

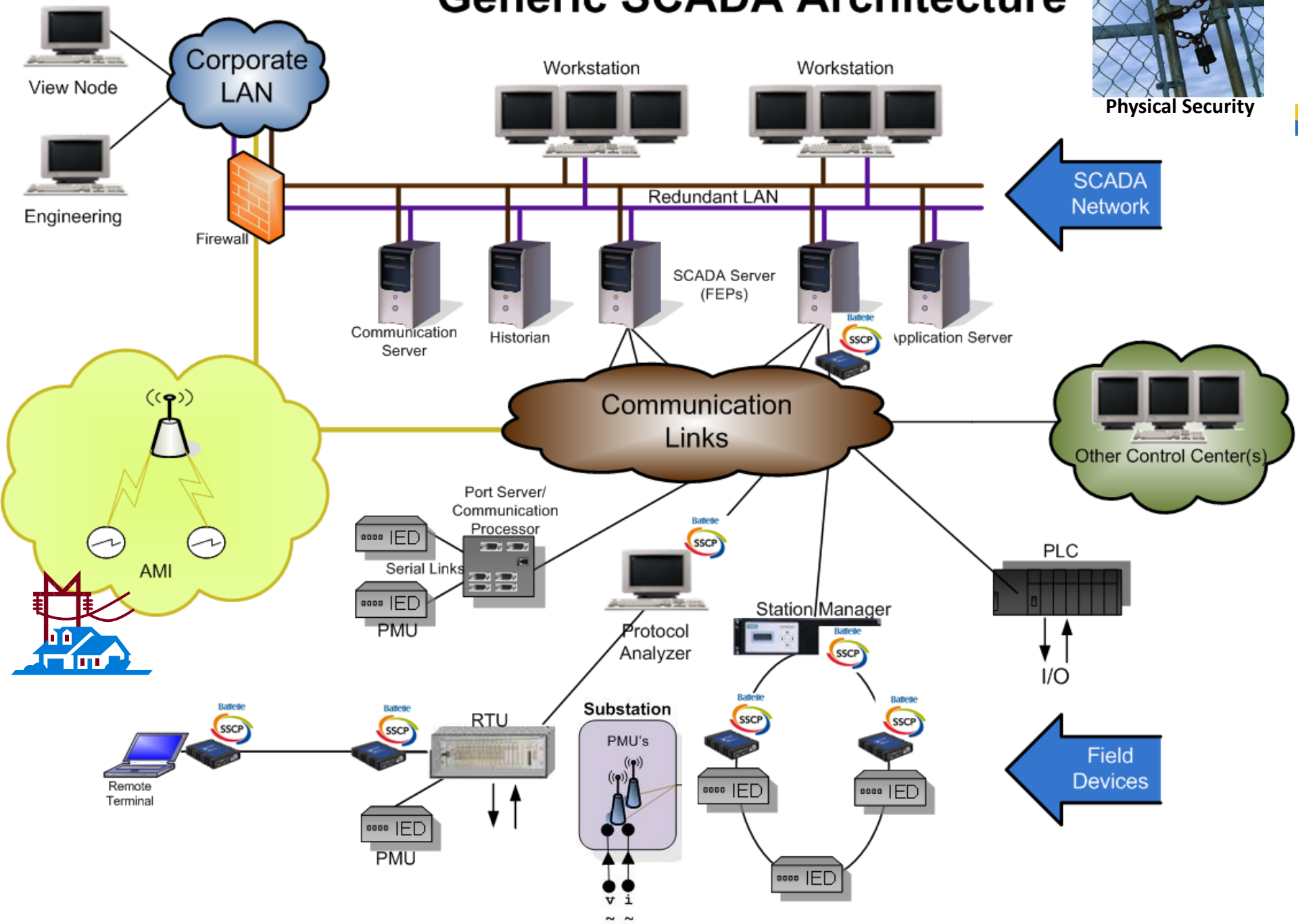
13 CEDS projects started in 2010 to help harden the U.S. energy infrastructure against cyber intrusion

8 Industry-led projects

5 National Laboratory-led projects

Generic SCADA Architecture

Physical Security



Industry-Led Projects

1. **Watchdog –** Develop a Managed Switch for the control system local area network (LAN) that uses whitelist filtering and performs deep packet inspection→**Schweitzer Engineering Laboratories**, *CenterPoint Energy Houston Electric, Pacific Northwest National Laboratory*

2. **Whitelist Anti-Virus for Control Systems -** Develop a whitelist anti-virus solution for control systems integrated with substation-hardened computers and communication processor→**Schweitzer Engineering Laboratories**, *Dominion Virginia Power, Sandia National Laboratories*

3. **Security Core Component -** Develop a near-real-time cyber and physical security situational awareness capability for the control system environment→**Siemens Energy Automation**, *Sacramento Municipal Utilities District, Pacific Northwest National Laboratory.*

4. **Role Based Access Control -Driven (RBAC) Least Privilege Architecture for Control Systems** - Develop a least-privilege architecture for control systems that is driven by role-based access control (RBAC)→**Honeywell International**, *University of Illinois, Idaho National Laboratory*

Industry-Led Projects

5. **Tools and Methods for Hardening Communication Security of Energy Delivery System** - Research vulnerabilities in energy sector communication protocols and develop mitigations that harden these protocols against cyber attack while enforcing proper communications→**Telcordia Technologies**, *University of Illinois, Electric Power Research Institute, DTE Energy.*

6. **SIEGate** - Develop a Secure Information Exchange Gateway (SIEGate) that provides secure communication of data between control centers→**Grid Protection Alliance**, *University of Illinois, Pacific Northwest National Laboratory, PJM, AREVA T&D.*

7. **Centralized Cryptographic Key Management** - Develop a cryptographic key management capability scaled to secure communications for the millions of smart meters within the smart grid advanced metering infrastructure→**Sypris Electronics**, *Purdue University Center for Education and Research in Information Assurance and Security, Oak Ridge National Laboratory, Electric Power Research Institute*

8. **Padlock** - Develop a low-power, small-size dongle (or plug-in device) that provides strong authentication, logging, alarming, and secure communications for intelligent electronic devices (IED) in the field operating at the distribution level→**Schweitzer Engineering Laboratories**, *Tennessee Valley Authority, Sandia National Laboratories*

National Laboratory-Led Projects

1. **High-Level (4th Gen) Language Microcontroller Implementation**—limits direct access to device memory and hardens microcontrollers against low-level cyber attacks→ **Idaho National Laboratory**, *Siemens Corporate Research*

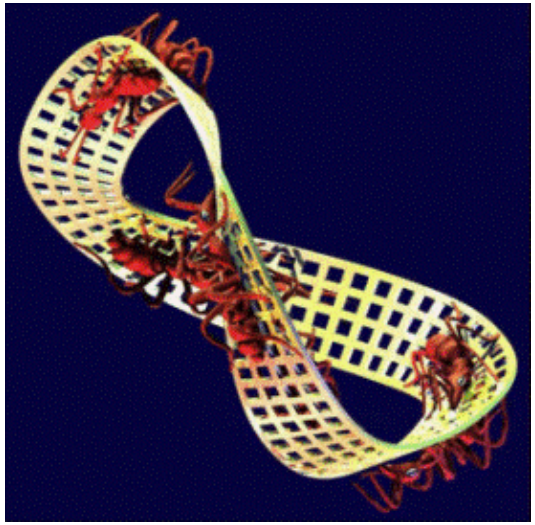
2. **Control Systems Situational Awareness Technology Interoperable Tool Suite**—a situational awareness tool suite for control systems that will show network communications, collect wireless mesh network data message routes, report unexpected behavior, monitor system health, distinguish between component failure and cybersecurity incidents, perform data fusion and determine global effects for local firewall rules→ **Idaho National Laboratory**, *Idaho Falls Power, Austin Energy, Argonne National Laboratory, University of Illinois, Oak Ridge National Laboratory, University of Idaho*

3. **Automated Vulnerability Detection for Compiles Smart Grid Software**—automated vulnerability detection for static analysis of compiled software and device firmware→ **Oak Ridge National Laboratory**, *Software Engineering Institute, University of Southern Florida, EnerNex Corporation*

National Laboratory-Led Projects

4. **Next Generation Secure, Scaleable Communication Nework for the Smart Grid**—a secure, scalable communication network for the smart grid using an adaptive hybrid spread-spectrum modulation format to provide superior resistance to multipath, noise, interference, and jamming→ **Oak Ridge National Laboratory**, *Pacific Northwest National Laboratory, Virginia Tech, OPUS Consulting, Kenexis Consulting.*

5. **Bio-Inspired Technologies for Enhancing Cybersecurity in the Energy Sector**—bio-inspired technologies using lightweight, mobile agents (Digital Ants) across multiple organizational boundaries found in smart grid architectures to correlate activities, produce emergent behavior, and draw attention to anomalous conditions → **Pacific Northwest National Laboratory**, *Wake Forest University, University of California-Davis, Argonne National Laboratory, SRI International*.



For more information …

Contact:

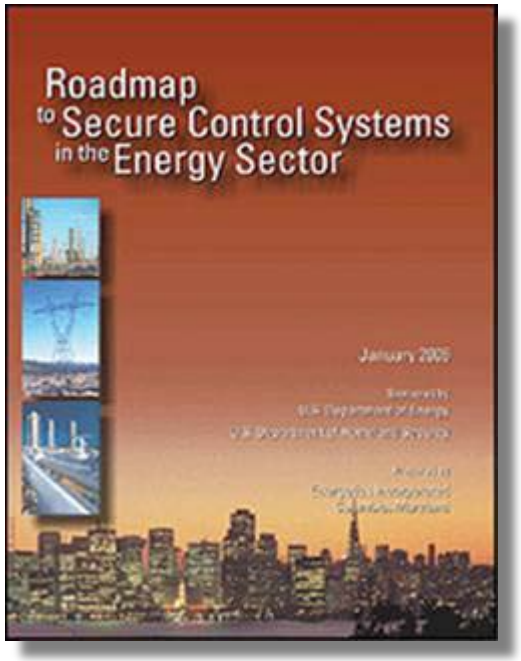
US Department of Energy

Carol Hawk
Carol.Hawk@hq.doe.gov
202-586-3247

Diane Hooie
Diane.Hooie@netl.doe.gov
304-285-4524

Visit:

www.oe.energy.gov/controlsecurity.htm

www.controlsystemsroadmap.net

ie Roadmap
interactive energy Roadmap to secure control systems