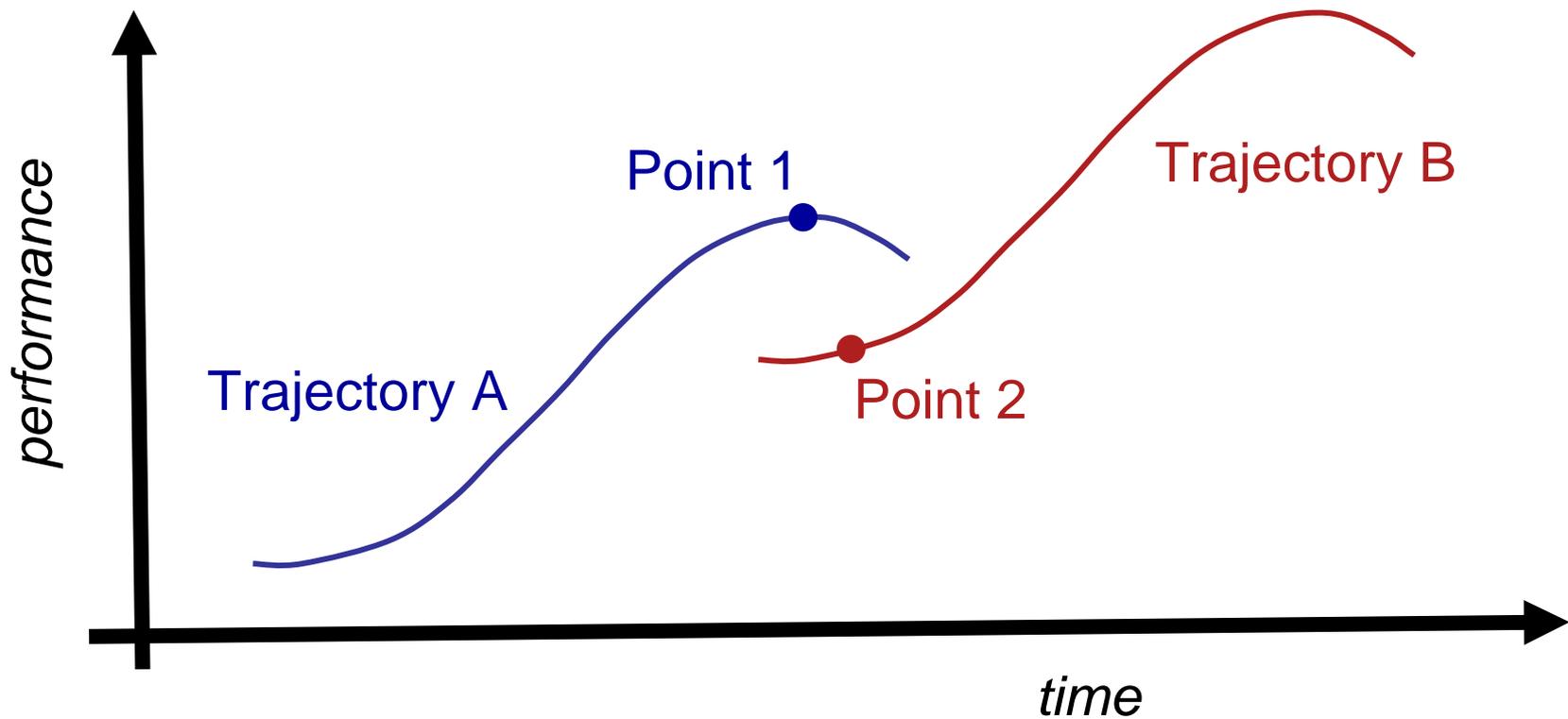


Enhancing Control Systems Security in the Energy Sector

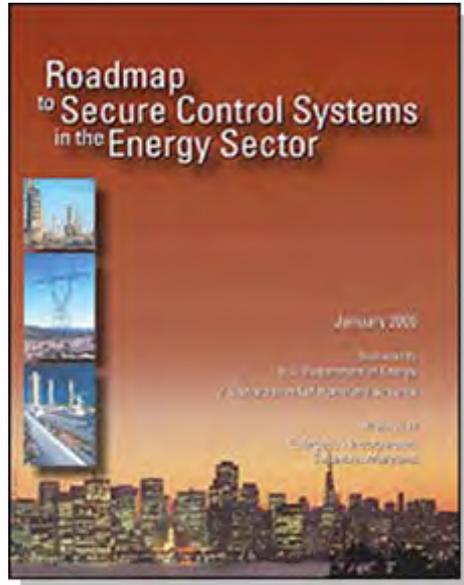
Hank Kenchington
Control Systems Security
Office of Electricity Delivery and Energy Reliability
U.S. Department of Energy

Getting on the Next Track



A Framework for Public-Private Partnership

Roadmap to Secure Control Systems in the Energy Sector



- Industry-driven synthesis of public and private sector input
- Identifies energy sector's most critical control system security challenges, R&D needs, and implementation milestones
- Provides strategic framework to align public-private investments

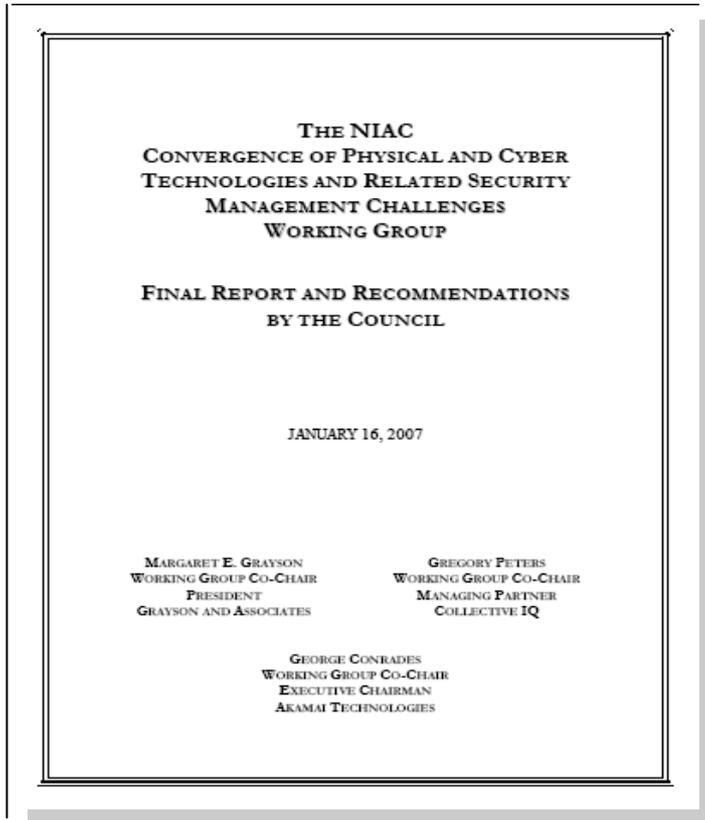
Vision

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

Key Strategies and selected Milestones

Measure and Assess Security Posture	Develop and Integrate Protective Measures	Detect Intrusion and Implement Response Strategies	Sustain Security Improvements
Milestones	Milestones	Milestones	Milestones
<p>50% of asset owners and operators performing self-assessments of their control systems using consistent criteria (2008)</p> <p>Fully automated security state and common response of control system networks (2015)</p>	<p>Secure connectivity between business systems and control systems within corporate network (2009)</p> <p>Secure control system architectures produced with built-in, end-to-end security (2015)</p>	<p>Cyber incident response is part of emergency operating plans at 30% of control systems (2008)</p> <p>Self-configuring control system network architectures are in production (2015)</p>	<p>Compelling, evidence-based business case to increase private investment in control system security (2007)</p> <p>Cyber security awareness, outreach, and education programs integrated into energy sector operations (2015)</p>

National Infrastructure Advisory Council Cites Roadmap Model and Vision



The NIAC recommends that:

1. The President direct all critical infrastructure sectors to set the goal:
By 2015, control systems for critical applications will be designed, installed, operated and maintained to survive an intentional cyber assault with no loss of critical function.
2. The Department of Homeland Security (DHS) and Sector-Specific Agencies (SSAs) collaborate with their respective owner/operator sector partners to develop sector-specific roadmaps using the ***Energy Sector Roadmap*** as a model.

National SCADA Test Bed

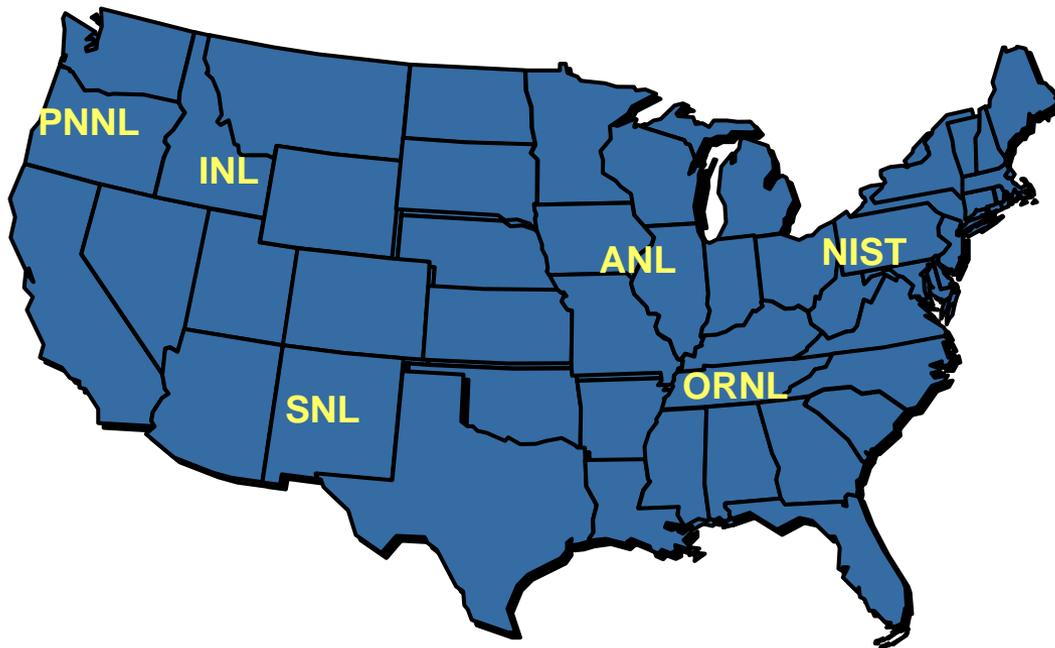
...established 2003

PURPOSE

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

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

Bruce Schneier,
Beyond Fear



NSTB FY06 Activities ...aligned to support Roadmap goals

Goal 1. Measure and Assess Security Posture

- Conduct cyber security assessments of 6 control systems widely used across energy sector in test bed environment
- Conduct onsite assessments of 4 systems
- Conduct cyber security assessment of ICCP implementations

Goal 2. Develop and Integrate Protective Measures

- Protocol Authentication
- Evaluate technology trends impacting control systems security (e.g., IPv6)
- Develop Virtual Control Systems Environment Tool

Goal 3. Detect Intrusion and Implement Response Strategies

- OPSAID - Open PCS Architecture/Interoperable Design

Goal 4. Sustain Security

- Conduct 5 workshops on control systems vulnerabilities and mitigation techniques
- Continue to work with PCSF and others (e.g., NERC, AGA, API, INGAA)
- Accelerate Standards development
- Coordinate with DHS and other agencies
- Measure and communicate progress

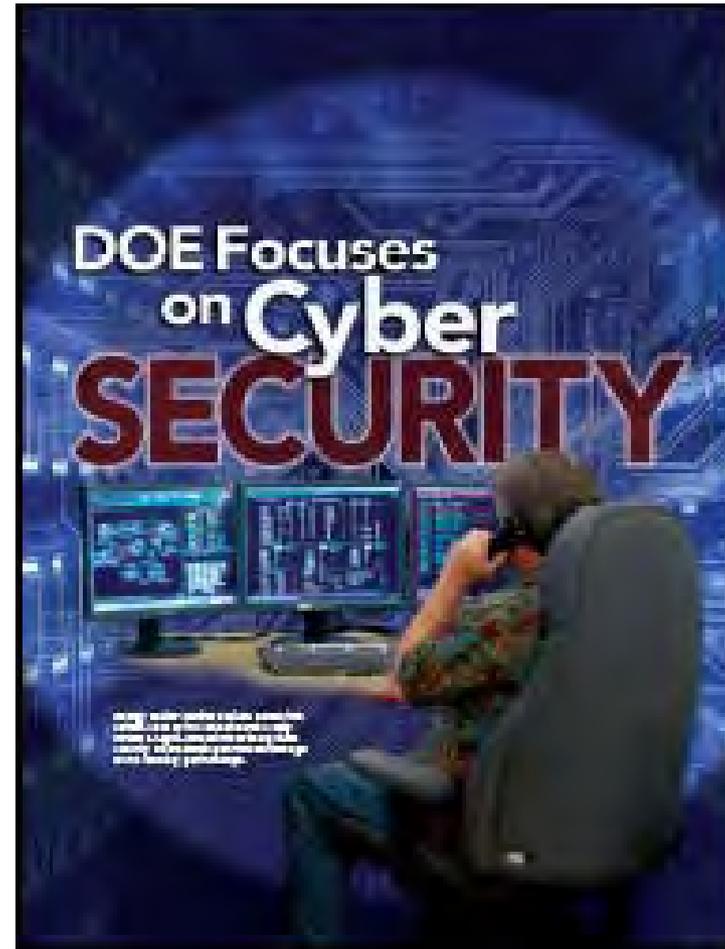
National SCADA Test Bed: Recent Accomplishments

1. Control System Assessments - ABB, AREVA, GE, Siemens, OSI, Telvent
 - 14 next-generation systems now operational
 - 49 patches downloaded
2. *Lessons Learned Report* - supports Common Procurement Language project
3. Trained for over 800 end-users
4. Working with NERC, developed mitigation strategies for “Top 10” vulnerabilities
5. Performance testing and cryptographic analysis of AGA 12
6. Protocol Authentication
7. Launched industry partnership to develop OPSAID
8. Outreach via NERC, FERC, EPRI, KEMA, EEI, INGAA, API, AGA, NRECA, I3P, PCS Forum, NSF, SANS Summits, and international
9. Standards: ISA SP-99; IEC TC 57, WG 15; Standard Procurement Language
10. Peer Review with industry panel – several “course corrections”

See reports at: www.oe.energy.gov/randd/css.htm

Sustain Security Improvements

- ◆ “Partnering for Cyber Security at DOE’s National SCADA Test Bed” - *T&D World, March 2007*
- ◆ “SCADA Gets Tough” - *Pipeline & Gas Journal, February 2007*



NSTB Plans for FY07

- ◆ Continue system assessments and outreach
- ◆ Work with vendors and standards groups to commercialize Protocol Authentication
- ◆ Advance OPSAID
- ◆ Develop “end-to-end” risk assessment tool
- ◆ Enhance threat awareness
- ◆ Issue industry solicitation for advanced technology development – notice on www.netl.gov in March
- ◆ Working with Critical Infrastructure Partnership Advisory Council to implement Roadmap

A New, Web-Based Tool



- ◆ On-line Roadmap Mapping Tool hosted by PCSF
- ◆ So far: >70 projects mapped by 10 organizations
- ◆ Projects mapped to Roadmap challenges
- ◆ Facilitates leveraging activities; helps identify gaps
- ◆ Measure progress
- ◆ Official launch: TODAY!

www.pcsf.org/roadmap

ADDRESSING ROADMAP CHALLENGES

- Overview
- Strategies
 - Measure and Assess Security Posture
 - Develop and Integrate Protective Measures
 - Detect Intrusion and Implement Response Strategies
 - Sustain Security Improvements

[SEARCH PROJECTS](#)

[ADD A NEW PROJECT](#)

[LEARN ABOUT THE ROADMAP](#)



Recent Additions: AGA-12 Performance Testing & Cryptographic An...

Total Projects: 84

Leaders from the energy sector and the government have recognized the need to plan, coordinate, and focus ongoing efforts to improve control system security. These leaders concur that an actionable path forward is required to address critical needs and gaps and to prepare the sector for a secure future. Their commitment helped to launch a public-private collaboration to develop a [Roadmap to Secure Control Systems in the Energy Sector](#). The Roadmap focuses on the goals and priorities for improving the security of control systems in the electric, oil, and natural gas sectors over the next decade.



EXPLORE THE ROADMAP PROJECT DATABASE

The [Interactive Roadmap](#) showcases a set of projects mapped to specific strategies and challenges.

Contributors include:

[NSTB](#)
[PNNL NCASSR](#)
[TCIP](#)
[TNS, Inc. & Digital Bond, Inc.](#)
[TSWG](#)

The challenges identified in the Roadmap fall within four strategy areas. View challenges by strategy:

- [Measure and Assess Security Posture](#)
- [Develop and Integrate Protective Measures](#)
- [Detect Intrusion and Implement Response Strategies](#)
- [Sustain Security Improvements](#)

ADDRESSING ROADMAP CHALLENGES

- ▣ Overview
- ▣ Strategies
- ▣ Measure and Assess Security Posture
- ▣ Develop and Integrate Protective Measures
- ▣ Detect Intrusion and Implement Response Strategies
- ▣ Sustain Security Improvements

SEARCH PROJECTS

ADD A NEW PROJECT

LEARN ABOUT THE ROADMAP

This Website
Designed & Maintained by



[Home](#) > [Overview](#) > [Search](#)

Search the Roadmap Projects Database

Search Options

Search By Keyword:

Filter By Strategy:

1. Measure and Assess Security Posture

Filter By Organization:

DHS/HSARPA SBIR

Filter By Date:

January

2007

Search

ADDRESSING ROADMAP CHALLENGES

- Overview
- Strategies
 - Measure and Assess Security Posture
 - Develop and Integrate Protective Measures
 - Detect Intrusion and Implement Response Strategies
 - Sustain Security Improvements

SEARCH PROJECTS

ADD A NEW PROJECT

LEARN ABOUT THE ROADMAP

[Home](#) > [Overview](#) > [Strategies](#)

Strategies

Click on a strategy to explore its challenges and associated projects.



Companies should thoroughly understand their current security posture to determine system vulnerabilities and the actions required to address them.

Within 10 years, the sector will help ensure that energy asset owners have the ability and commitment to perform fully automated security state monitoring of their control system networks with real-time remediation capability.

As security risks are identified, protective measures should be developed and applied to reduce system risks. Security solutions will be developed for legacy systems, but options will be constrained by the limitations of existing equipment and configurations.

Within 10 years, next-generation control system components and architectures that offer built-in, end-to-end security will replace many older legacy systems.

Because few systems can be made totally impervious to cyber attacks all the time, companies should possess sophisticated intrusion detection systems and a sound response strategy.

Within 10 years, the energy sector will operate control system networks that automatically provide contingency and remedial actions in response to attempted intrusions into the control systems.

Maintaining aggressive and proactive control system security over the long term will require a strong and enduring commitment of resources, clear incentives, and close collaboration among stakeholders.

Over the next 10 years, energy asset owners and operators are committed to working collaboratively with government and sector stakeholders to accelerate security advances.

ADDRESSING ROADMAP CHALLENGES

- Overview
- Strategies
 - Measure and Assess Security Posture
 - Develop and Integrate Protective Measures**
 - Detect Intrusion and Implement Response Strategies
 - Sustain Security Improvements

SEARCH PROJECTS

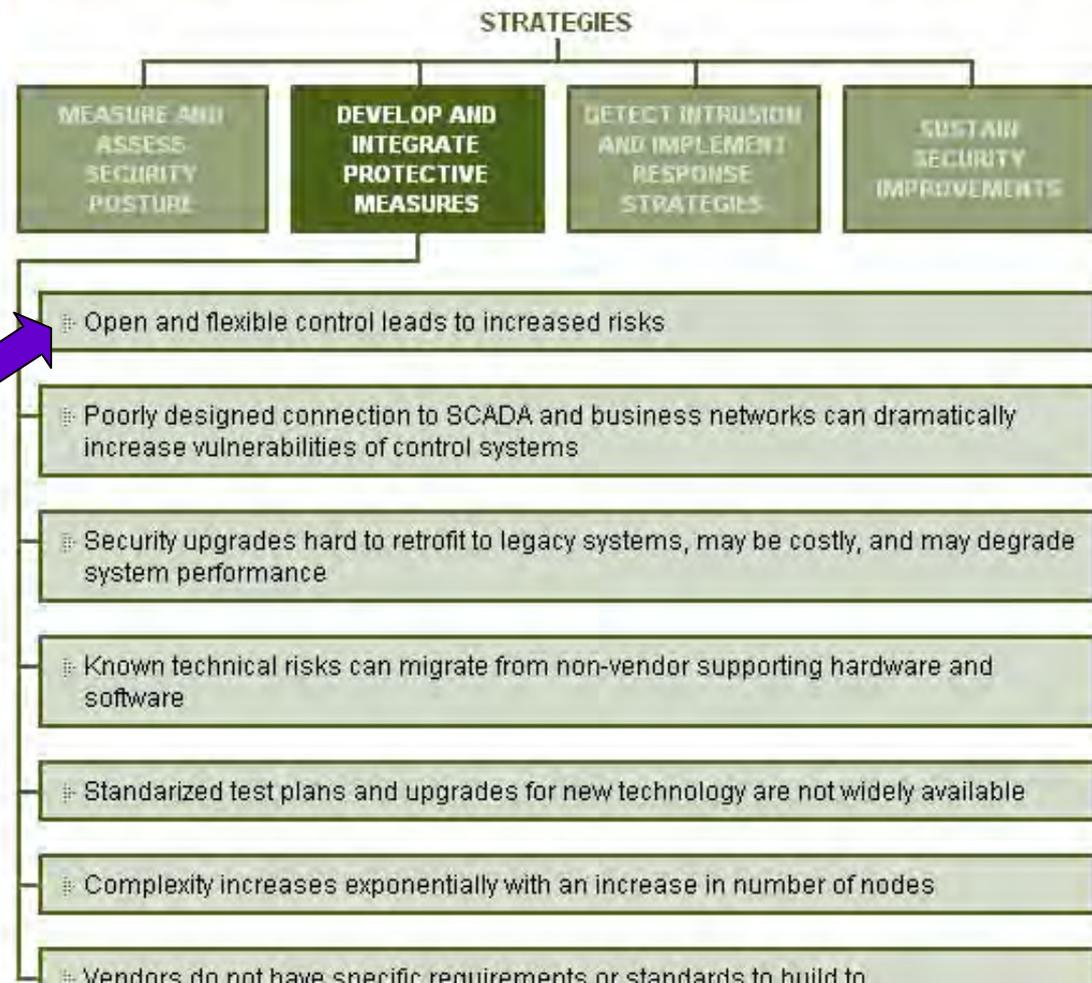
ADD A NEW PROJECT

LEARN ABOUT THE ROADMAP

Home > Overview > Strategies > Challenges

Develop and Integrate Protective Measures: Challenges

Today's control systems are increasingly interconnected and operate on open software platforms that increase vulnerabilities and risks. Poorly designed connections between control systems and enterprise networks also increase risks. Security improvements for legacy systems are limited by the existing equipment and architectures that may not be able to accept security upgrades without degrading performance. New architectures must be designed to address potential threats that have not yet surfaced and to accommodate the exceptionally large number of nodes and access points that increase security concerns.



SEARCH PROJECTS

ADD A NEW PROJECT

LEARN ABOUT THE ROADMAP

STRATEGIES

MEASURE AND ASSESS SECURITY POSTURE

DEVELOP AND INTEGRATE PROTECTIVE MEASURES

DETECT INTRUSION AND IMPLEMENT RESPONSE STRATEGIES

SUSTAIN SECURITY IMPROVEMENTS

Open and flexible control leads to increased risks

PROJECTS:

[Add a project to this Challenge](#)

DHS/HSARPA SBIR

- [Secure SCADA Toolkit](#) [Edit](#)
- [SureSense Security Information Management](#) [Edit](#)
- [Secure Cryptographic Management System](#) [Edit](#)
- [Asier12](#) [Edit](#)

I3P

- [Process Control Systems Security Project: Unifying Stakeholders and Security Programs to Address SCADA Vulnerability and Infrastructure Interdependency](#) [Edit](#)

MS-ISAC

- [SCADA Procurement Project](#) [Edit](#)

NIST

- [PCSRF](#) [Edit](#)
- [Control Systems Security Protection Framework Requirements Review](#) [Edit](#)
- [SCADA Protection Profile](#) [Edit](#)
- [SP800-53 Baseline Security Controls for SCADA and DCS](#) [Edit](#)
- [ISA-SP99](#) [Edit](#)

NSTB

- [SCADA Protocol Authenticator](#) [Edit](#)
- [SCADA/EMS Assessments](#) [Edit](#)

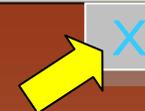
TCIP

- [Secure and Reliable Computing Base](#) [Edit](#)
- [Trustworthy Data Collection and Control Infrastructure](#) [Edit](#)

TSWG

- [SCADA Security Pocket Guide](#) [Edit](#)
- [SCADA Security Pocket Guide Training Support Package \(TSP\)](#) [Edit](#)





Project Details

[Edit](#)

Project Name: SCADA Protocol Authenticator

Lead Organization: NSTB

Principal Investigator: Pacific Northwest National Laboratory

Contact Name: Mark Hadley

Contact Email: Mark.Hadley@pnl.gov

Contact Phone:

Last Edited: 1/11/2007 9:57:53 AM

Project Start Date:

Funding To Date: Unknown

Project Participants:

Project Description: The SCADA Protocol Authenticator task will continue development of a novel SCADA communications authenticator technology developed by the Pacific Northwest National Laboratory (PNNL) and funded by the U.S. Navy. The Secure SCADA Communications Protocol (SSCP) wraps original, serial SCADA communication traffic with a unique identifier and an authenticator. The SSCP then uses a unique identifier in the wrapper to ensure the communication is valid, and can detect and prevent various attack scenarios including "man-in-the-middle", injected traffic, or message replay. The SSCP is envisioned to be available as an embedded software solution running on the SCADA master or input/output server, as a bump-in-the-wire industrial computer, or as a small micro-controller dongle. The authenticator technology directly supports the Roadmap to Secure Control Systems in the Energy Sector milestone targeting widespread implementation of methods for secure communication between remote-access devices and control centers. In terms of the DOD technology readiness level definitions, the SSCP has currently achieved level 7 (i.e., system prototype demonstration in an operational environment). The goal for this project will be to move the SSCP toward technology readiness (level 8), where the technology has been proven to work in its final form and under expected conditions. Comprehensive testing will be performed to confirm that the technology will fulfill its technical objectives when deployed under a variety of expected conditions in the field. The goal is to facilitate earlier industry adoption of a novel security technology that is well suited for securing control systems used by energy infrastructures.

**Preliminary Results/
Deliverables:**

Website:
(for more info)

Improvements

SEARCH PROJECTS

ADD A NEW PROJECT

LEARN ABOUT THE ROADMAP



STRATEGIES

MEASURE AND ASSESS SECURITY POSTURE

DEVELOP AND INTEGRATE PROTECTIVE MEASURES

DETECT INTRUSION AND IMPLEMENT RESPONSE STRATEGIES

SUSTAIN SECURITY IMPROVEMENTS

Open and flexible control leads to increased risks

PROJECTS:

[Add a project to this Challenge](#)

DHS/HSARPA SBIR

- [Secure SCADA Toolkit](#) [Edit](#)
- [SureSense Security Information Management](#) [Edit](#)
- [Secure Cryptographic Management System](#) [Edit](#)
- [Asier12](#) [Edit](#)

I3P

- [Process Control Systems Security Project: Unifying Stakeholders and Security Programs to Address SCADA Vulnerability and Infrastructure Interdependency](#) [Edit](#)

MS-ISAC

- [SCADA Procurement Project](#) [Edit](#)

NIST

- [PCSRF](#) [Edit](#)
- [Control Systems Security Protection Framework Requirements Review](#) [Edit](#)
- [SCADA Protection Profile](#) [Edit](#)
- [SP800-53 Baseline Security Controls for SCADA and DCS](#) [Edit](#)
- [ISA-SP99](#) [Edit](#)

NSTB

- [SCADA Protocol Authenticator](#) [Edit](#)
- [SCADA/EMS Assessments](#) [Edit](#)

TCIP

- [Secure and Reliable Computing Base](#) [Edit](#)
- [Trustworthy Data Collection and Control Infrastructure](#) [Edit](#)

TSWG

- [SCADA Security Pocket Guide](#) [Edit](#)
- [SCADA Security Pocket Guide Training Support Package \(TSP\)](#) [Edit](#)

ADDRESSING ROADMAP CHALLENGES

Overview

Strategies

Measure and Assess
Security Posture

Develop and Integrate
Protective Measures

Detect Intrusion and
Implement Response
Strategies

Sustain Security
Improvements

SEARCH PROJECTS

ADD A NEW PROJECT

LEARN ABOUT THE ROADMAP

Home > Overview > Strategies >> Add New Project

Add A New Project

Complete the form below to add a new project. *Items marked with an asterisk (*) are required.*

* Project Name:

* Lead Organization:

* Map Project To:

(In the grey form below, select challenges to add the project to.)

1. Select a *Strategy*,

Strategy:

Measure and Assess Security Posture

2. Select a *Challenge*,

Challenge:

- Risk factors are not widely understood or accepted by technologists and managers
- Insufficient security metrics limit threat analysis capability
- Existing standards lack clear measurement specifications
- Consistent metrics are not available to measure and assess security status
- Insufficient tools and techniques exist to measure risk
- No standards exist to assess cyber vulnerabilities
- Threats are hard to demonstrate and quantify
- Intellectual property rights of asset owners are hard to protect

Select Item

Hide Selection Form

(Continue to select and add as many challenges as needed.)

Principal Investigator:

You're Invited!!

- Get on the **next track** with the *ieRoadmap*.
- Make sure your contributions and organization are recognized.
- Visit the website, get registered, and add project descriptions.
- All entries reviewed prior to posting.
- Stop by the NSTB booth for more info.

www.pcsf.org/roadmap



Contributors include:

- NSTB
- PNNL NCASSR
- TCIP
- TNS, Inc. & Digital Bond, Inc.
- TSWG

in four strategy areas. View challenges

Strategies