INL/EXT-21-64999

Cybersecurity for Distributed Wind

What Operators Need to Know

Idaho National Laboratory

CYBERSECURITY FOR DISTRIBUTED WIND – WHAT OPERATORS NEED TO KNOW

As an operator of a distributed wind asset or a system that includes distributed wind, you are probably familiar with basic concepts of cybersecurity. You are also likely familiar with your system's basics and how it might fit within the larger context of a "distributed energy resource (DER) transition." However, until INL published the *Cybersecurity Guide for Distributed Wind* in 2021, few resources addressed a growing need to secure distributed wind systems. The Guide is a richly detailed resource outlining a distributed wind system's possible architectures, relevant standards, risk management strategies, and key recommendations for stakeholders. This document highlights key actionable insights from the Guide that operators can use to quickly develop their cybersecurity strategy.

A key aspect of cybersecurity is that it cannot exist in a vacuum, but rather must consider the system and all of its interconnected parts holistically. In addition, many cybersecurity standards have been carefully developed, but not all aspects of these standards that apply to distributed wind or to all installations. Therefore, we discuss the aspects of the standards that best apply to different configurations of distributed wind systems. Even for systems that are not required to meet specific cybersecurity standards, the standards can be utilized as a reference for best practices. Distributed wind systems can come in a variety of architectures and applications, so there is no one-size-fits-all approach to cybersecurity. However, we have included recommendations to inform operators of the common risks, unique challenges, and operational responsibilities in running secure systems.

DEFINING DISTRIBUTED WIND

The Wind Energy Technologies Office defines distributed wind in terms of technological application, based on a wind plant's location relative to end-use and power distribution infrastructure, rather than technology or project size. The criteria include:

- **Proximity to End Use:** Wind turbines that are installed near the end-use for the purposes of meeting onsite energy demand or supporting the existing distribution grid.
- **Point of Interconnection:** Wind turbines that are connected on the customer side of the meter (also known as behind-the-meter), directly to the distribution grid, or are off-grid in a remote location.

Distributed wind energy systems can range in size from a 5kW turbine at a home to multi-megawatt turbines at a manufacturing facility or interconnected to a local distribution system. Based on this definition, there are three basic **reference architectures** for distributed wind:

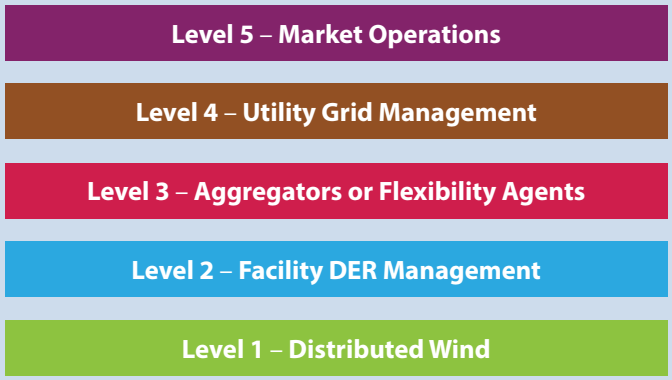
1. Customer-based, behind-the-meter wind turbines
2. Utility/aggregator managed individual wind turbines
3. Wind turbines in microgrids

Distributed wind installations are rising, with more than 1,145 MW of capacity from over 85,000 turbines installed between 2003 and 2019 in the United States, Puerto Rico, the U.S. Virgin Islands, and Guam. Consideration of cybersecurity is necessary as distributed wind penetration continues to rise.

DEFINING AN ARCHITECTURE

Distributed wind installations can range from individual wind turbines supporting home or building loads, to combinations of wind turbines and other energy resources in a microgrid, to complex virtual power plants (VPPs) designed to provide grid services and meet market requirements.

Understanding the architecture of a distributed wind system in the context of other systems and functionalities provides a foundation on which to begin to address cybersecurity needs. The architecture for any individual system should cover each of the five layers below. While an operator should prioritize the systems under their control, understanding threats at each level will provide a depth of defense and safeguard the system should others be compromised.



***Bottom line:** Every distributed wind system is unique. Effective cybersecurity begins with understanding the system at hand.*

UNDERSTANDING THE PROBLEM SPACE: WHY DISTRIBUTED WIND IS UNIQUE

The Department of Energy published a Roadmap for Wind Cybersecurity in 2020, which details wind cybersecurity challenges and recommendations. Below, we reiterate some of the key findings from the Roadmap on the need for cybersecurity and the unique challenges of securing distributed wind systems:

Shifts in wind energy system designs demand changes in our approach to cybersecurity. The demand for distributed wind is growing and becoming an increasing part of the "smart grid" landscape. In particular, "smart" inverters are now required to support the dynamic operation of distributed wind, leading to the need for bidirectional communications. Local and remote connectivity among turbines, control equipment, control centers, and business networks will use a range of communication protocols, which expand the scope of monitoring and protection but also introduce new cybersecurity challenges.

Cyber threats to wind energy technology have been established and demonstrated, both in theoretical and real-world instances. Academic research has found vulnerabilities in wind technology, allowing mis-operation of wind assets. Cybersecurity firms have documented incidents that demonstrate malicious cyber-actors are interested in wind, resulting in actual shutdowns of wind assets. Operators should be familiar with these incidents and ensure they have necessary monitoring to detect if similar attacks target their systems. Wind assets are unique due to the number of moving parts, which means that cyber-attacks have the potential to cause expensive physical damage. As generation resources, wind assets also have the potential to cause destabilizing effects on connected systems if compromised.

Distributed wind turbines can be installed for a variety of applications, but most stakeholders may be unfamiliar with basic cybersecurity. Because distributed wind can cover anything from a single turbine to a collection of turbines tied into the local distribution system, not all vendors, customers, or installers may be familiar with the cybersecurity risks or mitigations associated with wind systems. Most stakeholders will not be able to take the time or effort required to understand all relevant guidelines, such as IEEE P1547.3. When operators assume responsibility for wind assets, they must diligently assess the practices of manufacturers and installers to ensure operations do not suffer from unnecessary cyber risks.

CHALLENGES IN SECURING DISTRIBUTED WIND

- Cybersecurity must be "end-to-end" and "throughout the complete lifecycle" of distributed wind systems.
- The wind plant lifecycle involves many parties; effective cybersecurity practices are difficult to establish, maintain, and trace through the supply chain.
- Different protocols are used across different manufacturers. No single standard protocol is used across the industry, and some proprietary protocols are used.
- Systems may be internet-connected to facilitate remote control and monitoring of distributed turbines; special care must be taken to protect communications over these "no-trust" networks.
- Distributed wind systems come in many sizes, for many applications, and in different relationships to distribution systems. There is no one-size-fits-all solution for securing distributed wind systems.
- No established cybersecurity standards specific to wind energy exist; some standards may apply to distributed wind, but this is not universally true, which makes standards difficult to specify for distributed wind.
- Few incentives for wind energy stakeholders have been established to prioritize cybersecurity over other investments (e.g., reliability, performance, etc.).
- Distributed wind stakeholders may not have access to the information sharing groups that do exist.
- There are few and underdeveloped wind-specific cybersecurity services, products, and strategies.

Further development of standards and guidelines for distributed wind systems is needed, particularly in the area of cybersecurity. Standards for communications, equipment, and security practices are currently underdeveloped or absent from the wind industry. While a few distributed wind systems may fall under NERC CIP guidelines, most do not. Additionally, while distributed wind can benefit from work on generic DERs, there are aspects of distributed wind systems that require additional considerations. For instance, there are gaps in the data and semantic industry standard models associated with treating wind as a DER (see IEC 61850-7-420, and IEC 61400-25-2).

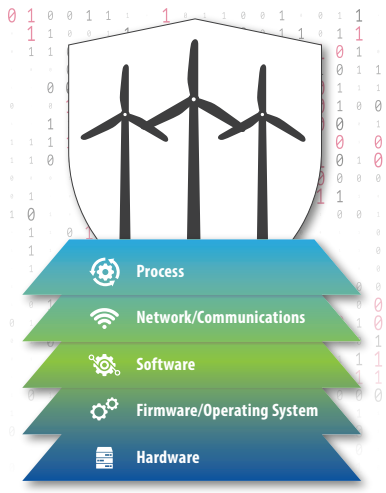
***Bottom line:** Cyber threats can be exposed on any part of the system and throughout the lifecycle of the assets.*

UNDERSTANDING THE RISK

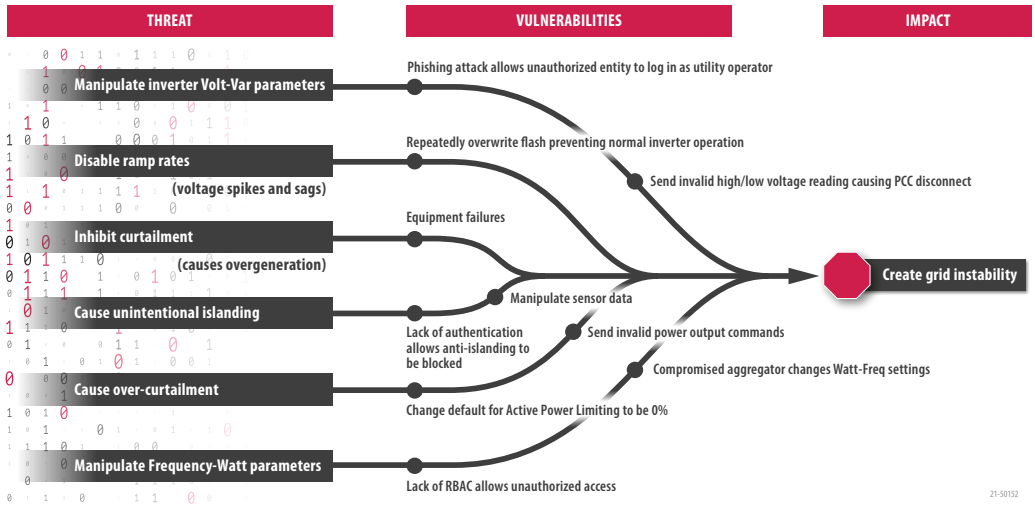
It is impossible to predict and protect against all possible cyberattacks, so the goal of any cybersecurity strategy is to minimize risk and then plan for the inevitable deliberate or inadvertent cyberattack.

To address risk for distributed wind operations, it is important to examine the individual aspects of risk. The first step is to better understand the **capabilities, intents, and opportunities** of potential adversaries. When examining cybersecurity threats in more detail, note that they can be either **intentional or unintentional**. Intentional threats include actions carried out by an adversary. Unintentional threats can include equipment failures, natural disasters, or mistakes by someone with authorized access and privileges to a system. Intentional cybersecurity threats, on the other hand, are malicious and driven by the particular objective of the adversary, which can vary widely.

The vulnerabilities of equipment and associated communications must also be understood in order to appropriately assess potential impacts of successful cyberattacks, including the financial, power system, societal, and legal ramifications, along with their probability of occurring. Ultimately, operators can assess the costs for mitigating the vulnerabilities relative to their impacts to determine appropriate actions..



Potential vulnerabilities in the system



Inverter-based DER attack tree example, captures threats and consequences.

CYBERSECURITY STANDARDS: ONE WAY TO MANAGE RISK

Operators should use cybersecurity standards and best practice guidelines to support the risk management process and establish security programs and policies for operational technology (OT) environments. Relevant key standards and guidelines have already been developed for DER, telecommunication, and power system security. Cybersecurity planning should use these standards and guidelines to improve resilience, security, and interoperability throughout the energy OT environment, using the appropriate guidelines and procedures for the relevant purposes at the right time.

In the *Cybersecurity Guide for Distributed Wind*, the authors provide a framework to consider cybersecurity standards, categorizing standards by their focus area (general IT, energy systems OT, detailed technical level), and by their type (describing "What" should be done versus "How" to apply specific technologies). Some key cybersecurity standards and guidelines to consider with respect to distributed wind cybersecurity include:

- **NIST Cyber Security Framework,** which identifies the key "what" cybersecurity requirements, not only to protect against cyberattacks but to prepare for coping and recovering from the inevitable successful attacks. It also references most of the other key cybersecurity standards and thus can be seen as the overarching cybersecurity framework.
- **IEEE P1547.3,** which provides guidelines and recommendations for DER. This standard, still under development, addresses most of the cybersecurity requirements for distributed wind, particularly with respect to operating DER.
- **IEC 62351 family of standards** is being developed to address the need to design cybersecurity robustness and resilience into Industrial Automation and Control Systems (IACS), covering both organizational and technical aspects of security over the life cycle of systems. Although initially focused on industrial automation, this cybersecurity set of standards has also been adopted by the energy sector, since it provides a methodology for applying security in operational and field environments for cyber-physical systems.
- **NERC CIP standards likely do not apply** to a given distributed wind deployment, but because of the increasing attention on DERs with respect to the reliable operation of the bulk electric system, it is useful to review the NERC CIP definitions of impacts to see where they could potentially apply in the future to aggregated DER.

***Bottom line:** Understanding and managing the risks associated with operations will help secure distributed wind.*

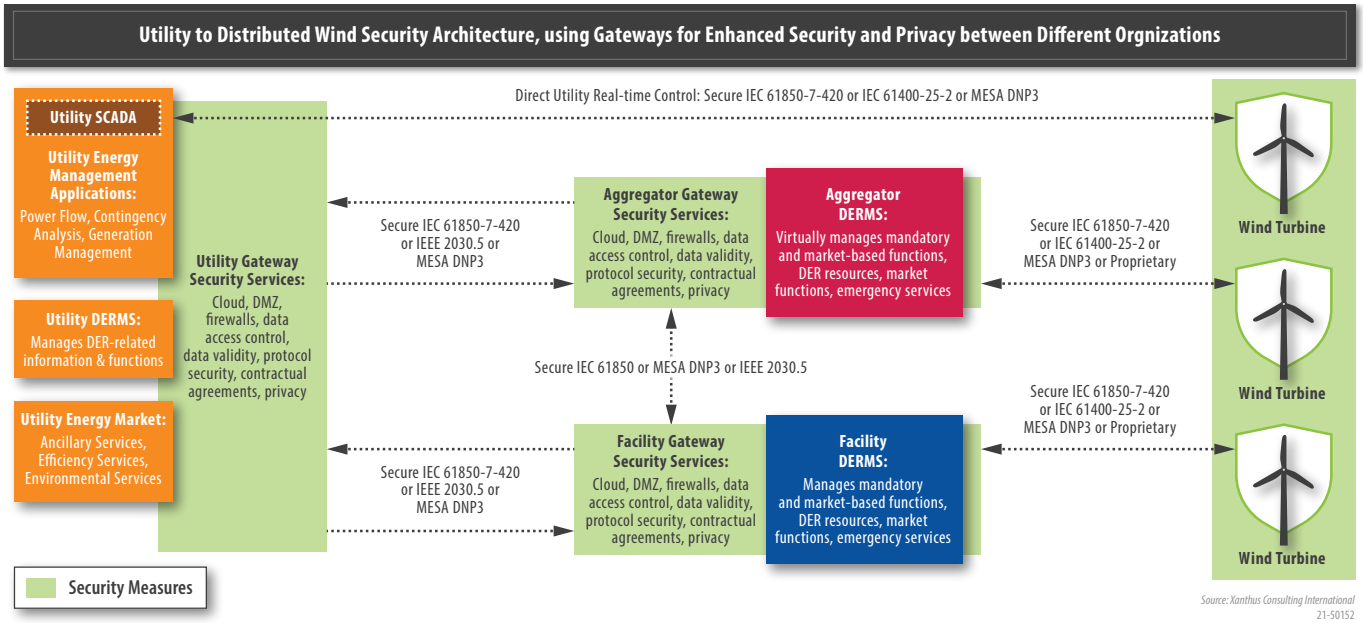
PRIORITY AREAS FOR OPERATORS

Operators are responsible for ongoing cybersecurity of the system. Even well-designed cybersecurity measures can fail when executed poorly, and operators must be able to recognize evolving threats facing their system. As noted above in the introduction, Defining Distributed Wind, there are three basic reference cases, each with its own unique set of vulnerabilities and impacts:

- **Customer-based, behind-the-meter wind turbines,** where the impact of losing or misusing a single behind-the-meter distributed wind turbine would be minimal to grid resilience from the grid operator's perspective. Meanwhile, the unexpected loss of a number of wind turbines behind-the-meter could cause serious problems for a large industrial plant operator if the local grid cannot handle the sudden addition of new load.
- **Grid-connected utility or aggregator-managed wind turbines,** where the risk would be minimal for the loss of a single wind turbine, but the propagation of a cyber-attack through many turbines could cause erratic behavior, potential failure of the turbines, and consequential disturbances or outages of the grid.
- **Wind turbines in microgrids** (which could be a single home or a large community or even a town), where cyber-attacks could have minimal or enormous impacts, depending upon the situation. The key issue is not the size of an individual wind turbine itself, but the possibility that the cyber malware could spread to other wind turbines or other electrical equipment, as well as affecting the characteristics of the surrounding DER and loads.

For distributed wind, IEEE P1547.3 should form the basis of cybersecurity recommendations with special emphasis placed on the security of the RBAC capabilities due to the remote location and mechanical vulnerabilities of distributed wind.

Regardless of the installation type, **authentication** of the source and recipient of data and **authorization for access** to the systems are **key cybersecurity requirements** for operators, best implemented using role-based access control (RBAC). Confidentiality is important where privacy and/or market interactions are involved. Some operators may have access to distributed wind systems directly through a local interface, while most operators will likely require remote access. The figure below illustrates key areas where cybersecurity is essential to interactions between distributed wind turbines and facilities, utilities, and aggregators.



As grid operators consider making IEEE 1547-2018 a mandatory or recommended standard for DER interconnections, distributed wind operators should pay special attention to its companion guide, IEEE P1547.3, which covers cybersecurity recommendations for DER. Specifically, of the topics covered in Section 5 of the standard, operators may take part in:

- Risk assessment and management (RA)
- Communication network engineering (NE)
- Access control (AC)
- Data security (DS)
- Security management (SM)
- Coping with and recovering from (CM) security events

***Bottom line:** Cybersecurity recommendations for DER should start with the IEEE P1547.3 recommendations.*

RECOMMENDATIONS SPECIFIC TO DISTRIBUTED WIND

Cybersecurity solutions, particularly if they already exist within established communication networks and protocol standards, should not be re-invented within distributed wind systems with the implementation of proprietary or custom protocols. If a proprietary protocol must be utilized for a particular data exchange within a distributed wind system, steps should be taken to minimize the associated risk. Mitigations can include implementing gateways that separate inbound and outbound data flows or virtual private networks (VPNs) that provide a secure wrapper for the proprietary protocols.

For distributed wind installations sited in rural areas or inaccessible areas, access control should cover additional issues related to that isolation. For instance, physical access attempts and entries may not be noticeable for long periods of time, while cyber access attempts and successful local logins may not be visible if the expectation is that physical access is limited. Given the unique circumstances of these sites, the Guide recommendations the following principles regarding physical and local access for isolated systems:

- Passwords for local access at each wind turbine site should be unique for each user or role.
- Role-based access control permissions should be established so that only permissions required for the role are allowed for local access.
- Local access attempts, whether successful or not, should be logged and alarmed with a higher priority than if the wind turbine were located in a building or populated area.
- Access by applications connected locally (e.g., maintenance laptop) without appropriate credentials should be prevented.
- Physical access to the site should be limited to a given set of stakeholders under specific conditions (e.g., maintenance), and within specific time frames (e.g., 1 working day) for different situations.
- Logs of physical access should be kept.

Risk assessments must consider the isolated and rural locations of many turbines. Risk assessments should consider cyber and physical access, as described above, and environmental issues, including:

- The likelihood and potential impacts from storms or environmental events (ice, strong wind gusts) at the actual site (hilltop, ocean, narrow valley, surrounding buildings) rather than just within a general location, and include the possibility of physical damage such as wind-blown tree branches, (salt) water spray, bullets, and collisions from vehicles.
- Identification of any necessary physical protections against environmental events that should be included in the design and implementation, particularly with respect to the wind turbines' mechanical parts.

***Bottom line:** Distributed Wind systems can be located in remote areas; cybersecurity measures should consider this.*

RECOMMENDATIONS SPECIFIC TO DISTRIBUTED WIND (CONTINUED)

Because distributed wind systems can be located **in areas without reliable cellular or internet availability,** speed and bandwidth for remote communications can be lacking:

- The design of communication traffic management should include the ability to prioritize for critical security and power system data within the communication network, possibly at a higher priority than normal monitoring to ensure that remedial actions can be taken.
- Certain cybersecurity management requirements, such as certificate revocation lists (CRLs), may not be able to be updated to the local distributed wind controller in a timely manner. For most situations, therefore, management of CRLs should be handled remotely through Online Certificate Status Protocol (OCSP) services.

Because distributed wind systems may **utilize untrusted or public communications infrastructure:**

- Communications may not be able to use the commonly available protocols (i.e., IEC 61850 IEC 61400-25, IEEE 1815 [DNP3], IEEE 2030.5, and SunSpec Modbus), due to communication response delays or slow data exchange rates. Nonetheless, authentication and authorization should still be included.

Because **legacy communication protocols** may be in use for distributed wind that may not align with the capabilities afforded by the protocols now in use for other types of DER:

- Rather than inventing new semantic data objects to fill gaps, IEC 61850-7-420 should be used to fill gaps in IEC 61400-24-2.
- Data security should be added to any of the protocols used for distributed wind.

Because of the **sensitivity of the physical equipment** for distributed wind system, additional types of sensors focused on the mechanical equipment, as well as associated warnings and alarms, should be included as needed for cybersecurity. Specifically:

- Some sensor data should be treated as time-sensitive data, such as warnings and alarms, with timestamps and checks to determine it has arrived within the specified time period.
- Redundant sources of data should be used for critical sensor information.

A PARTING THOUGHT

Distributed wind is becoming commonplace in the broader context of DER. With an increased presence of DER within the electric power grid, utilities are no longer solely responsible for grid security. The various non-utility stakeholders in distributed wind play a key role in this new operating paradigm. As illustrated in this document as well as the broader *Cybersecurity Guide for Distributed Wind*, a recommended strategy for all stakeholders is to utilize the recommendations provided in IEEE P1547.3 as a basis for distributed wind cybersecurity guidance. It is, however, important to identify specific items or aspects of these recommendations that are key for distributed wind security generally and the given system specifically. With the discussion and basic recommendations provided here, the hope is that distributed wind operators will have a better understanding of the importance of addressing cybersecurity at all stages of a system's lifecycle as well as of the relationships (direct and indirect) between the various elements that make up the power grid.

***Bottom line:** Cybersecurity should be built into distributed wind systems and its related components from the start.*

For Further Reading:

- *Cybersecurity Guide for Distributed Wind*, August 2021
- U.S Department of Energy, Office of Energy Efficiency & Renewable Energy, "Roadmap for Wind Cybersecurity," July 2020.
- IEEE P1547.3 "Guide for Cybersecurity of Distributed Energy Resources Interconnected with Electric Power Systems" (pending)
- NIST Cybersecurity Framework
- ISO/IEC 27000 Cyber Security Standards
- NISTIR 7628 "Guidelines for Smart Grid Cybersecurity"
- NERC Critical Infrastructure Protection (CIP) standards
- IEC 62443 Series for Industrial Automation
- IEC 62351 "Cybersecurity standards and guidelines for the Smart Grid"
- Internet Engineering Task Force (IETF) Standards
- IEEE 1686 "IEEE Standard for Intelligent Electronic Devices Cyber Security Capabilities"

About the Authors

Megan J. Culler
Power Engineer / Researcher, Idaho National Laboratory

Sean Morash
Principal Consultant, EnerNex

Frances Cleveland
President and Principal Consultant, Xanthus Consulting International

Jake P. Gentle
Program Manager, Idaho National Laboratory

Brian Smith
Principal Consultant, EnerNex

Idaho National Laboratory

Critical Infrastructure Security and Resilience

resilience.inl.gov/MIRACL

Prepared for the **U.S. Department of Energy Wind Energy Technologies Office under DOE Idaho Operations Office**

Contract DE-AC07-05ID14517