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

Metrics and Tools for Measuring Cyber Resiliency of Electrical Grids

CREDC
CYBER RESILIENT ENERGY DELIVERY CONSORTIUM

Advancing tools for measuring and improving electric grid cybersecurity

This research identifies and validates metrics and tools for quantifying the cyber resilience of power grid systems against targeted attacks. The research team is taking a multi-step approach to measuring the level of security across microgrids, distribution systems, and large-scale electric transmission systems. In developing the resiliency metrics, the team extends and combines common impact metrics from both the cyber domain and the power domain to address resiliency at the device and system levels. The project establishes quantifiable resiliency metrics and develop tools to analyze cyber vulnerabilities. These tools will have long-term applications for measuring incremental security improvements brought about by techniques such as reconfiguration, redundancy, partitioning, non-persistence, and automated response.

KEY TAKEAWAYS

- Develops metrics for quantifying device and system resiliency to cyberattacks
- Introduces tools to system operators to analyze and improve network security
- Addresses devices in microgrid, distribution, and transmission infrastructures not covered by programmable logic controller standards

OUTCOME

Energy delivery system operators may use the tools developed to enumerate general security and attackability scores for individual network components and prioritize necessary security upgrades. Additionally, they are also able to use these tools to predict the level of impact potential exploits will have on cyber-physical systems to ensure necessary preventative measures are taken.

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.
RUTGERS	Lead institution; develops models of component-level trust and resiliency suitable for measurement and inclusion in a tool: develops a Trusted Safety Verifier tool for programmable logic controllers and intelligent electronic devices.
WASHINGTON STATE UNIVERSITY	Partner institution; develops system level resiliency tools: Cyber-Physical Security Assessment Metric for distribution systems, Cyber-Physical Transmission Resiliency Assessment Metric for transmission systems, and CyPhyR for analyzing microgrid resiliency.
SIEMENS	Industry collaborator

CONTACT INFORMATION

Initial Leads:

Carol Hawk
Program Manager

Saman Zonouz
Rutgers Site Lead, Assistant Professor
Rutgers University
848-445-8508
saman.zonouz@rutgers.edu

Adam Hahn
Site Lead, Assistant Professor
Washington State University
509-335-2343
ahahn@eec.wsu.edu

Anurag Srivastava
Associate Professor
Washington State University
509-335-2348
asrivast@eecs.wsu.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