INL/RPT-24-76133-Revision-0

Attack Surface of Wind Energy Technologies in the United States

January 2024

Sarah G. Freeman, Matthew A Kress-Weitenhagen, Jake P Gentle, Megan Jordan Culler, Megan Mincemoyer Egan, Remy Vanece Stolworthy

Changing the World's Energy Future

Idaho National Laboratory

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

INL/RPT-24-76133-Revision-0

Attack Surface of Wind Energy Technologies in the United States

Sarah G. Freeman, Matthew A Kress-Weitenhagen, Jake P Gentle, Megan Jordan Culler, Megan Mincemoyer Egan, Remy Vanece Stolworthy

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, DE-AC07-05ID14517

Idaho National Laboratory

INL/RPT-24-76133

Attack Surface of Wind Energy Technologies in the United States

Sarah G. Freeman
Matthew A. Kress-Weitenhagen
Jake P. Gentle
Megan J. Culler
Megan M. Egan
Remy V. Stolworthy

January 2024

Idaho National Laboratory

CYBERCORE integration center

TABLE OF CONTENTS

ACRONYMS **4**

EXECUTIVE SUMMARY **5**

REPRESENTATIVE WIND PLANT ARCHITECTURE **7**

Electric Connections 8

Wind Plant Communications 8

Collector Substation 9

External Communications 10

Protocols 11

THREAT ACTORS AND CYBER ADVERSARIES **12**

Internal Threat Groups 13

External Threat Groups 16

POTENTIAL ATTACK VECTORS **17**

Physical Access 18

Cyber Access via OEM or Trusted Third-Party Infrastructure 19

Transient Cyber Assets 19

IMPACTS **20**

Wind Asset Health and Damage 20

Loss of Remote Monitoring 20

Power System Stability 20

Ancillary Services 21

Power Dispatch 21

Reputational Damage 21

USE CASE: INDUSTROYER IN UKRAINE 2016 ..... **21**

USE CASE: SPOWER AND FIREWALL VULNERABILITIES **23**

USE CASE: POETRAT AND STAGE ONE RECONNAISSANCE **25**

USE CASE: WIPER ATTACKS AGAINST VIASAT **26**

USE CASE: CHINESE RECONAISSANCE ACTIVITY **28**

BEST PRACTICES AND RECOMMENDATIONS **28**

Importance of Information Sharing 31

Resources for Incident Response 32

CONCLUSION **32**

TABLE OF FIGURES

Figure 1. Plant interconnection through collector substation. 7
Figure 2. Nacelle components. 8
Figure 3. Collector substation communications. 9
Figure 4. Internal and external wind-plant communications network configuration. 10
Figure 5. Internal and external threat groups 12
Figure 6. Columbia River wind plants. 18
Figure 7. Prioritized security controls for AOO. 30

ACRONYMS

APT	Advanced Persistent Threat
AOO	Asset Owner/Operator
AWEA	American Wind Energy Association
BES	Bulk electric system
C2	Command and control
Cal-CSIC	California Cybersecurity Integration Center
CESER	Cybersecurity, Energy Security, and Emergency Response
CIP	Critical infrastructure protection
CIS	Center for Internet Security
CIRT	Cyber Incident Response Team
CISA	Cybersecurity and Infrastructure Security Agency
CSIS	Center for Strategic and International Studies
DHS	Department of Homeland Security
DMZ	Demilitarized Zone
DOE	Department of Energy
DoS	Denial of service
DNI	Director of National Intelligence
EERE	(DOE Office of) Energy Efficiency and Renewable Energy
EIA	Energy Information Administration
E-ISAC	Energy Information Sharing and Analysis Center
FBI	Federal Bureau of Investigation
FTP	File Transfer Protocol
ICS	Industrial control system
INL	Idaho National Laboratory
IT	Information technology
LAN	Local Area Network
NERC	North American Electric Reliability Corporation
NERC CIP	NERC Critical Infrastructure Protection
OEM	Original Equipment manufacturer
OLE	Object linking and embedding
OPC	OLE for Process Control
OT	Operational technology
PAC	Programmable automation controller
PCC	Point of common coupling
PLC	Programmable logic controller
PoC	Point of connection
RAT	Remote access trojan
RTU	Remote terminal unit
SaaS	Software as a service
SCADA	Supervisory control and data acquisition
SME	Subject matter expert
TLS	Transport-layer security
U.S.	United Sates
VPN	Virtual Private Network
WETO	Wind Energy Technologies Office
WTG	Wind turbine generator

EXECUTIVE SUMMARY

The United States (U.S.) National Cyber Strategy, released in March 2023, highlighted the growing threats and risks that American critical infrastructure faces in cyberspace, stating:

> *The governments of China, Russia, Iran, and North Korea are aggressively using advanced cyber capabilities to pursue objectives that run counter to our interests and broadly accepted international norms. Their reckless disregard for the rule of law and human rights in cyberspace is threatening U.S. national security and economic prosperity [0]*

China and Russia have become more sophisticated in their attacks and likely possess the means to put the U.S. energy sector at risk. According to the U.S. Intelligence Community's Annual Threat Assessment, "China almost certainly is capable of launching cyber-attacks that could disrupt critical infrastructure services within the United States" and presents the broadest, most active, and most persistent cyber espionage threat to U.S. entities.[2] Similarly, Russia is "particularly focused on improving its ability to target critical infrastructure, including … industrial control systems (ICS), in the United States as well as in allied and partner countries, because compromising such infrastructure improves and demonstrates its ability to damage infrastructure during a crisis."[2] Although a lesser threat than China and Russia, Iran has also targeted critical infrastructure when opportunities arise, making them a greater threat to sectors with more-vulnerable assets.[2]

At the same time, the U.S. energy sector is in flux. Increasingly, renewable energy represents a core component of the U.S. national and regional generation capacities. According to the U.S. Energy Information Administration (EIA), the total annual power generation from wind assets in the U.S. increased from about 6 billion kilowatt-hours (kWh) in 2000 to about 380 billion kWh in 2021. It now represents 9.2% of the U.S.' total generation capacity.[3] With this growth, wind generation comprises an increasingly large part of the energy portfolio, which has seen a rise in attacks over the last five years. Multiple cyber-attacks and intrusions in 2022 targeted the wind-energy sector, including ransomware attacks on Nordex and Deutsche Windtechnik control centers, disabling SATCOM modems serving ENERCON wind turbines, and an espionage campaign against wind-energy companies working in the South China Sea.[4–7] As the percentage of power generation from wind assets grows, and attacks on the energy sector rise in complexity and frequency, cybersecurity for wind energy technology becomes increasingly and urgently important, consonant with its growing value as a target for cyber-attacks.

Low-cost, reliable electrical energy production from wind relies upon automation and control systems, arguably more so than traditional thermal generation. These same systems, however, can serve as the target of adversaries' cyber-attacks. Idaho National Laboratory (INL), at the request of the Department of Energy's (DOE's) Office of Cybersecurity, Energy Security, and Emergency Response (CESER) and Energy Efficiency and Renewable Energy's (EERE's) Wind Energy Technologies Office (WETO), evaluated a generalized wind plant architecture to understand the classes of potential threat actors

and the vectors[1] that could enable a cyber-attack. This evaluation explores the attack surface of a representative wind plant, identifying potential methods and vectors that an adversary could leverage to conduct a cyber-attack. Included in this assessment are some recommended mitigations and approaches. Each recommendation requires a full security evaluation, cost/benefit analysis, and risk analysis by each owner and operator.

[1] An *attack vector* is the means by which an adversary gains access to the victim's network or systems and delivers a malicious payload. In contrast, an *access vector* refers only to how an adversary gains access to a vulnerable system or network. The relationship between access and attack vectors is mirrored in other threat intelligence terminology, such as Computer Network Exploitation (CNE) and Computer Network Attack (CNA), where CNE refers to an adversary gaining access and CNA refers to an adversary causing a malicious impact.

REPRESENTATIVE WIND PLANT ARCHITECTURE

The design diversity of wind plants' automation and control systems makes sector-wide cybersecurity risks, mitigations, and regulations challenging. Wind plants can differ in terms of size, generation capacity (e.g., number and size of turbines), network design, communications protocols, control center structure (e.g., unique control center per wind plant or a centralized hub), maintenance practices, and geographic locations (e.g., offshore or onshore, geographically remote or easily accessible). Due to these variations, establishing a common set of security requirements is not possible; however, general security guidance can be shared.

A representative wind plant architecture is helpful, not only to identify relevant security guidance, but also to characterize common access and attack vectors and describe potential attack surfaces. An attack surface is defined as the sum of exposed systems, networks, or other cyber assets that an adversary can target to gain access to and, ultimately, cause a malicious impact. Representative architectures and their associated attack surfaces can help identify attack scenarios and counterstrategies. This section includes a representative wind plant architecture developed by INL, based on past wind plant assessments and academic research (Figure 1). It is not intended to be all-encompassing; rather, it serves as a basis for collective foundational understanding about how adversaries could target wind technologies within the U.S.

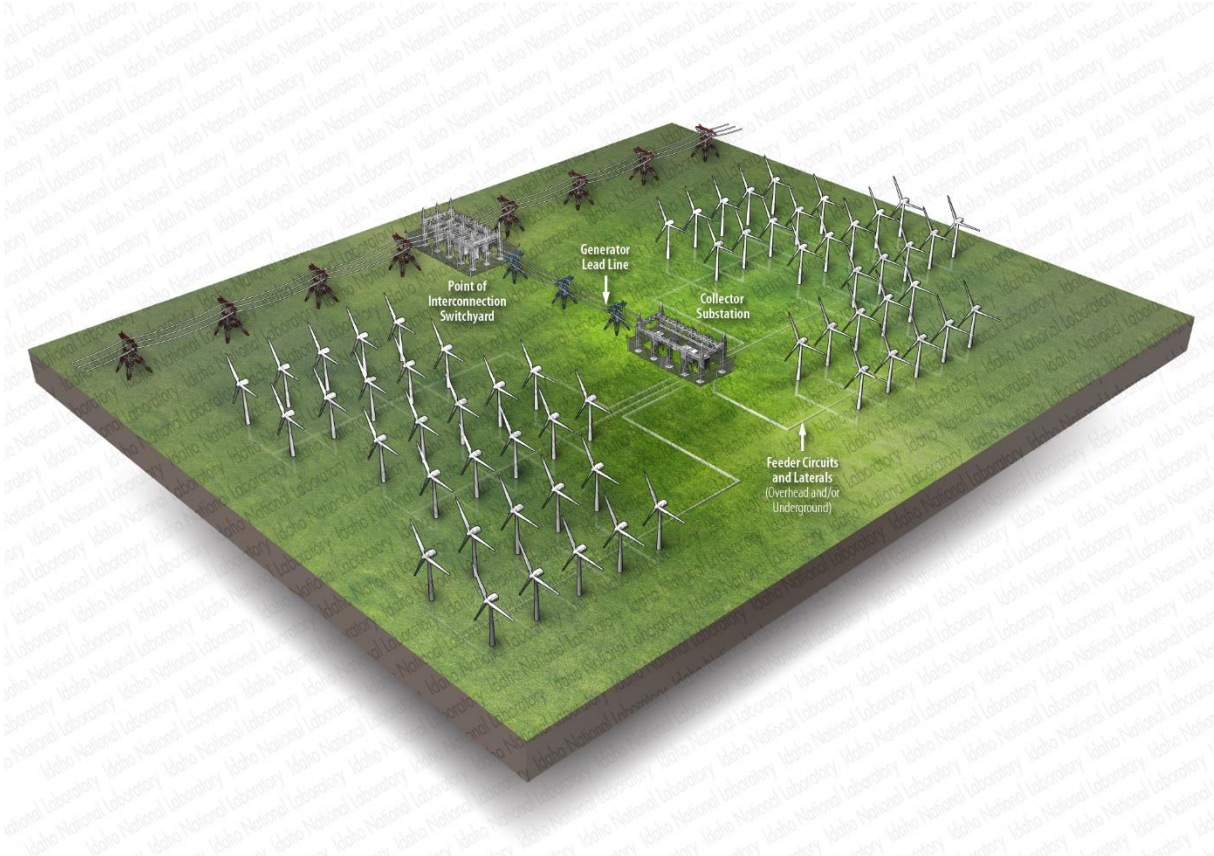


Figure 1. Plant interconnection through collector substation.

Electric Connections

Wind plants generate electricity through the conversion of rotational kinetic energy and can be made up of a collection of wind turbine generators (WTGs), a collector substation (or substations), and/or the necessary transmission (or sub-transmission) lines.[8] Wind plants can be connected to transmission or distribution feeders, but most wind plants likely to be valuable targets in a cyber-attack are large enough to be connected via transmission to the bulk electric system (BES).[9] Step-up transformers can be used to convert the output voltage from the WTGs to an appropriate level for transmission. This process would occur at the collector substation, as seen in Figure 1.

Digital control equipment for power production, weather sensing, and nacelle operation, such as programmable logic controllers (PLCs) or programmable automation controllers (PACs), is often housed in the WTG nacelle (see Figure 2) but may be found in the tower base as well.[8]

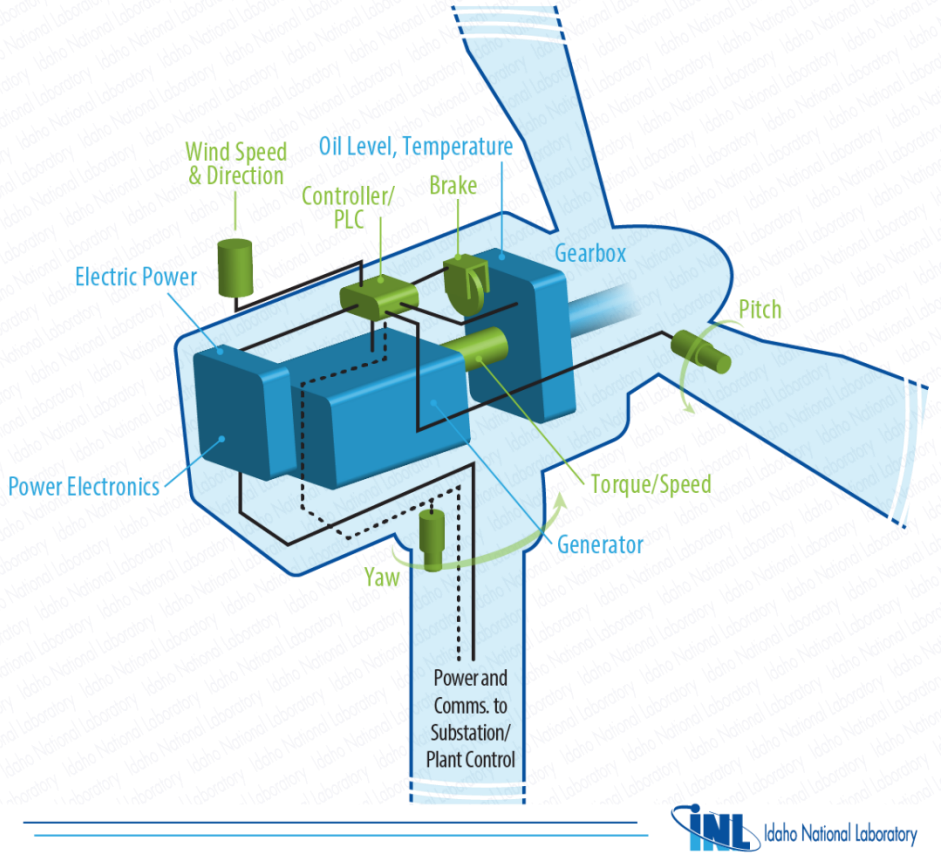


Figure 2. Nacelle components.

Wind Plant Communications

Fiber-optic communication lines typically run from the nacelle to the tower base before connecting to other WTGs and external communications infrastructure.[10,11] In many cases, these smaller WTG groups are connected together for increased resiliency of the communications infrastructure at the cost of creating a flatter operational technology (OT) network.[11] Frequently, these network designs are deliberately introduced to

reduce operational complexity; however, these designs can also benefit adversaries and allow them to move laterally throughout the wind plant.

Although not considered a standard practice, asset owner-operators (AOOs) can employ wireless technology throughout the nacelle, tower, and wind plant, instead of the more common fiber-optic communications infrastructure.[12] There are some operational benefits to this design, such as reduced deployment cost and greater flexibility, depending upon the choice of wireless technology (e.g. IEEE 802.11). The integration of wireless communication into the wind plant can enable additional cyber-attacks by expanding the attack surface of the wind plant and increasing the number of access points available to the adversary. The inclusion of wireless communications, including potential benefits and security implications, should be carefully evaluated on a case-by-case basis by the AOO. The wind power industry continues to research the efficacy of wireless communications.[13,14]

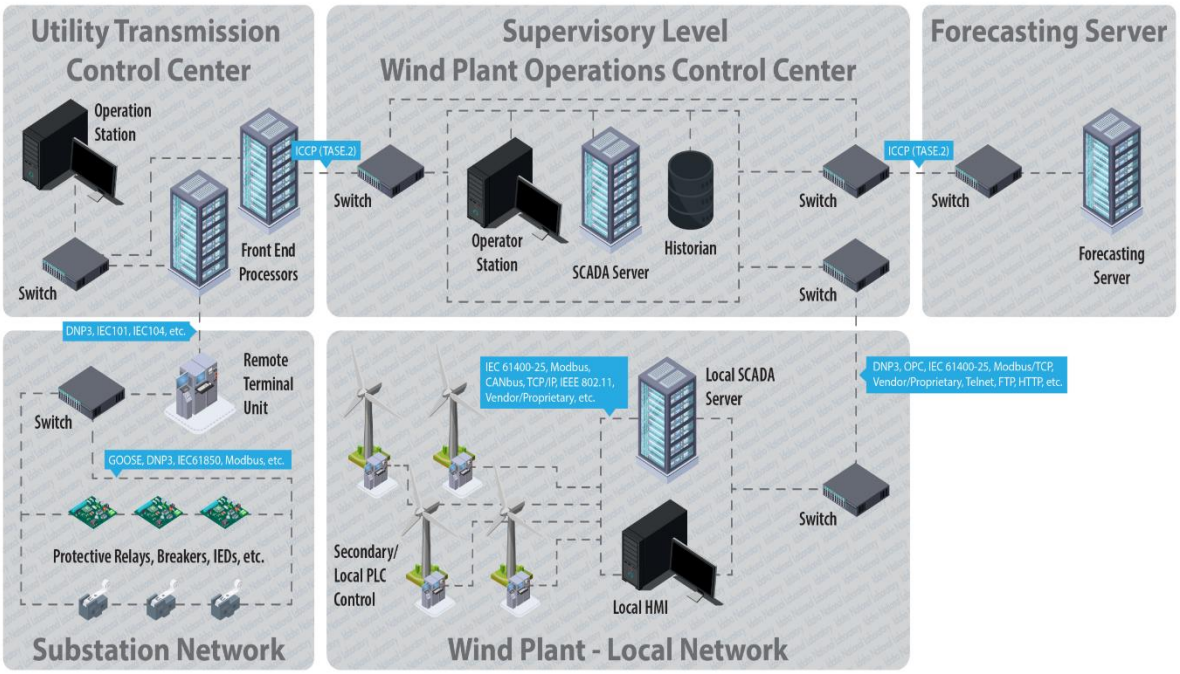


Figure 3. Collector substation communications.[Error! Reference source not found.**]**

Collector Substation

The collector substation typically has two physically and logically segmented networks: 1) wind plant operations and 2) transmission control (under regional power utility's control), both shown in Figure 3. Wind plant operations are typically limited to downstream of the point of connection (PoC), the point at which the wind units are electrically connected to the local power system. Transmission control typically occurs upstream of the point of common coupling (PCC), which is the point where the local power system is connected to the bulk power system. In some cases, the PoC and PCC are co-located; in other cases, there may be a larger local system that serves some local loads. Depending on the ownership and operation of the plant there may be less segmentation and separation between these networks.

The wind plant operations control center communicates with WTGs and supervisory control and data acquisition (SCADA) equipment in the field, using various SCADA and ICS networking protocols (e.g., Object Linking and Embedding (OLE) for Process Control (OPC), Modbus/TCP, vendor/proprietary, Telnet, File Transfer Protocol (FTP) or Hyper Text Transfer Protocol (HTTP) to enable remote control of assets. In contrast, the transmission control center relies on energy management protocols (i.e., DNP3 within the U.S.) to communicate with remote terminal units (RTUs), relays, circuit breakers, and other substation equipment. Outside of the North American grid, alternative protocols are used to communicate with substation equipment, most commonly IEC 60870-5-101 and 104.

External Communications

Wind plants require external communications for a variety of purposes. Data acquisition and monitoring are required for optimal operation of the wind farm and successful integration into the grid. Direct communication with the grid operator is also needed to ensure safe and reliable use of the wind plant power. This data, whether collected for the wind plant AOO or collected for the grid operator, will likely be stored in a control center, and used for short- and long-term planning. Vendors, manufacturers, and other external collaborators may also need access to data to provide device health monitoring, maintenance, or upgrade services. This level of data interconnection is not possible without eventually feeding through local area networks (LANs) and, eventually, to internet-facing corporate networks.

Figure 4 illustrates a typical architecture of these external communications, showcasing the complexity of data flow outside of a wind plant and emphasizing the involvement of numerous stakeholders. It also provides recommendations for the placement of

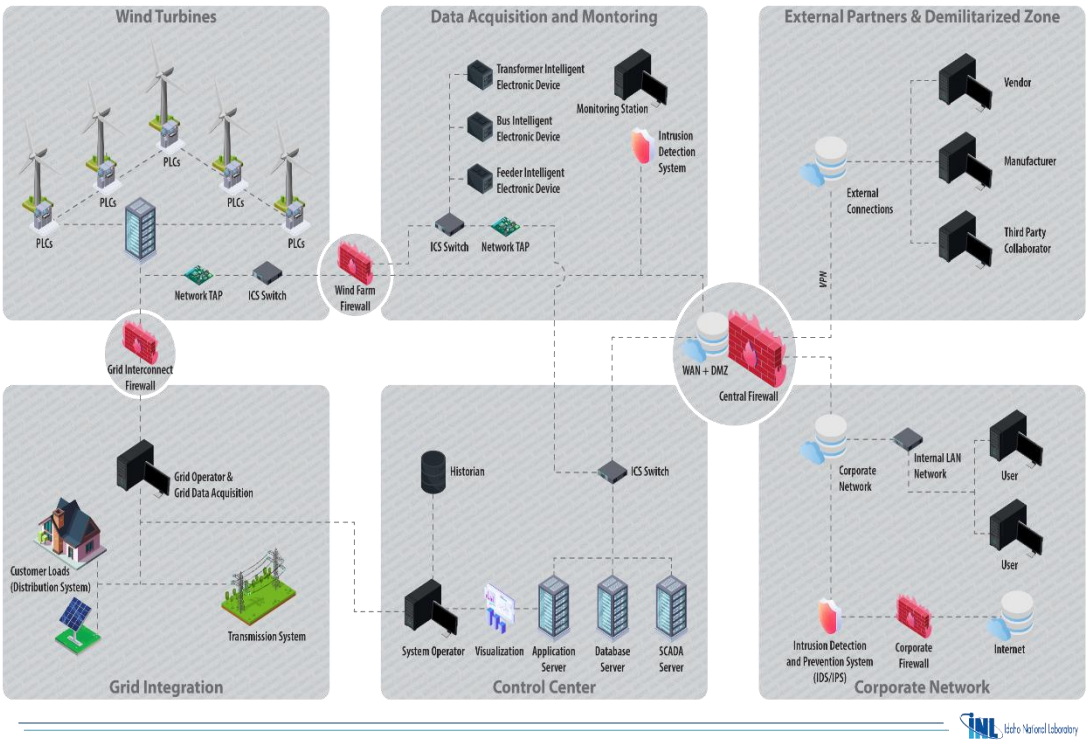


Figure 4. Internal and external wind-plant communications network configuration.

firewalls, intrusion detection systems, and demilitarized zones (DMZs) to ensure the difficulty for adversaries to access critical data or control functions.

Protocols

IEC 61400-25 is the communications protocol most commonly used in wind plant operations, though protocols used vary depending on manufacturer.[16,17] Based heavily on IEC 61850, IEC 61400-25 was developed to enable increased integration and data sharing with electricity control systems.[18] The primary goal was to define and standardize details required to connect the components of wind power plants in a multi-vendor environment and to exchange the information among all wind plant components. In the past, wind plants operated independently from larger grid operations and systems. The increased adoption of and reliance on wind power dictated a need for greater integration and control with the larger energy systems. The market growth and increasing number of manufacturers, integrators, and suppliers also intensified the need for a common framework.

IEC 61400-25 defines a common information model to share equipment and subsystem parameters and states throughout the system.[19] Common components of the WTG (e.g., wind turbine, control center, etc.) are structured as "logical nodes" storing data related to that component (e.g., status, settings, etc.). This information model is not limited to the wind turbine itself, but also includes additional systems in the wind plant, such as meteorological systems. The model was designed to be easily altered so that additional logical nodes can be added as needed. [19]

Additionally, IEC 61400-25 defines the required base communication services necessary to support various operational actions, including establishing a communication link, reading or writing variables, modifying setpoints, or sending commands to the WTG. These communication services also facilitate event monitoring and logging, which are critical for identifying malicious adversary behavior and conducting cyber forensic analysis after an attack.

The standardization of logical node structure provides adversaries the opportunity to query and communicate with the system just as a normal operator would. A motivated adversary, even one without substantial experience in IEC 61400-25, can learn to "live off the land" and use the existing and deployed infrastructure for malicious purposes.

IEC 61400-25 and similar protocols provide operational continuity at two levels. First, the health and status of individual WTGs are provided to the operations control system (sometimes referred to as the wind plant management system).[17] Second, data are also provided to the connected transmission operator through the wind plant collector substation.[20] The collector substation represents the larger grid interface, a transfer point for power produced by the WTGs. Depending on the individual wind plant design, these collector substations may be owned by the transmission operator, the AOO, or jointly. Irrespective of design, both the AOO and the transmission operator are provided production metrics (e.g., quantity of electricity generation per site) from the collector.

THREAT ACTORS AND CYBER ADVERSARIES

The commissioning, maintenance, and operation of wind plants involve various individuals or groups, collectively referred to as actors. These actors, along with others external to normal life cycle operations, may have benign or malicious intentions. In certain instances, actors who are typically benign may be coopted by malicious entities to facilitate the access or information collection required for a cyber-attack.

Any actor may represent a threat vector based on their role and access. Figure 5 provides a high-level delineation of responsibilities. The actors in the internal group will have authorized cyber and physical access to a wind plant due to their normal job responsibilities. In contrast, the external group does not, by definition, have authorized cyber and physical access to the wind plant assets. Some internal actors should only have access (either cyber or physical) to specific activities or contracts. For example, a field technician should only have access enabled while on contract for a particular wind plant. However, even after the contract ends, that technician will retain insider knowledge about the technologies, architecture, and operations of the plant. It is important wind plants acknowledge and track these individuals to ensure they do not retain more physical or digital access than needed.

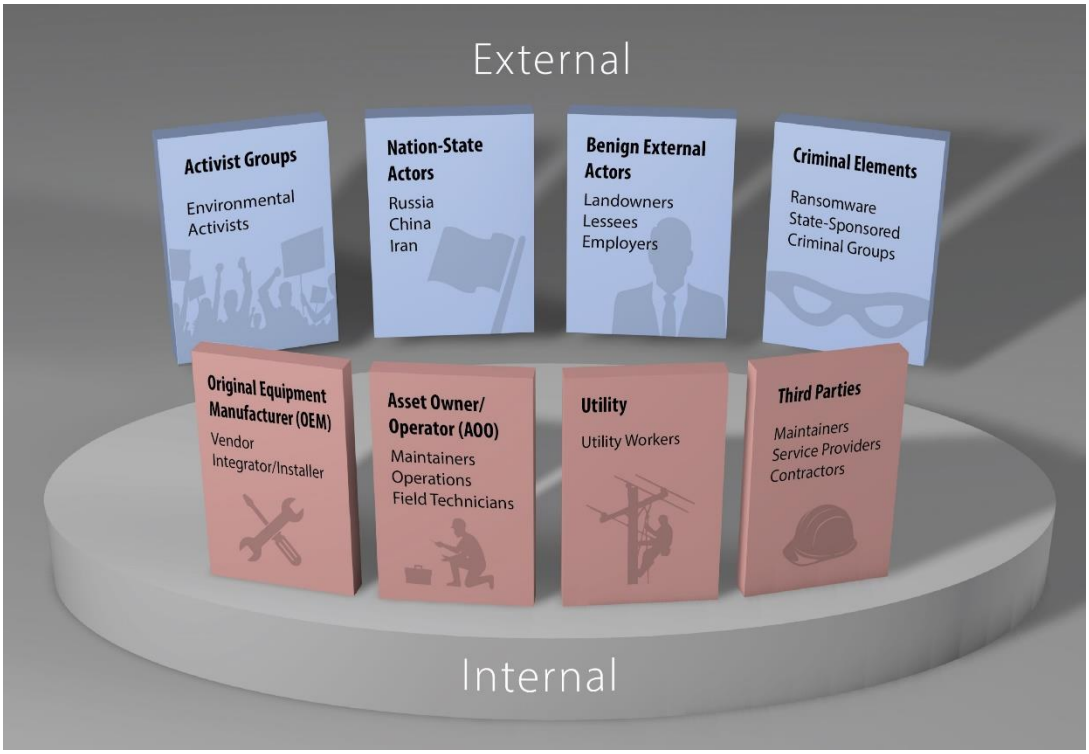


Figure 5. Internal and external threat groups.

AOOs should evaluate their processes and procedures for contracted entities (e.g., field technicians, original equipment manufacturers [OEMs], integrators). Topics for evaluation include the management of transient cyber assets, control of engineering design documentation, and network and control system equipment specifications (e.g., vendor, model, version of hardware and software). Transient cyber assets, as they are described in the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards, include equipment that periodically connects

(for less than 30 consecutive days) to bulk electric system cyber assets, a network within an electronic security perimeter, or a protected cyber asset. Examples include laptops or other data devices that are used for data transfer, vulnerability assessments, maintenance, or troubleshooting. These transient cyber assets are significant targets for cyber-attacks because they can introduce access or malware to otherwise segmented networks or equipment. They may not be directly managed by the AOO, but even if they are managed by third parties, OEMs, or other internal actors, the AOO should be aware of their purpose and enforce policies for how they interact with the system.

Internal Threat Groups

Any entity that either currently has or previously had legitimate access to the wind plant operations, network, applications, or other physical or cyber access to a wind plant is considered an internal actor. The internal actor has a role in the normal business processes for wind plant operations.

Asset Owner/Operator (AOO) or Aggregator

The wind AOO conducts the administrative operations of the wind plant, and its employees may have broad and varying responsibilities. An AOO fulfills the power sale contracts, maintains land lease agreements, and ensures daily operations and maintenance. By role, the AOO maintains both cyber and physical access to wind plant assets, but they also have the authority to delegate tasks and operations to other entities (e.g., asset owner contracts daily operation and operator subcontracts field equipment servicing). Through this delegation, the AOO may provide both cyber and physical access to trusted third parties. An aggregator serves a similar role to an AOO but may perform duties for multiple wind sites that may have different owners, collected at a single PCC.

While it is generally considered rare that an AOO or aggregator would become malicious, a few concerns must be considered with these groups. A disgruntled or bribed employee might be tempted to share critical information with outside parties that could be malicious. An employee may not even intend to grant access to an outside enemy, but by clicking on a malicious phishing email may install malware that grants an adversary initial access into a wind system. It is said that the weakest link in security for most organizations is the people, and the people with the highest levels of physical and cyber access to a wind plant will be part of the AOO organization.

Original Equipment Manufacturer

OEMs design, build, and implement power production equipment for the AOO. This group also includes subcontractors supporting an installation during construction. In many cases, AOOs may contract with OEMs for long-term support and maintenance of their products, a relationship that may provide long-term remote access to the wind plant for OEMs (and their subcontractors). AOOs may also face certain warranty requirements for the purchased equipment that require that OEMs maintain regular or periodic access to the equipment. Finally, the adoption of big data analytics in the industry has also resulted in a number of OEM services for health monitoring of the wind plant and its equipment.

Personnel in this category — e.g., OEM employees, vendors under subcontract to the OEM, integrators — will have varying levels of cyber and physical access to the wind plant. Past years have witnessed the deliberate targeting of OEMs to gain access to the AOOs. In July 2018, the Department of Homeland Security warned that Russian

state-associated hackers have targeted the relationship between AOOs and vendors since 2016, gaining access to a number of U.S. utilities.[21] In one instance, the attackers used this connection to collect sensitive utility information, including network configuration and deployed equipment data (e.g., vendor, model, and version of hardware and software). More recently, in March 2022, turbine manufacturer Nordex SE was hit by Conti ransomware.[22] Turbines continued operating, and communications with grid operators were unaffected. However, Nordex Group disabled its own remote access to its turbines to ensure the attack could not spread. Given the adversary benefit in targeting OEMs, organizations should take extra precautions to limit the release of sensitive OT information and access.

OEMs may also be compromised via a supply chain attack. An adversary may start the attack by compromising the design, manufacturing, or shipping processes of the OEM. They may intentionally introduce a bug in software or plant a monitoring device in hardware. These attacks are dangerous because they take advantage of the trust relationship between an OEM and an end user. Organizations should include a supply chain review process as part of their vetting for new equipment or software.

Utility

The utility receives generated power from the wind plant through a collector substation connection, as depicted in Figure 1. Utility employees will likely have physical and cyber access to the systems at the substation during normal operations. This access may also grant them physical and cyber access to the wind plant assets, depending on the wind plant design. Normal business operations may include utilities sending requests to wind plants to provide grid services, such as voltage support. This gives them legitimate reason to send commands and ensures the existence of infrastructure to support access to wind farms, which could potentially be abused by a malicious adversary if the utility is compromised. Techniques of "living off the land," or using legitimate programs and tools with authorized access, are increasingly common from attackers, which makes detection more difficult.

Additionally, substation equipment vendors and OEMs will have knowledge of the equipment in use and may have remote access to the equipment based on contracts. Attacks that target utilities may have an impact on wind plants, even without wind plant architectures being the primary target. For example, in May of 2023, several Danish companies in the energy sector were compromised in a coordinated attack. Attackers gained access to some of the companies' ICSs, and several companies had to go into island mode operation.[23]

Maintainers and Technicians

Maintainers may be employed to serve diverse customers throughout a region, especially when asset owners in that area possess a limited number of turbines and are unable to appoint dedicated personnel for the maintenance of their wind fleet. Maintainers may be granted temporary remote or onsite access to the systems for routine maintenance or problem solving. These maintainers or technicians can be on both short- and long-term contracts. These short-term contracted technicians would retain insider knowledge but should not be considered authorized personnel outside of the contract period. INL subject matter experts (SMEs) have observed that short-term contracted field technicians will have authorized access to wind plant systems for the

duration of a contract (e.g., assigned to work at Wind Plant A one week and Plant B the next).

From a cyber threat perspective, maintainers may not be subject to security standards targeted at utilities, owners, or vendors. This has the potential to lead to avoiding best practices. Due to the nature of their work, they may also be granted elevated levels of access to wind plants. Depending on the access control policies of the host, this access may or may not be revoked when the technician is no longer on site. The equipment used by maintainers and technician and their access credentials provide normal access while onsite and under contract, but if this equipment is transient across different wind farms, it can present a higher risk as a cyber-attack access vector. The 2018 American Wind Energy Association (AWEA) Conference, highlighting an event in which a technician accidentally downloaded malware to a laptop while staying in a hotel. The next day, the technician plugged the same laptop into the wind plant network, turbines were infected with the malware and stopped working one by one.[24]

In April 2022's Deutsche Windtechnik AG event a company specializing in the maintenance of wind turbines was hit with an attack believed to be ransomware.[25] Like the Nordex Group ransomware event, Deutsche Windtechnik chose to shut off their remote monitoring connections to about 2,000 wind turbines, but reported that wind turbine operations were never in danger. Regular operations resumed within three days.

Integrator/Installers

Wind installers or integrators may be hired to design, build, or install wind plant systems. They often work closely with both the OEM and the utility. To execute their work, they need intimate knowledge of the system and privileged access to configure the system. An adversary may target an integrator or installer to steal information about a system, which could be used in a later compromise. Alternatively, if the installer still has access to the system after it is commissioned, they could be targeted by an adversary to use those privileges to compromise the system. Installer personnel onsite with access to wind farm networks present a similar threat and risk as maintainers and technicians on short-term contracts, described above.

Third-Party Services and Data Collectors

Third-party services may include data aggregators, software-as-a-service (SaaS) providers, cloud system providers, or communication providers. Third-party services are increasingly common, and most wind plants rely on at least one external service. Collecting data from wind turbines is critical to the business processes for many internal stakeholders. Data on performance and equipment health monitoring are used to run operations safely, minimize operating costs, proactively predict maintenance needs, and allow wind assets to participate in energy and ancillary service markets. SaaS providers may offer services to optimize wind plant output, collect data for health, performance, or other monitoring, or even provide security solutions. Depending on the nature of the services they provide, they may have access to sensitive field data or even a two-way communications link. Organizations should thoroughly vet their service providers, which may include setting requirements to do business and regular reporting from providers to ensure continued compliance with organizational policies. If an adversary gains access to large amounts of data aggregated together, they can learn valuable information about the equipment, operation, and performance of wind plants.

External Threat Groups

An external actor is considered any entity not supporting wind plant operations and outside the normal relationship topology for wind plant operations. External actors may gain knowledge of the system through open-source reconnaissance or probing of internal actors. The two types of outsider categories are benign and malicious.

Landowners (Benign)

Landowners lease property to wind plant asset owners for construction and operations. The property is only a portion of the overall amount owned by the landowner and, in most cases, is agricultural. As the landowner continues to plant the residual property, they and others involved in the landowner operations have incidental physical access to the wind plant.

These benign external actors may act as a threat even if they have no malicious intent. Landowners and their employees may accidentally damage equipment or underground lines during routine activities. AOOs can mitigate this threat by ensuring there are proper physical restrictions like fences protecting assets and assets that cannot be physically restricted are well-identified and protected.

Activist Groups (Malicious)

Activist groups have been noted to protest the development and commissioning of wind plants based on perceived environmental risks. As recorded in a June 2020 Energy Information Sharing and Analysis Center (E-ISAC) assessment, a group of anti-wind plant protestors in Hawaii disrupted construction during 2019, claiming that the proposed wind plant would result in noise pollution and migraines for nearby residents.[26]

On the extreme end of the activist spectrum, eco-terrorists can use violence or threats of violence to further their cause.[27] Europe has seen an increase in physical attacks on wind plants and wind generation operations over the last three years.[28] As organization within these groups increases, technological threats become another tool to further an environmental agenda. Due to a lack of data related to attacks against wind infrastructure, specific statistics on activist group attacks are not available.

Cyber & Physical Criminal Elements (Malicious)

Criminal element refers to malicious external actors who seek to damage or disrupt the wind plant operations for their own gain. Motivations for their criminal activity vary; they may exploit systems to gain information, create disruption, or cause damage. A growing threat from criminal elements is financially motivated cyber-attacks. Ransomware impacting ICS is on the rise because criminals know these systems provide critical services, and it is costly and damaging if systems are taken offline.[29] If adversaries can deploy ransomware on the right systems, AOOs are more likely to pay larger sums to get control of their systems right away rather than trying to remove the ransomware themselves, which takes significantly more time. Two European wind sector entities, maintenance company Deutsche Windtechnik and turbine manufacturer Nordex, were hit with ransomware in March and April 2022. Both attacks forced the companies to proactively turn off their remote communications to wind turbines, resulting in a loss of remote monitoring and control. It is not clear whether either of these companies paid a ransom or for how long remote communications were disabled.

Although the motives of financial gain, disruption, or damage may be the primary goal, disruption or damage to the wind sector, in particular, may not be the goal.

Ransomware or other denial-of-service attacks may be opportunistic or even affect accidental victims. For example, a denial-of-service attack of Utah-based renewable energy independent power producer sPower created interruptions to remote monitoring and control of generation assets, but it is believed that attackers may not have even known they were affecting power system operations. In another incident, thousands of wind turbines lost remote connectivity capabilities due to an attack on satellite communication modems primarily intended to affect Ukrainian military communications as Russia invaded, but had effects far beyond that goal. Both events are described in more detail later in this report.

Nation-State Actors (Malicious)

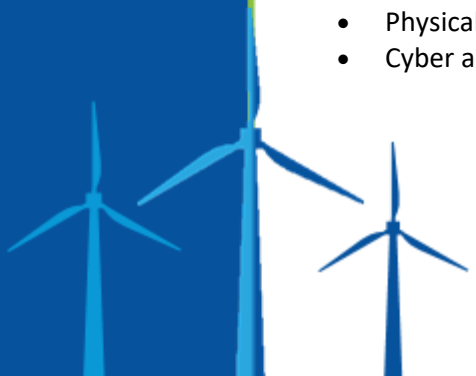
Nation-state actors and state-sponsored activities continue against energy sector and critical infrastructure targets. Nation-state actors are the most consequential threat against the U.S. electric sector although reporting does not currently indicate wind farms will specifically be targeted by these actors. The risks and threats to wind energy from nation-state actors are likely to increase as renewable energy plays a larger and more important role in the U.S. electric grid or if these assets can be used in grid-forming modes or for black-start requirements. Specific wind turbines or farms could also be targeted if they specifically support facilities or power requirements for national security-critical facilities, such as military bases.

Nation-state threat actors may employ a variety of different attack vectors, but AOOs should be particularly watchful for reconnaissance activities that are notably hard to detect and should conduct their own internal threat assessments to patch critical gaps in security. In 2022, China-based cyber threat actors known for espionage and reconnaissance activity targeted a European company involved in the installation and construction of an offshore wind farm in the Strait of Taiwan.[30] Nation-state actors are likely to employ cyber tactics in their attack but could also feasibly compromise an insider (either with or without the insider's knowledge) to gain privileged credentials, critical information, or even physically steal assets or carry out attacks. In other sectors, particularly in times of conflict, nation-state actors have also directly or indirectly supported criminals, private contractors and other non-state actors in conducting espionage and attacking targets to achieve the objectives of the state, increase resources, maintain deniability, and not risk burning key access vectors and custom malware or tools.[31,32]

POTENTIAL ATTACK VECTORS

As mentioned previously, attack vectors refer to the access methods employed by an adversary to gain initial access to a victim's network or systems and achieve a malicious effect. Based on the representative wind plant architecture and attack surface, INL researchers classified groups of attack vectors by 1) close, physical access, 2) remote, cyber-enabled means, or 3) blended cyber-physical attacks. Significantly, adversaries can use either physical or cyber access to enable attacks, as well as a combination of the two, known as blended cyber-physical attacks. Past research has defined access vectors that can be leveraged by an adversary to enable a cyber-attack.[17]

- Physical access at the wind turbine or collector substation
- Cyber access via remote connections



- Targeting of transient cyber assets (e.g., field technician maintenance equipment); this can be classified as a physical, cyber, or cyber-physical attack, depending on the method of compromise.

Physical Access

An individual wind plant may stretch tens of miles in remote geographical areas. For example, the Columbia River area near Kennewick, Washington, contains over 1,900 turbines spread over 1,000 square miles (Figure 6). The remote location increases the effort needed to respond to a breach of a WTG. Physically accessing the wind turbine or collector substation may allow an adversary to connect directly to physical equipment or to the wind plant or substation network. In either case, physical access can be leveraged to gather critical information to be used for future attacks. This access can also enable future attacks through the prepositioning of cyber tools. Additionally, an adversary could leverage insider knowledge or current physical access authorization to conduct cyber-attacks. An insider will possess substantial information gathered during operation and maintenance duties. For example, an insider would know plant layout, control system equipment and versions, and any security features that must be bypassed.

Currently, physical protection mechanisms are limited. Industry research is investigating the viability of adding physical intrusion detection mechanisms into the SCADA system for monitoring physical access to the WTG towers.[33]

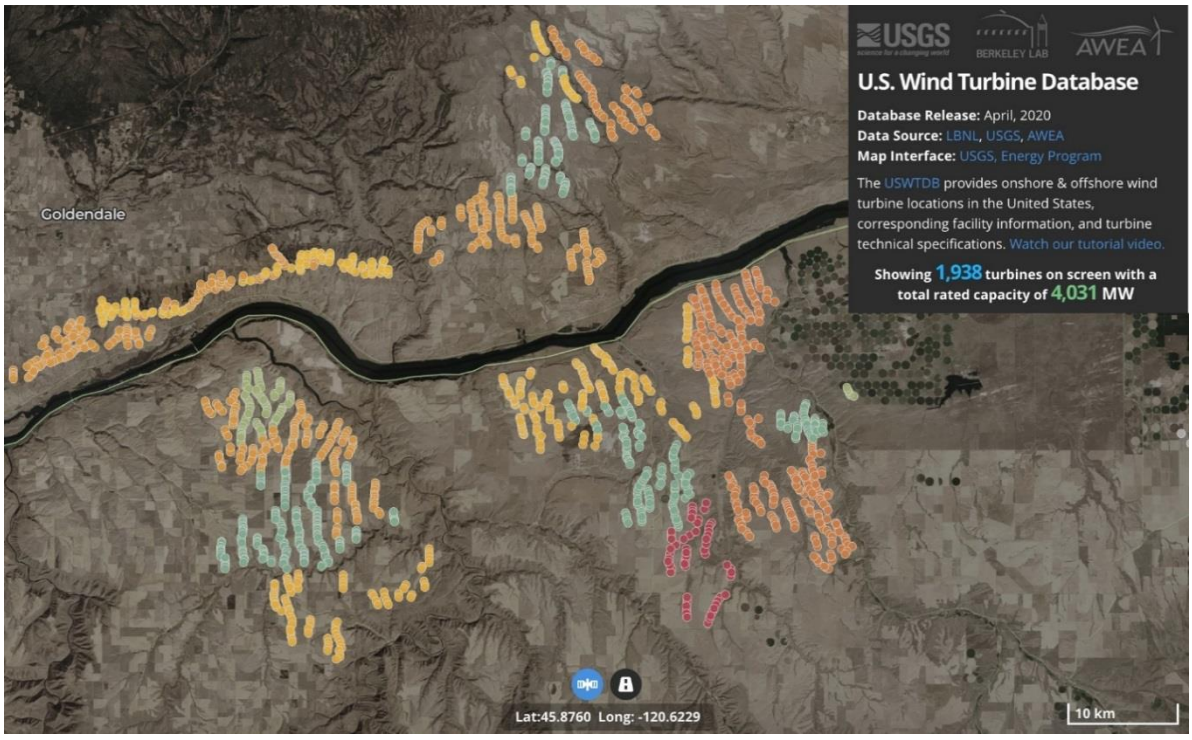


Figure 6. Columbia River wind plants.[34]

Figure 6 exemplifies the wide expanse of wind plant footprints. To put a perimeter fence around an individual wind plant would be prohibitively expensive. Therefore, wind plant asset owners integrate physical security into the tower, typically through the installation

of door locks at the WTG tower base. Implementations range from access control locks, which track authorized individuals, to simple padlocks.

Although WTGs may be geographically remote and spread out, physical access to the turbines can be easier than access to traditional, centralized generation facilities. Fences can easily be scaled, or gate locks cut. Doors to WTGs should be physically secured but may not always be. This necessitates that AOOs implement policies regarding physical monitoring and external devices. Controls such as blocking access to external devices (e.g. USBs) by default, adding cameras to WTG sites, and ensuring WTGs require unique passwords or locks can help mitigate the risk of physical access.

Cyber Access via OEM or Trusted Third-Party Infrastructure

Wind plant control networks are bespoke and custom-built to meet customer and OEM requirements. Many of the common components are described in Figure 4. INL researchers have observed individual virtual private network (VPN) connections as typical external methods of access for OEM, vendors, or asset owners. As noted by one researcher, in many cases, wind plant vendors and OEMs have unfettered remote VPN access to control networks for monitoring, software upgrades, and maintenance.[17] Alternatively, wind plant control networks can be accessed through direct connection equipment present in a WTG. Any of these components or connections can be targeted and coopted by an adversary.[35,36]

It is worth noting that this communication infrastructure may also include wirelessly connected devices. As previously stated, some unique market advantages accrue to wireless sensors and distributed systems. The extent of this practice or of an OEM implementing wireless technologies to eliminate wired data communications media like copper wire or fiber optics is not known. If present within the wind plant design, these wireless access point devices increase the attack surface of a wind plant and provide an alternative access vector for motivated adversaries. A cyber-attack impacting wireless communication devices can also cut off remote monitoring and control for AOOs, as happened when Viasat cellular modems were rendered inoperable by wiper malware. ENERCON and their customers lost access to 5800 wind turbines across central Europe. [6]

OEMs may also introduce temporary wireless access points during the construction and commissioning phases of a wind plant to accommodate internet connectivity prior to establishing the final communications infrastructure. INL assessment teams have observed that these access points are occasionally left behind for convenience by technicians. Due to the potential risk posed by such equipment, AOOs should validate that these devices are compliant with the organizational cybersecurity plan or make plans to remove them when possible.

Transient Cyber Assets

To aid in maintenance and operations, field technicians use authorized laptops with all the appropriate OEM software, production updates, and diagnostic tools for systems within the wind plant. The laptops introduce a cyber threat vector into the wind plant that may circumvent security protections on the wind plant network. These assets can be leveraged by adversaries to access and impact wind plant assets either deliberately (e.g., in the case of a disgruntled employee) or through attacks of opportunity (i.e., non-targeted cyber-attacks). A technician's compromised laptop could introduce malware to WTG systems, as a target of opportunity, due to out-of-date anti-virus definition files or

lack of operating system patching. Once systems are infected, potential effects may include malware propagation throughout the network, data encryption for ransom, or data destruction.[37] The most devastating potential effect results in cyber-physical damage.

The incident recounted at the 2018 AWEA WINDPOWER conference is a relevant example to consider, showing that a technician accidentally infected a field service laptop with malware after accessing the Internet for personal use. After the technician connected the infected laptop to the wind plant, the malware spread to several plant systems. [24] This incident highlights an attack of opportunity; although the wind plant likely was not the primary target of this malware campaign, it was designed to infect all vulnerable devices when presented with the opportunity. A cybersecurity researcher presented a similar hypothetical attack in 2017, noting that ransomware or destructive malware from a laptop can easily propagate through wind plant data communications.[38]

IMPACTS

The compromise of wind assets can have a wide range of impacts on the assets themselves and on the systems to which they are connected. The larger the wind plant size, the larger the impact will be on the connected power grid if there is a breach.

Wind Asset Health and Damage

One of the most obvious consequences of a wind plant breach is the potential for damage to wind assets. A physical attack could damage control systems or potentially even the tower or blades. A well-designed cyber-attack could cause a turbine to shut down suddenly, aging the braking system more rapidly than designed. A cyber-attack could even modify internal controls and force the system to exceed its (heat, speed, etc.) limits, which could cause immediate damage or age the hardware. A lot of planning goes into the development and operational plan of a wind plant. If the components do not meet their expected lifetimes, long-term plans for the generation sources of a transmission system can be affected, and short-term repairs can be costly.

Loss of Remote Monitoring

Incidents in the past five years have shown that loss of remote monitoring is one of the most likely effects of cyber-attacks on wind plants. Although it may not be the highest consequence impact, it has affected many types of stakeholders involved in wind operations, from AOOs to maintainers to OEMs. Interruptions can last from hours to days. While loss of remote monitoring typically does not affect the ability of the wind plant to generate power and interact with the BES, it is worth noting that as wind penetration increases, it will become more important to the stability and reliability of the grid, which will make timely and accurate access to data more important for all stakeholders. Additionally, if multiple stakeholders rely on common infrastructure (physical communication devices or cloud repositories and services), attacks on one stakeholder may have further reaching impacts.

Power System Stability

Beyond the scope of the local power system, the compromise of a wind asset can have far-reaching impacts on a transmission system. The sudden loss of wind generation,

whether through cyber or physical attack, can cause a mismatch of power generation and load, creating voltage depression—or worse. If the quality of service decreases sufficiently, the system may have to drop loads in the short term and bring on more costly generation sources in the longer term.

Similarly, the compromise of other basic functions of a wind plant, such as curtailment, connecting when commanded, or disconnecting when commanded, can decrease the reliability of the system. For example, curtailing when load is high or failing to curtail when load is low can have destabilizing effects on the voltage of the connected system.

Ancillary Services

Having wind systems installed can provide services to the grid beyond meeting the immediate demand for power. Wind assets can provide voltage and reactive power support to the transmission system. The inverters may have the ability to act in grid-forming mode, or act as frequency support. Using wind to serve part of the demand can free up other low-cost sources to act as spinning reserve, which saves money. Additionally, wind plants can be part of microgrid designs, where if part of the transmission system is lost, the wind plant can stay online and continue to serve local loads. All these functions are important benefits of installing wind assets, so compromising these functions or making them unavailable would have adverse effects on the connected system.

Power Dispatch

A final factor to consider in the compromise of wind assets is the variable nature of the output of wind plants. While general daily and annual trends may be predicted, the exact output at a certain time is variable and dependent on a wide range of factors. This opens the system up to the possibility of a stealthier attack, particularly in the form of data manipulation. If an attacker is able to change the reported output of a wind plant, it can affect operational decisions made at the plant and transmission level. It could affect the decision to turn other sources on or off and could even lead to reliability problems like overloaded lines that cause tripping or blackouts. While this would take an extreme attack, it is a type of threat not considered for traditional generation sources. Thus, it deserves attention from wind operators.

Reputational Damage

A secondary impact of any cyber-attack on the wind industry is reputational damage. This can affect the victim organization, their partner organizations, and even the industry at large. For example, customers may not care that a loss in wind generation was due to a cyber-attack on an OEM; instead, they might blame the utility for the disruption. Frequent attacks or attacks of significant impact have the potential to damage the industry's reputation as a viable and reliable energy source, making it more difficult to deploy new installations and meet renewable energy targets.

USE CASE: INDUSTROYER IN UKRAINE 2016

In December 2016, Ukrainian transmission operator Ukrenergo experienced a cyber-attack at a single transmission substation north of the capital, Kyiv.[39] In contrast to a similar attack the year before, cyber forensic analysis indicated that the modular malware employed in the 2016 attack could have been used to conduct an automated

and synchronized attack against a much larger region.[2] The attackers used preprogrammed malware modules to communicate with electric grid equipment in the field.

Attackers designed Industroyer, a modular malware framework, to enable direct interaction with ICS equipment via commonly used industrial protocols: IEC 60870-5-101, IEC 60870-5-104, IEC 61850, and OPC.[40] Industroyers' modules were designed to enumerate the substation environment and attempt to change the state of substation equipment (e.g., closed breakers were opened, resulting in a disruption to power delivery). In April 2022, in the wake of the Russian invasion of Ukraine, a revised version of Industroyer again targeted a Ukrainian energy provider. The new version, Industroyer2, was limited to interactions with IEC 60870-5-104, but was discovered, according to the Ukrainian government, before it could cause any impact.[40] Industroyer2 was more configurable than previous versions, and along with this malware, several wipers were deployed with the intent of destroying data and evidence of the attack shortly after the malware was scheduled to execute.

Although several lessons can be taken from the attacks in Ukraine, a key one for wind industry AOOs is that the 2016 incident demonstrates adversaries already possess the means to disrupt renewable power delivery. As noted previously, many of these protocols are used extensively for electric grid substation control and operations. In the U.S., the most prevalent protocol to communicate with substations is DNP3; however, a similar DNP3 module would be trivial to implement. Given this reality, AOOs should monitor for odd behaviors in the collector substation known or suspected to be adversary preparatory actions prior to escalating attack operations. For example, OPC-enabled[3] devices can be limited to status updates only, restricting adversary manipulations.

Another lesson worth noting is the trend demonstrated in the progression of the Industroyer malware. ICS-focused malware is increasingly more modular, allowing attackers to adapt the malware for various targets, rather than custom development of malware that works only against a specific target or application. This is important to the wind industry, noting that commonalities in architectures, protocols, and tools may be valuable targets for adversaries.

Observed MITRE ATT&CK techniques[4] during this event include:

- **Valid Accounts (T0859):** Adversaries may steal credentials for services to access systems or bypass existing security controls.[41] Attackers employed valid accounts to remotely access substation infrastructure through VPNs in the 2016 attack.[42]

[2] Although widely reported as a "fully automated attack," INL investigation of cyber forensic information indicates that although the attack could have been automated, attackers instead used a web shell to interact with the victim's environment in real time.
[3] OLE OPC is a software communications standard to increase interoperability and enable communications with industrial hardware. OPC is implemented in multiple sectors, including energy, critical manufacturing, water and wastewater, among others.
[4] MITRE's ATT&CK and ATT&CK for ICS frameworks are useful for describing the actions an adversary may take to gain access to and exploit a victim's network and systems. The ATT&CK for ICS framework describes adversary activity across 12 tactics (initial access, execution, persistence, privilege escalation, evasion, discovery, lateral movement, collection, command and

- **Manipulation of Control (T0831):** Adversaries may manipulate physical process control within the industrial environment by changing setpoint values, tags, or other parameters.[43] The Industroyer malware included modules that allowed adversaries to send commands to open substation breakers, resulting in a power outage.[44]
- **Denial of Service (T0814):** Adversaries may perform denial-of-service (DoS) attacks to disrupt expected device functionality.[45] The Industroyer malware included a module that, when executed, rendered a specific series of Siemens Siprotec relays unresponsive. [44]
- **Loss of Safety (T0880):** Adversary actions may result in a loss of safety, either intentionally or unintentionally as a result of other adversary actions.[46] The Industroyer module dos.exe disrupts protective relay functionality, resulting in a loss of safety event.[44]
- **Theft of Operational Information (T0882):** Adversaries may steal operational information on a production environment, including human/machine interfaces or engineering workstations, as a direct mission outcome for personal gain or to inform future operations.[47] During the 2016 attack in Ukraine, attackers compromised the data historian in a substation environment, garnering critical information.[42]

USE CASE: SPOWER AND FIREWALL VULNERABILITIES

On March 5, 2019, the Western Electricity Coordinating Council reported a cyber event that caused "interruptions of electrical system operations."[48,49] Although the cause was not immediately apparent, it was later reported that Utah-based renewable energy generator SPower experienced several temporary disruptions in their communications infrastructure. After the event, cyber forensic analysis identified the disruptions were initiated when an unidentified remote attacker exploited a known vulnerability in a Cisco firewall, forcing multiple reboots of the device. As a result of the exploitation, the control center experienced a DoS condition and loss of view to field equipment and generation sites. These loss-of-view conditions were relatively short, around five minutes each, but the continued rebooting and DoS conditions recurred over a 12-hour period. According to NERC CIP guidelines, the victim of the cyber-attack, the control center, was a low-impact control center.[50]

control, inhibit response function, impair process control, and impact) and 81 techniques. Additional information can be found at: https://attack.mitre.org/and https://attack.mitre.org/techniques/ics/

Although this cyber-attack had no impact on electricity generation output, the event highlights some significant lessons for AOOs. First, the event emphasized the importance of effective patch management strategies—the vulnerability exploited in 2019 was previously disclosed. AOOs should closely monitor vendor patch releases and alerts and apply necessary security changes promptly. Similarly, by limiting the number and exposure of internet facing devices, AOOs can directly challenge specific techniques employed by adversaries.[5]

Second, this cyber-attack demonstrates the prevalence of traditional information technology (IT) infrastructure within the operational technology (OT) environment. Cyber-attacks targeting OT environments are not limited to purely OT and ICS targets. By disrupting IT and communications infrastructure, adversaries can impact the operations of critical infrastructure. In 2015 and 2016, an attacker (or attackers) used a similar technique to conduct DoS against serial-to-Ethernet converters located within the power distribution systems of unspecified Baltic states.[51] Similar to the SPower incident, the attackers did not initiate an outage, but their manipulations resulted in loss of view and challenged normal operations. These events highlight the need to ensure a limited and robust security perimeter wherever possible to decrease the attack surface.

Another more-recent example of this type of incident occurred in May 2023 in Denmark. Twenty-two energy companies, including small power and water utilities that operated wind and solar assets, were compromised via unpatched vulnerabilities and a few zero-day vulnerabilities in Zyxel firewalls.[52] In some cases, the affected organizations were forced to enter an islanded mode of operation, disconnected from the Internet and any other non-essential network connections. Some organizations lost visibility to remote connections for a time while they were dealing with the incident although there was no significant, material impact to energy operations.

This event underscores the importance of the effective patch management strategies mentioned previously. Some organizations assume that because a firewall is relatively new, it is safe, while other mistakenly assume that their vendor is responsible for patching.[52] Still others deliberately opt out of updates because, while the software is free, there is a cost from the vendor to maintain updates. Some organizations did not even know that the exploited device was on their system, either because they did not keep an asset inventory to track that information, or because a supplier had installed the device without their knowledge (it was installed as part of a camera system setup).

The various difficulties in patch management demonstrated by the Denmark events highlight that a key prerequisite to effective patch management is asset inventory, both hardware and software bills-of-materials. Identification is a key component in cybersecurity risk frameworks that enable future protection and mitigation components.

Observed MITRE ATT&CK techniques during these events include:

- **Exploit Public-Facing Application (T0819):** Adversaries may seek to leverage weaknesses on Internet-facing systems, programs, or assets to gain access to internal networks or initiate an unexpected behavior.[53] Cyber forensic analysis of

[5] Both MITRE ATT&CK and ATT&CK for ICS recognize the exploitation of Internet-facing equipment and systems as a technique used by several APTs. (See T1190: "Exploit Public-Facing Application" for additional information - https://attack.mitre.org/techniques/T1190/.)

logs following the sPower event indicate that a remote adversary exploited a previously identified and publicly known vulnerability in a vendor's firewall.[50]

- **Denial of Service (T0814):** Adversaries may perform DoS attacks to disrupt expected device functionality.[45] In March 2019, adversary exploitation of a vulnerability in a vendor firewall resulted in a DoS condition at the control center, during which operators were unable to communicate with field equipment.[50]
- **Denial of View (T0815):** Adversaries may cause a denial of view in an attempt to disrupt and prevent operator oversight on the status of an ICS environment.[55] Exploitation of a vulnerability in a vendor's firewall initiated a series of five-minute communication outages over a span of 12 hours, disrupting operators' view and communications with field devices during the SPower event.[56]

USE CASE: POETRAT AND STAGE ONE RECONNAISSANCE

In April 2020, Talos, Cisco's security team, published their analysis of a recently observed remote access trojan (RAT). Talos researchers named this Python-based malware poetRAT based on references to William Shakespeare within the code. Collectively, the poetRAT campaign represents typical stage one[6] reconnaissance: the malware included credential harvesting tools, keyloggers, screen captures, file stealers, and system information collection capabilities. Talos researchers found that the poetRAT campaign was interested in government and wind infrastructure in Azerbaijan.[57]

In October 2020, Talos researchers posted an update to their analysis. Since poetRAT was first discovered in February 2020, the malware authors adopted additional techniques to challenge reverse engineering of the components and identification of malicious activity. However, some aspects of the campaign persisted, such as the continued reliance on spearphishing to gain initial access to the victims.[57] Although this campaign focused on infrastructure outside of the U.S., AOOs must remain vigilant because these activities demonstrate recent and deliberate targeting of wind infrastructure and SCADA systems for information collection. The goals of this campaign remain unknown; however, such reconnaissance could enable future and more damaging cyber-attacks.

Observed MITRE ATT&CK techniques during this event include:

- **Drive-by Compromise (T0817) (*suspected*):** Adversaries may gain access to a system during a drive-by compromise, when a user visits a website as part of a regular browsing session. With this technique, the user's web browser is targeted and exploited simply by visiting the compromised website.[58] Security researchers investigating PoetRAT have hypothesized that victims may be enticed to visit malicious websites through social networking platforms.[57]

[6] SANS identifies Stage I of the ICS cyber kill chain as the stage in which adversaries conduct espionage and other information-collection activities, enabling future attacks. (Additional information can be found here: https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297.)

- **Spearphishing Attachment (T0865) (*suspected*)**: A variant of spearphishing, a spearphishing attachment includes the appending of malware to an email.[59] Security researcher analysis indicates that PoetRAT may be distributed as a Word attachment as part of a larger spearphishing campaign.[57]
- **Virtualization/Sandbox Evasion: System Checks (T1497.001)**: Adversaries may employ techniques designed to detect virtualization and analysis environments. Malware may be preprogrammed to check against a set of conditions. If any of these conditions are true, then the malware may revert to preprogrammed evasion techniques.[60] PoetRAT checks the size of the environment; if the environment is smaller than 62 GB, it assumes it is in a sandbox environment, overwrites the malware scripts, and deletes itself.[57]
- **Non-Application Layer Protocol (T1095):** Adversaries may use a non-application-layer protocol for communication between an infected host and a command and control (C2) server.[61] The PoetRAT uses transport layer security (TLS) over port 143 for communication with the C2 server.[57]
- **Boot or Logon Autostart Execution: Registry Run Keys/Startup Folder (T1547.001):** Adversaries may achieve persistence by modifying the registry or startup folder in Windows.[62] Security researchers observed several registry modifications, including an addition to RUN hive to enable execution on system startup.[57]
- **Automated Exfiltration (T1020):** Adversaries may exfiltrate data, such as sensitive documents, through the use of automated processing after they are gathered.[63] PoetRAT employs a module called dog.exe to exfiltrate files after they are modified by the user via an email account or a File Transfer Protocol (FTP) connection.[57]
- **Video Capture (T1125):** An adversary can leverage peripheral devices (e.g., integrated cameras or webcams) or applications (e.g., video call services) to capture video recordings.[64] The PoetRAT module bewmac records the victim's webcam.[57]
- **Screen Capture (T1113):** An adversary may take screen captures of a victim's system to gather information about the infected host and user.[65] The PoetRAT module, smile.py conducts screen captures of the victim's system.[57]
- **Data from Local System (T1005):** Adversaries may search local system sources such as file systems or local databases to find information of interest.[66]

USE CASE: WIPER ATTACKS AGAINST VIASAT

In February 2022, the Viasat-operated KA-SAT network and customer modems were targeted by a wiper malware deployed by Russian state-sponsored actors, resulting in the loss of remote monitoring and control of 5800 ENERCON wind turbines across Europe.[67] The attack began with high volumes of malicious traffic originating from several SurfBeam 2 and SurfBeam 2+ modems, temporarily knocking many modems offline. This attack lasted several hours, with other modems continuing the attack as Viasat worked to remove the malicious modems from the network. A second stage of the attack overwrote key data in flash memory on over 40,000 modems across Europe, causing these modems to go offline and preventing them from reconnecting for approximately 45 minutes.

To conduct this attack, the Russian state-sponsored actors exploited a VPN misconfiguration, allowing them to move laterally throughout the network and leverage management tools to communicate with and overwrite data on customer modems. The U.S. and European governments assessed that "Russia launched cyber-attacks in late February against commercial satellite communications networks to disrupt Ukrainian command and control during the Russia invasion."[68] The attack was directed against a single Viasat subsidiary, Skylogic, which provides wholesale broadband services in Europe on Viasat's behalf.[69] It did not impact Viasat's other customers using the KA-SAT network or any of their other worldwide services. However, this attack does show the complex nature of satellite communication ownership and operations which are typically wholly outside of an end user's control, subjecting customers—including wind farm AOOs—to any risks present in multiple third-party company operations.

The modems impacted by the attackers included those in 5800 turbines manufactured, monitored, and controlled by German company ENERCON. These modems facilitated ENERCON's SCADA system communications, so when the modems went offline, ENERCON and their customers lost remote monitoring and control capabilities, although the turbines continued to be operational. This attack exemplifies the wind industry's reliance on third-party communications providers for operations, which can be vulnerable to disruption even if the wind energy company is not directly targeted. ENERCON was able to recover 95% of the turbines within two months by replacing the SATCOM modems or restoring SCADA communications through long-term evolution (LTE)/mobile channels. As a result of the attack, ENERCON began offering LTE-based retrofit packages to address the identified challenge of backup communication links.[67]

Observed MITRE ATT&CK techniques during this event include:

- **External Remote Services (T0822):** Adversaries may leverage external remote services, such as VPNs, to gain initial access to networks.[70] In this case, a misconfigured VPN client enabled the adversary to gain a point of presence within Viasat and Skylogic's network.[69]
- **Remote Services (T0886):** Adversaries may leverage remote services and related functionality to move laterally through a network or networks.[71] Attackers leveraged legitimate remote management functionality intended to delivered software updates to the modems in order to deliver wiper malware and delete modem configuration data.[69]
- **Denial of Service (T0814):** Adversaries may perform DoS attacks to disrupt expected device functionality.[45] During the ViaSat attack, an increase of traffic from attacker-controlled equipment flooded network resources, disrupting communications from legitimate sources.[69]
- **Data Destruction (T0809):** Adversaries may choose to perform data destructive attacks via malware, tools or other non-native files, either to affect device operation or to destroy artifacts left by their operations.[72] Adversaries deliberately destroyed configuration files within customer-owned equipment so that these devices could not communicate with KA-SAT resources.[69]
- **Loss of View (T0829):** Adversaries may cause a sustained or permanent loss of view where the ICS equipment will require local, hands-on operator intervention—for instance, a restart or manual operation.[73] Wiping the SATCOM modems on the

turbines disrupted ENERCON's SCADA communications and inhibited both ENERCON's control center and its customers from being able to monitor or control the turbines. Remediation required technicians to replace the modems on all turbines without a backup communication method, such as a secondary cellular modem.

USE CASE: CHINESE RECONAISSANCE ACTIVITY

From at least April to June 2022, a cyber espionage campaign targeted companies involved with wind turbines in the South China Sea, among other victims, according to an August 2022 report from cybersecurity research company Proofpoint and consulting firm PwC's joint threat intelligence teams. The threat actors used phishing emails, often posing as a fictional media company, the "Australian Morning News." and would send a URL to a malicious domain that delivered the ScanBox malware framework. Targets included "heavy industry and manufacturers responsible for the maintenance of offshore wind farms [and] manufacturers of installation components used in offshore wind farms."[74] This campaign was attributed to a threat group called Red Ladon, a "China-based, espionage-motivated threat actor" that overlaps with Advanced Persistent Threat (APT) 40. Prior to this campaign, in late March 2022, Proofpoint observed the same group conducting phishing activities against a European equipment manufacturer, the components of which were used in the installation of an offshore wind farm in the Strait of Taiwan.[74]

The victimology of this campaign demonstrates that cyber threat actor have an understanding of how many entities are involved in wind energy generation and, particularly, that state-backed actors have are capable and see the value of targeting a broad swath of them. In this instance, the activity targeted multiple companies involved in the maintenance and installation of components in offshore wind farms.[74] Furthermore, the Chinese threat actor recognized the strategic importance of wind energy generation in the South China Sea and information gained from this espionage campaign about the project's build specifications and operational details of companies involved could transfer to U.S. wind energy sector entities in the future.

Observed MITRE ATT&CK techniques during this event include:

- **Phishing: Spearphishing Attachment (T1566.001), Spearphishing Link (T1566.002):** Adversaries may send spearphishing emails with a malicious link in an attempt to gain access to victims' systems. Spearphishing may also involve such social engineering techniques as posing as a trusted source.[75] In this case, the attackers frequently posed as a fictional media publication and sent a malicious Rich Text Format (RTF) attachments or provided a URL to the malicious website that would subsequently download their ScanBox malware.[74]

BEST PRACTICES AND RECOMMENDATIONS

The Center for Internet Security (CIS) provides a solid foundation for improving an organization's security posture. Although fundamentally IT-focused, many of these recommendations and defensive strategies can be applied to wind AOOs.[76] In 2019, SANS Technical Director of ICS/SCADA Education Programs Tim Conway expanded on these security concepts during the AWEA WINDPOWER Conference's cybersecurity

panel, Winds of Change.[77] Rather than attempt to address all 18 of CIS's security controls, INL cybersecurity analysts highlighted a select few for prioritization of limited security resources (Figure 7). All CIS security controls should be examined and used as applicable. By focusing on this smaller group of security controls, wind plant AOOs can quickly bolster their security posture:

- **Inventory and Control of Enterprise Assets (CIS Control #1):** AOOs should actively inventory, track, and manage all enterprise assets on the network connected to infrastructure. IT and OT networks should be continuously monitored to identify unauthorized or unmanaged assets within the environment.
- **Inventory and Control of Software Assets (CIS Control #2):** AOOs should actively inventory, track, and manage all software on the network to ensure that only authorized software can be installed and executed within both the IT and OT networks. AOOs should consider soliciting third-party security reviews of their networks and critical systems to identify potential weaknesses. This security control is particularly significant because adversaries will often spend substantial resources scanning target systems and networks to identify vulnerable software that can be exploited to gain remote access. Additionally, by identifying the most important software, AOOs can ensure that suitable backup copies of critical software are well protected and maintained.
- **Secure Configuration of Enterprise Assets and Software (CIS Control #4):** AOOs should record and track the configuration of mobile devices, laptops, servers, and workstations used throughout their IT and OT enterprise. Additionally, these organizations should also studiously implement a procedure to ensure change-management logs are maintained. Additional information on change management procedures can be gathered from NERC CIP-010-3, "Configuration Change Management and Vulnerability Assessments."[78] Configuration management is a critical step in the identification of malicious activity because it serves as a baseline against which versions of hardware and software can be compared. Ideally, AOOs with higher security maturity will also ensure that gold copies[7] of software and hardware are secured and maintained. A robust hardware and software gold-copy library can decrease the time required for recovery following a cybersecurity incident—for example if ransomware is introduced into the AOOs networks.

[7] Gold copies refers to the practice of maintaining clean, unadulterated, and unmanipulated copies of software and hardware.

Figure 7. Prioritized security controls for AOO.

- **Access Control Management (CIS Control #6):** AOOs should manage and track the ongoing operation's use of ports, protocols, and services on network devices to harden their devices and systems and limit the attack surface that is available to the adversary. A common tactic of cyber-attacks is to identify vulnerable remote services for targeted exploitation or to use uncommon ports and services for more-covert C2 channels following successful exploitation.
- **Malware Defenses (CIS Control #10):** AOOs should work to prevent and control the installation, spread, and execution of malicious applications, code, or scripts on enterprise assets. Focusing on the prevention, spread and execution of malicious applications is critical for maintaining protection of sensitive information, and sustaining the functionality of enterprise assets.

- **Network Monitoring and Defense (CIS Control #13):** AOOs should establish and maintain comprehensive network monitoring and defense strategies. This involves the implementation of sophisticated processes and tools to ensure continuous network surveillance. Intrusion detection systems (IDS) play a pivotal role in identifying and alerting upon unauthorized access. INL has partnered with the Department of Homeland Security's Cybersecurity Infrastructure Security Agency (CISA) to develop cutting-edge tools for network monitoring and defense. Released in 2021, the Malcolm network traffic analysis tool is an open-source solution that provides IT network administrators and AOOs greater visibility into their computer network traffic and improves their ability to detect anomalous system behavior.[79] This type of data is also incredibly helpful to personnel during incident response, should an attack occur.
- **Service Provider Management (CIS Control #15):** AOOs should develop a process to evaluate service providers who hold sensitive data or are responsible for an enterprise's critical platforms or processes. AOOs should ensure their providers protect platforms and data appropriately.
- **Incident Response and Management (CIS Control #17):** Wind industry AOOs, just like other critical infrastructure operators, should develop, implement, and train incident response procedures (e.g., plans, defined roles, training, communications, management oversight). Spending time beforehand developing and training incident response procedures can save time, money, and energy responding to a cyber event. Additionally, training empowers employees to respond to an incident quickly and efficiently.

Importance of Information Sharing

In July 2020, DOE's WETO introduced the Roadmap for Wind Cybersecurity, which outlines potential strategies to improve the robustness and resilience of wind energy in the U.S.[15] One core tenant of the roadmap is the creation of a wind cyber culture that encourages information sharing throughout the industry. In addition to establishing the recommended CIS controls, AOOs should also seek to establish collective sharing of observed threat activity, organization best practices, and defensive strategies, information that can improve the cybersecurity and resiliency of the industry.

In 2019, the E-ISAC provided guidance on the types of events that should be shared among industry participants, listed in Table 1.[80]

Table 1. Examples of Information Organizations Should Share (E-ISAC).

Physical Security Events	Cybersecurity Events
Unusual observation, suspicious activity, or surveillance of facilities	Unexplained OT-device behavior (e.g., freezes, reboots, or failures)
Misrepresentation of affiliation	Suspicious network traffic within a trusted environment or from a trusted partner's account
Unmanned aircraft system incidents, activities, or regulations	Suspicious interaction attempts against remote against remote access solutions (VPN concentrators, jump boxes, remote email solutions, etc.)

Physical Security Events	Cybersecurity Events
Theft, loss, or diversion of key safety or security systems	Unexplained internal or external login attempts
Activist activities	Targeted phishing activity with well-defined purpose and objective
Expressed or implied threats	Vulnerability probing and exploitation activity
Breach or attempted intrusion	Malware delivered to or found in enterprise or operational equipment
SCADA/ICS anomalies coincident with a physical security event	Any other analysis, insights, or forensic artifacts from incident response and threat hunting
Gunfire damage or other vandalism	

Resources for Incident Response

As described above in CIS Control 17, planned and exercised cybersecurity incident response will reduce the probability of substantial impact to or downtime of wind energy assets. It is important AOO leadership knows what potential impact there could be to help leaders prioritize remediation or restoration decisions that best support key assets. Although the private sector will be the primary responders to incidents, including AOOs, equipment vendors, and cybersecurity companies specializing in IR, government organizations have some resources that may be helpful for the wind energy sector.

At the federal level, CISA has certain resources to support when cyber incidents impact critical infrastructure entities, such as regional cybersecurity advisors, who can provide cyber preparedness, assessments and protective resources and incident coordination during cyber threats, disruptions, and attacks. Additionally, organizations can report anomalous cyber activity or cyber incidents to CISA 24/7 online, by calling or emailing.[81] Finally, although not wind sector specific, CISA has online and in-person incident response trainings, including training in means of defending against ransomware attacks and understanding indicators of compromise.

Certain states also have resources available to support incident response for critical infrastructure entities. For example, New York's Cyber Incident Response Team (CIRT) provides free cyber incident response, as well as proactive cybersecurity services including cybersecurity risk assessments and training to eligible entities.[82] The California Cybersecurity Integration Center (Cal-CSIC) also provides a response team to lead cyber threat detection, reporting, and response to public and private entities across the state.[83]

CONCLUSION

Wind generation has grown markedly in recent years with the introduction of innovative techniques and wind plant designs, along with a significant growth in usage in many regions and countries. The IT/OT designs and life cycle of wind plants are unique compared to both traditional power and traditional enterprise systems, giving them distinct attack surfaces to be addressed. While many best practices currently used in

other industries and sectors are applicable to the wind industry, cybersecurity mitigations should be prioritized according to unique wind power needs.

Adversaries have increased their targeting of energy sector assets globally since 2015, as manifested in the cases of Industroyer (2016), SPower (2019), and poetRAT (2020). In more recent years, a marked increase in cyber events has affected wind stakeholders, as demonstrated by the Viasat attack (2022), Deutche Windtechnik (2022), and Nordex SE (2022). Compromise and cyber manipulation of wind plant data communication flows, either by remote access or physical intrusion, could have significant impacts, including loss of generation capability or physical damage to a WTG or its components.

The specific adversarial techniques used to compromise and exploit wind assets are not well understood, in part due to limited visibility within the OT environment (e.g., controllers, networks, and buses, etc.). Additional research is necessary to categorize the best methods to monitor a wind plant for adversary activity; however, this document identifies some initial attack surface areas and threat vectors for consideration, including vendor and OEM connections and transient cyber assets. These connections and components are attractive targets for adversary activity because they can enable remote and synchronized attacks against a number of wind plant assets. Additionally, wide adoption of information sharing practices among government and private sector representatives is necessary to ensure that observed adversary tactics and techniques are properly disseminated. Wind industry cyber resilience requires a coordinated public and private response.

REFERENCE LIST

1. The White House, "National Cybersecurity Strategy," March 2023, accessed August 1, 2023, https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.
2. Office of the Director of National Intelligence, "Annual Threat Assessment of the U.S. Intelligence Community," ODNI., February 6, 2023, accessed August 1, 2023, https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf.
3. Energy information Administration, "Wind Explained: Energy generation from wind," April 20, 2023, accessed May 22, 2023, https://www.eia.gov/energyexplained/wind/electricity-generation-from-wind.php.
4. Jonathan Greig, "German Wind Farm Operator Confirms Cybersecurity Incident," The Record, April 28, 2022, accessed August 1, 2023, https://therecord.media/german-wind-farm-operator-confirms-cybersecurity-incident-after-ransomware-group.
5. Lawrence Abrams, "Wind turbine firm Nordex hit by Conti ransomware attack," Bleeping Computer, April 14, 2022, accessed August 1, 2023, https://www.bleepingcomputer.com/news/security/wind-turbine-firm-nordex-hit-by-conti-ransomware-attack.
6. Juan Andres Guerrero-Saade and Max van Amerongen, "AcidRain | A Modem Wiper Rains Down on Europe," Sentinel Labs, March 31, 2022, accessed August 1, 2023, https://www.sentinelone.com/labs/acidrain-a-modem-wiper-rains-down-on-europe/.
7. Michael Raggi and Sveva Scenarelli, "Rising Tide: Chasing the Currents of Espionage in the South China Sea," Proofpoint, August 30, 2022, accessed August 1, 2023, https://www.proofpoint.com/us/blog/threat-insight/chasing-currents-espionage-south-china-sea.
8. Utility Variable-Generation Integration Group, *Wind Operating Practices Guidebook*, chap. 2.6.2, 2.6.3.
9. "Bulk Electric System Definition Reference Document," North American Electric Reliability Corporation, v.3 (2018).
10. Utility Variable-Generation Integration Group, *Wind Operating Practices Guidebook*, 2.1.7, 2.6.4, 2.6.5.
11. David Ferlemann, "Wind Farm Security Analysis and Attack Mitigation," (Ph.D. diss., University of Tulsa, 2017), 1-56.
12. "Wind power needs communication," Siemens, accessed October 12, 2020, https://new.siemens.com/global/en/markets/wind/equipment/industrial-communication.html.
13. Mohamed A Ahmed et al., "Wireless Network Architecture for Cyber Physical Wind Energy System," *IEEE Access* 8 (2020): 40180–97.
14. Mohamed Ahmed and Young-Chon Kim, "Wireless Communication Architectures Based on Data Aggregation for Internal Monitoring of Large Scale Wind Turbines," *International Journal of Distributed Sensor Networks,* 12(8): 14, August 2016, accessed October 11, 2020, https://www.researchgate.net/publication/306378752_Wireless_Communication_Architectures_Based_on_Data_Aggregation_for_Internal_Monitoring_of_Large-Scale_Wind_Turbines.
15. DOE-EERE/Wind Energy Technologies Office, "Roadmap for Wind Cybersecurity," 20 July 2020, Accessed 26 September 2020, https://www.energy.gov/sites/prod/files/2020/08/f77/wind-energy-cybersecurity-roadmap-2020v3.pdf.
16. Bertram Lange, "Assessing the Impact of Cyber Security on the Nations' Windfarms" (USE 61400-25 User Group, Boulder, CO, July 16, 2019), 9.

17. Jason Staggs, David Ferlemann, and Sujeet Shenoi, “Wind Farms Security: Attack Surface, Targets, Scenarios and Mitigations,” *International Journal of Critical Infrastructure Protection* 17 (2017): 3-14.
18. Karlheinz Schwarz, “IEC 61850, IEC 61400-25, and IEC 61970: Information Models and Information Exchange for Electric Power Systems”, 20 Jan. 2004, accessed May 22, 2023, www.nettedautomation.com/download/Paper_IEC61850_Distributech_2004-02-10.pdf
19. E. San Temlo, I Canales, J. L. Villate, E. Robles, and S. Apiñaniz, “The Use of IEC 61400-25 Standard to Integrate Wind Power Plants in to the Control of Power System Stability,” *European Wind Energy Conference & Exhibition* (2007): 1-5.
20. Utility Variable-Generation Integration Group, *Wind Operating Practices Guidebook*, Section 2.6.3.
21. Gavin Bade, “Russian hackers infiltrated utility control room, DHS says,” July 24, 2018, accessed October 16, 2020, https://www.utilitydive.com/news/russian-hackers-infiltrated-utility-control-rooms-dhs-says/528487/.
22. Nordex Group, “Update on cyber security incident,” April 12, 2022, https://www.nordex-online.com/en/2022/04/update-on-cyber-security-incident/.
23. “The attack against Danish critical infrastructure, SektorCert, November 2023. https://sektorcert.dk/wp-content/uploads/2023/11/SektorCERT-The-attack-against-Danish-critical-infrastructure-TLP-CLEAR.pdf
24. Ros Davidson, "AWEA 2018: Increase in Cyber Security Attacks 'inevitable', Expert Warns." Windpower Monthly. May 8, 2018. Accessed August 05, 2023. https://www.windpowermonthly.com/article/1464061/awea-2018-increase-cyber-security-attacks-inevitable-expert-warns.
25. Ransomware attack hits Deutsche Windtechnik,” Secure Reading, April 27, 2022, https://securereading.com/ransomware-attack-hits-deutsche-windtechnik/.
26. Electricity Information Sharing and Analysis Center, “Wind Farm Security: Best Practices and Lessons Learned,” June 2020, accessed October 19, 2020, https://esigom.groups.io/g/main/attachment/243/0/TLP%20GREEN_E-ISAC%20Wind%20Farm%20Security%20White%20Paper_FINAL%20VERSION.pdf.
27. “The Threat of Eco-Terrorism,” FBI, accessed June 16, 2020, https://www.fbi.gov/news/testimony/the-threat-of-eco-terrorism.
28. Michael Waters, “Anti-Wind Farm Activism Is Sweeping Europe—and the U.S. Could Be Next,” Earther, accessed June 16, 2020, https://earther.gizmodo.com/anti-wind-farm-activism-is-sweeping-europe-and-the-us-c-1829627812.
29. Selena Larson and Camille Singleton, “Ransomware in ICS Environments,” Dragos, Inc., December 15, 2020, accessed January 26, 2021, https://www.dragos.com/resource/ransomware-in-ics-environments/.
30. Michael Raggi and Sveva Scenarelli, “Rising Tide: Chasing the Currents of Espionage in the South China Sea,” Proofpoint, August 30, 2022, accessed October 26, 2023, https://www.proofpoint.com/us/blog/threat-insight/chasing-currents-espionage-south-china-sea
31. CISA, “Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure”, CISA, May 9, 2022, accessed October 26, 2023, https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-110a.
32. Simon Handler, “The 5x5 – China’s Cyber Operations,” Atlantic Council, January 30, 2023, accessed October 26, 2023, https://www.atlanticcouncil.org/content-series/the-5x5/the-5x5-chinas-cyber-operations/.
33. “Why Windfarms Need to Step up Cyber Security,” DNV GL, accessed July 16, 2020, https://www.dnvgl.com/article/why-windfarms-need-to-step-up-cyber-security-128082.
34. “Viewer | USWTDB,” accessed July 10, 2020, https://eerscmap.usgs.gov/uswtdb/viewer/#9/45.7464/-120.3691.

35. "Industrial VPN Vulnerabilities Put Critical Infrastructure at Risk," BleepingComputer, accessed August 7, 2020, https://www.bleepingcomputer.com/news/security/industrial-vpn-vulnerabilities-put-critical-infrastructure-at-risk/.
36. "Getting from 5 to 0: VPN Security Flaws Pose Cyber Risk to Organizations with Remote OT Personnel," *Claroty* (blog), July 28, 2020, https://www.claroty.com/2020/07/28/vpn-security-flaws/.
37. Jason Staggs, "Adventures in Attacking Wind Farm Control Networks" (PPT, BlackHat, Las Vegas, NV, July 25, 2017), https://www.blackhat.com/docs/us-17/wednesday/us-17-Staggs-Adventures-In-Attacking-Wind-Farm-Control-Networks.pdf.
38. Jason Staggs, David Ferlemann, and Sujeet Shenoi. "Wind Farm Security: Attack Surface, Targets, Scenarios and Mitigation." International Journal of Critical Infrastructure Protection 17 (2017): 3-14. DOI:10.1016/j.ijcip.2017.03.001.
39. Andy Greenburg, "CrashOverride: The Malware that Took Down a Power Grid," June 12, 2017, accessed October 23, 2020, https://www.wired.com/story/crash-override-malware/.
40. ESET Research, "Industroyer2: Industroyer reloaded," April 12, 2022, accessed February 21, 2023, https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/.
41. MITRE, "Valid Accounts," accessed May 22, 2023, https://attack.mitre.org/techniques/T0859/.
42. Joe Slowick, "Anatomy of an Attack: Detecting and Defeating CRASHOVERRIDE," October 12, 2018, accessed November 10, 2020, https://www.dragos.com/wp-content/uploads/CRASHOVERRIDE2018.pdf.
43. MITRE, "Manipulation of Control," accessed May 22, 2023, https://attack.mitre.org/techniques/T0831/.
44. Anton Cherepanov, "A New Threat for Industrial Control Systems," June 12, 2017, accessed October 23, 2020, https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf.
45. MITRE, "Denial of Service," accessed May 22, 2023, https://attack.mitre.org/techniques/T0814/.
46. MITRE, "Loss of Safety," accessed May 22, 2023, https://attack.mitre.org/techniques/T0880/.
47. MITRE, "Theft of Operational Information," accessed December 4, 2023, https://attack.mitre.org/techniques/T0882/.
48. E&E News,"OE-417 Electric Emergency and Distribution Report – Calendar Year 2019," accessed October 22, 2020, https://www.eenews.net/assets/2019/04/30/document_ew_03.pdf.
49. Sean Lyngaas, "Utah renewables company was hit by rare cyberattack in March," October 31, 2019, accessed April 10, 2020, https://www.cyberscoop.com/spower-power-grid-cyberattack-foia/.
50. NERC, "Lessons Learned: Risks Posed by Firewall Firmware Vulnerabilities," accessed October 22, 2020, https://www.nerc.com/pa/rrm/ea/Lessons%20Learned%20Document%20Library/20190901_Risks_Posed_by_Firewall_Firmware_Vulnerabilities.pdf.
51. Stephen Jewkes and Oleg Vukmanovic, "Suspected Russia-backed hackers target Baltic energy networks," May 11, 2017, accessed October 23, 2020, https://www.reuters.com/article/us-baltics-cyber-insight/suspected-russia-backed-hackers-target-baltic-energy-networks-idUSKBN1871W5.
52. Connor Jones, "Inside Denmark's hell week as critical infrastructure orgs faced cyberattacks," The Register, November 13, 2023, accessed November 29, 2023. https://www-theregister-com.cdn.ampproject.org/c/s/www.theregister.com/AMP/2023/11/13/inside_denmarks_hell_week_as/.
53. MITRE, "Exploit Public-Facing Application," accessed May 22. 2023, https://attack.mitre.org/techniques/T0819/.

54. NERC, “Lessons Learned: Risks Posed by Firewall Firmware Vulnerabilities,” accessed October 22, 2020, https://www.nerc.com/pa/rrm/ea/Lessons%20Learned%20Document%20Library/20190901_Risks_Posed_by_Firewall_Firmware_Vulnerabilities.pdf.
55. MITRE, “Denial of View,” accessed May 22, 2023, https://attack.mitre.org/techniques/T0815/.
56. Blake Sobczak, “First-of-a-kind U.S. grid cyberattack hit wind, solar,” E&E News, October 31, 2019, accessed October 26, 2023, https://subscriber.politicopro.com/article/eenews/1061421301.
57. Warren Mercer, Paul Rascagneres and Vitor Ventura, “PoetRAT: Python RAT uses COVID-19 lures to target Azerbaijan public and private sectors,” *Talos*, April 16, 2020, accessed October 23, 2020, https://blog.talosintelligence.com/2020/04/poetrat-covid-19-lures.html.
58. MITRE, “Drive-by Compromise,” accessed May 22, 2023, https://attack.mitre.org/techniques/T0817/.
59. MITRE, “Spearphishing Attachment,” accessed May 22, 2023, https://attack.mitre.org/techniques/T0865/.
60. MITRE, “Virtualization/Sandbox Evasion: System Checks,” accessed November 10, 2020, https://attack.mitre.org/techniques/T1497/001/.
61. MITRE, “Non-Application Layer Protocol,” accessed November 10, 2020, https://attack.mitre.org/techniques/T1095/.
62. MITRE, “Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder,” accessed November 10, 2020, https://attack.mitre.org/techniques/T1547/001/.
63. MITRE, “Automated Exfiltration,” accessed November 10, 2020, https://attack.mitre.org/techniques/T1020/.
64. MITRE, “Video Capture,” accessed November 10, 2020, https://attack.mitre.org/techniques/T1125/.
65. MITRE, “Screen Capture,” accessed November 10, 2020, https://attack.mitre.org/techniques/T1113/.
66. MITRE, “Data from Local System,” accessed November 10, 2020, https://attack.mitre.org/techniques/T1005/.
67. Enercon, “Over 95 per cent of WECs back online following disruption to satellite communication,” April 19, 2022, accessed February 21, 2023, https://www.enercon.de/en/news/news-detail/cc_news/show/News/over-95-per-cent-of-wecs-back-online-following-disruption-to-satellite-communication/.
68. U.S. Government Attributes Cyberattacks on SATCOM Networks to Russian State-Sponsored Malicious Cyber Actors,” CISA, May 10, 2022, accessed October 26, 2023, https://www.cisa.gov/news-events/alerts/2022/05/10/us-government-attributes-cyberattacks-satcom-networks-russian-state.
69. ViaSat, “KA-SAT Network cyber attack overview,” accessed June 20, 2022, https://www.viasat.com/about/newsroom/blog/ka-sat-network-cyber-attack-overview/.
70. MITRE, “External Remote Services,” accessed June 20, 2022, https://attack.mitre.org/techniques/T0822/.
71. MITRE, “Remote Services,” accessed June 20, 2022, https://attack.mitre.org/techniques/T0886/.
72. MITRE, “Data Destruction,” accessed May 22, 2023, https://attack.mitre.org/techniques/T0809/.
73. MITRE, “Loss of View,” accessed May 22, 2023, https://attack.mitre.org/techniques/T0829/
74. Michael Raggi and Sveva Scenarelli, “Rising Tide: Chasing the Currents of Espionage in the South China Sea,” Proofpoint, August 30, 2022, accessed August 1, 2023, https://www.proofpoint.com/us/blog/threat-insight/chasing-currents-espionage-south-china-sea.
75. MITRE, “Phishing: Spearphishing Link,” accessed May 22, 2023, https://attack.mitre.org/techniques/T1566/002/.

76. Center for Internet Security (CIS), “The 18 CIS Critical Security Controls” accessed November 16, 2023, https://www.cisecurity.org/controls/network-monitoring-and-defense.
77. Jeff Pack, “Recapping AWEA’s 2019 Cybersecurity Panel,” accessed September 14, 2020, https://energycentral.com/c/cp/recapping-awea%E2%80%99s-2019-cybersecurity-panel?term=power-delivery.
78. North American Electric Reliability Corporation (NERC), “NERC-CIP-010-3: Cyber Security — Configuration Change Management and Vulnerability Assessments,” Effective 1 October 2020, accessed January 13, 2021, https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-010-3.pdf.
79. Malcolm, “Malcolm: A powerful, easily deployable network traffic analysis tool suite” accessed November 16, 2023, https://malcolm.fyi/.
80. Energy-Information Sharing and Analysis Center (E-ISAC), “Guide for Information Sharing,” September 2019, accessed 25 September 2020, https://www.eisac.com/cartella/Asset/00007920/TLP_WHITE_E-ISAC_Information_Sharing_Guide.pdf?parent=120640.
81. Cybersecurity and Infrastructure Security Agency (CISA), “CISA Central,” accessed December 4, 2023 https://www.cisa.gov/cisa-central.
82. New York State Division of Homeland Security and Emergency Services, “Cyber Incident Response Team,” accessed December 4, 2023, https://www.dhses.ny.gov/cyber-incident-response-team.
83. California Governor’s Office of Emergency Services, “California Cybersecurity Integration Center,” accessed December 4, 2023, https://www.caloes.ca.gov/office-of-the-director/operations/homeland-security/california-cybersecurity-integration-center/.