INL/CON-21-63570-Revision-0

# A Cyber-Resilience Risk Management Architecture for Distributed Wind

October 2021

Changing the World's Energy Future

Megan Jordan Culler, Jake P Gentle, Sean Morash, Brian Smith, Frances Cleveland

Idaho National Laboratory

## DISCLAIMER

This information was prepared as an account of work sponsored by an agency of the U.S. Government. Neither the U.S. Government nor any agency thereof, nor any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness, of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the U.S. Government or any agency thereof.

INL/CON-21-63570-Revision-0

# A Cyber-Resilience Risk Management Architecture for Distributed Wind

Megan Jordan Culler, Jake P Gentle, Sean Morash, Brian Smith, Frances Cleveland

October 2021

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

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

# A Cyber-Resilience Risk Management Architecture for Distributed Wind

Megan J. Culler
*Idaho National Laboratory*
Idaho Falls, ID, USA
megan.culler@inl.gov

Sean Morash
*EnerNex*
Knoxville, TN, USA
smorash@enernex.com

Brian Smith
*EnerNex*
Knoxville, TN, USA
bsmith@enernex.com

Frances Cleveland
*Xanthus Consulting International*
Boulder Creek, CA, USA
fcleve@xanthus-consulting.com

Jake Gentle
*Idaho National Laboratory*
Idaho Falls, ID, USA
jake.gentle@inl.gov

***Abstract*—Distributed wind is an electric energy resource segment with strong potential to be deployed in many applications, but special consideration of resilience and cybersecurity is needed to address the unique conditions associated with distributed wind. Distributed wind is a strong candidate to help meet renewable energy and carbon-free energy goals. However, care must be taken as more systems are installed to ensure that the systems are reliable, resilient, and secure. The physical and communications requirements for distributed wind mean that there are unique cybersecurity considerations, but there is little to no existing guidance on best practices for cybersecurity risk management for distributed wind systems specifically. This research develops an architecture for the consideration of cyber risks associated with distributed wind systems. The architecture takes into account the configurations, challenges, and standards for distributed wind to create a risk-focused perspective that considers of threats, vulnerabilities, and consequences, with special emphasis on what sets distributed wind systems apart from other distributed energy resources (DER). We discuss common distributed wind architectures and how they are interconnected to larger power systems. Because cybersecurity cannot exist independently, the cyber-resilience architecture must consider the system holistically. Finally, we discuss the implementation of a risk assessment process that uses the cyber-resilience framework to address challenges specific to distributed wind.**

***Index Terms*—cybersecurity, resilience, distributed wind, distributed energy resource**

## I. Introduction

Wind energy installations are growing, and distributed wind plays an important role in that growth. The United States wind capacity was estimated as 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 100 times that amount could be feasibly installed, 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 will play a major role in meeting this goal, distributed wind is also critical. Distributed wind can be used to offset local load, ease burdens on transmission systems, and support microgrid and islanding functions, setting it apart from bulk wind.

The growing market opportunities and installation trends motivate the need for a comprehensive risk analysis of distributed wind. While traditional reliability planning accounts for higher frequency events, those methods often fail to account for high-impact low-frequency (HILF) events, such as cyberattacks, that are traditionally considered in the resilience domain. Despite their lower probability of occurrence, these resilience events must be accounted for in risk management.

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, prepare for, and adapt to disruptive events and recover rapidly from any disturbance to an acceptable state of operation" [5]. Resilience covers both cyber and physical disruptions, a concept reinforced by the White House, who stated, "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" [6].

As stated in the definition above, resilience refers to the identification and preparation for hazards, not just the response and recovery for events that do occur. This means that threat identification and risk classification is just as important as response plans. In this work, we highlight these initial stages of resilience. Successful identification and preparation for cyber risks is the best way to ensure that response and recovery is most effective. Resilience against cyber events is a necessary consideration for distributed wind systems, no matter their size or deployment configuration. In this research, we present the

This research was sponsored by the Department of Energy (DOE) Wind Energy Technologies Office (WETO) under DOE Idaho Operations Office Contract DE-AC07-05ID14517. The views and opinions of the authors expressed herein do not necessarily state or reflect those of the U.S. Government of any agency thereof.

cyber-resilience risk architecture for distributed wind, which takes traditional risk assessment and resilience concepts and applies them to the specific challenges for distributed wind.

### A. Related Works

Cybersecurity for DER is an active area of research, but the holistic consideration of cybersecurity risks to distributed wind systems has not been well studied. This research fills gaps by considering the unique needs of cybersecurity for distributed wind and evaluation of cybersecurity risks.

Multiple works have proposed cybersecurity frameworks for DER. Powell et. al. propose a framework centered on cyber governance and management of DER devices [7]. Other work provides specific recommendations for DER based on common attack types [8]. Simulations can be used to create more specific mitigation strategies [9]. Trusted execution environments and secure communications are also suggested security methods for DER [10], [11] These works do not consider a holistic risk perspective, and they provide recommendations for generic DER, while our work focuses on unique considerations for distributed wind.

Li et. al. discuss cybersecurity risks to microgrids from a similar perspective to our approach [12]. Similarly, the NIST cybersecurity framework has been adapted to DER and smart grids [13], [14]. As with other works, they do not consider distributed wind specifically. Additionally, while their approach considers vulnerabilities, vectors, and consequences, they do not consider adversarial intent and capabilities explicitly as part of the likelihood analysis.

There are some analyses that do consider cybersecurity to distributed wind specifically, but they tend to focus on specific vulnerabilities rather than the broader risk perspective [15], [16]. Analysis of cyber-physical failures reveals the power system reliability consequences [17]. Our research builds on this work by considering the many components of cybersecurity risks to distributed wind systems.

## II. Background

### A. Defining Distributed Wind

The DOE 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 [18]. Wind turbines that are installed at or near the point of end use, used to help meet onsite energy demand, or support the distribution grid are said to be in close proximity to end-use, and thus classified as distributed wind. Wind turbines that are connected behind-the-meter, directly to the distribution grid, or off-grid are also classified as distributed wind installations. Distributed wind energy systems can be used in residential, agricultural, commercial, industrial, and community applications, and can range in size from 5 kilowatts to multi-megawatt turbines.

### B. Distributed Wind Interconnections

Distributed wind turbines can be treated similarly to any other DER when they are connected to the distribution grid. They must meet all grid interconnection requirements, such as those defined in IEEE Std 1547:2018 and any utility-specified requirements, as well as cybersecurity requirements, such as those defined in IEEE 1547.3 [19].

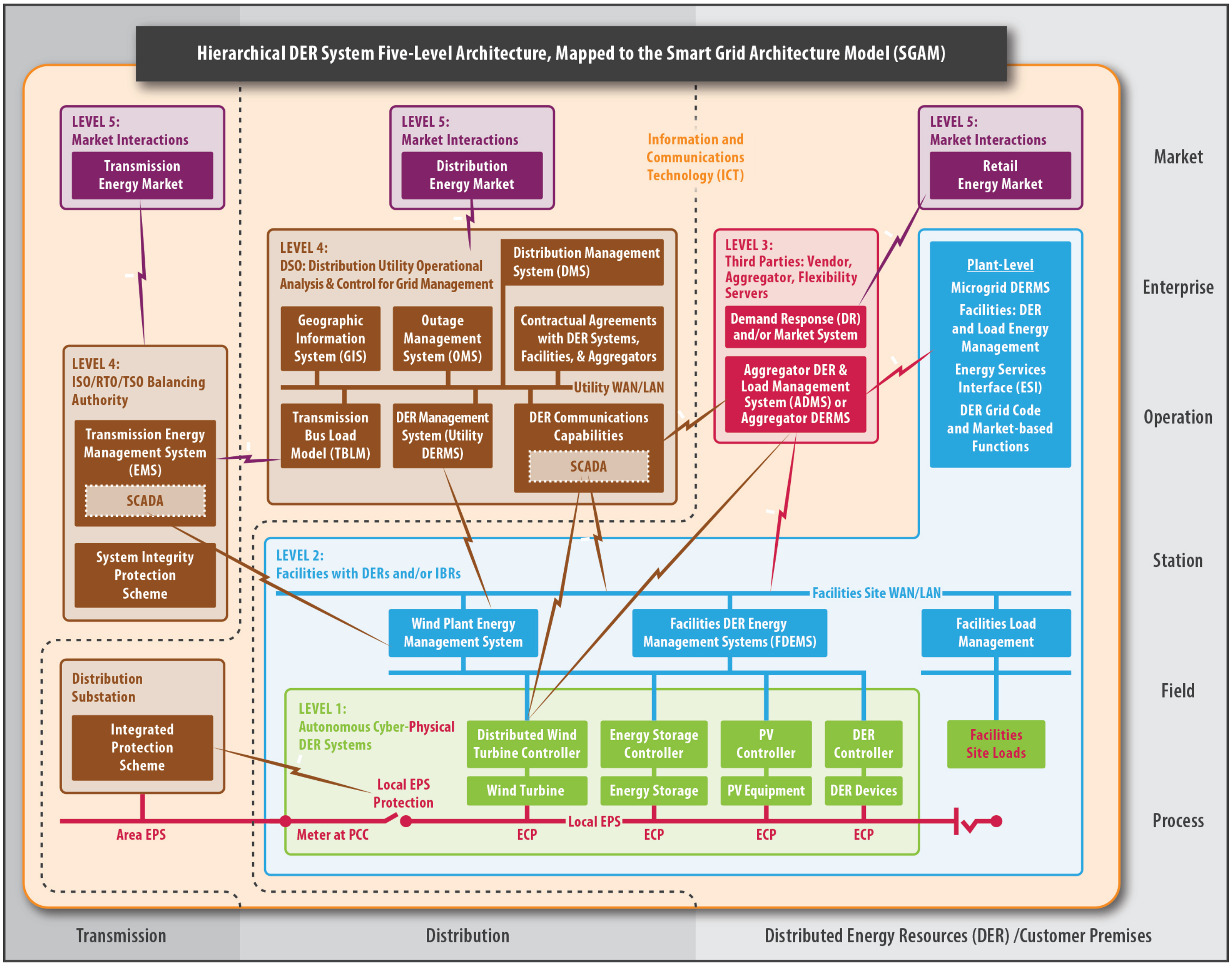
There are many stakeholders and systems that are involved with distributed wind assets and operators. Understanding these relationships, shown in Figure 1, as they relate to the operation of DER provides a foundation on which to begin to address cybersecurity needs. The different levels of electric system operation each may impact distributed wind and are defined for the puproses of this work as:

1) Level 1 (DER) includes the actual DERs interconnected to local grids at Electrical Connection Points (ECPs) and to the utility grid at the Point of Common Coupling (PCC). These DERs are usually operated autonomously. Logical communication interactions with other systems support the necessary information exchanges.
2) Level 2 (Facility DER Management) is where a facility DER management system (facility DERMS) manages the operation of the Level 1 DERs. The logical communication interactions are shown between the facility DERMS and other energy related stakeholders.
3) Level 3 (Third Parties: Aggregators) shows market-based aggregators and retail energy providers (REP) who request or command DERs to take specific actions, such as turning on or off, setting output, or providing ancillary services.
4) Level 4 (Utility Operational Grid Management) determines what requests or commands should be issued to which DERs. Distribution system operators must assess if efficiency or reliability of the power system can be improved by having DERs. Transmission system operators (TSOs), regional transmission operators (RTOs), or independent system operators (ISOs) may interact directly with larger DERs or aggregated DERs.
5) Level 5 (Market Operations) involves the larger energy environment where markets influence DER to provide market-based services.

The first stage of resilience is identification, which includes both identification of the system of interest and the likely hazards. Understanding the distributed wind interconnections is critical to inform the threats and potential impacts of cyber hazards. All of these interdependencies can have an impact on the overall risk profile of a distributed wind system. Each connection is an opportunity for a threat actor to take advantage of vulnerabilities and additional access points. It exposes all of the connected systems to potential consequences of an attack on the distributed wind system, and vice versa. These interdependencies are critical to identify cybersecurity risk in preparation for cyber resilience.

### C. Cybersecurity Standards and Guidelines

There are many cybersecurity standards and guidelines relevant for DER in general which therefore may apply to distributed wind. Given the complexity of business processes and the wide variety of cyber assets used in power system


Hierarchical DER System Five-Level Architecture, Mapped to the Smart Grid Architecture Model (SGAM)
LEVEL 5:
Market Interactions
Transmission Energy Market
LEVEL 5:
Market Interactions
Distribution Energy Market
Information and Communications Technology (ICT)
LEVEL 5:
Market Interactions
Retail Energy Market
Market
LEVEL 4:
DSO: Distribution Utility Operational Analysis & Control for Grid Management
Distribution Management System (DMS)
Geographic Information System (GIS)
Outage Management System (OMS)
Contractual Agreements with DER Systems, Facilities, & Aggregators
Utility WAN/LAN
Transmission Bus Load Model (TBLM)
DER Management System (Utility DERMS)
DER Communications Capabilities
SCADA
LEVEL 3:
Third Parties: Vendor, Aggregator, Flexibility Servers
Demand Response (DR) and/or Market System
Aggregator DER & Load Management System (ADMS) or Aggregator DERMS
Plant-Level
Microgrid DERMS
Facilities: DER and Load Energy Management
Energy Services Interface (ESI)
DER Grid Code and Market-based Functions
Enterprise
Operation
LEVEL 4:
ISO/RTO/TSO Balancing Authority
Transmission Energy Management System (EMS)
SCADA
System Integrity Protection Scheme
LEVEL 2:
Facilities with DERs and/or IBRs
Facilities Site WAN/LAN
Wind Plant Energy Management System
Facilities DER Energy Management Systems (FDEMS)
Facilities Load Management
Station
Field
Distribution Substation
Integrated Protection Scheme
LEVEL 1:
Autonomous Cyber-Physical DER Systems
Distributed Wind Turbine Controller
Energy Storage Controller
PV Controller
DER Controller
Facilities Site Loads
Local EPS Protection
Wind Turbine
Energy Storage
PV Equipment
DER Devices
Process
Area EPS
Meter at PCC
Local EPS
ECP
ECP
ECP
ECP
Transmission
Distribution
Distributed Energy Resources (DER) /Customer Premises

Source: Xanthus Consulting International
21-50152

Fig. 1. Architecture of distributed wind integration into larger systems.

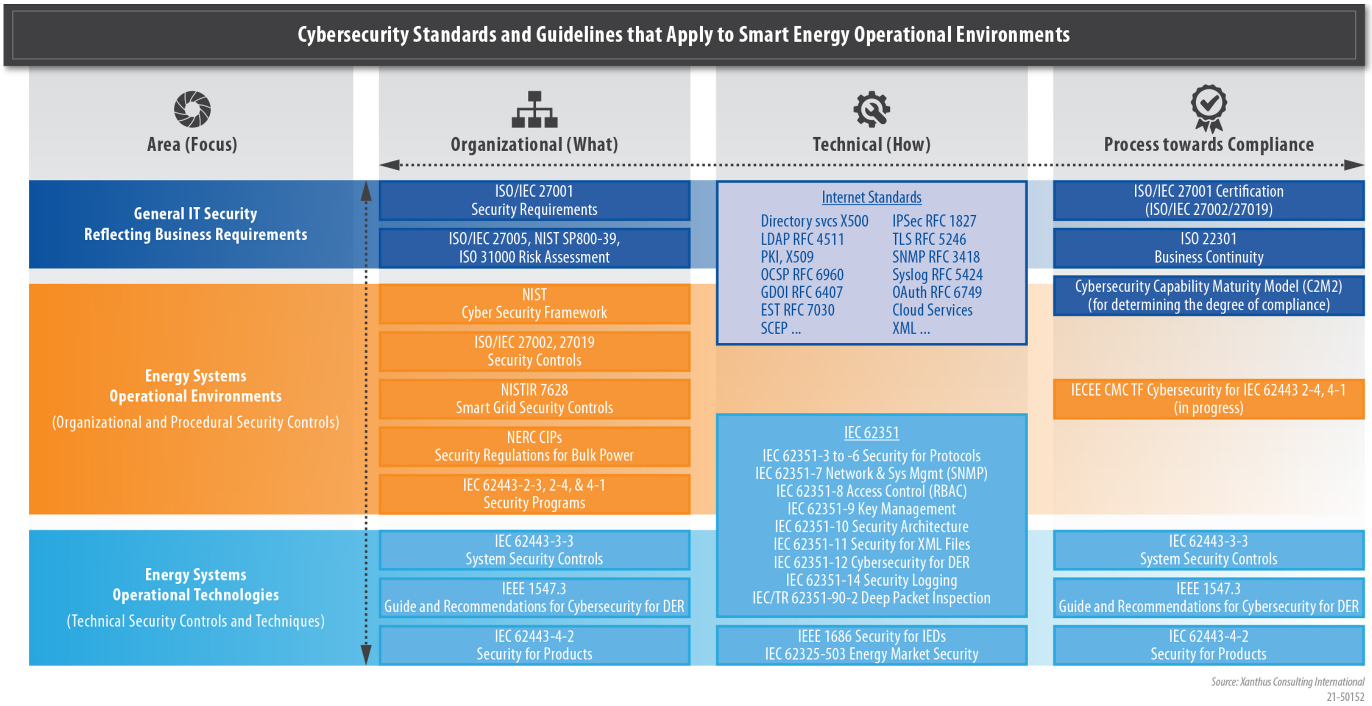
operations, no single cybersecurity standard can address all requirements, controls, resilience strategies, and technologies.

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). A breakdown of relevant standards is provided in Figure 2. These standards and their appropriate usage for distributed wind environments is described more fully in [20]. Cybersecurity standards and best practice guidelines should be used to support the risk management process but cannot on their own guarantee resilience.

## III. Need for Distributed Wind Cyber-Resilience

Distributed wind can be configured in a variety of architectures, and it is affected by, and has an impact on, all connected systems. Because of both the power and communication interconnections, cyberattacks impact distributed wind systems in a variety of ways. The remote access requirements associated with distributed wind can provide points of access for a cyber adversary. A cyberattack on a third party can impact distributed wind controls, or even infect the turbine controls if malware propagates through the communications system. Finally, if a cyberattack does affect the power output of a distributed wind system, it can negatively impact the stability of the connected power systems.

The bidirectional communication required for smart-grid operation creates additional cybersecurity risks. Local and remote connectivity will use a range of standard and proprietary communication protocols, expanding the scope of monitoring and protection [21]. Academic works have described the harmful effects of attacks which compromise the communication infrastructure, including compromising SCADA systems to



Cybersecurity Standards and Guidelines that Apply to Smart Energy Operational Environments

| Area (Focus) | Organizational (What) | Technical (How) | Process towards Compliance |
|---|---|---|---|
| General IT Security<br>Reflecting Business Requirements | ISO/IEC 27001<br>Security Requirements<br>ISO/IEC 27005, NIST SP800-39,<br>ISO 31000 Risk Assessment | Internet Standards<br>Directory svcs X500<br>LDAP RFC 4511<br>PKI, X509<br>OCSP RFC 6960<br>GDOI RFC 6407<br>EST RFC 7030<br>SCEP ...<br>IPSec RFC 1827<br>TLS RFC 5246<br>SNMP RFC 3418<br>Syslog RFC 5424<br>OAuth RFC 6749<br>Cloud Services<br>XML ... | ISO/IEC 27001 Certification<br>(ISO/IEC 27002/27019)<br>ISO 22301<br>Business Continuity<br>Cybersecurity Capability Maturity Model (C2M2)<br>(for determining the degree of compliance) |
| Energy Systems<br>Operational Environments<br>(Organizational and Procedural Security Controls) | NIST<br>Cyber Security Framework<br>ISO/IEC 27002, 27019<br>Security Controls<br>NISTIR 7628<br>Smart Grid Security Controls<br>NERC CIPs<br>Security Regulations for Bulk Power<br>IEC 62443-2-3, 2-4, & 4-1<br>Security Programs | IEC 62351<br>IEC 62351-3 to -6 Security for Protocols<br>IEC 62351-7 Network & Sys Mgmt (SNMP)<br>IEC 62351-8 Access Control (RBAC)<br>IEC 62351-9 Key Management<br>IEC 62351-10 Security Architecture<br>IEC 62351-11 Security for XML Files<br>IEC 62351-12 Cybersecurity for DER<br>IEC 62351-14 Security Logging<br>IEC/TR 62351-90-2 Deep Packet Inspection | IECEE CMC TF Cybersecurity for IEC 62443 2-4, 4-1<br>(in progress) |
| Energy Systems<br>Operational Technologies<br>(Technical Security Controls and Techniques) | IEC 62443-3-3<br>System Security Controls<br>IEEE 1547.3<br>Guide and Recommendations for Cybersecurity for DER<br>IEC 62443-4-2<br>Security for Products | IEEE 1686 Security for IEDs<br>IEC 62325-503 Energy Market Security | IEC 62443-3-3<br>System Security Controls<br>IEEE 1547.3<br>Guide and Recommendations for Cybersecurity for DER<br>IEC 62443-4-2<br>Security for Products |

Source: Xanthus Consulting International
21-50152

Fig. 2. Relevant cybersecurity standards and guidelines.

allow unauthroized control of a wind plant and multiple attack paths that cause substation disruption [15], [16]. Real-world incidents have also demonstrated the modern risk of cyber threats to wind systems [22]–[26].

From the perspective of a distributed wind system, it may be impossible to guarantee that the system is totally secure due to the number of dependencies and external links. These concerns demonstrate the need a cyber-resilience architecture to evaluate distributed wind. This cyber-resilience architecture can help stakeholders identify the most critical risks for their particular system. Additionally, the Idaho National Laboratory provides specific best practices for stakeholders in their cybersecurity guide for distributed wind [20]. The reference architecture provided in Figure 1 can be used to understand the attack surface for a system and to develop mitigations that address various components of the risk. In order for systems to have cyber resilience, they must be able to identify, prepare for, and detect cyber incidents. Knowing that these incidents are possible, impactful, and difficult to totally protect against is a key first step in building up resilience.

## IV. Cyber-Resilience Risk Architecture for Distributed Wind

In this section, we describe the breakdown of cybersecurity risk as it relates to distributed wind. The concept of risk is commonly illustrated using the model:

$$\text{Risk} = \text{Likelihood x Consequence}$$

Recognizing that likelihood is a function of adversarial behavior and weaknesses in the target, the model can become:

$$\text{Risk} = \text{Threat x Vulnerability x Consequence}$$

This simplified model identifies three key components of risk: threat, vulnerability, and consequence, which will each be discussed in more detail. The model expresses that each of these components can have a scaling effect on the overall risk when measured against a baseline. We do not define explicit metrics or units for risk, but rather emphasize that it is relative and dependent on many factors. For instance, unlikely threats with potentially large consequences may have similar risk as threats with medium likelihood and consequence.

To manage risk, it is necessary to manage the individual elements to the best extent possible. Although there may be common combinations of threats, vulnerabilities, and consequences used for prevalent attacks, these elements are independent from one another. Threat represents the ability of the actor perpetrating the attack. Vulnerability represents the weakness of the system to succumbing to the attack. Consequence represents the outcome if the attack is successful. Each element can be mitigated by adding resilience to the system, specifically through protection, detection, response, and recovery measures. With the mitigations in place, our qualitative risk model becomes:

$$\text{Risk} = (\text{Threat-}M_T) \text{ x } (\text{Vulnerability-}M_V) \text{ x } (\text{Consequence-}M_C)$$

In the model above, $M_T$ is mitigations to threats, $M_V$ is mitigations to vulnerabilities, and $M_C$ is mitigations to consequences. Each element in the model is described in more detail below.

### *A. Threats: Adversaries and Objectives*

The threat component of risk refers to the the capabilities, intents, and opportunities of potential adversaries. Threats can be both intentional and unintentional, but are nevertheless dependent on the capability of the threat actor. We can express the breakdown of threat as:

$$\text{Threat} = \text{Intent x Capability x Opportunity}$$

Here, intent is considered to be the adversarial objective, the outcome that the threat actor is trying to accomplish. The actions of a threat actor can be either intentional or unintentional. Unintentional cybersecurity threats are not maliciously motivated and, in many cases, are centered around errors by someone with authorized access and privileges on a system. In particular, employees with access to critical systems have high capabilities and may unintentionally create threats through misuse or mistake. Employee awareness of cyber risks is critical to minimizing threats. Intentional cybersecurity threats, on the other hand, are maliciously motivated and are driven by a particular objective of the adversary, which can vary widely.

Capability of a threat actor is the ability of the actor to execute their intent or otherwise perform malicious actions, even if these actions are unintentional. Threat actors can have capabilities across a wide spectrum. Here we define four adversary archetypes with different levels of capability to represent the range of possibilities.

- **Hacker**: An example of a threat actor with limited capabilities would be a single entity or small group of individuals motivated by curiosity, notoriety, fame, or attention, and may or may not target specific organizations. The skill set of this group may not be advanced, but through use of automated attack scripts and protocols that can be downloaded readily from the Internet, they can orchestrate make sophisticated attacks. This group may also be referred to as script kitties.
- **Insider**: 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. A disgruntled insider combines this capability of higher access with an intent to cause harm due to a perceived slight or general frustration with the target. Insider threats also include third-party vendors and employees who may accidentally introduce malware into systems, representing the same capability with a different intent. That is, an insider may make a mistake, thereby unintentionally introducing a threat to the system.
- **Organized Group**: This type of adversary is typically more organized and funded than hackers or insiders, creating the potential for higher capabilities. They often have a specific target, and can tailor their capabilities towards the target. Examples can include a corporate organization engaged in espionage, organized crime aimed at financial extortion via mechanisms such as ransomware, financial theft or blackmail, or hacktivists concerned with supporting political agendas.
- **Hostile Nation-State or Terrorist**: This type of adversary is often structured, sophisticated, and well-funded. Their capabilities allow them to launch advanced persistent threat (APT) campaigns, where an adversary gains unauthorized access and remains undetected for an extended period, pivoting into deeper and more sensitive networks before launching a targeted, high-consequence attack. These organized and persistent threat actors are often seen only by the digital traces they leave behind.

The final component of threat to consider is opportunity. Opportunity is the access an adversary has. There must be a path through which the adversary can interact with the target to have a successful attack, even if the adversary has strong intent and capability. Note the difference between opportunity and vulnerability. Opportunity is access to a target, while vulnerability is a weakness in implementation or design.

### *B. Vulnerabilities: Common Attack Vectors*

A vulnerability is a weakness which can be exploited by an adversary to gain unauthorized access to or perform unauthorized actions. The vulnerability may be a flaw in either design or implementation of 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 that details the different levels where a vulnerability might exist. The top process level is reliant on the integrity of the lower layers, so the vulnerabilities of the elements in these layers is also critical.

- **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. Hardware-level vulnerabilities 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) includes data and instructions to control the hardware and its functionality, ranging from booting the hardware to providing runtime services to loading an OS. Vulnerabilities at this layer could be exploited by an adversary to disrupt the software layer's capability to support the process.
- **Software Layer**: The software layer is comprised by one or more applications that collectively allow the system to function as designed. 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. Note that energy networks and ICS networks in general are typically flat and may lack the segmentation necessary to protect critical processes.
- **Process Layer**: At the top of the model is the process itself. For 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.

### C. Consequences: Impacts

Consequences can be defined by the impacts they have, who is affected by the impacts, and what the severity of the impact is. One method of relating potential consequences to a distributed wind environment is identified in the Industrial Control System (ICS) Cyber Kill Chain concept [27]. Using this concept, the goals an adversary may choose 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, shown in Table I.

| Loss | Denial | Manipulation |
|---|---|---|
| Loss of view<br>Loss of control | Denial of view<br>Denial of control<br>Denial of safety | Manipulation of view<br>Manipulation of control<br>Manipulation of safety<br>Manipulation of sensors and instrumentation |

TABLE I
CONSEQUENCE CATEGORIES USING THE ICS CYBER KILL CHAIN

In a distributed wind system "Manipulation of Control" 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.

Various stakeholders will experience consequences differently. Utilities may feel the impact of a loss of control event via energy imbalance in the system. Operators may experience propagated failures or equipment damage. Manufacturers or installers may be responsible for financial liability or may experience damaged reputations if their errors or oversights created vulnerabilities that were exploited in the attack.

Impacts can be quantified using the Consequence-driven Cyber-informed Engineering (CCE) scoring method described in CCE Phase 1: Consequence Prioritization [28]. This method allows users to determine the severity of high consequence events, define appropriate criteria for scoring, and weight different zones of impact.

### D. Mitigations: Resilience by Design

Cyber resilience must consider all aspects of risk in order to understand the hazards that may be faced. Putting together the threats, vulnerabilities and consequences into an attack vector shows all the places in which the hazards can be mitigated, whether through preparation, detection, or response and recovery. These elements of resilience may help reduce risk by affecting any component of the risk model.

Identification and preparation can include threat classification, by viewing the system through the eyes of an adversary. It can also include patching vulnerabilities and designing systems with backups and fail-safes, ensuring systems are robust even when attacks are carried out.

Detection can include the discovery of vulnerabilities, the sensing of attacks in progress, or recognition of likely threat actors.

Response and recovery are effective tools for mitigating consequences with real-time actions. The response component of resilience can also apply as the response to vulnerability disclosures in supply chain elements.

Figure 3 shows an example attack tree for a distributed wind asset. The boxes on the left show the intent of the attack, critical to the threat component. The nodes on the attack path represent exploited vulnerabilities that help achieve the objective. The box on the right shows a single possible consequence. The attack tree framework can be created for specific systems, working either from left to right (bottoms up) or right to left (top down). Multiple attack trees leading to various impacts may reveal common threats and vulnerabilities, assisting in the prioritization of cyber resilience actions. This specific example was created through a short brainstorming session with participants holding different perspectives.

A full cyber-resilience plan should consider multiple consequences and should note that vulnerabilities can be repeatedly exploited on different attack paths. Even if the resilience measures cannot be well quantified, it qualitatively suffices to recognize that these measures reduce risk. For specific systems, it may be possible to detail or quantify the risk reduction from the resilience measures.

## V. Recommendations for Assessing Cybersecurity Risk for Distributed Wind

The cyber-resilience risk architecture is key for evaluating cyber risks to distributed wind. Without proper identification of threats and holistic risk analysis, later stages of resilience like preparation, detection, response, and recovery for a cyber incident will be far less effective. In this section, we outline recommendations for implementing risk analysis considering the unique properties of distributed wind. The core recommendation is that stakeholders review cybersecurity and stakeholder recommendations in IEEE 1547.3, Guide for Cybersecurity of Distributed Energy Resources Interconnected with Electric Power Systems [29]. There are two aspects of distributed

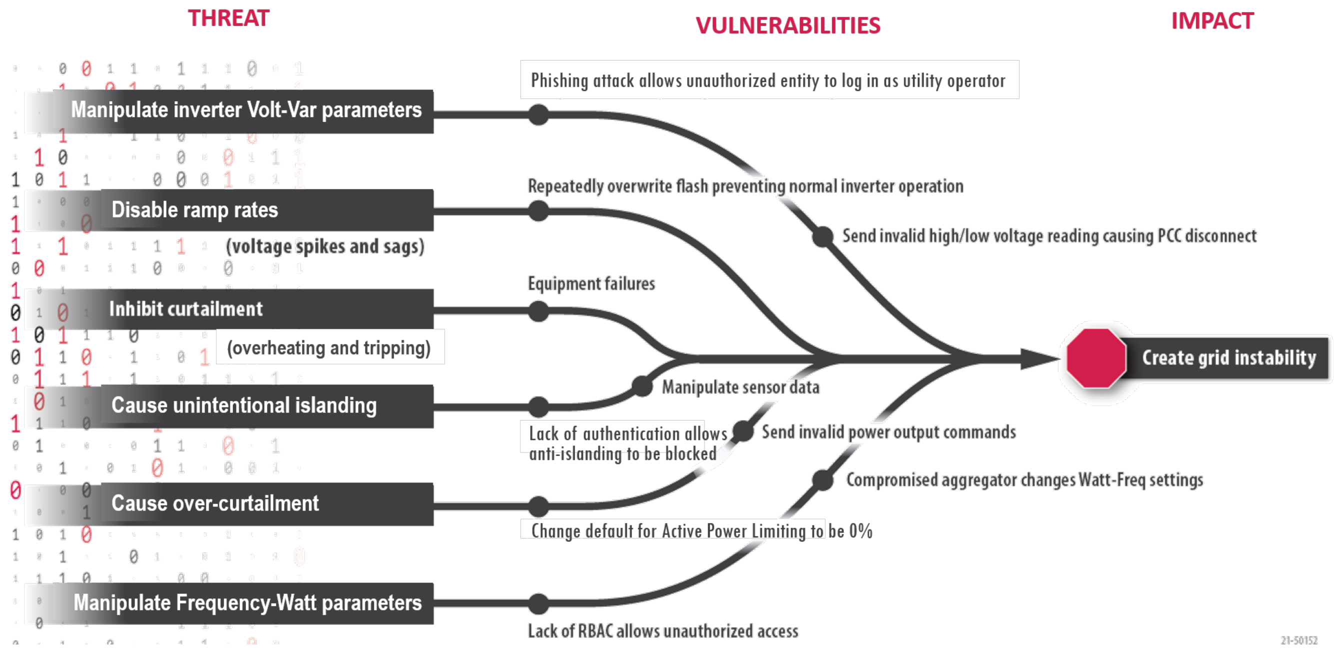

THREAT
VULNERABILITIES
IMPACT
Phishing attack allows unauthorized entity to log in as utility operator
Manipulate inverter Volt-Var parameters
Repeatedly overwrite flash preventing normal inverter operation
Send invalid high/low voltage reading causing PCC disconnect
Disable ramp rates
(voltage spikes and sags)
Equipment failures
Inhibit curtailment
(overheating and tripping)
Create grid instability
Manipulate sensor data
Cause unintentional islanding
Lack of authentication allows anti-islanding to be blocked
Send invalid power output commands
Compromised aggregator changes Watt-Freq settings
Cause over-curtailment
Change default for Active Power Limiting to be 0%
Manipulate Frequency-Watt parameters
Lack of RBAC allows unauthorized access
21-50152

Fig. 3. Example attack tree for distributed wind.

wind that are different from most other DER: Distributed wind is often located in remote areas and may be difficult to access, both physically and with reliable communications, and distributed wind has mechanical requirements, in particular, the rotating blades, the turning nacelle, and the gears to convert the blade rotation to the higher speed needed for the generator.

Cyber threats are one primary focus of risk assessment for all types of DER, and are covered extensively in IEEE 1547.3. However, for distributed wind installations which are sited at locations that are difficult to access, risk assessments should cover additional issues related to that isolation:

- 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 that may compromise local controls and communication.
- Risk assessments should enumerate all remote access capabilities and who has access. Given that remote control and monitoring is used for wind turbines more than other assets, access control should carefully managed.
- Risk assessments should consider physical impacts from cyberattacks, as there are many mechanical moving parts.
- Risk assessments should also include possibilities of physical damage such as wind-blown tree branches, (salt) water spray, bullets, and collisions from vehicles.

## VI. Conclusion

The work presented here outlines a cyber-resilience risk architecture for distributed wind. The chief contributions are (1) motivation for the need of distributed wind-specific cybersecurity, and (2) an architecture for risk that considers threats, vulnerabilities, and consequences associated with cybersecurity for distributed wind holistically. Together, these provide a starting point for stakeholders to consider their distributed wind cybersecurity risk profile. This architecture focuses on the identification stage of resilience, which is key to informing the later stages of resilience. Although this architecture does not explicitly discuss detection, response, or recovery methods for cyber incidents involving distributed wind, it does build a risk analysis architecture that can be utilized throughout the resilience process. The paper also outlines key recommendations for implementing risk assessments considering the remote nature of distributed wind installations.

## Acknowledgment

The authors would like to thank partners on the Microgrids, Infrastructure Resilience and Advanced Controls Launchpad (MIRACL) team at the National Renewable Energy Laboratory, Sandia National Laboratory, and Pacific Northwest National Laboratory for their feedback and support on this project. They would also like to thank DOE WETO program managers Bret Barker and Patrick Gilman for their support.

## References

[1] U.S. Energy Information Administration, “Electricity explained: Electricity in the united states.”

[2] U.S. Department of Energy, Wind Energy Technologies Office, “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. Lanz, 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, Tech. Rep., 2016.

[5] S. A. Bukowski, M. J. Culler, J. P. Gentle, J. C. Bell, C. R. Rieger, and E. Bukowski, "Distributed wind metrics for electric energy delivery systems," Idaho National Laboratory, Tech. Rep., May 2021.

[6] "Economic benefits of increasing electric grid resilience to weather outages," Aug. 2013.

[7] C. Powell, K. Hauck, A. Sanghvi, A. Hasandka, J. V. Natta, and T. Reynolds, "Guide to the distributed energy resources cybersecurity framework," National Renewable Energy Laboratory, Tech. Rep., Dec. 2019.

[8] R. S. de Carvalho and D. Saleem, "Recommended functionalities for improving cybersecurity of distributed energy resources," in *2019 Resilience Week (RWS)*, vol. 1, 2019, pp. 226–231.

[9] N. Duan, N. Yee, A. Otis, J.-Y. Joo, E. Stewart, A. Bayles, N. Spiers, and E. Cortez, "Mitigation strategies against cyberattacks on distributed energy resources," in *2021 IEEE Power Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, 2021, pp. 1–5.

[10] D. J. Sebastian, U. Agrawal, A. Tamimi, and A. Hahn, "Der-tee: Secure distributed energy resource operations through trusted execution environments," *IEEE Internet of Things Journal*, vol. 6, no. 4, pp. 6476–6486, 2019.

[11] N. Jacobs, S. Hossain-McKenzie, D. Jose, D. Saleem, C. Lai, P. Cordeiro, A. Hasandka, M. Martin, and C. Howerter, "Analysis of system and interoperability impact from securing communications for distributed energy resources," in *2019 IEEE Power and Energy Conference at Illinois (PECI)*, 2019, pp. 1–8.

[12] Z. Li, M. Shahidehpour, and F. Aminifar, "Cybersecurity in distributed power systems," *Proceedings of the IEEE*, vol. 105, no. 7, pp. 1367–1388, 2017.

[13] C. Powell, K. Hauck, T. Reynolds, A. Sanghvi, M. D. Touhiduzzaman, and J. Van Natta, "Distributed energy resources cybersecurity framework: Applying the nist risk management process," National Renewable Energy Laboratory, Tech. Rep., Oct. 2020.

[14] J. Marron, A. Gopstein, N. Bartol, and V. Feldman, "Cybersecurity framework smart grid profile," National Institute of Standards and Technology (NIST), Tech. Rep. NIST Technical Note 2051, Jul. 2019.

[15] A. Zabetian-Hosseini, A. Mehrizi-Sani, and C.-C. Liu, "Cyberattack to cyber-physical model of wind farm scada," in *IECON 2018 - 44th Annual Conference of the IEEE Industrial Electronics Society*, 2018, pp. 4929–4934.

[16] "Wind farm security: attack surface, targets, scenarios and mitigation," *International Journal of Critical Infrastructure Protection*, vol. 17, pp. 3–14, 2017.

[17] H. Wu, J. Liu, J. Liu, M. Cui, X. Liu, and H. Gao, "Power grid reliability evaluation considering wind farm cyber security and ramping events," *Applied Sciences*, vol. 9, no. 15, 2019.

[18] "Distributed wind." [Online]. Available: https://www.energy.gov/eere/wind/distributed-wind

[19] "IEEE standard for interconnection and interoperability of distributed energy resources with associated electric power systems interfaces," *IEEE Std 1547-2018 (Revision of IEEE Std 1547-2003)*, pp. 1–138, 2018.

[20] M. J. Culler, B. Smith, F. Cleveland, S. Morash, and J. P. Gentle, "Cybersecurity guide for distributed wind," Idaho National Laboratory, Tech. Rep., 2021.

[21] "Roadmap for wind cybersecurity," U.S. Department of Energy Wind Energy Technologies Office, Tech. Rep., 2020.

[22] ICS-CERT, "XZERES 442sr wind turbine vulnerability," Aug. 2018. [Online]. Available: https://ics¬cert.us-cert.gov/advisories/ICSA-15-076-01

[23] North American Electric Reliability Corporation, "Lessons learned: Risks posed by firewall firmware vulnerabilities," Tech. Rep., Sept. 2019.

[24] R. Davidson, "AWEA 2018: Increase in cyber security attacks 'inevitable', expert warns."

[25] B. Sobczak, "Grid leaders clear the air around Russian hacking," *Energywire*, Aug. 2019. [Online]. Available: https://www.eenews.net/stories/1060091819

[26] C. Bennett, "Russian hackers have infiltrated the US," *The Hill*, Nov. 2016. [Online]. Available: https://thehill.com/policy/cybersecurity/223266-report-russian-hackers-infiltrate-us

[27] M. Assante and R. Lee, "The industrial control system cyber kill chain," Tech. Rep., Oct. 2015.

[28] S. G. Freeman, N. H. Johnson, and C. P. St. Michel, "CCE phase 1: Consequence prioritization," Idaho National Laboratory, Tech. Rep. INL-EXT-20-58089, May 2020.

[29] "IEEE P1547.3$^{\text{TM}}$ , draft guide for monitoring, information exchange, and control of distributed resources interconnected with electric power systems," pending publication.