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

Secure Cloud SCADA for Energy Delivery Systems

CREDC
CYBER RESILIENT ENERGY DELIVERY CONSORTIUM

Securing and advancing SCADA control systems with the near-limitless potential of the cloud

Supervisory control and data acquisition (SCADA) systems monitor and control electric transmission by communicating with on-site field remote telemetry units (RTUs) that report details of the local system state back to a master. RTUs are often legacy devices with limited computational capacity, causing time-criticality and latency issues in SCADA frameworks. Cloud-based SCADA theoretically eliminates these constraints and enables advanced analytics for security and operational applications within energy delivery systems (EDS). This project builds on an existing micro-service cloud model that engages cloud-based processing components to securely obtain, curate, and archive measurements from cyber-physical systems and analyze them to develop lightweight workflows across the SCADA framework.

KEY TAKEAWAYS

- Develops and demonstrates new edge-to-cloud architecture variants for supervisory control and data acquisition
- Leverages an existing micro-service cloud model to advance supervisory control and data acquisition processes, system controls, and security
- Detects possible network attacks and determines intelligent responses using machine learning and other cutting-edge technology

OUTCOME

This project operationalizes cloud-based SCADA systems to detect physically inconsistent system states, which may indicate an attack on measurements, and uses this information to conduct simulations evaluating the impact of control commands before execution. This allows EDS operators to develop more robust architectures and networks without exceeding the built-in computational capacity of system components.

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
OSIsoft.	Engages stakeholders
DUKE ENERGY®	Engages utility stakeholders

CONTACT INFORMATION

Initial Leads:

Carol Hawk
Program Manager

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

Alfonso Valdes
Principal Research Scientist
Information Trust Institute
University of Illinois
217-244-5147
avaldes@illinois.edu

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

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