A presentation from the 2009 Topical Symposium:

Energy Security: A Global Challenge

Hosted by:
The Institute for National Strategic Studies
of
The National Defense University

29-30 September 2009

By
JEFFREY DAGLE

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
30 SEP 2009		**00-00-2009 to 00-00-2009**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Summary of Cyber Security Issues in the Electric Power Sector	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Pacific Northwest National Laboratory,Energy Technology Development Group,P.O. Box 999,Richland,WA,99352**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
2009 Topical Symposium: Energy Security: A Global Challenge, 29-30 Sep 2009, Washington DC

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**12**	

Summary of Cyber Security Issues in the Electric Power Sector

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

Energy Grid Security Panel
Energy Security: A Global Challenge
Symposium hosted by National Defense University
September 30, 2009

Pacific Northwest
NATIONAL LABORATORY

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
- Smart Grid security considerations
- The path forward

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

Pacific Northwest
NATIONAL LABORATORY

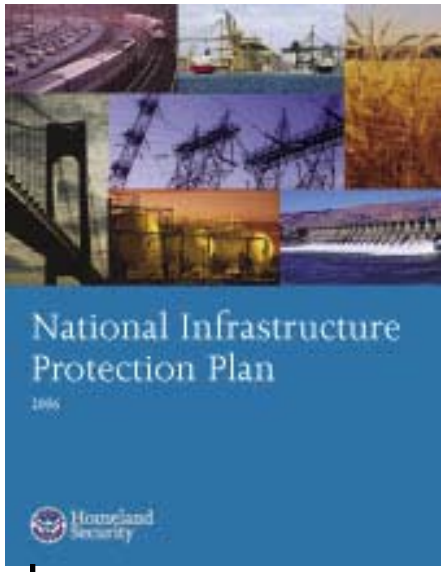
Trends Impacting Control System Security

- **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

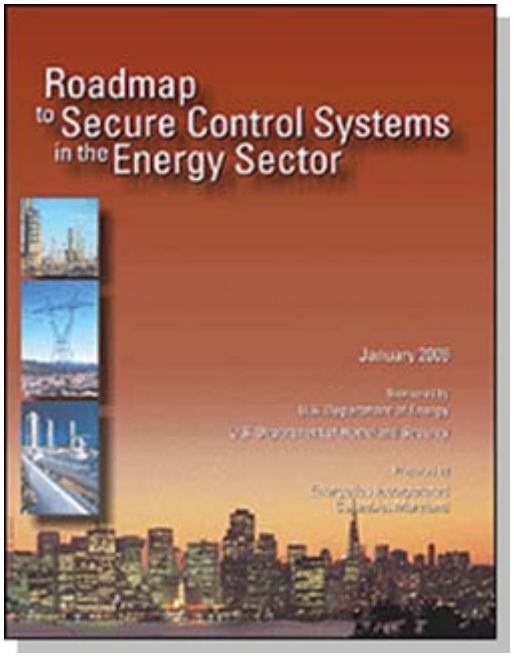
- Industry has long history of planning for and coping with natural disasters and other reliability events
  - Through industry standard operating procedures, there is much effort expended to reduce likelihood of cascading outages leading to widespread blackouts
- Historically, cyber security focused 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

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

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

Available from:
http://www.oe.energy.gov/controlsecurity.htm

Roadmap Vision

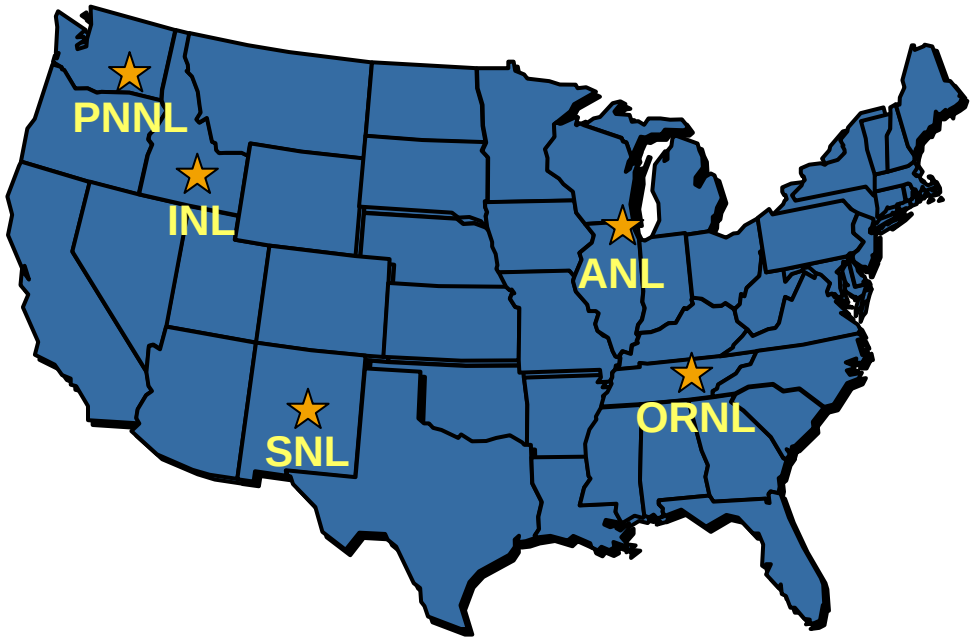
In 10 years, control systems for critical applications will be designed, installed, operated, and maintained to ***survive*** an intentional cyber assault with no loss of critical function.

Pacific Northwest
NATIONAL LABORATORY

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

Pacific Northwest
NATIONAL LABORATORY

Identifying Risks of Implementing Smart Grid Systems (an All Hazards Approach)

- Complexity
  - Introduces potential vulnerabilities
  - More access points (increased exposure)
  - Difficult to manage a complex system
- Power system would be more vulnerable to communication (or software) disruptions
  - Denial of service (e.g., unintentional load shedding)
  - Potential for common failure modes across connected systems
  - Software/system integrity (e.g., firmware, logic bomb, supply chain, etc.)
- Intelligence gathering tool for the adversary
- Potential for breach of customer privacy
- Implementation issues
  - Inappropriate or premature mandating of technologies that aren't appropriate for the application
  - Potential for technology obsolescence

Mitigating Smart Grid Implementation Risks

- Develop security controls
  - Policies, procedures, control baselines, reference architectures, conformance and interoperability testing, certification
- Need built-in (rather than bolt-on) security
- Apply good security practices
  - Follow best practices, established standards when available
- Apply defense-in-depth concepts
  - Redundancy, zones, proxies, role-based authority, etc.
- Instill a culture of security
  - Training, awareness, adequate resources, management support
- Develop transition strategy that maximizes interoperability, security, reliability, etc.
- Forensics and enforcement
- Establish trusted technology supply chain

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