E10 - Hardening Wind Energy Systems from Cyber Threats

ESW&G – Grid Integration
Jay Johnson
Sandia National Laboratories
August 3, 2021
Project Summary:
• The team is investigating wind network hardening and security sensing and response technologies to provide wind site cyber resilience.
• These technologies and defense techniques will be shared broadly with the wind industry to harden communication systems to cyberattacks and detect adversary actions.
• To quantify differentiating benefit of different hardening technologies, the team is using a red teaming approach to demonstrate the significance of integrating these technologies in relevant wind site topologies within a cyber-physical co-simulation environment
• Key project partners: DNK Consulting, multiple wind stakeholders

Project Objectives 2019-2020:
• Create five topologies with a combination of hardening technologies.
• Design theoretical attack patterns and quantitative scoring methodologies for red team assessments.
• Survey commercial cybersecurity technologies that can be incorporated into wind systems.

Overall Project Objectives:
• Conduct adversary-based (red team) assessments of different defenses to score their effectiveness against different attack scenarios.
• Advise the wind industry of improvements to wind site security with the successful deployment of different cybersecurity technologies.

Project Start Year: FY20
Expected Completion Year: FY22
Total expected duration: 3 years

FY19 - FY20 Budget: $500k/year

Key Project Personnel:
Sandia: Jay Johnson (PI), Brian Wright
INL: Jake Gentle, Craig Rieger, Bev Novak, Tyler Phillips, Michael McCarty

Key DOE Personnel: Jian Fu (PM)
GOAL:
Recommend cybersecurity defenses for wind sites using adversary-based assessments of virtualized wind site networks

Project Objectives
- FY19 - Build power system and networking co-simulation environment where cyber-attacks are reflected on the power simulation
- FY20 - Implement different cybersecurity defenses in the network emulation
- FY21 - Conduct adversary-based (red team) assessments of different defenses to score their effectiveness against different attacks

Outputs
- Open-sourced baseline wind site networking topology for industry/researchers
- Cybersecurity survey of cyber hardening technologies
- Hardening technology evaluation approach correlated to MITRE ATT&CK framework
- Quantitative cyber-physical scores for different hardening technologies/topologies

Impact
- Actionable, quantitative guidance for the wind industry on the best cybersecurity technologies to defend against local and remote wind site cyberattacks.
**Program Performance – Scope and Execution**

- FY20 milestone - Define co-simulation environment with networking components, virtualized wind site operation center, wind turbine components, and transmission power system.
  - Highly challenging, technical work to integrate a live, cyber-physical co-simulation environment that incorporates human inputs.
  - Baseline networking topology was created based on literature reviews and site interview.
  - Wind Turbine Generators (WTGs) are represented with Modbus Servers that include nameplate data, power system measurements, and control points.
  - The Power system Model is a well-studied 2000-bus Texas model that runs in PowerWorld Dynamic Studio.

---

**ACTIVSg2000: 2000-bus synthetic grid running in PowerWorld**  
**Virtual Machines including WTG Modbus Servers**  
**Virtualized Wind Site Networks**  

Cyber-physical testbeds for scalable, repeatable and comprehensive red team assessments
**SCEPTRE Co-simulation**
- Realistic communication networks and power system simulations in the SCEPTRE platform
- Used to assess the cybersecurity posture of the different cyber security architectures/defenses with a red team

**Initial Networking Design**
- Representative communications from Original Equipment Manufacturers (OEMs), Owner/Operators, and the utility/grid operator to wind site
- Wind Site segmentation using virtual local area networks (VLANs) with dedicated network for operational technology (OT) traffic

**Wind Turbine Emulation**
- Simplified Modbus Remote Terminal Unit (RTU) wind turbine controller includes active and reactive setpoints and power system measurements

**Power Simulation**
- Texas power simulation executed in PowerWorld to measure cyber-attack impact
Program Performance – Accomplishments & Progress

• **Project Accomplishments**
  - Created virtualized wind site topologies with power system data, virtualized wind turbines, and live site controllers
  - Integrated multiple hardening technologies into the co-simulation environment
  - Established cyber-physical scoring mechanisms based on the impact to the site network and power grid
  - Created local and remote cyberattack scenarios, correlated to MITRE ATT&CK

• **Presentations**

• **Copyrighted Open-Source Software**
  - Secure Wind Plant phēnix Topologies
Program Performance – Upcoming Activities/Schedule

- In FY21, the team is deploying five topologies to demonstrate the spectrum of wind site security from baseline security to heavily fortified. Technologies include:
  - **OT Encryption**: encrypts traffic to the wind turbine network
  - **Role-based access control (RBAC)**: requires users to be authenticated/authorized before making changes to wind turbine setpoints.
  - **SIEM**: security information and event management (SIEM) system collects log data to alert admins of potentially malicious cyber activities
  - **NIDS**: network-based intrusion detection system (NIDS) uses deep-packet inspection to alert admins and/or SIEM system to anomalous network traffic.
  - **HIDS**: host-based intrusion detection system (HIDS) that alerts admins, SIEM, or SOAR system to changes to the server by monitoring logs, directories, files, and registries.
  - **SOAR**: Security Orchestration, Automation, and Response collects alerts and automates responses to threats.
- In FY22, the team will perform red team assessments on each of the topologies, score the results with cyber-physical metrics, and widely share these results.

<table>
<thead>
<tr>
<th></th>
<th>Encryption</th>
<th>RBAC</th>
<th>SIEM</th>
<th>NIDS</th>
<th>HIDS</th>
<th>SOAR</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
<td>x</td>
</tr>
</tbody>
</table>
Team will continue to brief relevant stakeholders (POP, ESIG, cyber workgroups, etc.)

Survey sent to cybersecurity vendors, renewables OEMs and Owners/Operators

Cybersecurity survey results will be shared broadly.

SNL, INL, and NREL are working to assemble a small, invite-only workshop for wind cybersecurity to discuss many of the topics presented here.