American Water Works Association
The Authoritative Resource on Safe Water

SAND2009-2291C

2009 Water Security Congress

OPSAID: Open PCS Security Architecture for Interoperable Design

April 10, 2009

Ronald Halbgewachs

Sandia National Laboratories

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

Sandia
National
Laboratories

A Challenge: Industrial Control Systems Cyber Security for Water Systems

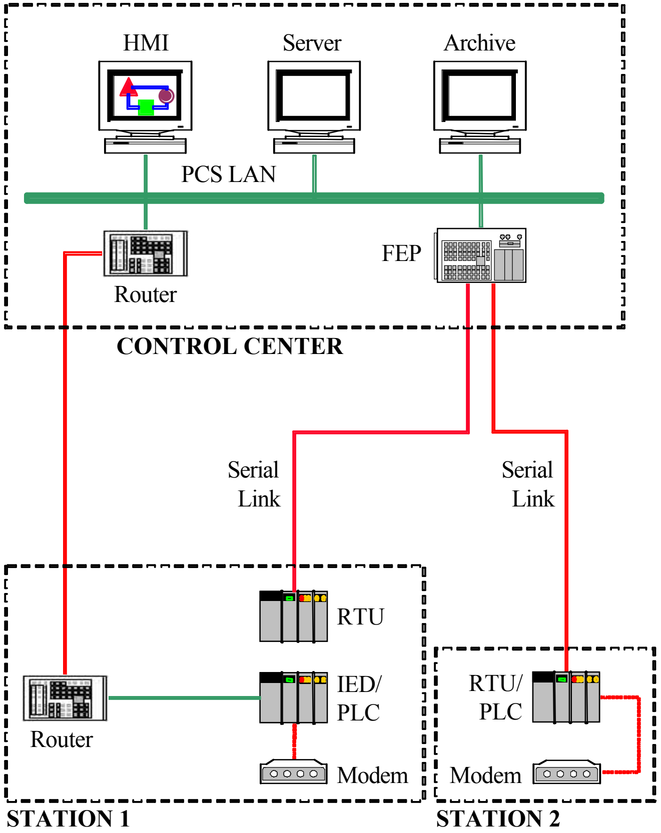
- ***"In ten years, industrial control systems for critical applications will be designed, installed, and maintained to operate with no loss of critical function during and after a cyber event."*** [1]
  - How can current, legacy control systems be secured while new architectural designs for secured cyber control systems are being implemented?
  - How can new secured systems be phased into existing operations?
  - How can cost-effective cyber security & interoperability solutions be attained without major disruptions in service?

[1] Roadmap to Secure Control Systems in the Water Sector, Water Sector Coordinating Council Cyber Security Working Group, March 2008, Vision, p21.

Process Control Systems (PCS) Security Risks

Historically PCS

- Not connected to business networks or Internet; isolated environments
- Recent use of conventional hardware, COTS, connectivity, & network services have dramatically heightened security risk
- Currently most PCS automation hardware & software cannot support needed security
- Legacy Serial Links moving to Internet Protocol (IP) Links



Fundamental Design Principles

- OPSAID-compliant systems will have no impact on operational configurations of existing automation systems

- The design provides secure management capability to augment current practices

- Adding an OPSAID overlay inserts monitoring and logging capabilities to supervise system security and state-of-health

Why OPSAID?

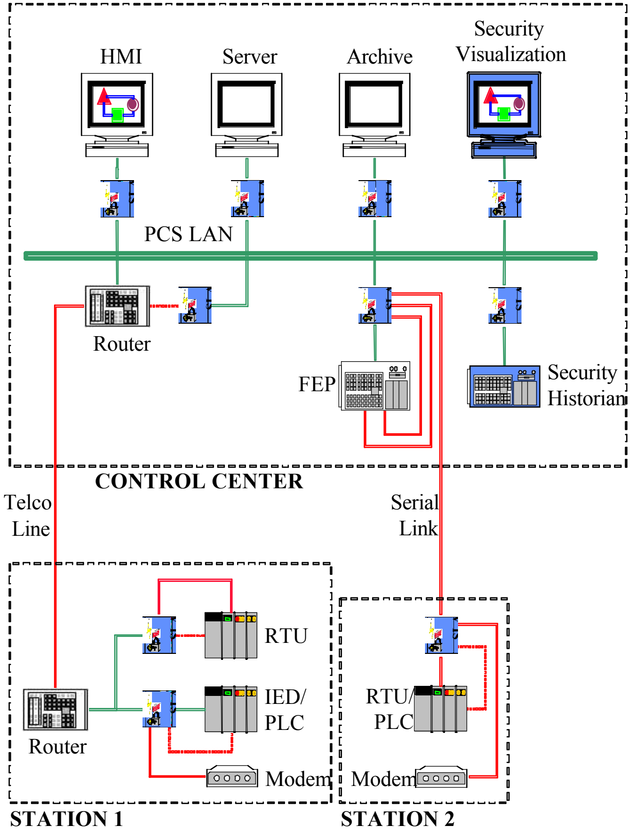
- Architecture design is based entirely on open-source software and standardized hardware
- Uses the open architecture to promote interoperability
- Brings the security of legacy systems to an acceptable level
- Provides a path forward for the development of inherently-secure PCS components in the future
- Provides a design basis for vendors to build secure, interoperable devices
- Produces a means for asset owners & providers to be selective in purchasing control system equipment from vendors to best meet the system needs

Reduce the Risk

- Utilize systems that offer built-in cyber security.

- Develop components that operate with any control system.

- “Raise the bar” – make an attack more and more difficult for an adversary; eliminate the lower level threats by making any attack more costly in time, skill level, access, & money.



Sandia National Laboratories

OPSAID Security Features

- Virtual Private Network - Interoperability of control system elements
- Use of encryption and data authentication
- System intrusion detection and prevention
- Firewalls and network filtering
- Authentication and logging for remote access
- Public Key Infrastructure – generate, sign, and validate digital signatures including a certificate authority
- Host intrusion detection and prevention
- Control system monitoring and visualization of the monitored information
- Data logging capture for replay and forensic analysis

Development Approach

- Perform the research, design, & development of an advanced-functionality, open & interoperable security architecture. (Started with internal Laboratory research funding)

- Build a proof-of-concept prototype based upon open-source software & standardized hardware to demonstrate & test the architecture. (DOE funding support)

- Information about OPSAID is available on The Center for SCADA Security website

  http://www.sandia.gov/scada/documents.htm

Technology Transfer/Collaboration

- Functional testing of OPSAID was initially accomplished with Entergy Corporation (utility partner) and Schweitzer Engineering Laboratory (SEL) (vendor partner). (DOE funding support)

- Current industry outreach for end-user application/adoption is being accomplished through another DOE program called the Lemnos Interoperable Security Program to develop and perform testing based upon the OPSAID architecture. (DOE funding support)

- Lemnos Partners: EnerNex Corporation, Schweitzer Engineering Laboratory, Sandia National Laboratories, Tennessee Valley Authority.

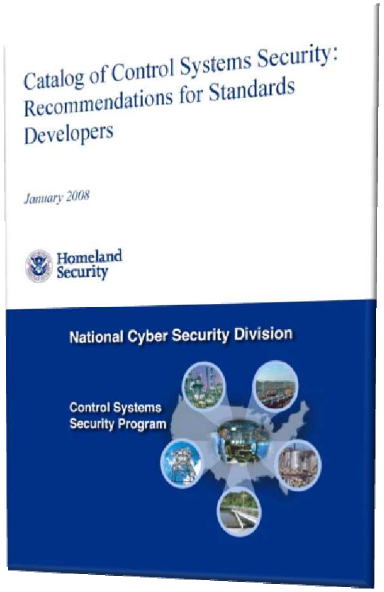
- The Lemnos program includes site testing at TVA and a “plugfest” with other control system vendors, currently scheduled to be held at the ISA Annual Conference, Houston, TX, October 6-8, 2009.

→ This presentation to the AWWA Water Security Conference is sponsored by the Department of Homeland Security, National Cyber Security Division, Control Systems Security Program.

Another Resource for Information Control Systems Security

Catalog of Control Systems Security: Recommendations for Standards Developers, DHS, January 2008, http://www.us-cert.gov/control_systems/

- Provide guidance for cyber security requirements specific to control systems
- Support standards bodies and industry associations to implement sound security practices in current standards
- The Catalog is not limited for use by a specific industry sector but can be used by all sectors
- The Catalog can be used:
  - As a source for cross-sector standards information
  - As a discussion tool to promote security awareness
  - To mitigate vulnerabilities identified during assessments, audits, and cyber incidents
  - To develop policies and procedures
  - For employee training and awareness



Catalog of Control Systems Security: Recommendations for Standards Developers

January 2008

Homeland Security

National Cyber Security Division

Control Systems Security Program

OPSAID Contact Information

Ron Halbgewachs
Sandia National Laboratories
P.O. Box 5800, MS 1235
Albuquerque, NM 87185

rdhalbg@sandia.gov

OPSAID Additional Information

- OPSAID Specifications follow:
  - Software Implementation
  - Hardware Prototype

- Lemnos information available at

  http://www.oe.energy.gov/DocumentsandMedia/5-Lemnos.pdf

OPSAID Prototype Software (Release 2)

- Virtual Private Network – strongSwan
- Embedded Linux (Debian, Ubuntu, Gentoo)
- IPsec using AES encryption (128 bits, 256 bits)
- Network intrusion detection – Snort
- Host intrusion detection – OSSEC HIDS
- Public Key Infrastructure – Openssl/strongswan/CertAuth
- Firewall – uses iptables
- Message communication logging – syslog-ng
- Security historian database – MySQL
- Configuration access to devices – ssh
- Visualization of message logging – Java/OpenGL

OPSAID Prototype
HW Platform (Release 2)

- Mini-ITX board & fanless enclosure
- 1 GHz VIA processor
- PCI expandability

- 2 Ethernet & 6 serial connections (expandable)
- 1 Gbyte flash ROM
- 1 Gbyte RAM