Open PCS Security Architecture For Interoperable Design (OPSAID)

A Department of Energy / National SCADA Test Bed Project

fact sheet
06/02/08

Information Assurance & Survivability

Overview:

The OPSAID program provides a design basis for vendors to build add-on security devices. The addition of these devices can bring the security of legacy systems up to an acceptable level, while providing a path forward for the development of inherently-secure PCS elements in the future. In contrast to some security solutions, the OPSAID effort is based entirely on open-source software and standardized hardware, using an open architecture to promote interoperability. This program was initially funded internally by Sandia, but has since been funded by the DOE/OE NSTB program to advance the concept to an initial design.

PCS Security Risks:

Historically, Process Control Systems (PCS) have not been connected to business networks or the Internet, which has to some extent shielded them from cyber attacks. The recent use of conventional operating systems, computing hardware, connectivity, and network services in control and automation systems have dramatically heightened the security risks. Most available automation hardware and software cannot support needed security services to mitigate these risks.

Fundamental Design Principles:

- OPSAID-compliant systems will have no impact on operational configurations of existing automation systems (except for some small latency)
- The design will provide secure management capability to augment current practices
- Adding an OPSAID overlay inserts monitoring and logging capabilities to supervise system security and state-of-health

Design Considerations:

- Open-architecture design standards-based hardware and software
- Add-on design defines requirements for intrinsic security capabilities in future control systems and components
- Design integrates with most legacy systems as well as modern ones
- Minimize retrofitting and meet operational, physical, and maintenance requirements

Features:

- Virtual Private Network
- Encryption & data authentication
- Logging & forensics support
- Intrusion detection & prevention
- Firewall and network filtering
- Authentication and logging for remote access
- Control system visualization & monitoring

Researcher Contact Information:

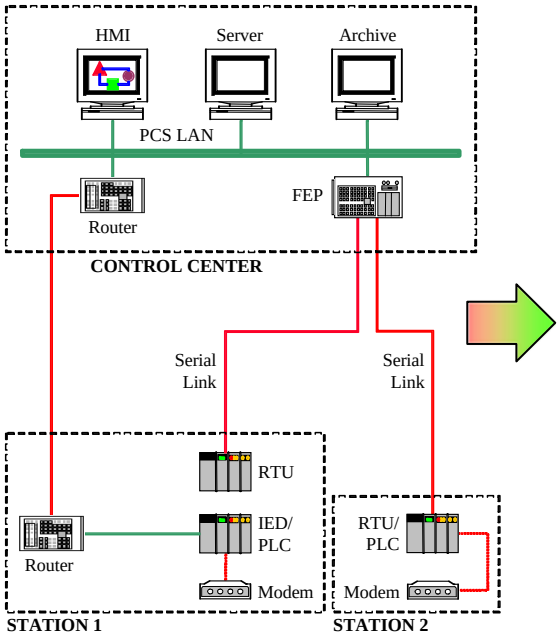
Ron Halbgewachs (505-844-8054)
rdhalbg@sandia.gov
Sandia National Laboratories
P.O. Box 5800, MS-1235
Albuquerque, NM 87185-1235

Adrian Chavez (505-284-6664)
adrchav@sandia.gov
Sandia National Laboratories
P.O. Box 5800, MS-0672
Albuquerque, New Mexico 87185-0672

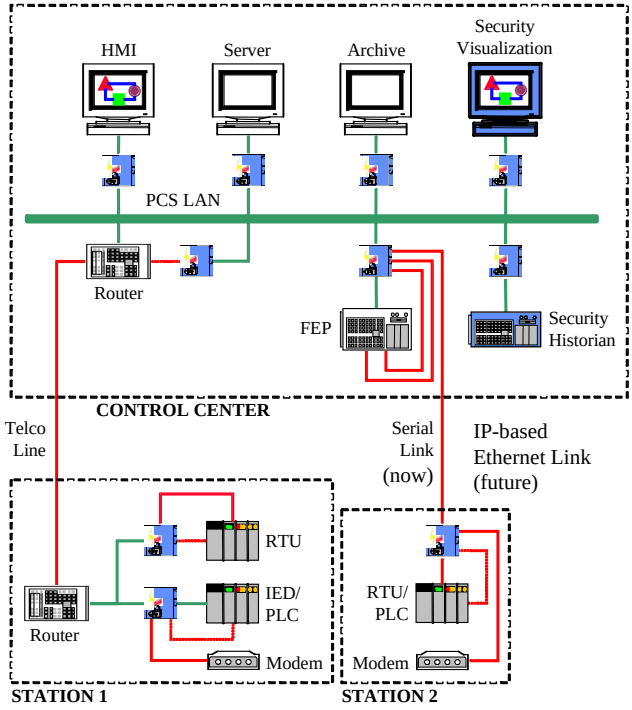
DOE/NSTB OPSAID Application For Secure Process Control Systems

Information Assurance & Survivability

Original, Poorly Secured Control Systems



Highly Secured Control Systems



Prototype - Hardware Platform 1

- PC104 architectural & industrial enclosure
- Hardware-accelerated encryption
- 533MHz XScale processor
- 2 Ethernet & 4 serial connections (expandable)
- 8 binary status inputs (expandable)
- 16MB or 32MB flash ROM
- CompactFlash slot for additional storage

Prototype - Hardware Platform 2 (Release 1)

- Mini-ITX board & fanless enclosure
- 1GHz VIA processor
- 2 Ethernet & 6 serial connections (expandable)
- PCI expandability
- 1 GB flash ROM
- 1 GB RAM

Software

- Virtual Private Network (strongSwan)
- Embedded Linux (Debian, Ubuntu, Gentoo)
- IPsec using AES encryption
- Snort network intrusion detection
- Firewall (using iptables)
- syslog-ng for logging communication
- MySQL database on security historian
- ssh for configuration access to devices
- Java/OpenGL visualization of logging

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.