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

CYVET: A Cyber-Physical Security Assurance Framework Based on a Semi-Supervised Vetting Approach

OAK RIDGE National Laboratory

Addressing verification and validation of operational technology

The project team is developing and delivering a cybersecurity verification and validation framework for testing operational technology (OT) equipment, software, and the underlying control system architecture. The application of cybersecurity best practices within OT environments is a relatively novel concept, with significant disconnects between unsecured network architectures, vendor-supplied built-in device security enhancements, and network operator awareness. The CYVET tool applies a framework that is designed to comprehensively address these disparities by vetting vendor claims and customer requirements against proven device capabilities. This project verifies and validates the compliance of OT devices and vendor supplied features with recognized security standards. Additionally, CYVET demonstrates the application of new technologies at end-user facility in the energy sector.

KEY TAKEAWAYS

- Addresses a critical gap in the energy sector's verification and validation capabilities during infrastructure improvement, equipment procurement, and compliance certification processes
- Establishes a standardized cybersecurity rating system for energy infrastructure components
- Enables system designers to validate the security of hardware and software components they plan on installing in critical energy systems

OUTCOME

CYVET operationalizes a cybersecurity rating system similar to the Energy Star energy efficiency rating system. It enables system designers to evaluate cybersecurity claims from vendors before incorporating components into their system design. This allows OT users to both guarantee the security of system elements and take better advantage of their equipment's built-in security features by establishing a more comprehensive understanding of the underlying technology.

PARTICIPANTS	ROLE
Oak Ridge National Laboratory	Project lead; research and development, coordination, and delivery of the technical solutions
University of Nebraska-Lincoln	Subcontractor; contributes algorithms, software, and hardware advancements in cyber-physical security
National Strategic Research Institute at the University of Nebraska	Technological transfer partner; facilitates or enables commercialization of findings, results, and prototypes
NUtech Ventures	Commercialization liaison to the power industry
OPPD Omaha Public Power District	Stakeholder advisor and potential future adopter
Nebraska Public Power District	Stakeholder advisor and potential test site for demonstration
LES Lincoln Electric System	Stakeholder advisor and potential future adopter
South Sioux City	Stakeholder advisor in renewal energy and state-of-the-art equipment deployments

CONTACT INFORMATION

Initial Leads:

Carol Hawk
Program Manager

Juan Lopez Jr.
Principal Investigator
Oak Ridge National Laboratory
865-576-5752
lopezj@ornl.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: September 2019 – October 2022

Total Award Value: $3,441,316
DOE Share: $2,986,801
Cost Share: $454,515

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