U.S. DEPARTMENT OF
ENERGY

Office of
Cybersecurity, Energy Security,
and Emergency Response

ADDSec: Artificial Diversity and Defense Security

Sandia
National
Laboratories

Using software-defined networks to enhance situational awareness in energy delivery systems

Artificial Diversity and Defense Security (ADDSec) leverages software-defined networking to introduce randomness into control system networks and extend solutions from the local network area to the wide area network. ADDSec is comprised of three main components: Automatic Reconfigurable Network Settings (ARN), Randomizing Application Instructions Sets (RAIS), and Machine-based Dynamic Defense (MDD). ARN manages network configurations, securely communicates reconfiguration specifications, and ensures uninterrupted connectivity between nodes. RAIS randomizes the instruction sets that execute programs on end devices, providing protection against code injection attacks, buffer overruns, and reverse engineering of software. MDD dynamically defends against active attacks by recognizing patterns, providing situational awareness, and taking appropriate actions. The project consists of research, development, and demonstration activities to build a vetted, open-source solution that incorporates a secure, scalable, resilient communications framework; enhanced security for energy sector protocols; and a framework for computation to support advanced situational awareness and analysis. Commercialization efforts will occur alongside development activities.

KEY TAKEAWAYS

- Proactively classifies and mitigates threats at both the host and network levels of a control system as they are detected
- Brings moving-target capability to wide area networks in the energy sector
- Scales to large networks while avoiding implementation and design errors

OUTCOME

ADDSec delivers a resilient and secure communications mechanism to support modern grid operations. It improves the security posture for utility infrastructure by enhancing security of both known and unknown protocols and by extending security protection through internal perimeter protections for utility infrastructure. ADDSec is an extensible platform that enables future computation, data analytics, and enhanced situational awareness. It is built with open-source tools that are interoperable with commercially available products and can be retrofitted into existing systems already in operation.

PARTICIPANTS	ROLE
Sandia National Laboratories	Project lead; develops machine learning algorithms and moving target defense strategies
Lawrence Livermore National Laboratory	Incorporates Network Mapping System (NeMS) to provide situational awareness to network administrators
FORT BELVOIR LEADERS IN EXCELLENCE	Provides a representative microgrid environment to deploy and test ADDSec technologies
Chevron	Offers technical guidance so that the ADDSec technologies can be integrated within Oil & Natural Gas systems
GRIMM	Conducts independent 3rd party red team assessment to provide cyber security evaluation and guidance of the ADDSec technologies
SEL SCHWEITZER ENGINEERING LABORATORIES	Vendor partner with a commercial product that is compatible with the ADDSec technologies

CONTACT INFORMATION

Initial Leads:

Carol Hawk
Program Manager

Adrian Chavez
Principal Investigator
Sandia National Laboratory
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: October 2014 – December 2021

Total Award Value: $2,998,364
DOE Share: $2,998,364
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: September 2021