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

Visually Explainable and Actionable Alert System in SCADA Networks

CREDC
CYBER RESILIENT ENERGY DELIVERY CONSORTIUM

Analyzing and visualizing the large volume, velocity, veracity, and variety of alerts on industrial control networks in real time

Supervisory control and data acquisition (SCADA) networks for industrial control systems generate a large amount of diverse data at high velocities. Implementing policies to handle security alerts at the transport, operational, or content levels individually can overwhelm control centers. System operators could struggle to explain or act upon these alerts. This project develops an explainable and actionable alert system that allows operators to efficiently and effectively respond to anomalous SCADA system events. The system aggregates anomalous data into multi-level meta-alerts, which are categorized and assigned confidence coefficients to determine how and in what order meta-alerts are sent to SCADA control system operators, ranked by urgency. The highest ranked alerts are sent to the control center where causal reasoning analysis and real-time visualization tools assist the operators to explain the meta-alerts and suggest actions to remediate.

KEY TAKEAWAYS

- Aggregates anomalous control system data into multi-level, actionable, and visualized meta-alerts
- Contextualizes automatically generated meta-alerts to determine their cause and propose rapid mitigation plans
- Ranks meta-alerts by order of urgency to ensure operators respond to the most critical situations first

OUTCOME

This project delivers a network-agnostic and visually strengthened alert system that can be plugged into the control center of any SCADA system for rapid identification and response to anomalous behavior. The system minimizes the need for human-led forensic analysis before determining rapid response mitigation plans.

PARTICIPANTS	ROLE
CREDC CYBER RESILIENT ENERGY DELIVERY CONSORTIUM	The CREDC performs multidisciplinary research and development that focuses on the cybersecurity of energy delivery systems. The central project goal is to create an ecosystem where research results lead directly to the development of applications and methodologies, which are then validated in realistic contexts.
UNIVERSITY OF ILLINOIS URBANA-CHAMPAIGN	Leads research, development, and testing
NREL NATIONAL RENEWABLE ENERGY LABORATORY	Tests the system in their visualization testbed

CONTACT INFORMATION

Initial Leads:

Klara Nahrstedt
Professor
University of Illinois
217-244-6624
klara@illinois.edu

Shane McFly
Cybersecurity Research Scientist
National Renewable Energy Laboratory
303-384-6539
Shane.McFly@nrel.gov

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

This is a subproject sponsored by the CREDC academic consortium, led by the University of Illinois.

CREDC Period of Performance: October 2015 – May 2022

CREDC Total Award Value: $28,099,258
DOE Share: $22,476,290
Cost Share: $5,622,968

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