INL/RPT-24-76227-Revision-0

Attack Surface of Wind Energy Technologies in the United States

January 2024

Megan Jordan Culler, Megan Mincemoyer Egan, Remy Vanece Stolworthy, Jayden Loo, Jake P Gentle

Changing the World's Energy Future

INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance, LLC

INL/RPT-24-76227-Revision-0

Attack Surface of Wind Energy Technologies in the United States

Megan Jordan Culler, Megan Mincemoyer Egan, Remy Vanece Stolworthy, Jayden Loo, Jake P Gentle

January 2024

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

January 15, 2024

Presenter Name
Title

Attack Surface of Wind Energy Technologies in the United States

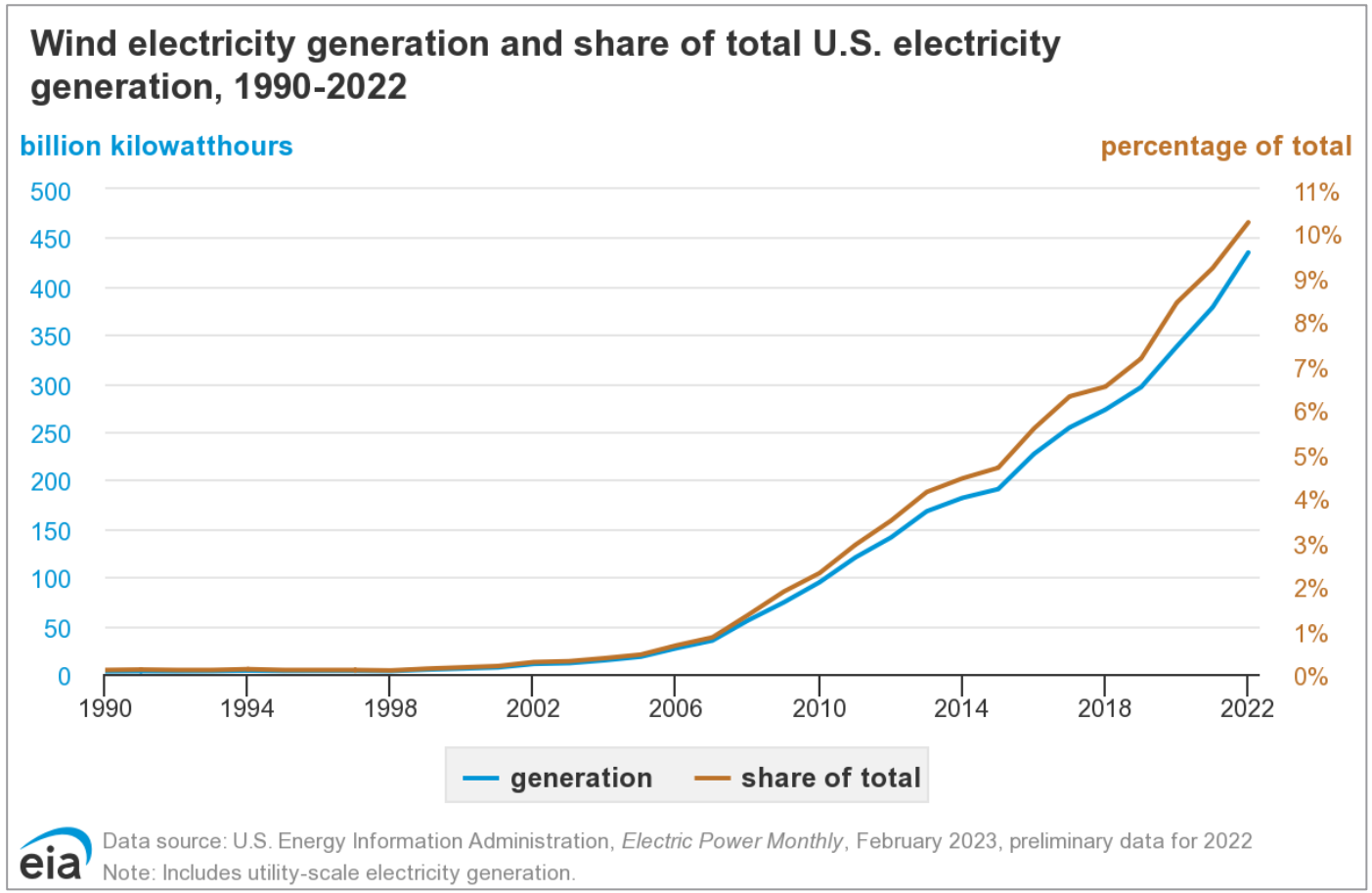
Cyber Threat Assessment

Battelle Energy Alliance manages INL for the
U.S. Department of Energy's Office of Nuclear Energy

Idaho National Laboratory

INL/RPT-24-76227

Increase in Wind Energy Production



10.25% of the U.S. total generation capacity in 2022 [1]

Recent Wind Cyber Attacks

- Increased wind sector influence
- Primary U.S. adversaries
  - China
  - Russia
  - Iran
  - North Korea
- Development of more sophisticated attacks

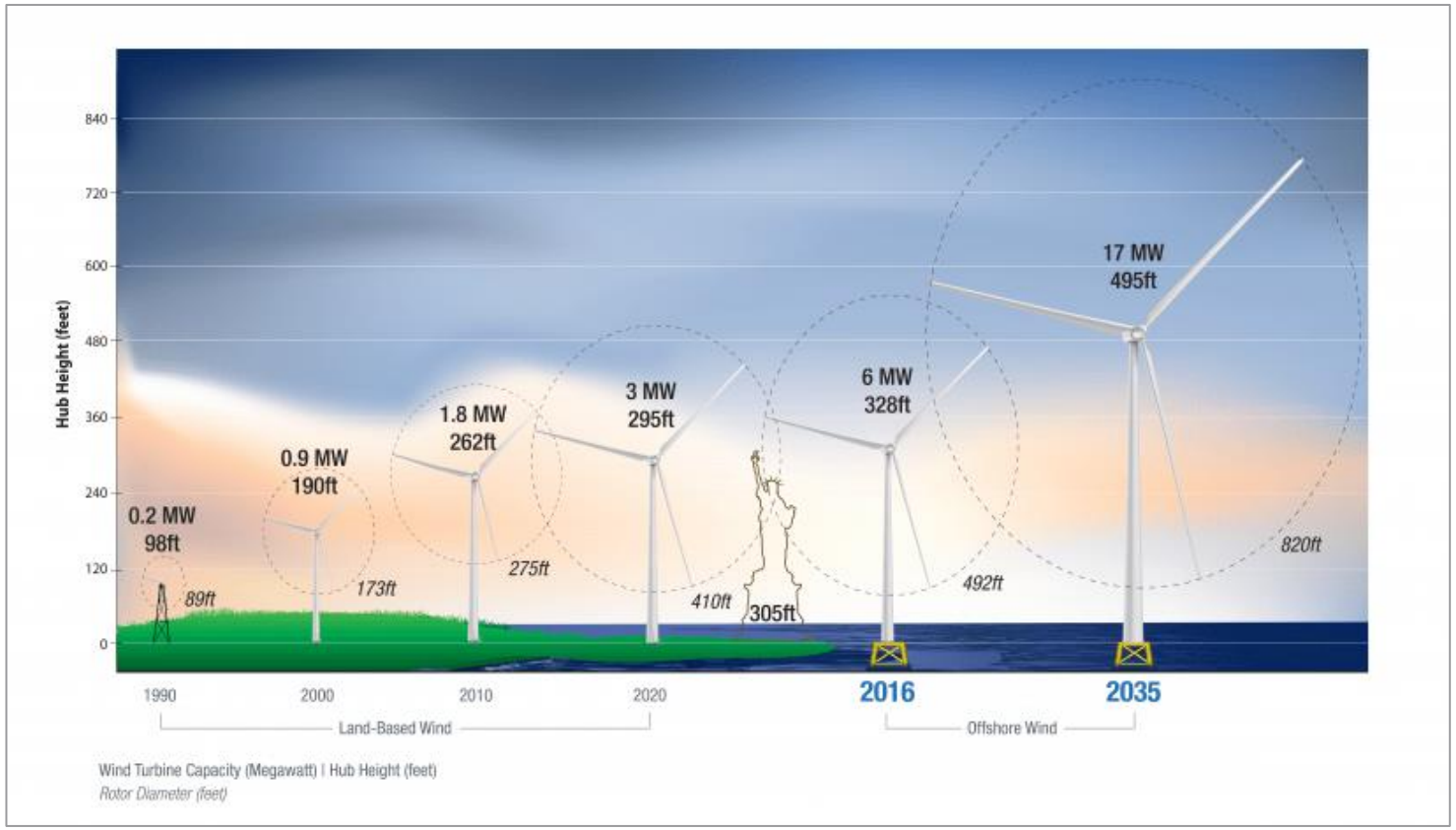
Wind Plant Challenges

- Communication with wind plants is needed
  - Geographically separated turbines
  - Increases the attack surface
- Many stages in a wind plant life cycle
  - Involves many different actors
- Cyber attacks have already occurred
  - Few wind specific cybersecurity standards
  - Cybersecurity is not a priority
    - Reliability and performance prioritization
  - Limited threat information sharing
  - Few, underdeveloped cybersecurity services, products, and strategies

https://www.energy.gov/sites/default/files/2020/08/f77/wind-energy-cybersecurity-roadmap-2020v3.pdf
https://resilience.inl.gov/wp-content/uploads/2021/11/21-50152_CG_for_DW_R5.pdf

Wind Plant Diversity

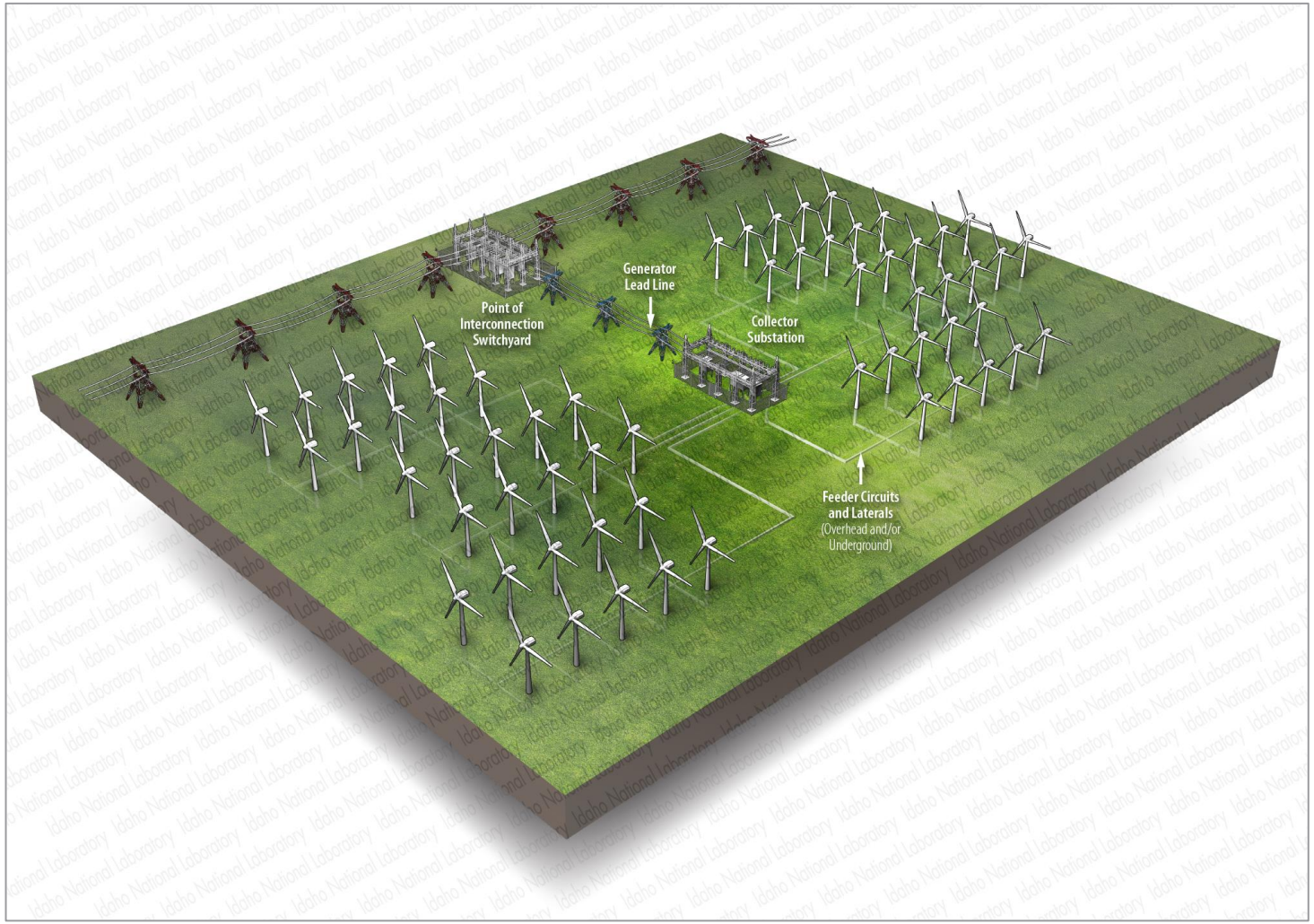
- Cybersecurity practices may change based on plant:
  - Size
  - Generation Capacity
    - # of Turbines
    - Size of Turbines
  - Network Design
    - Fiber Optic
    - Wireless
  - Communication Protocols
  - Control Center Design
  - Maintenance
  - Location
    - Offshore/Onshore

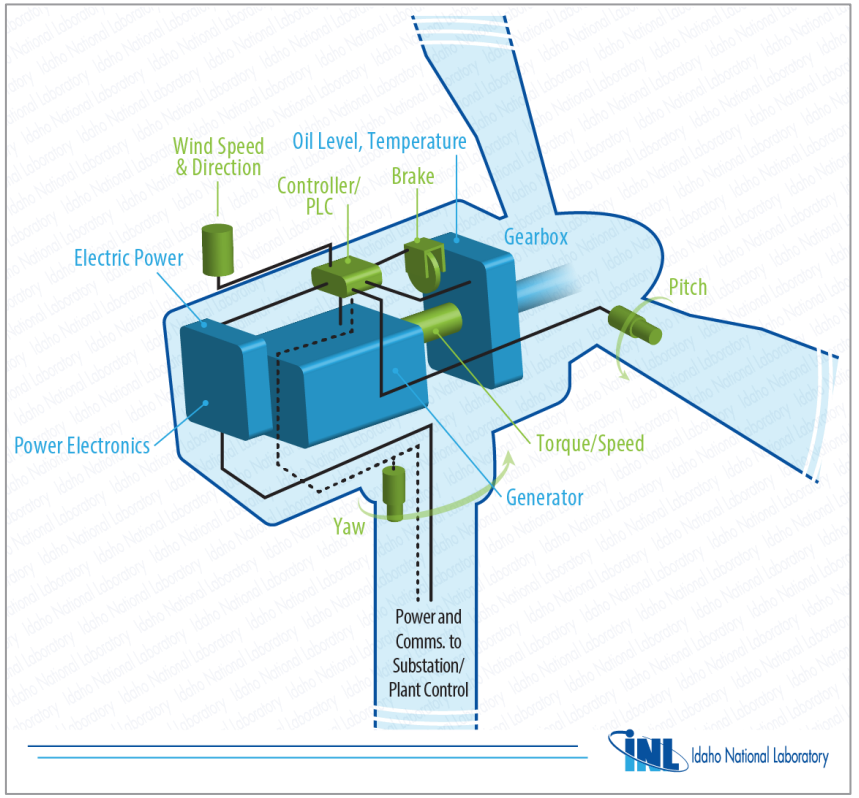


Increase of wind turbine sizes and power generation [2]

Representative Wind Plant Architecture

Representative architecture helps provide baselines to discuss cybersecurity guidance and common attack vectors

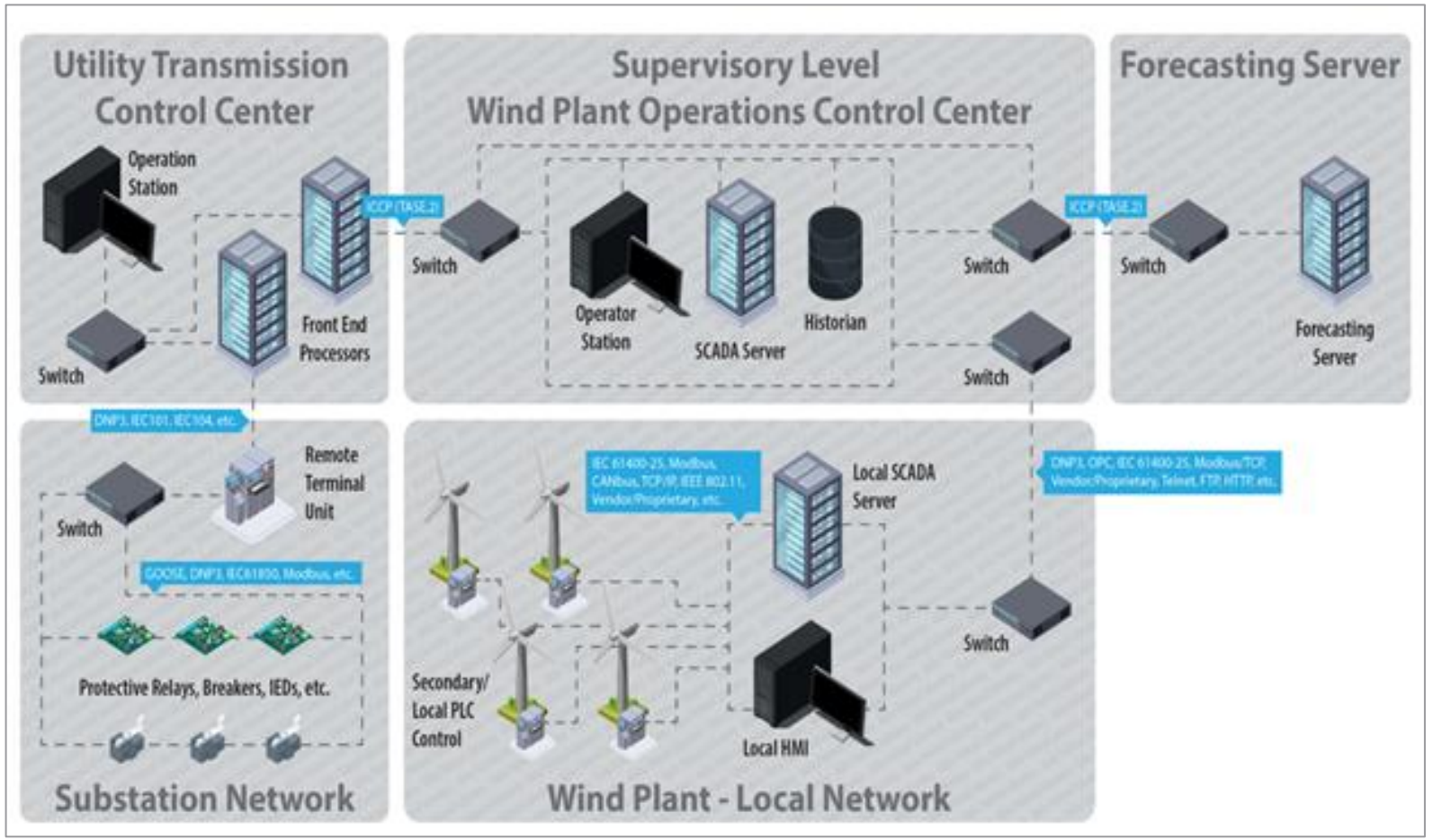




- Many components in wind turbines that are critical to device health and performance
- Points of interconnection aggregates individual turbines connected to the grid

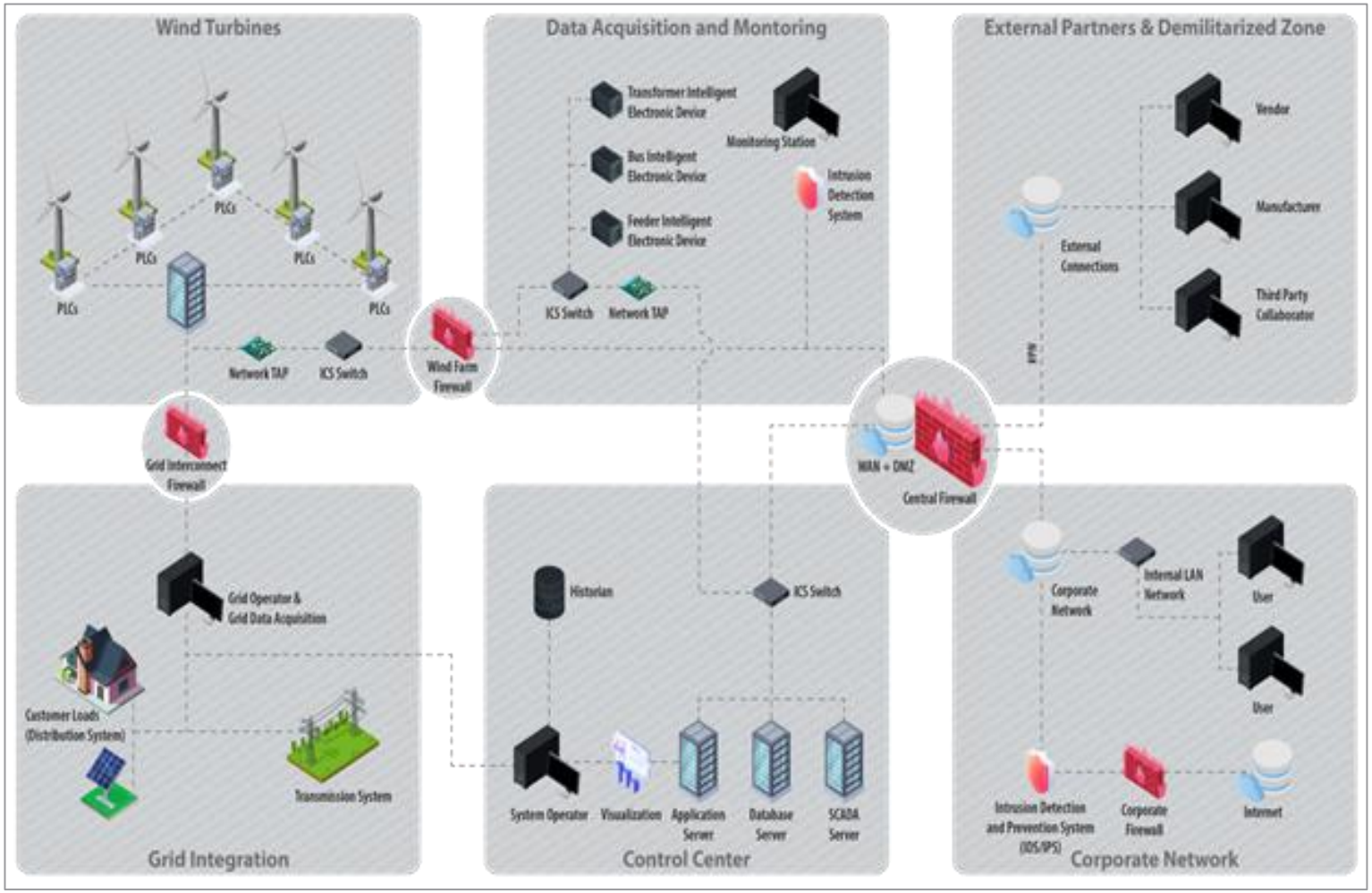
Collector Substation Communications

- Wind plant operations
  - SCADA control to downstream devices
- Transmission control
  - Upstream of PCC
  - Energy management protocols
- Segmented networks provide different levels of access and control
  - Traffic monitoring
  - Access control



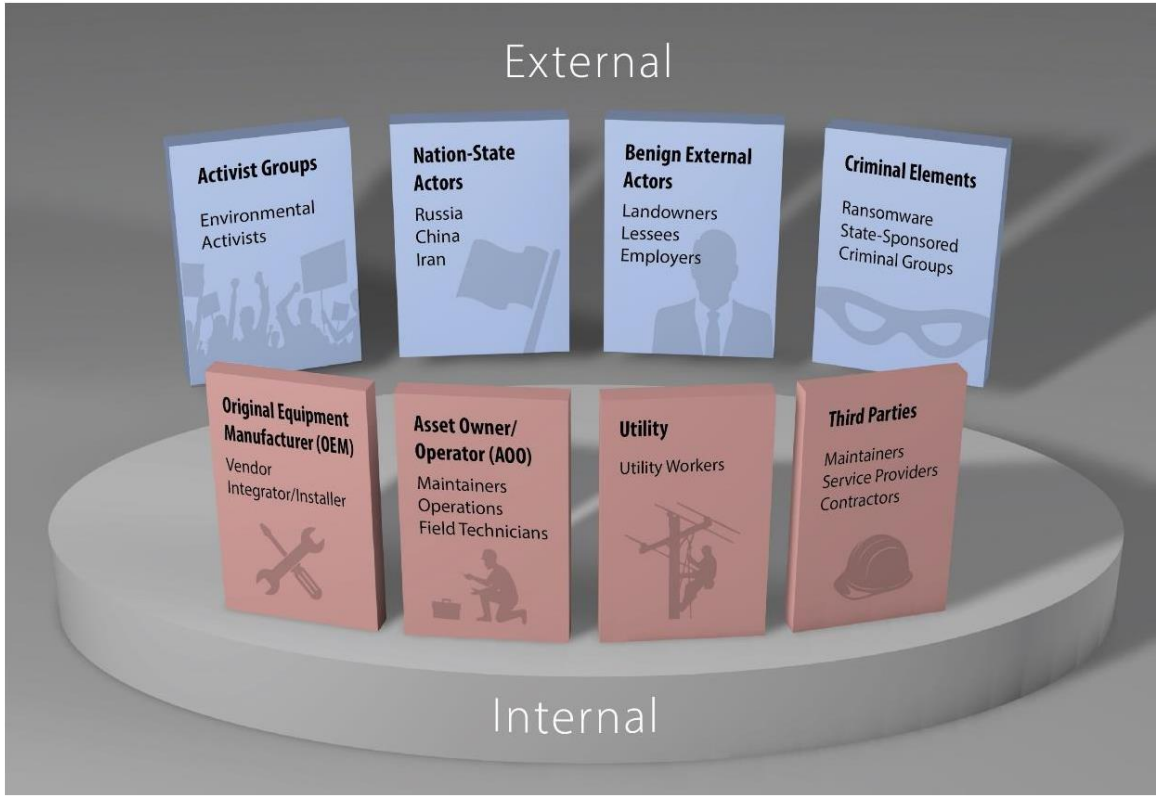
Internal and External Communications

- Multiple stakeholders need access to data
  - Turbine manufacturers
  - Wind plant operators
  - Utilities



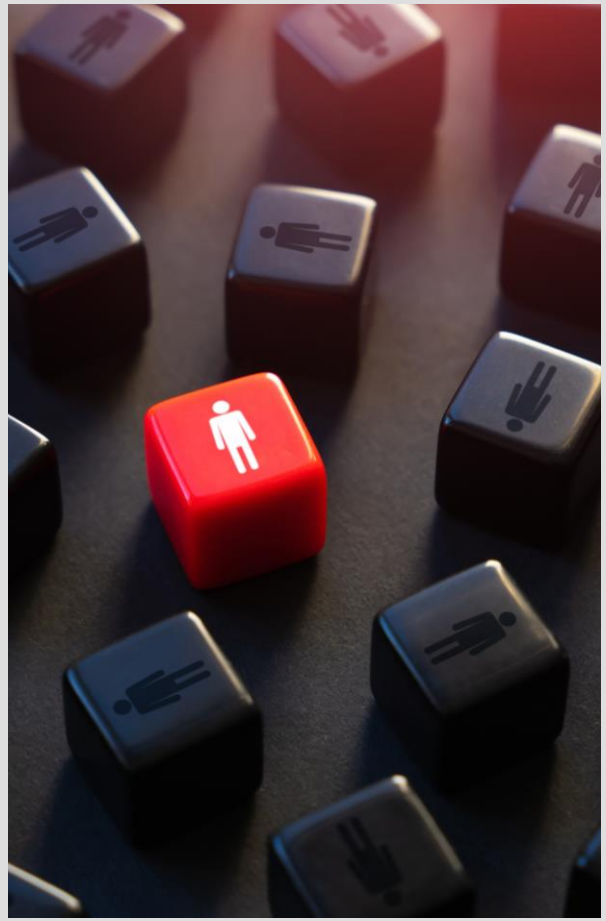
Types of Threat Actors and Cyber Adversaries

- **Threat** - Any event that may adversely affect an organization's ability to operate efficiently
- **Threat Actor** - Those who pose a threat to an organization
- A variety of different "actors" may interact with a wind site
  - Those involved in commissioning, maintaining, and operating a wind site
  - May have malicious or benign intent
- Added actors may increase the attack surface of a wind farm



Internal Threat Groups

- **Internal Threat Actor**
  - Entity that has or previously had legitimate access to wind plant operation, network, or applications
  - Has a role in normal business operations
  - Most have benign intentions, but could be compromised to act against the system
- Includes the following actors:
  - Asset owners/operators (AOO)
  - Original equipment manufacturers (OEM)
  - Utility
  - Maintainers and technicians
  - Integrators and installers
  - Third-party services and data collectors



Examples of Internal Threat Actors & Known Incidents

AOO	OEM	Utility	Maintainers	Integrators & other third-parties
• Disgruntled employee • Phishing victim	• (March 2022) Nordex SE hit by ransomware • (Nov. 2023) Vestas hit by ransomware	• (May 2023) Danish utilities compromised by coordinated attack, forcing islanded operations	• (2018) U.S. technician accidentally downloaded malware from hotel, later plugged into wind plant network and turbines stopped working.	• SaaS providers • Data collectors • Installers • Developers

External Threat Groups

- **External Threat Actor**
  - Does not directly support wind plant operations
  - May gain knowledge of system through reconnaissance
- May have benign or malicious intentions:
  - Benign
    - Landowners
    - Lessees
    - Workers with physical access
  - Malicious
    - Activist groups
    - Criminal elements
    - Nation-state actors

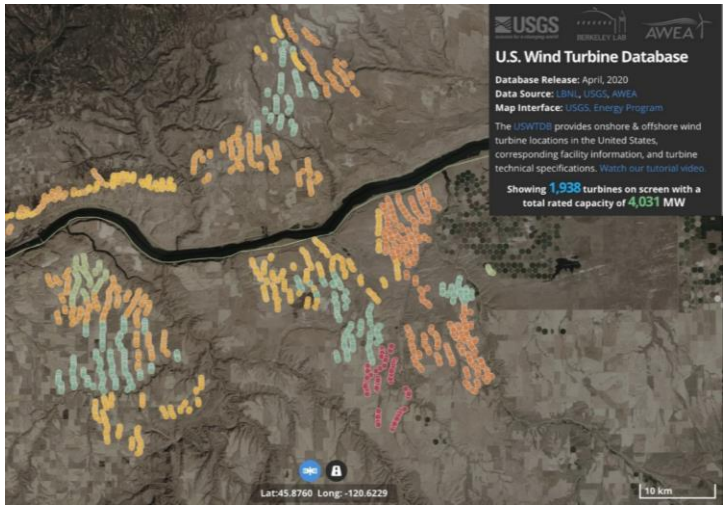
Examples of External Threat Actors & Known Incidents

Benign external actors	Activist groups	Criminal organizations	Nation-state actors
• Landowners • Land tenants • Land staff • General public	• (2019) Anti-wind protestors in Hawaii disrupt construction • Rise in eco-terrorist attacks in Europe	• Ransomware groups affected 3 wind companies within 6 months • Exploiting known vulnerabilities • Ex: (2019) IPP sPower affected by denial-of-service on comms equipment	• Reconnaissance activity and advanced persistent threats (APTs) • Russian attack on SATCOM infrastructure affected 5800 turbines • Chinese espionage targeting offshore wind in Strait of Taiwan and India

Attack Vectors

Physical Access

- Physical wind turbine generator (WTG) access
  - Takes time to respond to intrusions



Cyber Access

- VPN exploitation
- Wireless
- Temporary access points
- Pivoting from enterprise network

Transient Access

- Authorized external devices
- Infected technician equipment

Impacts

- Wind asset health and damage
- Loss of remote monitoring
- Power system stability

Critical failures can lead to severe physical damage.

Comprise of large wind sites may have huge impacts on the sites themselves, and even other connected devices.

- Ancillary services
- Power dispatch
- Reputational damage

Use Cases with MITRE ATT&CK

- **Industroyer** – Power delivery disruption
- **sPower DoS** – Firewall vulnerability exploitation
- **PoetRAT** – Discovery of a reconnaissance tool
- **ViaSat DoS** – Destruction of wind turbine monitoring hardware
- **Chinese Reconnaissance Activities** – Wind farm supplier attacks
- **European Ransomware Attacks** – Russian supporters target wind farms

INDUSTROYER

S·POWER
An AES and AIMCo Company

Viasat

MITRE

Industroyer (2016)

UKRENERGO

- Designed to disrupt electrical substation ICS
  - Modular
  - Very adaptable
  - Targeted IEC 60870-5, IEC 61850, and OPC protocols
  - Easy to implement for other protocols like DNP3
- Disrupted power delivery
- Industroyer2 (2022)
  - More configurable
  - Accompanied by wipers to destroy evidence of attack
  - Discovered before attacks could disrupt power delivery

Takeaways for wind:

- Adversaries possess means to disrupt power delivery
- ICS malware is increasingly more modular

MITRE ATT&CK

- Valid Accounts (T0859)
- Manipulation of Control (T0831)
- Denial of Service (T0814)
- Loss of Safety (T0880)
- Theft of Operational Information (T0882)

sPower Denial-of-Service (March 15, 2019)

- Utah-based independent power producer sPower
- Known vulnerability exploited in Cisco firewall
  - Forced firewalls to reboot repeatedly
  - 5-minute interruptions occurred repeatedly over 12-hour period
- Disabled communication to generation sites
  - Loss of view to field equipment and generation sites
- Did not affect power generation
  - Thought to be a test or scan
  - Adversaries may not have known what they were affecting

Takeaways for wind:

- Effective patch management strategies key
- Limit exposure of internet facing devices
- Note prevalence of IT infrastructure in the OT environment

MITRE ATT&CK

- Exploit Public-Facing Application (T0819)
- Denial of Service (T0814)
- Denial of View (T0815)

S·POWER
An AES and AIMCo Company

Denmark energy companies compromised in coordinated attack (May 2023)

- 22 energy companies, including small power and water utilities that operated wind and solar assets affected
- Unpatched vulnerabilities and zero-day exploits used
  - Some assumed new equipment was safe or that vendor was responsible for patching
  - Some deliberately opted out of updates due to maintenance charges
  - Some did not know exploited device was on their system
- Some organizations forced to disconnect from the internet and non-essential network connections
  - Caused lost connection to remote devices in certain cases
  - No material impact to energy operations

Takeaways for wind:

- Asset management critical
- Understand vendor agreements and responsibilities (both ways)

MITRE ATT&CK

- Exploit Public-Facing Application (T0819)
- Denial of Service (T0814)
- Denial of View (T0815)

PoetRAT (2020)

- Campaign included government and wind infrastructure targets in Azerbaijan
  - Deliberate attacks with unknown intentions
- Python-based remote access trojan (RAT)
  - Harvesting tools
  - Keyloggers
  - Screen captures
  - File stealers
  - System information collection tools

- Delivered using a Microsoft Word macro
- Continued reliance on spearphishing to gain initial access

Takeaways for wind:

- Early signs of reconnaissance should not be ignored
- Staff training remains critical

MITRE ATT&CK

- Drive-by Compromise (T0817)
- Spearfishing Attachment (T0865)
- Virtualization/Sandbox Evasion: System Checks (T1497.001)
- Non-Application Layer Protocol (T1095)
- Boot or Logon Autostart Execution: Registry Run Keys/Startup Folder (T1547.001)
- Automated Exfiltration (T1020)
- Video Capture (T1125)
- Screen Capture (T1113)
- Data from Local System (T1005)

ViaSat Denial-of-Service (February 24, 2022)

- Attack against the ViaSat KA-SAT network
  - Russian state-sponsored actors in attack coordinated with invasion of Ukraine
- DoS caused by an attacker exploiting a VPN appliance misconfiguration
  - Allowed for rewriting of flash on customer modems
  - Made the modems unable to access the network
  - Required replacement devices
- Caused loss of remote monitoring of 5,800 ENERCON wind turbines
  - 1217 wind farms, 10GW generation capacity
  - Customers relied on ENERCON's infrastructure – no backup links
  - Took almost two months to bring 95% of turbines back online

Takeaways for wind:

- Risk associated with reliance on third-party infrastructure
- Wind may be a casualty, even if not a direct target

MITRE ATT&CK

- External Remote Services (T0822)
- Remote Services (T0886)
- Denial of Service (T0814)
- Data Destruction (T0809)
- Loss of View (T0829)

Chinese Reconnaissance Activities (2022)

- Attacks were caused by the Red Ladon adversary group
- Phishing emails delivered a JavaScript based reconnaissance framework called ScanBox
- Targeted attacks against:
  - European equipment manufacturer that provided components to offshore wind farm in the Strait of Taiwan
  - Australian news outlets
  - Malaysia based entities
- Similar attacks by TAG-38
  - Entry point was third-party camera devices
  - Targets included North-Indian state load dispatch centers, nationa emergency response systems, and offshore wind infrastructure

Takeaways for wind:

- State actors have interests in targeting wind companies
- State actors recognize the strategic importance of wind generation

MITRE ATT&CK

- Phishing: Spear phishing Link (T1566.002)

European Ransomware Attacks

- Vestas (November 2021)
  - Cyber incident reported (widely believed to be ransomware – Group using Lockbit 2.0 took credit)
  - IT systems shut down across multiple business units
  - Data stolen, some personal data publicly released
  - Ransom not paid (“failed in attempt to extort”)
- Nordex SE (April 2022)
  - Conti ransomware
  - IT systems and remote access to managed turbines shut down to prevent spread
- Deutsche Windtechnik AG (April 2022)
  - Controlled shut down of remote monitoring for turbines
  - Regular activity restored within 3 days
  - Evidence found of Conti ransomware on IT systems

Takeaways for wind:

- Track reliance on third-party services and OEM access
- Ransomware continues to be prevalent, and indirectly impacts OT

Recommendations

Threat Information Sharing

Physical Security Events

- Unusual observation, suspicious activity, or surveillance of facilities
- Misrepresentation of affiliation
- Unmanned aircraft system (UAS) incidents, activities, regulations
- Theft, loss, or diversion of key safety or security items, systems and technologies
- Activist activities
- Expressed or implied threats
- Breach or attempted intrusion
- SCADA/control system anomalies coincident with a physical security event
- Gunfire damage or other vandalism

Cybersecurity Events

- Unexplained OT device behavior (e.g., freezes, reboots, or failures)
- Suspicious network traffic within a trusted environment or from a trusted partner's environment
- Suspicious interaction attempts against remote access solutions (VPN concentrators, jump boxes, remote email solutions, etc.)
- Unexplained internal or external login attempts
- Targeted phising activity with a well-defined purpose/objective
- Vulnerability probing and exploitation activity
- Malware delivered to or found in enterprise or operational equipment
- Any other analysis, insights, and forensic artifacts from incident response and threat hunting

References

[1] U.S. Energy Information Administration. "Wind Explained." Accessed August 8, 2023. https://www.eia.gov/energyexplained/wind/electricity-generation-from-wind.php.

[2] Office of Energy Efficiency and Renewable Energy. "Wind Turbines: the Bigger, the Better." Accessed August 8, 2023. https://www.energy.gov/eere/articles/wind-turbines-bigger-better#:~:text=The%20average%20capacity%20of%20newly,MW%20or%20larger%20also%20increased.

[3] Kelci McKendrick. "Cause of damage to 2 wind turbines near Helena being investigated." Enid News & Eagle. Accessed August 8, 2023. https://www.enidnews.com/news/local_news/cause-of-damage-to-2-wind-turbines-near-helena-being-investigated/article_7beb1b5c-09d9-11ec-af6b-eb6234c3a442.html

Idaho National Laboratory

Battelle Energy Alliance manages INL for the U.S. Department of Energy's Office of Nuclear Energy. INL is the nation's center for nuclear energy research and development, and also performs research in each of DOE's strategic goal areas: energy, national security, science and the environment.