Integrated Security System (ISS)

A security platform providing multi-layer intrusion detection and security management for a networked energy control architecture

A cost-shared effort between industry and

U.S. DEPARTMENT OF ENERGY | Cybersecurity, Energy Security, and Emergency Response

Cyber Security for Energy Delivery Systems

ISS

Project Lead:
Siemens Corporate Research

Partners:
Rutgers University
Idaho National Laboratory

The Concept

The Integrated Security System (ISS) is a security platform that provides multi-layered security features and intrusion detection at the field device, network, and control system levels. The ISS operates as part of the security layer that integrates within the grid's energy process systems layer and the automation and control layer. The power grid's automation and control layer monitors and controls power transmission and distribution processes, while the security layer provides security features. This separation of responsibilities enables ISS to integrate with legacy energy control systems without compromising control performance, reliability, stability, and availability.

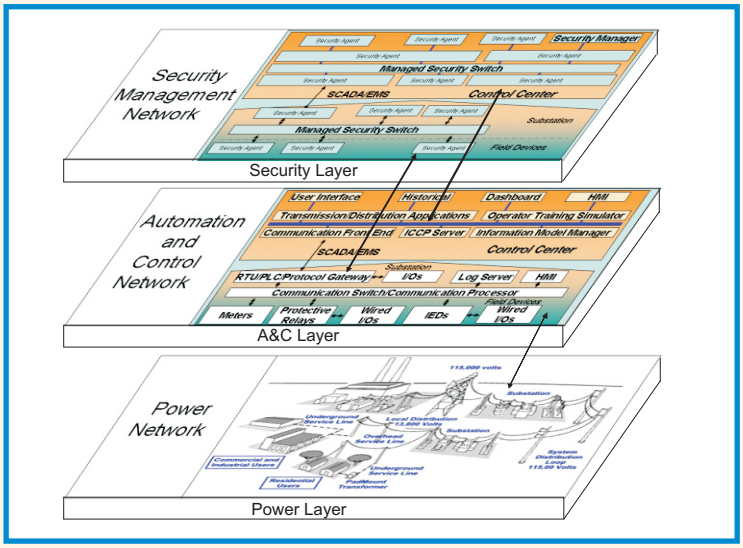
The ISS has three components in development—agents, managed switches, and managers:

Security agents vary in complexity and protect network field devices with functions such as access control. Security agents for intelligent electronic devices (IEDs) contain simple rules and decision making capabilities, including event logging and reporting, whereas agents for higher-level field devices like programmable logic controllers (PLCs) contain more complex rules for intrusion and event detection within the controllers.

Managed security switches work as network devices, connecting controllers, remote terminal units (RTUs), human machine interfaces (HMIs), and servers in the substation and control center. The switches manage system networks, prioritize data, and protect bandwidth.

The security managers control the security policies of the security agents and switches, collect and analyze security agent and switch information, and acquire vulnerability patches from vendor servers and download them to the appropriate security agents. Security managers themselves can be protected by a utility's existing IT security solutions.

Diagram of the ISS Platform



The Approach

Security agents, switches, and managers each provide intrusion detection capabilities to the field devices, network, and system, respectively. ISS uses an anomaly-based intrusion detection mechanism combined with model-based probabilistic techniques to pre-define system information traffic patterns and minimize false alarms caused by random traffic patterns.

The project team developed an initial ISS prototype including two stand-alone security agents, a security agent application for a protected device, a managed security switch, and a security manager. The team designed an initial vulnerability test for this prototype and used the results to develop the second prototype for the substation level. A second vulnerability test was conducted at the end of 2009.

The ISS team has also worked with other DOE cost-shared project teams to ensure the ISS incorporates or is interoperable with newly commercialized security technologies.

Next Steps

In 2010, the team will engage Los Alamos National Laboratory to review and evaluate the performance of the design and implementation prototype. Next, the team will work to translate the software to other systems, and begin early translation and testing on selected embedded devices.

Benefits

- Applies to electricity, oil, and natural gas SCADA systems
- Allows energy asset owners to design a secure control system architecture
- Protects both new and legacy control systems
- Protects against denial of service attacks
- Provides centralized management, reporting, and in-band updates for a distributed solution
- Performs independent of the underlying operating system
- Conforms to the North American Electric Reliability Corporation Critical Infrastructure Protection standards 005 and 007

Cybersecurity for Energy Delivery Systems (CEDS)

CEDS projects are funded through the Department of Energy's (DOE) Office of Cybersecurity, Energy Security, and Emergency Response (CESER) 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 emergency disruptions due to cyberattacks.

For more information: https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/cybersecurity-research-development-and

Initial Leads
Carol Hawk, Program Manager

Livio Dalloro
Siemens Corporate Research
609-734-3571
livio.dalloro@siemens.com

Paul Skare
Siemens
952-607-2071
paul.skare@siemens.com

Current Contact as of Aug. 2020

Akhlesh Kaushiva
Program Manager
DOE CESER
202-287-6062
akhlesh.kaushiva@hq.doe.gov