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

Operational Technology Network Best Practices Language and Library

CREDC
CYBER RESILIENT ENERGY DELIVERY CONSORTIUM

Codifying best practices for resilient operational technology and automated system analysis

This project and development initiative designs and implements a non-proprietary specification for best practices for operational technology (OT) networks that is suitable for machine automation. There currently is no formalized language for encoding best practices such as network segmentation, protocol translation and separation, and access control rules, making it difficult to automate adherence to universal standards. The research team is developing and extensively documenting an open-source library of OT best practice rules in standardized language. The language and library make it possible to analyze OT networks against a selected set of best practice rules to identify which rules the network complies with or fails to follow. The team will embed the library into a testbed platform, develop a user-friendly interface, and validate the language and library.

KEY TAKEAWAYS

- Develops a universal library of best practices for enhancing the resilience of operational technology
- Creates standardized language to support machine-automated analysis of policy adherence
- Enables network operators to effectively manage inter-meshed policies across complex infrastructures

OUTCOME

This project delivers the first non-proprietary language and library for the secure and resilient implementation and automated analysis of OT across the energy sector. The developed product minimizes the technical and financial barriers facing OT network operators to adhere to industry standard best practices, such as those developed by the National Institute of Standards and Technology.

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	Lead institution. Researches, develops, and documents OT best practices; creates language and library for automated system analysis
np network perception	Provides technical support; contributes customer feedback to the development of the library; and identifies potential customers for testing and evaluation

CONTACT INFORMATION

Initial Leads:

David M Nicol
CREDC Principal Investigator
Director, Information Trust Institute
217-244-1925
dmnicol@illinois.edu

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