SANS SCADA Conference 2012

Progress in implementing the
“Roadmap to Achieve Energy Delivery Systems Cybersecurity”

Hank Kenchington
Deputy Assistant Secretary R&D
Office of Electricity Delivery and Energy Reliability
Department of Energy
Electric Grid – *Electricity + ICT*

1. Power System Infrastructure

2. Information Infrastructure

Source: Electric Power Resource Institute (EPRI)
2011 NERC Risk Ranking and Evolution

Reference: 2011 Long-Term Reliability Assessment (Fig. 43, pg. 73), North American Electric Reliability Corporation, November 2011.
The United States cannot succeed in securing cyberspace if it works in isolation. The Federal government should enhance its partnership with the private sector.

The public and private sectors’ interests are intertwined with a shared responsibility for ensuring a secure, reliable infrastructure.

*White House Cyberspace Policy Review, May 2009*
2006 Roadmap – a “framework for participation”

- Based on energy stakeholder needs
- Provides strategic framework to:
  - align activities to common goal
  - coordinate public and private activities
  - stimulate investments in control systems security
- Recognized by:
  - White House Cyberspace Policy Review
  - President’s National Infrastructure Advisory Council
  - NERC Critical Infrastructure Protection Committee

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.
# 2006 Roadmap – Key Strategies & Goals

<table>
<thead>
<tr>
<th>Measure and Assess Security Posture</th>
<th>Develop and Integrate Protective Measures</th>
<th>Detect Intrusion &amp; Implement Response Strategies</th>
<th>Sustain Security Improvements</th>
</tr>
</thead>
<tbody>
<tr>
<td>...fully automated security state monitoring and control systems networks with real-time remediation</td>
<td>...new systems with built-in, end-to-end security will replace older legacy systems</td>
<td>...systems provide contingency and remedial actions in response to attempted intrusions</td>
<td>...effective incentives to accelerate investment in secure control system technologies and practices</td>
</tr>
</tbody>
</table>
Public-Private Working Group Oversees Roadmap Implementation

Critical Infrastructure Partnership Advisory Council

Electricity Sub-Sector Coordinating Council

Government Energy Coordinating Council

Oil & Natural Gas Sub-Sector Coordinating Council

- ERCOT
- Ergon Refining, Inc.
- FERC
- ISEO - Ontario
- NERC
- Progress Energy
- Western Refining
- Alyeska Pipeline
- BP
- Department of Energy
- DHS
- Edison Electric Institute
- El Paso Corporation
Tangible progress to reduce cyber risks since 2006

*An extensive list of achievements and ongoing activities is available in Appendix B of the 2011 Roadmap to Achieve Energy Delivery Systems Cybersecurity*

**Measure and Assess Security Posture**
- Over 37 vulnerability assessments of SCADA systems and components – “hardened” systems now available and being deployed (INL)
- Bandolier Security Audit Files by Digital Bond enable asset owners to audit/optimize the security configurations of control systems (Digital Bond, Inc.)
- Developed guide for vulnerability assessments per NERC CIP standards (SNL)

**Develop and Integrate Protective Measures**
- Hallmark – secure SCADA communications protocol developed and commercialized (PNNL and SEL, Inc.)
- Lemnos - interoperable configuration profile for creating secure communications channels between various vendor products (SNL, Enernex, SEL Inc.)
- ASAP-SG security profiles for AMI, third-party data access, DA et al

**Detect Intrusion and Implement Response Strategies**
- ICS-CERT established by DHS to address threats and vulnerabilities
- NESCO/NESCOR – information sharing community; testing protocols; vulnerability analysis of smart grid technologies (e.g., SEP 1.x)
- Cybersecurity Operations Center – AEP, Lockheed, 16 other utilities

**Sustain Security Improvements**
- Over 2300 representatives from energy sector have participated in control systems security training events supported by DoE
- Cybersecurity Specialist Certification program to support workforce development
“Body of knowledge” for control systems security has expanded considerably

2006
• Control systems Cyber Security Defense in Depth Strategies
• Mitigations for Security Vulnerabilities Found in Control System Networks

2007
• NERC Top Ten Vulnerabilities of Control Systems and their Associated Mitigations
• Hardening Guidelines for OPC Hosts
• Recommended Practices Guide For Securing ZigBee Wireless Networks in Process Control System Environments
• Securing WLANs Using 802.11i
• Using Operational Security (OPSEC) to Support a Cyber Security Culture in Control Systems Environments (2007)
• Advanced Metering Infrastructure Security Considerations
• Guide to Critical Infrastructure Protection Cyber Vulnerability Assessment
• Threat Analysis Framework
• Impacts of IPv6 on Infrastructure Control Systems
• Security Metrics for Process Control Systems

2008
• Common Cyber Security Vulnerabilities Observed in Control System Assessments
• AMI System Security Requirements
• Cyber Security Procurement Language for Control Systems
• Securing Control System Modems
• NIST Special Publication 800-82: Guide to Industrial Control Systems (ICS) Security

2009
• Primer Control Systems Cyber Security Framework and Technical Metrics
• Wireless System Considerations When Implementing NERC Critical Infrastructure Protection Standards
• NIST Special Publication 800-53: Recommended Security Controls for Federal Information Systems Appendix I Industrial Control Systems

2010
• Guidelines for Smart Grid Cyber Security (NISTIR 7628)
• NIST Framework and Roadmap for Smart Grid Interoperability Standards

http://www.controlsystemsroadmap.net/documents.shtml
Grid modernization requires seamless, secure communications across multiple interconnected domains and platforms.

Florida Power and Light

Generic Smart Grid Communications Architectures

Enhanced Performance & Diagnostics

Power Plant
Transmission/Substation Intelligence
Phasor Measurement Units • Microprocessor Based Protection • Digital Disturbance Recorders • Intelligent Electronic Devices
Distribution Intelligence
Automated Feeder Switches • Capacitor Controllers • Fault Indicators • Throw-over Switch & Network Protector Monitors

Home Energy Controllers
Smart Meter
Grid Integration of Distributed Generation
Customer Education

Workforce Education Curriculum

Home Intelligence
Home Area Network (HAN)
Solar (or Wind)
Smart Thermostat
Smart Meter
House

Feeder Automation
Local Area Network (LAN)
AMI Collector
Line Switch with Radio Transceiver
Distribution Poles

Substation Automation
Wide Area Network (WAN)
Communications Tower
Power Delivery WAN
Fiber Optic
Smart Substations (Transmission & Distribution)

Transmission Automation
Substation Tower
Utility Central Operations
ISO
+$9 billion in public/private investments in Smart Grid technologies now being deployed
2011 Roadmap – updated to address progress, advancing threat, and changing technology landscape

- **2020 vision**
  - Dynamic and uncertain threat and technology environment
  - Long term view

- **Resilient energy delivery systems**
  - Expanded landscape
  - Smart grid technologies
  - Survivability and continuity of critical services

- **Survive a cyber incident**
  - Natural and manmade threats
  - Intentional and unintentional
  - Targeted/untargeted attacks

---

**2006 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.

**2011 Vision**

By 2020, resilient energy delivery systems are designed, installed, operated, and maintained to *survive* a cyber incident with no loss of critical function.
2011 Roadmap strategies - modified and added “culture of security”

2006 Roadmap

**Measure and Assess Security Posture**
Energy asset owners are able to perform fully automated security state monitoring of their control system networks with real-time remediation.

**Develop and Integrate Protective Measures**
Next-generation control system components and architectures that off built-in, end-to-end security will replace older legacy systems.

**Detect Intrusion and Implement Response Strategies**
Control system networks will automatically provide contingency and remedial actions in response to attempted intrusions.

**Sustain Security Improvements**
Energy asset owners and operators are working collaboratively with government and sector stakeholders to accelerate security advances.

2011 Roadmap

**Build a Culture of Security**
Cybersecurity practices are reflective and expected among all energy sector stakeholders.

**Assess and Monitor Risk**
Continuous security state monitoring of all energy deliver system architecture levels and across cyber-physical domains is widely adopted by energy sector asset owners and operators.

**Develop and Implement New Protective Measures to Reduce Risk**
Next-generation energy delivery system architectures provide “defense in depth,” and employ components that are interoperable, extensible, and able to continue operating in a degraded condition during a cyber incident.

**Manage Incidents**
Energy sector stakeholders are able to mitigate a cyber incident as it unfolds, quickly return to normal operations, and derive lessons learned from incidents and changes in the energy delivery systems environment.

**Sustain Security Improvements**
Collaboration between industry, academia, and government maintains cybersecurity advances.
DOE Portfolio Strategy to support Roadmap

Roadmap drives project selection for near, mid, and long term focus

Higher Risk, Longer Term Projects
→ Core NSTB Program
→ Academia Projects
→ No Cost Share

Medium Risk, Mid Term Projects
→ National Laboratory Led Projects
→ Lower Cost Share

Lower Risk, Short Term Projects
→ Industry Led Projects
→ Higher Cost Share

Path to Commercialization

Training, Education, Standards Development, and Other Outreach Activities

Academia Projects (TCIPG)
- Cornell University
- Dartmouth College
- University of California, Davis
- University of Illinois
- Washington State University

Core NSTB Program
- Argonne National Laboratory
- Idaho National Laboratory
- Oak Ridge National Laboratory
- Los Alamos National Laboratory
- Pacific Northwest National Laboratory
- Sandia National Laboratories

Industry-led Projects
- SEL, Inc.
- Siemens
- Telcordia
- Sypris
- Honeywell
- Digital Bond, Inc.
DOE National SCADA Test Bed (NSTB)

….. a national resource to support control systems security in the energy sector

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
- Control Systems Analysis Center

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

LOS ALAMOS Cybersecurity Program

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

Bruce Schneier, Beyond Fear
1. **Control Systems Situational Awareness Technology Interoperable Tool Suite** — a situational awareness tool suite to show network communications, collect wireless mesh network data message routes, report unexpected behavior, monitor system health, distinguish between component failure and cybersecurity incidents, 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*

2. **Automated Vulnerability Detection for Compiled 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*

3. **Next Generation Secure, Scaleable Communication Network 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.*

4. **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.*
Industry-led projects (transition technology to market)
(competitive award in 2010, 3 year duration with minimum 30% cost-share)

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


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

5. **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.

6. **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
Academia activities to support Roadmap

Trustworthy Cyber Infrastructure for the Power Grid (TCIPG)
University Illinois – Urbana/Champaign, UC-Davis, Dartmouth, Cornell, Dartmouth

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

- Secure and Real-Time Communication Substrate
- Automated Attack Response Systems
- Risk and Security Assessment
- Enhance, Apply, and Support Use of TCIP Test Bed
- Technology Transition and Industry Interactions
- Education and Workforce Development
- Trustworthy Substation Automation Technologies
- Trustworthy SCADA and Wide Area Transmission Networks and Applications
- Trustworthy Distribution Technologies
- Education and Workforce Development

Funding: $18.8 million over 5 years (2009-2014) from DOE with DHS contributions

Software Engineering Institute (SEI)
Federally funded R&D center at Carnegie Mellon University

- SCADA Source Code Analysis and Conformance Testing – Source Code Analysis Laboratory (SCALe)
- SHIMyS: Is Some Hacker (Hiding) In My System?
- Self Verifiable SCADA Systems
Key Near-term Activities to support Roadmap

• **$4.5 Billion Smart Grid Investment Program** – Project awardees develop cybersecurity plan that includes evaluation of cyber risks and planned mitigations, cybersecurity criteria for device and vendor selection, and relevant standards or best practices

• **Cybersecurity specialist certification guidelines** – PNNL and NBISE to develop a smart grid cybersecurity specialist competency model and approach for certification based on demonstration of knowledge, skills, and abilities

• **NESCO/NESCOR** – enhance information sharing and public/private communications; penetration testing guidelines; cybersecurity assessments of smart grid technologies – SEP. 1.X

• **Guidelines for Smart Grid Cyber Security** – ASAP-SG; Co-chair Cyber Security Working Group with NIST to develop NISTIR 7628

• **Electric Sector Cybersecurity Risk Management Process Guideline** – a risk management model for cybersecurity tailored to electricity sector needs – IT and OT

• **Cybersecurity Risk Management Maturity Model** – White House initiative led by DOE partnering with DHS to develop maturity model to assess cybersecurity posture of sector
Power Grid Impacts Resulting From Unintentional Demand Response

by Jeff Dagle, Pacific Northwest National Laboratory

Friday, February 3, 2012 at 1PM (Central Time)

NCSA Auditorium, University of Illinois | Webcast

Live webcast URL option #1 (non-interactive)
http://mediapointe.ncsa.illinois.edu:8080/live.sdp

Live webcast URL option #2 (interactive to support Q&A; no password required)
https://ncsatraining.webex.com/ncsatraining/onstage/g.php?d=809672303&t=a

Abstract: The emerging "smart grid" will enable the increased use of digital technology to improve reliability, security, and efficiency of the electric power system. A valuable smart grid feature is the ability to curtail load through demand response. Another application will be the ability to disconnect or reconnect service to individual meters. One of the unintended consequences being postulated is the unintended or malicious mis-operation of either demand response or customer connection. The concern is simultaneous operation in large numbers could create a disruption to the reliability and integrity of the bulk electric power system.
For more info, contact:

Carol Hawk,
Program Manager for DOE Cybersecurity for Energy Delivery Systems

Carol.hawk@hq.doe.gov

www.controlsystemsroadmap.net