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

A Conceptual Framework for the Assessment of Integrated Energy Storage Resources

CREDC
CYBER RESILIENT ENERGY DELIVERY CONSORTIUM

Preparing for the secure introduction of renewable energy source within smart grid infrastructures

This project develops an analytic framework for the economic, environmental, and security assessment of power systems with integrated renewable energy storage resources (ESR). As smart grid systems become increasingly able to accommodate renewable energy sources, new security requirements will be needed to ensure resilient integrations of ESRs into pre-existing infrastructures. The research team's investigation assesses the nature and scope of the information transmitted through the computer/control/information (CCI) layer of smart grid networks, and identifies and analyzes the security threats that must be addressed to enable the successful implementation of ESRs to bring about smart grid energy delivery system (EDS) resiliency. The integration of ESRs into the power system requires smart grid CCI layer implementation for the effective utilization of these resources. This work addresses specific issues related to performance, robustness, communication, economics, and security to fully realize the benefits that ESRs provide and ensure their effective utilization.

KEY TAKEAWAYS

- Identifies pathways to securing energy storage resources for power systems with integrated renewable energy inputs
- Analyzes the integration of energy storage resources with specific consideration to information layer communication in smart grid infrastructures
- Evaluates robustness and survivability of new platforms and systems

OUTCOME

This research identifies secure protocols for smart grid infrastructures based on varying and interoperable implementations of integrated ESRs, providing the electric grid with the resiliency needed to be better equipped to handle deeper penetrations of integrated ESRs.

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.
ILLINOIS	Leads research, development, and testing

CONTACT INFORMATION

Initial Leads:

Carol Hawk
Program Manager

George Gross
Professor
University of Illinois
217-244-6346
gross@illinois.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