# Cybersecurity Guide for Distributed Wind

August 2021

Megan J. Culler | Brian Smith | Frances Cleveland | Sean Morash | Jake P. Gentle

Idaho National Laboratory

INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance, LLC
INL/EXT-21-62264 Revision 0

# SUMMARY

Distributed wind sits at the intersection of grid-connected, off-grid, and behind-the-meter cyber-physical electric energy systems. The physical properties and communications requirements for distributed wind systems mean that there are unique cybersecurity considerations, but there is little to no existing guidance on best practices for cybersecurity. This document is intended to be a starting point for distributed wind stakeholders including manufacturers, installers and integrators, and operators (facility, aggregator, or utility). We discuss common distributed wind architectures and describe their role in the larger power system, pointing out some of the key connections to be aware of. Cybersecurity cannot exist in a vacuum, but rather must consider the entire system and all its connections holistically. The role of distributed wind and the functions it can serve are described to gain understanding of the full range of capabilities. The purpose and application of relevant standards that may apply to certain distributed wind systems are presented. These standards may not apply to all installations, but even for systems that are not required to meet these standards, they can be a good reference for best practices. A holistic threat perspective is used to describe the adversaries, threats, and potential impacts of cyberattacks, with special emphasis on what sets distributed wind systems apart from other distributed energy resources (DER). Finally, we present recommendations for cybersecurity, both in terms of needs of the system and roles that specific stakeholders should fulfill. Distributed wind systems can come in a variety of architectures and applications, so there is no one-size-fits-all approach to cybersecurity. However, this document contains the relevant information for stakeholders to identify the cybersecurity needs of their system, refer to relevant standards, and apply best practices in a manner most consistent with their security and operational goals

MEGAN J. CULLER
*Power Engineer/Researcher, Idaho National Laboratory*

BRIAN SMITH
*EnerNex*

FRANCES CLEVELAND
*Xanthus Consulting International*

SEAN MORASH
*EnerNex*

JAKE P. GENTLE
*Program Manager, Idaho National Laboratory*

## ACKNOWLEDGEMENTS

The Idaho National Laboratory team would like to thank contributors and sponsors for this work including:

The Wind Energy Technologies Office:

- Patrick Gilman
- Bret Barker

Microgrids, Infrastructure Resilience, and Advanced Controls Launchpad partners:

- Sandia National Laboratory
- Pacific Northwest National Laboratory
- National Renewable Energy Laboratory

EnerNex

Xanthus Consulting International

# 1. INTRODUCTION

Wind energy is one of the fastest growing sources of new energy installations in the United States, and distributed wind represents an important component of those installations. The total wind capacity in the United States was estimated at 110,809 megawatts (MW) at the end of the third quarter of 2020, representing over 7.3% of all installed generation capacity[1,2]. The Department of Energy's (DOE) Wind Energy Technologies Office (WETO) estimates that there is potential for installing 100 times that amount, and the DOE has set a vision for supplying 20% of end-user demand by 2030 and 35% of demand by 2050 with wind sources[3,4].

While bulk wind projects, including onshore and offshore wind farms, will play a major role in the development of wind over the next few decades, distributed wind will also play an important role. Distributed wind can be used to offset local load, ease burdens on transmission systems, and support microgrid and islanding functions. These functions set distributed wind apart from bulk wind.

From 2003 to 2019, 1,145 MW of distributed wind capacity from over 85,000 wind turbines was installed across the 50 states, Puerto Rico, the U.S. Virgin Islands, and Guam.[5] More and more of these installations are commercial and industrial projects, doubling from 2016 to 2017, and tripling from 2017 to 2018.[6] On top of that, distributed wind for utility customers is a large part of new installed capacity, while capacity installed by agricultural and residential customers is declining.[7] Notably too, in aggregate terms, the resource potential for distributed wind exceeds the U.S. electricity demand. Small and medium size turbines alone could provide for almost 120% of 2015 total U.S. electricity demand, and large turbines serving behind-the-meter loads for commercial or industrial users could provide the capacity to serve 370% of 2015 total electricity demand.[4] Economically, the feasible capacity to be installed over the next several decades is much smaller, and the market potential is still uncertain, but the resource potential for distributed wind suggests very favorable conditions.

The growing market segment and trends for rising commercial, industrial, and utility use distributed wind projects all motivate the need for a comprehensive risk analysis of distributed wind. This risk analysis should encompass not just traditional reliability considerations, but resilience as well. Resilience in the context of distributed wind power is defined by INL as: "a characteristic of the people, assets, and processes that make up the electric energy delivery system (EEDS) and their ability to identify, pre-

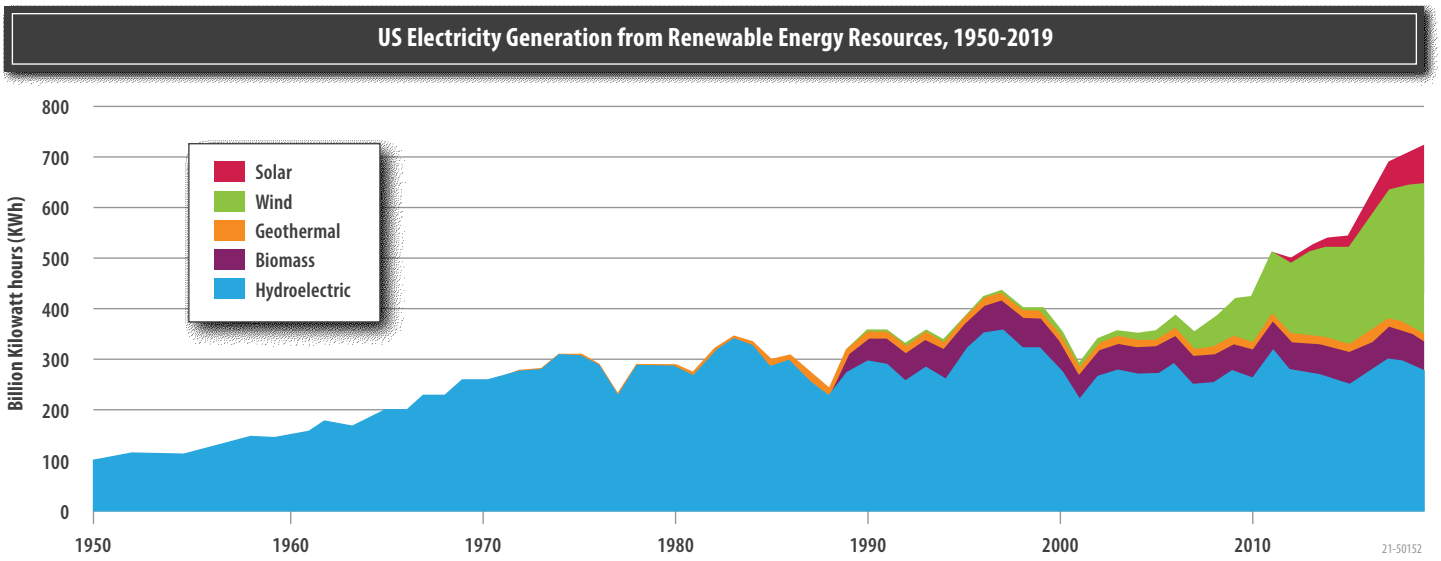



*Figure 1: Wind energy represents over 7% of all U.S. electricity generation, and about 42% of renewable energy generation in 2019. Adapted from [1].*

[1] U.S. Energy Information Administration, *"Electricity Explained: Electricity in the United States,"* 20 March 2020. [Online]. Available: https://www.eia.gov/energyexplained/electricity/electricity-in-the-us.php.

[2] WETO, U.S. Department of Energy, "*U.S. Installed and Potential Wind Power Capacity and Generation,*" [Online]. Available: https://windexchange.energy.gov/maps-data/321

[3] U.S. Department of Energy, *"Wind Vision: A New Era for Wind Power in the United States,"* 2015

[4] E. Lantz, B. Sigrin, M. Gleason, R. Preus and I. Baring-Gould, *"Assessing the Future of Distributed Wind: Opportunities for Behind-the-Meter Projects,"* National Renewable Energy Laboratory, Golden. CO, 2016

[5] A. Orrell, D. Preziuso, S. Morris, and J. Homer, *"2019 Distributed Wind Data Summary"*, Pacific Northwest National Laboratory, Richland, WA, 2020. Available: https://www.energy.gov/eere/wind/2019-wind-energy-data-technology-trends

[6] U.S. Department of Energy Wind Energy Technologies Office, *"Roadmap for Wind Cybersecurity"*, U.S. Department of Energy, 2020

[7] A. Orrell, D. Preziuso, S. Morris, J. Homer and N. Foster, *"2018 Distributed Wind Market Report"*, Pacific Northwest National Laboratory, Richland, WA, 2020

pare for, and adapt to disruptive events (in the form of changing conditions) and recover rapidly from any disturbance to an acceptable state of operation."[8] Resilience covers both cyber and physical disruptions. The White House specifically calls this out as they discuss resilience for the smart grid: "The critical infrastructure, the Smart Electric Grid, must be resilient – to be protected against both physical and cyber problems when possible, but also to cope with and recover from the inevitable disruptive event, no matter what the cause of that problem is – cyber, physical, malicious, or inadvertent."[9] In particular, the fact that these installations may be smaller than bulk wind installations and connected to distribution systems rather than transmission systems means that they may not fall under existing cybersecurity guidelines for the bulk power industry, such as the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) guidelines. However, they do fall under the cybersecurity guidelines for distributed energy resources (DER), specifically the Institute of Electrical and Electronics Engineering (IEEE) P1547.3, the Guide for Cybersecurity of Distributed Energy Resources Interconnected with Electric Power Systems, which is still under development, but which provides very detailed recommendations for DER cybersecurity.[10]

Because of distributed wind's growing importance in the future energy ecosystem, this document is intended to provide cybersecurity guidance to key distributed wind stakeholders. The remainder of Chapter 1 discusses some of the key aspects of distributed wind, including definitions, functionalities, and relevant standards. Chapter 2 discusses the need for cybersecurity in distributed wind and how to approach threat assessments. Chapter 3 provides recommendations for cybersecurity for distributed wind both from a system perspective and from a stakeholder perspective.

## 1.1 DEFINING "DISTRIBUTED WIND"

The DOE Wind Energy Technologies Office (WETO) defines distributed wind based on a wind plant's location relative to end-use and power distribution infrastructure, rather than by technology or project size.[11] Wind turbines that are installed at or near the point of end use, so that the turbine helps meet onsite energy demand or supports the operation of the existing distribution grid, are said to be in close proximity to end-use, and thus classified as distributed wind. Wind turbines that are connected on the customer side of the meter (behind-the-meter), directly to the distribution grid, or are off-grid in a remote location are also classified as distributed wind installations. Distributed wind energy systems can be used in residential, agricultural, commercial, industrial, and community applications, and they are not limited to small turbines. They can range in size from 5 kW to multi-megawatt turbines. In fact, 87.22% of new distributed-wind capacity installed in 2018 came from projects using large-scale wind turbines (greater than 1 MW in size)[7].

The DOE found that distributed wind systems could feasibly be installed on approximately 49.5 million residential, commercial, or industrial sites, or about 44% of all U.S. buildings.[4] This shows that there is a meaningful opportunity for distributed wind to play an increasing role in the U.S. electricity sector.

## 1.2 DISTRIBUTED WIND REFERENCE ARCHITECTURE

### 1.2.1 DISTRIBUTED WIND STAKEHOLDERS

The future "smart energy" power systems are being radically changed with the introduction of high penetrations of DERs, including distributed wind, which require not only different power system structures but also greatly expanded communication capabilities.

Direct control of these DERs by distribution system operators (DSOs) is neither technically feasible nor contractually acceptable for the thousands, if not millions, of DERs interconnected with the electric distribution system. At the same time, utilities are responsible for meeting the reliability and electrical requirements within their distribution systems and therefore require information on the locations, capabilities, and operational status of these DERs. It has also become clear that these DERs can greatly assist in meeting these utility requirements effectively and efficiently, thus making DER operators proactive stakeholders in managing the electric power system.

There are many different types of stakeholders involved in managing the power system with DERs. Each of these stakeholders has different business requirements and drivers which must be coordinated and managed to ensure the operation of the power grid is safe, reliable, efficient, environmentally sensitive, and least cost. Information exchange is critical to accommodate these complex and dynamic power system requirements, and management of these information exchanges needs to be organized and interoperable.

Examples of the key different stakeholders involved with DER and their possible interactions are illustrated in Figure 2, including the three main types of stakeholders responsible for implementing and managing cybersecurity: DER manufacturers, DER

[8] S. Bukowski et al., *"Distributed Wind Resilience Metrics for Electric Energy Delivery Systems,"* Idaho National Laboratory, Idaho Falls, ID, 2021. [Online]. https://resilience.inl.gov/wp-content/uploads/2021/06/INL_21-50152_Distributed-Wind_Resilience-Metrics_Final_Online-1.pdf

[9] *"Economic Benefits of Increasing Electric Grid Resilience to Weather Outages,"* Executive Office of the US President, August 2013. See: http://www.smartgrid.gov/sites/default/files/doc/files/Grid%20Resilience%20Report_FINAL.pdf

[10] Revision to IEEE 1547.3-2007 - Guide for Cybersecurity of Distributed Energy Resources Interconnected with Electric Power Systems. [Online]. https://standards.ieee.org/project/1547_3.html

[11] U.S. Department of Energy Wind Energy Technologies Office, *"Distributed Wind."* Available: https://www.energy.gov/eere/wind/distributed-wind

integrators, and DER operators. The gray arrows indicate interactions that could range from paper documents, to emails, to special types of communications. The red arrows indicate the use of communication protocols for managing DERs, which is the interaction we focus on for cybersecurity in this document. The colors of the boxes indicate the type of stakeholder: market, utility, aggregator, or facility.

Because these different stakeholders have different requirements and types of information exchanges, the communication protocols and the information models used are also often different. Therefore, it is important to better understand the architectures of DER systems and how the different stakeholders fit into these architectures.

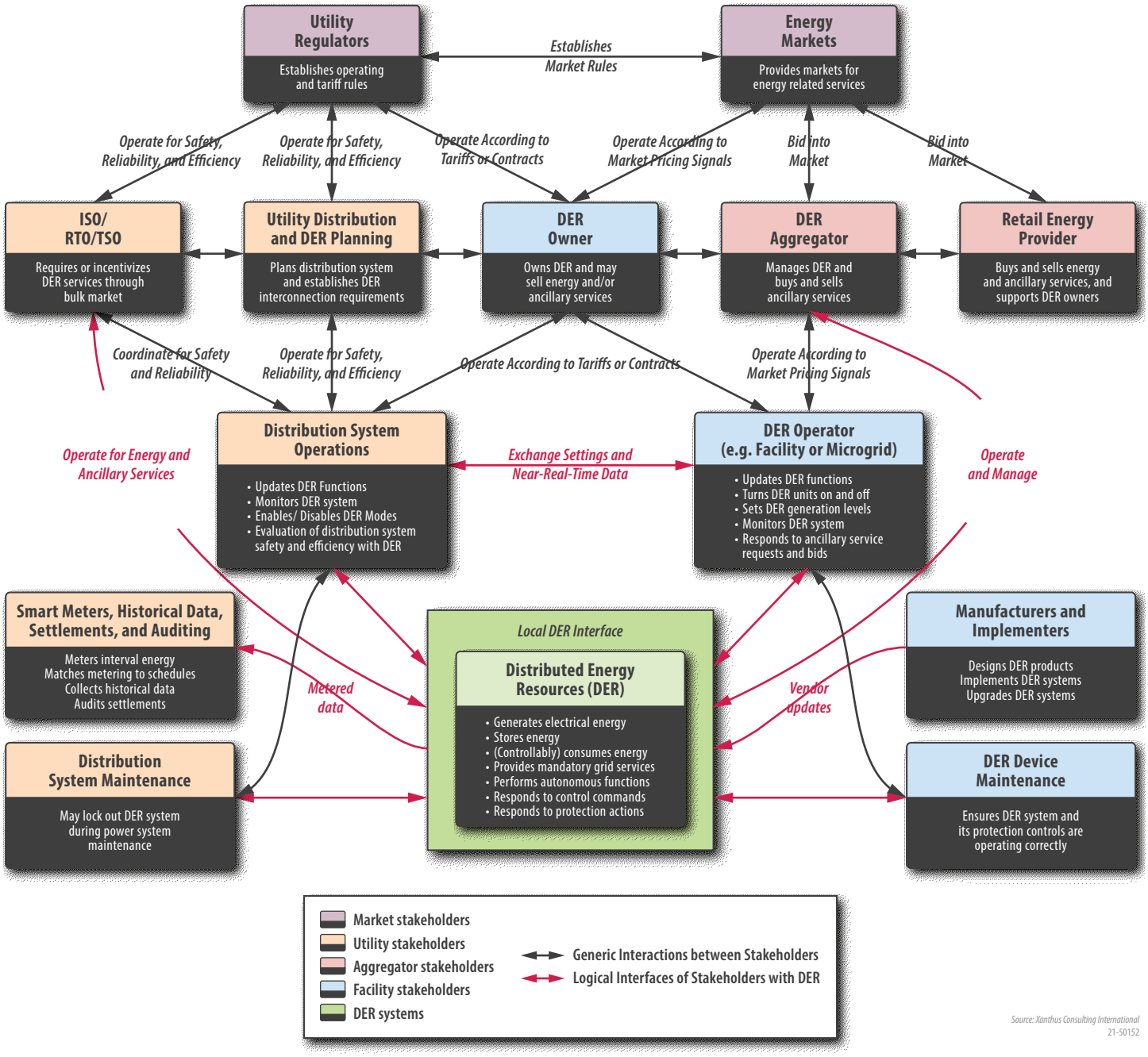
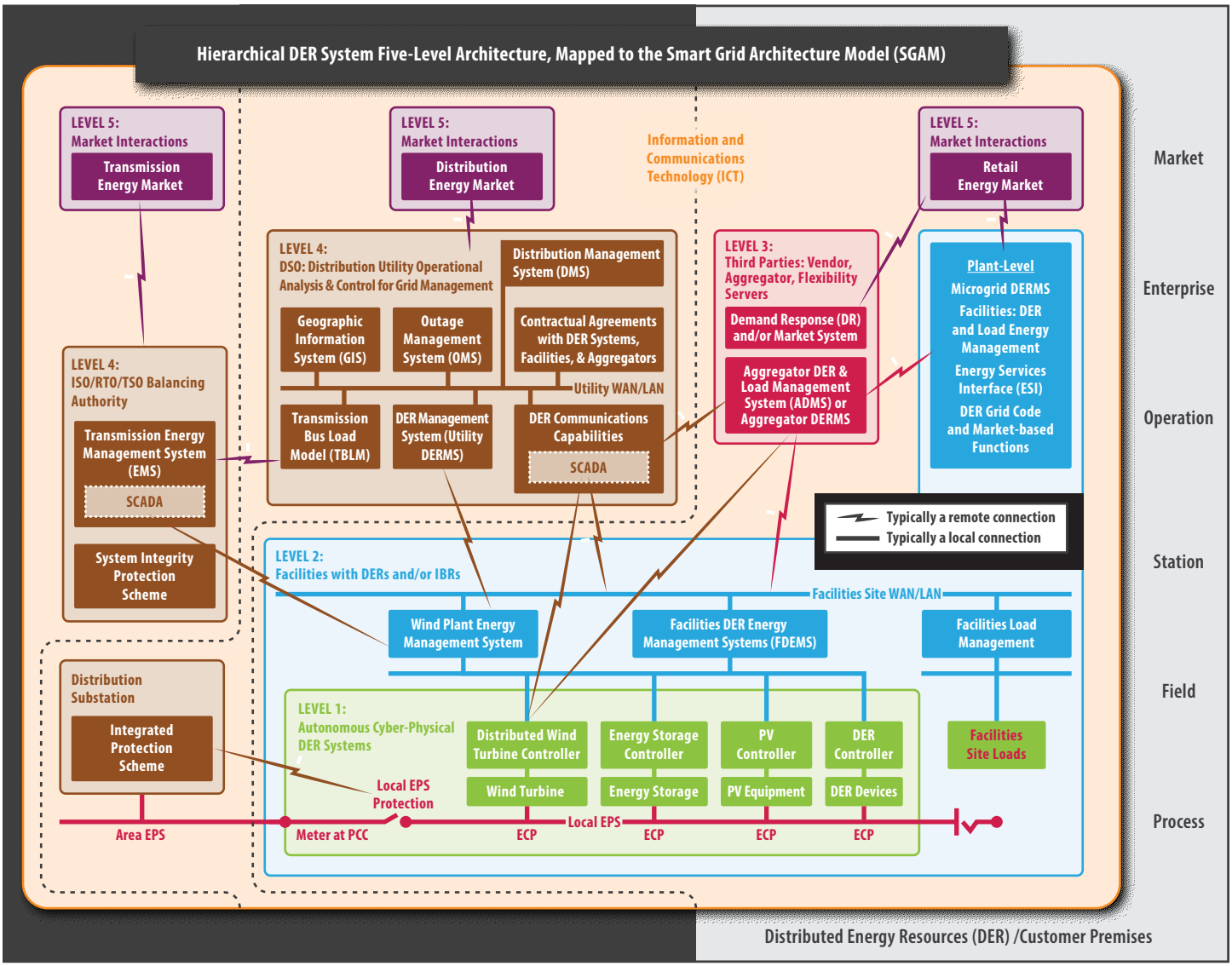



*Figure 2: DER Stakeholders*

### 1.2.2 OVERALL ARCHITECTURE OF INTEGRATED DISTRIBUTED WIND

Distributed wind installations can range from individual wind turbines managed by an aggregator to complex virtual power plants (VPP) managed as a plant, potentially with other DERs, to meet grid and market requirements. Distributed wind turbines, when connected to the distribution grid, either directly or through a facility like a campus, industrial plant or microgrid, should be treated like any other DER from an operational and electrical standpoint. This implies that distributed wind installations should meet all grid interconnection requirements, such as those defined in IEEE Std 1547:2018[12] and any utility-specified interconnection requirements, as well as cybersecurity requirements, such as those defined in IEEE P1547.3.

For this reason, the interconnections and management of distributed wind can be viewed in the context of a generic DER. An overall reference architecture from the standpoint of DER operation is introduced in Figure 3. In this figure, multiple types of DER are shown to inclusively represent the types of heterogeneous systems that may exist.




Source: Xanthus Consulting International
21-50152

*Figure 3: Architecture of Distributed Wind integrated into larger DER plants and facilities*

[12] IEEE Std 1547-2018 *"IEEE Standard for Interconnection and Interoperability of Distributed Energy Resources with Associated Electric Power Systems Interfaces"*, 2018

This reference architecture is useful for understanding the relationships and interdependencies among systems as they relate to the operation of DER and provides a foundation on which to begin to address cybersecurity needs. The different "levels" noted in the diagram and described below represent functional areas, with the potential logical communication interactions between systems also identified:

**LEVEL 1**

**DERs** (green in Figure 3) are the lowest level and include the actual cyber-physical DERs themselves. These DERs will be interconnected to local grids at Electrical Connection Points (ECPs) and to the utility grid through the Point of Common Coupling (PCC) (the ECP and the PCC may be the same if the DER is directly grid-connected). These DERs will usually be operated autonomously. In other words, these DERs will be running based on local conditions, such as photovoltaic systems operating when the sun is shining, wind turbines operating when the wind is blowing, electric vehicles charging when plugged in by the owner, and storage systems as operated by the customer. This autonomous operation can be modified by DER owner preferences, pre-set parameters, and commands issued by utilities and aggregators. Logical communication interactions cross the border of this green rectangle to support the necessary information exchanges.

**LEVEL 2**

**Facility DER Management** (blue in Figure 3) is the next higher level in which a facility DER management system (facility DERMS) manages the operation of the Level 1 DERs. This facility DERMS may be managing one or two DERs in a residential home, but more likely will be managing multiple DERs in commercial and industrial sites, such as university campuses and shopping malls. Utilities may also use a facility DERMS to handle DERs located at utility sites such as substations or power plant sites. For utilities, facility DERMS are viewed as field systems; however, from a facility's point of view, facilities may be seen as enterprises in their own right. The logical communication interactions are shown between the facility DERMS and other energy related stakeholders.

**LEVEL 3**

**Third Parties: Aggregators or Flexibility Agents** (red in Figure 3) shows market-based aggregators and retail energy providers (REP) who request or even command DERs (either through the facility's DERMS or via aggregator-provided direct communication links) to take specific actions, such as turning on or off, setting or limiting output, providing ancillary services (e.g., volt-VAR control), and other grid management functions. Aggregator DER commands would likely be price-based either to minimize customer costs or to respond to utility requirements for safety and reliability purposes. The combination of third parties (this level) and facilities (level 2) may have varying configurations, responsibilities, and operational scenarios but, overall, still fundamentally provide the same services.

**LEVEL 4**

**Utility Operational Grid Management** (brown in Figure 3) applies to utility applications that are needed to determine what requests or commands should be issued to which DERs. Distribution system operators (DSOs) must monitor the distribution power system and assess if efficiency or reliability of the power system can be improved by having DERs modify their operation. This utility assessment involves many utility control center systems, orchestrated by the distribution management system (DMS). Transmission system operators (TSOs), regional transmission operators (RTOs), or independent system operators (ISOs) may interact directly with larger DERs and/or may request services for the bulk power system from aggregated DERs through the DSO or through the REP/Aggregators. Once the utility has determined that modified requests or commands should be issued, it will send these either directly to a DER, indirectly through the facility DERMS, or indirectly through the REP/Aggregator.

**LEVEL 5**

**Market Operations** (purple in Figure 3) is the highest level, and it involves the larger energy environment where markets influence DER to provide market-based services. The TSO markets are typically bid/offer transaction energy markets between individual DER owner/operators and the TSO. At the distribution level, the markets are not yet well-formed, and, over time, may be based on individual contracts, special tariffs, demand-response signaling, and/or bid/offer transaction energy markets. At the retail level, markets can indicate general or locational marginal prices (LMP) for energy, active power, reactive, or other types of ancillary services that DER might provide.

With this larger context for DER integration in mind, we can consider configurations that are most common for distributed wind.

### 1.2.3 CUSTOMER-BASED, BEHIND-THE-METER WIND TURBINES

Customers may include small wind turbines behind the meter with the intention to serve their own loads and reduce their reliance on the local utility. In this case, they may have a configuration similar to that seen in Figure 4. These turbines may or may not be combined with other DER units, such as PV systems and battery storage systems. If they export power to the grid (according to contractual arrangements with the utility), that export may be limited in order to avoid any grid impacts. Monitoring and control communications are managed within the facility, so cybersecurity requirements are contained within the facility.

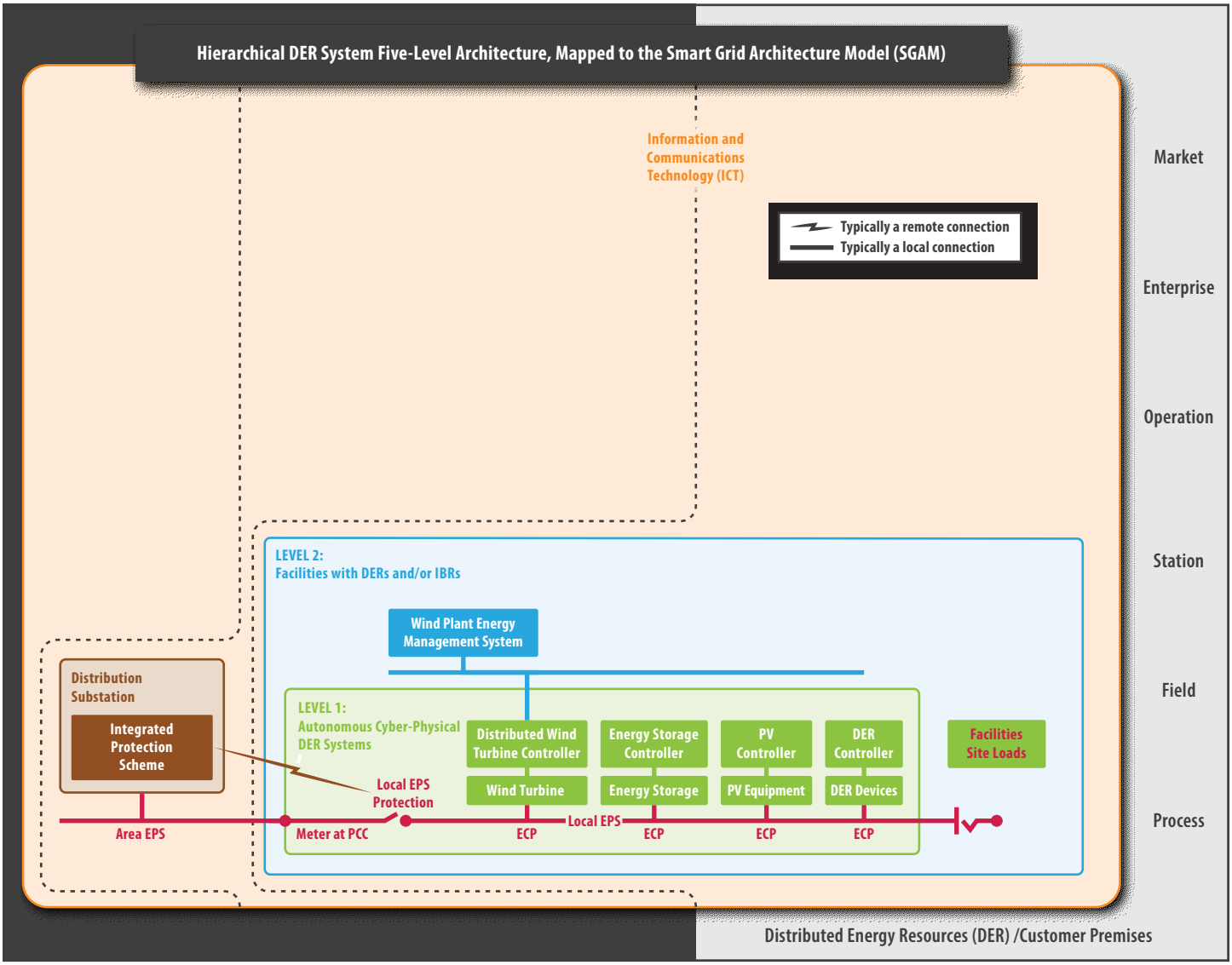
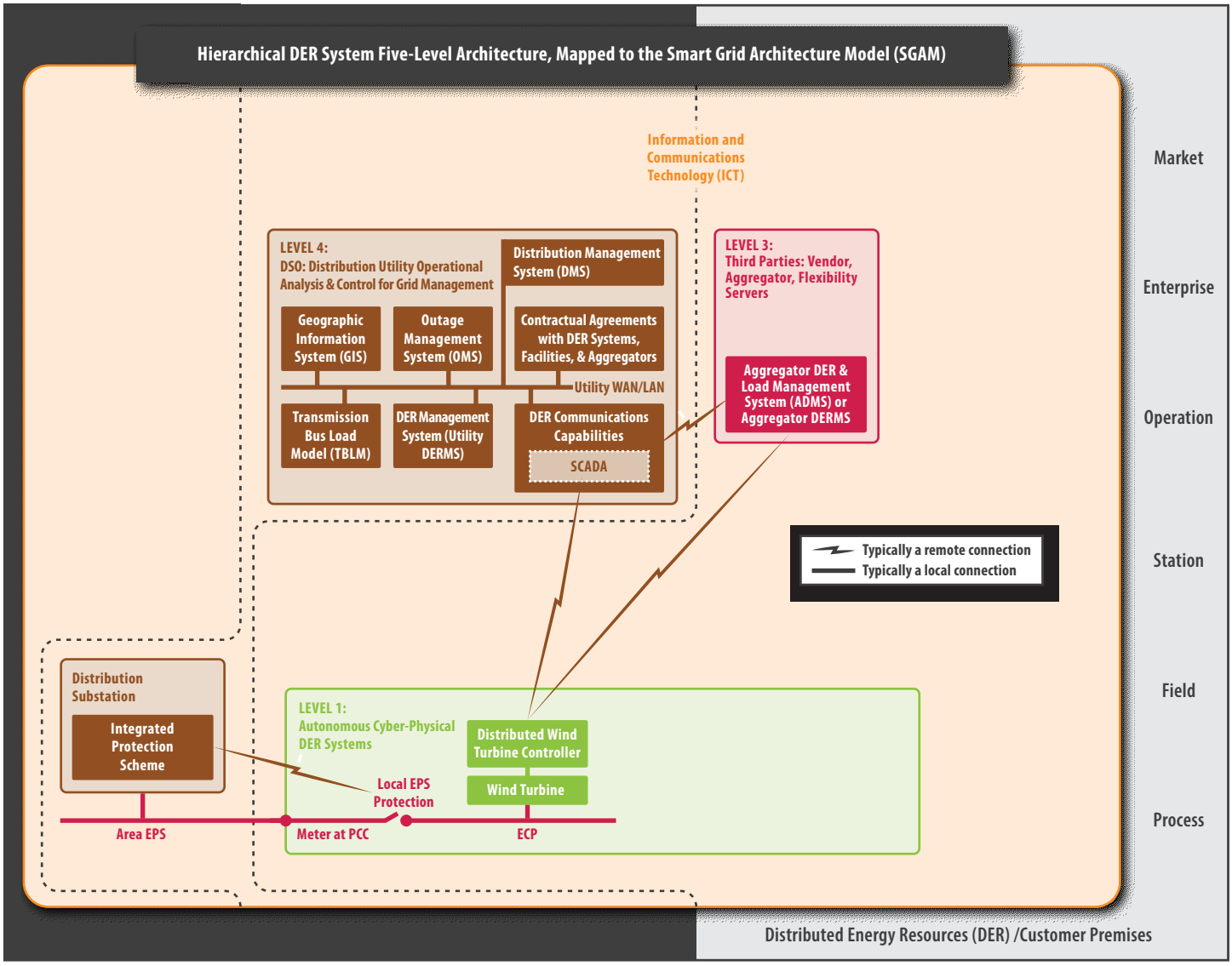



*Figure 4: Customer-based Behind-the-Meter Wind Turbines*

Source: Xanthus Consulting International
21-50152

### 1.2.4 UTILITY OR AGGREGATOR-MANAGED, GRID-CONNECTED, INDIVIDUAL WIND TURBINES

The simplest grid-connected configuration for wind turbines is that of individual turbines or a small grouping of turbines directly tied to a utility or managed by an aggregator, as seen in Figure 5. These wind turbines are widespread across various territories, sited in locations determined to be the best locations for reliable, steady, and strong wind. Because they are not in wind farms, they are individually connected to the distribution system and managed either by the utility or, more often, by an aggregator. Cybersecurity is focused on the monitoring and control communications between the individual wind turbines and the utility or aggregator.

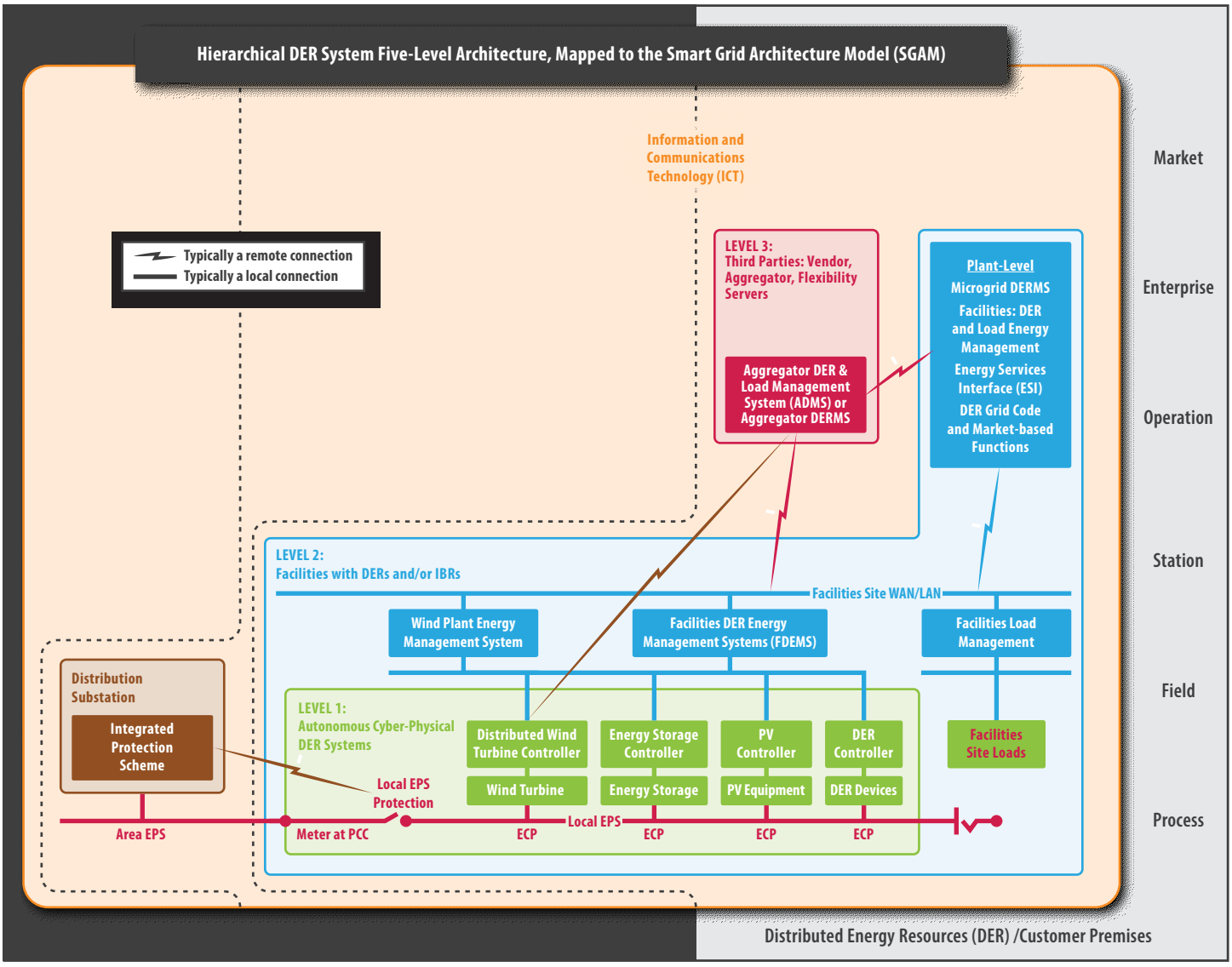



Source: Xanthus Consulting International
21-50152

*Figure 5: Utility or Aggregator Managed Individual Wind Turbines*

### 1.2.5 WIND TURBINES IN MICROGRIDS

Another configuration to consider is wind turbines in microgrids, whether these are grid-connected, intentionally or unintentionally islanded, or off-grid (see Figure 6). In this scenario, cybersecurity needs to encompass all the stakeholders, including the wind turbine units, other DER units, the facility DERMS, and the aggregators.




Source: Xanthus Consulting International
21-50152

*Figure 6: Microgrid, Campus, or Community with Wind Turbines*

## 1.3 RELEVANT STANDARDS AND REFERENCES FOR DISTRIBUTED WIND

### 1.3.1 FUNCTIONAL STANDARDS AND REFERENCES

Several standards have been developed which define the basic functionality of DER as related to grid operations and data modeling. Appendix A identifies key documents and references such as:

- **IEEE 1547-** The IEEE Standard for Interconnection and Interoperability of Distributed Energy Resources with Associated Electric Power Systems Interfaces is being integrated into many State electrical codes. IEEE 1547 defines a variety of grid functions and capability requirements for DER.
- **IEC 61850-7-420 –** This semantic data model covers all the information data objects needed for some specific types of DER (PV systems, battery storage systems, fuel cells, combined heat and power, and diesel generators), but it also includes semantic models for DER functions. In particular, it meets the IEEE 1547 interoperability requirements as well as most of the market-based functions.

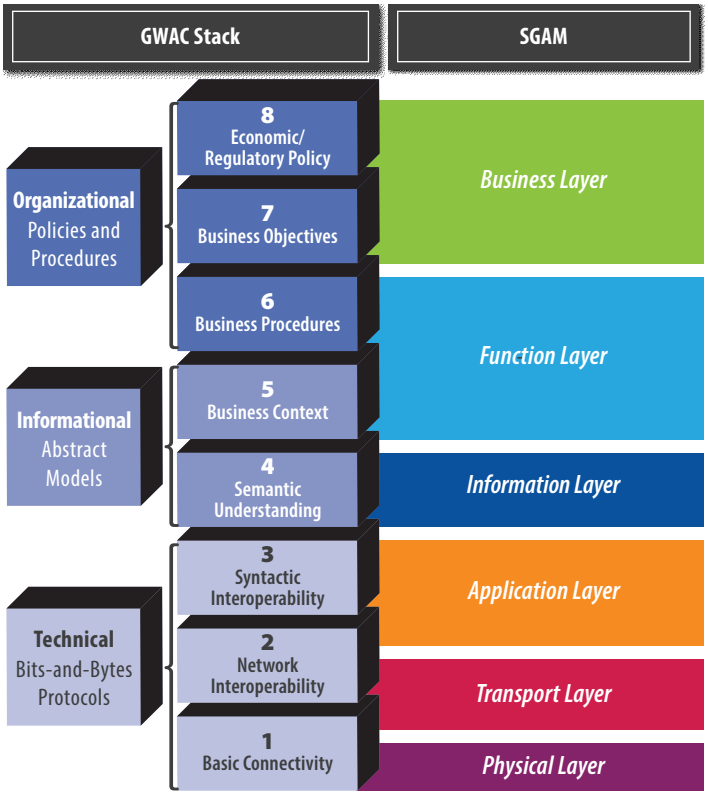



*Figure 7: GWAC Stack and SGAM*

- **IEC 61400-25-2 –** This standard provides a semantic data model for wind power plants as well as the individual wind turbines. A semantic model is the equivalent to a language: in an international meeting, a decision is made on what language to use for conversations between people from different countries, such as French, Chinese, or (often) English. The wind power language is defined in IEC 61400-25-2

### 1.3.2 COMMUNICATIONS FOR DER AND DISTRIBUTED WIND

#### 1.3.2.1 Structure of Communication Protocols

Communications involve more than the traditional concept of communication protocols (e.g., just bits and bytes going over a wire). The exchange of information involves multiple layers of interactions, involving business purposes down to the various media that could transport the information. Two methods that can be utilized to organize these layers of information exchange are the GridWise Architecture Council (GWAC) Context-Setting Framework, also known as the GWAC Stack, and the International Electrotechnical Commission's (IEC) Smart Grid Architecture Model (SGAM)[13]. There are differences between the two models in that the GWAC stack has 8 layers while the SGAM identifies 6 communication layers, but these two models are easily "mapped" to each other. The following are the primary layers (see Figure 7):

- **Business Objectives, Economic/Regulatory Policy, Business Layer:** This layer covers the business purposes for communications, including providing information for business decisions, meeting regulatory requirements, and requiring interoperability.
- **Business Context and Procedures, Function Layer:** This layer addresses the functionality and use of the data within business contexts, such as "this collection of settings, monitored information, commands, defaults, timing, etc. provide the information exchange requirements for the voltage-reactive power function" or "this is the sequence of steps with specific data exchanged in each step for a DER to perform the frequency ride-through function".
- **Semantic Understanding, Information Layer:** This layer provides the meaning of the data and acts as "nouns" in the sense of "this is the three-phase rms voltage measurement on Feeder A in Substation Z", "this is the maximum active power rating of DER B right now", or "this is the updated setting for reactive power for power plant Y".

[13] "IEC Smart Grid Standards Map," International Electrotechnical Commission (IEC). [Online]. http://smartgridstandardsmap.com/

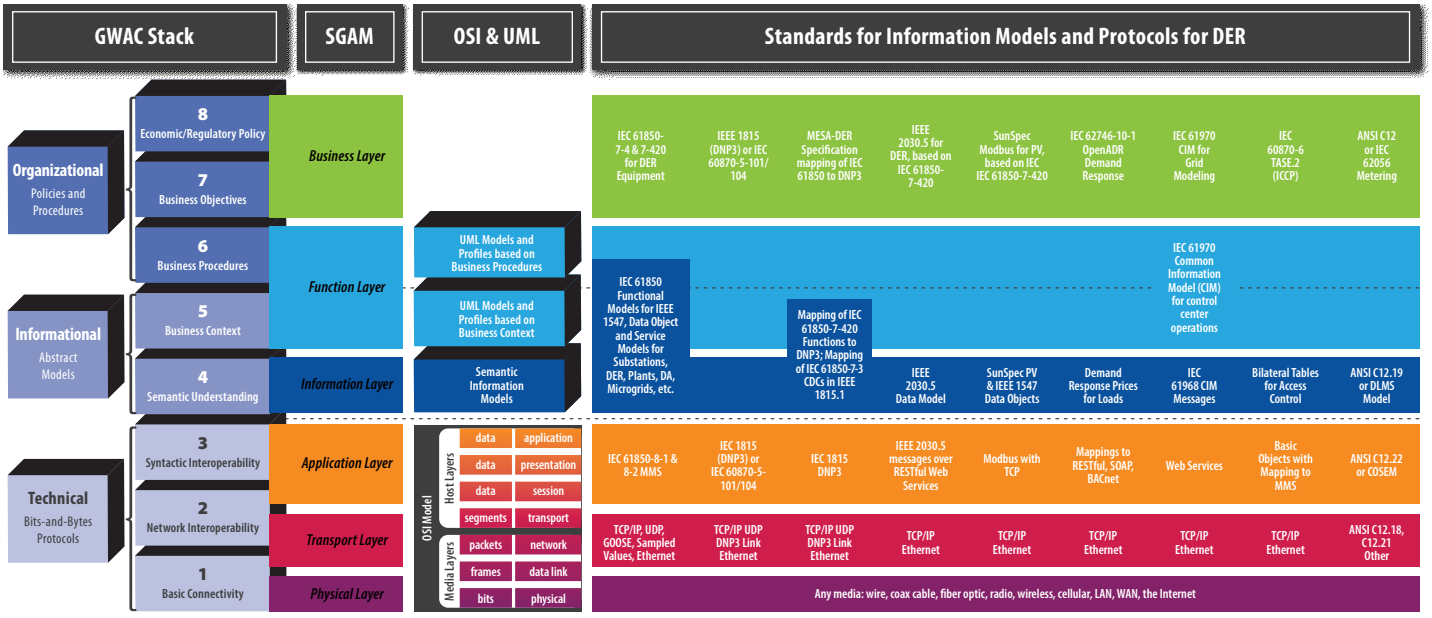
- **Syntactic Interoperability, Application Layer:** This layer provides the communication services and acts as "verbs" in the sense of "getting data", "monitoring data", "controlling data", "setting data values". It does not cover the meaning of the data, only the services.
- **Network Interoperability, Transport Layer:** This layer transports the information, usually in message packets, from one end to the other end. This may involve going through multiple nodes, gateways, routers, etc.
- **Basic Connectivity; Component Layer:** This layer encompasses the physical media, such as wires, fiber optics, coaxial cable, local area networks (LANs), and wide area networks (WANs).

#### 1.3.2.2 Range of Communication Protocol Structures

There are many different communication protocols, information models, and cybersecurity standards for DER that naturally extend to distributed wind. Each has specific capabilities based on their origins and purposes, although some have expanded over time. The core communication protocols and information models are and their relation to the illustrated in Figure 8. Appendix B provides details for four key DER communication protocols: Distributed Network Protocol (DNP3), IEC 61850-7-420, IEEE 2030.5, and SunSpec Modbus.

### 1.3.3 CYBERSECURITY STANDARDS AND GUIDELINES

There are many cybersecurity standards and guidelines relevant for DER in general and therefore applicable to distributed wind to some degree. Given the complexity of business processes and the wide variety of cyber assets used in the power operations environment, no single cybersecurity standard can address all security requirements, security controls, resilience strategies, and technologies particularly for such a complex domain as DER. For that reason, it is useful to categorize the key cybersecurity standards and guidelines. For instance, some standards and guidelines are focused on the high-level organizational security requirements and more detailed recommended controls (What), while other standards focus on the technologies that can be used to supply these cybersecurity controls (How). A third category provides guidance on how to comply with the standards (Process toward Compliance). These categories are discussed in Appendix C, which identifies the key documents along with a brief overview of each.




*Source: Xanthus Consulting International*
21-50152

*Figure 8: Core communication protocols and information models for Distributed Energy Resources (DER)*

# 2. QUALIFYING THE PROBLEM SPACE

## 2.1 THE NEED FOR DISTRIBUTED WIND CYBERSECURITY

The DOE published a Roadmap for Wind Cybersecurity in 2020, which details the challenges, motivation, and recommendations for wind cybersecurity.[14] Many of the findings in this report are directly applicable to distributed wind. We reiterate here some of the key findings which motivate the need for distributed wind cybersecurity and expand on some of the unique needs of distributed systems.

**A shifting wind energy design landscape demands an altered cybersecurity paradigm.** As discussed previously, the demand for wind energy and for distributed wind is growing and becoming an increasing part of the "smart-grid" landscape. The bidirectional communication required for this operation introduces significant cybersecurity concerns. Modern inverters are required for the dynamic operation of distributed wind systems, which require internal and external information and thus network communication capabilities. Local and remote connectivity among distributed wind turbines, control equipment, control centers, and business networks will use a range of standard and proprietary communication protocols, expanding the scope of monitoring and protection.

**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[15]. Cybersecurity companies have monitored and documented incidents that suggest malicious cyber-actors may be interested in wind. Wind assets are unique in the cybersecurity landscape due to the number of moving parts, which means that cyberattacks have the potential to cause expensive and dangerous physical damage. As inverter-based resources, wind assets also have the potential to cause destabilizing effects on connected systems if compromised, and numerous academic works have described the harmful effects of such an attack. From compromised SCADA systems allowing unauthorized control of a wind plant[16] to substation disruption through cyber and physical attack paths[17] to vulnerabilities in specific wind systems[18] and injection of malicious code,[19] the potential for cyberattacks on wind plants are diverse. Additionally, there is evidence that cyberattacks on wind energy systems have occurred.

**Distributed wind turbines can be installed for a variety of applications, but not all stakeholders may be familiar with the basic cybersecurity practices.** Because distributed wind can cover anything from a single turbine installed at a school for primarily educational purposes, to powering a remote off-grid location, or a collection of turbines powering local load or tied into the local distribution system, it may not be the case that all vendors, customers, or installers are familiar with the cybersecurity risks or mitigations associated with the wind systems. It may not seem like a risk to connect a system over a local network or directly to the internet, and some stakeholders will not take the time or effort required to understand all NERC CIP guidelines or all IEEE P1547.3 guidelines.[20] This document is intended to highlight the important risks and point readers to the appropriate sections of relevant standards to make it easy for distributed wind stakeholders to safely and securely install their systems.

**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 some distributed wind systems may fall under NERC CIP guidelines, not all do. Additionally, while distributed wind systems can benefit from work done around generic DER, there are aspects of distributed wind systems that require additional considerations (see Section 2.2- Challenges to Securing Distributed Wind Systems).

## 2.2 CHALLENGES TO SECURING DISTRIBUTED WIND SYSTEMS

Challenges to addressing cybersecurity for distributed wind installations stem from many factors. These can range from technology availability, capabilities and evolution to resource and finan-

[14] U.S Department of Energy, Office of Energy Efficiency & Renewable Energy, *"Roadmap for Wind Cybersecurity"*, July 2020.

[15] U.S Department of Energy, Office of Energy Efficiency & Renewable Energy, *"Roadmap for Wind Cybersecurity"*, July 2020, Section 3

[16] Zabetian-Hosseini, Asal, Ali Mehrizi-Sani, and Chen-Ching Liu. *"Cyberattack to Cyber-Physical Model of Wind Farm SCADA."* Paper presented at the 44th Annual Conference of the IEEE Industrial Electronics Society, Washington, D.C., October 2018. DOI:10.1109/iecon.2018.8591200.

[17] Staggs, Jason, 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.

[18] ICS-CERT. *"XZERES 442SR Wind Turbine Vulnerability."* Last modified August 27, 2018. [Online]. https://ics¬cert.us-cert.gov/advisories/ICSA-15-076-01.

[19] Yan, Jie, Chen-Ching Liu, and Manimaran Govindarasu. "Cyber Intrusion of Wind Farm SCADA System and Its Impact Analysis." Paper presented at the 2011 IEEE/PES Power Systems Conference and Exposition, Phoenix, Arizona, March 2011. DOI:10.1109/psce.2011.5772593.\

[20] IEEE 1547.3, *"Guide for Cybersecurity of Distributed Energy Resources Interconnected with Electric Power Systems"*, pending publication

cial constraints. Some aspects to consider are listed below. Many may mirror those in the DOE Roadmap for Wind Cybersecurity.

- Different protocols are used across different manufacturers. There is no single commonly accepted standard protocol, and some proprietary protocols are used, making it difficult to recommend best practices for setting up secure communication channels.
- Systems may be internet-connected for easy monitoring. The remote location of many turbines motivates even more remote controls and monitoring for distributed wind. Special care must be taken to protect these communications.
- Cyber incidents targeting wind energy systems have already occurred, just as with other aspects of the energy sector, and will likely increase in sophistication and number.[21,22,23,24]
- The wind plant lifecycle involves many parties; effective cybersecurity practices are difficult to establish, maintain, and trace through the supply chain, from construction to operation to repowering to decommissioning.
- 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.
- Few established cybersecurity standards specific to wind energy exist; some standards may apply to distributed wind if the system is large enough, but this is not universally true for distributed wind, which makes it difficult to ensure security.
- Few incentives for wind energy stakeholders have been established to prioritize cybersecurity over other investments (e.g., reliability, performance, etc.). Even fewer incentives exist for distributed wind systems, which may involve stakeholders who are not involved in distribution systems.
- Cyber threat, vulnerability, incident, and mitigation information sharing is limited among wind energy stakeholders in general. Distributed wind stakeholders may not have access to the information sharing groups that do exist.
- The current market offers few and underdeveloped wind-specific cybersecurity services, products, and strategies.
- Installation and maintenance of distributed wind systems lends itself to allowing more personnel representing different interests (installation crew, technicians, utilities, asset owner/operators) access to the system over its lifetime. This creates opportunity for reconnaissance, holes in supply chain tracking, and higher potential for insider threats.

## 2.3 RISK MANAGEMENT FOR DISTRIBUTED WIND SYSTEMS

It is impossible to predict and protect against all possible cyberattacks, so the goal of any cybersecurity strategy is to minimize risk. To address risk for distributed wind installations, it is important to examine the individual aspects of risk. In the traditional sense, the concept of risk is often illustrated using the model:


This model is a simplified expression aiming to show a relationship among the components of risk. Each of these components is covered in more detail below. Generally, the model expresses that each component influences the overall risk measure relative to a baseline. Risk assessments should consider a variety of threats, vulnerabilities, and consequences in an effort to canvas the potential outcomes wholistically. There is no explicit metric or units for risk defined here, and the components themselves can be defined differently by different organizations. Rather, risk is assessed on a relative basis. The threats, vulnerabilities, and consequences for a given system all contribute in different ways. For instance, unlikely threats with potentially large consequences may have similar risk as threats with medium likelihood and consequence. It is important to note that this is a model to demonstrate the relationships between the elements of risk as opposed to a mathematical model to calculate risk.

To manage risk, it is necessary to manage the individual elements that comprise risk to the best extent possible. Each element has sub-elements and considerations outlined below.

[21] North American Electric Reliability Corporation. Lesson Learned: Risks Posed by Firewall Firmware Vulnerabilities. Published September 4, 2019. Accessed November 20, 2019. [Online]. https://www.eenews.net/assets/2019/09/06/document_ew_02.pdf.

[22] Davidson, Ros. "AWEA 2018: Increase in Cyber Security Attacks 'inevitable', Expert Warns." Windpower Monthly. May 8, 2018. Accessed August 05, 2019. [Online]. https://www.windpowermonthly.com/article/1464061/awea-2018-increase-cyber-security-attacks-inevitable-expert-warns

[23] Sobczak, Blake. "Grid Leaders Clear the Air around Russian Hacking." Energywire. August 1, 2018. Accessed August 05, 2019. [Online]. https://www.eenews.net/stories/1060091819.

[24] Bennett, Cory. "Russian Hackers Have Infiltrated the US." The Hill. November 04, 2016. Accessed August 05, 2019. [Online]. https://thehill.com/policy/cybersecurity/223266-report-russian-hackers-infiltrate-us

### 2.3.1 THREATS: ADVERSARIES AND OBJECTIVES

Assessing risk begins with a better understanding of the capabilities, intents, and opportunities of potential adversaries. Threats can be both intentional and unintentional, but also must be evaluated by the capability of the adversary. Similar to the risk model, threat is a measure of an adversary's intent and capability.

**Threat = Intent x Capability**

Within this model, intent is considered to be the adversarial objective. Effectively, what is the adversary trying to accomplish? When examining cybersecurity threats in more detail, it is important to note that the actions of an adversary can be either intentional or unintentional. Unintentional cybersecurity threats are not malicious and in many cases are centered around errors or mistakes by someone with authorized access and privileges to a system. Intentional cybersecurity threats, on the other hand, are malicious and driven by a particular objective of the adversary which can vary widely.

One way of examining adversary objectives more closely is to look at the different types of adversaries along with their capabilities, which is the ability of the adversary to execute on their intent (or otherwise perform malicious actions). There are no standard definitions of adversary types. To support the discussion within the context of this document, four basic adversary types are identified as follows:

- **Hacker –** The basic form of a cybersecurity adversary can be a single entity or a small group of individuals. The motivation of the basic adversary in attacking a system varies but is typically centered around curiosity, notoriety, fame, or attention. While the skill set of this group in the past may have not been considered advanced, automated attack scripts and protocols that can be downloaded readily from the Internet make sophisticated attacks easier to orchestrate.
- **Insider -** Disgruntled insiders are another form of a cybersecurity adversary. Insiders often do not need a high degree of computer knowledge to manipulate a system or access sensitive data because they may be authorized to do so. Insider threats also include third-party vendors and employees who may accidentally introduce malware into systems.
- **Organized Group -** This type of adversary is typically more organized and funded than hackers or insiders and has a specific target. Examples can include a corporate organization engaged in espionage to steal trade secrets or to disclose damaging information, organized crime aimed at financial extortion via mechanisms such as ransomware, financial theft or blackmail, or hacktivists concerned with supporting political agendas. These groups are typically motivated by financial gains but may have more altruistic provocations.
- **Hostile Nation-State or Terrorist -** This type of adversary is often very structured, sophisticated, and well-funded. They are most capable of launching cyberattacks labeled as advanced persistent threats, where an adversary gains unauthorized access to a network or system and remains undetected for an extended period. These more sophisticated, organized, and persistent threat actors are often seen only by the digital traces they leave behind. Hostile nation-states and terrorist adversaries target groups such as financial institutions, political establishments, military organizations, media outlets, utilities, or manufacturing facilities with goals to disrupt major aspects of society.

### 2.3.2 VULNERABILITIES: COMMON ATTACK VECTORS

In terms of cybersecurity, a vulnerability is a weakness which can be exploited by an adversary to gain unauthorized access to or perform unauthorized actions on a system. For distributed wind installations, vulnerabilities can exist in many forms that may allow an adversary to perform actions such as run code, access a system's memory, install malware, or steal, destroy or modify data. To better understand the context of vulnerabilities in distributed wind installations, it is helpful to categorize them in terms of a layered model as shown in Figure 9. While the top layer illustrates the primary process of monitoring and controlling the mechanical and electrical characteristics of the wind turbine, it relies on the integrity of the lower layers, and thus the vulnerabilities of the elements in these layers is also critical.

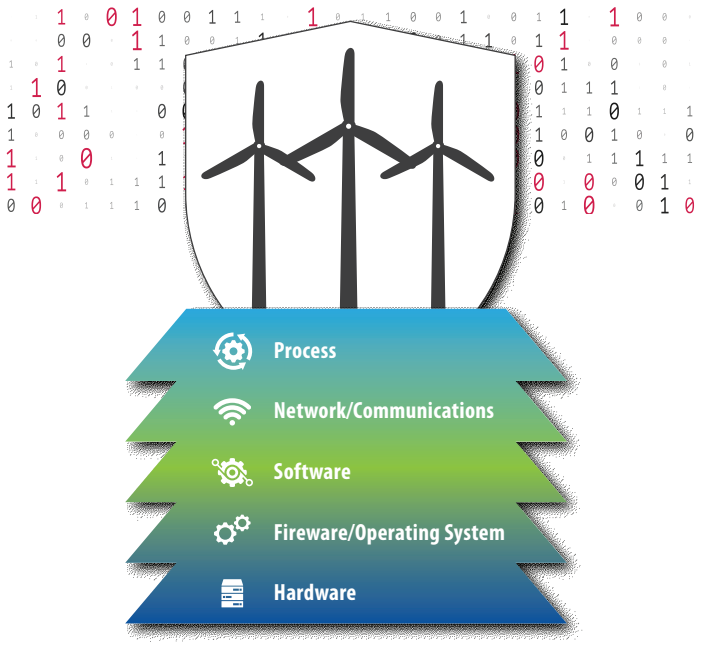



*Figure 9: Layered Distributed Wind Control System Model*

- **Hardware Layer -** This is the foundational layer of the model and includes components such as processors, memory, expansion cards, storage media, and communication interfaces. Hardware attacks such as fault injection and backdoors can occur at this layer allowing an adversary to gain access to stored information or to disrupt hardware level services. The hardware-level vulnerabilities also are a concern during the entire lifecycle of a system from design to disposal. Supply chain security relating to hardware components is a key issue since hardware trojans can be injected in any stage of the supply chain prior to installation and commissioning of the system.
- **Firmware or Operating System Layer -** The firmware or operating system (OS) relies on the lower hardware layer and supports the functions of the software layer above. It includes data and instructions to control the hardware, and its functionality ranges from booting the hardware providing runtime services to loading an OS. Vulnerabilities within the firmware or OS could be exploited by an adversary to disrupt the software layer's capability to support the process.
- **Software Layer -** The software layer is comprised of one or more applications that collectively allow the system to function as designed to support the process. Software can range from custom developed code to commercial-off-the-shelf (COTS) code. Examples of vulnerabilities in the software layer include simple coding errors, poor implementation of access control mechanisms, and improper input validation.
- **Network or Communications Layer -** The network or communications layer handles the movement of data packets internally and externally within a system. Vulnerabilities in this layer may include items such as poor perimeter defenses, weak firewall rules, lack of segmentation, or clear text protocols being utilized.
- **Process Layer -** At the top of the model is the process itself. In terms of distributed wind, this is the process of monitoring and controlling the mechanical and electrical characteristics of the wind turbine. Components within distributed wind installations may lack basic authentication and accept any properly formatted command. An adversary wishing to control the process can do so by establishing a connection with the system and sending the appropriate commands.

Vulnerabilities can be thought of as the building blocks of an attack vector, which is a sequence of steps performed by an adversary during a cyberattack. One method of modeling the relationships between threats, attack vectors, and impacts is referred to as an attack tree diagram. Figure 10 represents an attack tree model for an inverter-based DER asset.

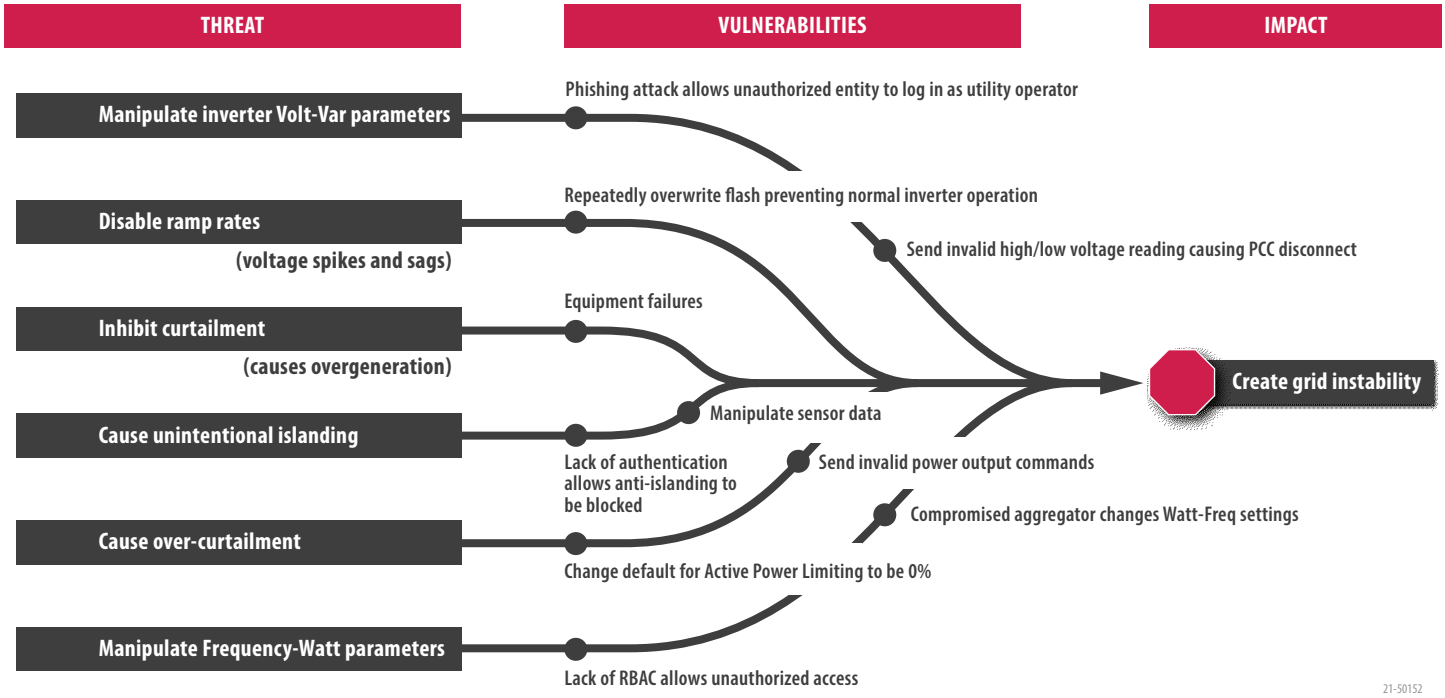



*Figure 10: Inverter-based DER Attack Tree Example*

### 2.3.3 CONSEQUENCES AND IMPACTS

One method of relating potential consequences, or impacts, of a successful compromise to a distributed wind environment is identified in the Industrial Control System (ICS) Cyber Kill Chain concept outlined in *The Industrial Control System Cyber Kill Chain*[25]. Using this concept, the methods an adversary may utilize to achieve a given functional impact are broken down into three main categories: loss, denial, and manipulation. Further decomposition of these provides nine specific methods that include a loss of view, denial of view, manipulation of view, denial of control, loss of control, manipulation of control, activation of safety, denial of safety, manipulation of safety and manipulation of sensors and instruments as illustrated in Figure 11.

These methods become the basic building blocks that can be used by an adversary in an attack on a distributed wind environment to achieve a desired outcome such as disrupting operations and/or damaging equipment. For instance, "Manipulation of Control" by an adversary may cause a wind turbine to cease generation, or "Manipulation of Sensors and Instruments" may lead to the wind turbine operating outside of its safety parameters.

Based on this concept, examples of potential impacts to key stakeholders of distributed wind installations related to each of these methods are provided in Appendix D..

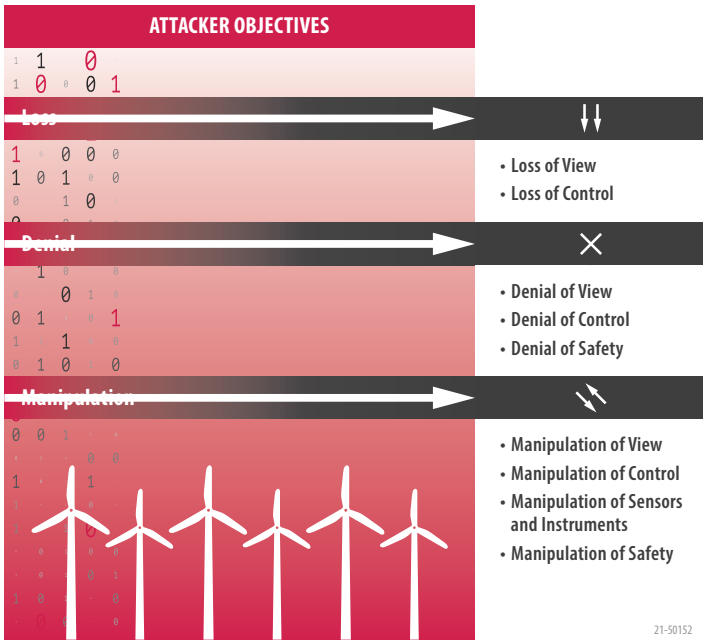



*Figure 11: Attacker Objectives and Methods According to the ICS Cyber Kill Chain*[25]

[25] M. Assante and R. Lee, "The Industrial Control System Cyber Kill Chain," SANS Institute, October 5, 2015. [Online]. https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297

# 3. KEY RECOMMENDATIONS FOR IMPROVING CYBERSECURITY OF DISTRIBUTED WIND INSTALLATIONS

The cybersecurity recommendations for distributed wind outlined in this report focus on two primary areas: DER communication protocol-specific cybersecurity recommendations as well as cybersecurity and stakeholder recommendations based on IEEE P1547.3, *Guide for Cybersecurity of Distributed Energy Resources Interconnected with Electric Power Systems*.[26]

Since IEEE P1547.3 covers DER in general, it should be used as a basis for distributed wind cybersecurity and stakeholder recommendations. It is, however, important to identify specific items or aspects of these recommendations which are key for distributed wind security. Specifically, there are two aspects of distributed wind that are different from most other types of DER:

- Distributed wind is often located in remote areas and may be difficult to access both physically and with reliable communications. (See Figure 12)
- Distributed wind has mechanical requirements, in particular, the rotating blades, the turning of the nacelle into (and out of) the wind, and the gears (if part of the design) to convert the slower blade rotation speed to the higher speed needed for the generator. (See Figure 13)

Just like other DER, distributed wind turbines can range in size, typically between 1 kW and 1 MW. This difference in size can have some implications on what cybersecurity recommendations are applicable to any specific implementation, but these implications are generally the same as for other DER. However, some distinctions on cybersecurity based on size are identified in this document as they are particularly pertinent.

Therefore, the focus of the recommendations that follow for distributed wind is on the impacts of these differences from typical DER cybersecurity recommendations. These are discussed in the following sections.

## 3.1 DISTRIBUTED WIND CYBERSECURITY RECOMMENDATIONS

### 3.1.1 OVERVIEW OF IEEE P1547.3 GUIDE FOR CYBERSECURITY OF DER INTERCONNECTED WITH ELECTRIC POWER SYSTEMS

As throughout this document, distributed wind is viewed from the lens of more general DER. For this reason, the cybersecurity recommendations for DER are also pertinent to distributed wind. Over the last years (2020 and 2021), a major effort has been underway to develop cybersecurity guidelines for DER in IEEE P1547.3. This guide provides specific and actionable technical recommendations for cybersecurity in the DER environment. The key sections include the following:

- **Section 4:** Cybersecurity Considerations for DER Interconnected to the Power System. This section provides an overview of key cybersecurity issues facing DER for non-cyber experts.
- **Section 5:** Technical Cybersecurity Recommendations for DER Operations. This section provides detailed cybersecurity considerations and recommendations that are unique or critically important for DER. Specifically, recommendations in the following categories are made:
  - Risk assessment and management (RA) recommendations
  - Communication network engineering (NE) recommendations

*Figure 12: Distributed wind is often located in remote areas*

*Figure 13: Distributed wind has mechanical requirements*

[26] IEEE 1547.3, "*Guide for Cybersecurity of Distributed Energy Resources Interconnected with Electric Power Systems*", pending publication.

- Access control (AC) recommendations
- Data security (DS) recommendations
- Security management (SM) recommendations
- Coping with and recovering from (CM) security events recommendations

- **Section 6:** DER Stakeholder Roles and Responsibilities Recommendations. This section highlights the different roles and responsibilities that various DER stakeholders would have. In particular it identifies both "engineering" security recommendations as well as "cyber" security recommendations.
- **Annex B:** Overview of DER Communications Protocols in IEEE 1547. This annex provides brief descriptions of IEEE 2030.5, IEEE 1815 (DNP3), SunSpec Modbus, and IEC 61850, as well as the MESA mapping of the IEC 61850-7-420 data model to DNP3.
- **Annex C:** Overview of Other DER Related Standards
- **Annex D:** Brief Descriptions of Key Cybersecurity Standards. This annex includes ISO/IEC 2700 series, National Institute of Standards and Technology (NIST) Cybersecurity Framework, NISTIR 7628, IEC 62443 series, IEC 62351 series, and various Internet cybersecurity standards
- **Annex E:** Guideline Recommendations Based on NIST Cybersecurity Framework. This annex provides detailed cybersecurity recommendations and justifications as listed in the NIST Cybersecurity Framework for four key DER stakeholders:
  - Security for Grid Operators for their Interconnected DER
  - Security for DER Facility Owner/Operators
  - Security for DER Aggregators/Energy Service Providers
  - Security for Vendors/Implementors of DER Systems

The following sections describe some of the most relevant recommendations as applied to distributed wind.

### 3.1.2 RISK ASSESSMENT RECOMMENDATIONS FOR DISTRIBUTED WIND

As noted in Section 2.3, risk is essentially the impact of an event scaled by the likelihood of that event. Risks will always be a part of any complex system, partly because no one can foresee all possible events and partly because risk must be balanced against the cost to ameliorate the risk. For putting astronauts in space, almost no cost limit is placed on diminishing risk because the impact of a failure could be catastrophic. However, for installing a wind turbine in a farmer's field, the cost of additional safeguards and technologies can have a major effect on deciding what safeguards are worthwhile.

To ameliorate risk, resilience needs to be improved. Resilience needs to account for all types of events, whether they are physical or cyber. For instance, a physically frozen gearbox has the same impact on resilience as an unauthorized or erroneous cyber shut-down command, while often the cause of such an event is not immediately clear.

Cyber threats are one primary focus of risk assessment for all types of DER, and are covered extensively in IEEE P1547.3. However, for distributed wind installations which are sited in rural areas or at sites that are difficult to access, risk assessments should cover additional issues related to that isolation, since cyber technologies, such as sensors, monitoring, and control, could help ameliorate the risks:

- The cross-organizational agreements that cover reliability, security, and emergency maintenance should include very specific assignments of responsibility for who will physically access the site under what conditions, and within what time frame for different situations.
- Risk assessments should include the likelihood and possible impacts from physical tampering and physical access, including over prolonged periods of time, so that locks, gates, sensors, or even CCTV may be needed to ameliorate those risks.

For all distributed wind installations, risk assessments should include environmental issues:

- Risk assessments should evaluate the likelihood and the impacts from storms or environmental events (cold, heat) at the actual site (hilltop, ocean, narrow valley, surrounding buildings) rather than just within a general location. As climate change causes more extreme events and more frequent events, additional types of sensors should be included and calibrated, with warnings and alarms provided with high importance.
- Risk assessments should drive what physical protection from those events should be included in the design and implementation, particularly with respect to the wind turbines' mechanical parts.
- Risk assessments should also include possibilities of physical damage such as wind-blown tree branches, (salt) water spray (if in/near the ocean), bullets, and collisions from vehicles.

### 3.1.3 COMMUNICATION NETWORK ENGINEERING RECOMMENDATIONS FOR DISTRIBUTED WIND

For distributed wind installations located in areas without reliable cellular or Internet availability, communication network engineering may imply different technologies, such as very

small aperture satellites (VSAT), specialized radio systems, or methods for improving the reliability of what communication technologies are available. These issues may imply:

- The bandwidth available for communications may not be adequate for "typical" traffic needed for monitoring of equipment and its security. Therefore, the design of communication traffic management should include the ability for critical security and power system data to be received in a timely manner, possibly at a higher priority than normal monitoring.
- Communications may not be able to use the commonly available protocols, due to communication response delays or slow data exchange rates. Nonetheless, authentication and authorization should be included in any protocol used.
- Certain cybersecurity management requirements, such as certificate revocation lists (CRLs) may not be able to be updated in a timely manner to the local distributed wind controller. Therefore, management of CRLs should be handled remotely for most situations, with revocations of specific certificates available through Online Certificate Status Protocol (OCSP) services.

### 3.1.4 ACCESS CONTROL RECOMMENDATIONS FOR DISTRIBUTED WIND

Again, IEEE P1547.3 covers the key remote and local access control recommendations for DER. However, for distributed wind installations which are isolated, control over local access is particularly important. 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 and would be easily detected, as it might be for most DERs located in buildings or in populated areas. Therefore, local access control recommendations for distributed wind include additional issues:

- Passwords for local access at each wind turbine site should be unique.
- Role-based access control permissions should be established so that only those access capabilities applicable to the role are allowed for local access.
- Local access attempts, whether successful or not, should be logged and should be 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) which do not have appropriate credentials should be prevented rather than just logged.

### 3.1.5 DATA SECURITY RECOMMENDATIONS FOR DISTRIBUTED WIND

For distributed wind installations, because of the sensitivity of their mechanical equipment for stress or failure, additional types of sensors for this mechanical equipment, as well as associated warnings and alarms, should be included. Specifically:

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

For historical reasons, the communication protocols used for distributed wind may not be the same as those now being used for other types of DER. In particular, the IEC 61400-25-4 semantic model identifies 5 protocols mappings: to SOAP-based web services, OPC/XML-DA, IEC 61850-8-1 MMS, IEC 60870-5-104, and IEEE 1815 (DNP3). In addition, the IEC 61400-25-2 does not include all data exchange requirements for distributed wind since it was developed for wind power plants, not individual wind turbines. Specifically, no control commands exist for individual wind turbines, nor do any of the IEEE 1547 grid code capabilities exist.

For this reason, cybersecurity for the distributed wind protocols may not meet the recommendations in IEEE P1547.3, although each of the IEC 61400-25-4 protocols has associated cybersecurity. Therefore:

- Data security should be added to any of the protocols used for distributed wind.
- Rather than inventing new semantic data objects to fill gaps, the data objects from IEC 61850-7-420 semantic model should be used to fill any semantic gaps in IEC 61400-25-2. This approach would improve interoperability and avoid possible attack vectors. Ideally, the combining of these two semantic models should be undertaken by the IEC.

### 3.1.6 SECURITY MANAGEMENT RECOMMENDATIONS FOR DISTRIBUTED WIND

The security management recommendations for DER in IEEE P1547.3 cover the security management recommendations for distributed wind, with the management of RBAC permissions and the timestamped logging of security events paramount.

### 3.1.7 COPING WITH AND RECOVERING FROM SECURITY EVENTS FOR DISTRIBUTED WIND

The coping and recovery recommendations for DER in IEEE P1547.3 cover the same recommendations for distributed wind, although some recovery efforts may be affected by the remote locations of the distributed wind turbines.

## 3.2 DISTRIBUTED WIND STAKEHOLDER RECOMMENDATIONS

The previous section described recommendations specific to the technologies used in distributed wind. Another challenge of cybersecurity is deciding who is responsible for different cybersecurity tasks. Section 6 of IEEE P1547.3 provides recommendations for different DER stakeholders including:

- Manufacturers of DER systems
- Integrators and installers of DER systems
- Testing personnel
- DER owner/grid operators/aggregators
- DER facility ICT management
- DER security managers
- DER maintenance personnel

We refer the reader to IEEE P1547.3 for more comprehensive recommendations that should form the basis of cybersecurity stakeholder recommendations. The remainder of this section discusses specific issues related to distributed wind for a subset of these stakeholders.

### 3.2.1 VARIATIONS IN CYBERSECURITY RESPONSIBILITIES OF DISTRIBUTED WIND STAKEHOLDERS

Different stakeholders have different responsibilities for cybersecurity for distributed wind systems. Even for the same stakeholder, the characteristics of the distributed wind capabilities, physical location, grid location, and utility requirements can require different levels of cybersecurity and different technologies.

The key distributed wind stakeholders include:

- Distributed wind manufacturers
- Distributed wind integrators and installers
- Distributed wind operators, who could be facility (owner) operators, utility operators, aggregator operators, or other third parties

Other distributed wind stakeholders include testing personnel, maintenance personnel, and security management personnel. However, these stakeholders would mostly have the same cybersecurity responsibilities for any DER. Therefore, the focus in this section is on the three key distributed wind stakeholders.

As noted in the section on distributed wind reference architectures, there are three basic architectures:

- Customer-based, behind-the-meter wind turbines
- Utility or aggregator managed individual wind turbines
- Wind turbines in microgrids

Even within these architectures, however, there are large differences in the cybersecurity risks posed by the wind turbines. For residential or small commercial facilities, the impact of losing or misusing a single behind-the-meter distributed wind turbine would be minimal to grid resilience, while for a large industrial plant, the unexpected loss of a number of wind turbines behind-the-meter could cause serious problems not only for the plant but for the local grid if the feeder's load were to surge rapidly.

For grid-connected wind turbines managed by utilities or aggregators, the risk would be less for the loss of a single wind turbine but the propagation of a cyberattack through many turbines could cause erratic behavior and potential failure of the turbines and consequential disturbances or outages of the grid.

For wind turbines located in microgrids (which could be a single home or a large community or even a town), cyberattacks could have minimal to 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 the characteristics of the surrounding DER and loads.

Although the cybersecurity requirements for distributed wind stakeholders are mostly the same as for other DER stakeholders, there are also a few different cybersecurity requirements due to the often-remote locations of distributed wind turbines, the mechanical aspects of rotating blades and gears, and the exposure to weather and storms. In addition, the reality is that some owner/operators of distributed wind turbines may be more knowledgeable about cybersecurity than others, may be able to implement more cybersecurity-related equipment, or may have more contingency capabilities that would ameliorate the risk.

### 3.2.2 DISTRIBUTED WIND MANUFACTURER RECOMMENDATIONS

In all cases, manufacturers should design distributed wind systems with security and resilience from the very beginning. All systems should have built-in physical and electrical protection that is designed and implemented by the manufacturer to prevent

failures from common problems, such as electrical interference, voltage spikes, cold, heat, jostling during shipping, and many other protections.

In addition, all distributed wind systems that are interconnected to the utility grid should include grid protection schemes, such as anti-islanding disconnection or intentional microgrid islanding. Although these design features reflect the engineering of the distributed wind system, since many of these features are now managed by cyber technologies (computer-based technologies), the cybersecurity for these engineering designs should be built into the systems and components from the start.

Distributed wind systems should also have their cyber components (microchips, communication modules, etc.) protected against changes that are "operationally" unreasonable, harmful, or unsafe. In addition, components should include "proof-of-identity" (such as trusted protected module (TPM) chips) to counter imitations and to provide accountability.

A few issues are possibly more critical for distributed wind manufacturers as opposed to other DER manufacturers. These include:

- Since distributed wind systems may not be easily accessible, the manufacturer's design of distributed wind systems should include more "autonomous failsafe" capabilities, including default actions if different conditions occur such as the loss of communications, the possible invalidity of key power system data, or possible physical or cyber intrusions.
- Manufacturers should include the IEEE 1547:2018 capabilities in the design of the distributed wind turbines and/or their controllers, particularly the voltage and frequency ride-through functions, the droop function, the voltage-reactive power function, and the limit active power function. The enabling and disabling of these functions should be protected so that only authenticated and authorized users can issue those commands and any associated settings.
- As with all DER, validity checking of data should be required, but with distributed wind, due to the sensitivity of the mechanical equipment, the manufacturer should require validity checking of all parameters that could harm the mechanical equipment, including combinations of parameters (e.g., issue a brake command to the blades at the same time as requesting additional active power).

All wind turbines should include role-based access capabilities, although smaller turbines might employ "standardized" roles with "standardized" capabilities. In all cases, control capabilities should be separated from monitoring capabilities, vendor upgrades and patches should be validated through two-factor authentication, and security logging should not be changeable.

### 3.2.3 DISTRIBUTED WIND INTEGRATOR AND INSTALLER RECOMMENDATIONS

Integrators and installers of distributed wind systems may have broader variations in their cybersecurity responsibilities. For smaller installations, "turnkey" approaches may be the most practical. These turnkey cybersecurity responsibilities should include:

- A cybersecurity contract should be signed by all stakeholders. It should lay out the responsibilities of each stakeholder with respect to documentation of the wind turbine, the cyber protection measures available for operation and maintenance purposes, the notification requirements on the detection of possible cyber problems (cyberattacks or cyber equipment failures), any coping plans, and any recovery plans.
- There should be proof that all applicable national, regional, and utility cybersecurity requirements are included, documented, and tested for the distributed wind system.
- All appropriate cybersecurity measures are enabled when the distributed wind system is installed.
- The user's password must be changed before the wind turbine is first turned on.

For larger and more customized installations, additional cybersecurity responsibilities should be included:

- Communication networks should be designed to isolate power system management from business networks.
- Communication "conduits" between different networks, such as firewalls and gateways, should be locked down to ensure that only authorized data can be exchanged between networks.
- Network management, such as with Simple Network Management Protocol (SNMP), should provide monitoring of key network parameters.
- Role-based access control (RBAC) should permit only authorized users (human and software applications) to view, read, write (control), create, and delete data. This RBAC capability could range from simple (read-only wind turbine data for most users, read-write for operators) to detailed assignment of data access permissions of many different users (utility operator, wind operator, aggregator, maintenance, vendor, etc.) to different types of data (power data, mechanical data, alarms, maintenance data, etc.)

Although all of the IEEE P1547.3 recommendations for integrators and installers are relevant for distributed wind, some recommendations are more appropriate to "critical" distributed

wind, either due to their size, their purpose, and/or their impact on the grid. These include:

- The integrators should ensure that redundant or backup communications are available. This may imply the use of backup communications via satellite or special radio-based systems.
- Since communications may be lost, integrators should enable all critical functions and/or set the default actions that the wind turbine should take under different situations. These situations could be physical events like storms or could be cyber events like conflicting data being received from redundant sources.
- The integrators should test all the scenarios, either as part of studies or in the field.

Since manufacturers usually include options for different types and levels of security, it is up to the integrators to meet the distributed wind owner or regional cybersecurity requirements (which may be mandated by the utility interconnection requirements) through the appropriate selection and testing of the cybersecurity cryptography suites, methods for establishing secure channels, and implementing appropriate key management processes.

### 3.2.4 DISTRIBUTED WIND OPERATOR (FACILITY/UTILITY/AGGREGATOR) RECOMMENDATIONS

For distributed wind operators (facility/utility/aggregator), authentication and authorization for role-based access to the systems (RBAC) are the most critical communications cybersecurity requirements. Confidentiality is important where privacy and/or market interactions are involved. Some operators may have access to distributed wind systems directly through a local HMI while remote access by most operators would require access via a network. Figure 14 illustrates the security architecture for interactions between distributed wind turbines and facility, utility, and aggregator operators.

IEEE P1547.3 covers the recommendations for these operators, but special emphasis should be on the security of the RBAC capabilities due to the remote location and mechanical vulnerabilities of distributed wind.

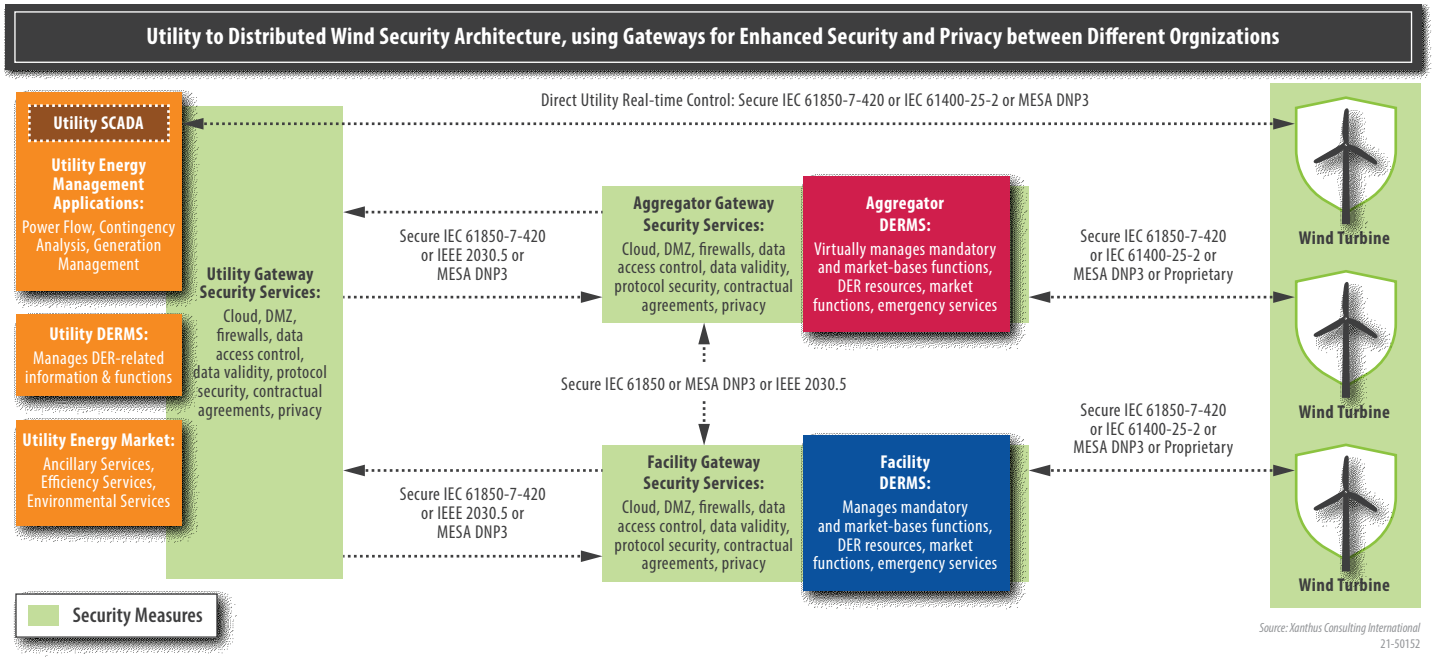



*Figure 14: Example of distributed wind security configurations with gateways to minimize the security and privacy risks between organizations*

## 3.3 CYBERSECURITY RECOMMENDATIONS FOR KEY DER COMMUNICATION PROTOCOLS

### 3.3.1 KEY CYBERSECURITY REQUIREMENTS FOR DER COMMUNICATION PROTOCOLS

Some of the most vulnerable aspects of any DER are exchanges of data between stakeholders, particularly with the DER itself. Communication protocols carry this data and therefore these protocols should be protected against cyber threats.

For distributed wind systems, the security requirements must reflect that there can be physical impacts due to deliberate or even inadvertent cyber events. Therefore, the key security requirements for data that could impact these cyber-physical systems are availability, integrity, confidentiality, authentication, authorization, and non-repudiation. Each of these security requirements are described below. Most of these security requirements rely primarily (but not exclusively) on cryptographic techniques, but data integrity and availability often rely more on engineering techniques (e.g. data validation, network design, and redundancy) than cryptographic techniques:

- **Authentication** verifies the identity of entities and provides assurance on both sides of a communication link that the entity is who it says it is. This assurance can be made through digital certificates or other security tokens which are formally bound to that entity. Mutual authentication should be used every time an association is established between entities.
- **Authorization** establishes the access requirements, namely which users or systems or applications are permitted to read, write, create, delete, etc. specific types of information. RBAC is the primary technique for ensuring that the access to stored data or to data in transit is authorized. Authorization ensures that only authorized users, devices, and systems, based on their roles, may access (monitor, control, update, etc.) specific information. This prevents unauthorized entities from modifying or even accessing information that they should not be able to access.
- **Availability** is the probability that an asset, under the combined influence of its reliability, maintainability, and security, will be able to fulfill its required function over a stated period, or at a given point in time[27]. Availability, more than the other security requirements, generally relies on engineering design, configuration management, redundancy, functional analysis, communication network analysis, and engineering practices. For instance, availability can be enhanced not only if systems, applications, and communication networks are redundant, but also if their performance and health is continuously monitored. Cyber-physical systems require high availability as they operate in very dynamic and rapidly changing situations. Monitoring the availability of the networks, systems, and applications through SNMP or other networking techniques is critical to reliable operation of these cyber-physical systems.
- **Integrity** provides mechanisms to detect unauthorized and unintentional data modifications, dropped, or repeated messages (e.g., data integrity). Integrity also reflects the logical correctness and reliability of the operating system, the logical completeness of the hardware and software implementing the protection mechanisms, and the consistency of the data structures and occurrence of the stored data. Cryptographic authentication algorithms typically calculate a message authentication code or digital signature to verify the authenticity and integrity of the message. Integrity of data is critical for cyber-physical systems since they rely on accurate information to perform their activities. Encryption does not necessarily provide integrity. Therefore, additional security techniques such as digital signatures or hashing techniques need to be used to ensure that data in transit has not been modified.
- **Confidentiality** protects information from unauthorized or unintended disclosure. To protect data (e.g. power controls functions, communication functions, personally identifiable information) from disclosure during transmission, cryptographic mechanisms are used. Encryption algorithms are used to transform plaintext data, using an encryption key, into unintelligible data called ciphertext. Decryption algorithms are used to transform ciphertext data, using an encryption key, back to plaintext. In addition, forward secrecy in the form of a new session key per transport layer security (TLS) session is used, thereby preventing the leaking of all data once a key is compromised.
- **Non-repudiation** prevents the denial of having received data that was sent to the entity or the denial of authorship of data that was sent by the entity. Non-repudiation entails mechanisms such as acknowledging the receipt of data and the use of digital signatures.

It is important to note that defense-in-depth of these cyber-physical systems lies not just with cryptography. Techniques such as filtering network traffic by port and IP addresses, patch management, secure network architecture, operating system hardening, and log monitoring are also necessary cybersecurity requirements.

[27] *IEC 62443-1-1: Industrial communication networks – Network and system security – Part 1-1 Terminology, concepts and models,* International Electrotechnical Commission, 2009.

### 3.3.2 CYBERSECURITY CHARACTERISTICS OF KEY DER PROTOCOLS

Although many communication protocols can be (and are being) used to communication with DER, IEEE 1547-2018 identifies four standard (or de facto standard in the case of SunSpec Modbus) communication protocols that are predominantly used for interactions with DER and would most likely be used for distributed wind. Since this IEEE DER interconnection standard is expected to be required for most DER that are interconnected to the grid, it is most likely that these will also be used for distributed wind. Therefore, it is important to assess what these communication protocols can be used for and what their cybersecurity characteristics are.

The four communication protocols consist of the following (see Appendix B for more details on each protocol):

- IEC 61850 (IEC 61400-25)
- IEEE Std 1815 (DNP3)
- IEEE 2030.5
- SunSpec Modbus

As shown in Table 1, the characteristics of each of these communication protocols include:

- **Standards and documents defining the DER protocols.** Specifically for standards to be "interoperable" (i.e. able to be used across many different utilities, devices, and implementations), they must include information models that clearly define the meaning of the protocol's bits and bytes being exchanged. For example, data point #123 should always mean the same thing (e.g. active power output) whether the protocol is sending the data to utility A or to utility B. In addition, some standards include cybersecurity within the standard itself, while other reference other cybersecurity standards.
- **DER protocol purposes, capabilities, strengths, and weaknesses.** The communication standards were all originally developed with different purposes, which makes them more appropriate for some applications than for others. For instance, IEC 61850 was originally developed for protective relaying in substation automation (sub-second latencies), and later expanded to DER, while DNP3 was developed for SCADA interactions (1 or 2 second latencies) and it (or its sister protocol IEC 60870-5-104) is used by most utilities around the world. IEEE 2030.5 was developed for multi-second to multi-minute interactions with home devices, while Modbus was developed for internal device engineering purposes without cybersecurity requirements.
- **DER protocol cybersecurity capabilities.** The communication standards include different types of protection, authentication, authorization, encryption, and cryptographic key management. Each of the four protocols have different cybersecurity capabilities. Modbus does not have any intrinsic security capabilities and needs to be transmitted through VPNs for security.

*Table 1: DER Protocol and Cybersecurity Characteristics*

| DER Communications | IEC 61850 (IEC 61400-25) | IEEE 1815 (DNP3) | IEEE 2030.5 | SunSpec Modbus |
|---|---|---|---|---|
| **DER Protocol Structure** | | | | |
| **Protocol Specification** | IEC 61850-8-1 (MMS client server) or IEC 61850-8-2 (XMPP)<br>Web services<br>IEEE 1815 (DNP3)<br>IEC 60870-5-101/104<br>OPC/UA | IEEE Std 1815 (DNP3): DNP3 serial or DNP3 Networked | IEEE 2030.5 RESTful client-server web services (HTTPS over TCP/IP) | Modbus |
| **Information Model** | IEC 61850-7-420 | MESA Specification mapping of IEC 61850 to DNP3 Application Note | IEEE 2030.5 XML schema + California Smart Inverter Profile (CSIP) | SunSpec or MESA Models |
| **Cybersecurity** | IEC 62351 Series for the IEC protocols | IEEE Std 1815 SA v5 current. (v6 under development). Based on IEC 62351-5 | IEEE 2030.5 and CSIP | None |

| DER Communications | IEC 61850 (IEC 61400-25) | IEEE 1815 (DNP3) | IEEE 2030.5 | SunSpec Modbus |
|---|---|---|---|---|
| **DER Protocol Capabilities** | | | | |
| **Scope of DER Monitoring and Control** | DER units, DER systems, DER facilities, DER plants, microgrids | DER units, DER systems, DER facilities, DER plants, microgrids | DER units, DER systems, DER facilities, DER plants | DER components, DER controllers, DER units, DER facilities, DER plants |
| **Specific DER Types Supported** | PV systems, PV panel and controller, energy storage systems, battery components, fuel cells, combined heat and power, diesel generators, hydro plants, gas turbines | PV systems, energy storage systems, battery components | PV systems, home automation devices | PV systems, PV panel and controller, energy storage systems, storage components, |
| **DER Functions Supported** | IEEE 1547 functions, market-based functions, autonomous functions, microgrid functions, scheduling of functions | IEEE 1547 functions, market-based functions, autonomous functions, scheduling of functions | IEEE 1547 functions, market-based functions, autonomous functions | IEEE 1547 functions, market-based functions, autonomous functions |
| **Scope of Information Model** | DER functions, DER controllers, DER devices, substation automation, protective relaying, distribution automation | DER functions, DER controllers, RTUs, distribution automation | DER functions, home automation | DER functions, DER controllers, DER devices |
| **Implementation of Information Model** | IEC 61850-6: System Configuration Language (SCL) | Manual | Manual | Manual |
| **Types of Data Transmitted** | DER nameplate & operational settings, IEEE 1547 functional parameters, control, status, measurements, schedules, alarms, logs, etc. | Data objects with defined attributes and priority levels | DER measurement and control data | DER measurement and control data |
| **Data Acquisition Modes** | Publish/Subscribe | Poll/Respond with Report by Exception<br>Unsolicited Reporting | Publish/Subscribe | Poll/Respond Only |
| **Device Time Synchronization Supported** | Yes | Yes | Yes | No |
| **Time Tagged/Event Data Supported** | Yes | Yes | Yes | No |
| **Supported Transport Layer Protocols** | IEC 61850-8-1 (Client-Server, GOOSE), IEC 61850-8-2 (XMPP) over UDP or TCP | Serial, TCP, or UDP | TCP or UDP | Serial or TCP |
| **Supported Network Layer Protocols** | IPv4, IPv6 | IPv4, IPv6 | IPv4, IPv6 | IPv4, IPv6 |
| **Performance characteristics of protocol** | Monitoring and control in real-time (4 ms for GOOSE and sampled values, 1 second for client-server) | Monitoring and control in real-time (a few ms for point-to-point, 1 second for client-server) | Monitoring and control in near-real-time (multiple seconds to minutes for monitoring and using restful scheme for control) | Monitoring and control in real-time (a few ms for device level interactions, 1 second for client-server) |
| **Testing and Certification Program** | Yes, UCA International User Group | Yes, DNP Users Group | Yes, SunSpec certifies the results from authorized Test Labs | No |

| DER Communications | IEC 61850 (IEC 61400-25) | IEEE 1815 (DNP3) | IEEE 2030.5 | SunSpec Modbus |
|---|---|---|---|---|
| **DER Protocol Cybersecurity Capabilities** | | | | |
| **Associated Protocol Cybersecurity Requirements** | IEC 62351 series | IEEE Std 1815 (based on IEC 62351-5 and currently being updated to v6) available for both DNP serial and DNP LAN/WAN | IEEE 2030.5 + CSIP | Modbus TCP via a TLS 1.2 wrapper. No security available for Modbus serial. |
| **Application Layer Authentication Supported** | Yes, IEC 62351-4 (MMS, XMPP), IEC 62351-6 (GOOSE) | Yes, based on IEC 62351-5 | Yes, authenticated encryption of client identity<br>No authentication of individual users within client facilities | No |
| **Transport Layer Authentication Supported** | Yes, IEC 62351-3 with specific requirements for TLS 1.2 or 1.3 | Yes, TLS 1.2 for TCP | Yes, TLS 1.2 for TCP | No for Modbus serial<br>Yes for Modbus TCP, TLS 1.2 for Modbus TCP |
| **Authorization Supported** | Yes, Role-based access control by type of service and by specific data objects, as defined in IEC 61850-90-19, based on IEC 62351-8 and using XACML (in process) | Yes. In v6, AMP provides an optional centralized authorization mechanism in which the connectivity and RBAC roles permitted for each pair of devices in the system is approved via a centralized system called an Authority. Optionally, Access Control Lists (ACLs) may be configured on the outstation to enforce permissions at a per-point level. | Yes, access control of clients by white listing in servers. Access control by type of service (read, write, control) | No |
| **Confidentiality** | Yes, IEC 62351-4: Available at both Application Layer and Transport Layer | Available at Application Layer in new version 6 and at Transport Layer | Mandatory encryption of client identity | Only at Transport Layer |
| **Integrity Protection and Tamper Detection** | Yes, via IEC 62351-3 and IEC 62351-4 | Yes, by v5 or v6 | Yes | No |
| **Non-Repudiation** | Via security logging and network management in IEC 62351-7 | Not natively | Not natively | Not natively |
| **Man-in-the-Middle Protection** | Yes, via IEC 62351-3 and IEC 62351-4 | Yes, by TLS | If TLS is end-to-end | If TLS is end-to-end |
| **Masquerade Protection** | Yes, via IEC 62351-3 and IEC 62351-4 | Yes, by v5 or v6 | Using white listing in server | No |
| **Replay Protection** | Yes, via IEC 62351-3 and IEC 62351-4 | Yes, by v5 or v6 | Yes | No |
| **Cryptographic Key Management and Distribution** | IEC 62351-9: Public Key Infrastructure (PKI). Use X.509 digital certificates for authentication. | Public Key Infrastructure (PKI). Use X.509 digital certificates for authentication | CSIP document, Public Key Infrastructure (PKI). Use X.509 digital certificates for authentication | Public Key Infrastructure (PKI). Use X.509 digital certificates for authentication for Modbus-TCP |
| **Symmetric Keys** | IEC 62351-9: Secret keys, Group Domain of Interpretation (GDOI) for groups of devices | Secret keys, pre-shared keys in v5 (v6 uses a Low-Entropy Shared Secret (LESS) for enrollment) | Secret keys | No |
| **Certificate Revocation Management** | IEC 62351-9: Certificate Revocation List (CRL), Online Certificate Status Protocol (OCSP) | Certificate revocation handled at Master Station. | Certificates do not expire, so CRLs and OCSP prohibited | No |
| **Encryption Technologies** | TLS_DH_DSS_WITH_AES_256_SHA as mandatory, but others are permitted | Multiple TLS cipher suites are permitted, but TLS_RSA_WITH_AES_128_SHA shall be supported at minimum | TLS_ECDHE_ECDSA with AES_128_CCM_8 | None |
| **Deep Packet Inspection** | IEC 62351-90-2 recommendations | Outside scope of standard | Outside scope of standard | Outside scope of standard |
| **Security Management** | IEC 62351-9: Enrolment of devices. Encryption technologies can be renegotiated | IEEE Std 1815 update (in process) | Encryption technologies fixed for devices | None |
| **Testing and Certification of Cybersecurity** | IEC 62351-100-1 for IEC 62351-3; IEC 62351-100-6 for IEC 62351-6 (in process) | DNP Users Group and authorized test labs | Yes, SunSpec certifies the results from authorized Test Labs | No |

# 4. CONCLUSION

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 and the various non-utility distributed wind stakeholders play a key role in this new paradigm. The growth of DER across the grid mandates consideration of cybersecurity through a new lens. Distributed wind systems must account for the communications, remote access, and physical isolation characteristics that will play a role in cybersecurity risks.

Cyber threats to wind energy technology have been demonstrated in academic exercises, and real-world attacks have shown that wind energy companies are valuable targets for cyber adversaries. It is important that systems with distributed wind consider the cybersecurity implications as wind penetration continues to increase.

Distributed wind systems can come in a variety of sizes and applications. The distinctiveness of each system makes it difficult to prescribe precise recommendations that are applicable across all systems or account for all roles for all stakeholders. The guidance in this document is broadly applicable but requires some discernment on the part of the user to apply the recommendations to their specific system and ensure that appropriate actor roles and requirements are specified.

As illustrated in this document, a recommended strategy for users is to utilize the recommendations provided in IEEE P1547.3, Guide for Cybersecurity of Distributed Energy Resources Interconnected with Electric Power Systems as a basis for distributed wind cybersecurity guidance. It is, however, important to identify specific items or aspects of these recommendations which are key for distributed wind security. Specifically, there are two aspects of distributed wind that are different from most other types of DER:

- Distributed wind is often located in remote areas and may be difficult to access both physically and with reliable communications.
- Distributed wind has mechanical requirements including, the rotating blades, the turning of the nacelle into (and out of) the wind, and the gears (if part of the design) to convert the slower blade rotation speed to the higher speed needed for the generator.

Specific areas where guidance for distributed wind installations may vary from or may need more emphasis than typical DER include:

- **Risk assessment and management (RA) recommendations -** For distributed wind installations, risk assessments should factor in the exposure to the environmental elements and potential physical isolation of the systems.
- **Communication network engineering (NE) recommendations -** For distributed wind installations, the design of communication traffic management should include the ability for critical security and power system data to be received in a timely manner, possibly at a higher priority than normal monitoring. Authentication and authorization should be included in any communications protocol used for data exchanges within and between systems.
- **Access control (AC) recommendations -** For distributed wind installations which are isolated, control over local access is particularly important and should include elements such as the use of unique passwords, RBAC, access management, and active monitoring.
- **Data security (DS) recommendations -** For distributed wind installations, because of the sensitivity of their mechanical equipment for stress or failure, additional types of sensors for this mechanical equipment, as well as associated warnings and alarms, should be included.
- **Security management (SM) recommendations -** The security management recommendations for DER in IEEE P1547.3 cover the security management recommendations for distributed wind, with the management of RBAC permissions and the timestamped logging of security events paramount.
- **Coping with and recovering from (CM) security events recommendations -** The coping and recovery recommendations for DER in IEEE P1547.3 cover the same recommendations for distributed wind, although some recovery efforts may be affected by the remote locations of the distributed wind turbines.

Different stakeholders have different responsibilities for cybersecurity for distributed wind systems. Even for the same stakeholder, the characteristics of the distributed wind capabilities, physical location, grid location, and utility requirements can require different levels of cybersecurity and different technologies. A summary of the recommendations for key distributed wind stakeholders is below.

With the discussion and basic recommendations provided within this paper, the hope is that distributed wind stakeholders will have a better understanding of the importance of addressing cybersecurity at all stages of a system's lifecycle and the relationships (direct and indirect) between the various elements that make up the power grid.

## RECOMMENDATIONS FOR DISTRIBUTED WIND STAKEHOLDERS

### Manufacturers

Manufacturers should design distributed wind systems with cybersecurity factored in from the very beginning. This includes elements such as systems having their cyber components (microchips, communication modules, etc.) protected against changes that are "operationally" unreasonable, harmful, or unsafe. In addition, components should include "proof-of-identity" (such as TPM chips) to counter imitations and to provide accountability. All wind turbines should include role-based access capabilities, although smaller turbines might employ "standardized" roles with "standardized" capabilities.

### Integrators and Installers

Integrators and installers should document and test all applicable national, regional, and utility cybersecurity requirements relevant to distributed wind systems. They should verify that all appropriate cybersecurity measures are enabled when the distributed wind system is installed and that user passwords are changed before the wind turbine is first placed in service. Further, communication networks should be designed to isolate power system management from business networks.

### Wind Operators

This stakeholder group could be facility (owner) operators, utility operators, aggregator operators, or other third parties. For distributed wind operators, authentication and authorization for access to the systems are the most critical communications cybersecurity requirements. Confidentiality is important where privacy and/or market interactions are involved.

# APPENDIX A RELEVANT FUNCTIONAL AND COMMUNICATIONS STANDARDS ASSOCIATED WITH DISTRIBUTED WIND SYSTEMS

Several standards have been developed which define the basic functionality of DER as related to grid operations and data modeling. These standards help to ensure that the various stakeholders identified in the distributed wind reference architecture are aligned on expectations, definitions, and intended business practices

## A.1 IEEE 1547-2018 "GRID CODE" FUNCTIONS

Grid codes represent key mechanisms that utilities utilize to ensure safe and reliable interconnection processes when connecting new resources. IEEE 1547[28] defines several grid code functions that DER should (or shall, depending on the jurisdictional requirements) be capable of providing. IEEE 1547 is most applicable to grid connected distributed wind systems and those systems should be compliant with that standard. For other connection scenarios, such as behind the meter or off-grid, IEEE 1547 may still provide useful guidance for ensuring the stability and reliability of the local power system. Although the primary intention behind these DER capabilities was what photovoltaic systems should provide, it has become clear that these same requirements should apply to storage and to distributed wind turbines if they are considered as DER rather than part of a transmission-connected wind power plant.

Whether or not the IEEE 1547 grid code functions are mandatory, they should be managed securely in order to avoid power system disruptions. These key grid code functions include:

- **Disconnect / Connect –** Ability to be interconnect to local EPS.
- **Cease to Energize / Return to Service –** Cessation of active power delivery under steady-state and transient conditions and limitation of reactive power exchange / Enter service following recovery from a trip.
- **High/Low Voltage Ride-Through (Fault Ride-Through) –** Ability to withstand voltage disturbances inside defined limits and to continue operating as specified.
- **High/Low Frequency Ride-Through –** Ability to withstand frequency disturbances inside defined limits and to continue operating as specified.
- **Dynamic Reactive Current Support –** Ability to respond to sharp voltage spikes and dips through dynamic use of reactive power.
- **Frequency Watt (Frequency Droop or Frequency Sensitivity) –** Ability for the DER to actively limit the DER maximum active power as a function of the frequency following a frequency-active power piecewise linear characteristic.
- **Volt-Watt –** Ability for the DER to actively limit the DER maximum active power as a function of the voltage following a voltage-active power piecewise linear characteristic.
- **Fixed (Constant) Power Factor –** When in this mode, the DER shall operate at a constant power factor.
- **Fixed (Constant) Reactive Power –** When in this mode, the DER shall maintain a constant reactive power .
- **Volt-VAr –** When in this mode, the DER shall actively control its reactive power output as a function of voltage following a voltage-reactive power piecewise linear characteristic.
- **Watt-VAr –** When in this mode, the DER shall actively control the reactive power output as a function of the active power output following a target piecewise linear active power-reactive power characteristic, without intentional time delay. In no case, shall the response time be greater than 10 s.
- **Active Power Limiting –** Ability to limit active power as a percentage of the nameplate active power rating.
- **Active Power Setting** –– Ability to set active power at a specified percentage of the nameplate active power rating.
- **Low Frequency-Active Power Emergency for Demand Side Management (fast load shedding) –** Ability to support underfrequency load shedding programs and expected frequency restoration time.
- **Monitoring Key Status, Alarm, and Measurement Values –** This information is indicative of the present operating conditions of the DER
- **Scheduling of Power Settings –** Ability to receive power settings and functions and execute them at a later time.

[28] *IEEE 1547-2018 - IEEE Standard for Interconnection and Interoperability of Distributed Energy Resources with Associated Electric Power Systems Interfaces.* [Online]. https://standards.ieee.org/standard/1547-2018.html

## A.2 DER MARKET-BASED FUNCTIONS IN IEC 61850-7-420 FOR DISTRIBUTED WIND AS A DER

The primary purpose of distributed wind turbines is to provide renewable energy in the form of active power. However, active power is not the only service that distributed wind can provide.

Many additional functions that could be provided by DER, beyond those identified in IEEE 1547, are beneficial to grid operations and/or to customers. Since these functions would not be mandated, the incentive to provide them would most likely be financial or market-based.

Distributed wind could be used by owner/operators to benefit financially from some of these market-based functions. These "market-based" functions include some of the ISO/RTO ancillary services even if the wind turbines are connected at the distribution level, so long as the ancillary services do not exceed local constraints. Other market-based functions are focused on behind-the-meter service to reduce load costs or increase revenue from generation.

In situations where distributed wind turbines are part of a larger DER facility, such as a campus, shopping mall, or community microgrid, they could simply be seen as another DER, albeit with distinct characteristic and capabilities. Some of the market-based functions include:

- **Energy arbitrage by reducing/increasing the energy demand/generation based on price:** The DER optimizes financial results of operations by shifting the energy production from lower price to higher priced times, and the corresponding shifting of energy use from higher price to lower priced times.
- **Peak power limiting:** The DER limits the load at the Referenced ECP after it exceeds a threshold target power level.
- **Load following:** The DER counteracts the load by a percentage at the referenced ECP after it starts to exceed a threshold target power level.
- **Generation following:** The consumption and/or production of the DER counteracts generation power at the referenced ECP.
- **Dynamic active power smoothing:** The DER produces or absorbs active power in order to smooth the changes in the power level at the referenced ECP.
- **Rate of change of power – dW/dt:** The DER changes its real power output or input to provide frequency support to maintain frequency within normal limits.
- **Automatic generation control (AGC):** The DER responds to raise and lower power level requests to provide frequency regulation support.
- **Operating reserve (spinning reserve):** The DER provides operating reserve.
- **Synthetic or artificial inertia frequency-active power:** The DER responds to the rate of change of frequency (ROCOF) by changing its real power output or input to minimize spikes and sags.
- **Coordinated charge/discharge management:** The DER determines when and how fast to charge or discharge so long as it meets its target state of charge level obligation by the specified time.
- **Frequency-active power smoothing:** The DER responds to changes in frequency at the referenced ECP by changing its consumption or production rate based on frequency deviations from nominal, as a means for countering those frequency deviations.
- **Power factor limiting (correcting):** The DER supplies or absorbs reactive power to hold the power factor at the referenced ECP within the power factor limit.
- **Delta power control:** The DER decreases active power output to ensure there remains spinning reserve amount that was bid into the market.
- **Power ramp rate control:** The power increase and decrease is limited by specified maximum ramp rates.
- **Dynamic volt-watt:** The DER dynamically absorbs or injects additional reactive power in proportion to the instantaneous difference from a moving average of the measured voltage.
- **Microgrid separation control (intentional islanding):** The DER facilitates the islanding of microgrids by adjusting power output to improve transient stability posture.
- **Provide black start capability:** The DER facilitates the start-up of the system from an de-energized state.
- **Provide backup power:** The DER provides reserve power of the system in case of the failure of other generation units.

## A.3 IEC 61850-7-420 DER SEMANTIC DATA MODEL

Communication standards, including semantic models and protocols, are critical to interoperability. Semantic models provide accurate understanding and structures of the data to be exchanged, and the protocols provide the means to transport this data between (authorized) entities. Although generally looked on as good engineering practices, the use of semantic models also improves security by allowing the data being exchanged to be vetted for reasonability and validity, while the formal structures of the data objects help prevent malware from sneaking into data packages.

One of the most important semantic models for the energy industry is IEC 61850. Although best known for its substation automation semantic models, it has also been extended to DER. The IEC 61850-7-420 DER data model covers all the information data objects needed for some specific types of DER (PV systems, battery storage systems, fuel cells, combined heat and power, and diesel generators), but it also includes semantic models for DER functions. In particular, it meets the IEEE 1547 interoperability requirements as well as most of the market-based functions, as illustrated in Figure 15.

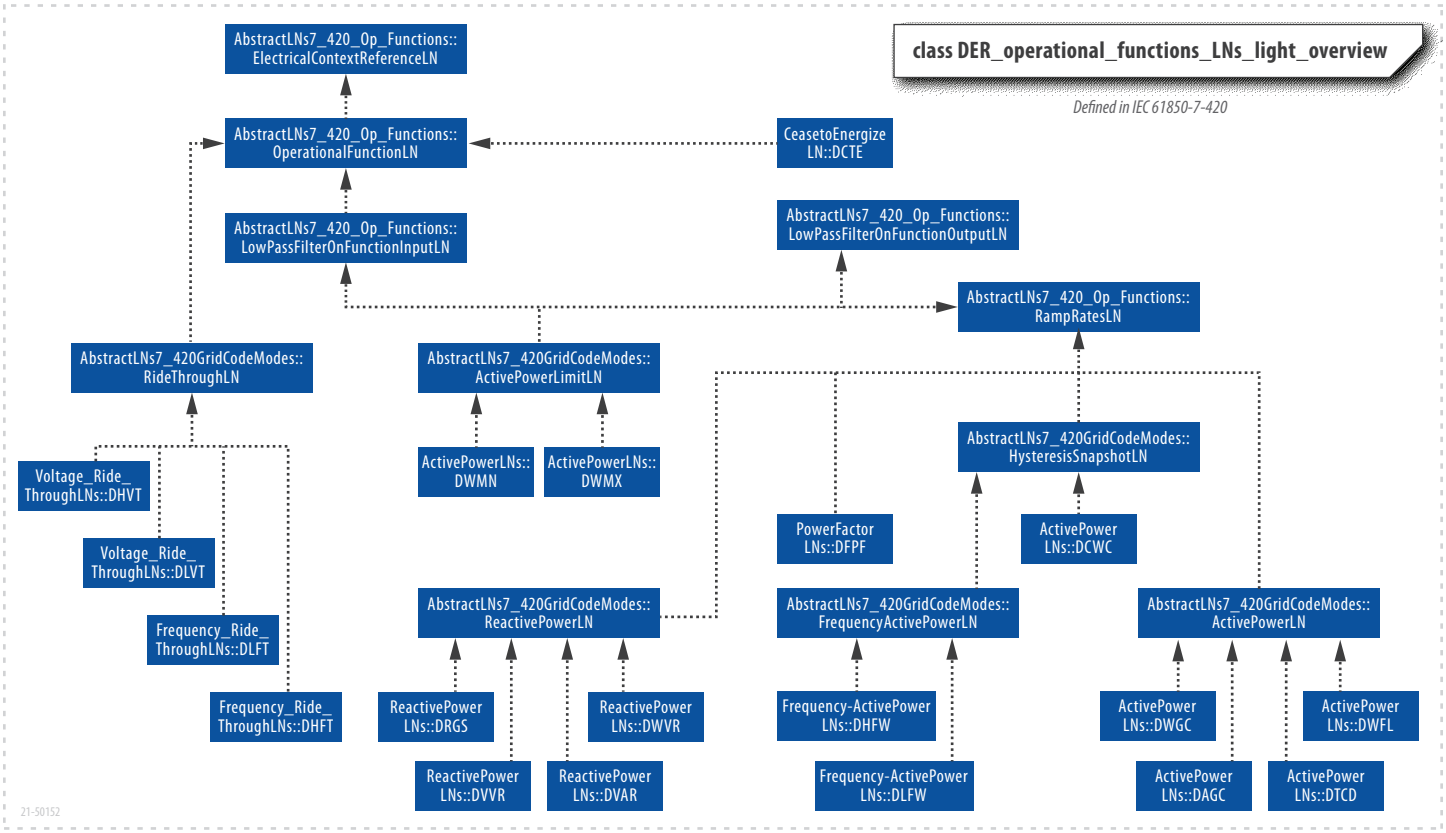



*Figure 15: IEC 61850-7-420 DER data model*

## A.4 IEC 61400-25-2 DATA MODEL FOR WIND POWER PLANTS

The IEC 61400-25-2 standard provides a semantic data model for wind power plants as well as the individual wind turbines, as shown in Figure 16. A semantic model is the equivalent to a language: in an international meeting, a decision is made on what language to use for conversations between people from different countries, such as French, Chinese, or (often) English. The wind power language is defined in IEC 61400-25-2. The purpose of this semantic model is to promote interoperability by having well-defined names for each type of data (e.g. wind turbine connection status, turbine rotation speed, wind gust alarm), thus permitting the many different external systems (e.g. utility SCADA system, aggregator system, local energy management system) to accurately understand the meaning of the data they receive from a wind power plant.

The focus of the IEC 61400-25 series is on the communications between wind power plant components such as wind turbines and external systems such as utility SCADA systems. Internal communication within wind power plant components is outside the scope of the IEC 61400-25 series..

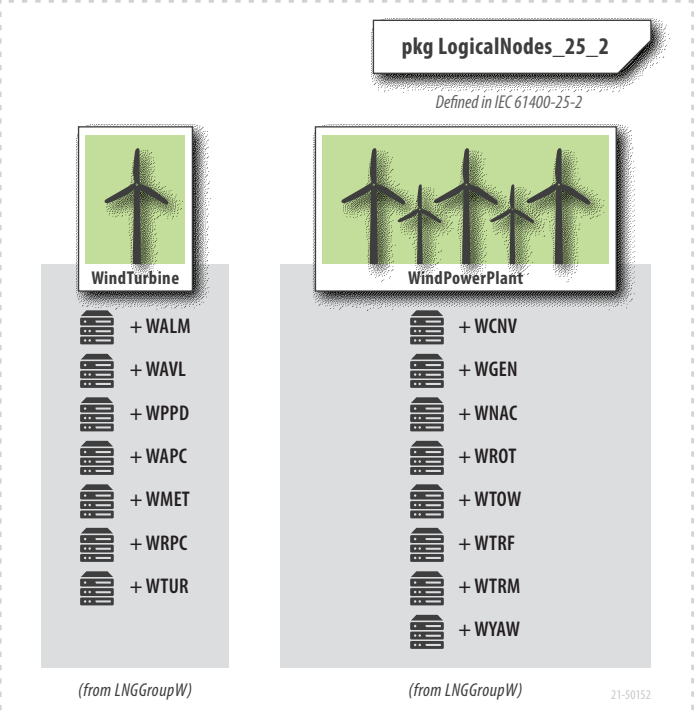



*Figure 16: IEC 61400-25-2 Data model for wind power plants and wind turbines*

This wind data model covers information on the components of wind turbines but does not include any control commands since those are internal to the wind plant. The key wind turbine "logical nodes" (an IEC 61850 term used to define a group of data objects associated with a particular purpose) are:

- WGEN: Wind turbine generator information
- WROT: Wind turbine rotor information
- WYAW: Wind turbine yaw information
- WNAC: Wind turbine nacelle information
- WCNV: Wind turbine converter information
- WTRF: Wind turbine transformer information

The data from individual wind turbines is aggregated at the wind power plant level to be available to external SCADA systems. There are also some basic control commands that the external SCADA system could request of the wind power plant related to active and reactive power (e.g. requested active power output or reactive power output from the wind power plant). The key wind plant "logical nodes" are:

- WALM: wind plant alarms
- WAVL: wind plant availability
- WAPC: wind plant active power monitoring and control
- WRPC: wind plant reactive power monitoring and control
- WMET: wind plant meteorological information

Since it is concerned primarily with the wind power plant, the IEC 61400-25-4 data model is only partially applicable to distributed wind turbines. The gaps and issues include the following:

- The data model does not include any control commands to the individual wind turbines since it assumes that the wind power plant controller will manage those commands. But if a distributed wind turbine is isolated or is part of a facility, like a campus, with other types of distributed energy resources, this wind data model does not permit active management of the wind turbine.

- The data model only includes basic active power and reactive power control commands (to the wind power plant level), and does not include any advanced grid code functions, such as those defined in IEEE 1547. Therefore, this data model assumes that any more complex functions are handled at a higher level than the distributed wind turbine itself. This assumption may be valid for some grid codes and market-based functions, but others, such as frequency and voltage ride-through, frequency-watt, and volt-var functions, cannot rely on typical communications since response times must be within milliseconds and availability must be very high.
- Currently IEC 61850-7-420 does not include models of wind turbines (to avoid conflicts with IEC 61400-25-2), but if distributed wind is to be treated as DER, then a data "profile" needs to be developed that includes the relevant portions of IEC 61400-25-2 and IEC 61850-7-420. This wind model is compliant with the IEC 61850 data modeling rules and can therefore be easily integrated with the IEC 61850-7-420 data model for cases where distributed wind turbines are providing DER-type grid services (see section Appendix A and section A.2).

## A.5 MAPPING OF IEC 61400-25-2 AND IEC 61850-7-420 DATA MODELS TO DNP3

Most utility SCADA systems in the U.S. use DNP3 (IEEE Std. 1815) as their protocol for interacting with field devices such as remote terminal units (RTUs). However, DNP3 does not have a semantic model associated with it, so that each utility decides how to map their data points. This approach was fine for utilities interacting only with their own equipment, but if they now need to interact with DER units and plants owned and operated by different companies, then a single semantic model is critical for interoperability.

For the wind domain, the IEC 61400-25-2 has been mapped to 5 different protocols (IEC 61400-25-4) including DNP3. IEC 61850 in general has also mapping of its Common Data Classes (CDC) to DNP3 in the IEEE Std. 1815.1, while the IEC 61850-7-420 data model has been mapped to DNP3 in the MESA-DER specification (see the third item in Figure 17). This provides a complete semantic and protocol combination for DER for those entities that want to use the DNP3 protocol.

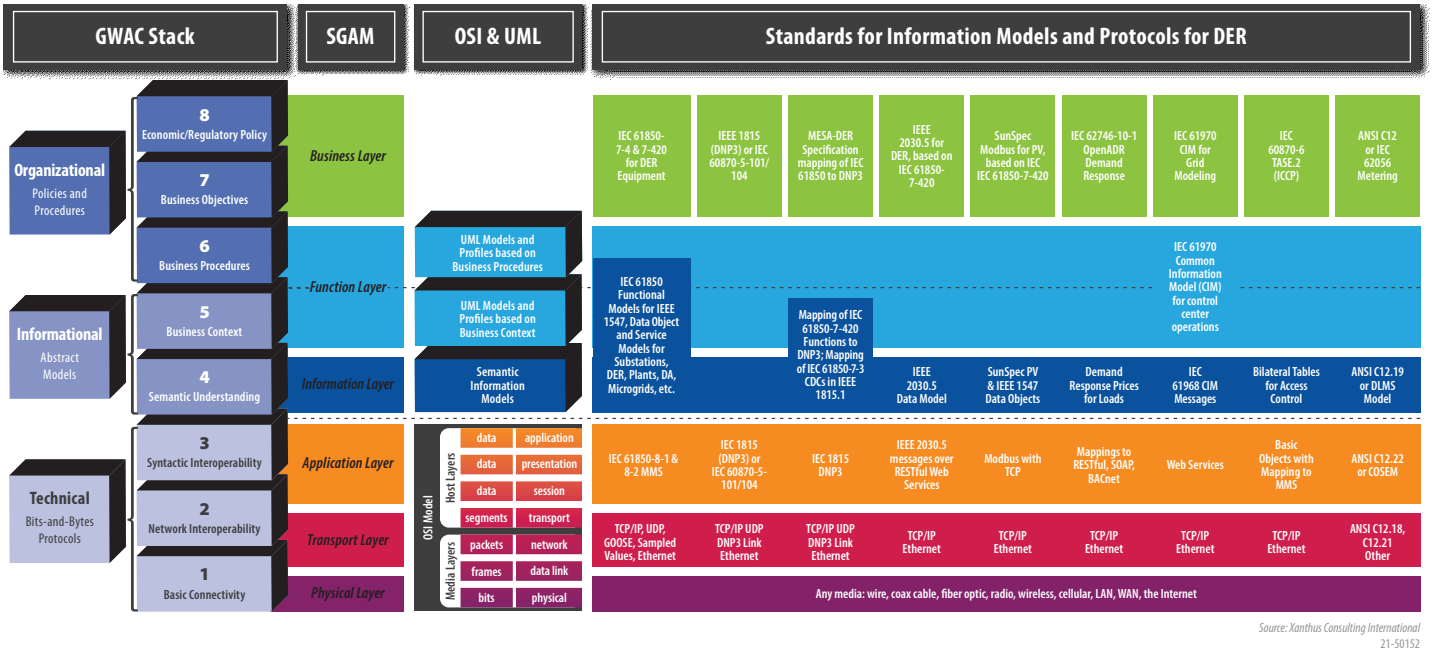



*Figure 17: Semantic and protocol standards for DER*

# APPENDIX B KEY DER COMMUNICATION PROTOCOLS

While there is a wide range of communication protocols for power systems equipment and many proprietary solutions developed by individual vendors, only a few standardized protocols exist for DER equipment. At this time, IEEE Std 1815 (DNP3), SunSpec Modbus, and IEEE 2030.5 are included in IEEE 1547-2018, while IEC 61850 is noted as being acceptable and is being implemented world-wide for DER. IEC 61400-25-2 could use the same security as IEC 61850 if mapped to the MMS protocol, while the other protocols identified in IEC 61400-25-4 would require different security.

Although the DER industry is primarily focused on IEC 61850, IEEE 2030.5, IEEE Std 1815, and Modbus, other information exchange techniques have been suggested by different organizations. These information exchange techniques are incorporated using different models, such as messaging using the IEC Common Information Model (CIM) for power system configurations, OpenADR for demand response market information, or a field message bus approach (e.g., OpenFMB). Industrial automation protocols, such as OPC/UA, have also been suggested for some types of interactions such as the interactions between utilities and large wind power plants using IEC 61400-25-2.

It is understood that many proprietary protocols have already been implemented; however, it is not possible to determine what cybersecurity capabilities these proprietary protocols may or may not have, so these are not included in this assessment. The most practical method of handling these proprietary protocols is to implement gateways which can separate inbound and outbound data flows, and/or Virtual Private Networks (VPNs) to wrap the proprietary protocols.

Since most DER vendors, including distributed wind turbines, will be planning to implement one or more of the IEEE Std 1547-2018 protocols as the interconnection requirements become either mandatory or recommended, determining the security capabilities of the different protocols will become key for securing DER communications. The selection of which protocol to use would typically stem from a utility requirement. The functionality of the four protocols is discussed briefly in the following sections.

## B.1 DISTRIBUTED NETWORK PROTOCOL (DNP3)

DNP3, defined in IEEE Std 1815, is the protocol most commonly used in utility SCADA systems for communications with their RTUs in substations and on feeders. DNP3 is based on the IEC 60870-5-101/104 standards, which were originally released in 1993. In addition to similar message structures, they also share common cybersecurity requirements. The DNP3 protocol defines different structures for binary, analog, and control objects, but does not have a specific information model. Each utility and each vendor define what each DNP3 data point means; thus DNP3 is not interoperable from a semantic perspective. For that reason, the MESA-DER specification was developed to provide an interoperable communications specification of data exchanges for DER with a special focus on utility-scale energy storage system (ESS). It combines two international standards, IEC 61850-7-420 (DER semantic data model) and IEEE Std 1815 (DNP3) into a single interoperable DER communications standard. Specifically, it maps the utility SCADA protocol, IEEE Std 1815 (DNP3) standard, to the IEC 61850-7-420 DER information model standard, thus creating an interoperable profile of DER functions, monitored information, and control commands.

## B.2 IEC 61850-7-420

IEC 61850-7-420 is the information model for communication and control of DER devices that defines the types of data that can (or must) be exchanged for different functions and for different types of DER. The functions include all of those currently defined in different contexts, but also many additional functions that are added as new requirements are defined, such as for electric vehicles, thermal storage, gas generation, and more. The IEC 61850-7-420 information model includes not only the DER functions but also defines the models for interactions between the functions, the resources (generators, storage, and controllable load), the electrical connection points (point of common coupling, point of connection), and power management which iteratively collects the data from all inputs and orchestrates the actual output of each DER unit. IEC 61400-25-2 is the IEC 61850 standard for wind power plants.

## B.3 IEEE 2030.5

IEEE 2030.5 was originally called the Smart Energy Profile (SEP) 1.x and was based on Zigbee Smart Energy 1.X wireless transport layers. It was focused on communications for integrating consumer devices and Home Area Networks (HANs) into the smart grid. HANs were designed to provide customers with performance and management functions such as energy usage information, pricing and billing, demand response and load control, device discovery, and service provider alerts. Eventually it was decided to standardized SEP as the IEEE 2030.5 standard with a more developed information model of the different HAN domains, including a basic information model of DER, based on IEC 61850-90-7, a precursor to IEC 61850-7-420. IEEE 2030.5 application layer now used the Restful XML technology.

## B.4 SUNSPEC MODBUS

The SunSpec Alliance has developed specifications that describe DER-specific information models mapped to Modbus data exchange formats that can be used by DER systems. Modbus is a control protocol that was originally developed by Modicon (now Schneider Electric) in 1979. Due to being one of the first communication protocols developed and also because of its simple construction, it has been very widely deployed across a broad range of devices, including controllers for DER. Measurement and control are performed through what are called Modbus registers, which are just functional addresses on a device that are tied to a certain input or output. There are no standardized semantic formatting or meanings for any of these registers, so that each implementation for a device type and vendor is unique. While it was originally a serial protocol, Modbus has been extended in recent years to work over TCP/IP. The SunSpec information models are based on the IEC 61850-7-420 information models and include nameplate information, monitoring data, and many of the grid support functions, including those defined in IEEE 1547-2018.



# APPENDIX C RELEVANT CYBERSECURITY STANDARDS ASSOCIATED WITH DISTRIBUTED WIND SYSTEMS

## C.1 OVERVIEW OF CYBERSECURITY STANDARDS

Cybersecurity standards and best practice guidelines should be used to support the risk management process and establish security programs and policies for OT environments. Specifically, cybersecurity technologies, if they already exist as standards for communication networks and protocols, should not be re-invented by vendors without significant support from the cybersecurity standards community and with a detailed assessment of the OT environment where they are planned to be used.

Key cybersecurity standards and best practice guidelines have already been developed for different areas and purposes of security. Cybersecurity planning should use these cybersecurity standards and guidelines to improve resilience, security, and interoperability throughout the energy OT environment, using the right standards, guidelines, and procedures for the right purposes at the right time.

Given the complexity of business processes and the wide variety of cyber assets used in the power operations environment, no single cybersecurity standard can address all security requirements, security controls, resilience strategies, and technologies particularly for such a complex domain as DER. For that reason, it is useful to categorize the key cybersecurity standards and guidelines. For instance, some standards and guidelines are focused on the high-level organizational security requirements and more detailed recommended controls (What), while other standards focus on the technologies that can be used to supply these cybersecurity controls (How). A third category provides guidance on how to comply with the standards (Process toward Compliance). These categories are illustrated in Figure 18:

- The "What" cybersecurity standards provide requirements or "controls" that should be applied, but do not address how to provide or implement these controls. For instance, a control could be that two-factor authentication should be used, but it does not identify what technologies or methodologies could be used for that purpose. Another control could state that communication protocols should authenticate both the sender and the receiver each time they establish a connection but does not define how that authentication would be done.

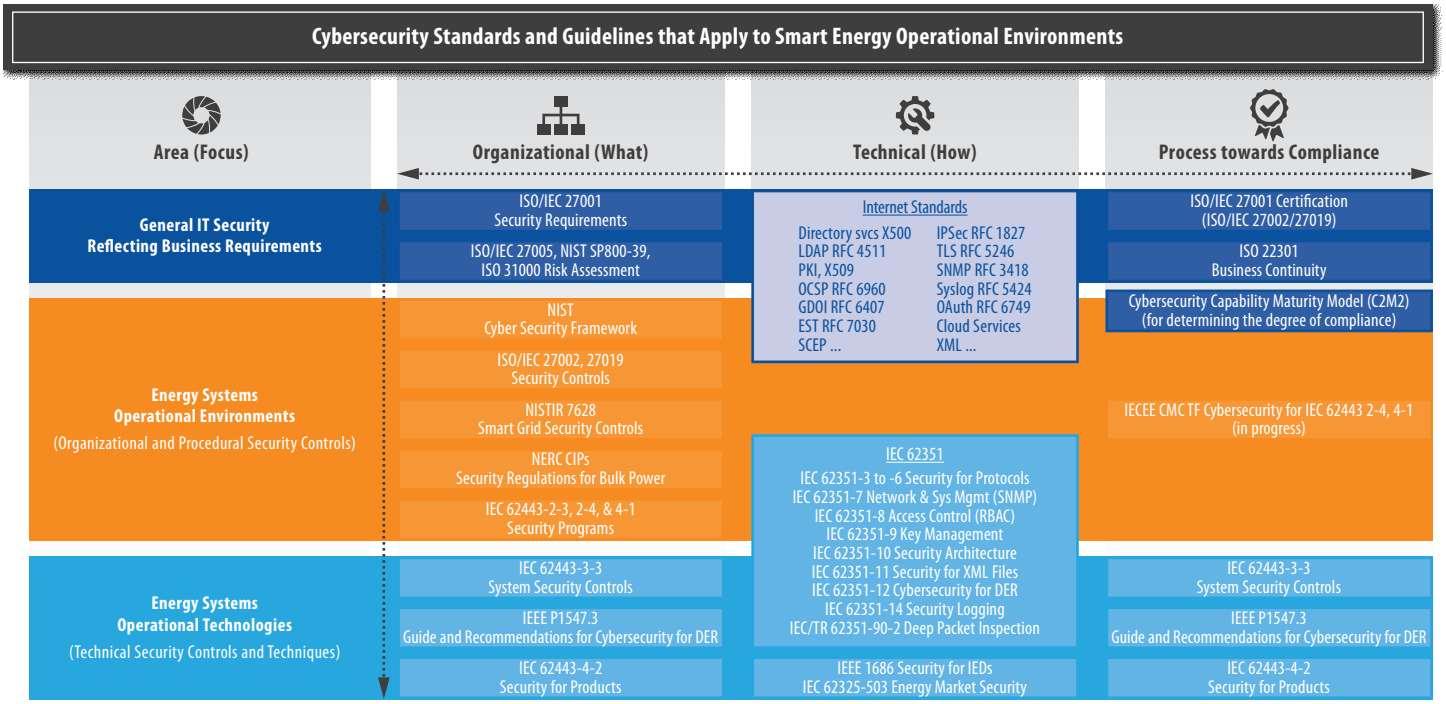



*Figure 18: Cybersecurity Standards and Guidelines that Apply to Smart Energy Operational Environments*

Source: Xanthus Consulting International
21-50152

- The "How" cybersecurity standards specify the technologies that could be used for the "What" controls. For instance, the requirement for two-factor authentication could be met by using one-time passwords. Or authentication by a protocol could define the exact messages, the exact interactive steps, and the results if authentication has failed.
- The "Process toward Compliance" cybersecurity standards include the testing and auditing procedures that must be followed in order to be certified as compliant. Some standards do exist for such compliance, but in other cases, that work is still in progress.

In addition to categorizing cybersecurity standards by their type (What, How, Compliance), they can also be characterized by their focus: High General level, High Energy-specific level, and Detailed Technical level.

- High General cybersecurity standards cover the very basic cybersecurity requirements that could be applicable to any scenarios, but do not give much specific advice for any specific business sector. These standards are usually more applicable to information technology (IT) environments.
- High Energy-specific cybersecurity standards apply the general requirements to (in this case) the energy business sector. In particular, these energy sector standards adapt the general requirements so that they can better apply to operational technology (OT) environments.

There are many cybersecurity standards and guidelines relevant for DER. The following list identifies the key documents, and each is discussed in more depth in the subsequent sections.

- 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
- IEEE P1547.3 Guide for Cybersecurity of Distributed Energy Resources Interconnected with Electric Power Systems

## C.2 NIST CYBERSECURITY FRAMEWORK

The NIST Cybersecurity Framework (see Table 2) provides a policy framework of computer security guidance for how organizations can assess and improve their ability to identify their cyber assets, prevent security events where possible, detect security events as they inevitably occur, respond to and cope with security events even while they are impacting system functions, and ultimately recover from such security events.

*Table 2: NIST Cybersecurity Framework*

| Function Unique Identifier | Function | Category Unique Identifier | Category |
|---|---|---|---|
| ID | Identify | ID.AM | Asset Management |
| | | ID.BE | Business Environment |
| | | ID.GV | Governance |
| | | ID.RA | Risk Assessment |
| | | ID.RM | Risk Management Strategy |
| | | ID.SC | Supply Chain Risk Management |
| PR | Protect | PR.AC | Identity Management & Access Control |
| | | PR.AT | Awareness and Training |
| | | PR.DS | Data Security |
| | | PR.IP | Information Protection Processes & Procedures |
| | | PR.MA | Maintenance |
| | | PR.PT | Protective Technology |
| DE | Detect | DE.AE | Anomalies and Events |
| | | DE.CM | Security Continuous Monitoring |
| | | DE.DP | Detection Processes |
| RS | Respond | RS.RP | Response Planning |
| | | RS.CO | Communications |
| | | RS.AN | Analysis |
| | | RS.MI | Mitigation |
| | | RS.IM | Improvements |
| RC | Recover | RC.RP | Recovery Planning |
| | | RC.IM | Improvements |
| | | RC.CO | Communications |

The benefit of using the NIST Framework allows for an organization to have a common language and systematic methodology for managing cybersecurity risk. The NIST Framework core functions include activities to be incorporated in a cybersecurity program that can be tailored to meet any organization's

needs. The Framework is designed to complement, not replace, an organization's cybersecurity program and risk management processes. The Framework helps guide key decision points about risk management activities through the various levels of an organization, from senior executives to business and process level, and implementation and operations as well.

## C.3 ISO/IEC 27000 ISMS FAMILY

The ISO/IEC 27000 family of cybersecurity standards and best practices focuses on "Information Security Management System (ISMS)" and consists of a series of documents that cover a wide range of cybersecurity requirements and guidelines for all types of information-based systems. These standards are published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). As cybersecurity has become increasingly critical to all information-based systems, this family of cybersecurity standards has grown substantially over the last years.

ISO/IEC 27000 itself provides a standard vocabulary while ISO/IEC 27001 (in conjunction with other standards) provides the framework for audits and certification of an organisation's ISMS. The other ISMS standards consist of inter-related documents, already published or under development and/or update, and contains several organizational components.

## C.4 NISTIR 7628 GUIDELINES FOR SMART GRID CYBERSECURITY

The NISTIR 7628 consists of guidelines intended primarily for addressing cybersecurity of Smart Grid systems and the constituent subsystems of hardware and software components. The NISTIR 7628 guidelines are very similar in scope to the ISO/IEC 27019 standard, except these guidelines focus exclusively on the Smart Grid sector. It defines approximately 300 high-level security controls, based on similar security controls in other NIST documents, including the NIST Framework (see Table 3).

*Table 3: NIST Smart Grid Security Requirements Families*

| Ref. | NIST Smart Grid security requirements families |
|---|---|
| SG.AC | Access Control |
| SG.AT | Awareness and Training |
| SG.AU | Audit and Accountability |
| SG.CA | Security Assessment and Authorization |
| SG.CM | Configuration Management |
| SG.CP | Continuity of Operations |
| SG.IA | Identification and Authentication |
| SG.ID | Information and Document Management |
| SG.IR | Incident Response |
| SG.MA | Smart Grid Information System Development and Maintenance |
| SG.MP | Media Protection |
| SG.PE | Physical and Environmental Security |
| SG.PL | Planning |
| SG.PM | Security Program Management |
| SG.PS | Personnel Security |
| SG.RA | Risk Management and Assessment |
| SG.SA | Smart Grid Information System and Services Acquisition |
| SG.SC | Smart Grid Information System and Communication Protection |
| SG.SI | Smart Grid Information System and Information Integrity |

## C.5 IEC 62443 CYBERSECURITY STANDARDS FOR INDUSTRIAL AUTOMATION

The international series of standards IEC 62443 are being developed jointly by the IEC TC65 and the ISA99 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. It can be used in conjunction with the ISO/IEC 27000 series (in particular with ISO/IEC 27019 for the energy domain) and with IEC 62351 which provides security technology standards.

## C.6 IEC 62351 CYBERSECURITY STANDARDS FOR POWER SYSTEMS

The IEC 62351 series of standards include cybersecurity technologies for the communication protocols defined by the IEC TC 57, specifically the IEC 60870-5 series (including IEEE Std 1815 (DNP3) as a derivative standard), the IEC 60870-6 series, the IEC 61850 series, the IEC 61970 series, and the IEC 61968 series. As shown in Figure 20, there is not a one-to-one correlation between the IEC TC57 communication protocol standards and the IEC 62351 security standards. This is because many of the communication protocols rely on the same underlying standards at different layers.

The IEC 62351 series also defines the cybersecurity requirements for implementing security technologies in the operational environment, including objects for network and system management (e.g. with SNMP), RBAC, cryptographic key management, and security event logging.

Technical specifications for conformance testing, applicable for these standards, are also being developed as part of this series as IEC/TS 62351-100-xx.

IEC 62351 standards profile the use of existing internet standards whenever possible to meet domain-specific needs. Reusing the same security standards across different communication protocols supports the interoperability of these protocols.

## C.7 NERC CRITICAL INFRASTRUCTURE PROTECTION STANDARDS RELATED TO DISTRIBUTED WIND TURBINES

NERC developed the Critical Infrastructure Protection (CIP) standards to address cybersecurity of system that may affect the reliable operation of the bulk electric system (BES). As developed by the NERC, the BES definition includes all the larger elements and facilities that are necessary for the reliable operation and planning of the interconnected bulk power system (BPS). With the growing prevalence of DER, NERC has identified that under-

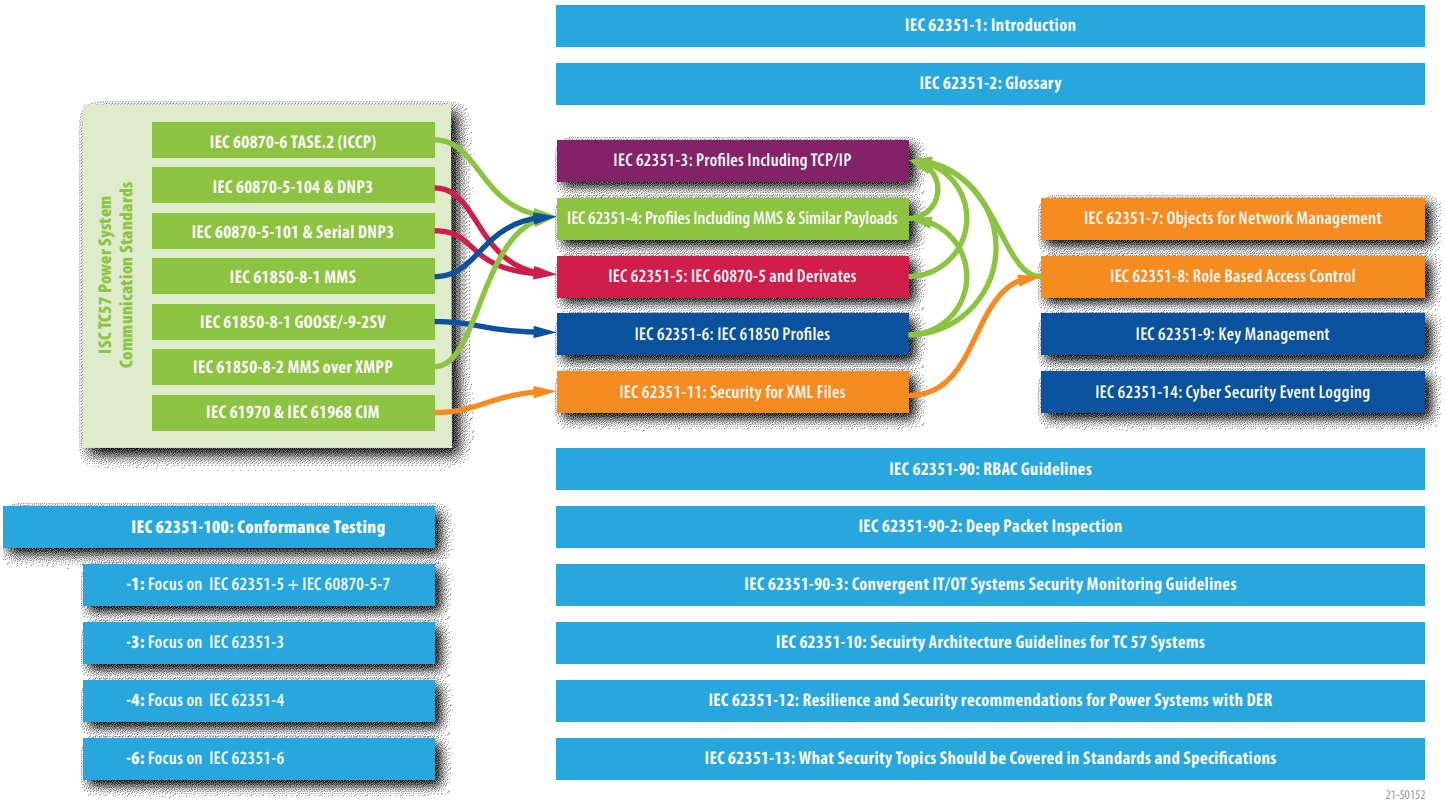



*Figure 20: IEC 62351 series of cybersecurity standards*

standing DER is becoming an important consideration for BPS reliability. For example, a cyberattack that affects large numbers or aggregations of DER could potentially impact to the Transmission Operator's ability to reliably operate the BES.

Currently, the NERC CIP standards would not be directly applicable to the distributed wind configuration presented in Section 1.2 because they do not meet the BES threshold. The NERC CIPs focus on the Cyber Assets of BES. In particular, BES Cyber Assets are those which are greater than 75 MVA aggregated or greater than 20 MVA as a single unit and connected on a 100 kV circuit or higher, that, *"if rendered unavailable, degraded, misused, or destroyed, would adversely impact the reliable operation of the BES within 15 minutes of the activation or exercise of the compromise".* This assessment cannot include the redundancy of these BES Cyber Assets, in which some other assets are used to replace the lost functionality.

Because of the increasing attention of DERs role in the reliable operation of the BES however, it is "useful" to review the NERC CIP definitions of impacts to see where they could potentially apply in the future to aggregated DER. Impact ratings are important in the context of the NERC CIP standards as they identify which requirements are applicable for specific assets. BES Cyber Assets are categorized as High, Medium, or Low impact:

- **High Impact Cyber Assets** are essentially bulk power system control centers. DER systems are not included in this category.
- **Medium Impact Cyber Assets** are the large BES generation systems: commissioned generation, by each group of generating units at a single plant location, with an aggregate highest rated net real power capability of the preceding 12 calendar months equal to or exceeding 1500 MW in a single Interconnection. For each group of generating units, the only BES cyber systems that meet this criterion are those shared BES cyber systems that could, within 15 minutes, adversely impact the reliable operation of any combination of units that in aggregate equal or exceed 1500 MW in a single Interconnection. There are other non-generation criteria, but for DER it is most likely that the generation criteria will be the applicable requirement.
- **Low Impact Cyber Assets** are all other BES-related cyber systems that are *associated* with BES assets and that meet other applicability qualifications, including having an aggregated capacity greater than 75 MVA, an individual capacity greater than 20 MVA, and interconnected on a circuit greater than 100 kV.

## C.8 IEEE P1547.3 GUIDE AND CYBERSECURITY RECOMMENDATIONS FOR DER

IEEE P1547.3 covers cybersecurity issues and recommendations for DER in general. In addition to introductory material, it contains the following sections:

- **Section 4**: Cybersecurity considerations for DER interconnections. This section is primarily informative for the general reader to ensure that the full context of cybersecurity for DER is understood. For instance, it discusses the various architectures and stakeholders involved in DER development, integration, and operations. It covers basic cybersecurity issues of cyber-physical systems, the differences, and similarities of IT security versus OT security, and the use of NIST Cybersecurity Framework as an organizational structure.
- **Section 5**: Technical cybersecurity recommendations. This section provides very precise recommendations for different aspects of DER architectures and operations, including:
  - Risk assessment and management (RA) recommendations
  - Communication network engineering (NE) recommendations
  - Access control (AC) recommendations
  - Data security (DS) recommendations
  - Security management (SM) recommendations
  - Coping with and recovering from (CM) security events recommendations
- **Section 6**: Recommendations for different DER stakeholders. This section focuses on the specific recommendations for some of the key stakeholders, including:
  - Manufacturers of DER systems
  - Integrators and installers of DER systems
  - Testing personnel
  - DER owner/grid operators/aggregators
  - DER facility ICT management
  - DER security managers
  - DER maintenance personnel
  - DER operator coping actions during a security event
  - DER recovery actions after a security event
- **Section 7**: Testing and commissioning of cybersecurity
- **Annexes A – H**: Relevant communication and cybersecurity standards and best practices

# APPENDIX D POTENTIAL CYBERATTACK IMPACTS

Based on the ICS Cyber Kill Chain concept, examples of potential impacts to key stakeholders of distributed wind installations related to these methods are provided in Table 2. Note that these are only a small sample of the potential impacts and not an exhaustive listing.

*Table 4: Potential Impacts by Stakeholder Group*

| POTENTIAL IMPACT BY STAKEHOLDER | | | |
|---|---|---|---|
| **Event** | **Utility (Non-Operator)** | **Operator (Facility/Aggregator/Utility)** | **Manufacturer, Integrator, or Installer** |
| **Loss of View** | | • Loss of revenue | • Reduce reputation<br>• Financial liability |
| **Loss of Control** | • Energy imbalance | • Propagated failures<br>• Injury<br>• Equipment damage | • Reduce reputation<br>• Financial liability |
| **Denial of View** | | • Improper operation | • Reduce reputation<br>• Financial liability |
| **Denial of Control** | | • Improper operation | • Reduce reputation<br>• Financial liability |
| **Denial of Safety** | • Injury | • Injury | • Reduce reputation<br>• Financial liability |
| **Manipulation of View** | • Improper control decision | • Improper control decision | • Reduce reputation<br>• Financial liability |
| **Manipulation of Control** | • Additional energy resources<br>• Injury | • Loss of reliable operation<br>• Activation of critical load algorithm<br>• Loss of required generation<br>• Failure to meet contractual obligations | • Reduce reputation<br>• Technical investigation<br>• Financial liability |
| **Manipulation of Sensors and Instruments** | • Energy imbalance<br>• Failure of regulatory compliance | • Improper operation<br>• Severe mechanical damages<br>• Loss of revenue resource<br>• Increased operation and maintenance costs | • Reduce reputation<br>• Increase after-sale expenses<br>• Potential product call-back<br>• Financial liability |
| **Manipulation of Safety** | • Extended restoration time<br>• Failure of regulatory compliance | • Injury or death<br>• Loss of intellectual property<br>• Technical investigation | • Devalue brand name<br>• Reduce market share<br>• Decommission the product from the market<br>• Financial liability |

# SELECT ACRONYMS

| | |
|---|---|
| ADMS | Aggregator DER and Load Management System |
| AGC | Automatic Generation Control |
| BES | Bulk Electric System |
| BPS | Bulk Power System |
| CDC | Common Data Classes |
| CIM | Common Information Model |
| CIP | Critical Infrastructure Protection |
| COTS | Commercial Off The Shelf |
| CRL | Certificate Revocation List |
| DER | Distributed Energy Resources |
| DERMS | Distributed Energy Resource Management System |
| DMS | Distribution Management System |
| DMZ | De-militarized Zone |
| DNP | Distributed Network Protocol |
| DOE | Department of Energy |
| DR | Demand Response |
| DSO | Distribution System Operator |
| ECP | Electrical Connection Point |
| EEDS | Electric Energy Delivery System |
| EMS | Energy Management System |
| EPS | Electric Power System |
| ESI | Energy Service Interface |
| ESS | Energy Storage System |
| FDERMS | Facility DER Energy Management System |
| GIS | Geographic Information System |
| GWAC | GridWise Architecture Council |
| HAN | Home Area Network |
| IACS | Industrial Automation and Control System |
| ICS | Industrial Control System |
| ICT | Information and Communications Technology |
| IEC | International Electrotechnical Commission |
| IEEE | Institute of Electrical and Electronics Engineers |
| IP | Internet Protocol |
| ISMS | Information Systems Management System |
| ISO | Independent System Operator |
| ISO | International Organization for Standardization |
| IT | Information Technology |
| LAN | Local Area Network |
| LMP | Locational Marginal Price |
| MMS | Manufacturing Message Specification |
| NERC | North American Electric Reliability Corporation |
| NIST | National Institute of Standards and Technology |
| NISTIR | National Institute for Standards and Technology Interagency or Internal Report |
| OCSP | Online Certificate Status Protocol |
| OMS | Outage Management System |
| OPC | Open Platform Communications (formerly OLE for Process Control) |
| OS | Operating System |
| OSI | Open Systems Interconnection |
| OT | Operational Technology |
| PCC | Point of Common Coupling |
| PV | Photovoltaic |
| RBAC | Role-Based Access Control |
| REP | Retail Electric Provider |
| ROCOF | Rate of Change of Frequency |
| RSO | Regional System Operator |
| RTO | Regional Transmission Operator |
| RTU | Remote Terminal Unit |
| SCADA | Supervisory Control and Data Acquisition |
| SEP | Smart Energy Profile |
| SGAM | Smart Grid Architecture Model |
| SNMP | Simple Network Management Protocol |
| TBLM | Transmission Bus Load Model |
| TCP | Transmission Control Protocol |
| TLS | Transport Layer Security |
| TPM | Trusted Platform Module |
| TSO | Transmission System Operator |
| UML | Unified Modeling Language |
| VPP | Virtual Power Plant |
| VSAT | Very Small Aperture Satellite |
| WAN | Wide Area Network |
| WETO | Wind Energy Technologies Office |
| XML | Extensible Markup Language |

## DISCLAIMER



Idaho National Laboratory
Critical Infrastructure Security and Resilience
Idaho Falls, Idaho 83415

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