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

# Cyber Resilient Metrics for Bulk Power Systems

CREDC
CYBER RESILIENT ENERGY DELIVERY CONSORTIUM

*Quantifying system resilient for fast and effective risk identification and mitigation*

The North American bulk power system (BPS) is made up of a complex network of cyber-physical interconnections. This infrastructure facilitates long-distance power transmission, but also presents an attractive surface for cyber-attacks. To understand and quantify the security posture of energy delivery systems (EDS), the project team is developing critical cyber resilience metrics for comprehensive risk assessment and mitigation programs. The researchers are working with ReliabilityFirst to model and identify BPS design parameters – such as firewall rules, network paths, node recovery time, backup resources available – and quantify resilience levels across four critical areas of system security: robustness, redundancy, resourcefulness, and rapidity. These cyber resilience metrics will deliver EDS operators highly detailed insights into the ability of security controls to ensure operational resilience within unique network topologies, identify potential vulnerabilities, and help develop cost-effective mitigation plans.

## KEY TAKEAWAYS

- Analyzes bulk power systems across complex cyber-physical topologies to prioritize corrective actions for system configurations to mitigate risks and maximize resilience
- Simplifies bulk power system assessment processes to encourage more frequent risk analysis and mitigation
- Demonstrates and validates the self-assessment tool for the sector in collaboration with ReliabilityFirst, one of the eight FERC regional entities ensuring power system reliability

## OUTCOME

This research provides cyber resilience metrics capable of facilitating effective risk management decision making in BPS. This creates the capacity for asset owners to prioritize corrective actions through identification of resilient system configurations, critical vulnerabilities, and cost-effective security controls.

| 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. |
| OLD DOMINION UNIVERSITY | Lead institution; develops resilience metrics and methodology for creating attack graphs against which resiliency is assessed. Develops prototype tool for use by industry partner. |
| UNIVERSITY OF ILLINOIS URBANA-CHAMPAIGN | Partner institution; provides modeling methodologies in support of Old Dominion University tool development. |
| RELIABILITYFIRST | Industry partner for demonstration, validation, and sector outreach. |

## CONTACT INFORMATION


**Initial Leads:**

**Carol Hawk**
Program Manager

**Sachin Shetty**
Site Lead, Associate Professor
Old Dominion University
757-686-6233
sshetty@odu.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