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

Survivable Industrial Control Systems

Sandia National Laboratories

A resilient, proactive industrial control system solution that correlates aggregated cyber-physical events

Industrial control systems (ICS) are often statically configured over long periods of time and have predictable communication patterns. The static and highly predictable nature of these systems creates an environment in which an adversary is well positioned to plan, craft, and launch new attacks. System operators must be ready to react to new threats, but are often only able to mitigate threats after post-forensic analysis. As these threats continue to evolve, the security protections must become more proactive to be effective. This project automatically and proactively detects and responds to both cyber- and physical-based threats by advancing and building upon the host-based event monitoring capabilities developed and optimized during the Cyber-Physical Modeling and Simulation for Situational Awareness (CYMSA) project and the Artificial Diversity and Defense Security (ADDSec) project, which provides the ability to monitor both host- and network-based events. Enhancements to both projects include introducing distributed controllers, optimizing moving target defense parameters, and correlating events observed from software-defined networking flows with data from the deployed CYMSA field sensors.

KEY TAKEAWAYS

- Provides a resilient and interoperable software-defined networking solution to improve availability of industrial control systems
- Enables survivable industrial control systems use in energy and the oil and natural gas sectors

OUTCOME

This project combines the capabilities of CYMSA's physical and cyber detection agents with the ADDSec proactive detection and response framework. The CYMSA events detected in real time are provided as inputs into the ADDSec detection module where new mitigating responses are developed. Both projects are enhanced and integrated into a single tool that supports next generation environments, such as software-defined networking (SDN) deployments.

PARTICIPANTS	ROLE
Sandia National Laboratories	Project lead; performs research and development (R&D) to incorporate cyber-physical-based threats to the ADDSec project
Chevron	Provides R&D guidance so that these technologies can be applied to the oil and natural gas sector
Georgia Tech Research Institute	Expands the CYMSA tool so microgrid environments can be monitored and enables the ADDSec technology to rapidly respond to detected alerts
GRIMM	Provides an independent third-party cybersecurity red team assessment
Pacific Northwest NATIONAL LABORATORY	Distributes the SDN controller on which the ADDSec technology is built to improve security and performance of SDN networks deployed within energy delivery systems
SEL SCHWEITZER ENGINEERING LABORATORIES	Provides a commercial SDN switch that is compatible with the ADDSec and CYMSA tools so that correlations between SDN metrics and control system data can be used to detect cyber threats

CONTACT INFORMATION

Initial Leads:

Carol Hawk
Program Manager

Adrian Chavez
Principal Investigator
Sandia National Laboratories
505-284-6664
adrchav@sandia.gov

Current Contact as of February 2020:

Akhlesh Kaushiva
Senior Technical Systems and Cybersecurity Advisor
Department of Energy (DOE)
Office of Cybersecurity, Energy Security, and Emergency Response (CESER)
202-287-6062
Akhlesh.Kaushiva@hq.doe.gov

Period of Performance: May 2018 – October 2021

Total Award Value: $800,000
DOE Share: $800,000
Cost Share: $0

CYBERSECURITY FOR ENERGY DELIVERY SYSTEMS (CEDS)

CEDS projects are funded through DOE CESER, which aims to enhance the reliability and resilience of the nation's energy infrastructure by reducing the risk of energy disruptions due to cyberattacks.

Website: https://www.energy.gov/ceser

Date Written: June 2021