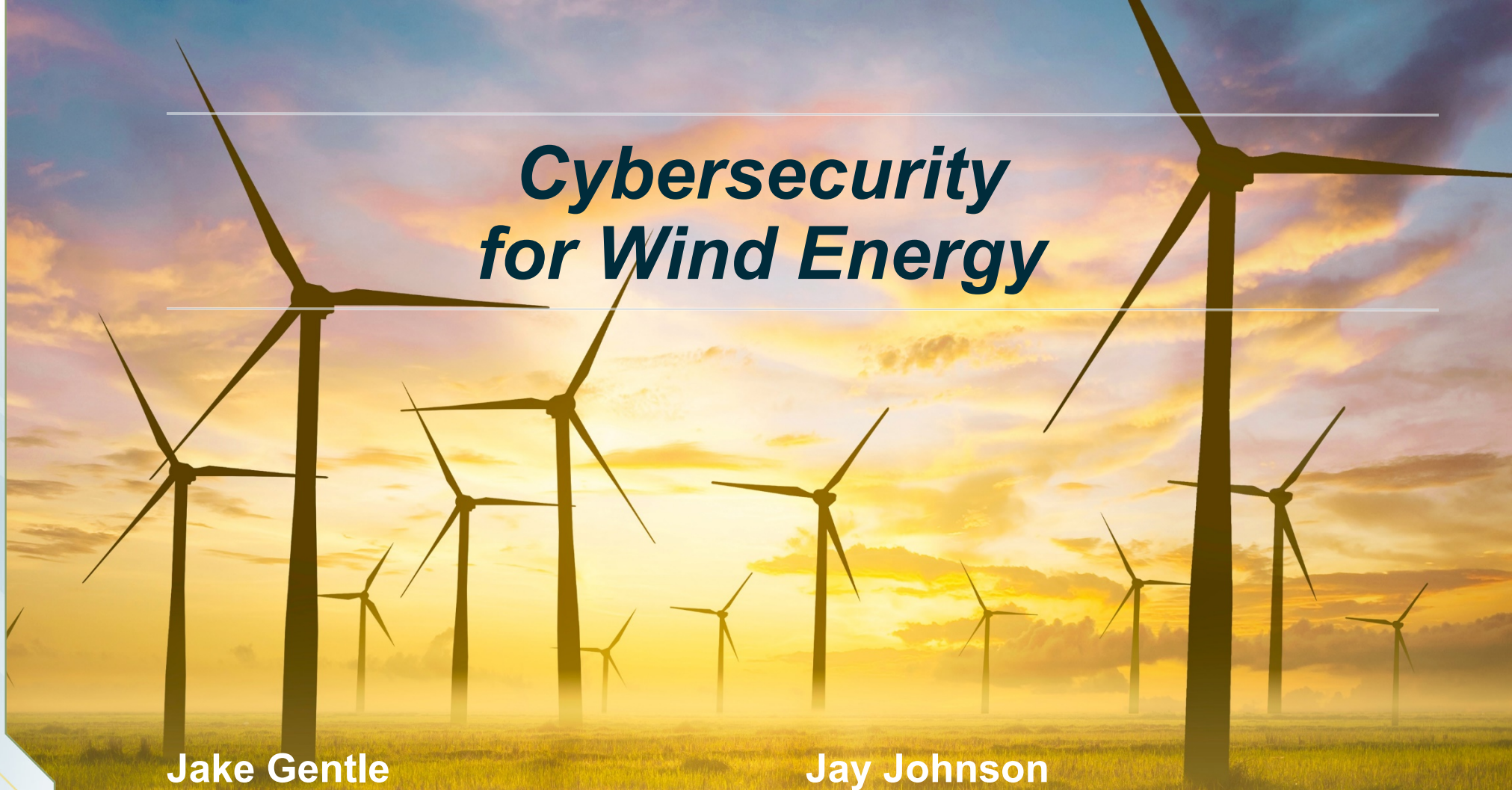
Cybersecurity for Wind Energy



Jake Gentle
Senior Power Systems Engineer
Idaho National Laboratory

Jay Johnson
Principal Member of Technical Staff
Sandia National Laboratories

Protect Our Power - Best Practices in Utility Cybersecurity Conference
27 January 2020

INL/CON-20-57174
SAND2020-0568 PE

www.inl.gov

INL
Idaho National Laboratory

The Roadmap for Wind Cybersecurity

Objectives:

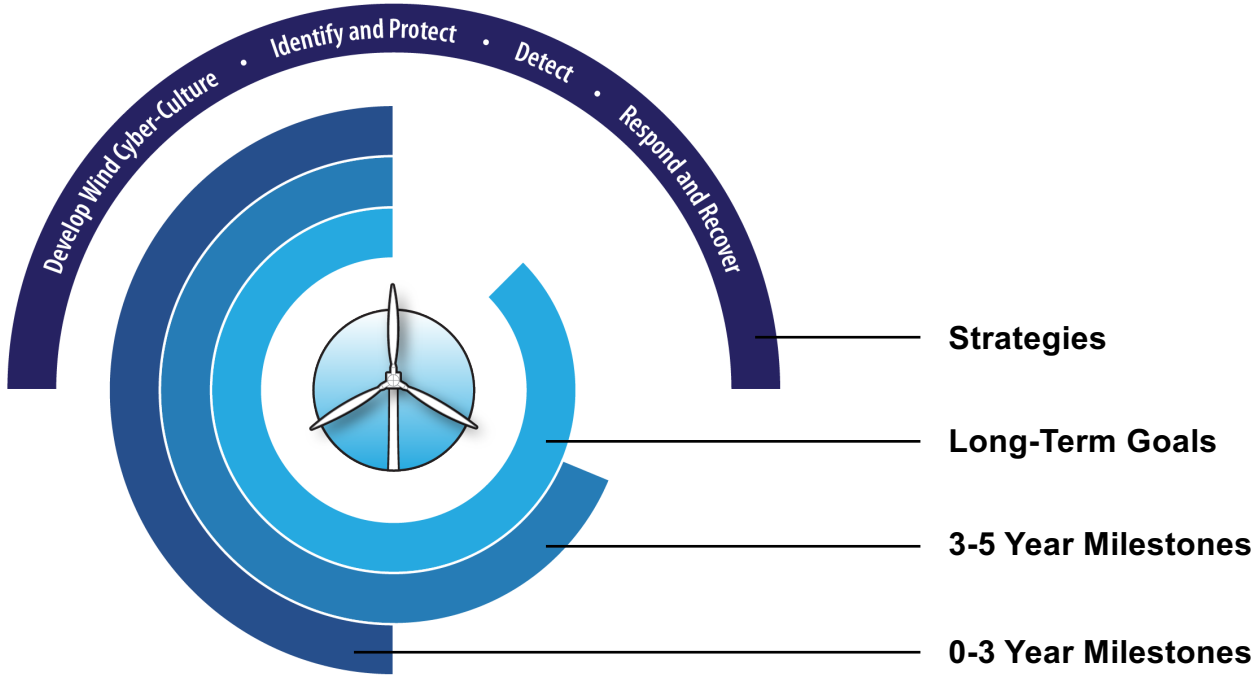
- Provide preliminary outline of wind energy technology baselines
- Describe wind energy threat landscape
- Identify current trends in cybersecurity Research & Development
- Outline Research & Development needs
- Highlight addressable gaps in wind energy cybersecurity
- Highlight existing good practices
- Promote standards development in cybersecurity for wind
- Engage wind stakeholders in Roadmap efforts
- Promote wind cybersecurity information sharing and situational awareness

Vision

By 2030, wind energy systems are designed, retrofitted, and operated to be resilient to cyber-events, minimizing potential impacts to the power grid.

Challenges

- Increasing cyber-incidents targeting wind energy systems
- Difficult to establish effective cybersecurity practices
- Wind energy assets require robust cybersecurity practices
- No single cybersecurity strategy can apply to all wind plants
- Available cybersecurity options may be too costly
- Few wind-specific cybersecurity standards exist
- Few incentives to prioritize cybersecurity
- Limited information sharing among wind stakeholders
- Few wind-specific cybersecurity services available



Roadmap Overview

Chapters generally address the state-of-the-art, gaps/opportunities, and future of wind energy cybersecurity

1. Introduction

2. National Energy Cybersecurity Efforts

3. Wind Energy Technology Landscape

4. Wind Cyber-threat Landscape

5. Wind Cybersecurity R&D

6. Standards Development

7. Recommended Practices

8. Stakeholder Engagement

9. Conclusions

Wind Cyber Landscape

Current State of Wind Energy Technology

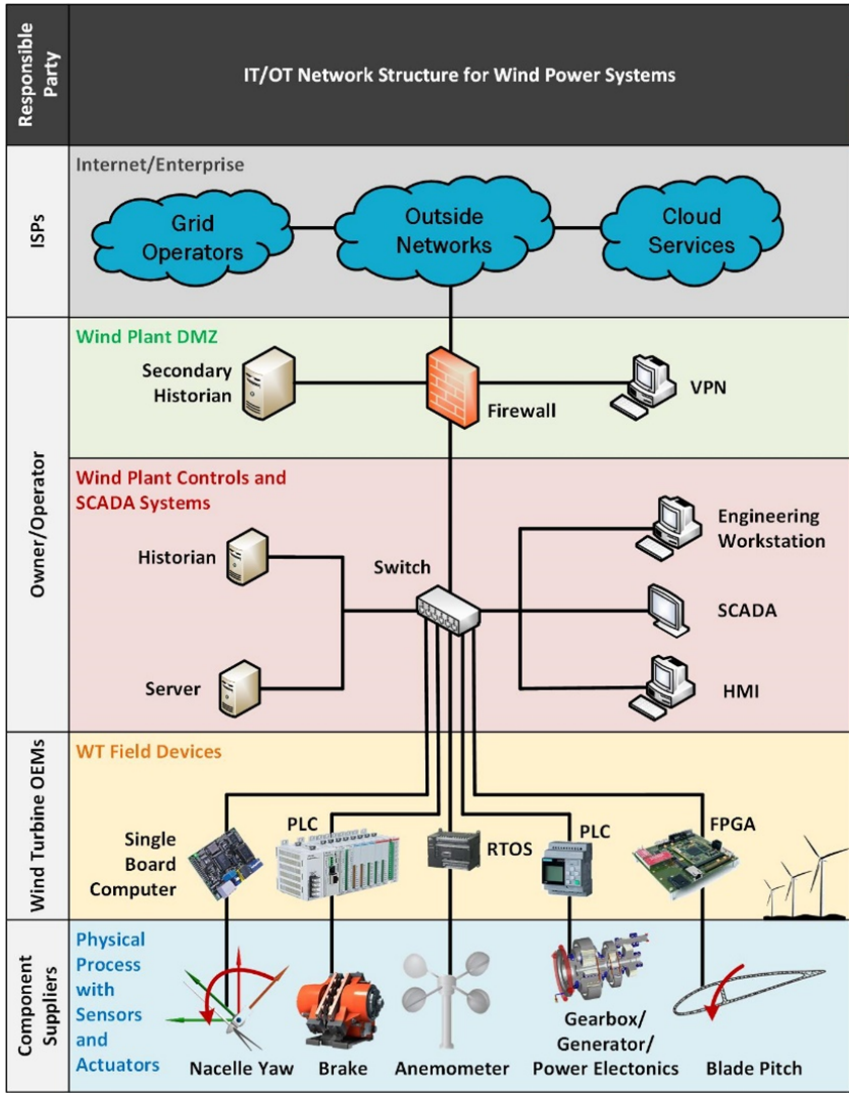
- Increasing reliance on internal, external data for dynamic operation
- Diverse equipment makes, models, configurations (even within a plant)
- Diverse implementations of technologies
- Heavy reliance upon remote access technologies (wireless, cellular)
- Widespread use of OT communications protocols with known vulnerabilities
- Lack of standardization in wind energy communication protocols

The Cyber-threat Landscape

- Targeted cyberattacks on wind plants have already occurred
- Researchers regularly discover wind-specific cyber vulnerabilities and exploits
- Open source information, SHODAN, poorly secured web-accessible control platforms mean easy adversarial access
- Wind turbines could provide “pivotal” access into transmission and distribution system networks, bulk electric system (BES)
- Potential consequences: permanent physical damage, power disruption, loss of system integrity

IT/OT Wind Plant Infrastructure

- Purdue Model (provides reference architecture for secure network application layers) applies to wind systems
- Left column indicates ownership and access
- Many parties “touch” the communications and operations of a wind plant
- Highly reliable communication infrastructure in wind plants is critical for the real-time operation, monitoring, and control of both wind turbines *and* the power grid to ensure grid stability
- The number of parties involved in and accessing wind system communication infrastructures may also provide an attack vector for cyber-adversaries
- *Need:* A *wind-specific* secure network reference architecture



Wind Cyber R&D

- National Institute of Standards and Technology (NIST) Framework approach: Identify, Protect, Detect, Respond, Recover
- R&D topics can be associated with multiple locations in the communication network

Identify

- It is essential to identify and document network components and critical assets to reduce the attack surface and potential impact for wind cyber-systems
- Threat models, cyber assessments, virtualized testbed environments, and tools/methods for calculating risk are some of the tools that may lead to a better protected wind system environment

Protect

- It is important to create defensive mechanisms to protect against identified attack vectors
- There are established methods and advanced protection techniques for preventing unauthorized network access (e.g. firewall whitelisting/blacklisting, proxies, virtual private networks[VPNs])

Wind Cyber R&D (continued)

- **Detect/Analyze**
  - Advanced wind cybersecurity systems must include tools to capture, analyze, and visualize near-real-time data to reduce the exposure to cyberattack
  - Detecting adversarial actions on wind control networks is necessary to implement appropriate countermeasures

- **Respond**
  - Wind systems must implement countermeasures to increase system resilience, extend the time and difficulty of perpetrating the attack, and minimize the impact to their assets and throughout the grid
  - Proper wind cybersecurity responses include information sharing platforms between government agencies and the private sector, cyber-forensics, cybersecurity investigations, and dynamic assessment technologies that conduct real-time analytics on data streams

- **Recover/Manage**
  - Tools, resources, and funding are needed to assist the wind sector with system recovery and overall wind turbine and wind plant resiliency to cyber-incidents
  - Concepts such as resetting the system to a known good state are important to ensure restoration of wind systems after an event

Standards Development

Equipment

- North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards can be used as a foundational means of implementing cybersecurity controls for wind equipment
- Given the number and variety of wind energy equipment continuously released, more wind-specific equipment standards should be researched and developed

Communication

- Very few cybersecurity standards or guidelines currently exist for wind energy communications
- Some wind system owners use general communications standards designed for other energy (or other) sector facilities (IEC 61850, IEC 62351, etc.) but these do not address wind-specific cybersecurity needs

Recommendation:
Standards certification

- A certification process establishing that wind facilities possess at least a minimum level of digital protections is needed
- Certification would ensure that interoperable wind systems have lateral, encompassing protection of assets based on the same standards implementation

Recommended Practices

Cybersecurity programs

- Cyber-informed Engineering (CIE)
- Consequence-driven Cyber-informed Engineering (CCE)
- C2M2
- NIST
- RMF (DOD)

Technical practices

- Network segmentation and zoning
- Role-based access controls
- Remote accessibility management

Cyber-hygiene

- Promoting cyber-hygiene in the context of OT beyond basic corporate (IT) cybersecurity training is needed for the wind industry
- Encouraging the applicability and implementation of existing cyber-hygiene good practice guides for wind energy such as NIST's *Guide to Industrial Control Systems Security* is a good baseline activity

Recommended Practices (continued)

- **Administrative practices**
  - Facilitating greater cooperation among wind energy stakeholders will lead to better industry-wide execution of cybersecurity programs and practices
  - Currently, major challenges to overcome in achieving greater cooperation on cybersecurity issues are:
    - Workforce
    - Cost
    - Competition
    - Liability
    - Information silos
    - Control

- **Supply chain security**
  - Based on the number of foreign manufacturers involved in the manufacturing of wind energy, technologies require greater supply chain security
  - Remote access to wind turbine equipment from foreign companies is permitted, but should be researched and formally considered further

- **Physical security**
  - Existing wind plant infrastructure often have limited on-site physical security
  - Better-defined and implemented physical security guidelines for wind facilities should be developed

Opportunities for Wind Stakeholder Engagement

- Leveraging existing resources, particularly by encouraging wind stakeholders not yet familiar with existing information sharing mechanisms and working groups is necessary
- Developing additional wind-specific cybersecurity information sharing capabilities is also needed

- **Information sharing**
  - Electricity Information Sharing and Analysis Center (E-ISAC)
  - **Opportunity: Wind-specific ISAC**
- **Working groups**
  - International Electrotechnical Commission (IEC) Technical Committee (TC) 88
  - USE61400-25 user group
  - ESIG Operations and Maintenance Users Group
- **Vendor engagement**
  - More stringent vetting process of original equipment manufacturer (OEM) cybersecurity practices
  - More scrutiny of foreign-owned wind OEMs, vendors
  - Influence vendors to make cybersecurity a priority

USE61400-25
IEC 61400-25 user group

ESIG
ENERGY SYSTEMS INTEGRATION GROUP

AWEA

Opportunities for Wind Stakeholder Engagement (continued)

- **Cybersecurity exercises**
  - U.S. Cyber Command
  - Department of Homeland Security Red/Blue training
  - Cyber Strike
  - NERC GridEx
  - FBI CyberGuard
- **Incident response**
  - DOE CESER-ISER and DHS National Cybersecurity & Communications Integration Center (US-CERT, ICS-CERT)
  - Encourage establishment of cyber-emergency response plans including roles, responsibilities
- ***Research need:* Power system contingency planning**
  - Broader research of cybersecurity implications of growing wind energy upon transmission/distribution system, and broader bulk electric system (BES)
  - Broader research of cybersecurity implications integration
  - Research of cybersecurity implications of US offshore wind (largely unexplored)

WIND-Centric Cyber R&D and Outreach

Define and promote implementation of basic cyber-hygiene

- Promoting cyber-hygiene for OT environments, and wind facility environments, particularly
- NERC CIP requirements
- Encourage comprehensive owner/operator-to-vendor/OEM cyber-hygiene practices

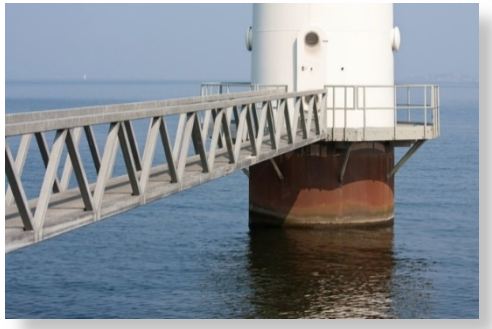
Help develop robust, consistent cybersecurity programs at wind facilities

- Develop or assist in the development of general cybersecurity policies and procedures for wind facilities
- Such cybersecurity-based policies and procedures should detail activities before, during, and after a cyberattack. These activities include cyber-incident reports, organizational roles, and system recovery

WIND-Centric Cyber R&D and Outreach (continued)

- **Develop and encourage participation in wind-specific cybersecurity information sharing mechanisms**
  - The growing diversity of wind technology suggests that the wind industry may benefit from its own information sharing platform in which more technologically specific threat and vulnerability information can be shared
  - Wind energy does not currently possess an industry-specific cyber-threat and -vulnerability sharing platform
  - Which organization (government, OEMs, owners/operators, or combination) can best lead this effort is to be determined
- **Encourage participation in cyber-emergency response and other cyber-preparedness exercises**
  - Wind industry personnel should participate in regular cybersecurity training to reduce the risk of a cyberattack
- **Promote the conducting of regular cyber-assessments**
  - Stakeholders cannot accurately define cyber-risk without conducting *regular* assessments that provide a full view of the cyber-threat landscape and wind sites' preparedness for adverse cyber-events

WIND-Centric Cyber R&D and Outreach (continued)



- **Further develop cybersecurity standards for wind energy technologies.**
  - Cyber-related standards for wind OT is underdeveloped
  - Facilitate wind stakeholder working groups to increase the industry's focus on cybersecurity
  - Potential for a wind facility cybersecurity certification process
- **Institute roles and responsibilities within wind entities, and throughout industry.**
  - Currently, stakeholders face some ambiguity about who is responsible for cybersecurity in OT equipment design, implementation, maintenance, etc.
  - Wind stakeholders—owners, operators, OEMs, standards developers, government, academia—need defined cybersecurity roles and responsibilities to which they are held accountable

Next Steps

- **Begin prioritizing and planning R&D activities**
  - Wind-specific information sharing, further standards development, wind energy cybersecurity assessments, and development of a wind-specific secure network reference architecture are among primary requirements and interests
- **Continue stakeholder outreach**
  - Protect Our Power at DistribuTECH, January 2020
  - ESIG Spring O&M User Group Meeting, March 2020
  - AWEA CLEANPOWER, June 2020
- **Roadmap is currently undergoing review cycles**
  - ☑ External Reviews
  - ☑ Revision, addition of figures
  - ☑ Final technical edit
  - ☑ Delivery to DOE WETO
  - ❑ Final DOE Reviews
  - ❑ Release to the public

Hardening Wind Systems R&D Project

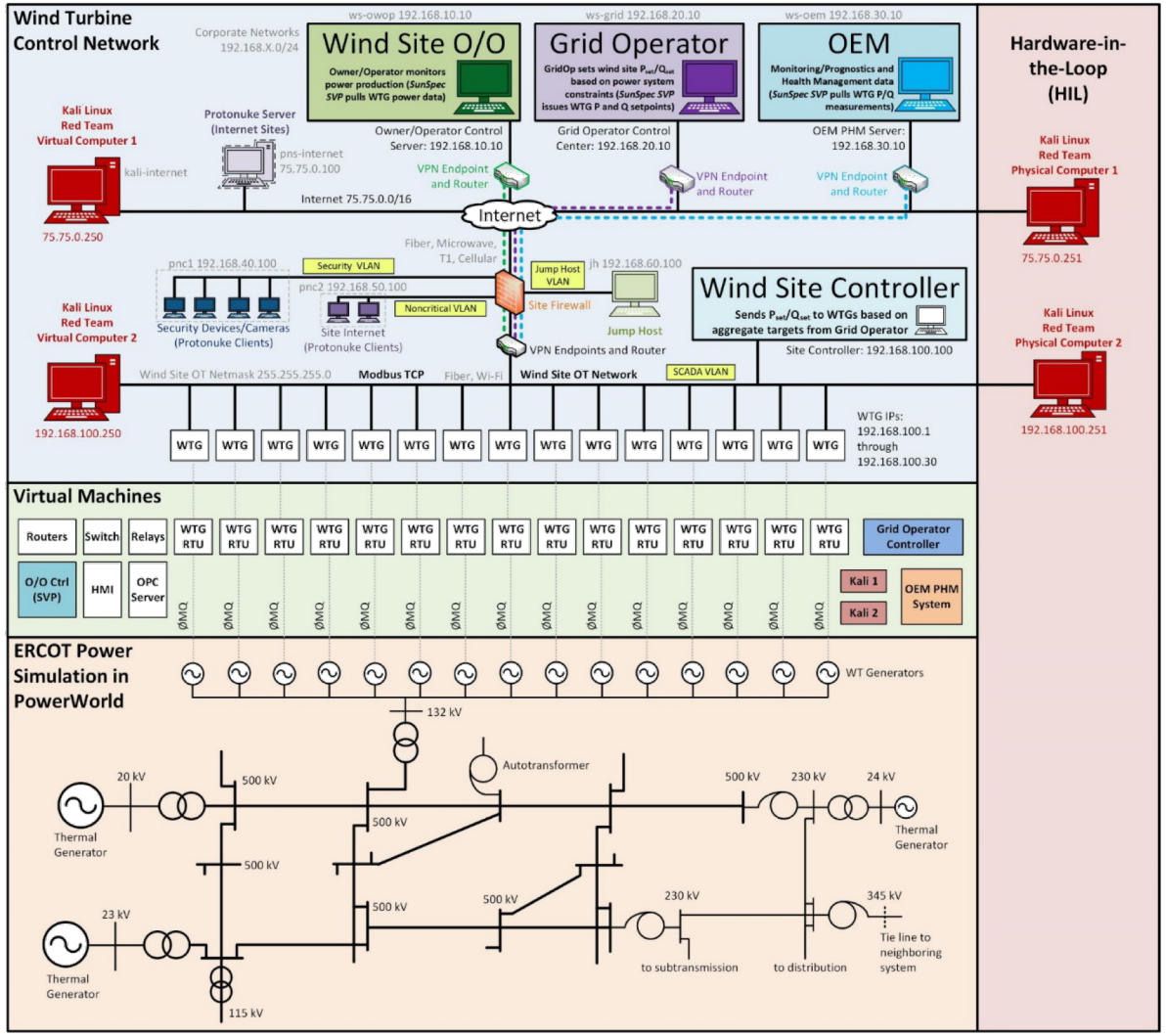
GOAL:

Recommend cybersecurity defenses for wind sites
using adversary-based assessments of virtualized wind site networks

- "Hardening Wind Energy Systems from Cyber Threats" Project
  - $1.5M, 3-year project funded by the DOE Wind Energy Technologies Office
  - Team: Sandia National Laboratories and Idaho National Laboratory
  - Kickoff meeting in Dec 2019
- Project Plan
  - Build power system and networking co-simulation environment where cyber-attacks are reflected on the power simulation
  - Implement different cybersecurity defenses in the network emulation
  - Conduct adversary-based (red team) assessments of different defenses to score their effectiveness against different attacks

SCEPTRE

- Cyber security assessments use realistic communication networks and power system simulations in the SCEPTRE platform
- SCEPTRE uses network emulation and analytics (Emulytics™) to model, simulate, emulate, test, and validate control system security and process simulations
- SCEPTRE is part of an Emulytics suite developed over a decade at Sandia for government agencies and military applications
- In this project, SCEPTRE will assess the cybersecurity posture of the different cyber security architectures/defenses with a red team



SCEPTRE
scada-as-a-platform™

Simulation Environment

Networking Design

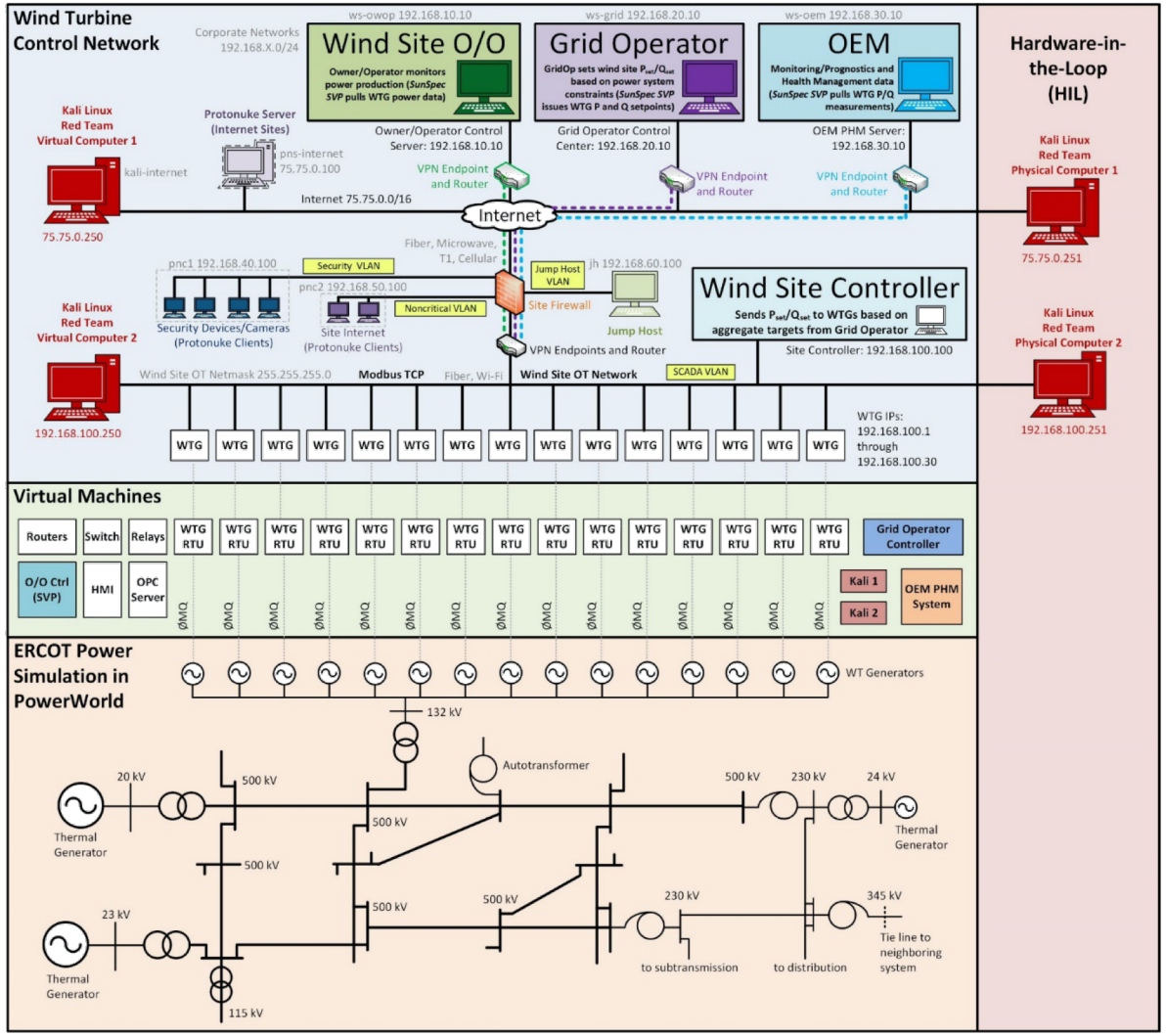
- Representative communications from OEMs, O/Os, and the utility/grid operator to wind site
  - Dedicated VPNs run from each entity to the OT VLAN
- Wind Site segmentation using VLANs with dedicated network for OT traffic

Wind Turbine Emulation

- Simplified Modbus RTU wind turbine controller includes P/Q setpoints and power system measurements

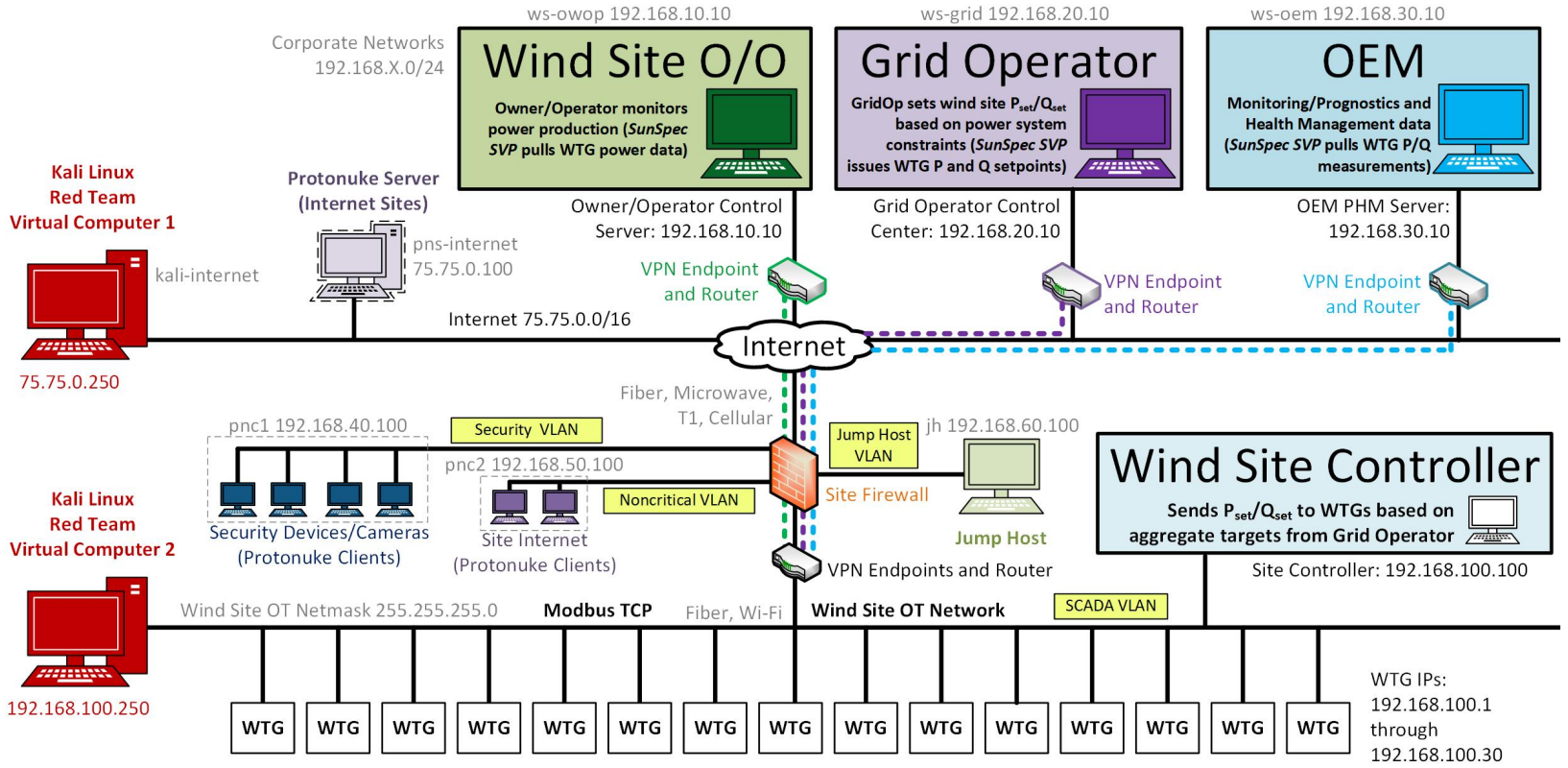
Power Simulation

- An ERCOT power simulation run in PowerWorld to measure cyber-attack impact



Initial Reference Architecture (based on multiple site visits)

- Wind Site VLANs are isolated from the internet using a Site Firewall
- VPNs to the OT network are available for O/O, Grid Operator, and OEM
  - O/O can monitor power production
  - Grid Operator can send active and reactive power setpoints to wind turbine generators (WTG)
  - OEM can monitor WTG operations for monitoring/ prognostics
- Security VLAN for site cameras
- Noncritical VLAN is site Wi-Fi for operators (e.g. webinars)
- Jump host allows remote users or local operator access to the OT VLAN



Our Requests

- Recommendations for the **Baseline Reference Architecture**
  - Is our reference architecture reasonable?
  - Can you share reference architectures and security recommendations with the team? (We can sign NDAs)
  - Is segmentation widely used? Is it typically done using VLANs?
  - Are there VPNs for the O/O, OEM, and grid operators?
  - Are jump hosts common?
  - What firewall rules are used at the site perimeter?
  - What role-based access controls exist at these sites?
  - What protocols are used on the site and within the turbines?

- Certain **attack vectors** should we investigate?
  - Denial of Service
  - MITM/Data Injection/Replay attacks
  - Escalation of Privilege
  - Spoofing
  - Tampering
  - Repudiation
  - Information disclosure

- What **defensive strategies** should we implement?
  - Segmentation/VLANing
  - Moving Target Defense
  - Encryption
  - IDS/IPS/Anomaly Detection
  - Firewall rules
  - Access controls/RBAC
  - SIEM/CPS analysis
- What **consequences of concern** should we investigate?
  - Cyber
    - Confidentiality
    - Integrity
    - Availability
  - Physical
    - Adaptive Capacity (Impact to Reserves)
    - Turbine Damage (e.g., Damage Equivalent Loads)
  - Financial
    - Market Prices

For additional questions, please contact us:

Jake Gentle – jake.gentle@inl.gov

Jay Johnson – jjohns2@sandia.gov