

**Sandia  
National  
Laboratories**



Idaho National Laboratory

# E10 - Hardening Wind Energy Systems from Cyber Threats

ESW&G – Grid Integration

Jay Johnson

Sandia National Laboratories

August 3, 2021



# FY21 Peer Review - Project Overview

### 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 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)

### 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 Impact

## 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

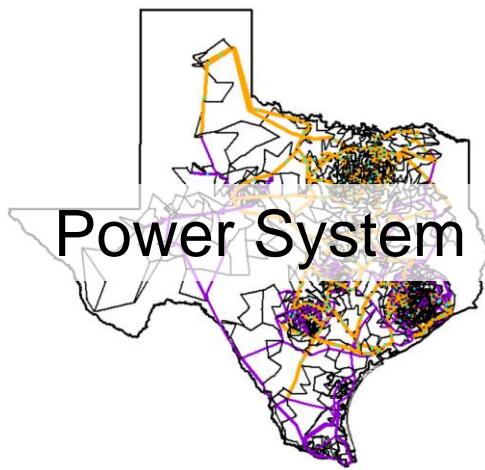
- Briefed Protect Our Power, Energy Systems Integration Group (ESIG) Operations and Maintenance (O&M) Users Group, Wind Cybersecurity Consortium
- Open-sourced baseline wind site networking topology for industry/researchers
- Cybersecurity survey of cyber hardening technologies
- Hardening technology evaluation approach correlated to MITRE ATT&CK framework
- Quantitative cyber-physical scores for different hardening technologies/topologies

### Impact

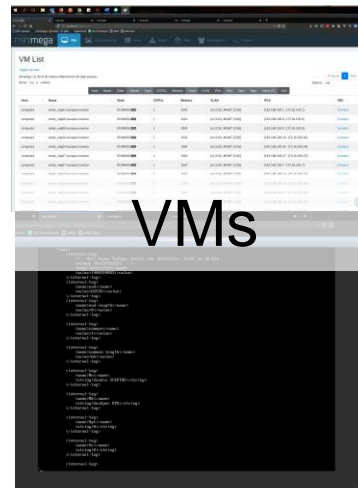
- Actionable, quantitative guidance for the wind industry on the best cybersecurity technologies to defend against local and remote wind site cyberattacks.

# Program Performance – Scope and Execution

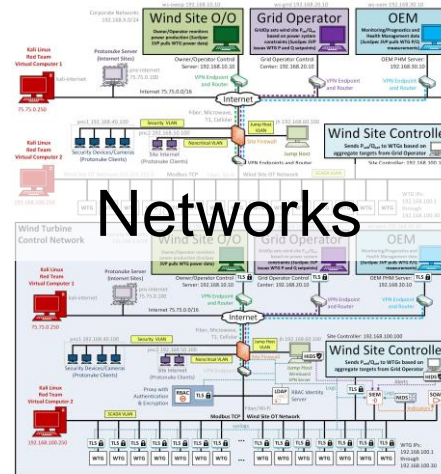
- FY20 milestone - Define co-simulation environment with networking components, virtualized wind site operation center, wind turbine components, and transmission power system.
  - Highly challenging, technical work to integrate a live, cyber-physical co-simulation environment that incorporates human 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.



+



+



=

Cyber-physical testbeds for scalable, repeatable and comprehensive red team assessments

ACTIVSg2000: 2000-bus synthetic grid running in PowerWorld

Virtual Machines including WTG Modbus Servers

Virtualized Wind Site Networks

# Program Performance – Accomplishments & Progress

## 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

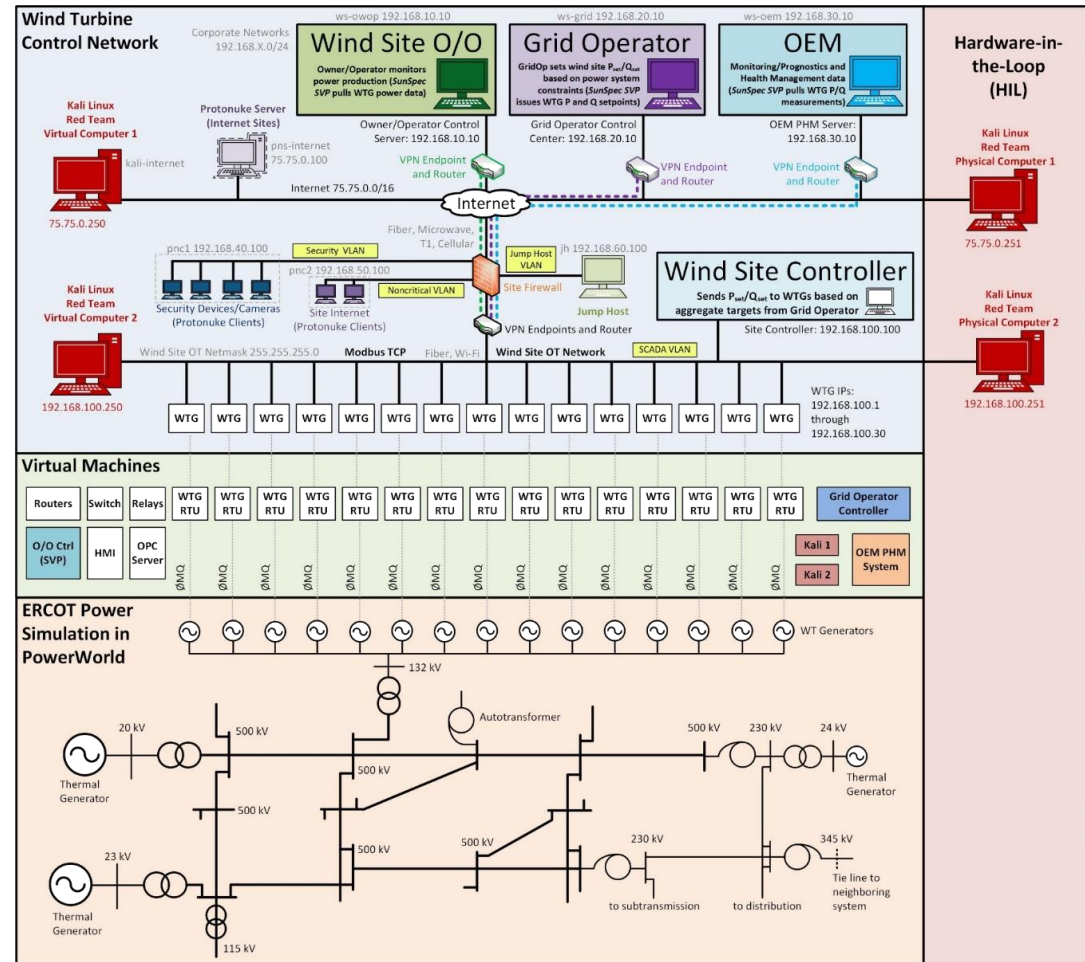
- Representative communications from Original Equipment Manufacturers (OEMs), Owner/Operators, and the utility/grid operator to wind site
- Wind Site segmentation using virtual local area networks (VLANs) with dedicated network for operational technology (OT) traffic

## 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

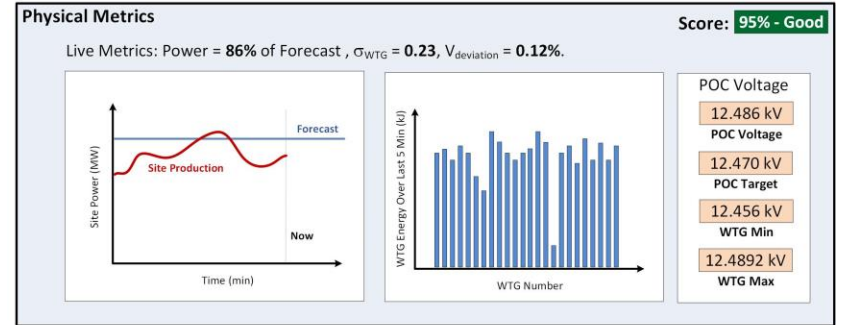
- Created virtualized wind site topologies with power system data, virtualized wind turbines, and live site controllers
- Integrated multiple hardening technologies into the co-simulation environment
- Established cyber-physical scoring mechanisms based on the impact to the site network and power grid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

## Presentations

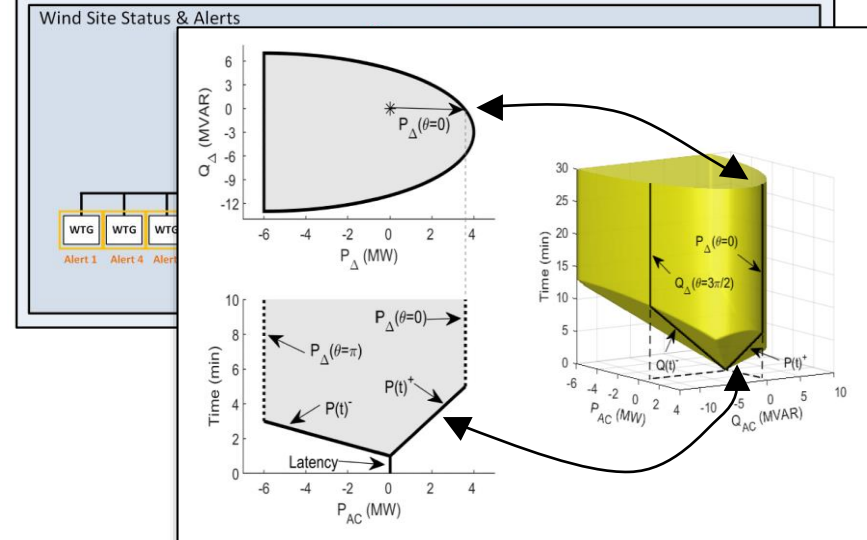
- J. Johnson, J. Gentle, C. Rieger, “Hardening Wind Energy Systems from Cyber Threats – Project Briefing,” Wind Consortium Meeting, 7 April 2021.
- J. Johnson, J. Gentle, “Hardening Wind Systems R&D Project,” ESIG O&M Spring 2020, 1 April 2020.
- J. Gentle, J. Johnson, “Cybersecurity for Wind Energy,” Protect Our Power - Best Practices in Utility Cybersecurity Conference, 27 Jan 2020.

## Copyrighted Open-Source Software

- Secure Wind Plant phoenix Topologies



## Example Scoring Metrics



# Program Performance – Upcoming Activities/Schedule

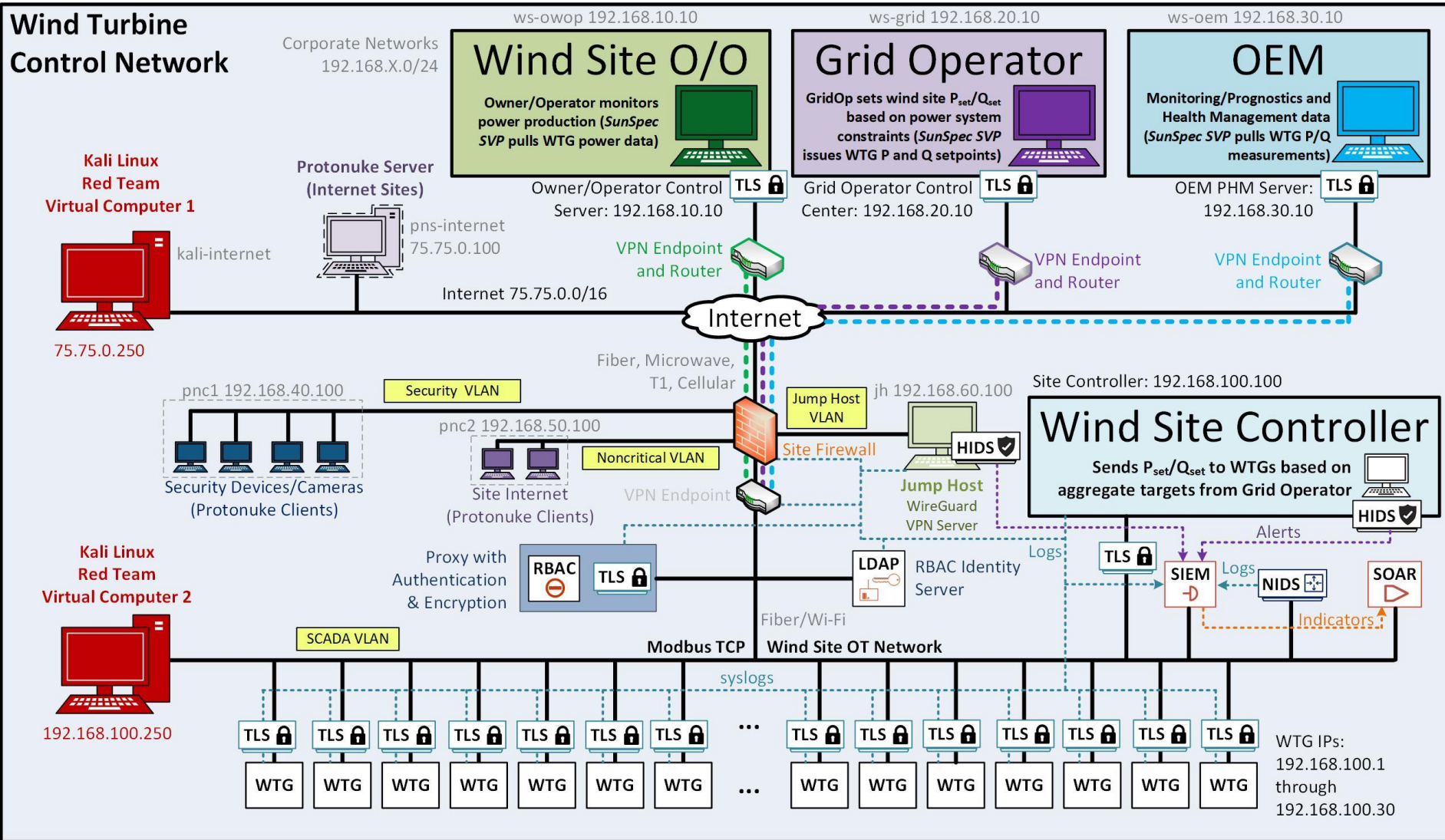
- In FY21, the team is deploying five topologies to demonstrate the spectrum of wind site security from baseline security to heavily fortified. Technologies include:
  - OT Encryption:** encrypts traffic to the wind turbine network
  - Role-based access control (RBAC):** requires users to be authenticated/authorized 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.

	Encryption	RBAC	SIEM	NIDS	HIDS	SOAR
1						
2	X	X				
3			X	X		
4	X				X	X
5	X	X	X	X	X	X

The image displays four screenshots of security software interfaces:

- Nozomi NIDS/SIEM:** A dashboard showing environment information (Assets: 6, Nodes: 343, Links: 38, Protocols: 22, Sessions: 237, Variables: 544) and a traffic flow graph. A large text overlay reads "Nozomi: NIDS/SIEM".
- Wazuh HIDS/SIEM:** A diagram showing a "Wazuh server" with components like Wazuh manager, Wazuh API, Filebeat, and Elasticsearch, connected to a "Monitored endpoint" with a Wazuh agent. A large text overlay reads "WAZUH HIDS/SIEM".
- OSSEC HIDS:** The OSSEC logo and the text "OSSEC HIDS".
- Demisto SOAR:** A workflow diagram for a "Task Details" window, showing steps like "Fetch MDS Reputation", "VirusTotal Hash Reputation for: #8decf2bb210b9f78978940a4c56e536", and "Fetch MDS Reputation". A large text overlay reads "SOAR".

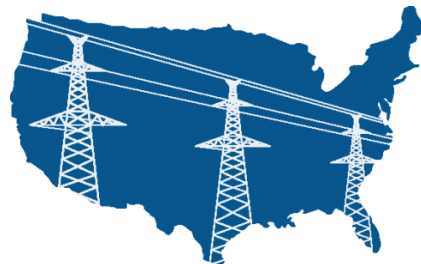
# Hardened Wind Site Topology





# Stakeholder Engagement & Information Sharing

- 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.



**PROTECT  
OUR  
POWER**



Example cybersecurity vendor survey results for HIDS providers.

Company	Solar	Wind	Electric Vehicles	Product name	Years on the market	HIDS Features											
						Protect from data egress	Attach external timing for log stamps	Support INDUSTRIAL CONTROL SYSTEM protocols	Detect new conversations	Decision support	Detects changes to firmware Applicable to Purdue layers 0, 1, or 2	Monitor unauthorized access	Monitor changes in device	Other	Other, please explain		
Alion				Big Data Platform (BDP)	8												
Dragos				Dragos	5												
Dragos				ProServices	5												Training, TTX, IRR, Penetration Testing, Arch Assessments, etc
Dragos				Threat Intelligence - WorldView	5												
Elastic				Elastic	9												
HP Inc.				Computers, Printers 3D Printers	81												Micro Virtual Machine
InZero Technology				TRIPliot	<1												
Iron Inc.				Smart grid	10+												
Mantis Networks				MantisNet CVF	1												Uniquely fingerprint authorized systems, detection of weak, or unsupported cryptographic traffic, introspection/analysis of any (TCP/IP) based industrial control system protocol
New Context				Threat Monitoring & Automated ResponsePlatform	0												
Optiv Federal				Security Matters (ForeScout)	5+												Optiv resells & provides services for ForeScout (Security Matters), Microsoft (CyberX), Clarity, and other ICS products
PFP Cybersecurity				PxScan Analytics	5												supply chain security
PFP Cybersecurity				pMon 751	5												supply chain security
PFP Cybersecurity				PFP Monitor	1												Out of band monitoring. Air-gapped deployment.
R&K Cyber Solutions LLC				Heartbeat	<1												
R&K Cyber Solutions LLC				USB-ARM	<1												
R&K Cyber Solutions LLC				Beholder													
Templar Shield				Splunk	15												
Templar Shield				Tenable	10												Uses PLC protocols to detect and alert to control changes. continuous monitoring
Verve Industrial Protection				Verve Security Platform	5+												A combination of agent based, and then change management/non-agent based data acquisition
Waterleaf International				Cyberleaf	<1												
Waterleaf International LLC				Cyberleaf	1												