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

# Cyber-Physical Resilience for Wind Power Generation

GE Global Research

*Applies cyberattack detection and accommodation to wind farms*

Wind power is expected to add more generation capacity to the national electric grid than any other energy resource. However, the information and operational technologies of wind turbines remain vulnerable to cyberattacks. This project develops new and adaptive defense technologies that enable wind power generation systems to survive sophisticated cyberattacks by enhancing the control system's detection, localization, and accommodation capabilities. This technology specifically addresses control system attacks that introduce unwanted, damaging, or disruptive modifications to sensing, command, and operational signals that prevent or impede normal power generation. The team will deliver field-tested and commercially viable autonomous anomaly detection and accommodation algorithms for wind power generation systems that are effective against attacks at the physical layer of the system. The project combines machine learning with physics-based models to detect, locate, and mitigate cyberattacks.

## KEY TAKEAWAYS

- Uses physical models and machine learning to detect, localize, and accommodate for cyberattacks against wind turbines
- Provides an active defense against spoofing by physically watermarking communications
- Achieves cross-fleet and cross-site scalability through deep reinforcement and transfer learning

## OUTCOME

The technology developed by this project accommodates and responds to attacks by operationalizing a novel systematic classification and risk prioritization structure for wind generation. Project analytics will be used to simulate and certify cybersecurity program designs prior to implementation. The commercial product guarantees false positive and false negative attack detection and localization at a rate of less than 1% and autonomously neutralizes more than 50% of attacks. This means the system can still generate electricity, even during active attack scenarios, overcoming the challenges of the intermittent nature of wind generation that can mask cyberattacks.

| PARTICIPANTS | ROLE |
|---|---|
| GE Global Research | Develops algorithms to prevent and detect attacks that leverage the physical nature of the control system devices |
| GE Renewable Energy | Uses detailed knowledge about wind farms and their vulnerabilities to provide foundational information about attack surfaces for wind energy applications |
| INL Idaho National Laboratory | Performs system testing for validation and verification |

## CONTACT INFORMATION


**Initial Leads:**

**Carol Hawk**
Program Manager

**Fernando D'Amato**
Principal Investigator
GE Global Research
518-387-7311
damato@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 – May 2022

**Total Award Value: $4,776,089**
DOE Share: $3,578,171
Cost Share: $1,197,918


**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