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

Supervisory Parameter Adjustment for Distribution Energy Storage

BERKELEY LAB

Automatic system reconfiguration to counteract cyberattacks

This project is developing the methodology and open-source tools that allow energy storage systems (ESS) to automatically reconfigure themselves to counteract cyberattacks both directly against ESS control systems and indirectly through the electric distribution grid. The team is analyzing the stability of ESS control systems and their interactions with the electric grid to determine what parameters an attacker would change if a given device were to be compromised. The team is using this information to develop a supervisory control framework driven by reinforcement learning that allows ESS devices to autonomously adapt in order to defend against a variety of cyberattacks. The framework also enables ESS devices to proactively identify potential instabilities in system components to enhance security. This project ensures that ESS devices maintain their own internal stability and mitigate instabilities in electrical grids caused by other components that have been compromised due to a cyberattack.

KEY TAKEAWAYS

- Develops a methodology and tools to protect energy storage systems in the event of a cyberattack
- Improves the security and robustness of energy storage system controls and device connections with the electric grid
- Delivers open-source solutions for broad implementation and customization across a variety of energy storage system infrastructures

OUTCOME

The team delivers tools to identify the components of the ESS control system that have been compromised during a cyberattack as well as policies for changing the control parameters of ESS to mitigate a wide variety of cyberattacks on both the ESS device itself and the electric distribution grid. The tools include simulation capabilities allowing utilities to study the performance of the developed algorithms on a network specific basis. By making these tools open source, vendors may customize the underlying algorithms to their specific ESS infrastructure and embed the developed control systems locally on ESS devices.

PARTICIPANTS	ROLE
BERKELEY LAB	Develops reinforcement learning and adaptive control algorithms for ESS device management
NRECA America's Electric Cooperatives	Integrates defensive algorithms into open source grid simulation tool (Open Modeling Framework)
ASU Arizona State University	Leverages expertise in electric grid optimization for algorithm development
SIEMENS	Red-team member; validates proper operation of supervisory control algorithms

CONTACT INFORMATION

Initial Leads:

Carol Hawk
Program Manager

Daniel Arnold
Co-Principal Investigator
Lawrence Berkeley National Lab
510-486-5564
dbarnold@llbl.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: September 2019 – December 2022

Total Award Value: $3,000,000
DOE Share: $3,000,000
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