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

Cybersecure Interconnection of Distributed Energy Resources

Lawrence Livermore National Laboratory

Securing the integration and application of distributed energy resources across the power grid

The expanding presence of distributed energy resources (DERs) across the power grid increases the risks of cyberattack against power distribution infrastructures. Utilities depend on specialized analytical tools to ensure the secure and reliable integration of DERs within the power grid. It is critical that these tools continue to advance in parallel with the increasingly large and complex network of DERs currently in use across the United States. This project researches, develops, and demonstrates a co-simulation tool that evaluates the multi-faceted cybersecurity risk of various DER integration schemes with the distribution system. This allows utility operators to analyze risks across communications and control pathways and design mitigation strategies for cyberattacks that exploit the high penetration of DERs to disrupt power systems.

KEY TAKEAWAYS

- Provides proactive, accurate, and defensible strategies for the cybersecure integration of distributed energy resources
- Enables rapid simulation without increased cost or time to interconnect at the utility and customer levels
- Couples power engineering and cybersecurity expertise to analyze impacts of potential cyberattacks against distributed energy resources and their control/communication systems on the power grid

OUTCOME

This tool enhances the resilience of energy delivery systems through proactively addressing the threat introduced by highly dispersed controllable DERs. This not only validates methods for the resilient implementation of DERs, but enables rapid and secure implementation of new DERs across the power grid.

PARTICIPANTS	ROLE
Lawrence Livermore National Laboratory	Develops DER cybersecurity analysis co-simulation tool modeling DERs, power grid equipment, and their communication and control systems.
REVOLUTIONARY SECURITY	Uses operational technology cybersecurity expertise to develop DER cybersecurity scenarios and effective mitigation strategies.
WATER | ENERGY | LIFE CITY OF RIVERSIDE PUBLIC UTILITIES	Advises on DER operation and cybersecurity as a utility and provides distribution grid and DER models.
smarter grid solutions	Provides DER Management Systems and control/communication architecture for modeling within a co-simulation tool.

CONTACT INFORMATION

Initial Leads:

Carol Hawk
Program Manager

Jhi-Young Joo
Principal Investigator
Lawrence Livermore National Laboratory
925-422-0074
joo3@llnl.gov

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

Period of Performance: July 2018 – September 2020

Total Award Value: $2,000,000
DOE Share: $2,000,000
Cost Share: $0

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