Objective

Develop commercially viable cyber protection technology for wind power generation systems that is effective against attacks at the control domain in the physical layer.

Schedule

- **Project dates:** Start: 10/01/18 -- End: 3/31/22*

Milestones

- Baseline Detection technology: 12/19
- Advanced Det. & Localization: 6/20
- Product requirements and strategy: 9/20
- Prototype build: 9/20
- Prototype validation: 12/20
- Advanced accommodation: 2/21
- Field test: 3/22
- Red team assessment: 3/22

Total Value of Award: $3.6M (fed)+$1.2 (GE) = $4.8M

Funds Expended to Date: $2.9M / $4.8M = 61%

Performer: GE Research

Partners: GE Renewable Energy

Idaho National Lab

* No-cost extension pending approval
Advancing the State of the Art (SOA)

1-Current State of the Art

• Solutions address vulnerabilities at enterprise and operations layers of Energy Delivery Systems

2-Feasibility of approach

• Rigorous assessment completed for attack detection and neutralization using high fidelity models of wind turbines and actual control code

3-How GE approach is better than SOA

• Increased resilience and defense against sophisticated cyber threats
• Handles zero-day vulnerabilities (assumed attacker accessed the controller)
• Introduces defense at all layers of the control system architecture: layers 0 (device), 1 (controller), 2 (supervisory)
• Increased understanding of risks

• >7,500 attack cases simulated
• >500 normal scenarios simulated
• Detection performance surpassed program target of 1% FP & FN

Uses intimate knowledge of asset (design models, control code) to achieve unprecedented performance
Advancing the State of the Art (SOA)

4- Benefit to the end user
• Additional line of defense: complementary cybersecurity offering to the existing IT/OT solutions
• Highly accurate detection and localization for all critical attacks
• Fast and safe neutralization of 171 types of attacks

5- How our approach will advance the cybersecurity of Energy Delivery Systems
• Systematic approach developed for GE wind turbines but applicable to any utility scale wind turbines (may require re-tooling for non-GE assets)
• Can easily expand to new attacks types to address customer specific needs

6- Potential for sector adoption
• Engaged in technology discussions with 3 future potential customers with encouragement, but with caution due to the fact that wind power industry is a cost sensitive segment
• Strategy to introduce first generation of technology for detection and localization only, integrated in customers SCADA and SIEM systems; future versions to include neutralization
Progress to Date

**Major Accomplishments**

1. Designed most critical cyber-attacks for wind power generation
2. Developed novel attack detection & accommodation for wind turbine and demonstrated performance exceeding program goals
3. Developed multiple attack neutralization strategies:
   1. Reconfigurable virtual sensing
   2. Model based backup controller with and without curtailment
   3. Preventive shutdown
4. Defined product requirements and commercialization strategy
5. Discussed technology with 3 potential customers in the wind power utility sector and defined its potential integration in SCADA network
6. Designed and built cyber-security prototype for lab and field test
7. Designed and implemented Software in the Loop (SIL) and Hardware in the Loop (HIL) simulation platforms
8. Submitted 4 patent disclosures for attack detection, localization and neutralization
9. Reserved schedule for field test for phase 2 of the program
Challenges to Success

Challenge 1: Stringent performance in highly stochastic environment

Mitigation steps

- Massive design of experiments including datapoints of 30M floats at 500 normal operating conditions and > 140,000 attack cases
- Extensive feature engineering to provide discriminating data to ML algorithms

Challenge 2: Economic viability of cyber-security HW at each turbine

Mitigation steps

- Move the cybersecurity solution from turbine level to the farm level using EDGE devices
- Addressed high communication rates requirements targeting turbine fleet with high bandwidth SCADA
- Combine business case of cyber security with anomaly detection for O&M benefits

Challenge 3: Technology sustainability, support of diverse fleet

Mitigation steps

- Automated tools preparation for dataset generation
- Transfer Learning of decision models for expansion to other wind turbine fleets
Collaboration/Sector Adoption

**Plans to transfer technology/knowledge to end user**
- Prototype preparation and validation for field test 3/21
- Field test the technology at GE test facility (Lubbock, TX) 4/21–3/22
- Launch New Product Introduction program for productization, 6/21
- Field test customer site (early adopter in wind utility TBD) 6/22
- Product launch 12/22
Next Steps for this Project

Approach to the end of project

### Phase 1 (ending March 2021)
1. Field test plan
2. Complete detection with watermarking
3. Develop transfer learning tools for adapting solutions to site-specific characteristics
4. Prototype laboratory testing
5. Adapt technology to site turbine
6. Develop neutralization using advanced learning
7. Final report Phase 1

### Phase 2 (ending March 2022)
1. Prototype field test
2. Possible technology adjustment
3. Field testing Red team
4. Final report phase 2
Datasets

Normal

Normal Dataset Design of Experiments

- Sample full range of operation: wind speed, turbulence, shear, yaw, curtailment, ...
- Highly stochastic environment need extensive dataset coverage
  - Over 500 data points
  - Each including about 1M floats

Attack

Critical Attack Design

- Control and operability experts working as cyber-attacker
- Rank attacks by RPN
- Select the most critical

Elementary Attack Library

- Decompose critical attacks into elementary components
- Collect building blocks for critical attacks by type & location

Smallest Relevant Elementary attacks

- Define attack impact in terms of effects on power, loads, fatigue life, ...
- Iterate on attack size reached a “relevance threshold” wrt normal operation

Attack Design of Experiments

- Define attack cases in the range of operating conditions (wind speed, air density, yaw, ...)
- Define DoE on which to measure performance

• Over 170 attack types
• Over 7500 attack cases

U.S. DEPARTMENT OF ENERGY
OFFICE OF Cybersecurity, Energy Security, and Emergency Response
Detection and Localization architecture

Detection & Localization Module

- Monitoring nodes
  - Sensors
  - Setpoints
  - Controller signals

- Advanced Feature Generation
  - Statistical features
  - Physical consistency
  - Advanced temporal features
  - Transformed spaces

- Detection Module
  - ML decision models

Hierarchical Localization

- C1
- C2
- C3
- C4
- C5

- ML classifiers
  - System/Subsystem/node
  - Attack type

Minimal number of nodes to achieve target performance

Domain-specific knowledge

Machine learning technology to fine tune performance and adapt solutions
Neutralization architecture

Neutralization
- Applies optimal strategy to minimize attack impact, based on the real time assessment from the Detection and Localization
- Includes Virtual Sensing and Backup controller to counteract cyber attacks
Development/Testing Environments

Software in the loop (SIL) development

Processor in the loop (PIL) testing

* MATLAB/Simulink are registered trademark of The MathWorks, Inc.