Cyber Security for Energy Delivery Systems
Sans SCADA 2010 Summit
Orlando, FL
March 30, 2010
Bill Hunteman
DOE is the Sector-Specific Agency responsible for critical infrastructure protection for the energy sector
– defined as production, refining, storage, and distribution of oil and gas, and electric power (except for nuclear power facilities)

**DOE/OE Roles:**
– Collaborate with Federal agencies, state and local governments, and the private sector;
– Identify, prioritize, and coordinate protection of critical infrastructure and key resources in the energy sector;
– Reduce consequences of catastrophic failures
– Facilitate sharing of information about physical and cyber threat, vulnerabilities, incidents, potential protective measures, and best practices
– Conduct/facilitate vulnerability assessments
– Encourage risk management strategies
Cyber Security Challenges for Energy Sector

- **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
Modern Infrastructure Requirements Could Introduce Cyber Risk

- Automated data analysis and demand response capability
- Real-time, two-way communication with remote metering devices
- Use of web-enabled diagnostic middleware and software
- Use of more open, interoperable architecture designs
- Interdependent energy management systems

Increased reliance on automation, information, and communications technologies creates potential for new cyber vulnerabilities

Need for increased cyber security!
Putting Ideas into Action

1) Alliances Formed
   - Owners & operators
   - Equipment vendors
   - Industry organizations
   - Government agencies
   - Researchers

2) Priorities Outlined
   - >90 projects identified
   - All projects linked to the roadmap

3) ieRoadmap Created

4) Expert Working Group Formed
   - Identify gaps and opportunities
   - Guide public and private efforts
Aligning Efforts, Accelerating Solutions

- **Energy Sector’s** synthesis of critical control system security challenges, R&D needs, and milestones
- Strategic framework for aligning activities
- Catalyst for public-private collaboration
- Tool for focusing investment and accelerating solutions

**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.
## Roadmap 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><strong>Goals</strong></td>
<td><strong>Goals</strong></td>
<td><strong>Goals</strong></td>
<td><strong>Goals</strong></td>
</tr>
<tr>
<td>Energy asset owners are able to perform fully automated security state monitoring and control systems networks with real-time remediation (2015)</td>
<td>Next-generation control systems components and architectures produced with built-in, end-to-end security will replace older legacy systems (2015)</td>
<td>Control systems networks will automatically provide contingency and remedial actions in response to attempted intrusions (2015)</td>
<td>Implement effective incentives through Federal and state governments to accelerate investment in secure control system technologies and practices (2015)</td>
</tr>
</tbody>
</table>
Working Group Oversees Roadmap Implementation

Critical Infrastructure Partnership Advisory Council

- Electric Sector Coordinating Council
- Government Coordinating Council for Energy
- Oil & Natural Gas Sector Coordinating Council

Cross Sector Coordinating Council

IT Sector Coordinating Council
**ieRoadmap** – “weapon of mass collaboration”¹

Facilitates collaboration and measures progress

- On-line Roadmap Mapping Tool
- More than 60 projects mapped by 21 organizations

http://www.controlsystemsroadmap.net

---

1. CIDG, Corp.
2. Cisco Systems
3. DHS HSARPA
4. DHS National Cyber Security Division
   CSSP
5. Digital Bond
6. DOD Technical Support Working Group
7. DOE National SCADA Test Bed Program
8. Electric Power Research Institute (EPRI)
9. Information Trust Institute (ITI)
10. Institute for Information Infrastructure Protection (I3P)
11. Mu Dynamics
12. MS-ISAC
13. NIST
14. PNNL NCSSR
15. Raytheon
16. Siemens Corporate Research
17. SRI International
18. Tenable Network Security
19. Trustworthy Cyber Infrastructure for the Power Grid (TCIP)
20. U. of Illinois at Urbana-Champaign
21. Wurldtech Security Technologies

¹“Wikinomics, How Mass Collaboration Changes Everything”, Tapscott and Williams
DOE National SCADA Test Bed (NSTB) Program (Supports Roadmap)

Key Roadmap Strategies

1. Measure and assess security posture
2. Develop and integrate protective measures
3. Detect intrusion and implement response strategies
4. Sustain security improvements
NSTB Supports Roadmap

NSTB Key Activities

- Next Generation Control Systems
- System Vulnerability Assessments
- Integrated Risk Analysis
- Partnership and Outreach

- Trustworthy Cyber Infrastructure for the Power Grid
- Smart Grid Test Bed
- Modeling and Simulation
- Workshops

- Cross-cutting Technologies Development
- Cyber Assessments for Next-Generation Control Systems
- Scenario Analysis
- Advanced Red/Blue Training

- Industry-led Technology Development
- Operational Analysis
DOE National SCADA Test Bed (NSTB) Program

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
(5 DOE National Laboratories)

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
NSTB Vulnerability Assessment
(Industry Partners)
Enhanced SCADA Systems in Market TODAY!

Vendors

Cyber Assessment Results (proprietary)

SCADA Systems for Testing

Systems Modified, Retested

NSTB Assessments

Generic “Lessons Learned”

Next Generation SCADA Systems & Perimeter Defenses

Asset Owners

Enhanced SCADA/DCS systems for Industry
Cyber Security for Energy Delivery Systems Program (Key Areas)
Projects Showcased at DistribuTECH

- **Cyber Security Audit and Attack Detection Toolkit**—Bandolier Audit Files for optimizing security configurations and the Portaledge event detection capability for energy control systems
- **Hallmark Cryptographic Serial Communication**—a cryptographic card and link module integrating the Secure SCADA Communications Protocol to provide secure serial communications for existing and new energy control systems
- **Lemnos Interoperable Security**—a capability based on open-source specifications—demonstrated in a vendor product—that enables secured interoperability among energy control systems devices
- **Integrated Security System (ISS)**—a security platform providing multi-layer intrusion detection and security management to enable energy asset owners to design a secure, networked control systems architecture
- **Detection and Analysis of Threats to the Energy Sector (DATES)**—a security monitoring capability featuring multiple detection algorithms and cross-domain event correlation for defense against cyber attacks on energy control systems
- **Trust Anchor Lifecycle Attack Protection**—cryptographically secure software providing independent testing, monitoring, and control of energy control system component operation
Outcomes:
• Commercial Prototype
• Open Source Design
• Plugfest

Participants:
• Sandia National Laboratories
• Schweitzer Engineering Laboratories
• Tennessee Valley Authority
• 7 Network Security Vendors

Success Stories:
• Reference Taxonomy Completed
  • Vocabulary and set of metrics
  • Describe functionality within the network security domain
  • Available to developers, vendors, and asset owners.
• Designed, built, and tested a prototype of the SEL-3620 Ethernet Security Gateway
  • Interoperable
  • Capable of operating with existing IT and control systems
  • Uses intuitive, menu-driven web-based interface to create an Internet Protocol Security (IPsec) virtual private network (VPN).
• Plugfest!
  • Demonstrate interoperability
  • DistribuTech (March 2010, Tampa)
Secure SCADA Communications Protocol

**Challenge:**
- Time-critical serial data communications between substations and control centers poses high risk
- Provide data integrity (“cryptographic security”) in open protocol environment through message authentication
- Develop solutions for existing control systems and new control systems to mitigate network vulnerabilities

**Participants:**
- Developed by Pacific Northwest National Laboratories (PNNL)
- Prototype tested at CenterPoint Energy
- Commercialized by Schweitzer Engineering Laboratories, Inc.

**Accomplishments:**

**SSCP Technology Transfer Completed**
- Provides message integrity by marking original SCADA messages with a unique identifier and authenticator
- Receiving devices will validate before enacting commands

**Cryptographic Daughter Card**
- Electronic hardware card that runs the SSCP protocol

**Link Module**
- Hardware and firmware platform
- Provides the interface between the control system network and the CDC with SSCP
Cyber Security Audit and Attack Detection Toolkit

**Challenge:**

- Need to ensure/validate control systems in secure configuration
- Need to aggregate and correlate security events to identify attack attempts on control systems

**Participants:**

- OSISoft
- Tenable Network Security
- Energy Sector Asset Owners
- Commercialization by Digital Bond, Inc

**Accomplishments:**

Bandolier Project – Preventing and Detecting Cyber Attacks by Auditing Configuration

- Developed audit files for Siemens, Telvent, ABB, Matrikon, Emerson, AREVA, and SNC systems
- Audits check validity and reliability of the control system devices and applications

Portaledge Project – Improving Security of the Electric Network Using a “Real-time Cyber Event Manager”

- Identifies security events
- Incorporate those events into the PI server
- Correlates security event information to identify meta events (a sequence or “recipe” of events that indicates a specific attack goal or achievement)

Available as subscriber content on Digital Bond website

- Over 200 organizations subscribing
Advanced Network Toolkit For Assessments and Remote Mapping

- PASSIVE network discovery tool
- Input – network databases
- Output – graphical depiction of the network topology
- Benefits - network asset identification; facilitates implementation of industry standards
- Developed by DOE Sandia National Laboratory
**Protecting Intelligent Distributed Power Grids against Cyber Attacks**

*Siemens Corporate Research, Inc.*

**Outcomes:**
- Develop and demonstrate Software Prototype Demo/Risk Assessment and Security Optimization System

**Participants:**
- The Center for Advanced Energy Systems (CAES) at Rutgers University
- Siemens Power Transmission and Distribution (SPTD)
- Idaho National Laboratory (INL)

---

**Detection and Analysis of Threats to the Energy Sector (DATES)**

*SRI International*

**Outcomes:**
- Sector-wide Threat Analysis Portal
- Network IDS with control system aware knowledge base, model-based detection capability, and packet trace visualization tool to facilitate detecting
- Integrated sensor suite and situational awareness SEIM dashboard
- Applicable for both electric power and oil and gas

**Participants:**
- ArcSight
- Sandia National Laboratories
- Invensys
Trustworthy Cyber Infrastructure for the Power Grid (TCIPG)

Vision: Architecture for End-to-End Resilient, Trustworthy & Real-time Power Grid Cyber Infrastructure
## American Recovery and Reinvestment Act ($4.5 B) **Jumpstarts** Smart Grid

<table>
<thead>
<tr>
<th>Office of Electricity Delivery and Energy Reliability</th>
<th>$ Millions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Smart Grid Investment Grant Program; ≤3 years</td>
<td>$3,400</td>
</tr>
<tr>
<td>Smart Grid Demonstrations; 3-5 years</td>
<td>$615</td>
</tr>
<tr>
<td>Interoperability Framework Development by NIST</td>
<td>$10</td>
</tr>
<tr>
<td>Resource Assessment and Interconnection-Level Transmission Analysis and Planning</td>
<td>$80</td>
</tr>
<tr>
<td>State Electricity Regulators Assistance</td>
<td>$50</td>
</tr>
<tr>
<td>Enhancing State Government Energy Assurance Capabilities and Planning for Smart Grid Resiliency</td>
<td>$55</td>
</tr>
<tr>
<td>Workforce Development</td>
<td>$100</td>
</tr>
</tbody>
</table>
Cybersecurity ARRA Activities

Critical to Smart Grid Success

- Organized interagency group (DOE, NIST, FERC, DHS, CIA) for development of cybersecurity requirements for RFP
- Cybersecurity - major factor in Technical Merit Review
- Utilized technical merit review team and cybersecurity SME team to provide independent reviews
- DOE will work with grantees to ensure cybersecurity plans are adequate

“DOE may not make an award to an otherwise meritorious application if that application cannot provide reasonable assurance that their approach to cybersecurity will prevent broad based systemic failures in the electric grid in the event of a cybersecurity breach.”

Smart Grid FOA
Example “cyber-focused” SGDP Projects

- **Los Angeles Department of Water and Power Smart Grid Regional Demonstration Project** – Deploy SG systems at partners' university campus properties & tech transfer labs - gather data on how consumers use energy in a variety of systems, test next-gen cybersecurity technologies, & how to integrate plug-in hybrid electric vehicles into the grid. (ARRA DOE funding: $60.2M)

- **Southern Cal Edison - Irvine Smart Grid Demonstration** - Demonstrate integrated, scalable SG system that includes all interlocking pieces of an end-to-end Smart Grid system. Focus on interoperability and interactions between technologies and systems working at the same time - such as communications networks, cyber-security requirements, & interoperability standards, such as NIST & NERC cyber security standards. (ARRA DOE funding: $40.1M)

- **Battelle - Pacific Northwest Smart Grid Demonstration Project** - Spanning five states & affecting more than 60,000 consumers, demo & validate new SG technologies & inform business cases; provide two-way communication between distributed generation, storage, & demand assets & the existing grid infrastructure; quantify smart grid costs & benefits; & advance interoperability standards & cyber security approaches. (ARRA DOE funding - $88.8M)
ASAP-SG
Advanced Security Acceleration Project - Smart Grid

• Industry-government collaboration (50-50 cost share) to accelerate security standards development for Smart Grid (May 2009 – May 2010)

• Successor to ASAP which developed “Security Profile for Advanced Metering Infrastructure, v 1.0” - incorporated in NISTIR 7628

• DOE funding Software Engineering Institute and Oak Ridge National Laboratory working with Enernex

• Current industry sponsors:
  • American Electric Power
  • Con Edison
  • Consumers Energy
  • Florida Power & Light
  • Southern California Edison

• Partners are invited

• Contact Bobby Brown at Enernex
Upcoming Cybersecurity Activities for the Energy Sector

March 23-25
- Showcase Roadmap public-private partnership products at DistribuTECH

March
- Issue RFP for industry-led R&D projects to enhance cybersecurity of electric grid – including Smart Grid

April
- Issue RFP for “National Energy Sector Cyber Organization”
- Issue National Laboratory call for R&D projects to enhance cybersecurity of energy sector
- Release draft “revised” Roadmap to Secure Control Systems in the Energy Sector

June 21-25
- Conduct Red Team / Blue Team Training at INL focused on Oil and Natural Gas sector (Idaho Falls, ID)

July 21-22
- Conduct Peer Review of DOE Cybersecurity for Energy Delivery Systems (Alexandria, VA)
CSEDS Peer Review
July 20-22, 2010
Westin Alexandria – Alexandria, VA

- Presentations on upcoming products and technologies now in development by more than 30 DOE-supported or cost-shared projects
- First-hand reviewer feedback for current DOE work
- A poster session featuring innovative R&D to secure energy delivery systems
- Opportunities to network with experts from industry, academia, and national laboratories
• **Vision:** Partnership between the federal government and electric-sector stakeholders to help protect the Bulk Electric System and integrate smart grid technology to enhance security

• **Purpose:** To focus research, development and deployment priorities to ensure effective deployment of technology and software controls

• **$8.5M Funding Opportunity Announcement targeted for release end of April 2010**
Red Team/Blue Team Advanced Training

- 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
- 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
Get involved …

Roadmap Update
• Roadmap Reviewer
• Roadmap Security Champion

Project Contributor/Partner

Contact:

www.controlsystemsroadmap.net/workinggroup.aspx
For more info …

Contact:

*US Department of Energy*

Bill Hunteman  
[Bill.Hunteman@hq.doe.gov](mailto:Bill.Hunteman@hq.doe.gov)

Carol Hawk  
[Carol.Hawk@hq.doe.gov](mailto:Carol.Hawk@hq.doe.gov)

Visit:  

[www.oe.energy.gov/controlsecurity.htm](http://www.oe.energy.gov/controlsecurity.htm)  
[www.controlsystemsroadmap.net](http://www.controlsystemsroadmap.net)