U.S. Department of Energy
Office of Electricity Delivery
and Energy Reliability

DOE/OE
National SCADA Test Bed
Fiscal Year 2009 Work Plan

(REVISED 07/31/2009)

NSTB

National SCADA Test Bed

Enhancing control systems security in the energy sector

Fiscal Year

2 0 0 9

Work Plan

A plan of work for the National Laboratories that form the National SCADA Test Bed:

Argonne National Laboratory

Idaho National Laboratory

Oak Ridge National Laboratory

Pacific Northwest National Laboratory

Sandia National Laboratories

FOREWORD

The Department of Energy (DOE) Office of Electricity Delivery and Energy Reliability (OE) created the National SCADA Test Bed (NSTB) program with the mission to reduce the risk of energy disruptions due to cyber attack on control systems. So far the program's projects have uncovered a multitude of knowledge that has already increased the security of our energy control systems around the country. Since its inception, the program has formed valuable links between the government, the energy sector, and national laboratories to conduct research and development in the area of cyber security. Through these partnerships, the DOE/OE NSTB Program has identified ways to rapidly and effectively develop, integrate, and sustain security improvements (see sidebar).

This document is designed to help guide and strengthen the DOE/OE NSTB program's research and development (R&D) of advance security tools and to heighten awareness among energy sector partners of the more than 30 NSTB projects underway in FY2009.

The NSTB Team

Created in 2003, NSTB has served as a national resource to assist the energy sector (electric, oil, and natural gas) in identifying and solving today's SCADA (Supervisory Control and Data Acquisition) and control systems vulnerability issues, testing new and existing equipment, and developing secure architecture designs and technology advances. NSTB is a multi-laboratory partnership that draws on the integrated expertise and resources of the Argonne, Idaho, Oak Ridge, Pacific Northwest, and Sandia National Laboratories.

Key Accomplishments

To date, NSTB and its industry partners have produced tangible results, highlights include:

- NSTB has assessed the majority of the current market offering of SCADA systems in the electric and the oil and gas sector.
- More than 1,900 end users have been trained by NSTB on best practices for control systems security
- NSTB has conducted 21 on-site and test bed assessments, helping vendors to develop 11 hardened control systems designs.
- Development of the "ANTFARM" software: a no-cost tool that maps control system networks to help implement cyber security standards
- The Bandolier project by Digital Bond, which has released audit files to help asset owners configure their control system applications according to security best practices.
- The Hallmark project by Schweitzer Engineering to commercialize a hardware device using the Secure SCADA Protocol developed by PNNL. to ensures message integrity.
- The AMI (Advanced Metering Infrastructure) Security Standards by the AMI-SEC Task Force provide utilities and vendors with a set of requirements to help secure implementation of AMI.

NSTB combines a unique range of specialized laboratory resources to create realistic testing environments for SCADA communications and control systems. For example, the national test bed enables systems to undergo a level of rigorous testing that would be impossible to perform on systems in active service. The test bed provides a safe and isolated, yet real-world environment for testing and evaluating control system vulnerabilities and mitigation strategies. The NSTB team's primary goals are to accomplish the following:

- Raise industry awareness of control system cyber security vulnerability issues and mitigation techniques.
- Collaborate with industry to identify, assess, and mitigate current SCADA system vulnerabilities.
- Work with industry to develop near-term solutions and risk mitigation strategies for existing control systems.
- Conduct R&D to develop next-generation architectures for intelligent, inherently secure, and dependable control systems and infrastructures.

- Support development of national standards and guidelines for more secure control systems.

NSTB Helping Industry Partners

To accelerate the development of next generation control systems, DOE has provided nearly $8 million in funding for five industry-led, cost-shared projects. Launched in October 2007, NSTB and its national laboratories are working closely with all industry project leads to harmonize their control system security initiatives with NSTB and Roadmap goals and minimize duplication of efforts. For several projects, NSTB's national laboratory subject-matter expertise, unique capabilities, and specialized facilities are being leveraged in the R&D process. DOE's National Energy Technology Laboratory (NETL), through the DOE/OE NSTB program, is managing these projects, which are included in this work plan and expected to be completed over the next two years.

Roadmap Implementation

In 2005, DOE/OE and the U.S. Department of Homeland Security (DHS) collaborated with the electric, oil, and natural gas sectors stakeholders and with Natural Resources Canada to develop the *Roadmap to Secure Control Systems in the Energy Sector*. The roadmap defines the vision, goals, milestones, and priority activities that will be pursued by industry and government to secure all energy control systems from intentional cyber attack.

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.

Energy companies, vendors, industry organizations and federal agencies are all working together to make this vision a reality, through research in the following goal areas: Measure and Assess Security Posture, Develop and Integrate Protective Measures, Detect Intrusion and Implement Response Strategies and Sustain Security Improvements.

In a report to the President, the National Infrastructure Advisory Council (NIAC) recognized the Roadmap's success in developing and implementing cyber security solutions for control systems and recommended that all critical infrastructures adopt the Roadmap's goal of securing control systems against loss of critical function from intentional cyber attack by 2015. So far, the water sector has developed their own roadmap and efforts are underway by Chemical and Dams Sector with a similar vision and framework, while other sectors are expected to follow suit.

To keep industry engaged and aware of progress, The DOE/OE NSTB program created the interactive Energy Roadmap (ieRoadmap), an online database that allows researchers to self-populate their active R&D activities according to roadmap goals and provides opportunities for collaboration and information sharing. Since its launch in 2006, more than 60 projects have been shared by 18 public and private-sector organizations.

Energy Sector Control Systems Working Group (ESCSWG)

To support implementation of the Roadmap, the DOE/OE NSTB program facilitated the formation of the ESCSWG under the Critical Infrastructure Partnership Advisory Council (CIPAC) framework. The ESCSWG consists of senior representatives from the energy and government sectors, as designated by the Electric and Oil and Natural Gas Sector Coordinating Councils and the Government Coordinating Council for Energy. Since 2007, the Working Group has pursued innovative, facilitative, and practical initiatives to enhance the cyber security of the control systems across the entire energy sector by:

- Helping identify and implement practical, near-term activities that are high priority for the energy sector

- Promoting the value of achieving the goals of the Roadmap in the energy sector
- Recommending critical initiatives for public and private investment
- Measuring progress toward Roadmap goals and milestones

In 2008, its first year of operation, the ESCSWG increased the awareness and engagement of owners and operators in the Roadmap process and helped to baseline the current landscape of control systems security projects in the energy sector. The ESCSWG objectives for 2009 are to update the Roadmap, continue increasing the awareness and engagement of owners and operators in Roadmap related activities, and measure progress with the control systems security projects in the energy sector. For more information on ESCSWG accomplishments and plans, please see the ESCSWG Annual Report. A summary of the ESCSWG 2009 Work Plan can be found in Appendix B.

Multiyear Plan

Although many cyber security solutions will originate from the private sector, the coordination and transfer of these solutions involves national leadership, effective partnerships, and a shared vision of the future. Accordingly, the NSTB program has closely aligned its efforts with the roadmap, the DOE/OE mission, ESCSWG recommendations, the *National Strategy to Secure Cyberspace*, Homeland Security Presidential Directive-7, and additional federal efforts and policy guidance. The synthesis of this guidance was effectively realized through the establishment of a *DOE/OE NSTB Multi-Year Plan*, published in 2008, which outlines NSTB activities through 2013.

The *DOE/OE NSTB Multi-Year Plan* presents the NSTB program's strategy to reduce the risk of energy disruptions due to cyber attack on control systems. The four program activities outlined in the multi-year plan include: developing next-generation control systems technology, conducting systems vulnerability assessments, developing end-to-end risk analysis capabilities and partnering with public and private energy sector stakeholders to raise security awareness and leverage resources. Collectively, these research areas provide a sound foundation for collectively enhancing the security and reliability of the energy infrastructure. With the creation of the plan, the NSTB program and its partners have a clear guide to a reliable, secure future.

Work Plan

The NSTB program was created with a clear understanding that improving the security of SCADA and control systems is integral to protecting the energy infrastructure and the sectors it serves. As defined in its multiyear plan, all FY2009 NSTB program activities are aligned under four project areas:

- **Next-generation control systems:** Research and development that accelerates the development and deployment of hardened control systems with built-in security
- **System vulnerability assessments:** Rigorous tests that reveal exploitable systems vulnerabilities and encourage development of system fixes
- **Integrated risk analysis:** Developing means for stakeholders to assess their security posture that will hasten their ability to mitigate potential risks
- **Partnership and outreach:** Active partnerships that engage all stakeholders and encourage collaborative developments and dissemination of critical security information

DOE/OE NSTB has a generous number of ongoing activities in each area, all of which are detailed in the following pages.

Project Alignment with NSTB Program Elements

Project	Next Generation Control Systems	Integrated Risk Analysis	System Vulnerability Assessments	Partnership & Outreach
#1 Wireless	✓			
#2 Smart Grid Security Attributes	✓			
#3 Data Transfer Project	✓			
#4 Protocol Analyzer for the SSCP	✓			
#5 Cryptographic Trust Management	✓			
#6 Centralized Configuration Management for Field Devices	✓			
#7 Protecting Process Control Systems against Lifecycle Attacks using Trust Anchors	✓			
#8 Anomaly Detection and Distributed Active Response for Control Systems Networks	✓			
# 9 Trustworthy Wireless for Critical Infrastructure Sites	✓			
#10 Process Control Security under future National Grid Conditions	✓			
#11 Cyber-Physical Attacks and Cyber-Physical Security: The Second Line of Defense	✓			
#12 SCADA Systems Cyber Security Testing Through Portable Acceptance Test	✓			
#13 Cyber Security Audit & Attack Detection Toolkit	✓			
#14 Detection and Analysis of Threats to the Energy Sector (DATES)	✓			
#15 Lemnos Interoperable Security Program	✓			
#16 Protecting Intelligent Distributed Power Grids from Cyber Attack	✓			
#17 Hallmark Project	✓			
#18 Threat Characterization		✓		
#19 Real Time Security State Visualization Tool		✓		
#20 Virtual Control System Environment		✓		
#21 Impact Analysis of Cyber Attacks on Control Systems		✓		

#22 Risk Analysis / Outreach		✓		
#23 Consequence Modeling Tool		✓		
#24 Common Vulnerabilities Report – FY2009 Update			✓	
#25 Assess Control Systems in Test Bed Facilities			✓	
#26 Assess Control Systems in Asset Owner Facilities			✓	
#27 Test Bed Support			✓	
#28 Industry Outreach				✓
#29 Industry and Government Outreach				✓
#30 SCADA Security Training Workshops				✓
#31 PNNL Outreach				✓
#32 Intrusion Detection Outreach to Develop Utility Requirements				✓
#33 Roadmap Gap Analysis				✓

Table of Contents

NEXT GENERATION CONTROL SYSTEMS

1. Wireless

Lead: Jeff Dagle, PNNL
Partners:

1.1 Purpose

This project aims to improve security for control systems by conducting wireless security training for industry, developing guidance on where specific wireless technologies should and should not be deployed, and providing guidance on how to implement a defense in depth model for specific wireless technologies. This project will review various technologies to identify appropriate policies and procedures, develop industry and technology-specific security practices, and create training and vulnerability demonstration materials for industry.

1.2 Background

Wireless technologies are becoming accepted at an increasing rate in the electric sector. Historically the use of wireless was limited to SCADA radio and analog microwave. Today it is common to find the use of 802.11 (WiFi) on the corporate network. Engineers have cell phones and PDAs. Vendors are including wireless technologies as part of their product offerings as the cost to implement becomes minimal. Wireless technologies are being deployed in substations.

This effort will focus on energy sector application of wireless technologies. The use of wireless technologies is an important topic of current interest to electric power utilities. Applications of wireless technologies are being made for communication within a substation, between substations, between the control center and substations, and also to improve situational awareness of transmission and distribution lines. Appropriate use of wireless technologies, security of wireless technologies, and the impacts of wireless upon regulatory requirements all must be addressed.

1.3 Scope and Technical Approach

This project will utilize a phased approach to examine current and emerging wireless technologies. Industry momentum is currently focused on WiFi, WiMax, and Zigbee. For each of these wireless technologies, a white paper discussing appropriate use and security practices will be developed.

Two new hands-on demonstration activities will be designed, developed, and presented this fiscal year. The wireless technologies to be added are Zigbee and WiMAX. This fiscal year will also see the development of technical guidance for industry on where specific wireless technologies should be deployed and how the wireless environments should be secured using the defense in depth model identified in FY 2008.

A second focus area is white hat/white box testing of wireless technologies. This effort includes conference participation/presentation activities to increase security awareness. This effort will be staffed by the technical staff at PNNL involved in the operation of multiple wireless networks (mesh, point-to-point, etc.) and will address security issues such as boundary protection, rogue device detection, and defense-in-depth implementations.

A third technical area addressed is training for utility staff to improve understanding of wireless technologies, security, and technology selection.

1.4 Deliverables

Milestones

- March 2009 – Update training curriculum to include Zigbee and WiMax
- September 2009 – Application Guidance Documents

Primary Deliverables

- Wireless training class (venue TBD)
- Wireless Application Guidance Document

2. Smart Grid Security Attributes

Lead: Jeff Dagle, PNNL
Partners: ANL, INL, others TBD

2.1 Purpose

In collaboration with the Argonne National Laboratory (ANL) and the Idaho National Laboratory (INL), the Pacific Northwest National Laboratory (PNNL) will provide the U.S. Department of Energy (DOE) answers to the questions posed in Section 1309 of Title XIII of the Energy Independence and Security Act of 2007.

2.2 Background

This study will address the current application, scope, and security issues associated with Smart Grids, and how they are vulnerable to diverse security threats. It will also address how future Smart Grids, if implemented with the proper security attributes, can enhance infrastructure resiliency from all hazards. Future Smart Grids will be an important foundation for multiple uses of the electric power infrastructure. Our study will help guide the U.S. Government and industry toward more sound, safe, secure, and capable power infrastructures by providing guidelines, recommendations, and incorporating lessons learned from early adopters.

2.3 Scope and Technical Approach

Project team will research the current state, anticipated advancements, and implications of Smart Grid technologies to obtain a holistic view of the subject. Our plan consists of the following three steps:

- Form a diversified team that includes national laboratories, academia, global technology experts from the electric power industry, and the U.S. Government
- Assess the state-of-the-art in Smart Grid technology and *analyze the security implications from design through deployment, maintenance, and replacement*
- Provide to DOE our findings, including recommendations for the secure fielding of this technology in the United States.

PNNL will lead a diversified team in partnership with ANL, INL, academia, power industry experts world-wide, and the U.S. Government to do the following:

- Assess the current state-of-the-art in Smart Grid technology
- Bring to light the lessons learned in existing and planned Smart Grid deployments
- Anticipate the vulnerabilities inherent to this organic technology growth
- Provide recommendations for roles and responsibilities of government, implementers, and the research community.

2.4 Deliverables

Milestones

- November 2008 – Industry brainstorming workshop
- December 2008 – Complete draft available for stakeholder review
- January 2009 – Draft document available for second industry review

Primary Deliverables

- June 2009- Final Report

3. Data Transfer Project

Lead: Jeff Dagle, PNNL
Partners: Newton-Evans, Oncor Electric Delivery, PacifiCorp, ANL, others TBD **Technical Advisors**: Alliant Energy, El Paso Corporation, Ergon Refining Inc., NiSource, Control Center Solutions LLC, Progress Energy, Alyeska Pipeline Inc., Entergy Corporation

3.1 Purpose

This task aims to facilitate the secure, robust and timely transfer of data between control centers and other networks. This project is supported by ANL.

3.2 Background

Researchers from PNNL and other organizations will provide both electric and gas industry knowledge for this project. The research team will identify requirements for a "demilitarized zone" (DMZ) to provide defense in depth enabling more secure data transfer between control system, business, and potentially other networks in a timely and robust manner. A team of industry advisors will be engaged to provide examples of solutions currently in use, identify shortcomings with those implementations, and help identify requirements for the ideal solution, and understand tradeoffs between alternative approaches. PNNL staff with expertise in secure computing and networking will provide guidance on solutions from those environments that perform similar functions.

3.3 Scope and Technical Approach

Using its Electric Infrastructure Operations Center (EIOC), PNNL can design a DMZ, leveraging SCADA and wide-area measurement system data feeds. Together these data types and systems provide a good test environment in a realistic setting.

The team is developing a detailed control-system specific solution for DMZ use, which the advisory team will review. PNNL is also creating a best-practices guide for asset owners to implement the technology.

3.4 Deliverables

Milestones

- April 2009 – Advisory Team meeting at PNNL
- September 2009 – Proof of Concept Prototype

Primary Deliverables

- Proof of concept Prototype

4. Protocol Analyzer for the SSCP

Lead: Mark Hadley, PNNL
Partners: Applied Systems Engineering, Frontline, Siemens, Telvent, Schweitzer Engineering Laboratories, Triangle MicroWorks, CenterPoint Energy, others TBD

4.1 Purpose

This project has two primary goals. The first is to incorporate the Secure SCADA Communications Protocol into Test Set products. The second is to incorporate the SSCP into protocol analyzer products. Adding support for the SSCP in these various modes will enhance the ability of asset owners to monitor secured communication. In addition, control system device vendors will be able to test development of their products that support the SSCP.

4.2 Background

Current Secure SCADA Communications Protocol (SSCP) projects focus technology transfer efforts towards energy management system (EMS) vendors, protocol standards bodies, and legacy devices (through the Hallmark project), encompassing technology transfer in support of current, future, and legacy environments. One further area of technology transfer required is porting the SSCP to protocol analyzer and communication test set vendors. Asset owners use protocol analyzer and communication test set tools to support the day-to-day operation of electric generation, transmission, and distribution environments. One vender, Applied Systems Engineering, currently develops tools to support Master, RTU, and Line Monitoring modes for a variety of control system protocols and devices.

4.3 Scope and Technical Approach

The technical approach will be leveraging current vendor and asset owner relationships to confirm whether Applied Systems Engineering would be interested in partnering in this technology development effort, or find a suitable protocol test set vendor that would be willing to work with us to include the SCCP in their commercial protocol analyzer suite. Once the vendor relationship has been established, we will work with them to specify the SSCP protocol requirements, develop a real-time data capture engine, and design a visualization tool to interface with their product to provide appropriate SSCP status information.

4.4 Deliverables

Milestones

- December 2008 – Enact NDA with Triangle Micro Works (TMW)
- February 2009 – Provide SSCP Specification and Implementation Guidance Documents to TMW

Primary Deliverables

- Open source protocol analyzer (e.g., WireShark) available for demonstration

5. Cryptographic Trust Management

Lead: Jeff Dagle, PNNL
Partners:

5.1 Purpose

The purpose of this project is to create a software application to manage cryptographic keys to support the deployment of technologies developed to meet multiple Roadmap goals.

5.2 Background

The lack of a scalable technology to manage cryptographic keys for control system hinders the deployment of vendor products to secure control system communication. The prime example of this critical missing element is the failed deployment of products designed to the American Gas Association (AGA) 12 Cryptographic Standard. Without an industry acceptable, scalable, secure and robust mechanism to create cryptographic keys that supports the operational requirements of critical infrastructure asset owners, no cryptographic solution will be widely deployed. Comments received during the recent PCSF conference and the peer review for the Hallmark project echo this sentiment. Industry requires a cryptographic key management solution to further the deployment of technical solutions and to eliminate the risk associated with control system communication.

The introduction of cryptography into control systems represents a significant challenge to vendors, asset owners and standards bodies. The cryptographic goals for control systems differ significantly from corporate IT or Internet sites. The security objectives of IT Systems are confidentiality, integrity, and lastly availability. Control systems by contrast, the security objectives are:

1. Availability
2. Integrity
3. Confidentiality

In addition, the use of cryptography in control systems must support the multiple operational needs of asset owners without adversely affecting reliable operations or personnel safety. The cryptographic key management problem is made more complicated by the number of vendors creating security products, regulatory requirements to identify and protect critical information, and the automation of previously manual processes (e.g. automated meter reading).

Another hurdle to overcome is the potential size of a control system network. Managing cryptographic keys for a small utility with 30 substations can be done without automation. Managing keys for an automated meter reading environment with millions of smart meters cannot.

The following is a sample of the potential application of cryptographic solutions a single utility must manage:

- Automated Meter Reading
- Secure E-mail
- Validation of log files
- SSL connection for web based applications
- Secure ICCP or DNP
- Bump in the wire serial encryption or authentication devices
- Embedded or integrated authentication solutions
- Secure engineering access to field devices

- SCADA Radio networks
- Other wireless technologies (802.11, Bluetooth)
- Remote access (staff, vendor or site) via VPN or SSH

5.3 Scope and Technical Approach

This project will utilize key personnel at PNNL to lead the project and develop the solution. PNNL is uniquely qualified as a national lab given our knowledge of both public key and symmetric key cryptographic technologies. In addition, the PNNL project team will involve the Secure SCADA Communications Protocol commercialization vendors, NIST, NERC, and asset owners to provide industry requirements, review the design, provide feedback, and test the solution. The existing advisory team members working on the Visualization, Data Transfer, and SSCP projects will be approached regarding their interest in participating on this critical project.

This project will also utilize the Electric Infrastructure Operations Center (EIOC) at PNNL as a research and development environment. The EIOC is a logically and physically isolated network at PNNL that simulates a control center, is connected to multiple asset owners to receive multiple real-time data feeds, and can be configured to support a primary/failover control center environment.

The creation of a control system key management application will provide a key building block to allow the following Roadmap goals to be met:

- Widespread implementation of methods for secure communication between remote access devices and control centers that are scalable and cost-effective to deploy
- Next-generation control system components and architectures that offer built-in, end-to-end security will replace older legacy systems.
- Secure connectivity between business systems and control system within corporate network

While vendors will develop technical solutions for these goals, asset owners will not deploy them without the key management solution.

Benefit summary:

- Deployment of cryptographic technologies for control systems
- Address peer reviewer comments
- Trusted communication for control systems
- Support for current and expected NERC requirements to protect critical information and establish backup control centers
- Impact upon multiple critical infrastructure sectors
- Provide trust within and across organizational boundaries (e.g., support for phasor data, incident response data, etc.) to enable secure sharing of data
- Support for both public key and symmetric key architectures
- Vendor independent solution
- Support for both routable and serial communication environments
- Cost effective solution

5.4 Deliverables

Milestones

- April 2009 – Advisory team meeting at PNNL
- July 2009 – Key Management Requirements Document
- August 2009 – High Level System Design Specifications

Primary Deliverables

- Key Management Requirements Document
- High-level System Design Specifications

6. Centralized Configuration Management for Field Devices

Lead: Jeff Dagle, PNNL
Partners:

6.1 Purpose

This task aims to create a vendor independent software application that will enable asset owners to manage and enforce the configuration of all field devices from a central location.

6.2 Background

Many events occur on a control system network that requires an automated response. For example, an intrusion detection sensor identifies an unauthorized computing device, a field device receives a command using an unexpected protocol, or the configuration of a device is altered. Personnel actions, such as the retirement of an engineer or a change in roles or responsibilities require that access to devices be revoked. Likewise, responding to a natural disaster or the failure of the energy management system may require personnel and computers from other organizations be allowed to communicate with devices on the control center network. The ability to centrally manage changes to field devices does not exist today in an appropriate manner. As control system networks grow in size and complexity, and as regulatory requirements become more stringent, the ability to centrally manage remote devices is crucial to reliable operations.

It is common for substation engineers to have access to all substations operated by the asset owner. If the engineer retires, the individual user credentials must be revoked at all substations or the shared credentials must be changed. If a configuration management application exists, it requires that each substation be accessed in sequence. The other unattractive option is to visit each substation and make changes manually. The ability of an asset owner to meet regulatory requirements is hindered by the lack of a centralized configuration management solution. Specifically, NERC CIP-004 R4.2 states "The responsible entity shall revoke such access to Critical Cyber Assets within 24 hours for personnel terminated for cause and within seven calendar days for personnel who no longer requires such access to Critical Cyber Assets." The proposed solution addresses these needs.

6.3 Scope and Technical Approach

Previous solutions to manage device configuration have been proprietary by vendor or only provide the capability to modify a single device. Processing changes for groups of devices or modifying equipment from multiple vendors is not possible. This project will leverage the Secure SCADA Communications Protocol (SSCP) as the transport mechanism for communicating configuration changes or automated responses to remote devices. The SSCP library contains both encryption and authentication functions to meet the security objective of confidentiality. The SSCP also is designed to communicate these types of messages over the existing communication media with a unique pair of cryptographic keys. Finally, data protection within the SSCP is driven by the type of message; engineering access will utilize both encryption and authentication of the message while SCADA data will utilize only authentication. This provides better security and flexibility.

This project will utilize the Electric Infrastructure Operations Center (EIOC) at PNNL as a research and development environment. The EIOC supports real-time data, historical data, and research environments. The EIOC also contains a variety of vendor equipment. The solution will consist of two main

components, the user interface and an embedded software application that resides in vendor equipment to accept SSCP protected messages and interface and enact the requested change.

The project will utilize an industry advisory team to gather requirements, review the requirements document, and review the high level design for the graphical user interface and the method for communicating changes in a vendor neutral manner. For example, a tagged data approach similar to XML will provide the ability to interface with a variety of vendor products. The advisory team will also be used to further relationships with control system vendors and test concept systems.

Because of the challenges associated with this task identified at the DOE-OE Visualization and Controls peer review in Washington DC in October 2008, and the need to reallocate funding to other tasks, this task was scaled back significantly. FY09 activity will focus on developing a feasibility assessment report to define the challenges associated with this technology, provide a detailed characterization of existing technologies and approaches that are already available in the marketplace, and conduct a gap analysis to determine a focused area of research that may be recommended for DOE to pursue in fiscal year 2010.

The Roadmap goal addressed by this project is "Control system networks will automatically provide contingency and remedial actions in response to attempted intrusions". Other projects exist to develop signature and anomaly based intrusion detection capabilities. This project's focus is developing the automated response portion of the goal. In addition to intrusions, the automated response system can be used to meet regulatory requirements, apply security patches to remote devices, and monitor remote devices for unauthorized configuration changes. Centrally managing device configuration and automated responses directly support the operational needs of asset owners. The proposed solution will provide a graphical application where the user select a single, multiple, or all devices to which a configuration change or response should be made.

Benefits of this task include:

- Revoke access permissions with a single command
- Push software upgrades to field devices
- Operation over both routable or serial communication media
- Vendor independent
- Provide remote engineering access
- Authenticated and encrypted communication
- Enforcement and monitoring of device configuration
- Batch changes to devices to streamline management process and support operational requirements
- Regulatory compliance

6.4 Deliverables

Milestones

- July 2009 – Feasibility Assessment Report and Proposed Development Roadmap

Primary Deliverables

Feasibility Assessment Report and Proposed Development Roadmap

7. Protecting Process Control Systems Against Lifecycle Attacks Using a Trust Anchor Approach

Lead: Adrian Chavez (SNL)
Partners:

7.1 Purpose

This task explores a fundamentally different approach for ensuring process control system security. We introduce the concept of a trust anchor—an independent monitoring and control device that has access to a component's inner workings—that may be integrated into an untrustworthy system to inspect and verify its functions at the lowest level. This technology enables the trust anchor to dynamically monitor software integrity in real time, which greatly increases the risk to an adversary intending to insert malicious code. Sandia has already developed prototype trust anchors, but this technology has not yet been applied to process control system security.

7.2 Background

Critical infrastructure control systems are vulnerable to physical and cyber attack. Securing these systems is a top priority for the U.S., but ongoing efforts ignore important aspects of the information technology (IT) lifecycle and focus primarily on securing the operational phase of these systems. Adversaries have ample opportunity to compromise our critical systems at every stage of those systems' lifecycles.

Our current security techniques, analyzing and testing systems to find vulnerabilities followed by patching those vulnerabilities, is inadequate. This approach can never prove system security; it can only identify specific shortcomings. Our adversaries can rely on our inability to effectively analyze these systems to hide malicious function in hardware or software.

Program obfuscation technology developed by Sandia National Laboratories enables one of the most important features of trust anchors: It obfuscates their functions and renders them tamper-proof in a cryptographically secure manner.

7.3 Scope and Technical Approach

We will develop a prototype trust anchor demonstration on a programmable logic controller to be integrated into a process control system. To both verify the implementation's security and highlight the effectiveness of our approach, we will have a security evaluation performed on the system by an independent organization that routinely performs such services on process control systems. Finally, we will develop a set of use-cases and a plan for commercialization.

7.4 Deliverables

Milestones

- March 31, 2009 – An initial SCADA security scenario developed for the trust-anchor integration.
- June 30, 2009 – Prototype and demonstration of the trust-anchor concept tailored to SCADA environments.
- August 31, 2009 – Results obtained from an independently-performed vulnerability assessment and security evaluation. Final report detailing results achieved in this pilot program.

Primary Deliverables

- Final Report of Pilot Program

8. Anomaly Detection and Distributed Active Response for Control Systems Networks

Lead: Louis Wilder, ORNL
Partners:

8.1 Purpose

This task supports the development of automated, transparent, self learning tools that can predict, detect and respond to threats and attacks on the infrastructure, both physical and cyber. As part of this task, a white paper on "IDS state-of-art and approaches" will be completed before the Project Planning meeting January, 2009. This will be a draft document that will be expanded upon later in the year.

ORNL will develop the Silent Storm technology for distributed cyber-defensive active response to cyber attacks against Process Control and SCADA systems. This work directly addresses the research and development of Silent Storm's ability to detect and thwart the problem of cyber intrusion on SCADA systems.

8.2 Background

Critical infrastructure control systems are vulnerable to physical and cyber attack. Securing these systems is a top priority for the U.S., but ongoing efforts ignore important aspects of the information technology (IT) lifecycle and focus primarily on securing the operational phase of these systems. Adversaries have ample opportunity to compromise our critical systems at every stage of those systems' lifecycles.

Our current security techniques, analyzing and testing systems to find vulnerabilities followed by patching those vulnerabilities, is inadequate. This approach can never prove system security; it can only identify specific shortcomings. Our adversaries can rely on our inability to effectively analyze these systems to hide malicious function in hardware or software.

Program obfuscation technology developed by Sandia National Laboratories enables one of the most important features of trust anchors: it obfuscates their functions and renders them tamper-proof in a cryptographically secure manner.

8.3 Scope and Technical Approach

Currently, the Silent Storm architectural design is developed and the framework is under modification to adapt to the Silent Storm distributed architecture. Anomalous behavior and active response algorithms are being developed as part of the detection scheme. A requisition has been established for the purchase of a Cyber Test Lab from Siemens in support of the development and demonstration of Silent Storm. The Thyme development is on the way for the simulation development of protocol traffic in support of specific test scenarios. In FY 2008 ORNL demonstrated and reported on cyber security attack detection and distributed active response capability using the cyber test lab. In FY 2009 ORNL will continue the development and demonstration of the prototype distributed intrusion detection framework called SILENT STORM by January 7th, 2009.

8.4 Deliverables

- January 7, 2009 – Demonstration of Silent Storm distributed intrusion detection framework

Jan 27, 2009 – "IDS State of the Art" White Paper

9. Trustworthy Wireless for Critical Infrastructure Sites

Lead: Wayne Manges, ORNL
Partners: ANL

9.1 Purpose

Supported by ANL, ORNL will facilitate the development, adoption, and assessment of the options available for asset owners to measurably improve the security, reliability, and resilience (trustworthiness) in their SCADA and other related systems. The need for consistent and effective standards and metrics are identified in the Roadmap to Secure Control Systems in the Energy Sector as a critical priority.

9.2 Background

Much has been attempted in encouraging the adoption of state-of-the-art security measures in Supervisory Control and Data Acquisition (SCADA) systems. Electricity delivery and energy reliability have been identified as "critical" to the nation's infrastructure from both direct and indirect impact aspects and continue with the struggle of what to adopt. This task supports a part of the ORNL vision to assure that strategies for applying standards and/or regulations for secure data exchange and communication with the minimum actual, or opportunity, costs to the energy asset owners. A number of approaches have been identified that can help facilitate the adoption including standardization, industry/government consortia, regulatory pressures, as well as improvements in the quantitative understanding of the risk-benefit-cost triumvirate. ORNL's leadership in the development and adoption of robust, secure, reliable wireless communication for harsh environments has resulted in ORNL's strategic position with respect to existing and emerging standards for wireless communication including those used by SCADA systems.

Energy asset owners are facing a monumental challenge as they address compliance with the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Standards (CIP-002 through CIP-009). The increased use of wireless technologies and their introduction into control center networks and field devices compound this challenge, as ambiguity exists regarding applicability of the CIP requirements to wireless networking technologies. The requirement to monitor and control a utility's Electronic Security Perimeter (ESP) is defined in CIP-005. While wireless is neither explicitly included nor excluded from the requirements, wireless technologies provide electronic access and therefore must be considered under CIP-005.

9.3 Scope and Technical Approach

ORNL proposes the following key activities for FY2009:

- Support the ISA100 standards (Wireless Industrial Automation) development activity providing focus on the needs of the electric power industry.
- Provide leadership and support the ISA100 working group formed in 2007 focused on wireless trustworthiness. The working group conducts through bi-monthly telephone meetings and at least four face-to-face meetings during the year.
- Investigate the intersection of enterprise policy, regulatory compliance, and physical systems along with the technological options regarding deploying wireless technology in critical-infrastructure-protection designated utility sites.

- Prepare a specifications document describing the options for high security, high reliability application domains. The document will describe quantifiable performance with respect to reliability, throughput, range, latency, and security.
- Continue to integrate the above work with ongoing activities with DHS and DOE/EE related to wireless deployment in critical infrastructure sites.
- Facilitate the publication of the draft ISA100 TWWG work product "Trustworthiness in Wireless Industrial Automation."
- Configure an appropriately equipped laptop for testing against an existing SCADA system and document in a detailed report, suitable for publication, on the vulnerability testing of the wireless-enabled laptop in a prototypic SCADA System environment

A key potential vulnerability identified in numerous assessments involves the use of a laptop (or similar device) containing wireless interface capability inside the ESP. This activity will experimentally determine the system vulnerability of such a scenario and quantify the associated risk. This involves the following activities:

- Document and validate the scenario with participants from the utility industry and prepare a detailed test plan describing the actual test to be performed.
- Configure an appropriately equipped laptop for testing against an existing SCADA system.
- Execute the test planned and document the outcome with a detailed report suitable for publication.

9.4 Deliverables

- September 2009 - "Trustworthiness in Wireless Industrial Automation" - Draft ISA100 Trustworthy Wireless Working Group (TWWG) work product
- September 2009 - Report on the vulnerability testing of the wireless-enabled laptop in a prototypic SCADA System environment

10. Process Control Security under Future National Grid Conditions

Lead: Steve Fernandez, ORNL
Partners: EnerNex

10.1 Purpose

Programs conducted under the National SCADA test bed have developed a number of new secure network technologies that include proof-of-concept models and architectures with sensor systems implemented at the individual component level. However, to reach the Roadmap goal of wide spread deployment of these secure technologies, application of these technologies to all components of the national grid simultaneously is not required. The optimum trade-off between cost, utility buy-in, security reliability and resilience may require only the most critical components to receive the maximum level of protection or the greatest number of layers of defense in depth. The first objective of this study is to provide an efficient, accepted way to identify where the critical control systems that should be high-priority deployments are located within the grid. The study's second objective is to perform a pilot study with the cooperation of Consumers Energy of such a system within the Michigan distribution system.

10.2 Background

One specific challenge faced by the bulk electric system asset owners and operators working to meet the recently approved NERC CIP standards is the identification of cyber assets that are considered to be "essential" the power system elements identified as Critical Assets. The CIP 002-009 standards define the minimum requirements for the protection of these cyber assets which are referred to in the standard as Critical Cyber Assets. Cyber assets which do not meet the definition of "essential" are generally exempt from the NERC CIP requirements if they are not in the same electronic security perimeter. With the initial approved version of the NERC CIP standards, each utility may apply its own methods to categorize a cyber asset as "essential" or "non-essential". In most cases, the methods used for this categorization are typically based on a static model referenced back to the local critical asset(s) (such as a transformer or circuit breaker) and not the power system as a whole. This method is typically effective in finding the risk to the power system associated with direct relationships (i.e. Control System Element-to-Power System Element). It is not effective however, in identifying the risk to the power system associated with indirect relationships (i.e. Control System Element-to-Control System Element-to-Power System Element). In reality, control systems which are utilized today within the electric utility industry contain numerous components and have become increasingly integrated with other systems as well as the power grid itself creating numerous interdependencies. Utilities need to be able to consider both direct and indirect relationships when evaluating risk to the power grid at large associated with the compromise of any control system cyber asset. The benefit from this study would be development of a method to prioritize the deployment of critical new secure control systems.

Methods for looking at critical nodes have been explored since the mid-1990s evolving into the concept of a network's critical mission that must be served as described in 2005 by Quirk and Fernandez. (Quirk, Mihaela D. and Fernandez, Steven J. (2005) "Infrastructure Robustness for Multiscale Critical Missions," *Journal of Homeland Security and Emergency Management*: Vol. 2 : Iss. 2, Article 2.)

This analysis showed that the removal of a few highly connected nodes can cause a network to fail (by dividing the network into isolated islands of connectivity). However, the division of a network into pieces still capable of delivering the critical mission does not create a disruption until the pieces no longer have the attributes necessary to deliver the needed service. The smallest piece of power grid capable of

continuing critical service is called the *critical subnetwork.* A node whose loss separates a part of the grid into a piece smaller than the critical subnetwork then becomes a critical node where advanced secure control system architectures and technologies should be deployed first.

Critical sub networks were observed in the wider power grid when an island was created within the southern Louisiana area after a few critical nodes within the Entergy system were knocked out by Hurricane Gustav.

The analysis of dynamic networks such as the wide area grid complicates the identification of these critical nodes because active control systems will cause the pieces or critical subnetworks to constantly shift and re-configure in order to maintain critical service. Static maps of a network's connectivity (like a scale free network topology) do not provide a true picture of a dynamic network's operation. In addition to resiliency and self-healing effects, this dynamism also creates a new set of vulnerabilities. If one very simply assumes that the critical nodes are those either showing the highest connectivity or the highest loads, cascading failures can create other vulnerabilities to cascading failure by:

- **Load redistribution.** In most infrastructure networks, the loads carried by each node on the network are dynamically redistributed. If a network node is lost, due to accident or attack, the load that node carries is rapidly distributed to the other nodes on the network. In turn, these new nodes were not critical at the beginning of the event, but become critical as the event unfolds, perhaps in the matter of seconds.
- **Hi-load nodes and failure.** If a high-load node is removed from the network, the load it carries is redistributed to other nodes on the network. This increased flow causes less capable nodes to exceed their capacity. To protect these nodes from damage, control systems will automatically force the overloaded node to fail-over (shut down) creating new, smaller network pieces or critical sub networks. In other parts of the grid, the increased congestion will cause the overloaded node to become inefficient (bog down). Regardless, the result is a series of shut-downs or slow-downs that "cascade" through the network as the excess load is pushed to the next available node creating divisions smaller than the critical sub network geographically far from the original point of attack.
- **Network suppliers.** Some networks are vulnerable to undersupply (gas, electricity, and water). In these networks, an attack on a supply facility or connections from a supply facility will produce network failure as undersupplied nodes pull resources from the rest of the network.

10.3 Scope and Technical Approach

Oak Ridge National Laboratory has a proven track record of developing and demonstrating process control features on scales greater than proof-of-principle network pieces. This experience has been codified in a variety of local tools and models that can be easily adapted to model collections of critical sub networks, which in turn provide the capability to evaluate the impact of intrusions on re-configuration of these critical sub-networks. Further, ORNL has the ability and expertise scale up the models to evaluate reconfiguration of the grid using large scale simulations, thus enabling a sophisticated prediction of critical function availability required to meet the Roadmap end state.

This task will evaluate the approach of protecting critical sub networks as a reconfiguration strategy and assess the secure control system requirements to protect those critical sub networks. As architectures, strategies, policies and technology black boxes are proposed; a methodology is required to evaluate the comparative increases in reliability and security obtained.

This methodology will encompass tools and methodologies that enjoy consensus utility acceptance to support the utility business case for additional control system security. To understand the scope, magnitude, and priority of risks associated with distributed potential intrusions in a large scale system

composed of many critical sub networks, this task will develop a framework for organizing, aggregating, and prioritizing risks to maintaining grid critical functionality.

The primary deliverable of this task will be a draft framework requirements document. A simple ORNL model of the Michigan transmission grid and service area (~ 10^4 nodes) will be used to build the network models that could be used to "automatically provide contingency and remedial actions in response to attempted intrusions." Responses and reconfigurations in response to varying levels of penetration will be tested against the Michigan model. Increased penetrations would be modeled until reconfiguration can no longer maintain the service to the networks' critical functions.

10.4 Deliverables

- September 30, 2009 - Draft Framework Requirements Document

11. Cyber-Physical Attacks and Cyber-Physical Security: The Second Line of Defense

Lead: James Nutaro, ORNL
Partners:

11.1 Purpose

A practical cyber security system must keep intruders at bay and work harmoniously with the control system: if the imposition of effective security significantly degrades the control process, then the security solution is not practical. This task will demonstrate a framework and methodology for answering this critical question,

11.2 Background

Physical systems that are controlled by a computer over communication networks are susceptible to physical damage – even catastrophic failure – due to the action of the computer and behavior of the communication network. Control systems are designed to fail safely, but to decide which automatic safeguards must be part of a system engineers must carefully consider how a machine can fail, how often those failures are expected to occur, and the consequences of each type of failure. Malicious failures – computer failures due to cyber-attacks – upset these careful calculations. An attacker conducting the same risk analysis will find rare, but severe, types of failures that a reasonable design would omit from the set of installed safeguards. Having found these failure modes, an attack is designed to induce them with dangerous, possibly terminal, results.

To be effective, an approach to security for a control system must account for two facets of the control system that are inextricably linked with cyber-security. First, how does the control system respond to a cyber-attack which penetrates some distance into its computers and communications network? This is a question of vulnerability to cyber-security threats, and it is being addressed by our proposed task 2.4D and by related activities at the Sandia and Idaho National Laboratories.

The second facet is how the control system responds to a *working cyber-security system that keeps malicious users out*: what are the risks of *success*? Every security measure imposes a burden on the computers and communications network that the control system relies on for sensing and actuation, and this additional burden changes the dynamic performance these critical resources by adding delay, inducing jitter, and otherwise consuming resources that were previously available for control activities.

Before any security technology can be safely deployed within a critical control loop, it is essential to understand what effect this deployment will have on the dynamic performance of the controlled system. At worst, increased delay and greater jitter can destabilize the control system; at best there is some degradation in performance. Before a utility can accept a new security technology, it must have a reliable answer to three questions: how will the security measure degrade the dynamic performance of my control system, can I mitigate these effects, and is the loss of performance acceptable?

11.3 Scope and Technical Approach

ORNL proposes the following key activities for FY2009:

- A case study for the impact of cyber security overheads on control system performance at one of the critical sub-nodes identified in the Michigan transmission grid and service area model. This

analysis will consider the effect on the control system of 1) the extra network and computation load induced by the cyber-security system during normal operations, and 2) the reduced availability of computer and communication resources while an intrusion is being actively and successfully countered.

- Within the context of this case study, look at the mitigating effect of using alternative control schemes which may be more robust to disturbances in the control network.
- Provide a report describing our findings and making recommendations for an approach to future studies aimed at assessing the impact of cyber security features on control system operations, and the possibility of mitigating these effects by use of alternative or enhanced control technologies.

11.4 Deliverables

- Case study of cyber security overheads on control system performance at a critical sub node
- Report and a demonstration of the cyber-physical defense technology.

12. SCADA Systems Cyber Security Testing Through Portable Acceptance Test Apparatus and Protocols (PATAP)

Lead: Wayne Manges
Partners:

12.1 Purpose

This task supports the part of the vision to provide an honest broker environment where the business cases for investment in control system security advances can be developed within the existing energy asset owner business cases, independent of specific procurement sensitive constraints.

12.2 Background

Asset owners today are diligently awaiting the delivery of SCADA systems with the appropriate mix of cyber security, reliability, performance, and functionality. The suppliers are diligently working to deliver on the customer requirements while running a sustainable business. All of this depends on clearly understanding all stakeholders' expectations. The procurement process today is fraught with difficulties. One of these is the traditional acceptance test, usually carried out at the vendor site under very controlled conditions. Many times, the rosy results from the factory acceptance tests are not reproducible under the conditions of the actual deployment. We propose to begin the process of developing a solution to this dilemma by specifying, developing, and deploying, for use by end users and suppliers, a portable acceptance test apparatus and protocol that assures the performance specifications are met under the conditions specified.

12.3 Scope and Technical Approach

The PATAP would include hardware and software to connect to the system under test (SUT) and simulate analog, discrete, and network traffic typical of the final applications. Atypical situations would then be simulated to ensure that the SUT responds as expected. The fidelity of the simulations driving the apparatus would hinge on the fidelity of the models driving the outputs that are fed into the SUT. The closer the I/O and traffic can be made to simulate the actual deployed conditions, the more robust the test. The key is to use deterministic approaches to simulating the conditions, rather than stochastic.
The project would start with defining the requirements, developing specifications for the appropriate hardware and software, and then developing prototype software modules to provide the simulated I/O and traffic. The outcome would be a transportable set of hardware and software that can be used to execute more prototypic acceptance tests at vendor (or third party) sites.
The entire test system would be developed using open standards, as much as possible, so that others could provide suitable models and software modules. Since no proprietary hardware or software would be used, any vendor or end user could replicate the apparatus for its own use. Upgrades would be available as they are developed.

ORNL proposes the following key activities for FY2009:

- ORNL will develop system requirements document describing the testing system to be developed.
- ORNL will develop specifications for the hardware and software needed to fabricate the prototype system for testing.
- ORNL will procure the needed hardware and software to fabricate the test apparatus.

- ORNL will develop the modular software tools to facilitate the future development of models for component, subsystem, and full system testing.
- ORNL will package the test apparatus and demonstrate the feasibility of using the apparatus to perform acceptance testing on a suitable system under test at a specified site witnessed by the purchasing end user.

12.4 Deliverables

- Detailed System Requirements Document describing the functional, operational, and design requirements for the final product. Detailed specification for the design, fabrication, and deployment of the testing apparatus and protocol.

13. Cyber Security Audit and Attack Detection Toolkit

Lead: Dale Peterson**,** Digital Bond, Inc.

Partners: OSIsoft, Tenable Network Security, Constellation Energy, PacifiCorp Tennessee Valley Authority

13.1 Purpose

This two-year project aims to integrate control system intelligence into widely deployed vulnerability scanners and SEM, and to integrate security incident detection intelligence into control system historians. These upgrades will be provided at no or a low cost to control system asset owners. This task is aligned with the following Roadmap goals: Measure and Assess Security Posture, Detect Intrusion and Implement Response Strategies and Sustain Security Improvement.

13.2 Background

While many energy utilities employ vulnerability scanners and security event managers (SEM) on their enterprise systems, these tools often lack the intelligence necessary to be effective in control systems. There is a need to identify vulnerable configurations in control system devices and applications. This task aims to integrate vulnerability detection and security event management capabilities into systems currently deployed by a majority of the energy community.

13.3 Scope and Technical Approach

The security components of this project were designed and tested in three phases. The first phase was the development of the vulnerability scanner. The team selected 20 control system applications (e.g. real-time servers, historians, etc.) from owner participants, and collected system data from asset owners and vendors. They then created ".audit" good practice configuration files, and test these files on asset owner systems.

The second phase consisted of lab and field testing. Project team collected security data from asset owner's PI systems. Security events from data were identified, and used to develop "meta events" that can be detected as cyber attacks. These meta events were written into ACE incident detection modules, and tested on asset owner PI systems for two months. The third phase was the development of the Enterprise SEM. The team integrated the ".audit" files and ACE incident detection modules into the Tenable Security Center SEM. They identified enterprise SEM meta events from control and enterprise information, and test at asset owner facilities with a custom SEM.

13.4 Deliverables

Milestones Accomplished in 2008

- Completed installation and training of OSIsoft software
- Identified candidate systems and applications at asset owners for Nessus security audit files
- Developed Bandolier Security Audit Files for ABB, Siemens, SNC and Telvent

Milestones Planned for 2009

- Bandolier: Nessus Audit Files available on subscriber site.
- Portaledge: Release Version 1 ACE incident detection modules for testing at asset owner sites.
- Collect data from 20 systems

- February 2009 – Portaledge Attack Detection Modules
- April 2009 – Data collection from 20 systems for Nessus audit files

Primary Deliverables

- February 2009 – Version 1Portaledge Attack Detection Modules
- 2009 – Bandolier audit files for Areva, Emerson, Matrikon, OSIsoft, Wonderware

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

Lead: Alfonso Valdes, SRI International
Partners: ArcSight, Sandia National Laboratories, Invensys

14.1 Purpose

This project will develop intrusion detection systems (network, host, and device-level), event correlation framework, and a sector-wide, distributed, privacy-preserving repository of security events.

14.2 Background

Detecting cyber attacks against digital control systems quickly and accurately is essential to energy sector security. Current intrusion detection systems (IDS) continuously scan control system communication paths and alert operators of suspicious network traffic. But existing IDS, often not tailored to the control environment, typically offer limited attack response capability and frequently produce false alarms or fail to alert. Without carefully deployed monitoring, these devices can produce an overwhelming number of alarms that become difficult to correlate. This introduces system communication latency and slows incident response time.

14.3 Scope and Technical Approach

The two-year Detection and Analysis of Threats to the Energy Sector (DATES) project is a groundbreaking effort to develop the first integrated intrusion detection, security incident/event management (SIEM), and large-scale threat analysis capability for the energy sector. DATES will provide control system operators with enhanced incident detection and alerting tools through rigorous monitoring of threats at the network, host, and device levels. Integrating SIEM capabilities, the system will use attack models and information from prior events to automatically correlate alarms, distinguishing malicious cyber incidents from minor disruptions.

Additionally, utilities can lack an anonymous method to share threat information across the sector, which limits owner/operator threat visibility to what they can record on their own systems. DATES will create an anonymous global threat database, allowing utilities to securely report their threat data. System owner/operators can then view other sector security events in real time to obtain an accurate, high-level view of their security posture. Improving and integrating these security features will create an unprecedented defense system against increasingly sophisticated cyber attacks.

14.4 Deliverables

Milestones Accomplished in 2008

- Completed and delivered PCS-aware network IDS, including model-based detection for defense against 0-day attacks.
- Completed initial integration of the above IDS with the ArcSight Security Information/Event

Milestones Planned for 2009

- Complete initial installation of experimental DCS System at SRI.
- Integrate of IDS, SIEM with the DCS test bed.

- Implement comprehensive test mod/sim environment at Sandia with realistic process control system traffic and power model.
- Begin initial testing and refinement of DATES attack detection techniques using SRI and Sandia test environments.
- Extend/distribute models and simulations to represent larger scale systems.

Primary Deliverables

- 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

15. Lemnos Interoperable Security Program

Lead: Vishant Shah, EnerNex Corp.

Partners: Schweitzer Engineering Laboratories, Sandia National Laboratory, Tennessee Valley Authority

15.1 Purpose

The purpose of this project is to help vendors create more reliable, clearly defined, and interoperable security devices by following an agreed-upon set of vocabulary and metrics. If all vendors used this language, system operators could purchase two different products from two vendors knowing they would operate together and be interchangeable with other vendors' devices. This project is aligned with the Roadmap goal Detect Intrusion and Implement Response Strategies.

15.2 Background

As energy control systems employ more Internet-based features and routable communication methods, the need grows for enhanced security functions, such as firewalls, virtual private networks (VPNs), and intrusion detection systems. When purchasing network security products, today's control systems users cannot adequately compare products from different vendors because the industry lacks a widely accepted mechanism for evaluating functionality, performance, and interoperability. Different vendors offer products described in undefined terms, and the functional scope of one product rarely maps directly to another.

This lack of common definitions and metrics limits an organization's ability to effectively evaluate and compare products and security solutions, and heightens the risk of introducing incompatible products to the system.

15.3 Scope and Technical Approach

Project partners will independently create two pieces of a security function—a VPN tunnel—based on the newly developed vocabulary. The products will then be lab and field-tested to demonstrate their ability to effectively operate with each other in a control systems environment.

Development will be conducted in three phases. In the first phase EnerNex and project partners will conduct interviews to determine the functional and non-functional requirements for the OPSAID-defined security functions. For each function, the team will develop universal vocabulary, metrics, and testing procedures.

In the second phase, both Sandia National Laboratories (SNL) and Schweitzer Engineering Laboratories (SEL) will develop counterparts of a VPN tunnel, each designed to perform the same function. SNL will develop a reference implementation using open-source software, while SEL will develop a proprietary commercial prototype. Both partners will test their products individually for functionality, then the team will point the devices at each other across the Internet to see if they operate together. If lab tests are successful, the devices will be field tested at Tennessee Valley Authority (TVA) to evaluate control system impact.

In the final phase, the team will actively participate in conferences and trade shows to exhibit interoperability of the reference implementation and prototype. The team will invite industry members to a Plugfest, where other vendors can connect their products with the reference implementation to demonstrate their devices' interoperability.

15.4 Deliverables

Milestones

- Implement selected functional requirements in an open source reference design and commercial prototype.
- Tools for testing and validation of functionality and performance
- Specifications for vendors to participate in interoperability testing

Primary Deliverables

- June 2009 – Independent tests of respective designs, followed by interoperability testing at factory and lab facilities
- December 2009 – Preliminary interoperability testing with vendors using internet connections and in-person trials at TVA labs
- March 2010 - Presentation at DistribuTech

16. Protecting Intelligent Distributed Power Grids against Cyber Attacks

Lead: Dr. Dong Wei, Siemens Corporate Research

Partners: Center for Advanced Energy Systems at Rutgers University, Idaho National Laboratory, Siemens Power Transmission and Distribution

16.1 Purpose

This two-year project will develop a novel distributed and hierarchical security layer specific to intelligent grid design. This task supports the Roadmap goal Detect Intrusion and Implement Response Strategies.

16.2 Background

Intelligent power grids are interdependent energy management systems—encompassing generation, distribution, IT networks, and control systems—that use automated data analysis and demand response capabilities to increase system functionality, efficiency, and reliability. But increased interconnection and automation over a large geographical area requires a distributed and hierarchical approach to cyber security.

16.3 Scope and Technical Approach

A hierarchical power grid security system will be developed to produce an automated risk assessment graph of the physical grid that uses advanced simulation, machine-learning capabilities and dynamic evolution to identify threats based on simulation exercises and attack history. The hierarchical power grid security system will consist of three components: 1) security agents residing in or next to field devices and controllers; 2) security switches at the substation control level; and 3) security management systems distributed across the grid at the enterprise layer. Security agents will perform simple logging, reporting, and detection, while switches will manage data traffic and detect intrusion using network rules. Security management systems will generate new policies and updating existing ones based on simulation and historical information. These advanced management systems will connect to switches and agents, work as AAA (authentication, authorization, and accounting) servers, and acquire security patches and distribute them to control system components.

A network topology optimizer will also be developed to determine the best location (field device, substation control and enterprise level) for agents, switches, and management systems to ensure active contribution to network security. This distributed, hierarchical approach has the potential to offer an unmatched security solution for advanced power grids.

The project consists of two phases. In phase 1 (Design and Develop), the impact of cyber attacks on power control networks will be investigated to develop the risk-based critical asset identification system, including models and algorithms. In phase 2 (Test and Verify), the prototype software for risk analysis and security configuration optimization will be tested and verified. Two rounds of testing will be conducted at Idaho National Laboratory on the security agent, security switch, security manager and security integration configuration software.

In 2009, a technical advisory board with representatives from the power industry was assembled to guide R&D efforts.

16.4 Deliverables

Milestones Accomplished in 2008

- Investigation and technical report on potential cyber attacks and their impacts in power control networks
- Investigation and technical report on risk based critical asset identification systems
- Technical specification (system design) for integrated security system
- Topical report (assessment model) for risk assessment and critical asset identification

Milestones Planned for 2009

- April 2009 – First on-site test of the integrated security system at INL
- June 2009 - Software demo of risk assessment and security optimization system
- August 2009 – Second on-site test of the integrated security system at INL
- Develop educational materials for a graduate seminar course to be taught at Rutgers University
- Establish general guidelines for future product development and commercialization

Primary Deliverables

- September 2009 - Technical report of integrated security system
- September 2009 – Technical report of risk assessment model and tools

17. The Hallmark Project

Lead: Rhett Smith, Schweitzer Engineering Laboratories, Inc.
Partners: Pacific Northwest National Laboratory, CenterPoint Energy

17.1 Purpose

This project will commercialize the Secure SCADA Communications Protocol for secure, encryption-free communications between serial devices. SSCP provides message integrity by marking original SCADA messages with a unique identifier and authenticator before sending. The receiving device will scan the identifier and validate the message before enacting the command. Unauthenticated commands are logged and reported as errors. This project contributes to achieving the Roadmap goal of Detect Intrusion and Implement Response Strategies.

17.2 Background

Increased connectivity and automation in the control systems that manage the nation's energy infrastructure have improved system functionality, but left systems more vulnerable to cyber attack. Intruders could severely disrupt control system operation by sending fabricated information or commands to control system devices. To ensure message integrity, supervisory control and data acquisition (SCADA) systems require a method to validate device-to-device communication and verify that information has come from a trusted source and not been altered in transit. There is a lack of tested and validated security tools for message authentication.

Current technologies in the market offer message confidentiality by encrypting text upstream of modem-sharing devices; this eliminates the operational ability of skilled personnel or protocol analyzers to read messages, and is often a vendor-specific technology. The SSCP technology will offer a standard approach to message authentication without encryption.

17.3 Scope and Technical Approach

Over three years, the project team will implement this technology as a cryptographic daughter card (CDC), a hardware solution that Schweitzer Engineering Laboratories (SEL) will incorporate into a serial bump-in-the-wire device. This device can be applied easily to any legacy or existing control system without equipment reconfiguration or reprogramming. The team will validate the card under Federal Information Processing Standard (FIPS) 140-2, which accredits cryptographic technology. The CDC will also be available to other vendors, who can use it to increase security by adding cryptographic controls to both existing and future products.

Phase 1: Development of CDC and Integration into Link Module

- Establish method to transfer Secure SCADA Communications Protocol (SSCP) technology to the cryptographic daughter card (CDC) hardware component
- Translate the SSCP technology into a protocol-independent CDC
- Develop the CDC into a new bump-in-the-wire link authenticator module, expanding the SEL-3021 Serial Encrypting Transceiver product line
- Commercially produce and test the product at SEL's facilities

Phase 2: Lab and Field Testing

- Conduct a laboratory test of the link module (with integrated CDC) at CenterPoint Energy's test energy management system

- Measure control system and operator impact and communication latency
- Perform a two-month field test at CenterPoint Energy to demonstrate interoperability and identify lessons learned from an asset owner's perspective
- Compile extensive reports analyzing: impact to the end user; impact to the control system; and best practices for implementing this new technology
- Achieve FIPS 140-2 validation

17.4 Deliverables

Milestones Accomplished in 2008

Card Accomplishments:

- Designed, developed, tested and completed the software interface
- Designed and developed the framework (every function of the card besides protocol implementation)
- Began Protocol

Host Accomplishments:

- Began design work on PCB for host
- Began architectural design of the host system
- Began development of the web server and TCP/IP stack

Milestones Planned for 2009

- April 2009 – Deliver Working Prototypes
- September 2009 – Complete Field Testing at CenterPoint and PNNL
- August 2010 – Complete hardware based type and functional testing

Primary Deliverables

- Cryptographic Daughter Card (CDC) hardware for message authentication
- Commercial Prototype Bump in the Wire Module Integrating CDC

INTEGRATED RISK ANALYSIS

18. Threat Characterization

Lead: J. Michalski, SNL

18.1 Purpose

The information generated from this task will reduce the risk of energy disruption by providing utility owners with actionable threat information to facilitate corrective mitigation actions to be taken against the threat.

18.2 Background

The Threat Characterization task will provide a framework and tool for leveraging open and closed source data to better quantify the level of threat in terms that are meaningful to the energy asset owners. The threat characterization framework and discovery task will enable asset owners to receive actionable, well-defined threat information that is unclassified. An open web threat discoverability analysis is conducted to help answer the question: If an adversary wanted to know how to do 'bad thing X', could they learn how to do it from the Open Web? This is the first phase of our Threat Assessment process. In the second phase, we attempt to answer the question: Is adversary 'A' interested in a capability for doing 'bad thing X'?

18.3 Scope and Technical Approach

The approach in developing a represented tool (or suite of software tools) for threat discovery has been defined in a series of "process steps". This approach provides a means for systematically gaining insights to questions that would otherwise be difficult to obtain by other methods. Substantial progress has been made in FY07-FY08 to refine and integrate these steps in a suite of software tools and some initial results were obtained. Additional work is needed to improve on the techniques used in each of the steps and to provide a more automated approach in processing and interpreting the large-data sets that are presented to the analyst.

As the discovery process continues to mature, it is planned to use (in FY09) other datasets that have captured and cataloged large sets of pro-Islamic web sites. Currently, the data set we have identified comes with an English languish translation interface. This set will be used to answer the question: Are there any adversaries interested in exploiting any "discovered" vulnerability against the energy infrastructure? Once access to these new data-sets has been gained, the additional analysis results will be included as part of the quarterly threat discovery analysis reports.

18.4 Deliverables

Milestones

- February, May, August – Quarterly 2009 – Provide quarterly threat discovery analysis reports
- January-September 2009 – Provide Threat Analysis support to Task #4.

Primary Deliverables

- Threat Discovery Analysis Reports

19. Real Time Security State Visualization Tool

Lead: PNNL **Partners:** Stanford Graphics Lab, Schweitzer Engineering Laboratories, ANL
Technical Advisors: Alliant Energy, El Paso Corporation, Ergon Refining Inc., NiSource, Control Center Solutions LLC, Progress Energy, Alyeska Pipeline Inc., Entergy Corporation

19.1 Purpose

When implemented, the technology will be scalable to provide regional or national views, enabling event correlation, drill-down capabilities for detailed information, and provide multiple data feeds supporting different data formats.

19.2 Background

True situational awareness of energy infrastructure operations depends upon multiple factors. With the introduction of new technologies intended to enhance the security of control systems, there are additional requirements to monitor the real-time state of these security systems as deployed. Without this monitoring, there could be a false sense of security. This project will bring together various aspects of perimeter security, network traffic analysis, signature-based intrusion detection systems, and other security technologies into a visual environment to measure the real-time state and security level for the infrastructure as currently deployed.

19.3 Scope and Technical Approach

The technical approach will be to interface with other DOE control system security interfaces with multiple vendor data feeds are projects. A standard data interface will be developed to ensure the supported. The project will be guided with an industry advisory team. ANL is also supporting this project.

The advisory team was assembled in June 2008 and has scheduled its first meeting for December 2008. The team assembled an advisory team of utility and energy industry organizations to guide the team in determining what events should be monitored, how events should be correlated, and how events should best be displayed and reported.

PNNL is preparing information on project scope, representative display technologies, and event correlation and aggregation for the FY09 advisory team meeting.

This is the second year of a three year project. The focus of the second year (FY09) will be development and demonstration, with the third year (FY10) technology transfer.

19.4 Deliverables

Milestones

- April 2009 – Advisory Team meeting at PNNL
- September 2009 – Conceptual demonstration using the PNNL EIOC

Primary Deliverables

- Conceptual Demonstration

20. Virtual Control System Environment (VCSE)

Lead: R. Halbgewachs – SNL
Partner: DTE Energy

20.1 Purpose

Given a cyber-threat, the Virtual Control System Environment (VCSE) task will help asset owners and analysts understand what effects can be achieved on control systems if the threat were to be realized. This task will develop a modeling and simulation tool that can be used to analyze and assess threats and cyber vulnerabilities on control systems (CS) without risking disruptions to critical operations. The tool will also provide the means for evaluating selected mitigation options.

20.2 Background

Modeling tools such as the VCSE are needed to combat the challenging technological complexities associated with securing not only legacy systems but also for the integration of emerging control system components and system architectures. As control system architectures grow in complexity and interconnectivity with other networks, exposure to more sophisticated threats, and the trend toward incorporating conventional information technology (IT) solutions, modeling and simulation tools will be needed to assist asset owners in making better-informed decisions in the selection of security solutions for their current and next-generation systems.

20.3 Scope and Technical Approach

VCSE will permit the end-user to configure a simulation environment of control system devices and network communication protocols and enable real-time, hardware-in-the-loop connectivity for the purpose of understanding the effects of cyber-vulnerabilities on CS. The VCSE will reduce the risk of energy disruption by providing a realistic setting designed to replicate portions of a vulnerable infrastructure against which cyber attacks can be played out and effective mitigation tactics developed with no threat to the actual infrastructure.

20.4 Deliverables

Subtask 1: Develop a Regional Power System Model

This subtask will comprise the development of a regional power model with enough depth and breadth to explore several scenarios (see subtask 2 below) and required analytics from those scenarios. The term "regional" remains to be defined at this point, but is meant to be an area in scope larger than a single metropolitan area. The final definition will be coordinated with the Summer Workshop Planning Group in support of the scenarios to be modeled and analyzed.

- This model will be representative of the region in that there will be a rough similarity in terms of generators and generating capacities, load distribution regions, and protection mechanisms.
- The model will be developed from open source information as can be gained from web searches and open literature. This information may be augmented by interviews with subject matter experts (SMEs).
- The model will be validated with SMEs both within and outside of Sandia National Laboratories.

Subtask 2: Scenario Simulation and Analysis

This subtask will work with other NSTB projects (Specifically the threat analysis project) to develop different power system scenarios using the model developed in subtask 1 to analyze vulnerabilities and potential mitigations to those vulnerabilities. This task will include:

- Simulated attack vectors
- Appropriate visualizations to aid in analysis and explanation to interested stakeholders
- Quantitative analysis of the cyber effects and impacts

Subtask 3: VCSE Framework Software Enhancements

This subtask will provide the needed software and development needed to meet the needs that will arise as a result of the modeling and analysis needs and continue to mature the VCSE technology readiness level. One of the goals of the VCSE Project is that any effort or support related to the development of any software or models for specific tasks or analyses, will also be applicable to the improvement of VCSE proper. Enhancements to be delivered during FY09 will include:

(a) provide an improved and dynamic power system model,
(b) extend model scalability,
(c) design & develop breaker and power flow methods,
(d) fully integrate SoftPLC and DNP3 into VCSE,
(e) develop enhanced visualization capabilities for model representation and results analysis,
(f) develop new user interfaces for the ease of scenario development and VCSE usability,
(g) continue improvement and optimization of the core VCSE framework.

Subtask 4: VCSE Project Management

This task provides project management oversight for the overall operations of the VCSE work package. Activities associated with this task are: day-to-day management of the technical activities; the creation of a project plan and schedule for the development effort; establish software build-dates; provide cost, schedule, and performance status; manage internal and external interfaces; track changes, issues, and risks; and be responsible for the execution of the VCSE WP.

- Monthly – Provide monthly status reports
- Quarterly 2009 - Review meetings with the other NSTB task leads to gain further understanding of each work package's progress and deliverables and to develop interface requirements for integrating the other work packages into the VCSE test bed.

Milestones:

- April 2009 – Initial regional scale power model available and validated
- April/May 2009 – Scenario tested and analyzed against the regional scale power model.
- August 2009 – Simulation Development & Validation scenarios completed.
- September 2009 – Final report delineating the results of the simulation and analysis of the scenarios defined for the NSTB workshop.
- September 2009 – Project accomplishments and status report.

Primary Deliverables

- Final Report
- Project Accomplishments and Status Report

21. Impact Analysis of Cyber Attacks on Control Systems

Lead: J. Stamp and R. Laviolette, SNL

21.1 Purpose

This task provides a means to estimate electric supply interruptions that can be caused by cyber attacks

21.2 Background

In previous years, the work has focused on defining the cyber-to-physical bridge (linking cyber attack to grid events), developing prototype algorithms (for quantifiable impacts to reliability, and finite-state abstraction of dynamic grid and control system models), and second-generation versions of those algorithms (published work for the reliability analysis and extended detail in the dynamic models). The finite-state abstraction (FSA) work shows considerable promise to illuminate previously undetected opportunities for cyber attackers to cause a significant grid impact.

21.3 Scope and Technical Approach

We will continue to develop the FSA work to answer a very specific, pressing issue for impacts analysis: what is the sensitivity of key grid control setpoints in vulnerable cyber devices to grid operations and stability? Setpoints can include things like scheduled interchanges of power, diagnostic criteria for device malfunction, or safety settings (to detect when a line has touched grounds, for instance). To this time, there is absolutely no approach for these analyses extant.

Determine sensitivity of grid dynamic performance to grid control setpoints:

- Subtask 1: Develop metrics for grid performance that work effectively with FSA
- Subtask 2: Build sensitivity analysis technique for selected grid control setpoints
- Subtask 3: Test algorithms on representative systems

21.4 Deliverables

Milestones

- April 2009 – A technical report describing the advancements and results of this research

Primary Deliverables

- Final Technical Report

22. Risk Analysis / Outreach

Lead: L. Phillips - SNL

22.1 Purpose

Identify and rank electric power assets that if attacked would result in a disruption to the electric power grid and cause the greatest consequence (economics, human lives, etc).

22.2 Scope and Technical Approach

- Identify cyber-attack scenarios that can cause the greatest disruption to the U.S. power grid?
- Map electric power (EP) vulnerabilities to the scenarios?
- Characterize the types of installations most susceptible to the identified vulnerabilities?
- Provide regional or state locations as to where the U.S is most vulnerable?

Assumptions:

1. The threat is sophisticated and motivated to disrupt the U.S. power grid
2. Sources and methods are from open-sources (unclassified)
3. Initial investigation will focus on the Western Electricity Coordinating Council (WECC) region

22.3 Deliverables

Milestones:

- December 2008 – List all known electric power vulnerabilities with potential attack vectors targeting EP assets
- March 2009 – Impact models tailored for IEEE Reliability System Test
- April 2009 – Rank Scenarios by Impact. Generic Configuration of electric power installations corresponding to high impact scenarios.
- September 2009- Detailed cyber-risk analysis results (threat, effects, impacts, consequence)

Primary Deliverables:

- Detailed Cyber-Risk Analysis Report

23. Consequence Modeling Tool

Lead: B. Richardson, Lozanne Chavez, and Lane Yarrington (SNL)
Partner: Massachusetts Institute of Technology

23.1 Purpose

To assist in the identification of threats and threat vectors against control systems by creating methods to model the physical-impact consequences that would result from a cyber attack on a critical infrastructure-protection system.

23.2 Background

The consequence analysis method and framework developed by Sandia National Laboratories and Massachusetts Institute of Technology has provided the basis for the National SCADA Test Bed Consequences Modeling Tool (CMT). This method for modeling electric power grid consequences on a local level was developed as part of a Sandia Laboratory Directed Research and Development (LDRD) project[1]. The method begins with a utility-ranked list of consequence categories (environment, safety, economics, etc.) and produces a *value tree* that represents the consequences, to a utility, which are associated with losing physical system elements. Also, the method calculates a performance index to describe the overall consequence that a threat scenario creates. Utilizing the infrastructure impact rankings generated from the consequence models helps to identify which threats are of greatest consequence to a utility.

In the area of critical infrastructure protection, consequences can be defined at local, regional, and national levels. Each level can contain consequences that affect other critical infrastructures.

Physical system impacts do not affect all end-users in the same way. For example, losing power to several residences for several hours may have little impact on dollar cost, but losing the same amount of power over the same several hours at an industrial plant could lead to millions of dollars in lost production; this, in turn, could lead to adverse consequences in other critical infrastructures. Understanding only the impacts associated with a particular infrastructure does not accurately depict the *true* loss to the asset owner. The CMT was designed to give the utility owners a picture of the *total-costs* associated with an outage. Before the CMT can be used, stakeholders must define a value tree that reflects importance rankings for the individual components within their system.

23.3 Scope and Technical Approach

Based on the consequence-ranking framework[2], the software provides asset owners the cost—that is, loss in several dimensions—associated with an electronic power disruption; the CMT also provides an estimation of the consequences of a system failure to the serving utility at a local level. The information provided in this analysis enables 1) utility owners/operators to get the most out of their mitigation budgets and 2) cyber security providers to prioritize their development efforts.
Final development of the software will include development of a guided setup to assist end-users in creating the value tree and system map, and inputting known data about specific physical system

[1] LaViolette, Randal A., et al. "Towards Risk-Based Management of Critical Infrastructures: Enabling Insights and Analysis Methodologies from a Focused Study of the Bulk Power Grid," Sandia National Laboratories, February 2008, SAND2008-0910.
[2] Koonce, A. M. et al, "Bulk Power Grid Risk Analysis: Ranking Infrastructure Elements According To Their Risk Significance," Massachusetts Institute of Technology, Engineering Systems Division, September 2006. http://esd.mit.edu/WPS/esd-wp-2006-19.pdf

components, such as repair costs, repair times, number and types of customers served, etc. Once configured, this data can then be used to calculate costs of disruptions.

Use case testing of the software will include working with an electric utility to go through all the steps described above to configure the software, then executing some known disruption scenarios within the tool to see if the calculated consequence is what the utility would expect to see. For example, a user would specify two or three system generators that have gone out of service and the accompanying loads that were shed to see what the associated costs of the generators going out of service are.

Availability of the software will include obtaining copyright assertion rights for the software from DOE and either 1) making the software executable available to interested utilities and researchers, or 2) open sourcing the software code and providing it in a publicly-accessible forum for download, use, and enhancement.

23.4 Deliverables

Milestones

- April-September 2009 – Provide Consequence Analysis support to Task #22
- July 2009 – Self-guided setup and configuration module for the consequence tool.
- August 2009 – Provide the consequence software (executable and/or source code) freely to the public

Primary Deliverables

- Consequence Software (executable and/or source code)

SYSTEM VULNERABILITY ASSESSMENTS

24. Common Vulnerability Report – FY 2009 Update

Lead: Chaffin, INL

24.1 Purpose

To provide a better understanding for government and industry as to what vulnerability issues exist in industrial control systems associated with the energy sector.

24.2 Background

Laboratory and asset-owner onsite assessments have been performed by the program since its inception. Since 2006, a common vulnerability report has been written to provide a better understanding for government and industry as to what vulnerability issues exist in industrial control systems associated with the energy sector. In FY-2008 a report was developed including data from previous reports as well as adding data from the current year assessments.

The FY-2008 report was reformatted from the ground up to integrate the vulnerability information into a technical metrics methodology developed for industrial control systems. The FY-2009 report will incorporate lessons-learned from previous reports and direction recommendations produced by programmatic reviews to continue to improve this informational tool and provide data that can be more easily used to support government management needs as well as industry users.

24.3 Scope and Technical Approach

The INL will work with government and industry reviewers to improve the applicability of the report to meet their needs. Further development of a metrics-based analysis approach will be developed and applied to the data as well as the reporting of the information to provide more applicable and user-friendly information presentation.

- Document feedback to improve reporting based on NSTB Peer Reviewer and Program Review comments.
- Reformat the common vulnerability database to incorporate recommendations resulting from program reviews.
- Extract data from FY-09 assessment tasks to include in the database.
- Extract the new data from the database to support the FY-09 common vulnerabilities report and reformat the report.

24.4 Deliverables

Milestones

- Detailed technical “Common Vulnerabilities Report” – Oct 2009.
- Presentation Material: Summary level material suitable for managerial presentations.

Primary Deliverables

- Common Vulnerabilities Report 2009

25. Assess Control Systems in Test Bed Facilities

Lead: Lee, Idaho National Laboratory

25.1 Purpose

Test Bed system assessments provide a failsafe environment to perform a thorough cyber assessment of control systems and associated technologies using various networking configurations and real-world data communications to a wide selection of end devices located in a substation environment.

25.2 Background

The control systems are selected for assessment based on their prevalence in the energy infrastructure and on the willingness of industry partners to support the assessments by providing equipment and technical assistance when needed.

25.3 Scope and Technical Approach

The typical process followed in test bed assessments is to negotiate a loan of the selected control system from the vendor, set up the system in the Test Bed with support from the vendor, establish representative data traffic, and then attack the system to determine what cyber vulnerabilities might exist. Teams consisting of INL cyber researchers carry out the attacks. The results are provided to the vendor who then makes modifications to the system (either software patches or a new release to their product) and provides the modified system back to INL to reassess.

The reports to the vendors are highly proprietary since, as one vendor stated, they provide a roadmap on how to compromise their control system. However, the vendors have shared a significant amount of detail related to system vulnerabilities with their customers and in some cases have provided the customers with copies of the INL assessment reports. In this case, individual non-disclosure agreements (NDAs) are established between the vendor and each customer to help ensure information protection.

The following sequence is typically followed:

- A major vendor in energy sector control systems provides the control system, provides limited training, and provides technical support in setting up the system in the test bed. At the time the first collaboration with a given vendor is initiated, a cooperative research and development agreement (CRADA) is negotiated to establish scope, roles and responsibilities to ensure protection of sensitive information.
- An assessment plan is developed to identify specific functions of the system to be examined in the assessment.
- The system is operated within the test bed environment and a team of cyber researchers attempts to disrupt its operation through cyber attacks
- Vulnerabilities that are found during the assessment are documented in a proprietary report to the vendor. The report includes recommendations for mitigation approaches the vendor might use to reduce vulnerabilities.

In most cases the vendor implements fixes that are then assessed, along with additional items of interest identified during the first assessment but beyond the initial scope, during a second phase assessment. The systems identified below will be assessed, and the titles indicate whether a specific assessment is the initial (Phase 1) or a follow-on assessment.

The INL control system test bed facility charges in support of program usage are also funded through this task in support of continuing operation and maintenance of the resources for laboratory assessment and analysis efforts.

SCADA systems to be assessed within this subtask include the following:

- AREVA (Phase 3, planning completed in FY-08/09). This task is being jointly funded by DOE and the AREVA users through user maintenance contracts with AREVA.
- Siemens Spectrum Power 3 (Phase 2, planning completed in FY-08/09). This is a phase 2 validation project being worked with Siemens EMA to assess their progress in mitigation of Phase 1 assessment vulnerabilities as well as performing additional assessment for new issues of the system.

25.4 Deliverables

Milestones

- April/September – AREVA Phase 3, Lee
- July/December – Siemens Spectrum Pwr 3, Lee

Primary Deliverables:

- Final Reports To Vendors and DOE
- Vulnerability Identification and Mitigation Presentations

26. Assess Control Systems at Asset Owner Facilities

Lead: Lee, Idaho National Laboratory
Partners: Argonne National Laboratory, Sandia National Laboratories

26.1 Purpose

The major objective of this task is to determine the extent to which energy sector SCADA installations are vulnerable to directed cyber attacks and to provide recommendations for mitigation of common vulnerabilities identified. This is a direct response to the Roadmap priority of identifying best practices for physical and cyber security of energy-related installations and system control centers. ANL is supporting INL with this task.

26.2 Background

On-site assessments at asset owner facilities provide an opportunity for the NSTB program to learn from industry and provide control system, network architecture, and other security practice feedback to user production environments. Previously these system architectures have been limited to large-scale transmission control center SCADA/EMS control systems. With the emergence of new automation technologies, major suppliers of AMI systems are being added to assessment in FY-09.

Vulnerabilities found in test bed assessments are measured in the asset owner environment using methodologies utilized in the lab assessment to determine the effectiveness of the vendor patches and updates as well as validate the findings in a system provided to an asset owner for a production operation. The assessment is performed on a test, development or training system that mirrors the basic production configuration as much as possible to allow assessment of security without placing production systems at risk in the process.

26.3 Scope and Technical Approach

The typical process followed in on-site assessments is to select a suitable asset owner candidate, determine the scope of work and establish a CRADA, attend an onsite pre-assessment meeting to develop rules of engagement and collect information for onsite visit preparation, perform analysis of security aspects of the asset owner system architectures, visit the site for two weeks for the assessment team hands-on effort, and develop the final deliverables.

The reports to the asset owners are highly proprietary. However, the information gained in these assessments are shared by the asset owners, at a common vulnerability level, with others in industry. Information from these assessments are included in the Common Vulnerability for Control Systems database for inclusion in the annual update to the Control System Common Vulnerability report. The following sequence is typically followed:

- An asset owner in the energy sector provides an off-line control system that closely mirrors their production environment, provides technical support through drawings and documentation of their system architectures and security device configurations. At the time the first collaboration with a given asset owner is initiated, a cooperative research and development agreement (CRADA) is negotiated to establish scope, roles and responsibilities to ensure protection of sensitive information.
- An assessment plan with scope of work and development of attack targets and a rules of engagement agreement are developed to identify specific functions of the system to be examined

in the assessment as well as identify the operational boundaries established to ensure the assessment process impact to operations is minimized.
- The system is operated within the asset owner assessment environment and a team of cyber researchers attempt to disrupt its operation through cyber attacks and assess the overall cyber security posture of the operation.
- Vulnerabilities found during the assessment are documented in a proprietary report to the asset owner. The report includes recommendations for mitigation approaches the asset owner might use to reduce vulnerabilities.

SCADA systems to be assessed within this subtask include the following:
- Control Center installation for a Siemens TG System to provide validation of TG system reported vulnerability mitigations and installation cyber security condition (Planning completed in FY-08/09). Current planning includes including both electric and natural gas installations in the assessment scope.
- An oil/natural gas system application is planned for a second on-site assessment. The project will pursue an on-site assessment with a selected partner for FY-09. ANL will be assisting with this subtask.

26.4 Deliverables

Milestones:
- TBD –Electric and Natural Gas
- TBD – Oil/NG company installation

Primary Deliverables:
- Final system assessment report for Vendor and DOE

27. Test Bed Support

Lead: B. Richardson - SNL
Participants:

27.1 Purpose

The purpose of the test bed support task for the National SCADA Test Bed (NSTB) at Sandia National Laboratories (SNL) is to provide a secure, stable, realistic, and easily accessible environment to aide in the development and testing of new control system security enhancements. The facility and services offered through the NSTB/SNL test bed will be made available for use to both private (utility owners/operators, vendors) and public partners. Ensuring the capability of the NSTB/SNL test bed is maintained, will help reduce the risk to energy disruption by providing an independent, relevant-environment for evaluating and testing control system cyber-security products prior to deployment by the private sector.

PARTNERSHIP & OUTREACH

28. Industry Outreach

Lead: Shabbir Shamsuddin, ANL

28.1 Purpose

The purpose of the Outreach task is to establish effective communication with industry regarding control systems security. Industry input will be obtained on critical security issues, experience, best practices, application of standards, and feedback on NSTB products. Information to industry includes the results of assessments and analyses, recommended practices for improving security, and conducting workshops to enhance awareness and to present concepts for risk management, vulnerability mitigation, and security enhancement. It is through the outreach activity that the knowledge gained in assessments and analyses is passed on to industry for implementation. This same activity is used to obtain information and guidance from industry to help ensure NSTB program activities will provide results that are relevant to industry concerns and are usable in solutions to security challenges.

28.2 Background

The Outreach task is focused on communication with key members of industry (asset owners and major vendors) to help guide program activities into areas of value to owners and to pass on the information from those activities back to the vendors and owners. This exchange can be accomplished in a number of venues, with four general areas included in this activity:

- Participation in control systems and security related workshops and conferences;
- Participation in the users groups affiliated with the vendors of major SCADA/EMS systems;
- Development and selective presentation of security workshops to raise awareness and identify general mitigation strategies related to typical cyber vulnerabilities; and,
- Result of assessments and analyses presentation on web sites and in applicable publications.

A major challenge to the implementation of the information gained through laboratory investigations is getting the information into the hands of the asset owners who are able to utilize it. A number of obstacles must be overcome: convincing asset owners that a risk to their systems and businesses actually exists; providing to owners, and vendors, actionable information they can use to reduce security risks; and, ensuring that areas of research are addressing owner concerns.

The ANL team will continue to maintain a presence in the control systems community by attending conferences, industry association meetings, workshops, and user group meetings (subject to invitation) to ensure the Department of Energy (DOE)/NSTB Program's progress, Energy Sector Roadmap, and results are shared with pertinent industry associations and asset owners. In addition ANL will work with the AGA, INGAA, and API standards groups to incorporate NSTB test results and security practices into the industry standards. ANL will work with organizations affiliated with the energy sector to develop and strengthen control systems cyber security standards. The Roadmap to Secure Control Systems in the Energy Sector states that, "Mandatory security standards and interoperability protocols must be established and implemented to guide continuous development of reliable, highly functional control system technology and software, without which the integrity of next-generation control system architectures will be severely compromised."

This effort also supports the implementation goals of the Roadmap to Secure Control Systems in the Energy Sector by obtaining industry feedback and commitment to participate in needed activities. The project will be focused on increasing awareness of and compliance with the cyber security standards that

best enable the operators to protect their control systems from attack. This approach will also provide a means of verifying the utilization of the NSTB test results when applied to a real world control system.

This task supports the Roadmap to Secure Control Systems in the Energy Sector in several areas. Within the Roadmap's "Measure and Assess Security Posture" strategy, outreach supports the near-term milestone "Baseline security methodologies available, self assessments published and training provided." Outreach also addresses a key challenge identified in the "Sustain Security Improvements" strategy that notes "Limited knowledge, understanding, and appreciation of control systems security risks inhibit action." Outreach is focused on improving understanding of security vulnerabilities and potential mitigations.

28.3 Scope and Technical/Approach

The Outreach task includes several activities all intended to support communication with industry and other organizations participating in the national effort to improve security in critical infrastructure control systems. The primary activities are focused on facilitating two-way communication between NSTB program participants and others to provide input into NSTB programmatic and technical direction and to provide a mechanism for sharing knowledge gained in the NSTB with those who can benefit from that knowledge.

This effort will employ a multi-lab approach, in which ANL will participate consistent with its expertise and available resources. The ANL team will confer with organization representatives on a regular basis to keep abreast of current activities, interests and needs vis-à-vis control system security activities. The ANL team will attend organization conferences and workshops to present summaries of NSTB efforts and accomplishments. The ANL team will participate with standards development bodies to develop control systems-related standards impacting the security posture of energy infrastructure systems. The project will focus on increasing awareness of and compliance with the cyber security standards that best enable the operators to protect their control systems from attack. This effort will include meeting and coordination with relevant industry partners to plan and advise control system security standards work. It may also include meetings, presentations, and coordination with other associated organizations such as PCSF, NIST, ISA, I3P, AGA, INGAA, API, NPRA, etc. The industry outreach effort will provide industry feedback and foster commitment by industry partners to participate in needed control system activities.

(1) Subtask 1 – General outreach and communication efforts
This subtask includes several activities, including : (1) provide support to the DOE NSTB Web Site to serve as a standard means for external organizations to learn about and make ready contact with NSTB; (2) provide support in the preparation of articles for publications to share information gained in the Program and to enhance visibility of NSTB activities with the intent of increasing awareness of security issues and solutions; (3) respond to industry inquiries into the NSTB and, as allowed by limited funding, develop collaborative opportunities; (4) support industry efforts to enhance awareness of vulnerabilities and mitigation approaches; (5) participate in industry association meetings and events to share information gained in NSTB assessments and analyses and to obtain input on the security related interests and needs of those associations. Organizations of interest include AGA, AOPL, API, INGAA, and NPRA.

(2) Subtask 2 – Conference and user group participation
Participate (present, demonstrate) in control systems vendor user group meetings and other control systems and security conferences to share information obtained in NSTB assessments and analyses with industry representatives who can put that information to use. Organizations of interest include ASME, ISA, IEEE, PCSF, I3P, and NIST.
(3) Subtask 3 – Formal report

Meeting and trip reports detailing the contacts and accomplishments will be submitted as deemed necessary for the industry update to the DOE program manager.

The goals of the outreach task will be achieved by communicating results from NSTB assessments and analyses for use by vendors and asset owners; by attending conferences, industry association meetings, workshops, and user group meetings; by providing control systems security training; by disseminating program fact sheets, including the *Roadmap to Secure Control Systems in the Energy Sector* and other Program materials. Through these and other Outreach methods, NSTB will increase awareness of control systems security in the energy sector and of the NSTB program and its resources.

The Outreach task includes several activities all intended to support communication and cooperation with industry and other organizations participating in the national effort to improve security in critical infrastructure control systems. The primary activities are focused on facilitating two-way communication between the NSTB program and others to provide input into NSTB programmatic and technical direction and to provide a mechanism for sharing knowledge gained in the NSTB with those who can benefit from that knowledge.

This effort will employ a multi-lab approach, in which ANL will participate in accordance with its expertise and available resources. The ANL team will confer with organization representatives on a regular basis to keep abreast of current activities, interests and needs vis-à-vis control system security activities. The ANL team will attend organization conferences and workshops to present summaries of NSTB efforts and accomplishments. The ANL team will participate with standards development bodies to develop control systems-related standards impacting the security posture of energy infrastructure systems.

28.4 Deliverables

Milestones:

- Email notification, weekly teleconference briefings, monthly, and trip reports.

Primary Deliverables:

- Primary deliverables will be in the form of email, teleconference briefings, meetings or additional materials as agreed on by ANL and NSTB PM.

29. Industry and Government Outreach

Lead: Dave Kuipers, INL

29.1 Purpose

The goal of conference participation is to share usable security information with industry and government stakeholders in the energy sector so they have the knowledge needed to implement effective control system and related policy security improvements. The meetings, events and conferences conferences also provide opportunities to learn about "real life" security challenges faced by industry and government, with the benefit of being able to use that insight to ensure the program is focused on security priorities.

29.2 Background

Results from the cyber vulnerability assessments have been communicated to industry in two general types of conferences. The most detailed presentations have been made in meetings held by the individual SCADA system vendors and asset owner users, usually called user group meetings. The audience in these meetings is somewhat restricted through their business relationship with the vendor however dealing with vendors that cover approximately 85% of the electricity market we reach a significant number of asset owners in the electricity and other energy sector control system users. Details specific to the assessment results of that vendor's SCADA system can be shared without a significant concern about releasing business sensitive information.

Broader audiences are reached in more open security related conferences and events, the level of detail is reduced and vulnerabilities and methods of mitigation that are common to more than a single vendor are discussed. SANS, PCSF and other related control system conferences are typically targeted to reach both vendor and asset owner control system security personnel. In both of these forums, the objective is to enhance audience awareness and understanding of control system vulnerabilities and of the mitigation options that are available to them.

The NSTB program is increasing focus on ONG products and installations to improve the energy sector overall cyber security posture and move toward the goals outlined in the "Roadmap to Secure Control Systems in the Energy Sector" developed by industry and government in January 2006.

Public and private security issues associated with control systems are becoming more prevalent. The INL program has access to information, systems and parties that allow a big picture view of emerging issues and possible impacts to the energy sector critical infrastructure. The INL will support ongoing ICS-CERT activities with specific intent to understand and communicate energy sector specific information to the DOE-OE program management to support market impact analysis.

29.3 Scope and Technical/Approach

Presentations at general conferences, events and meetings are typically in response to invitations from the organizers to share information gained in the NSTB program. In some cases, NSTB participation as a panelist is requested. In the user group meetings, presentations typically involve a joint presentation with a representative from the applicable vendor to support a more comprehensive description of the vulnerabilities, recommended mitigation, and the action the vendor has taken or will take to address the issues. These meetings also present an opportunity to provide SCADA system asset owners with information they can use in taking their own action to address vulnerabilities in the systems of interest.

The INL will provide energy sector industrial control system specific analysis and reporting between the DHS CSSP and the DOE-OE NSTB Program Manager. The task will include support in development of agreements between the INL, DOE-OE, DHS CSSP, NERC and others as appropriate to fulfill the needs of this task.

29.4 Deliverables

Milestones:

- TBD – 7 User Group Meetings, Various
- TBD – E-SEC NW CIP Summit/ PCSF/ EMS UG/ NERC CIPC meetings/SANS/other meetings as invited or requested, Various
- LOE — Situational Awareness LOE Support, TBD

Primary Deliverables:

- Papers and presentations shared with audiences/meetings.
- LOE- coordination and analysis of control system energy sector related work in collaboration with the DHS CSSP/ICS-CERT program and according to agreements developed between programs. Deliverables will be in the form of email, teleconference briefings, meetings or additional materials as agreed on by INL and NSTB PM

30. SCADA Security Training Workshops

Lead: Gary Finco, INL

30.1 Purpose

This project aims to provide several levels of control systems cyber security training to a variety of organizational disciplines.

30.2 Background

To date the program has provided this training to 1989 people. The training program has proven invaluable in increasing the awareness of management and operations personnel in vendor and user organizations to the issues associated with control system cyber vulnerabilities and related topics. User organizations have initiated incorporation of cyber security concepts in their system upgrade project as a result of material presented in the workshops.

The INL has developed and presented Red/Blue team control system cyber security workshops over the past two years. Funding from multiple sources has supported this work. The workshop trainer personnel are highly experienced cyber researchers and have presented several courses. The equipment utilized for the course is available and fully integrated to provide classroom and hands-on training that simulates an attacker group attempting to gain access to a business and control systems operation and a defender group attempting to detect intrusion and defend their operation.

30.3 Scope and Technical Approach

The workshop training is provided in User Group meetings, conferences and other gatherings where vendor and/or user management, technical and operations personnel are available to attend in groups sized to optimize the course. Depending on the schedule, multiple courses are often provided to diverse disciplines at a given meeting to maximize the exposure of the training to the target audience. The training material is updated periodically to provide current training information. Training presentation costs are shared with the customer. The NSTB program typically funds the trainers' labor costs and the demonstration system development support. The customer funds classroom-related expenses and the trainers' travel expenses.

The Red/Blue team training is provided at the INL. Several days of classroom training culminates in a full day red/blue team exercise monitored and scored by an INL white team, followed by a wrap up day of exercise debrief, evaluation and final training. This course has received excellent reviews and is very relevant to potential attack on control systems. This subtask would target utility control system cyber security-related personnel. The outreach aspect of this subtask is providing training and experience to utility personnel on actual cyber security incidents and the real-time aspects of a concerted attack. The attendees fund their own travel and lodging expenses. Attendance fees are charged to offset a portion of the training costs.

30.4 Deliverables

Milestones:

- TBD – 2 each SCADA Security Workshops, Finco

- April – 1 each Electricity Sector Red/Blue Team Training Workshop, Finco
- July – 1 each ONG Sector Red/Blue Team Training Workshop, Hahn

Deliverables:

- Conduct 1 Electricity Sector Red/Blue Team Cyber Security Workshop
- Develop and Conduct 1 ONG Sector Red/Blue Team Cyber Security Workshop
- Copies of all training materials and names and affiliations of all attendees.
- Red/Blue Team Game Plan.
- Course attendee student profile summary.
- Student course feedback report.

31. PNNL Outreach

Lead: Jeff Dagle, PNNL
Participants:

31.1 Background

Continuation of FY08 authorization, including but not limited to supporting the NERC Critical Infrastructure Committee, Control System Security Working Group, and other activities at the direction of the DOE Program Manager.

31.2 Deliverables

The specific milestones and deliverables that will be accomplished will be determined throughout the course of the year in consultation with the DOE Program Manager as programmatic requirements for outreach activities are fulfilled working with industry and other stakeholders.

32. Intrusion Detection Outreach to Develop Utility Requirements

Lead: Steve Fernandez, ORNL
Partners: EnerNex

32.1 Purpose

The objective of this task is to understand and document the economic justification for deploying secure systems. The project will examine their concept of operations, their potential use cases, and standards environments that affect asset owners' business cases for aggressively deploying security advances. Building this consensus requires a different set of end user deployments, demonstrations and advocacy of user concerns.

32.2 Background

In order to assure that secure control systems are widely deployed, two key barriers need to be addressed with asset owners and utilities. The first barrier is identifying those assets that require higher levels of protection. This barrier is addressed in the ORNL Trustworthy Wireless project. The second barrier is that the deployment of secure control systems must fit within the business case of the utility/stakeholder. Unless the deployment fits into the business plans of the utility, protection systems will remain undeployed.

32.3 Scope and Technical Approach

The milestones associated with establishing such an owner based capability includes:

- Self organize a group of stakeholders to develop the key elements of the utility/stakeholder business case.
- Solicit involvement and announce a series of workshops for July and October 2009.
- Establish workshops associated with the Utili-sec meetings in July and October drawing from the owner organizations participating within the standards generating bodies.
- Develop a strategic plan based on the resultant requirements for information and evidence based business cases to compile and develop the data necessary for investment trade off information.

32.4 Deliverables

- July 2009 - Workshop
- August 2009- Draft Report based on July Workshop
- October 2009- Workshop
- November 2009- Final Report

33. Roadmap Gap Analysis

Lead: Jeff Dagle, PNNL
Partners:

33.1 Purpose

The objective of this project is to ensure that the Roadmap research agenda is successfully implemented.

33.2 Background

The Roadmap identifies what must be done, but the questions of "How" and "When" have not yet been fully answered. Research and implementation dependencies, ordering of milestones, ordering of goals, and identification of research gaps will be presented in a technical report for OE.

The Roadmap document outlines a comprehensive research agenda, but the implementation of the Roadmap is up for interpretation. Research organizations may choose to tackle the easier solutions first, leaving the more difficult challenges for later. With this approach, there is no guarantee that all Roadmap milestones and goals will be successfully met.

33.3 Scope and Technical Approach

This project will utilize key personnel at PNNL from the Secure Cyber Systems and the Energy Technology Development groups. Together this multi-disciplinary team brings together the nuclear, cyber security, and electric transmission and distribution disciplines. Key staff with expertise in strategic planning will also be utilized. The primary deliverables from this project include the Roadmap Implementation Guidance Document and a presentation to OE.

Benefits of this task will include:

- A strategic implementation plan for the Roadmap
- Identification of Roadmap goals and milestones at risk for not being met
- Identification of missing milestones
- Identification of sub-milestones
- Mapping of current research and development efforts to the Roadmap
- Inclusion of a feedback loop into Roadmap implementation

33.4 Deliverables

Milestones:

- March 2009 – Draft Report
- September 2009 – Final Report

Primary Deliverables:

- Final Report

APPENDIX A:
INDUSTRY PARTNERS

APPENDIX B: ENERGY SECTOR CONTROL SYSTEMS WORKING GROUP

The Working Group goals for 2009 are to update the Energy Roadmap, continue increasing the awareness and engagement of owners and operators in Roadmap-related activities, and measure progress with the control systems security projects in the energy sector. The 2009 work plan includes:

- **Roadmap Update** – working with all stakeholder groups in the energy sector, the Energy Roadmap will be updated in four phases:
  - Spring/Summer '09 – Over-the-Horizon Analysis: Convene subject matter experts to discuss the control systems security challenges the energy sector may face over the next 10 years and recommend potential end states and milestones to overcome them.
  - Spring/Summer '09 – Roadmap Gap Analysis: Determine the gaps in goals and priorities over the past three years, as well as the new end states; provide a technical analysis, using Pacific Northwest National Laboratory, on the interrelationships of ongoing research.
  - Summer '09 – Roadmap Update Workshop: Convene a broad section of energy sector stakeholders to clarify end states and milestones drafted as a result of the over-the-horizon and gap analysis activities.
  - Fall '09 – Revised Control Systems Roadmap: the ESCSWG and Roadmap Update participants will release a revised *Roadmap to Secure Control Systems in the Energy Sector* that more specifically addresses the security needs of today's control systems environment, such as Smart Grid technologies, increasingly sophisticated adversaries, and emerging standards requirements.
- **Roadmap Launch** – develop and implement Energy Roadmap '09 outreach strategy with a comprehensive communication plan and roll out strategy.
- **Roadmap Accomplishments** – evaluate improvements to control systems security in the energy sector, align results according to the new Roadmap framework, and establish a baseline for future improvements in control systems security.
- **Matchmaker Initiative** – develop mechanisms to link control systems security projects in the public and private sector with appropriate end-user project partners to increase project validation, ensure projects create an applicable end product, and introduce end users to forthcoming technologies:
  - Convene one or more Advisory Boards of public- and private-sector control systems security experts to advise research projects in specific control systems security areas, such as substation automation. Advisory Boards will ensure that projects are relevant, advance Roadmap goals, have adequate plans for collaboration and technology transfer, and are technically robust.
  - Create an online Matchmaking Tool that allows both project leads and end users to sign up and be matched based on the knowledge and level of effort needed to advance control systems security research; launch in Fall '09.
- Publish *ieRoadmap News* in Summer, Fall, and Winter '09.
- Conduct 2nd annual ieRoadmap Workshop in Winter '09.
- Further engage CEOs, asset owners, researchers, and government staff through continued briefings, advisory group participation, and personal outreach.
- Engage in standards development activities, such as NERC CIP and Smart Grid interoperability standards.
- Broaden focus and target outreach efforts to enhance security in the oil and natural gas sectors.

- Conduct monthly planning calls and hold more as needed.
- Leverage time at the Roadmap Stakeholder Review to conduct annual Working Group meeting.

NSTB

National SCADA Test Bed

Enhancing control systems security in the energy sector