



**Process Control Systems
Industry Conference**



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

Lemnos Interoperable Security Project

EnerNex
CORPORATION



DOE Roadmap Vision

- ◆ **In 10 years control systems for critical applications will be designed, installed, operated, and maintained to survive an intentional cyber assault with no loss of critical function.**
- ◆ **Goals:**
 - Measure and assess security posture
 - Develop and integrate protective measures
 - Detect intrusion and implement response strategies
 - Sustain security improvements

DOE Roadmap Challenges

- ◆ **Coordination of research & development**
- ◆ **Focused research & development efforts**
- ◆ **Ongoing oversight and industry involvement**



DOE Roadmap and Lemnos

◆ Goal

- Develop and integrate protective measures

◆ Outcomes

- Foster energy community standards acceptance for security interoperability

◆ Roadmap Challenges

- Lack of common vocabulary and metrics for evaluating security functionality and performance

◆ Approach

- Establish a Reference Language, Build a Reference Design, Illustrate Commercial Viability, and Promote the Process

◆ Progress/accomplishments

- Functional, non-functional, and testing requirements defined. Common terminology identified.

Project Participants

- ◆ *Brian Smith, Tennessee Valley Authority*

- Nation's Largest Public Power Company



- ◆ *Rhett Smith, Schweitzer Engineering Laboratories*

- Vendor: Protection, monitoring, control, automation, and metering of electric power systems



- ◆ *Ron Halbgewachs, Sandia National Laboratories*

- Science-based technologies supporting national security



- ◆ *Dave Teumim, Teumim Technical, LLC*

- Consultant for Sandia National Laboratories

- ◆ *Darren Highfill, EnerNex Corporation*

- Electric power research, engineering, and consulting



Security Interoperability

◆ Problem: No standardized or widely accepted mechanism to evaluate:

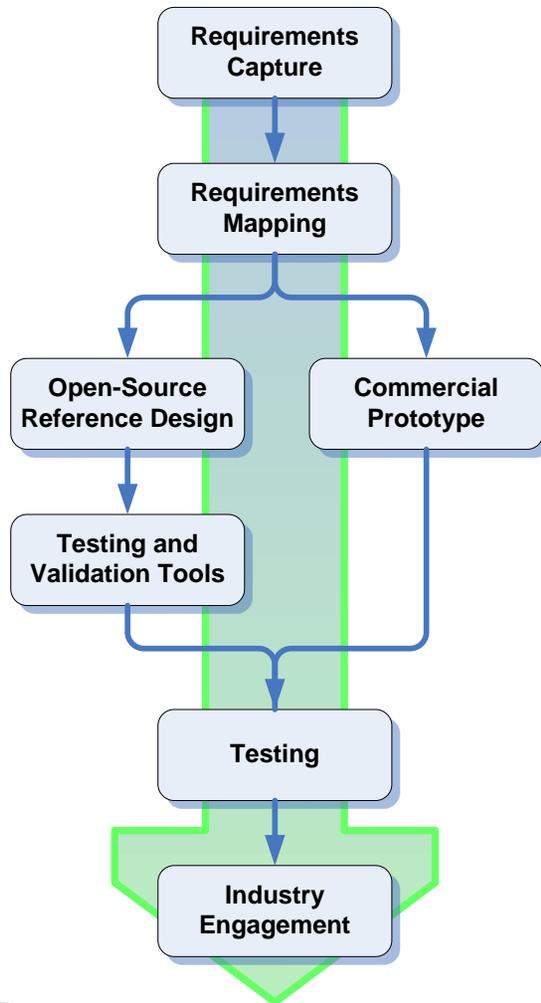
- Functionality
- Performance
- Interoperability



◆ Vendor Offerings:

- Rarely (if ever) map up scope “one-to-one”
- Lack of common definitions, metrics
- Limits ability to evaluate and compare

Program Overview



◆ Phase I

- Delineate the problem space
- Identify example to implement

◆ Phase II

- Build and test

◆ Phase III

- Engage the industry

Models of Secured Interoperability

- ◆ **Assume Equipment from Two Different Vendors**
- ◆ **Interoperability means the units can:**
 - #1 Talk to each other (same protocol)
 - #2 Act on the information exchanged to the benefit of both units
- ◆ **Three Ways to Interoperate:**
 - Both Parties Translate to a Third Common Language
 - One Party Supplies Translation Code to the Other
 - **Both Parties Use Same Basic Security Functions**
- ◆ **Security Interoperability**
 - Two different vendors pieces of security equipment can talk to each other
 - The two pieces of security equipment can exchange meaningful security information so that the resultant system is as secure or more secure than the individual units.

The Lemnos Model of Security Interoperability

- ◆ **Lemnos Model – Uses Security Function Building Blocks for:**
 - Secured Communications Channel
 - IPSEC
 - Messaging Channel (Logging messages to a central database)
 - Syslog
 - Others (Packet Filter Firewall using Iptables)

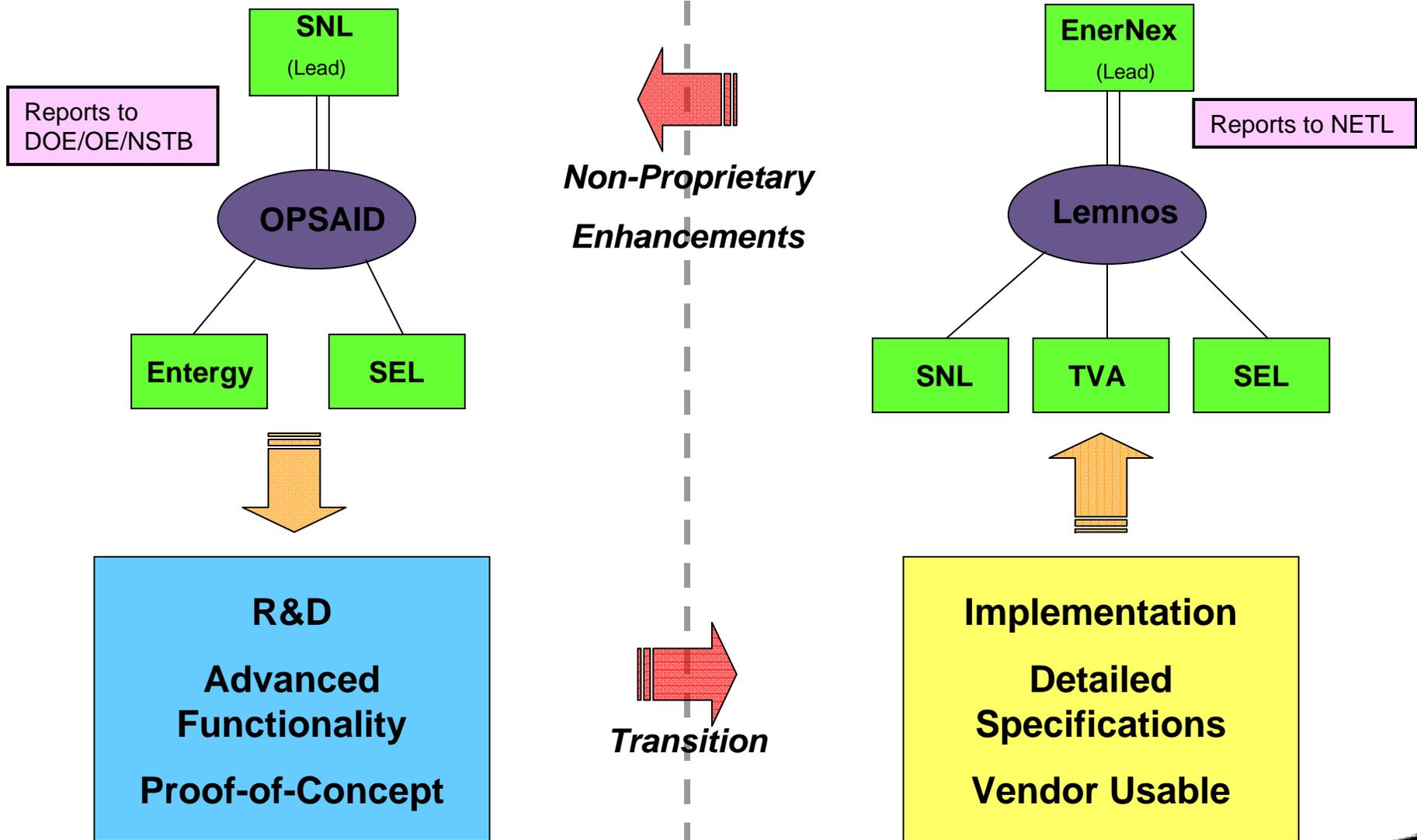
- ◆ **Vendors wanting to interoperate should have IPSEC and SYSLOG Capability**

- ◆ **Then we can proceed to discuss collaboratively what security information may be exchanged for benefit of securing the combined system**

Lemnos Project Developed from OPSAID

- ◆ **OPSAID (Open Process Control System Security for Interoperable Design)**
 - DOE NSTB funded project
- ◆ **OPSAID architecture and design is based entirely on Open Source Software and Standardized Hardware**
- ◆ **Reference architecture and configurations available to the public**

Relationship of OPSAID to Lemnos



Benefits of Lemnos Model for Energy Utilities

- ◆ At the PCSF 2007 OPSAID session energy utilities overwhelming wanted security equipment interoperability
- ◆ Energy utilities also voiced concerns about being “hitched” to only one security vendor with proprietary equipment that cannot interoperate with other vendor’s units.
- ◆ Lemnos can provide a convenient, readily available common denominator for this proprietary security equipment dilemma
- ◆ Lemnos offers a bottoms up “bandwagon” approach that leverages existing industry open source standards. This is in contrast to a top-down standards approach that requires wide committee consensus agreement and a lengthy process.
- ◆ Easy way to meet regulatory requirements

Benefits of Lemnos Model for Vendors

- ◆ **Shortened Development Cycle with OPSAID Code**
- ◆ **Uses Open Source Base Available to Public**
- ◆ **Vendors Can Include Value-Added Customization**
- ◆ **Lab and Field Proven Configurations**
- ◆ **Enhanced Ability to Meet Customer Needs**

Opportunities for Collaboration...Join Us !

- ◆ Interact with the Team (Utilities, Vendors) 2008
- ◆ Vendor Interoperability Lab Testing at TVA 2009
- ◆ Plugfest 2009
- ◆ Field Demonstration at TVA 2009