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

Resilient Energy Delivery and Control Systems (REDCS)

GE Global Research

Efficient and reliable anomaly detection for natural gas pipeline security

The Resilient Energy Delivery and Control Systems (REDCS) project leverages advancements in machine learning and controls theory to provide anomaly monitoring and prediction, attack isolation, and operational resiliency specifically for natural gas pipelines. REDCS conducts vulnerability assessments to determine critical pipeline segments; predicts, detects, and isolates cyberattacks with a false positive rate below 2%; introduces self-healing mechanisms for increased resiliency; and secures pipeline sensor communications. It delivers advanced modeling to expand system state awareness for utility owners and operators and is scalable across many different pipeline segments and configurations. REDCS' algorithms can also be applied to other energy delivery assets.

KEY TAKEAWAYS

- Predicts, detects, and isolates cyberattacks against natural gas pipeline components with more than 98% accuracy
- Facilitates the self-healing of attacked assets
- Secures critical sensor input/output communications across natural gas infrastructures

OUTCOME

REDCS' behavior-based anomaly detection and isolation algorithms are twice as accurate as, and 10 times faster than, conventional fault detection systems. It is also cost-effective for utility operators, streamlining to a single-day training and deployment process.

PARTICIPANTS	ROLE
GE Global Research	Conducts REDCS algorithm development, builds REDCS prototypes and secures critical system communications
Baker Hughes	Provides natural gas pipeline operational and cybersecurity knowledge, digital twins, potential path to commercialization, and the installation and decommissioning of the REDCS system in Phase 2
FLORIDA STATE	Builds a new cyber-attack generation system to identify attack types, increasing the overall detection accuracy of the REDCS system
intel	Conducts red team assessment of the prototype and helps identify cybersecurity vulnerabilities

CONTACT INFORMATION

Initial Leads:

Matthew Nielsen
Principal Investigator
GE Research
518-387-4233
nielsema@ge.com

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: August 2020 – August 2023

Total Award Value: $5,212,428
DOE Share: $2,999,916
Cost Share: $2,212,512

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