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

Cyber-Physical Protection for Natural Gas Compression

GE Global Research

Making natural gas compression stations more secure

One of the most important components of the natural gas (NG) distribution network is the compressor station. Located along a NG pipeline, these stations compress gas to a specified pressure to allow it to continue traveling along the pipeline to its destination. There are about 1,400 compressor stations along NG transmission pipelines in the U.S. that are critical to energy transport. This project develops a cyber-physical protection (CPP) system that minimizes damage to, and increases the resiliency of, NG pipeline compressor systems using advanced machine learning and control algorithms. Located at the asset and attached to the operational technology network, the CPP system monitors asset behavior to detect the presence of attacks, locates the point of the attack, neutralizes the attack, and forecasts emerging security issues or hard-to-detect stealthy attacks. The CPP system limits damage and provides resiliency to NG assets by monitoring critical nodes in the compressor system to quickly detect and alert operators to anomalies caused by cyberattacks. This project leverages machine learning to increase asset availability during cyberattacks.

KEY TAKEAWAYS

- Enables natural gas compressor stations to self-defend by advancing machine learning and control algorithms for cyber-physical models that monitor key nodes, detect anomalies, and neutralize cyberattacks
- Protects assets from damage and maintains system availability during cyberattacks
- Operationalizes a plug-and-play security tool for the oil and natural gas sector

OUTCOME

This CPP system enhances the resiliency and self-defense capabilities of critical NG compressor assets. The system benefits operators of NG compressors by providing a new layer of cyber-physical protection that limits damage to the asset by monitoring key nodes to detect anomalies and provides resiliency through its neutralization capabilities, increasing overall system availability in the presence of cyberattacks. The developed plug-and-play system is compatible with industrial communications protocols and can be easily installed across existing operational technology networks.

PARTICIPANTS	ROLE
GE Global Research	Conducts CPP algorithm development and secures system data
Baker Hughes	Provides compressor station cybersecurity knowledge, digital twins, potential path to commercialization, and the installation and decommissioning of the CPP system
INL Idaho National Laboratory	Conducts red team assessment of the prototype

CONTACT INFORMATION

Initial Leads:

Carol Hawk
Program Manager

Matthew Nielsen
Principal Investigator
GE Global Research
518-387-4233
matthew.nielsen@ge.com

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 2018 – December 2021

Total Award Value: $3,890,126
DOE Share: $2,906,693
Cost Share: $983,433

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