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

# Secure Supervisory Control and Data Acquisition Protocol Characterization and Standardization

Lawrence Livermore National Laboratory

*Protecting energy delivery systems using the secure supervisory control and data acquisition protocol for the 21st century*

Modeling and simulation are useful tools for analyzing cybersecurity in energy delivery systems but require the ability to simulate both network and physical processes. Multiple test models exist for physical process simulations but the availability of network models for operational technology environments is very limited — manually building a model in a simulation environment is a burdensome and lengthy task. This project develops and tests a capability to facilitate the automatic generation of models in a network simulator using passively captured network data. This capability generates a high-fidelity digital representation of the network that can be coupled with the physical process model to create a digital twin of the whole system. This enables a tailored analysis of the cybersecurity posture that reduces the impact of potential cyberattacks and allows network operators to assess the effectiveness of various mitigation strategies that could be deployed in the system.

## KEY TAKEAWAYS

- Creates realistic and high-fidelity models of supervisory control and data acquisition networks to evaluate protocols using data collected from network scanning tools
- Reduces cost for network model generation among multiple CEDS projects

## OUTCOME

This project develops the ability to create state-of-the-art high-fidelity network models that will benefit current and future CEDS objectives. It enables tailored analysis of cyber scenarios using digital twins.

| PARTICIPANTS | ROLE |
|---|---|
| Lawrence Livermore National Laboratory | Performs protocol characterization using virtual SCADA networks modeled on digital twins of live data |

## CONTACT INFORMATION


**Initial Leads:**

**Carol Hawk**
Program Manager

**Domingo Colon**
Principal Investigator
Lawrence Livermore National Laboratory
925-422-7892
colon3@llnl.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:** October 2017 – December 2020

**Total Award Value: $1,300,000**
DOE Share: $1,300,000
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