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

Energy Storage Security Using Microservices (ESSec)

Sandia National Laboratories

Using containers to protect energy storage systems

This project designs a secure and interoperable containerized suite of applications to protect energy storage system control software against cyber threats and attacks. Application containerization and orchestration enable the ability to upgrade software in real time, quickly launch new applications, detect compromised or crashed applications, and manage applications within a variety of energy storage systems without service disruption or downtime. The research team is developing live upgrade and mitigation services for utilities deploying microservices and using the common Open Field Message Bus protocol for the battery management system. This project validates emerging containerization services with open source software packages for energy storage systems, and will expand out to microservice architecture.

KEY TAKEAWAYS

- Reduces the attack surface by isolating processes within their own containerized operating system
- Identifies and replaces processes and applications that have been compromised with malware without disrupting operations
- Expands the potential for microservice interoperability across energy storage infrastructure

OUTCOME

This project protects energy delivery systems by widely deploying containerized environments so that even if an application is compromised, the adversaries cannot move beyond the container in which it is trapped. The project detects the intrusion, identifies the exploited application, isolates and patches that application, and then re-launches the patched application—all without interrupting system availability. This technology will be compatible with existing commercially available applications, ensuring the ability to directly integrate into industrial control system vendor products.

PARTICIPANTS	ROLE
Sandia National Laboratories	Project lead; performs research and development (R&D) to containerize and orchestrate energy storage systems for deployment across multiple utility sites
DUKE ENERGY®	Provides R&D guidance and a testbed with an EDS for ESSec technology deployment
Entergy	Provides R&D guidance and a testbed with an EDS for ESSec technology deployment
DTE	Provides R&D guidance and a testbed with an EDS for ESSec technology deployment
OPEN ENERGY SOLUTIONS INC	Provides R&D guidance and support to integrate the ESSec technologies into utility partner sites
SEL SCHWEITZER ENGINEERING LABORATORIES	Provides a commercial product capable of harnessing ESSec containerization and orchestration technologies to manage and deploy EDS software
GRIMM	Provides an independent third-party cybersecurity red team assessment of ESSec technologies

CONTACT INFORMATION

Initial Leads:

Carol Hawk
Program Manager

Adrian Chavez
Principal Investigator
Sandia National Laboratories
505-284-6664
adrchav@sandia.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: February 2020 – January 2023

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