# Lemnos Interoperable Security Program

## Creating common language and metrics for describing functions of network security tools and testing for interoperability

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.

Using the security functions described in the Open PCS (process control system) Security Architecture for Interoperable Design (OPSAID) and the Lemnos functional requirements, the project will define vocabulary, metrics, and testing methodologies for network security products. 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. The project aims to show that vendors can 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.

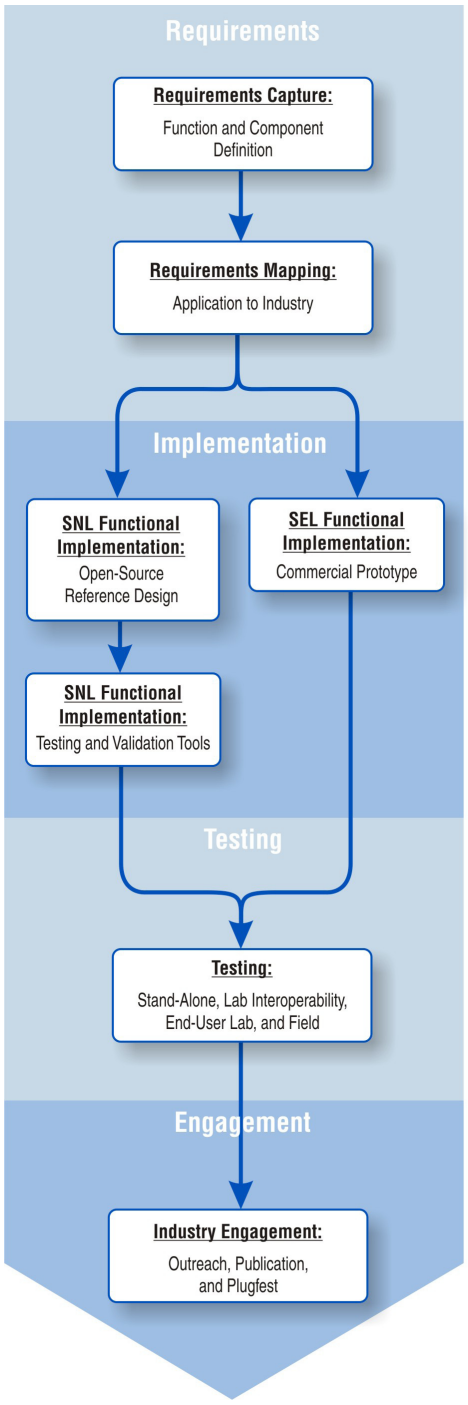
## National SCADA Test Bed

### Benefits

- Creates a universal way to describe and evaluate numerous control systems security functions
- Provides a method to demonstrate interoperability through independently manufactured security product prototypes
- Outlines a process for creating and demonstrating interoperability standards for energy control systems
- Ultimately helps control systems owners compare and evaluate security products based on function and system compatibility before purchasing

### Partners

- EnerNex Corporation
- Schweitzer Engineering Laboratories
- Tennessee Valley Authority
- Sandia National Laboratories




## Technical Objectives

### Define Functions

- Through interviews, EnerNex and project partners will 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.

### Build and Test

- 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.

### Exhibition and Engagement

- 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.

## End Results

By pursuing a common language, and using the reference implementation as a measuring device, the project team will:

- Demonstrate the success of this method in developing interoperable products
- Encourage industry-wide adoption of interoperability vocabulary and metrics as a first step toward industry standards

SNL will:

- Widely publish and publicize security functions and all vocabulary and metrics
- Publish open-source software used in the reference implementation
- Develop a lessons learned report detailing how the technology impacted the TVA control system

SEL will:

- Manufacture and market the commercial prototype to the control systems community

May 2008

### DOE National SCADA Test Bed (NSTB)

NSTB is a multi-laboratory resource that partners with industry and other government programs to test, research, and help design cyber security solutions to enhance control systems security in the energy sector and reduce the risk of energy disruption due to cyber attack.

### For More Information:

Hank Kenchington
Program Manager
DOE NSTB
202-586-1878
henry.kenchington@hq.doe.gov

Darren Highfill
EnerNex Corporation
865-218-4600 x6120
darren@enernex.com

### Visit Our Website:

www.oe.energy.gov/controlsecurity.htm