The Lemnos Interoperable Security Project

Brian Smith

Principal Consultant, EnerNex Corporation

ICSJWG 2010 Spring Conference

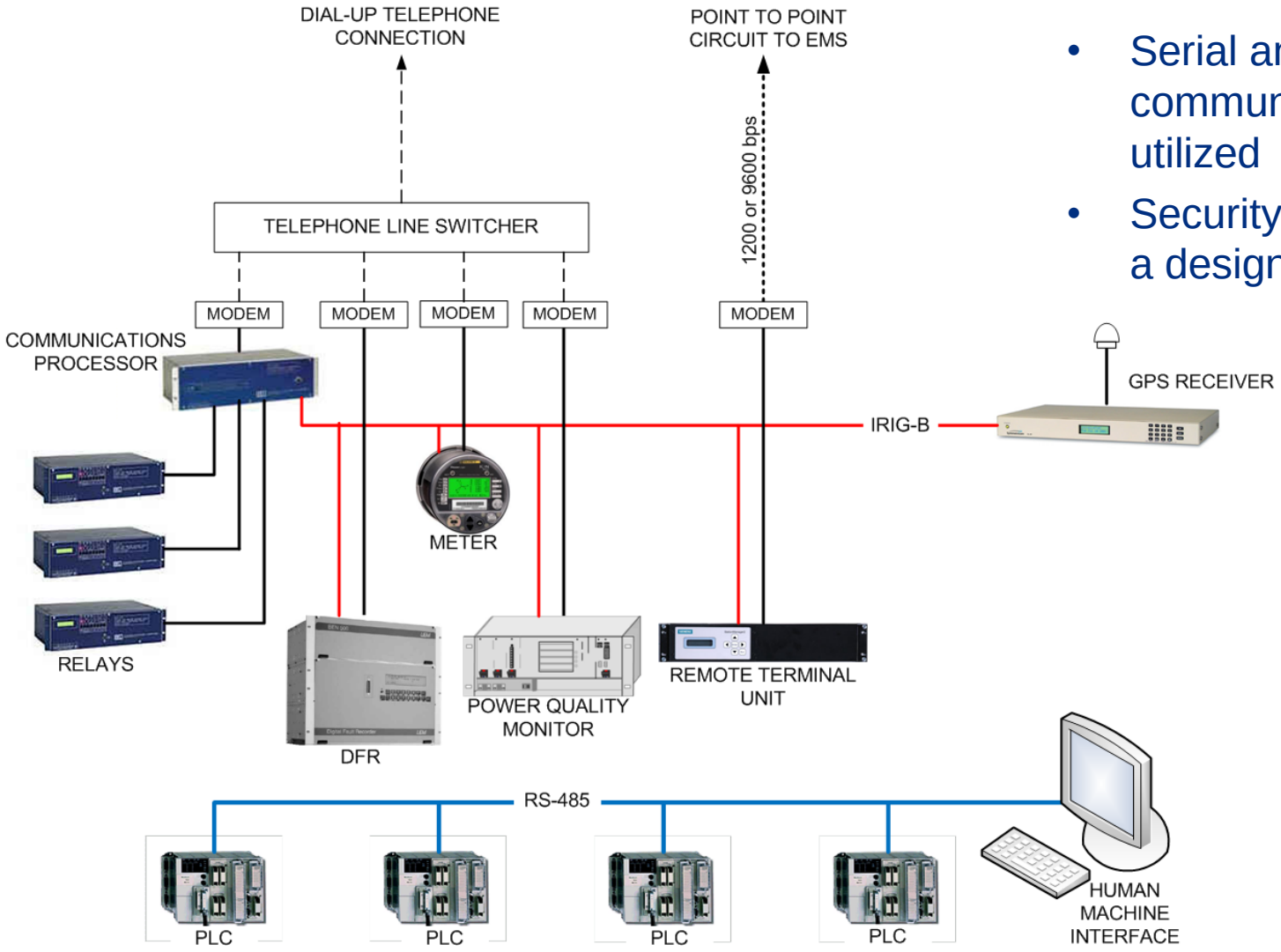
Energy Sector Challenges

- Security is more ***IMPORTANT*** than ever before as control system are evolving rapidly
  - Increasing use of Ethernet and IP communications
  - Connections to external systems
    - Supports changing operational and business needs
  - New and emerging regulatory requirements
- Implementing Security is more ***COMPLICATED*** than before
  - *End Users* are faced with limited security expertise
    - It shouldn't take a security expert to configure a device properly!
  - *Vendors* need alternatives to proprietary solutions
  - *End Users* and *Vendors* need a straight forward method to communicate user needs, product features, and configuration parameters relating to cyber security functions

Control System Architecture

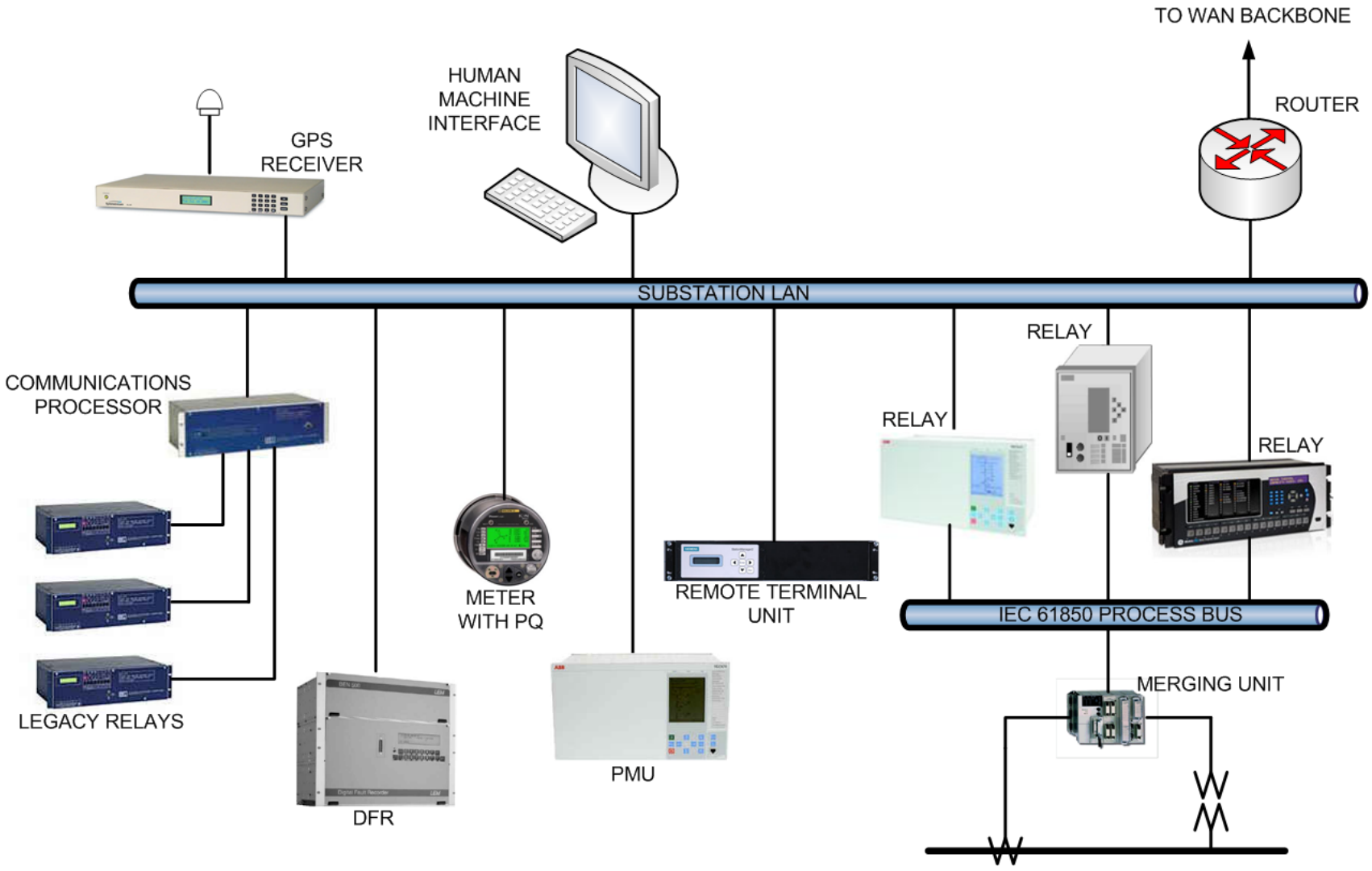
- Numerous architectures utilized throughout the ***ELECTRICITY***, ***OIL***, and ***GAS*** industries
  - More similarities than differences
- Characteristics of traditional control systems architecture
  - Single purpose networks
  - No connection to business networks
  - Serial heavily utilized
- Evolution to Ethernet and IP
  - Convergence to a single network
  - Multi-function end devices
  - Connections to other control systems
  - Connections to business networks

Traditional Substation Architecture



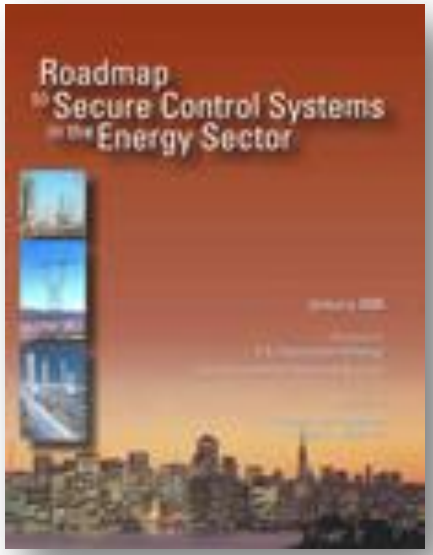
- Serial and dial-up communications heavily utilized
- Security generally wasn't a design requirement

Substation Architecture with Ethernet/IP



What is Lemnos?

- Lemnos is a DOE funded project to provide a security interoperability framework for use in the ***ENERGY SECTOR***
  - Supports the *Roadmap to Secure Control Systems in the Energy Sector*
  - Builds upon OPSAID which is a previous DOE project

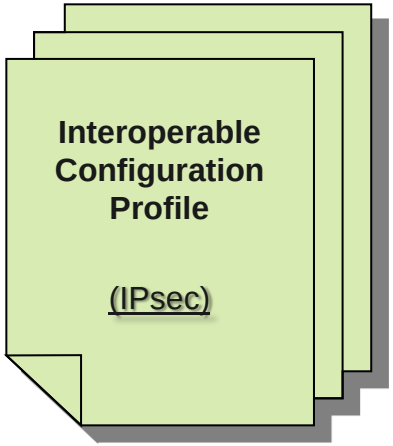


- Lemnos Partners
  - EnerNex Corporation (Prime Contractor)
  - Tennessee Valley Authority (Utility)
  - Sandia National Labs (FFRDC)
  - Schweitzer Engineering Laboratories (Vendor)

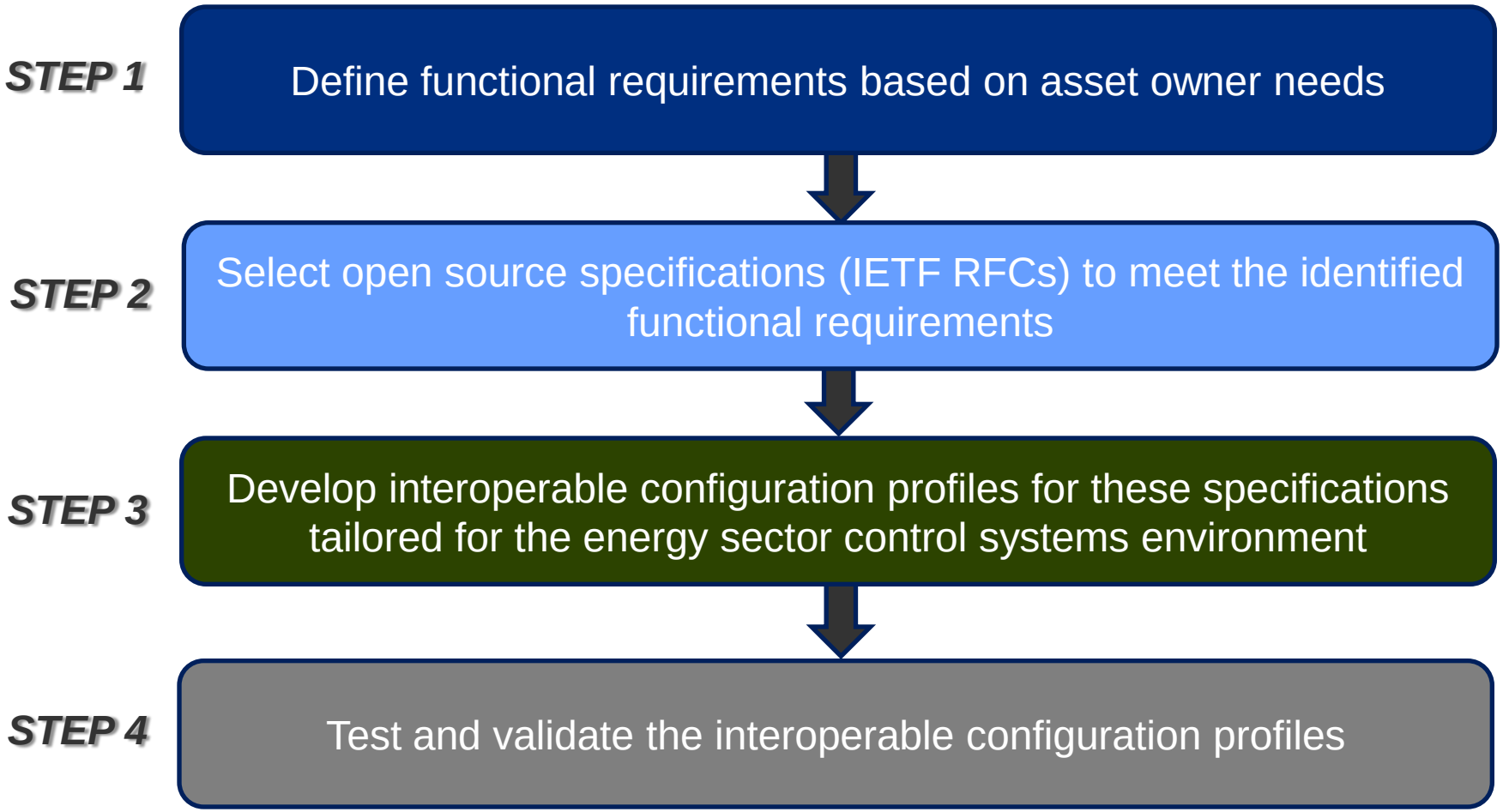
Lemnos Project Goal

- Enhance the interoperability of security devices from different vendors

  - Focuses on the development of ***INTEROPERABE CONFIGURATION PROFILES*** for widely accepted Internet protocols
    - Provides a design basis for vendors
    - Utilizes open-source software
    - Provides a reference point for End Users



Profile Development Method



Lemnos – Step 1

Define Functional Requirements

- Requirements identified based on asset owner needs
- Examples include:

Functional Requirement
Secure communications channel
Filter illegal network traffic
Notification, non-repudiation, traceability, and troubleshooting
Cryptography and password management
Detect malicious activity by monitoring network traffic
Monitor and analyze system processes
Identify, neutralize, or eliminate malicious software

Lemnos – Step 2

Select Open Source Specifications

- For each functional requirement, the philosophy is to select the most commonly used, well-proven, open source solution.
- Examples include:

Functional Requirement	Component	Module
Secure communications channel	Virtual Private Network	IPsec
Notification, Non-repudiation, Traceability, Trouble Shooting	Audit Log	Syslog

Lemnos – Step 3

Develop Interoperable Configuration Profiles

- Define parameters within the RFCs
  - Each RFC contains a myriad of choices
- Examples for IPsec include:

Configuration Parameter
Use ESP (Encapsulating Security Payload)
Use TUNNEL mode
Use HMAC for authentication
Use IKE Version 1
Use DH-5 (Diffie-Hellman Group 5)

Lemnos - Step 4

Test and Validate

- Demonstrate cyber security interoperability using the Interoperable Configuration Profiles
  - Long term tests to validate stability
  - Multi-vendor architecture
  - Simulated utility architecture
- Validate that the added security does not impact the reliability of the hosted power system applications

Lemnos Benefits

End User Perspective

- Enables End Users to choose ***BEST IN CLASS*** solutions for various facilities (versus a “one size fits all”)
  - For example, an electric utility may have unique needs for:
    - Communications Hub/Control Center
    - Substation LAN
    - Generating Plant DCS
    - Outdoor and Pole-top
- Reduction in setup/deployment time and effort
  - Lower Total Cost of Ownership
- Reduction in configuration errors

Lemnos Benefits

Vendor Perspective

- Permits shortened development cycle by providing reference design
  - OPSAID reference design available to public
  - Robustness of open source versus proprietary solutions
- Uses configurations proven in lab and field to secure control system communications in a way that doesn't trade off reliability
- Enhances the vendor's ability to meet the customer's needs
  - Provides a common understanding between customer and vendor

Project Status

- Two year project originally scheduled to complete March 2010
  - One year extension to 2011 for additional work
- Work to date has been focused on secure communications channel (IPsec) and Messaging channel (Syslog)
  - Interoperable Configuration Profiles completed
  - End User testing at TVA lab completed
- Public demonstrations held at ISA Expo and DistribuTECH
  - Additional vendors participating in demonstrations include:
    - ❑ RuggedCom
    - ❑ GarrettCom
    - ❑ Industrial Defender
    - ❑ N-Dimension
    - ❑ Phoenix Contact
    - ❑ SIEMENS

Additional Work for 2010

- Focus on:
  - Standardizing components of Syslog messages
  - Secure engineering access
    - Compliment to IPsec
    - SSH/SSL
  - Centralized authentication & authorization
    - LDAP
- Identify organization to become long term steward of the work after project completion

Discussion

Project Contacts

EnerNex Corporation

- Brian Smith - bpsmith@enernex.com

Tennessee Valley Authority

- John Stewart - jwstewart@tva.gov

Sandia National Laboratories

- Ron Halbgewachs - rdhalbg@sandia.gov
- Adrian Chavez - adrchav@sandia.gov
- Dave Teumim - dave431@enter.net (Sandia Contractor)

Schweitzer Engineering Laboratories

- Rhett Smith - Rhett_Smith@selinc.com