Control System Situational Awareness Technology

A situational awareness tool suite for control systems, customized by user needs

Background

Control systems are used in the energy sector to aid in managing and directing the processes that generate, transmit and distribute energy over a dispersed network of interconnected components. These systems are widely distributed throughout the grid and are manufactured by a wide variety of vendors. Enhancing situational awareness through the use of advanced technologies that acquire, analyze, correlate, identify and display Supervisory Control and Data Acquisition (SCADA) data can help inform appropriate responses in real-time to threats across the control system communications domain.

Barriers

- Energy sector system architectures are complex and widely distributed
- It is difficult to generate actionable and timely information for visualizing a security posture based on vast quantities of data from a variety of sources with differing levels of granularity
- There is a lack of available interoperable situational awareness tools for safeguarding critical infrastructure assets
- In some cases, existing security measures may be implemented inconsistently

Project Description

This project will develop a set of tools that support a comprehensive and consistent implementation of cybersecurity and provide situational awareness of the cybersecurity posture of control and sensor networks. The suite of technologies produced by this project will provide the following complementary capabilities:

- **Sophia Tool**: Provides users with a thorough view of communications between control system components connected via traditional IT networks and alerts upon deviations from whitelisted communication paths
- **Mesh Mapper Tool:** Collects and tracks message routing of wireless mesh network data to provide operations with indications of abnormal behavior within wireless sensor networks
- **Intelligent Cyber Sensor:** Distinguishes between component failure and cybersecurity incidents, and monitors the overall health of a system
- **Data Fusion System:** Identifies, reduces and characterizes data, providing integrated situational awareness of the cyber and operational health of control and sensor systems
- **Network Access Policy Tool:** Developed by the TCIPG program, this tool provides detailed network information in support of firewall rule generation. It will be integrated with the Situational Awareness tool suite

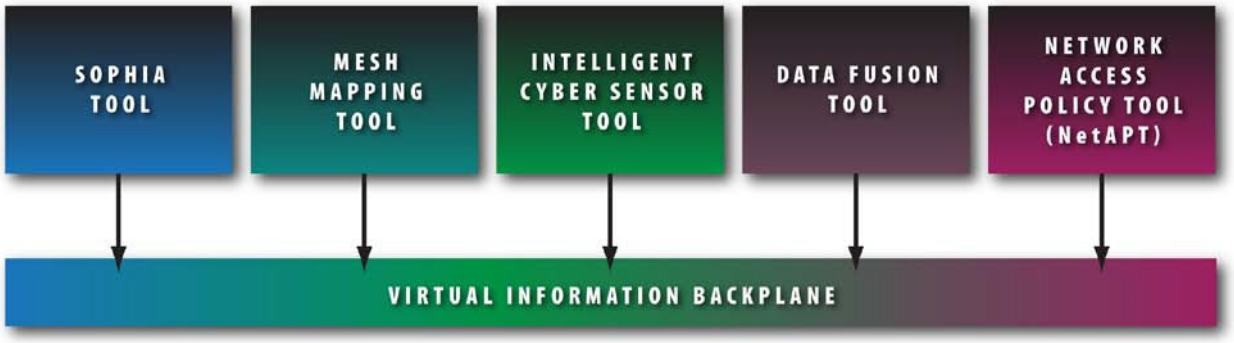
Benefits

- Shows network communications
- Collects wireless mesh network data message routes
- Reports unexpected behavior
- Monitors system health
- Distinguishes between component failure and cybersecurity issues
- Performs data fusion
- Determines global effects for local firewall rules

Partners

- Idaho National Laboratory
- Idaho Falls Power
- Austin Energy
- Argonne National Laboratory
- The University of Illinois at Urbana-Champaign
- Oak Ridge National Laboratory
- The University of Idaho

Situational Awareness Tool Suite



Technical Objectives

Each technology in the tool set will be developed to at least a proof-of-concept prototype and integrated for a final demonstration of its individual functionality and collective interoperability.

End Results

Project results will include:

- An interoperable set of tools that can be implemented either individually or collectively to help safeguard critical infrastructure assets
- Aid in developing a more comprehensive and consistent implementation of cybersecurity and provide situational awareness of the cybersecurity posture of control and sensor networks

Content last updated: August 2012

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

Dave Kuipers
National SCADA Test Bed
Program Manager
Idaho National Laboratory
208-526-4038
david.kuipers@inl.gov

Current Contact as of Aug. 2020

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