

Cyber Security of the Electric Power Grid

Jeff Dagle, PE
Chief Electrical Engineer
Energy Technology Development Group
Pacific Northwest National Laboratory
(509) 375-3629
jeff.dagle@pnl.gov

IEEE Power Systems Conference & Exposition
Seattle, WA
March 17, 2009

Outline

- ▶ Setting the context for challenges associated with control system security in the electricity sector
- ▶ Government efforts to address critical infrastructure protection for the electricity sector
- ▶ An overview of the Department of Energy's (DOE) National SCADA Test Bed Program
- ▶ An overview of the North American Electric Reliability Corporation (NERC) critical infrastructure protection efforts
- ▶ The “top 10” control system vulnerabilities in the electricity sector

Electric Power Grid Faces Major Challenges

Today

- 49% coal
- 20% natural gas
- 19% nuclear
- 7% hydro
- 4% renewable, misc.

• 1,000,000 MW

- 140 control areas
- 350,000 miles transmission lines
- ~10 million DG units

- Aging Infrastructure
- Growing threats to cyber & physical assets

Changing Supply Mix

Growing Demand Requirements

Increasing Grid Complexity

Increasing Energy Infrastructure Vulnerability

2035

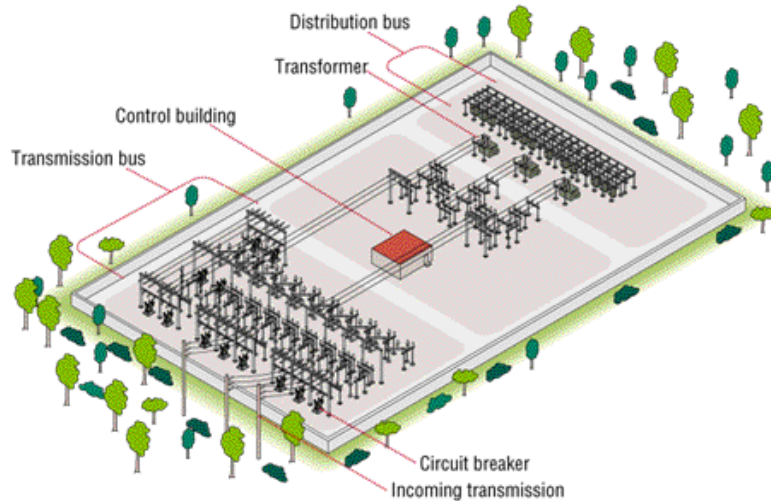
- Renewables increasing
- Nuclear increasing
- Fossil fuels decreasing

- 50% demand growth
- Increased load peaking
- More sensitive equipment
- Higher power quality demands

- More control area nodes
- More transmission lines needed
- >20 million DG units

- Increased interdependencies of electric & energy systems
- Material & resource limitations
- Increased use of automated controls

Supervisory Control and Data Acquisition (SCADA)



- Generator Set Points
- Transmission Lines
- Substation Equipment



- Critical Operational Data
- Performance Metering
- Events and Alarms

Communication Methods

- Directly wired
- Power line carrier
- Microwave
- Radio (spread spectrum)
- Fiber optic



Control Center

Displays network status, enables remote control, optimizes system performance, facilitates emergency operations, dispatching repair crews and coordination with other utilities.

SCADA is used extensively in the electricity sector. Other SCADA applications include gas and oil pipelines, water utilities, transportation networks, and applications requiring remote monitoring and control. Similar to real-time process controls found in buildings and factory automation.

What makes control system security unique?

Control Systems

- ▶ Top priority is reliability and safety, not security
- ▶ Breaches in security can have physical consequences
- ▶ Traditionally relied on implicit trust with isolated systems
- ▶ Vendors provide “turn key” systems with remote support access
- ▶ Default passwords are commonplace



Computer Security

- ▶ Traditional IT security tools may not work for control systems
- ▶ Enterprise networks are being connected to control systems
- ▶ Control system security issues may be overlooked because they are not managed by IT security



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



The Emerging Cyber Threat

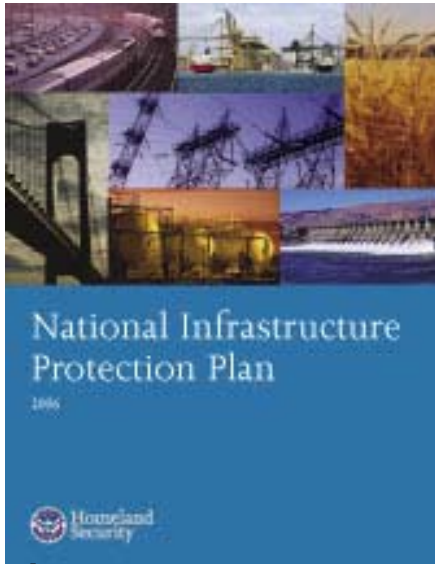
- ▶ Industry has long history of planning for and coping with natural disasters and other reliability events
 - Through industry standard operating procedures, there is much effort expended to reduce likelihood of cascading outages leading to widespread blackouts
- ▶ Historically, cyber security focused on countering unstructured adversaries
 - e.g., individuals, untargeted malicious software, human error
- ▶ Very little protection against structured adversaries intent on exploiting vulnerabilities to maximize consequences
 - e.g., terrorist groups, organized crime, nation states
 - Insider threat remains very challenging, can be used as part of structured threat vector
- ▶ New possibilities for widespread sustained outages resulting from cyber attack are now being contemplated
 - But industry still not ready to cope with this threat

Homeland Security Presidential Directive 7 Framework for National Critical Infrastructure Protection

Sector-Specific Agency	Critical Infrastructure/Key Resources Sector
Department of Agriculture ¹ Department of Health and Human Services ²	Agriculture and Food
Department of Defense ³	Defense Industrial Base
Department of Energy	Energy ⁴
Department of Health and Human Services	Public Health and Healthcare
Department of the Interior	National Monuments and Icons
Department of the Treasury	Banking and Finance
Environmental Protection Agency	Drinking Water and Water Treatment Systems
Department of Homeland Security <i>Office of Infrastructure Protection</i>	Chemical Commercial Facilities Dams Emergency Services Commercial Nuclear Reactors, Materials, and Waste
<i>Office of Cyber Security and Telecommunications</i>	Information Technology Telecommunications
<i>Transportation Security Administration</i>	Postal and Shipping
<i>Transportation Security Administration, United States Coast Guard⁵</i>	Transportation Systems ⁶
<i>Immigration and Customs Enforcement, Federal Protective Service</i>	Government Facilities

- DHS is responsible for coordinating overall national efforts
- DOE is Sector Specific Lead Agency for Energy

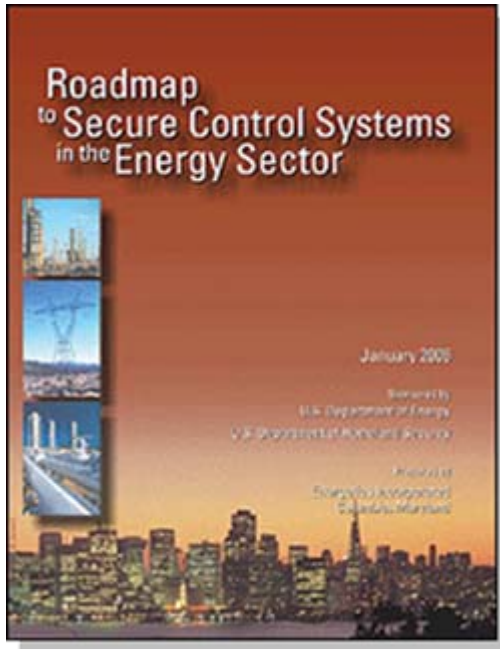
National Infrastructure Protection Plan (NIPP) Sector-Specific Plans (SSP)



- ▶ Detail the application of the NIPP risk management framework across each sector
- ▶ Are tailored to address the unique characteristics and risk landscapes of each sector
- ▶ Sector-Specific Agencies (SSAs) partner with Sector Coordinating Councils (SCCs) and Government Coordinating Councils (GCCs) to develop and implement the SSPs for the overall NIPP

**Sector-Specific
Plans (17)**

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 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>Secure connectivity between business systems and control systems within corporate network (2009)</p>	<p>Cyber incident response is part of emergency operating plans at 30% of control systems (2008)</p>	<p>Compelling, evidence-based business case to increase private investment in control system security (2007)</p>
<p>Fully automated security state and common response of control system networks (2015)</p>	<p>Secure control system architectures produced with built-in, end-to-end security (2015)</p>	<p>Self-configuring control system network architectures are in production (2015)</p>	<p>Cyber security awareness, outreach, and education programs integrated into energy sector operations (2015)</p>

Interactive Energy Roadmap (ieRoadmap)



Web-based Tool Tracks R&D Projects

Secure SCADA Communications Protocol

Safe Mapping and Reporting Tool (SMART)

Security Metrics for EMS

SCADA Honeynet

Survivability and Recovery of Process Control Systems - RiskMAP

Lead Organization:	I3P
Principal Investigator:	MITRE
Contact Name:	Jim Watters
Contact Email:	jwatters@mitre.org
Contact Phone:	781-271-2162
Last Edited:	2/19/2008 4:26:55 PM
Project Start Date:	4/2007
Funding To Date:	\$100K-\$500K
Technology Readiness:	Ready for Release
Project Participants:	MITRE
Project Description:	RiskMAP is a proven Risk-to-Mission Assessment Process tool that models key features of a corporation from the business objectives to the operational tasks and information assets needed to achieve them, to the network nodes that store, send and make the information available. RiskMAP uses the same model to map risks at the network level up to the business objectives level providing the corporate executive with solid, credible support for risk mitigation decisions.
Preliminary Results/Deliverables:	The first commercial tool using RiskMAP technology is in development by Matrikon, Inc
Website:	http://www.thei3p.org/projects/pcs07overview.html
Project Mapped To:	Roadmap challenges in the following areas: Measure and Assess Security Posture, Develop and Integrate Protective Measures, and Sustain Security Improvements

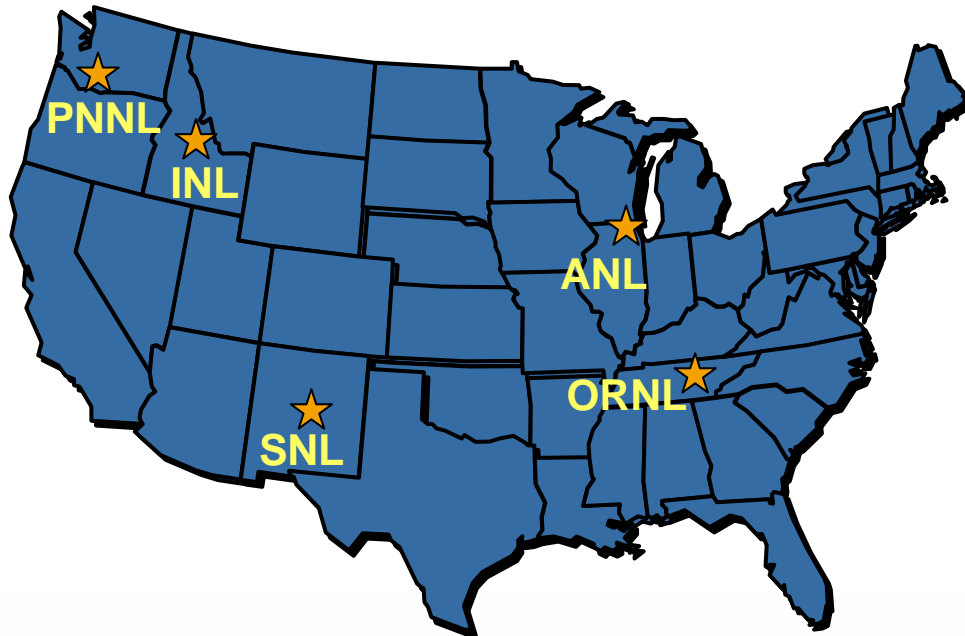
- Over 80 control systems R&D projects mapped to the Roadmap
- Helps identify active areas and exposes gaps in R&D
- Helps R&D partners collaborate and leverage resources
- Informs owners and operators of emerging technologies

www.pcsforum.org/roadmap

DOE National SCADA Test Bed (NSTB)

DOE multi-laboratory program ...established 2003

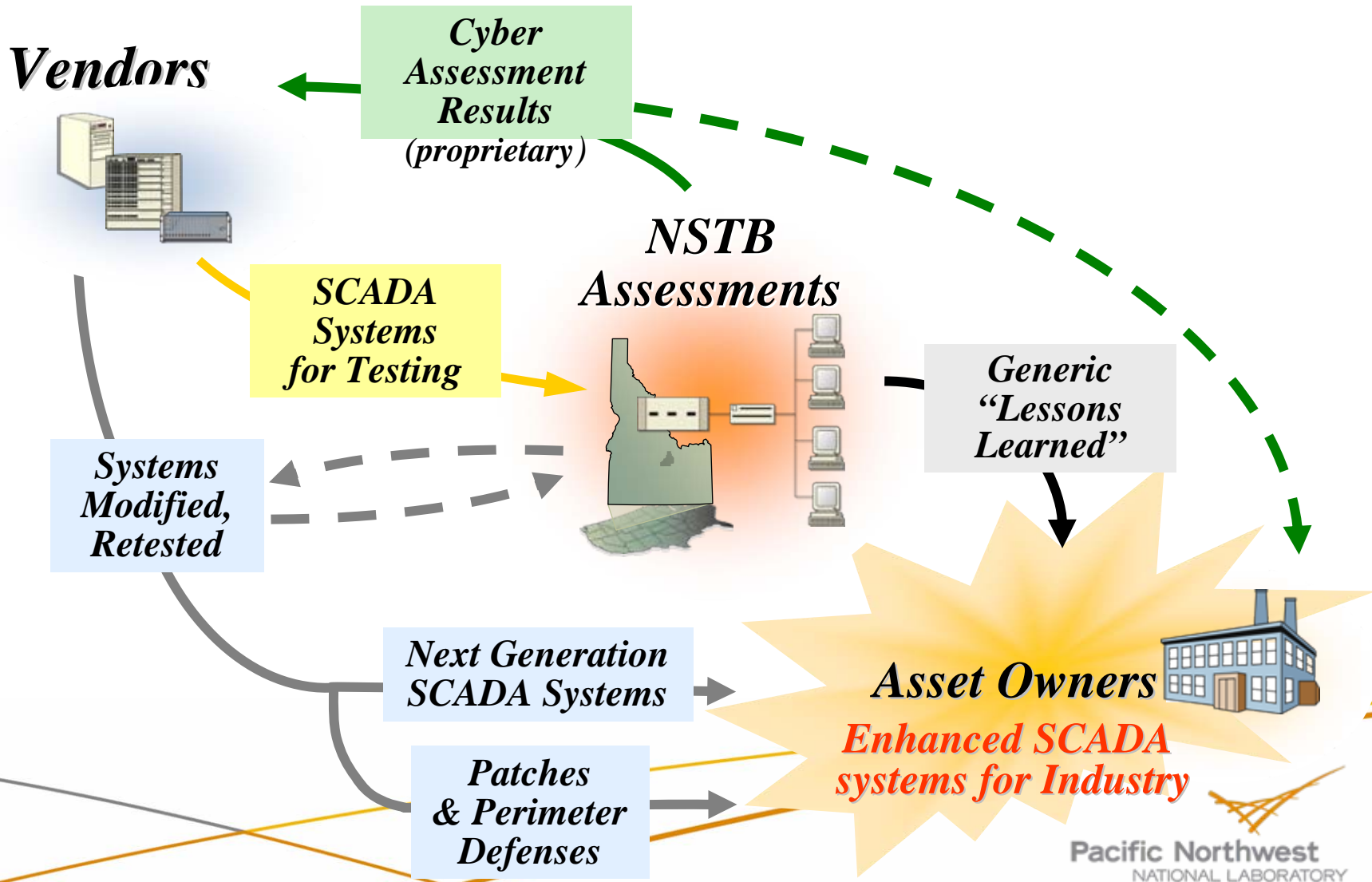
Supports industry and government efforts to enhance cyber security of control systems in energy sector



Key Program Elements

- Energy control systems vulnerability assessments and recommended mitigations
- Integrated risk analysis
- Secure next generation control systems technology R&D
- Public-private partnership, outreach, and awareness

Enhanced-Security SCADA Systems are in the Marketplace....Today!



North American Electric Reliability Corporation (NERC)

- ▶ Provides liaison and coordination for the electricity sector
 - Operates the Electricity Sector Information Sharing and Analysis Center (ES-ISAC) - <http://www.esisac.com/>
 - Critical Infrastructure Protection Committee (CIPC) is the primary focal point, with various working groups
- ▶ Security Standards and Guidelines
 - CIP-001 “Sabotage Reporting”
 - CIP-002 through CIP-009 “Cyber Security Standards”
- ▶ With Energy Policy Act of 2005, reliability standards (including security standards) are now mandatory
- ▶ NERC has been involved in many other initiatives, exercises, and activities over the past several years

Top 10 Control System Vulnerabilities

Prepared by the NERC CIPC Control System Security Working Group

1. Inadequate policies, procedures, and culture that govern control system security
2. Inadequately designed control system networks that lack sufficient defense-in-depth mechanisms
3. Remote access to the control system without appropriate access control
4. System administration mechanisms and software used in control systems are not adequately scrutinized or maintained
5. Use of inadequately secured wireless communication for control

Top 10 Control System Vulnerabilities

Prepared by the NERC CIPC Control System Security Working Group

6. Use of a non-dedicated communications channel for command and control and/or inappropriate use of control system network bandwidth for non-control purposes
7. Insufficient application of tools to detect and report on anomalous or inappropriate activity
8. Unauthorized or inappropriate applications or devices on control system networks.
9. Control systems command and control data not authenticated
10. Inadequately managed, designed, or implemented critical support infrastructure

Summary

- ▶ Cyber attacks can create service disruptions, and this trend is becoming more prevalent
- ▶ While recent industry-developed cyber security standards are a good start, more needs to be done to:
 - Reduce discretion
 - Eliminate loopholes
 - Provide more uniformity
- ▶ Much less staffing within industry than historic levels
 - Staffing shortfalls in certain disciplines becoming acute
- ▶ Information sharing not fully effective
 - Despite efforts to enhance public-private partnerships
 - Need meaningful vehicles for information exchange
- ▶ Fundamental need for new technologies with inherent security