NSTB

Fact Sheet

National SCADA Test Bed

Enhancing control systems security in the energy sector

Benefits

Working in partnership with the energy sector, the National SCADA Test Bed seeks to

- Identify and mitigate existing vulnerabilities.
- Facilitate development of security standards.
- Serve as an independent facility to test SCADA equipment and control systems.
- Identify and promote best cyber security practices.
- Increase awareness of control systems security within the energy sector.
- Develop advanced control system architectures and technologies that are more secure and robust.

Purpose

The NSTB supports industry and government efforts to enhance the cyber security of control systems used throughout the electricity, oil, and gas industries.

PROTECTING ENERGY INFRASTRUCTURE BY IMPROVING THE SECURITY OF CONTROL SYSTEMS

Improving the security of energy control systems has become a national priority. Since the mid-1990's, security experts have become increasingly concerned about the threat of malicious cyber attacks on the vital supervisory control and data acquisition (SCADA) and distributed control systems (DCS) used to monitor and manage our energy infrastructure. Many of the systems still in use today were designed to operate in closed, proprietary networks. Increasing use of common software and operating systems and connection to public telecommunication networks and the Internet have made systems more reliable and efficient—but also more vulnerable to cyber assaults. Both energy system owners and vendors have found it difficult to assess vulnerabilities in their systems in an operational environment and test or verify security upgrades prior to installation.

The National SCADA Test Bed Program is a national resource to help secure our nation's energy control systems. It combines state-of-the-art operational system testing facilities with research, development, and training to discover and address critical security vulnerabilities and threats the energy sector faces.

A National Resource for Industry

The DOE Office of Electricity Delivery and Energy Reliability established the NSTB to help equipment vendors and asset owners assess vulnerabilities in control systems hardware and software and verify security fixes using a full-scale infrastructure suite of facilities. The NSTB program offers the integrated expertise and resources of multiple national laboratories, including Idaho National Laboratory, Sandia National Laboratories, Argonne National Laboratory, Pacific Northwest National Laboratory, and Oak Ridge National Laboratory.

NSTB team members:

- Collaborate with industry to identify, assess, and mitigate current SCADA system vulnerabilities.
- Work with industry to develop risk mitigation strategies and raise industry awareness through training and outreach.
- Develop next-generation architectures and accelerate deployment of hardened systems with built-in security
- Perform integrated risk analysis to determine cyber security posture, prioritize investments, and support a cyber security business case.
- Support industry development of national standards, guidelines, and best practices for more secure control systems.

The NSTB provides modeling and simulation resources; comprehensive technical expertise in industrial SCADA systems; facilities that recreate real-world control systems, infrastructures, and networks; red team and assessment expertise; cryptography and information security capabilities; and other SCADA-related test bed and security activities.

NSTB Multi-Laboratory Team

Argonne National Laboratory

Idaho National Laboratory

Oak Ridge National Laboratory

Pacific Northwest National Laboratory

Sandia National Laboratories

Partners

Asset owners and operators

System developers, vendors, and integrators

User groups

Industry associations

Standards organizations

Other Federal agencies

For more information about NSTB, contact:

Dave Kuipers, Project Manager
Idaho National Laboratory
P.O. Box 1625
Idaho Falls, ID 83415-2604
208-526-4038
david.kuipers@inl.gov

Robert Pollock, Program Lead
Sandia National Laboratories
P.O. Box 5800/MS 0671
Albuquerque, NM 87185-0671
505-844-4442
rdpollo@sandia.gov

For Program Information, Contact:

Hank Kenchington
Deputy Assistant Secretary for R & D
U.S. Department Energy
Office of Electricity Delivery and Energy Reliability (OE-10)
1000 Independence Ave., SW
Washington D.C. 20585
202-586-1878
henry.kenchington@hq.doe.gov

Visit our website:

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

Facility Resources

The NSTB team offers 17 testing and research facilities, encompassing field-scale control systems, 61 miles of 138 kV transmission lines, seven substations, and state-of-the-art visualization and modeling tools.

IDAHO Critical Infrastructure Test Range
- SCADA/Control System Test Bed
- Cyber Security Test Bed
- Wireless Test Bed
- Powergrid Test Bed
- Modeling and Simulation Test Bed
- Control Systems Analysis Center

SANDIA Center for SCADA Security
- Distributed Energy Technology Laboratory
- Network Laboratory
- Cryptographic Research Facility
- Red Team Facility
- Advanced Information Systems Laboratory

PACIFIC NORTHWEST Electricity Infrastructure Operations Center
- SCADA Laboratory
- National Visualization and Analytics Center
- Critical Infrastructure Protection Analysis Laboratory

OAK RIDGE
- Large-Scale Cyber Security and Network Test Bed
- Extreme Measurement Communications Center

ARGONNE
- Infrastructure Assurance Center

Industry Partnerships

Partnership with industry enables NSTB work. Vendors provide control systems and security technologies for assessment in the test beds, while owners provide access to their control systems for on-site assessments and validation of test bed results. Recognizing the value of NSTB testing, user groups of several vendors have also come together to co-fund additional assessments. These industry partners are actively implementing improvements and providing guidance to help ensure program activities address real control system security issues. Several vendors, asset owners, and industry organizations are also partnering on R&D projects to ensure they deliver applicable results.

Achievements

Since 2003, the NSTB has assessed the majority of the current market offering of SCADA systems in the electric and the oil and gas sectors. Twenty test bed and on-site field assessments have led vendors to develop 11 hardened control system designs — and 21 of these systems are now deployed in the marketplace.

The NSTB team also has:

- Released an annual Common Vulnerabilities Report to extend the impact of assessments by releasing generalized vulnerability information and mitigation strategies for asset owners
- Trained more than 1,900 asset owners in introductory, intermediate, and advanced SCADA security
- Developed a week-long, hands-on Advanced Red Team/Blue Team Training course, an immersive experience that provides the look and feel of possible intrusion into participants' control system networks
- Developed 11 best practice documents
- Developed the Advanced Network Toolkit for Assessments and Remote Mapping (ANTFARM) to help asset owners map critical cyber assets
- Worked with industry to develop Bandolier audit files, which asset owners can use to optimize their security settings based on a best-practice configuration
- Begun commercializing the Secure SCADA Communications Protocol, which provides a secure method to communicate with remote devices
- Worked with industry to improve interoperability by developing a common set of definitions and metrics for security products and designing an Ethernet Security Gateway to test for interoperability with other products
- Worked with industry to develop Portaledge attack modules, which asset owners can incorporate into an existing tool to add advanced intrusion detection capabilities