Alliance Project: Cyber-Physical Security Unified Access Solution

Unified cyber-physical security to protect energy sector control systems and facilities

Background

The North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards require utility operators to control, monitor, and record physical access to cybersecurity assets and establish physical security perimeters (PSPs). Many operators engage security contractors to provide access controls, monitoring, intrusion detection, and other related physical security services; however, this adds cost, increases administrative complexity, and makes relating logical and physical access control records difficult. A solution that integrates logical and physical access controls into a unified trust management infrastructure can improve situational awareness while reducing total cost of ownership and increasing job efficiency.

Barriers

- Cost-efficient way to replace brass key physical security with centrally managed and monitored scalable solutions.
- Single solution that can be applied to a wide range of physical security perimeter sizes from the control house to the panel.
- Requirement that system operates on existing trusted management information technology (IT) infrastructure.
- Incorporation of multi-factor authentication in validating credentials.
- Product validation to FIPS 140-2 Level 2 requirements.

Project Description

The Alliance project is developing a proximity card reader and controller that allows physical and cybersecurity access to be monitored, tracked, and controlled using a single system. The reader and controller consist of four easy-to-deploy components:

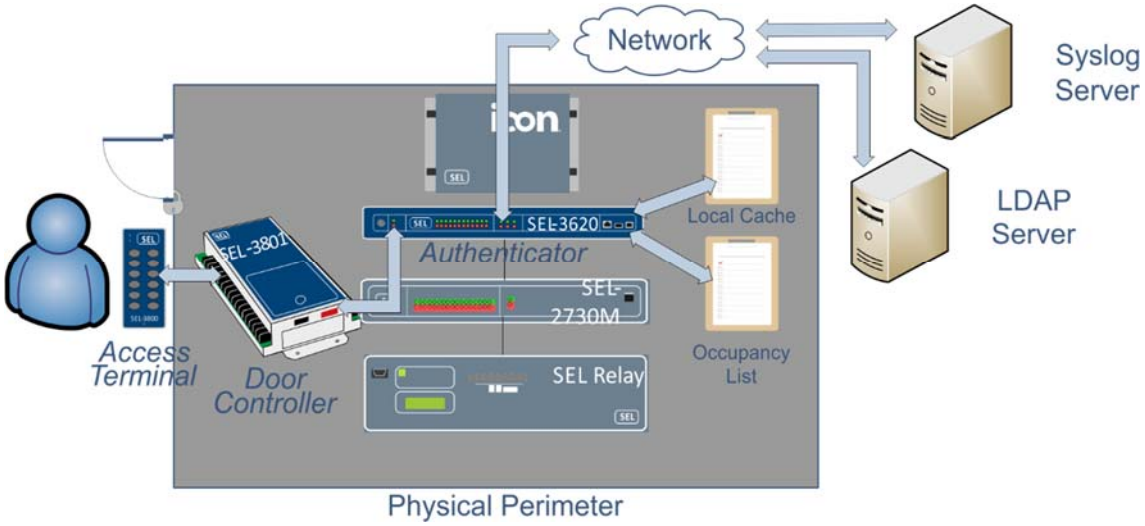
1. Access terminal (AT): The AT is an ISO 14443- / ISO 15693-compliant card reader that integrates with the SEL Lemnos and Padlock cybersecurity systems found in the commercially available SEL-3620 and SEL-3622.
2. Access control processor (ACP): The ACP is a peripheral device that controls the door lock and sensor hardware based on the authentication credentials gathered by the AT and authorized by the SEL-3620 or SEL-3622.
3. Enhanced firmware for the SEL-3620 and SEL-3622 security gateways: The SEL gateways communicate with the organization's active directory or RADIUS servers and are outfitted with enhanced firmware to proxy physical access requests and grant/deny responses. This unifies the trust, log, and administrative management of cyber and physical access control systems.
4. Card enrollment solution: This component associates physical access credentials with active directory user accounts.

Benefits

- Creates a single solution that protects both electronic and physical perimeter
- Integrates cyber and physical access records
- Enables operators to have better awareness of the system state
- Provides high granularity of cyber-physical access control—down to the rack level
- Lowers total cost of ownership, simplifies training, and eases and enhances the reliability of access control administration

Partners

- **Schweitzer Engineering Laboratories (SEL)**
- Sandia National Laboratories
- Tennessee Valley Authority



Product overview: system components and interconnections

Technical Objectives

This project is developing a cyber-physical access control system designed to be applied to power system facilities, as well as cabinets and panels that interoperate with the organization's existing cybersecurity system. The goal is to have a single trust management central directory and log management server, simplifying technical deployment, compliance, and administrative procedures while lowering the total cost of ownership and improving reliability. The access control reader will be ISO 14443 Type A and Type B, ISO 15693, and FIPS 140-2 Level 2 compliant. This solution allows utility operators to implement a single system solution to protect both cyber and physical security parameters while adhering to NERC CIP regulations.

Phase 1: Research and Development

- Design a cyber-physical access control system to withstand the IEEE 1613 and IEC 61850-3 environmental conditions
- Develop a method to unify the physical access control and monitoring technology with the cyber access control and monitoring technology to improve situational awareness
- Commercially release a cyber-physical access control reader for the energy sector
- Commercially release a door controller and security gateway able to control and merge with the existing cybersecurity infrastructure
- Commercially release the tools needed to ease commissioning and deployment of the physical access control credentials and associate them with Active Directory user accounts

Phase 2: Validation Testing

- Apply the technology in testing that models the field deployment and confirm operational functionality requirements are met
- Complete security robustness testing
- Author deployment and maintenance guides

End Results

Project results will include the following:

- Electronic cyber-physical access control solution that runs on the same cyber account management and log system
- Substation-ready IEEE 1613- and IEC 61850-3-compliant hardware for cyber-physical access control
- Situational awareness with the logs and reports required to ease NERC CIP compliance efforts

May 2015

Cybersecurity for Energy Delivery Systems (CEDS)

CEDS projects are funded through the U.S. Department of Energy's (DOE) Office of Electricity Delivery and Energy Reliability (OE) research and development (R&D) program, which aims to enhance the reliability and resilience of the nation's energy infrastructure by reducing the risk of energy disruptions due to cyber attacks.

Contact Information:

Carol Hawk
Program Manager
DOE OE R&D
202-586-3247
carol.hawk@hq.doe.gov

Rhett Smith
Sr. Product Manager
Schweitzer Engineering Laboratories
1-509-336-7939
Rhett_Smith@selinc.com

For More Information:

- http://energy.gov/oe/technology-development/energy-delivery-systems-cybersecurity
- www.controlsystemsroadmap.net