

Implementation of Resilience via Operational Controls



CREDC
CYBER RESILIENT ENERGY
DELIVERY CONSORTIUM

*Sophisticated
critical
infrastructure
controls for built in
resiliency*

Resilience is a key element in maintaining security of critical infrastructures. To achieve resiliency in a system requires specific elements in system design and operation. This project examines how security operational controls can be adapted to enable greater system resiliency. Developing the correct set of operational controls that facilitate both security and resiliency will enable energy companies to improve resiliency through normal operational elements. This project examines a set of operational controls that are commonly employed in IT systems to determine how they can contribute to resiliency.

KEY TAKEAWAYS

- Examines how standard operational controls can be used to maximize system resiliency
- Recommends resilient information technology control structures to enhance energy delivery system security
- Bolsters critical infrastructure data security through enhanced operator control, safety, and uptime for operational technologies

OUTCOME

This research provides the energy sector with the information needed to enhance cybersecurity programming through intelligent applications of operational technology. This will build resiliency directly into critical infrastructure, minimizing additional costs and efforts associated with adding cybersecurity elements on top of energy delivery system architectures.

PARTICIPANTS

ROLE



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.



Leads research, development, and testing



Engages oil and gas sector stakeholders

CONTACT INFORMATION

Initial Leads:

Carol Hawk
Program Manager

William Arthur Conklin
Site Lead, Associate Professor
University of Houston
713-743-1556
waconklin@uh.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