

NSTB

National SCADA Test Bed

enhancing control systems security in the energy sector

Visualization and Controls Program

Peer Review 2006

Secure Linux Appliance for PCS (SLAP): Open Architecture / Interoperable Design

Jason Stamp, Principal Investigator

Sandia National Laboratories

(505) 284-6797

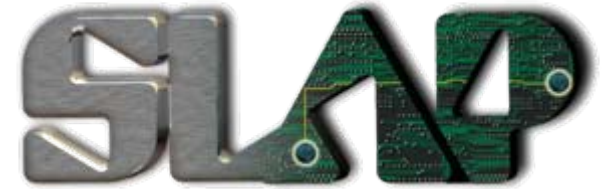
jestamp@sandia.gov



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.

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

Work Package Description

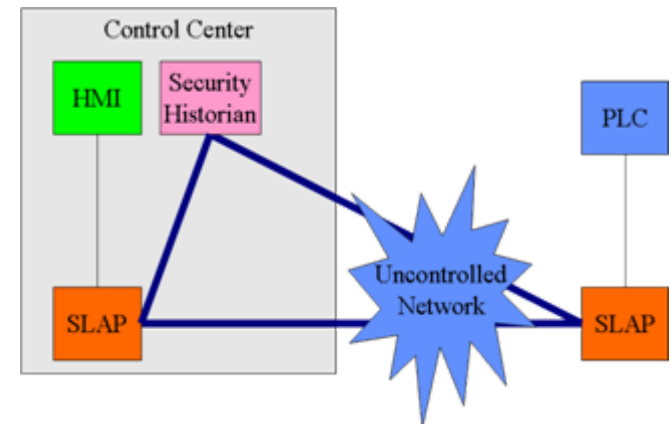


- Secure Linux Appliance for PCS (SLAP) system provides a *design* basis for vendors to build add-on security devices
- These devices will bring the security of legacy systems up to an acceptable level
- Design provides a path forward for the development of inherently-secure PCS elements in the future
- SLAP design effort is based entirely on open-source software and standardized hardware, using an open architecture to promote interoperability
- FY06 Budget: \$542k

An industry-driven, interoperable design for secure PCS devices that can be integrated into control systems

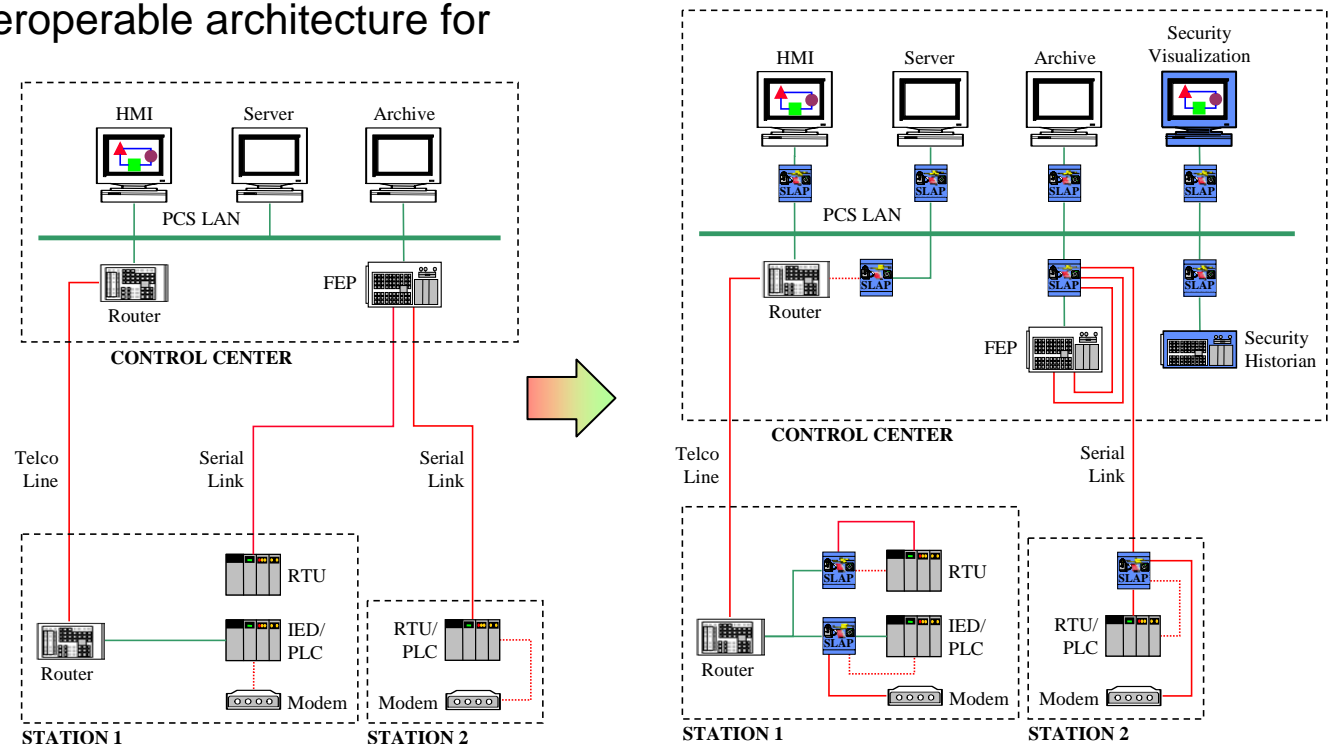
Industry Needs

- Problem:
 - PCS connected to business networks or the Internet
 - Recent use of conventional operating systems, computing hardware, connectivity, and network services in control and automation systems
 - Automation hardware and software cannot support needed security services to mitigate these risks
 - *Dramatically heightened security risks*
- **Solution: an open-architecture, interoperable design for PCS security devices and services**
 - Encryption & data authentication
 - Logging & forensics support
 - Intrusion detection & prevention
 - Firewall and network filtering
 - Encrypted serial communications
 - Authentication and logging for remote access
 - Control system visualization & monitoring
- The reference platforms are not the product; *the design is the goal*



Industry Benefits (Impacts)

- Secure PCS, including authenticated / encrypted communications
- Shield hosts with known vulnerabilities from the PCS network
- Add monitoring and visualization for PCS security and state-of-health
- Greatly improve configuration access to PCS devices
- Provide a design for future, inherently-secure PCS devices
- Provide an open, interoperable architecture for vendors to build security devices



Technical Approach

- A SLAP system will have no impact on the operational configuration of existing automation systems (except for some small latency)
- The design will provide secure management capability to augment current configuration practices
- Adding a SLAP system overlay inserts monitoring and logging capabilities to supervise system security and state-of-health
- Tasks:
 - Integration and Testing: develop the software and hardware for the SLAP reference architecture
 - Security Visualization: PCS security visualization
 - System Configuration and Deployment: develop an installation and key management strategy
 - Field Test: reference implementation will be integrated with an existing industry systems
 - Outreach: working agreements with industry and other agencies guide the SLAP development

Collaborations and Partnerships

- Entergy field test partner:
 - Successful two day field trip to Entergy in Baton Rouge (August)
 - Lab- and field-test SLAP prototypes
 - Provide key operational feedback on the SLAP/OAID
 - Defined Case 1 test to exercise SLAP reference build
 - Defined Case 1+ to get a sense of the final SLAP requirements
 - Draft test plan for lab test with Entergy completed
 - Entergy lab test scheduled for October 16-21 in Baton Rouge
- Teppco field test partner:
 - Planned Houston visit to Tom Frobase
 - Timeframe is 4Q06, 1Q07
 - Prototype test completed NSTB equipment
- NIST (Jim Gilsinn, Joe Falco) are reviewing the SLAP test procedure
- Others:
 - Network equipment vendor Teltone has joined the project (Ori Artman)
 - High percentage of the substation dialup market
 - Willing to share legacy technology with the team
 - Spoke to a wide range of networking vendors to understand how vendors view the legacy and next-generation landscape
 - A second networking vendor, TecSec, has asked to join the project (brings a key management infrastructure known as CKM)

Technical Progress - Accomplishments

- Completed development of the architectural layout for the OS images on new mini-ITX-based SLAP field platforms
- Technical details of second-generation reference implementation finalized:
 - Firewall, bridging, syslog-ng, IPsec, hash files, etc.
 - New work: basic serial architecture and configuration session capture
- Prototype security visualization and historian
 - Java-based graphical depiction of system conditions
 - Secondary database for visualization parameters
- Architecture for security monitoring of operational traffic (for Modbus, right now) and will working to extend it to DNP3
- Basic investigation of key management architectures is underway
- Very preliminary SLAP performance results

