INL/EXT-21-64285
Revision 1

Case Study: Applying the Idaho National Laboratory Resilience Framework to Iowa Lakes Electric Cooperative Distributed Wind Systems

March 2022

Megan J. Culler
Power Engineer, Idaho National Laboratory

Steve Bukowski, PhD, PE
Senior Research, Idaho National Laboratory

Jake P. Gentle
Program Manager, Idaho National Laboratory

Clarenz K. Velasco
Infrastructure Security Intern, Idaho National Laboratory

Idaho National Laboratory

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

INL/EXT-21-64285
Revision 1

Case Study: Applying the Idaho National Laboratory Resilience Framework to Iowa Lakes Electric Cooperative Distributed Wind Systems

Megan J. Culler
Power Engineer, Idaho National Laboratory
Steve Bukowski, PhD, PE
Senior Research, Idaho National Laboratory
Jake P. Gentle
Program Manager, Idaho National Laboratory
Clarenz K. Velasco
Infrastructure Security Intern, Idaho National Laboratory

March 2022

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

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

Page intentionally left blank

ACKNOWLEDGEMENTS

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

- The Wind Energy Technologies Office: Patrick Gilman and Bret Barker
- Microgrids, Infrastructure Resilience, and Advanced Controls Launchpad partners:
  - Sandia National Laboratory (SNL)
  - Pacific Northwest National Laboratory (PNNL)
  - National Renewable Energy Laboratory
- Iowa Lakes Electric Cooperative
- Special thanks to Sarah Barrows (PNNL), Kendall Mongird (PNNL) for technical discussions

Page intentionally left blank

CONTENTS

FIGURES

TABLES

ACRONYMS

DDOS	Distributed denial of service
DER	Distributed energy resource
DMZ	Demilitarized Zone
DNS	Domain name system
DOE	U. S. Department of Energy
EEDS	Electric-Energy Delivery System
ESS	Energy-storage system
ILEC	Iowa Lake Electric Cooperative
INL	Idaho National Laboratory
IP	Internet protocol
IPS	Intrusion-prevention system
IT	Information technology
LAN	Local area network
MIRACL	Microgrid, Infrastructure Resilience, and Advanced Controls Launchpad
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
OT	Operational technology
PNNL	Pacific Northwest National Laboratory
PPA	Power purchase agreement
QF	Qualifying facilities
RBAC	Role-based access control
RPS	Renewable portfolio standard
SCADA	Supervisory control and data acquisition
SNL	Sandia National Laboratories
T&D	Transmission and distribution
VPN	Virtual private network
WIRED	Wind Innovations for Rural Economic Development

Page intentionally left blank

EXECUTIVE SUMMARY

This report is a case study implementing the resilience framework for electric energy delivery systems developed by Idaho National Laboratory. The case study examines the resilience benefits provided by two LEC 10.5 MW wind power plants, each composed of seven GE 1.5 MW wind turbines for a total of 21 MW. Iowa Lakes Electric Cooperative owns and operates the two wind plants and sells the power to the local generation and transmission Corn Belt Power Cooperative. The wind installations primarily serve two local ethanol plants.

Resilience hazards can take a variety of forms, including severe weather events, equipment failures, wildlife or vegetation damage, or manmade intentional damage. In this case study, we focus on the effects from a cybersecurity hazard. Cybersecurity hazards are very difficult to model, since there are not only many types of attacks that can occur, but the effects of each type of attack will depend on the attacker's skill level and intent, the protections that are in place on the system, and the point-of-entry for the attack. However, to follow the resilience framework, we must make assumptions about the effects of the attack so we can model the impacts to the power system and quantify the resilience outcomes. A variety of attack types are discussed qualitatively to demonstrate the range of potential impacts, and a potential ransomware attack on Corn Belt Power Cooperative is described such that the generation capacity is limited, and the wind plants alone must provide energy for their local loads. This scenario represents an extreme and unlikely event but serves to demonstrate the resilience benefits of having local generation, even though that generation may be variable. Because the hazard we consider could potentially take many days to recover from, we consider hazard durations of 10 hours, 3 days, and 7 days to show a range of scenarios. We assume for this scenario that the inverters have grid-forming capabilities.

The initial results show that wind alone can serve the full demand from the local ethanol plants, sometimes for over 24 hours at a time, depending on wind resource. However, at other times, there is a high amount of variability. We wanted to show how to maximize potential resilience benefits for this scenario, so we considered two types of changes to the system that would enhance resilience. The first we considered was the addition of battery storage. We performed simulations with battery assets of different sizes and found that the addition of storage smoothed out the variability of the wind resource, enabling the load to be served for a longer period of time before any partial outages occurred, and enabling the load to be fully served for more time overall during the hazard duration. The second addition to the system that we considered was demand response. While we did not interact with the ethanol customers directly to know how feasible this was, it seemed reasonable that these chemical plants would not be able to tolerate a variable supply of energy, rapidly changing their energy use to match the wind production, or perform many shut downs and start ups in rapid succession. We proposed that they could, however, curtail their energy demand by slowing production during the hazard duration. The combination of curtailed demand and storage to smooth the wind production variability dramatically increased the resilience benefits for the system in the form of more time until a partial outage occurred and less load dropped during the duration of the outage.

This case study demonstrated many features of the resilience framework for electric energy delivery systems. It showed how the resilience framework can be used to evaluate hazard scenarios even when it is difficult to predict exactly how those hazards will manifest in a system. It demonstrated how the framework can be used to evaluate potential changes to the system (addition of storage and demand response) to find the maximum resilience benefits in an iterative manner. We also showed how important stakeholder input is into the selection of resilience metrics and resilience goals. For a different local load, the variability of wind may have been more acceptable or it may not have mattered how many times the load was shut on and off compared to the duration of the hazard when load was served. However, because the customer type was a chemical plant, these considerations applied, and impacted the resilience findings.

Page intentionally left blank

Case Study: Applying the Idaho National Laboratory Resilience Framework to Iowa Lakes Electric Cooperative Distributed Wind Systems

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 U.S. was estimated at 110,809 MW at the end of the third quarter of 2020, representing over 7.3% of all installed generation capacity [1, 2]. Distributed wind is an important part of the growing wind segment, with 1,127 MW from over 83,000 turbines installed across the 50 states, Puerto Rico, the U.S. Virgin Island, and Guam from 2003 to 2018 [3]. The growing market segment and trends for rising commercial-, industrial-, and utility-use distributed wind projects motivate the need for a comprehensive understanding of the resilience of distributed wind systems. Access to reliable, resilient power systems is important in 21st century—now more than ever. While all critical infrastructure sectors have important interdependencies, the power grid is inextricably tied to the successful operation of water treatment, communications, healthcare, and many other systems, because it provides an "enabling function" across all critical infrastructure sectors [4]. Moreover, the electric grid is being increasingly tested by a combination of physical and cyber threats. Terrestrial weather events, exacerbated by climate change and extreme weather conditions, happen with greater frequency and intensity. Space events have the potential to cause widescale effects across interconnections and borders. Aging grid infrastructure is not yet adequately prepared to accommodate rapid technological changes, including variable renewable resources, transportation electrification, energy storage, and carbon-free energy standards. Cyberattacks are seen with increasing frequency against the power grid, and the attacks are becoming more sophisticated and targeted toward electric energy systems.

Traditional metrics and evaluation methods for resiliency are not sufficient to evaluate the effect that distributed wind systems will have, particularly in light of the challenges described above. While the concept of resiliency is not new, its application to the electric grid is neither standardized nor well-defined. Additionally, little to no guidance exists on how to evaluate resilience, specifically for distributed wind systems. To fill this gap, the Idaho National Laboratory (INL), as part of the multi-laboratory Microgrids, Infrastructure Resilience, and Advanced Controls Launchpad (MIRACL) project, has developed a resilience framework for electric energy delivery systems (EEDS) [5]. The framework provides detailed steps for evaluating resiliency in the planning, operational, and future stages, and it encompasses five core functions of resilience. It allows users to evaluate the resilience of distributed wind, taking into consideration the resilience of the wind systems themselves, as well as the effect they have on the resiliency of any systems to which they are connected. Because distributed wind can operate in a variety of applications and at different scales, there is no one-size-fits-all approach for evaluating resiliency. However, this framework provides the tools and guidance for stakeholders to evaluate their current position, create resiliency goals, compare different investment options, and decide which metrics are most appropriate for their system.

In this document, the framework is applied to evaluate the resilience of distributed wind in the Iowa Lakes Electric Cooperative (ILEC) system to a cybersecurity hazard.

MIRACL Reference Systems

Reference systems were defined by the MIRACL team as operational distributed wind systems with significant data available for use in MIRACL research. The three primary MIRACL research areas of advanced controls, valuation, and resilience will be evaluated and applied to the identified reference systems.

Required Characteristics

Reference systems were chosen based on the following characteristics [6]

1. The reference system represents a real-world system with a nonlaboratory/nonacademic industry partner.
2. The MIRACL team has a point of contact who is interested in partnering and sharing data outlined in the technical parameters section of this report.
3. The identified reference systems cover unique MIRACL use cases.
4. The selected site either has wind turbines or could feasibly add wind turbines.

Desired Resilience Characteristics of EEDS

Resilience characteristics desired by the MIRACL team are:

1. Defined resilience goals or understandings of potential threats to the energy delivery system, including climate/weather, emissions, fuel availability, or other potential goals identified by stakeholders.
2. Recent changes to the EEDS that might include capital investments to address system change.
3. Open to information sharing on
    - Cybersecurity policy, guidelines, and practices (e.g., detection and response)
    - Information and/or operational technology networks for power systems operation and other associated networks.

ILEC was selected as the second MIRACL reference system based on the MIRACL team's ability to coordinate date requests, model development, and technical discussions with existing U. S. Department of Energy (DOE) Wind Innovations for Rural Economic Development (WIRED) awardees at the National Rural Electric Cooperative Association and Iowa State University. This reference system falls under the MIRACL Use Case 4: Front-of-the-meter distributed wind turbine deployments.

There are two ILEC 10.5 MW wind power plants, each composed of seven GE 1.5 MW wind turbines for a total of 21 MW. ILEC owns and operates the two wind plants and sells the power to the local generation and transmission Corn Belt Power Cooperative, which ultimately sells power to Basic Electric Power Cooperative. A 20-year power purchase agreement (PPA) was established in 2009.

Together, the two wind power plants generate about 77,000 MWh each year, which is about 12% of ILEC's electricity supply. The annual capacity factor of the wind plants is approximately 42%. The co-op financed the $43 million project with 0% interest clean renewable energy bonds, which are available to electric cooperatives and other public entities for many of the same kinds of renewable energy developments covered by federal production tax credits. This resulted in a $2.05/W cost of energy in 2009, which was a very good price at the time. Over a lifetime of 20 years, the installation costs can be distributed as 2.8¢/kWh.

Each 10.5-MW wind power plant is part of a distribution substation that services an ethanol plant that uses about the same amount of energy as is produced by the wind turbines annually. One plant is adjacent to the Green Plains ethanol plant near Superior, Iowa. The other plant is next to the Global Ethanol facility near Lakota, Iowa.

Each wind power plant connects to its respective distribution system through roughly 2-mile underground 3-phase lines to Corn Belt-owned substations. Within the Corn Belt substations, the wind plants connect to the same 12.47-kV bus that serves the associated ethanol plant. The substations connect to the external grid through transformer and 69-kV sub-transmission line. Most of the generation flows through the low-side bus of the substations and is used onsite by the ethanol plants; any excess wind production either flows out through the 69-kV transmission or is imported through the 69-kV line to serve the ethanol plants.

ILEC also has just over 3 MW of distributed generation, consisting of small wind and solar arrays dispersed through their eight-county system, which ILEC members have installed behind the meter to help offset their usage. Solar is the bulk of the 3 MW, as it has become less-expensive and less maintenance-intense to operate at the lower level for ILEC members.

INL Resilience Framework

The INL resilience framework has been developed to broadly apply to EEDS so that all elements of systems that contain distributed wind can be part of the resilience evaluation. The users or audience for this framework can include any stakeholders associated with the EEDS. Not all electrical energy systems have the same stakeholders; customers, owners, and operators are generally present, but have different interests. Considering the broad electrical grid, customers, regulators, investors, utility planners, engineers, and operators each have an interest in system resilience driven by different motivating factors.

In this document, the definition of resilience for EEDS as previously identified in the INL distributed wind metrics report is used:

> *The resilience of an EEDS is described as a characteristic of the people, assets, and processes that make up the EEDS and their ability to identify, prepare for, and adapt to disruptive events (in the form of changing conditions) and recover rapidly from any disturbance to an acceptable state of operation [7].*

This definition suggests a few key considerations. Resilience is unique in the depth and breadth of factors associated with the topic. It spans an assortment of technology resources and systems, geographic factors and constraints, risk-severity levels, and diverse stakeholder perspectives. This multiplicity of factors points to the need for a framework that is applicable across various situations and scenarios and that can be effectively implemented by different stakeholders.

A three-tiered approach is developed in the resilience framework. At the top level, three stages of resilience represent different times in a system's lifecycle and different means of evaluating and executing resilience. At the intermediate level, five core functions of resilience are defined, spanning the time stages. At the lowest level, process steps are described that correspond to implementing practices for resilience in each of the core functions. This tiered breakdown is shown in Figure 1.

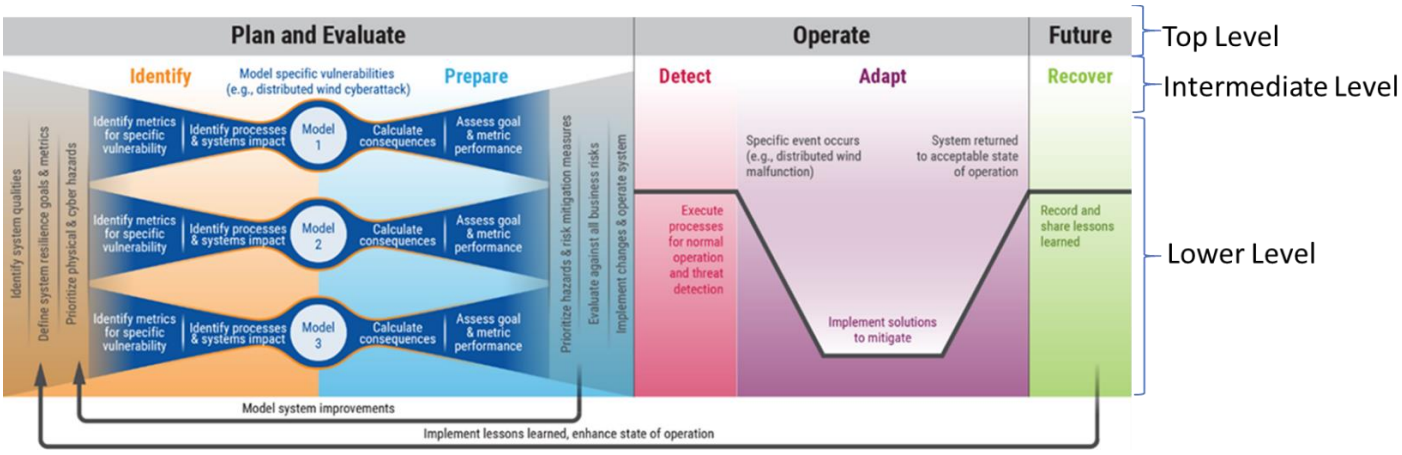

Figure 1. INL resilience framework.

The framework considers three stages of resilience to enable stakeholders to assess and improve their system's resilience throughout its lifecycle. Because considerations of time can vary based on where in the framework users find themselves, we simplify the time considerations to the planning, operational, and future stages. The planning stage uses future organizational needs and current system status to prepare for potential risks. The operational stage seeks to respond to active risks as prudently and efficiently as possible to maintain system resilience. The future stage seeks to improve on current system resilience and feeds back into the planning stage to promote continuous improvement. While all three stages are important, the planning stage (i.e., what is done in advance of the event) is critical in defining a system's resilience characteristics and in outlining how a system responds to an event. The case study presented in this document focuses on the planning stage to demonstrate how the framework can be used to add resilience planning to traditional planning efforts. In particular, it focuses on evaluating the resilience benefits of adding a distributed wind turbine.

The core functions in the framework are labeled identify, prepare, detect, adapt, and recover. These five functions stem from a rigorous analysis of definitions used across the industry, and they represent the core capabilities that a system must have to enable lifecycle resilience. While not an exact match, these core functions are partially derived from, and align with, the core functions of the National Institute of Standards and Technology (NIST) cybersecurity framework for critical infrastructure [8]. Using a structure similar to the NIST framework makes it recognizable and familiar and provides a well-established methodology. Within each core function, process steps are described that help walk stakeholders through the information gathering, evaluation, decision-making, and implementation processes they will need to ensure their resilience goals are maintained throughout the system lifecycle.

Also highlighted in the figure is the concept that a resilience framework should be cyclical in nature. Because a system's resilience is based on finite resources and time, it must continually evolve through this framework's risk management and capital investment steps at an appropriate level of scope and pace.

Stakeholders can use this framework as a key component to identify, assess, and mitigate risks associated with resilience. The framework is intended to be used alongside existing processes to determine gaps at each stage of resilience (planning, operational, and future) and to develop a program for systematically prioritizing and improving resilience planning. The framework is extensible; it is applicable at global and granular scales of system resilience planning and operations. The framework is also accessible to a wide variety of interested stakeholders, such as utility practitioners, regulators, environmental constituents, or interested members of national laboratories and academia. This document helps to outline the considerations and processes associated with holistic, long-term resilience planning.

Within this document, the framework emphasizes the planning stage before applying the framework to a utility planner considering multiple investments. While extensive processes are already in place for power system planning, this framework differentiates itself from other related risk frameworks or resilience metrics by considering an all-hazards approach that complements traditional reliability analysis. The framework includes the integration of the uncertainty of cyber effects, weather events, or intentional physical damage, and it creates a process for the model-informed consideration of each hazard.

FRAMEWORK APPLICATION

This document focuses on the planning stage of the framework, the process for which is shown in Figure 2. In this document, each step is explained briefly before demonstrating its application to the ILEC system.

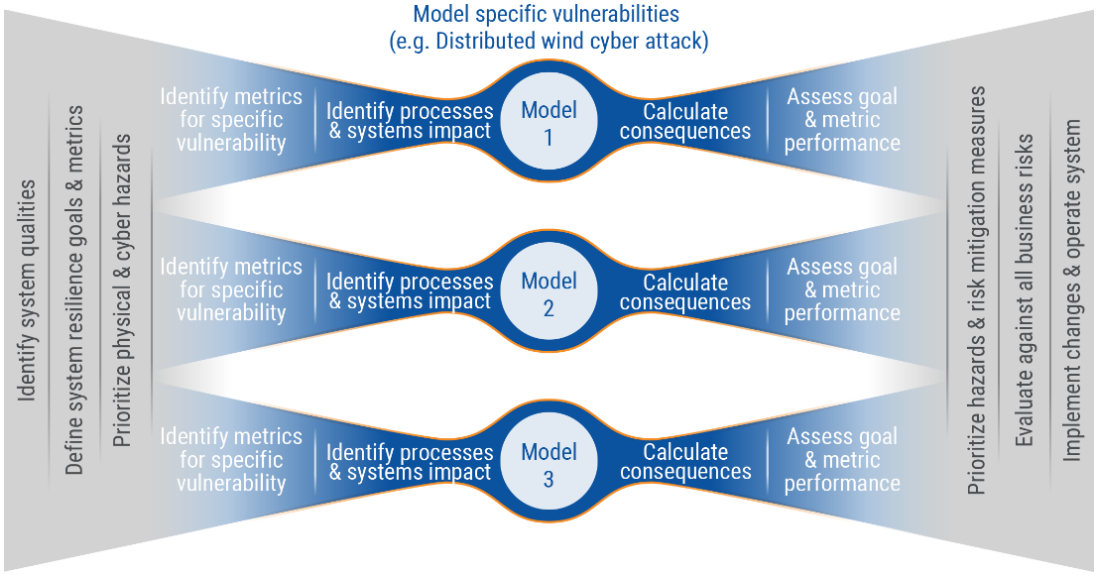

Figure 2. Nested planning bow tie.

The framework can be used for many types of resilience planning. For example, it can be used to evaluate current overall resilience or the resilience of certain subsystems. It can be used to explore existing resilience weak points and propose mitigations. It can also be used to evaluate the resilience benefits of a new investment.

In this study, we evaluate the resilience of the distributed wind subsystems to cybersecurity hazards. We show that the wind resource can benefit the overall system resilience during some hazards. We show that the practices in place make the wind systems resilient against some cybersecurity hazards, but significant risks remain associated with other cybersecurity hazards. Our MIRACL partners at Pacific Northwest National Laboratory (PNNL) assign value to the resilience provided by distributed wind and various mitigation measures based on costs and costs avoided in the different scenarios.

As a post-installation exercise, this methodology can be used to better understand the full value provided by a distributed wind asset and to motivate future upgrades or expansions on the distributed wind asset.

Identify System Characteristics

A successful resilience framework begins with identifying the system. Stakeholders must know their system characteristics and qualities to define the boundaries of stakeholder roles and evaluate the consequences of certain events. The system may be defined by some combination of geographic and electric boundaries, business processes, relevant time periods, or even components. It is important to note the characteristics of the turbine and the controller, including the ancillary services they can provide, the weatherization packages that are included, and the physical limitations with respect to external conditions (e.g. wind, temperature). Each system is unique; therefore, a system must be fully defined before its resilience and the relevant resilience scenarios can be uniquely defined.

ILEC serves 12,950 farms, homes, businesses, and industries. The co-op sells about 650 million kilowatt-hours annually. Of this, about 63% is commercial and industrial, and the remainder is residential and agricultural. ILEC is a member of two generation and transmission providers: Corn Belt Power Cooperative (Corn Belt) and Basic Electric Cooperative. Corn Belt became a member of Basic Electric in 2009. This arrangement means that ILEC sells power directly to Basic Electric but uses the Corn Belt transmission system [9].

Iowa Lake's territory is on the eastern slope of Buffalo Ridge. It offers some of the best wind resources in the country. In fact, Iowa ranks first in the nation for having the highest share of wind energy in the state's portfolio, at 58% as of May 2021 [10]. The two wind plants we study make up 11.8% of the ILEC production, which is lower than the state average, but does not necessarily represent all the ILEC wind assets, just these two distributed wind plants.

ILEC began discussing wind installation in 2004, but no final plans were made until 2007. Iowa was the first state in the country to pass a renewable portfolio standard (RPS), and at the time, wind was the most feasible renewable generation method [11]. By 2007, additional incentives had come into play, including the federal Energy Policy Act of 2005, which introduced a 0% interest Clean Renewable Bonds (CREBs) program and state policy that adopted a $0.01/kWh production tax credit for qualified wind facilities placed into service between 2005 and 2015 [12, 13]. This further reduces the lifetime cost of energy. At the time the two wind farms were built in 2009, the combined capacity of 21 MW made it the largest wind project to be designed, financed, and owned by any distribution electric cooperative at that time. Because of this, ILEC received DOE's Wind Cooperative of the Year award in 2011 as part of the Wind Powering America Initiative [14].

Table 1. Technical details describing system.

Category	Details
Generation sources of interest	Wind
	Imports from Corn Belt Transmission and Distribution (T&D)
Wind resources [9, 15]	Superior turbine farm • 10.5 MW capacity • Seven GE 1.5 MW turbines (model: 1.5 SLE with energy-storage system (ESS) pitch system) • 80 m (262 ft) hub height Lakota turbine farm • 10.5 MW capacity • Seven GE 1.5 MW turbines (model: 1.5 SLE with ESS pitch system) • 80 m (262 ft) hub height Interconnection system • 3 phase distribution • 7.2 kV phase voltage • 12.47 kV line voltage

Category	Details
	• Grounded Y connection (different from common large utility-scale wind farms which are at 34.5 kV Delta connections interconnected to transmission grid) Production • Averaged 40% capacity factor, with a high of 42% • Annual output projection 72,000 MWh (often exceeded) • Max of 84,000 MWh in 2014 Controls • Voltage and power regulation (not often used) • Voltage and frequency ride-through (static in the turbine, but there if needed) • Reactive power features (not used) Communications • Modbus, DNP3 and more used • Fiber ties turbines back to supervisory control and data acquisition (SCADA) at substations • Servers at substations allow remote access to data • Dedicated communication from substations to ILEC facilities Security • Password-protected access points with Role-based access control (RBAC) providing different levels of tiered access • VPNs in place • Multi-factor authentication needed to get into admin control room • Corn Belt can monitor at the substation, can open the substation breaker on the outgoing side • Corn Belt subject to NERC CIP requirements • Physical locks on control box of turbine • Physical locks on turbine door • Physical locks at substation server house + password-protected alarm system Weatherization • Cold weather package offers series of heaters for oil and gearbox, control boxes and nacelle • Derated production starts at ~-8°-10°; ceases operation at -20° • No de-icing or ice detection
Load [9]	Two ethanol plants connected to two substations installed by Corn Belt Substations each have up to 15 MW of transformation available Ethanol plants run at approximately 6 MW and 7–8 MW each but can range from 6–10 MW while operational. We assume a relatively flat load with 24/7 operations. Even when the plants go offline, they still used ~1 MW while undergoing maintenance.
Transmission [9]	Corn Belt Power 69 kV line ILEC sells all wind energy directly to Basin Electric, 20 year power purchase agreement (PPA) in place

Category	Details
	Ethanol plants purchase all electricity from ILEC through separate consumption meters

The sites are small enough to be Federal Energy Regulatory Commission (FERC) Qualifying Facilities (QF) and are therefore not subject to curtailment [9].

Define System Resilience Goals and Metrics

There is no one-size-fits-all approach for resilience in EEDS, or even for distributed wind. Stakeholders should come together to identify what resilience means in the context of their system. Stakeholders should identify what they wish to achieve with their system before appropriate metrics and models can be determined, and before investments can be made. At this stage, the system's resilience metrics should also be identified. The metrics that are useful for evaluating resilience will depend on each individual system and the individual risk, but certain metrics will persist through all scenarios. Data availability may drive decisions about what metrics to use. However, care should be taken so that metrics selected are specific enough to enable decision-making, whether for operational or planning purposes. Metrics should ideally aid in direct and indirect assessment of resilience, cover both quantitative and qualitative properties of the system, meet as many of the characteristics shown as possible, and consider the entire physical and operational scope of the system, including inputs, capacity, capabilities, performance, and outcomes [7].

Figure 3. Desirable characteristics for resilience metrics.

Resilience Goal 1: Maintain Operations During Cybersecurity Events under High Renewable Penetration

Iowa was the first state in the U.S. to adopt an RPS when they enacted the Alternative Energy Production law in 1983; the law requires its two investor-owned utilities (MidAmerican Energy and Alliant Energy Interstate Power and Light) to own or contract for a combined total of 105 MW of renewable generating capacity [16]. As of May 2021, Iowa has more than 11,778 MW of wind, solar, and energy storage capacity [10]. The Iowa Environmental Council, the state's largest non-profit

environmental coalition, published *Iowa's Road to 100% Renewable*, outlining potential paths to reach 100% renewable electricity in Iowa by 2050 [17]. Although ILEC is member-owned, not investor-owned, it is clear that using renewable resources for electric power generation is a high priority in the state.

The Iowa state goals for renewable energy were not necessarily developed as a resilience goal. However, diversifying energy sources reduces the dependency on any single resource, which increases resilience. As we consider long-term renewable energy mandates, including the executive order for carbon-free energy production by 2035 and net-zero emissions by 2050, increasing renewable energy production also prepares for the necessary energy transition to meet these mandates [18]. If this transition is made too suddenly, the infrastructure and processes will be barely equipped to operate under normal conditions, let alone resilience hazards. Instead, focusing on using the existing renewable sources to the greatest extent possible better prepared the system for future reliance on these resources when other non-renewable energy resources are retired.

This resilience goal can be evaluated with the resilience metrics presented in Table 2.

Table 2. Metrics toward evaluating renewable production.

Indirect Metric	Source
Wind production	ILEC data request
Imported generation	Synthetic data

Resilience Goal 2: Reduce Planned and Unplanned Outages for Ethanol Plants in the Presence of Cybersecurity Threats

For the substations analyzed, the loads of interests are the two ethanol plants. These plants run at a nearly constant output 24/7, and interruptions in service can be very costly. Thus, the second resilience goal that we consider for the distributed wind subsystems is to reduce the planned and unplanned outages for the ethanol plants. This may sound more like a reliability goal rather than a resiliency goal. However, the North American Electric Reliability Corporation (NERC) defines reliability using two core concepts: adequacy and operating reliability [19]:

- "Adequacy is the ability of the electric system to supply the aggregate electric power and energy requirements to the electric consumers at all times, taking into account scheduled and reasonably expected unscheduled outages of system components."
- "Operating reliability is the ability of the system to withstand sudden disturbances such as electric short circuits or unanticipated loss of system components."

This definition of reliability speaks to the ability to plan for scheduled or expected failures. It does not account for the high-impact low-frequency (HILF) events typically considered under the resilience domain. For this analysis in particular, which focuses on cybersecurity hazards, we note that the definition of reliability does not address hard-to-predict events like cyberattacks that can vary significantly in their impact. It is impossible to anticipate all types of cyberattacks or to predict exactly when they might occur.

This goal can be evaluated with the resilience metrics presented in Table 3.

Table 3. Metrics toward evaluating power quality.

Metric	Source
Outage duration	ILEC data request, assumptions

Prioritize Physical and Cyber Hazards

Stakeholders should work together to prioritize physical and cybersecurity hazards. This can be done by considering which impacts would be most damaging to the system and then which hazards are likely to cause them. The prioritization is used to identify what should be modeled and assessed further. After stakeholders understand the possible threats to a system, the risk of these threats should guide prioritization. Whether it is a physical or cybersecurity hazard, the following calculation is helpful in considering risk assessments.

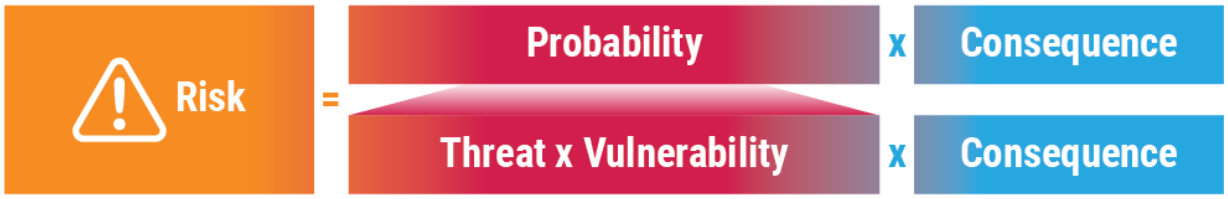

Figure 4. Risk assessment calculation.

Risk can be considered the probability (or likelihood) times the consequence (or impact). In this manner, a high-impact but unlikely event can be prioritized against a medium-impact, frequent event. The probability component includes both the threat and the vulnerability of the system to that threat. In the case of a cybersecurity hazard, threats should be evaluated within the constructs of intent and capability. For a weather-based hazard, the system may be vulnerable in different ways and in different geographic areas. Further, vulnerability may be dynamic. A system may include a defense mechanism or emergency state of operations that adjusts the system's vulnerability to various threats. The attributes of each hazard will need to be described in detail so that the consequence can be determined. Duration of the consequence should also be considered because it is a key resilience characteristic.

As previously mentioned, it is impossible to classify every possible cyberattack, but it is useful to consider a few common types of cyberattack, particularly those that have seen rising frequency in the energy infrastructure. For the primary risk prioritization, we consider the following scenarios, many of which are referred to in the wind cyber threat landscape in the DOE Roadmap for Wind Cybersecurity [20]:

- Ransomware
- SCADA compromise
- Cryptojacking
- Denial-of-service.

Ransomware

All organizations are at risk of being targeted by ransomware, but the threat of ransomware to operational technology (OT) assets and control systems is increasing. Although, historically, energy management networks were fully separated from business networks, modern technology makes it more and more difficult to make technological advances while maintaining security and separation. OT components are often connected to information technology (IT) networks, allowing a malicious actor to pivot from IT to OT networks [21]. The energy sector can be a particularly valuable target for adversaries because the highest security priority for electric energy systems is availability. The electric utility sector is seeing an increase in ransomware attacks, and examples are prevalent across the world [22, 23]. Recent attacks in related sectors indicate that ransomware can have an effect on operations in addition to compromising IT systems and payment infrastructure [24]. If ransomware can compromise the

availability of an electric energy OT system, attackers will have strong leverage against their victims to demand swift and large payment sums.

For the ILEC system, there are a few ransomware attack paths that we can consider.

Corn Belt ransomware

The first scenario we can consider is ransomware that hits the Corn Belt T&D co-op, rather than ILEC directly. If the ransomware infects the OT system of Corn Belt, it could cause inefficient or imprecise generation dispatch, leading to a lack of resources where they are needed. If ransomware infects the IT system such that operators feel it is unsafe to continue operations, then ILEC could lose access to the power imports it relies on to supplement wind power at the ethanol plant substations. The wind plants themselves are unaffected. The risk associated with this scenario is moderate because the wind turbines can still provide some power to the ethanol plants, but without the supplementary power from the transmission system, the ethanol plants will not likely be able to run at full output. Additionally, any excess power will have to be curtailed. This scenario could cause the system to fail in its achievement of both resilience goals: maximizing renewable energy output and providing constant and continuous power to the ethanol plants. These consequences are severe, but the likelihood of ransomware impacting the operational functionality of a transmission operator remains low. The combination results in a moderate risk.

Figure 5. Preliminary risk assessment of Corn Belt ransomware.

ILEC IT ransomware

If ILEC is directly compromised by ransomware, which could have many points of origin including phishing, improper USB use, known vulnerabilities, or zero-day exploits, then we assume that, at the very least, their enterprise systems will be compromised [25, 26]. In many cases, this can cause consequences that include unavailability of email servers and web-based bill-paying systems and the potential loss of sensitive data [27, 28]. This may not impact the ability of ILEC to operate its power systems if the IT and OT systems are well segmented. In this case, the consequences will be more business oriented than power system oriented. ILEC may need to meet mandatory reporting requirements and may have a duty to report the breach to their members. Consequences may include long-term loss of trust in the board, expensive overhaul of IT equipment, and increased potential for a more severe cyberattack if the exfiltrated data is sold or used to mount a more targeted campaign. These consequences point to an important difference between the short-term reliability impacts that consider only the power system and resilience impacts, which consider the lifetime of the system. Although the consequences are tolerable, both in terms of

short-term and long-term impacts, the likelihood of such an attack is rising. Many utilities across the U.S. have already experienced similar attacks.

Figure 6. Preliminary risk assessment of ILEC IT Ransomware.

ILEC OT ransomware

This scenario considers what would happen if ILEC was directly hit with a targeted ransomware attack that impacted OT systems or created significant instability on the IT side, forcing operators to choose to shut the power system down in order to protect its integrity and security. The consequences of this attack are more immediate and more directly measurable on the power system. In the worst case, we assume that the wind turbines are shut down. The ethanol plants would be served entirely by power imported from the transmission system, which would negatively affect the goal of using renewable energy. Corn Belt is fully capable of meeting this load, but the energy would come at a higher cost to ILEC.

Figure 7. Preliminary risk assessment of ILEC OT ransomware.

In both ILEC ransomware cases, the co-op would be responsible for deciding whether to pay the ransom or not, repairing or replacing equipment compromised in the attack, performing forensic analysis to determine whether data were exfiltrated and, if so, how it might be used or sold, and adding security to systems to ensure that a future ransomware attack is never successful.

SCADA Compromise

Academic and real-world events have demonstrated the possibility of an attack compromising the SCADA system of a wind turbine. In these types of attacks, an adversary may have the ability to directly change control system inputs or manipulate data coming from the turbines. The examples presented here were informed by the DOE "Roadmap for Wind Cybersecurity" [20].

In 2018, researchers demonstrated a cyberattack targeting a wind plant SCADA system. By compromising the SCADA system, they illustrated how an adversary could gain unauthorized control of a wind plant, send false commands to target components, and stop or potentially damage wind turbines. If successful, the cyberattack could lead to system instability or a cascading outage, depending on wind plant interconnectivity [29]. The researchers noted that access to the SCADA system could be achieved by physical access to a wind plant's local area network (LAN) via a local control panel or remotely via an external network. Although accessing a wind plant LAN via an external network is likely more challenging than physically accessing a geographically remote control panel, an attacker may be able to bypass firewalls between Internet-facing business networks and wind plant control or operational networks if firewalls and network communications are poorly configured. The physical and cybersecurity protections in place at the ILEC wind farms make both physical and external network access unlikely, but it is still a scenario that should be considered.

In 2017, researchers from the University of Tulsa described attacks focused on wind turbine control, turbine damage, wind plant disruption and damage, and substation disruption and damage [30]. Using custom-built tools, the researchers demonstrated the ease with which an attacker could fabricate and replicate turbine control messages; use a worm to propagate malicious, detrimental commands within a turbine or throughout a wind plant network; or exploit flat wind plant network topology "to block, modify and fabricate control messages at will." The vulnerabilities exploited by the researchers were all related to the lateral, unsecured implementation of control devices and communications across wind plants, lack of network segmentation, and lack of encryption for wind plant communications—all commonly observed characteristics of wind plants. Not enough data are available about the ILEC OT network topology to say exactly how protected ILEC is against a propagating worm-type attack, but it remains a valuable scenario to consider.

In 2011, researchers from Iowa State University and the Virginia Polytechnic Institute demonstrated how several vulnerabilities in the SCADA systems of 2-MW wind turbines could be exploited to cause "major problems within a power system, including economy loss, overspeed of a wind turbine, and equipment damage" [31]. The attack scenarios included physical- and network-access attack paths; ILEC may be most vulnerable to the method of installing surreptitious taps on fiber cables connected to wind turbines to pass false measurement data between turbines and the SCADA system using a man-in-the-middle (MiTM) attack.

These attacks are not just theoretically possible but have happened in real-world incidents. During a cybersecurity presentation at the 2018 American Wind Energy Association (AWEA) Conference, a technical expert illustrated how an unintentional cybersecurity event impacted an unnamed wind plant: "In one incident, a technician logged on to his laptop in a hotel and downloaded malware by mistake. When he went to work the next day and logged on, the wind plant became infected, and the turbines stopped working one by one" [32].

If a SCADA compromise were to occur, the consequences would be heavily dependent on the scale of the attack and adversary intent. It could affect a single turbine, in which case the consequences would be small. It could be limited to turbines connected to a single substation, in which case the effect is also limited, and additional power is imported from Corn Belt. The compromise could be severe if the attackers could manipulate the turbine controls in such a way that the power output has negative effects on the stability of the connected transmission system, potentially causing cascading effects. Even under the worst-case consequences, the probability of a SCADA compromise remains low since it would require targeted intent and specific system knowledge.

Figure 8. Preliminary risk assessment of SCADA compromise.

Cryptojacking

Cryptojacking is an attack in which adversaries use extra processing power to mine cryptocurrency. In 2018, an undisclosed wind plant experienced a cryptojacking attack. It slowed down the wind network, but not significantly enough to directly impact the turbine control and monitoring functions controlled by the workstations [33].

If this type of attack were to occur against ILEC, similar consequences would occur. There might be measurably increased latency for communications, but it is unlikely to affect power production or the ability to safely control the turbines. For this reason, it is classified as a low-risk hazard.

Figure 9. Preliminary risk assessment of cryptojacking compromise.

Denial-of-Service

In a denial-of-service (DoS) attack, the attacker floods systems, servers, or networks with traffic to exhaust resources and bandwidth. This attack can occur against any resource with which the attacker has the ability to communicate, such as servers, firewalls, or other network endpoints.

In 2019, a DoS attack occurred against the wind and solar provider sPower. This attack caused Cisco firewalls to reboot in 5-minute intervals over a 12-hour period. During the reboots, operators lost visibility and communications with solar and wind resources, although the attack did not affect the generation itself or the transfer of power [34]. This attack was not believed to be targeted, and the attackers may not have even known who the victims of their attack were [35].

We imagine a similar scenario happening on the ILEC system. Depending on exactly what resource was compromised by the DoS attack, it is unlikely that the attack would cause impacts on the ability of the turbines to produce power. However, loss of control and monitoring could affect the dispatch of the generators and could potentially have more significant consequences if important alerts or alarms went unseen by operators during the attack. Hackers employed a DoS attack against call centers in Ukraine during the infamous attacks on the Ukrainian power grid in 2015. This attack interfered with operators' ability to identify outage areas quickly [36]. In this way, DoS attacks could be part of a larger campaign, or they could simply unintentionally mask other issues in the system's operation.

Figure 10. Preliminary risk assessment of DoS attack.

After performing the preliminary risk assessment, we observe that ransomware and DoS attacks have the highest risk. A SCADA compromise is an advanced attack that is significantly less likely to occur than the other threats. A cryptojacking attack may be more common but will not likely have significant impact on the system.

Bow-Tie Analysis of Specific Hazards

Once stakeholders have identified and prioritized hazards, those that rank highest should be analyzed more closely. Certain hazards may be readily modeled while others may require testing new capabilities for the system to fully understand system preparedness. The bow-tie threat analysis uses the following steps, as seen in Figure 11, and each step is detailed below.

Figure 11. Bow-tie threat analysis.

1. **Identify metrics relevant for specific hazard.** For each scenario, metrics relevant to that hazard should be identified. These metrics will supplement the system metrics, which have been defined previously and provide evaluation criteria across multiple scenarios. These metrics may not be performance metrics, but rather measurements throughout the system necessary to properly understand the hazard.
2. **Identify processes and system impacted.** For the specific scenario, the relevant portions of the system should be identified. Portions of the system may include people, processes, and assets. Identification of the people, processes, and assets associated with a hazard may reveal a system vulnerability even before modeling.
3. **Model specific hazard.** Modeling the scenario may involve computer simulations, probability analyses, or test scenario procedures. Computer simulations are capable of modeling the impact of certain power system disruptions (e.g., contingency performance). Probability analyses may build on that computer simulation capability and incorporate weather and seismic activity to build survivorship models assessing asset fragility. Test scenario modeling may assess how humans, processes, technology, and infrastructure fare in a mock event.
4. **Calculate consequences.** Stakeholders should then calculate consequences of the hazard. How did the system perform against the hazard? Were the metrics identified effective in capturing those consequences? Did the system perform as expected, or were new characteristics of the system identified?
5. **Assess goal and metric performance.** Finally, for each scenario, performance should be evaluated by considering whether goals were met and whether metrics were within acceptable ranges. Stakeholders may ask themselves whether the overall goals were met. If not, do the goals need to be adjusted to be more relevant for the system? What can be improved to meet the goal?

Base Case

Each wind plant is connected to a 69 kV substation, and each substation serves one of the ethanol plants, as shown in Figure 12. The following assumptions drive our analysis of the system without any hazards.

- Lakota ethanol plant load data generated synthetically, mimicking yearly trends with average output between 6 and 7 MW
- Superior ethanol plant load data generated synthetically, mimicking yearly trends with average output between 7 and 8 MW
- Using wind plant production data (wind speed, production output, ambient temperature) from each turbine in the period June 1, 2020, 0:00 to July 21, 2021, 0:00
- Any load not served by wind turbines is imported from Corn Belt transmission system.

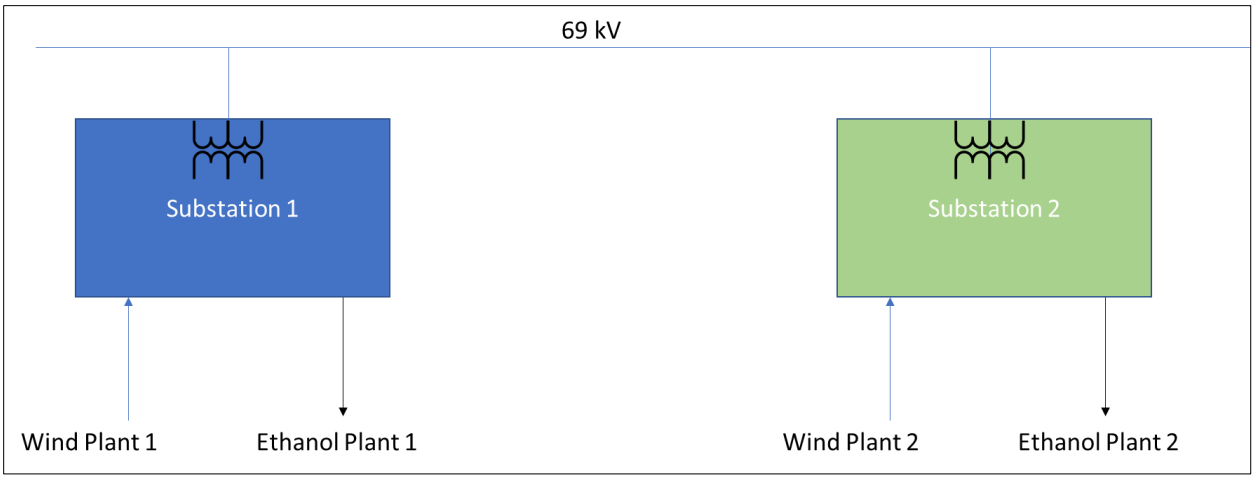

Figure 12. Substation layout.

Corn Belt OT Ransomware

Identify metrics relevant for specific hazard

Beyond the basic system metrics already identified, the metrics in Table 4 are necessary to properly evaluate a forecasted fuel shortage.

Table 4. Metrics needed for forecasted fuel shortage.

Metric	Source
Duration of Corn Belt outage	Assumption
Duration of uninterrupted power	Simulation
Percentage of time load is served during Corn Belt outage	Simulation
Load dropped during Corn Belt outage [kWh]	Simulation

Identify processes and system impacted

We consider three different outage durations caused by a ransomware attack on Corn Belt. In all outages, Corn Belt OT infrastructure is the only infrastructure affected. ILEC wind infrastructure is unaffected and can continue providing power to the local load. The first outage duration is a 10-hour outage. The ransomware does affect the Corn Belt power production, but quick incident response from Corn Belt allows them to verify that their OT systems are not infected and can be safely operated. The second is a 3-day outage. The ransomware infects parts of the data historian. Corn Belt is able to load data backups onto the servers and safely restart the system. The third is a 7-day outage. This is a more severe attack for which Corn Belt is not well prepared. With support from governmental agencies, Corn Belt pays the ransom and is able to restart their systems after a week-long halt on power production.

Without Wind

All of the load is served by the Corn Belt transmission system. The loss of Corn Belt means all power to the ethanol substations is lost. They will have to shut down or run at minimal levels with onsite backup generators.

Basic Wind

If the wind turbine inverter has basic grid-forming capabilities, the ethanol plants can be served by the immediate power output provided by the wind farms. The variability of wind may not be acceptable to the ethanol plants—they may not be able to vary their output based on the current power available—but we can still look at the power that could be provided in this case. We can also consider that in this scenario, the plants could cut their output so that only 50 or 25% of typical power is consumed.

If the load were more residential, this might be a more acceptable case. If the inverters do not have grid-forming capabilities, this is equivalent to the first scenario. All of the load would be dropped.

Advanced Wind

If there is a combined wind-storage option with advanced grid functions available, including grid-forming capabilities, then additional benefits can be provided by any wind overproduction charging the battery, and the battery helping to keep the power production constant for a period of time. The battery storage would be co-located with the wind, on the low side of the substation. We can consider multiple battery capacities. We can also consider that, in this scenario, the plants could cut their output so that only 50 or 25% of typical power consumed.

Our base case for battery storage is 32,000 kWh for each substation, which is 4 hours of storage for an 8 MW load, so it should serve each power plant for 4–6 hours with a full charge. This would cost approximately $420/kWh or $13.44 million according to estimates by PNNL [37]. We also consider 16,000 and 8,000 kWh of storage for each substation.

Model specific hazard

With the power production data that we have, we assume that the power needed as imports from Corn Belt is not served but wind operates as normal; thus, this amount is the amount of load dropped during each 10-minute interval (matching the granularity of the data). We enter a start time and end time for the Corn Belt outage. We assume that, if the battery is in place, it starts at full capacity, and begin by serving all of the load unmet by wind power with battery power until the battery is depleted. If there is wind overproduction, the excess charges the battery. We calculate the amount of time until the combined battery/wind production cannot serve the entire load. However, we assume that the plants will not fully shutdown the first time that the full demand cannot be met. We calculate the percentage of time during the Corn Belt outage that the full load is met—i.e., that there is no unmet demand. This percentage can change as we examine cases where the plants can curtail their power usage in response to the Corn Belt outage, using only 50 or 25% of their typical consumption. Finally, we calculate the unmet energy demand, in kilowatt-hours, of the plants during the Corn Belt outage.

Figure 13 shows the load lost during the example week-long outage with no battery storage. Because there is no battery, if wind does not serve the entire load, the load is dropped immediately, which is the case for this time period. However, there is a 2-day period in the middle of the week when wind fully serves the plants, so no load is dropped.

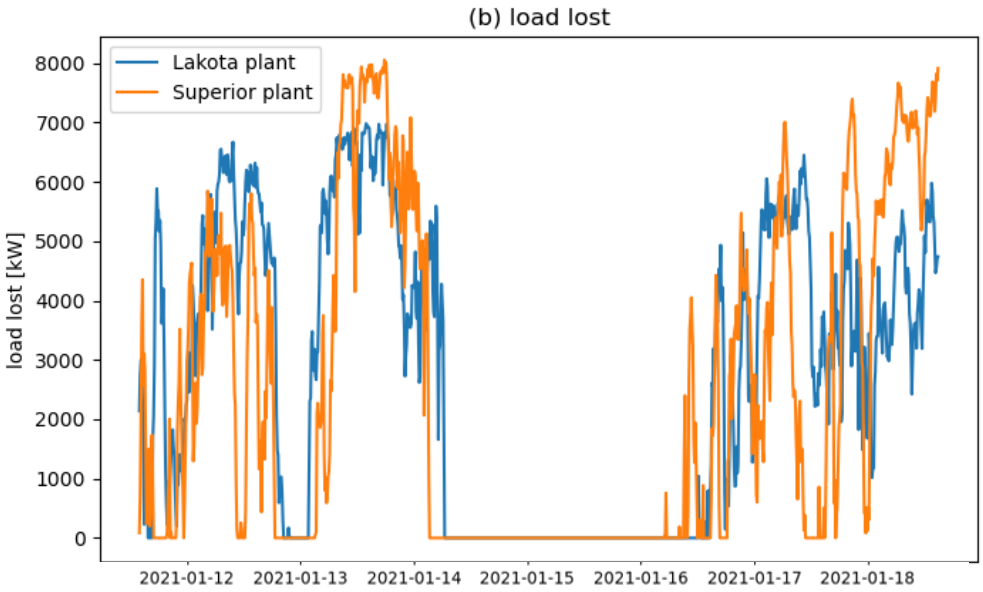

Figure 13. Week-long outage, no battery storage.

Note that for most of the time, as least some of the load is served, but over the week-long period, there is still a high degree of variability. Figure 14 shows the same outage period, but this time with 8,000 kWh of storage for each substation, which is sufficient for at least 1 hour of full load served by the battery.

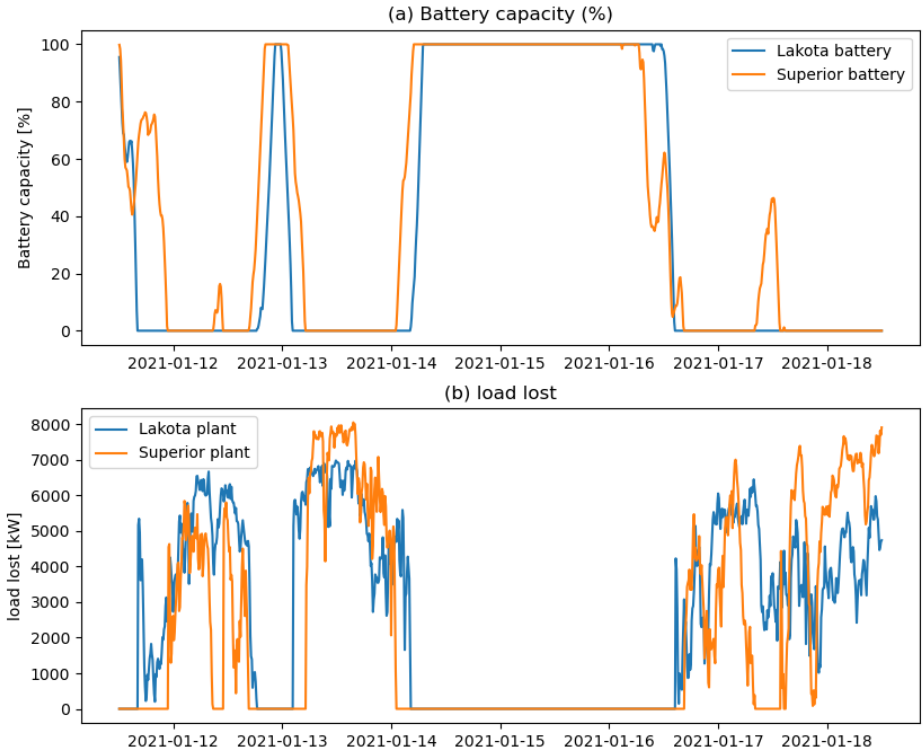

Figure 14. Example one week outage showing (a) battery capacity and (b) load lost for both substations/plants with 8,000 kWh battery storage capacity.

We can see that in Figure 14, the wind supplements the battery for about the first 6–12 hours of the outage, and no load is dropped until the battery is fully depleted. Later in the week, overproduction of wind charges the battery to full capacity, leading to extended periods of no load dropped compared to the no-storage case. In Figure 15, the battery capacity is increased to 32,000 kWh per substation, which will serve 4–6 hours of load on its own. Because of the increased capacity, it takes longer to fully discharge the batteries, again leading to longer periods of time when the load is fully served.

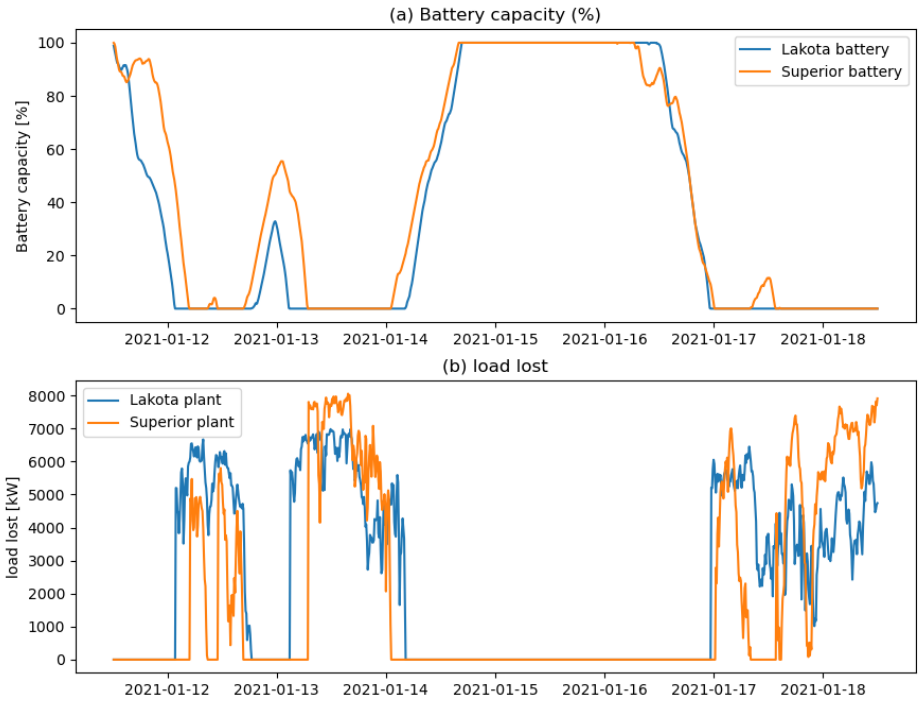

Figure 15. Example 1-week outage showing (a) battery capacity and (b) load lost for both substations/plants with 32,000 kWh battery-storage capacity.

Note that with larger battery capacity, there is a longer period of discharge to exhaust the battery's energy, but after that, the cases follow similar trends. Similarly, when wind overproduction charges the battery, the larger battery takes more time due to its larger capacity.

Calculate consequences

Without Wind

All of the load is served by the Corn Belt transmission system. The loss of Corn Belt means all power to the ethanol substations is lost. The average load lost (taken as a rolling average throughout the year) is shown in Table 5.

Table 5. Load lost with no wind.

Duration of outage	Lakota substation (load lost) [kWh]	Superior substation (load lost) [kWh]
10 hours	65,921	75,925
3 days	474,554	546,584
7 days	1,107,041	1,275,117

Basic Wind

This scenario, called "no storage," assumes grid-forming wind inverters, and assumes ethanol plants can tolerate variability, otherwise results will match without-wind scenario. Results are shown in Table 6, broken down by Corn Belt outage duration, and percentage of full power output demanded by the ethanol plants. Each result presented is the average of trials conducted every 4 weeks throughout the year of data.

Table 6. Results with no storage.

	Lakota			Superior		
Duration of outage	Time until load lost (avg). [hr]	Percentage of outage when load is served (avg.) [%]	Total load lost (avg.) [kWh]	Time until load lost (avg). [hr]	Percentage of outage when load is served (avg.) [%]	Total load lost (avg.) [kWh]
100% Load						
10 hours	1.94	31.90%	30,383	1.65	28.57%	34,753
3 days	1.94	27.81%	234,635	1.65	26.11%	263,487
7 days	1.94	26.12%	564,901	1.65	23.57%	661,607
50% Load						
10 hours	3.26	54.29%	11,692	2.60	54.40%	12,040
3 days	4.67	47.19%	84,031	3.13	47.19%	88,355
7 days	4.67	45.83%	204,464	3.13	44.42%	232,390
25% Load						
10 hours	4.67	60.95%	4,702	5.17	66.67%	4,677
3 days	7.86	63.03%	29,738	7.18	66.39%	29,433
7 days	7.86	61.48%	74,443	7.18	62.50%	81,343

Load is dropped in every case, but overall, the percentage of the outage when the load is fully served increases for longer durations, which seems counterintuitive. This may be in part due to the time intervals that were chosen, and it may be indicative that wind overall can provide for over 50% of the load, especially as that is averaged over longer periods of time.

Advanced Wind

Each result presented is the average of trials conducted every 4 weeks throughout the year of data. Table 7 shows results with an assumed storage capacity of 32,000 kWh for each ethanol plant, which is sufficient to supply approximately 4 hours of energy to the plants.

Table 7. Results with 32,000 kWh storage.

	Lakota			Superior		
Duration of outage	Time until load lost (avg). [hr]	Percentage of outage when load is served (avg.) [%]	Total load lost (avg.) [kWh]	Time until load lost (avg). [hr]	Percentage of outage when load is served (avg.) [%]	Total load lost (avg.) [kWh]
	100% Load					
10 hours	8.04	83.69%	9,421	8.12	82.86%	11,364
3 days	13.82	47.98%	185,812	14.37	46,54%	210,997
7 days	13.82	41.23%	487,652	14.37	37.41%	586,043
	50% Load					
10 hours	10	100%	0	9.83	98.33%	560
3 days	42.02	79.68%	34,628	39.82	78.80%	39,627
7 days	49.77	74.48%	107,735	41.88	69.67%	141,013

	Lakota			Superior		
Duration of outage	Time until load lost (avg). [hr]	Percentage of outage when load is served (avg.) [%]	Total load lost (avg.) [kWh]	Time until load lost (avg). [hr]	Percentage of outage when load is served (avg.) [%]	Total load lost (avg.) [kWh]
	25% Load					
10 hours	10	100%	0	10	100%	0
3 days	66.83	97.78%	1,948	69.27	97.93%	1,862
7 days	122.77	93.33%	16,325	134.36	93.03%	18,650

For the 10-hour outage, the combination of high battery storage capacity and wind means that the load can be fully served for the duration of the Corn Belt outage. This is especially true as the load decreases, but a very high load is served even when the load is at 100%, and it is served constantly for almost 9 hours.

Next, we consider what happens if the storage capacity is lower. Specifically, we consider battery storage sized for approximately 2 hours, with 1 hour of energy provided to each ethanol plant. These results are shown in Table 8.

Table 8. Results with 16,000 kWh storage.

	Lakota			Superior		
Duration of outage	Time until load lost (avg). [hr]	Percentage of outage when load is served (avg.) [%]	Total load lost (avg.) [kWh]	Time until load lost (avg). [hr]	Percentage of outage when load is served (avg.) [%]	Total load lost (avg.) [kWh]
	100% Load					
10 hours	6.23	67.14%	17,990	5.93	64.76%	20,108
3 days	9.42	42.29%	205,237	7.05	40.29%	232,075
7 days	9.42	37.92%	514,311	7.05	33.91%	613,899
	50% Load					
10 hours	8.5	86.90%	3,889	8.55	85.48%	4,925
3 days	25.94	71.18%	51,765	30.36	71.83%	55,715
7 days	26.07	67.41%	140,556	30.36	63.51%	172,423
	25% Load					
10 hours	10	100%	0	9.85	98.45%	247
3 days	51.15	91.35%	7,950	53.34	92.89%	6,698
7 days	76.15	87.51%	29,207	74.26	87.74%	31,128

The lower storage capacity has a noticeable impact on performance, but the system still performs well for reduced loads and shorter durations. Finally, we reduce the storage capacity to 8,000 kWh for each substation, which is sized for approximately 1 hour of service to each plant. These results are shown in Table 9.

Table 9. Results with 8,000 kWh storage.

	Lakota			Superior		
Duration of outage	Time until load lost (avg). [hr]	Percentage of outage when load is served (avg.) [%]	Total load lost (avg.) [kWh]	Time until load lost (avg). [hr]	Percentage of outage when load is served (avg.) [%]	Total load lost (avg.) [kWh]
100% Load						
10 hours	4.83	54.64%	23,087	4.42	52.26%	26,569
3 days	6.57	38.69%	216,108	5.08	36.19%	244,411
7 days	6.57	35.20%	531,454	5.08	31.39%	630,740
50% Load						
10 hours	6.95	74.88%	7,069	7.32	77.14%	7,570
3 days	14.05	64.43%	63,656	20.26	66.15%	67,029
7 days	14.05	61.28%	164,426	20.26	58.90%	192,861
25% Load						
10 hours	9.17	91.67%	1,334	8.79	87.86%	1,913
3 days	38.26	85.83%	13,979	27.80	86.13%	13,837
7 days	40.43	82.04%	42,868	39.89	81.13%	47,532

Again, we notice that performance decreases as storage capacity drops. Load is first dropped sooner, and more load is dropped overall.

Summary

Although the ethanol plants have slightly different loads, the overall results are similar, so we choose to plot only the Lakota substation results for the following graphs, which summarize the data. First, we examine the time until any load is first dropped in Figure 16. This is especially important for this system, because the ethanol plants may not be able to tolerate the variability in available power. This metric may represent the time that the plants remain operational if they choose to fully shut down after their load (or reduced load) can no longer be fully served.

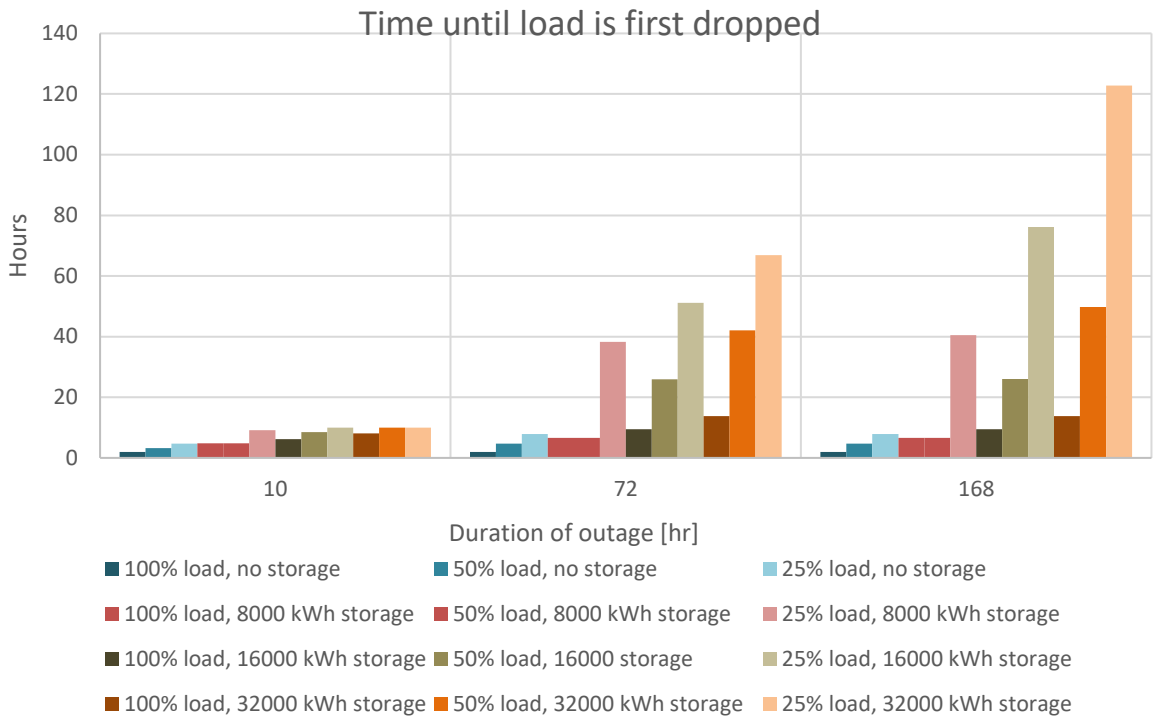

Figure 16. Summary of cases: time until load is first dropped.

We can see that the results of time until load is first dropped change more based on the percentage load that is used, as opposed to the change in storage capacity.

Figure 17 shows the percentage of the outage duration where the load (or reduced load) is fully served. If the ethanol plants can tolerate multiple startups and shutdowns in a short duration, then this metric represents the maximum output that the plants can have during the outage—i.e., even after the storage capacity first runs out, increased wind production later in the outage can serve load directly or recharge the battery.

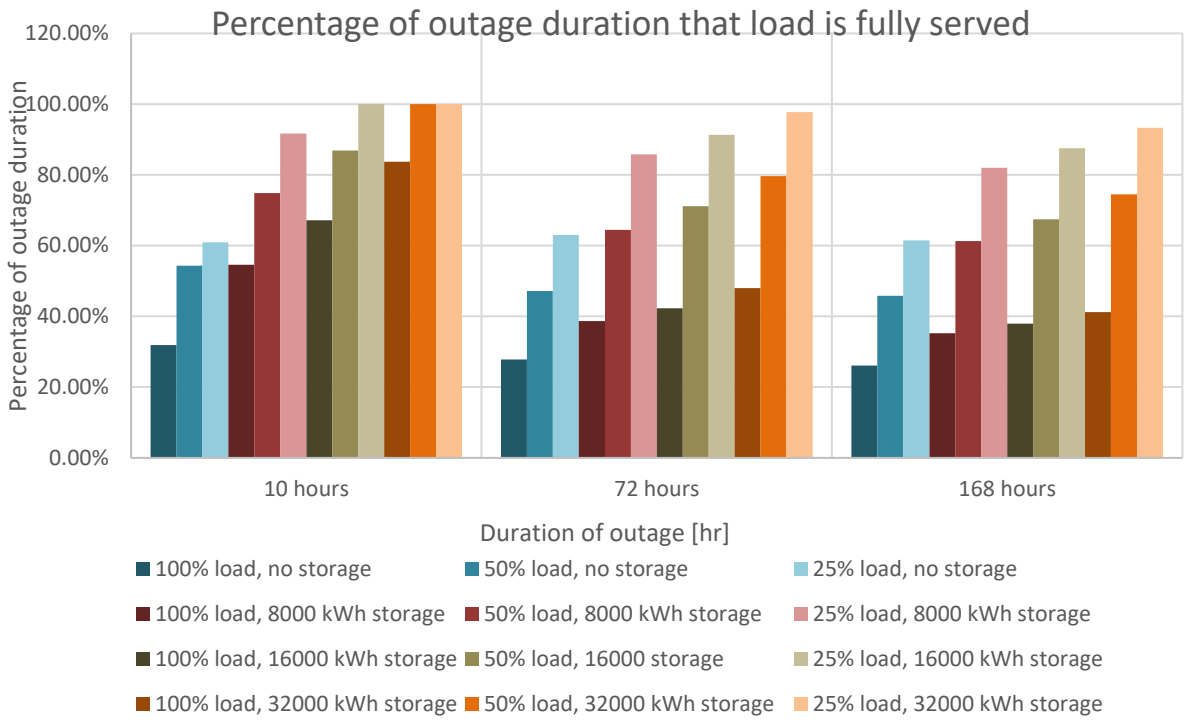

Figure 17. Summary of cases: percentage of time when load is fully served.

Changing the storage capacity has a more dramatic effect on the percentage of time that load is served than changing the load for a short duration outage, but changing the load is the most effective mitigation measure for all outage durations. Again, we can see that adjusting the load via demand-response measures has a greater impact on the ability of the system to serve the load than additional storage capacity. This trend is even more pronounced for the dropped load analysis in Figure 18, which makes sense because this is the variable most directly correlated to the adjusted demand.

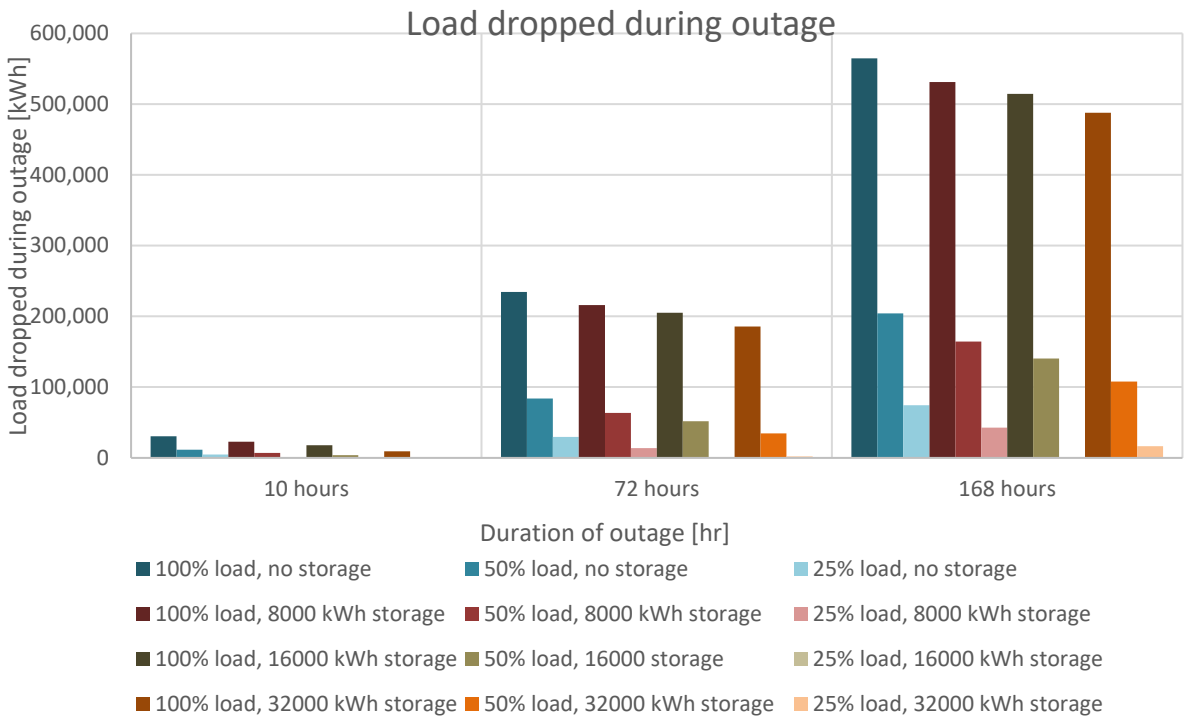

Figure 18. Summary of cases: percentage of time when varying load is fully served with different storage capacities.

Assess goal and metric performance

In response to the Corn Belt OT ransomware attack, ILEC wind provides some power to the ethanol plants. Wind and storage combined can keep full power supplied to the plants for longer durations and with less variability. Increased storage provides increased capability of the system to serve a constant load at the plants for a longer duration. Additional measures that decrease variability in load served include curtailing ethanol plant output so that they use 50 or 25% of their normal power. If it is feasible to run at these lower power levels, they can prevent a full plant shutdown, which can be costly and difficult to restart.

Table 10. Metrics towards evaluating renewable production.

Metric	Performance without wind	Performance with wind
Wind production	0	ILEC data request
Imported generation	Synthetic data, scaled if necessary	Synthetic data, scaled if necessary

Table 11. Outage duration.

Metric	Performance without wind	Performance with wind
Outage duration	See Table 5	See Table 6–Table 9

ILEC IT Ransomware

Identify metrics relevant for specific hazard

Beyond the basic system metrics already identified, the following metrics are necessary to properly evaluate a ransomware attack on the IT systems of ILEC.

Table 12. Metrics needed to evaluate ILEC IT ransomware attack.

Metric	Source
Duration of ransomware attack	Assumption
Number and type of systems affected	Assumption
Customer impact	Open-source research
Long-term impacts	Open-source research

Identify processes and system impacted

When ransomware infects a local utility, it is common for the attack to interfere with business operations. This often includes public-facing websites, billing systems, and internal email servers. If firewalls and demilitarized zones (DMZs) are properly implemented, IT ransomware may not affect OT systems, including control rooms, power system hardware, or networks connecting the two.

Model specific hazard

Without more specific information about the company's internal networks and server infrastructure, it is difficult to perform a detailed simulation analysis as we have done with the cases that affect power system operation. In this section, we discuss common attack paths and outcomes of ransomware that affect the business infrastructure for an electric utility.

The most common points of origin for ransomware include phishing, exploits of known vulnerabilities, and unintentional backdoors left open. An example of the last type is the Colonial pipeline hack, which took advantage of a virtual desktop application accidentally left running. It also used spearphishing techniques to get the password necessary to access the virtual desktop. Two-factor authentication was not used for the application.

After ransomware has infected one computer in a system, it uses automated techniques to spread throughout the network, and may intelligently search for critical applications or data before executing the payload. When the payload is executed, ransomware traditionally encrypts all of the files it has access to and sends a message to the company demanding payment in return for access to the decryption key. Although there may be a concern that the decryption key will not be delivered on payment, it is poor business for ransomware hackers not to provide this key. If there is not trust that the key will be received upon payment, fewer victims will pay. Not all victims will pay the attackers. Some companies may use internal professionals or external consultants to try to break down the malware and recover the files without getting the decryption key from the attackers. Depending on what data were compromised, some companies may also be able to restore the system and files using backups stored in a secure location, potentially only losing changes made since the last backup.

More recently, ransomware attackers have not just encrypted the files they have access to, but also extracted that data prior to encrypting it. They attempt to further motivate victims to pay the ransom rather than remove the encryption themselves by threatening to publish or sell sensitive data that was extracted. This can be especially damaging for utilities. If customer information is compromised, they may have mandatory data breach reporting requirements, which are damaging to reputations. Customer data breaches may also require payment for identity theft tracking services for those affected. Additionally, if data describing the power system is extracted, this could potentially be used by bad actors to mount more targeted and damaging attacks against the utility.

As discussed previously, one of the common effects of ransomware on utilities is interference with customer-facing services, including websites and bill paying services. Typically, in this situation, utilities suspend shut offs and late fees until the payment infrastructure is restored. This could affect the short-term finances for the utility, as most customers will wait until the electronic infrastructure is restored rather than paying by cash or check. It may also negatively affect customers' views of the utility, but effects from the loss of the bill-paying structure may not be long term.

Beyond customer interactions, it may be difficult to conduct other regular business operations for the extent of the ransomware attack.

Calculate consequences

Consequences will be highly dependent on the strain of ransomware, the defenses, network segmentation, employee training, and response ability of ILEC. Potential consequences were discussed in the previous section. The most important takeaways are the assumptions that the ransomware is limited to enterprise systems and does not compromise the OT network. However, utilities must be aware of the potential long-term impacts of this type of attack.

Assess goal and metric performance

We assume that the IT ransomware does not affect the immediate ability to operate the power system. There is no change in power production or distribution during the attack.

Using the metrics deemed most important for resilience early in the framework, this hazard does not pose a huge threat to resilience, and having distributed wind does not affect the resilience of the system under this hazard.

Table 13. Metrics toward evaluating renewable production.

Metric	Performance without wind	Performance with wind
Wind production	0	ILEC data request
Imported generation	Synthetic data, scaled if necessary	Synthetic data, scaled if necessary

Table 14. Outage duration.

Metric	Performance without wind	Performance with wind
Outage duration	None	None

ILEC OT Ransomware

Identify metrics relevant for specific hazard.

Beyond the basic system metrics already identified, the metrics listed in Table 15 are necessary to properly evaluate a ransomware attack that affects ILEC OT.

Table 15. Metrics needed to evaluate ILEC OT ransomware.

Metric	Source
Duration of attack	Assumption
Systems affected	Assumption
Load lost	Calculation
Power imports	Calculation

Identify processes and system impacted

For the purposes of this analysis, we assume that the ransomware attack does affect the Superior and Lakota wind turbines. The turbines may be the source of the attack, or they may be affected by propagating ransomware that originated elsewhere in the system.

Model specific hazard

We consider two cases here: one in which the turbines are the source of the attack and one in which the turbines are affected by ransomware that originated elsewhere in the system. As with the previous case, we discuss potential attack paths and outcomes, but without knowing more about the communications infrastructure, defenses and segmentation, and many assumptions, we cannot say with any amount of confidence what the most likely outcome would be.

Wind turbines as point-of-entry

One of the unique characteristics of distributed wind systems is their physical isolation. Wind turbines in general are often installed where the resource capacity is greatest, which may be in remote locations. Because of this, remote connectivity is needed for monitoring and control and is relied on more than a typical generation asset, where control centers may be onsite. If these remote access points are not properly secured, they can provide entry for an adversary into the system.

Since turbines tend to be located remotely and not visited often, it is possible that an adversary could physically access the turbine itself and use local access points at the turbine to load malware into the system. This malware could then propagate to the substations and back to the main control room in the worst case, or even just compromise the local hardware.

Another possibility is that a technicians or other service persons could accidentally infect their own machine, then compromise the wind turbine when they are servicing the machine. This exact scenario has happened, not with ransomware, but with other malware that caused turbines at a wind farm to stop working one by one [32].

Finally, turbine communications could be compromised directly if they are not properly secured. In a brief search by Forbes, 50 wind and solar machines with known vulnerabilities were found using Shodan, a search engine for Internet-connected devices [38]. These devices were found over six years ago, and while general security practices may have improved since then, the number of turbines installed is growing very rapidly, and there are no requirements readily available to installers or integrators to prevent this kind of access.

After ransomware compromises the turbines, it is likely that the turbines themselves will be shut down. It is possible that the ransomware could spread to the substations, potentially locking systems there, and in the worst case, shutting down the connection to Corn Belt.

The ransomware may spread even further into ILEC systems, potentially compromising more OT devices across their system or working its way into the enterprise system.

Wind Turbines Compromised after Alternate Point-of-Entry

Although we want to highlight the threat of ransomware infecting a system via the distributed wind turbines, this is not the only way that ransomware could affect the OT system of ILEC. Similar methods of entry could be used at other points in the system, and the ransomware could spread, eventually affecting the turbines. The effects on the power system, particularly on the Lakota and Superior turbines, may be similar. However, the different attack paths may need different mitigations to best ensure resilience against this hazard.

Calculate consequences

As discussed previously, ransomware could have a direct and limited effect on the wind turbines only. In this case, all power needed to serve the ethanol plants load could be imported from Corn Belt. There may be increased costs to ILEC compared to the base case, but there would be no load lost.

It is also possible that the ransomware could affect the substations as well. If the breakers have a fail-open condition, power from Corn Belt may be cut in addition to the wind turbines being compromised. In this case, all power sources for the ethanol plants are lost, and the load is dropped. Table 16 shows the average amount of energy consumed by each substation over different durations. This is the amount of load that would need to be imported from Corn Belt, if available, or that would be dropped.

Table 16. Average energy consumed at each substation.

Duration of outage	Lakota substation [kWh]	Superior substation [kWh]
10 hours	65,921	75,925
3 days	474,554	546,584
7 days	1,107,041	1,275,117

Assess Goal and Metric Performance

In response to the ILEC OT ransomware, the system may still be able to serve the two ethanol plants if the Lakota and Superior substations are not substantially compromised. In this case, although wind production may be halted, sufficient power may be imported from Corn Belt. Alternatively, if the substation is compromised and breakers are flipped, then the ethanol plants may be cut off from any production sources, in which case all the load from the ethanol plants will be dropped. In either case, the wind asset does not add any resilience through properties of its power production (Table 17). If anything, it is possible that the wind turbines could be used to help compromise the system, in which case the turbines are a vulnerability rather than a mitigation toward the ransomware hazard. In addition to the immediate power system effects, ILEC needs to consider the long-term impacts similar to the IT ransomware (Table 18).

Table 17. Metrics toward evaluating renewable production.

Metric	Performance without wind	Performance with wind
Wind production	0	0
Imported generation	Synthetic load data	Synthetic load data

Table 18. Outage duration.

Metric	Performance without wind	Performance with wind
Outage duration	None (or all)	None (or all)

DoS Attack

Identify metrics relevant for specific hazard.

Beyond the basic system metrics already identified, the metrics listed in Table 19 are necessary to properly evaluate a DoS attack

Table 19. Metrics needed to evaluate a DoS attack.

Metric	Source
Duration of attack	Assumption
Systems affected	Assumption
Customer impact	Open-source research

Identify processes and system impacted.

We assume that the DoS attack affects equipment that is between the wind turbine and the ILEC control center. This hazard is modeled on the attack that affected a firewall at Salt Lake City-based sPower [34]. However, this hazard could affect equipment other than firewalls. Although the sPower attack is one of the most notable because of its direct effect on operations, NETSCOUT, which maintains the Cyber Threat Horizon tracker in real time, recorded 1,780 distributed denial-of-service (DDoS) attacks against utilities worldwide between June 15 and August 21, representing a 595% year-over-year increase [39]. This is an unprecedented increase in DDoS attacks. In addition to the increase in frequency of attacks, the DDoS attacks are coming at higher speeds, with over four times as many packets being sent in the same amount of time.

Model specific hazard

Traditionally, DoS attacks send repeated packets to a device at high speeds with the goal of filling up all the available ports so that legitimate traffic cannot get in. However, many devices have basic DoS protection built in. When the device notices excess packets coming in from an unknown source, or even a known source if the Internet protocol (IP) is spoofed, then it may block that IP or drop packets from that source for a period of time. DDoS attacks are more advanced because the attacker spoofs many different IPs, so that the attack does not appear to be coming from a single source. This can trick many filters looking for attacks coming from a single source.

However, even a next-generation firewall that claims to have DoS protection built in cannot deal with all types of attacks. The fact is, firewalls just are not able to handle volumetric DDoS attacks. At best, a firewall may overload, freeze, and shut off all inbound traffic—including good customer traffic along with the bad attack traffic. At worst, a firewall may go into bypass mode and allow all traffic, good and bad, to flow. This puts the rest of the IT infrastructure, as well as its data, at risk [40].

An additional component to consider for DoS attacks is that the barrier to entry is low. It is not difficult to configure a program to send packets to a target at high speed. Slightly more advanced attacks will use botnets to increase the volume of packets send to a target during an attack, but even these attacks are widely available for purchase. This means anyone from hacktivists, to cybercriminals, to nation states may use DoS attacks.

A DoS or DDoS attack may hit different parts of the ILEC infrastructure. It can impact the IT networks, taking out websites, payment infrastructure, or internal networks. In this case, the attack acts

somewhat like the ILEC IT ransomware, but with less threat of the information being extracted and no ransom demanded. Like the sPower attack, the attack may also impact the OT infrastructure. In the best case, this could just limit operators' ability to receive data from the system, blocking their visibility. In the worst case, the DDoS attack could affect infrastructure, like switches, critical to the automated control and communication of the system. The physical power lines will not be affected, but if data cannot be shared throughout the system, no changes to settings may be made. This could affect the ability of the wind turbines to properly curtail their output or to provide ancillary services.

Calculate consequences

IT infrastructure is typically better protected against DoS and DDoS attacks, making it less likely that ILEC would be impacted by this type of attack. The most likely place where an IT DoS attack would have an impact is on a public-facing website, which may include payment systems.

A DoS attack on OT infrastructure that just blocks visibility into the system would have limited impacts, although it reveals the vulnerability of power systems to attacks and the importance of making sure devices are not publicly accessible. Instead, they should be hidden behind virtual networks and only accept traffic from known sources.

In the worst case, a DoS attack could impact the control and communications infrastructure of the automated power system. Some devices might have failsafe mechanisms that turn them off if communications are lost, and this could include the wind turbines.

DDoS threats are constantly evolving, and many hackers now use them as a smokescreen to launch a more sophisticated attack. They may be designed to knock a firewall or intrusion-prevention system (IPS) offline, opening the system to the delivery of more sophisticated malware or exfiltration of corporate data. Given that most companies now take more than 190 days to detect a data breach on their networks, this can give attackers a significant head start for their exploits. Application-layer and DNS based DDoS attacks can also cause significant outages and may go undetected by security staff and mitigation devices [41].

Assess goal and metric performance

In a DoS or DDoS attack, there may not be an immediate effect on the power system performance, but in the worst case, wind assets could shut down if the communication is blocked as a failsafe mechanism (Table 20 and Table 21).

Table 20. Metrics toward evaluating renewable production.

Metric	Performance without wind	Performance with wind
Wind production	0	ILEC data request
Imported generation	Synthetic data, scaled if necessary	Synthetic data, scaled if necessary

Table 21. Outage duration.

Metric	Performance without wind	Performance with wind
Outage duration	None	None

Prioritize Risk-Mitigation Measures

Based on the outcomes of the modeling, risk-mitigation measures should be prioritized. A single risk may have multiple mitigation options, and those options themselves may mitigate multiple risks. Risk-mitigation measures should include cost estimations and effectiveness metrics that evaluate the efficacy of a mitigation measure against a given risk. Return-on-investment (ROI) metrics should be calculated.

Mitigations against Hazard 1 (Corn Belt Ransomware) include:

- Ensure network segmentation in substations connected to Corn Belt
- Ensure wind-storage hybrid system is appropriately sized to support loads.

Hazard 2 (ILEC IT Ransomware) mitigations include:

- Segment enterprise networks
- Use two-factor authentication, especially on any remote access applications
- Require mandatory employee phishing training and testing
- Install DMZs where appropriate.

For Hazard 3 (ILEC OT Ransomware), the following ameliorations might be considered:

- Install backup generation for ethanol plants
- Create security plans for third parties, including maintainers and technicians
- Confirm fail safe operations are enabled and programmed correctly.

Mitigations against Hazard 4 (DoS Attack) would include:

- Ensure communications devices are not publicly searchable
- Install filters on all firewalls (easy to detect DoS and DDoS attacks)
- Use VPNs where appropriate
- Active and regular patching.

Evaluate Against All Business Risks

Once analysis shows how a hazard will impact the system, the system risks should be evaluated within the context of the broader business activities. Each risk and impact should be weighed against others. If there is a limited budget, it may be that only one of these projects can move forward. Ultimately, the goal is to enable decision-makers to improve system resilience over time. Decision-makers take the prioritized resilience measures and determine what can be done with regard to other business constraints (i.e., resources, budget, and feasibility).

This step allows a detailed cost-effectiveness analysis to occur. Financial tradeoffs are associated with many measures that will add resiliency. By evaluating the risk of a disruptive event against all other business risks, such as economic viability, public relations, or fines if proper cybersecurity measures are not taken, stakeholders can determine how much relative risk they are willing to assume.

Implement Changes and Operate System

This step includes reassessing the planning stage again to model system improvements to understand new system characteristics, ensure that the goals and metrics are still appropriate, and prioritize any additional measures that should be implemented. The recursive quality of planning will help to track resilience of the system over time, but also safeguard against resilience degradation. A resilient system does not necessarily stay that way over time: risks shift, assets age, and people change.

This step also includes transitioning to the operational stage of resilience. As plans are made to improve resilience, these plans should be executed by making changes in the operational space. This should include implementation across processes, equipment, design standards, or labor resources. The transition may occur on different time scales. Some changes can be implemented immediately; others will require a longer construction or roll-out period.

CONCLUSIONS

In this case study, we stepped through the planning stage of the INL resilience framework in detail with the goal of showing the resilience benefits and considerations of the ILEC distributed wind systems. We found that the local proximity of distributed wind to load centers alone provided a degree of resilience against a proposed ransomware hazard that affected the connected transmission provider. Although it does not represent the current state of the system, we evaluated the potential enhanced resilience benefits if the system included storage and demand response capabilities. These capabilities in particular were evaluated because of the resilience considerations for the end-use customer, two chemical plants that could not tolerate the high variability of wind resource generation alone.

Key takeaways:

- Hazards do not have to affect the system directly in order to be a resilience consideration. In this case, the ransomware attack did not directly affect ILEC, but instead shut down capabilities of the transmission provider, which still had a meaningful effect on the ILEC system.
- Key stakeholder input is critical to properly evaluating resilience benefits. For some customers, like agricultural or even residential, rolling short term blackouts may be acceptable. For the chemical plant customer in this case study, rolling blackouts would not be acceptable because of the cost, difficulty, and time required to perform start ups and shut downs of the plant.
- Cybersecurity hazards are difficult to model, because it is hard to predict exactly how they will manifest. However, it is possible to assign conditions to evaluate potential worst case scenarios, and it is also possible to perform a less intense walkthrough of the resilience framework and evaluate some hazards more qualitatively than quantitatively. While this may not produce metrics and values in the same way, it is still a useful exercise for thinking about possible hazards and mitigations.
- Cybersecurity hazards can have a real impact on power system operation. While IT systems are more traditionally targeted by cyberattacks, OT systems are vulnerable to both targeted and untargeted attacks. This is evidenced by many theoretical and real-world incidents.
- Storage and advanced controls (demand response) were found to have a very positive impact on the resilience benefits of the system when combined with the distributed wind generation source.
- Higher storage capacity generally leads to higher resilience benefits, however, there are diminishing returns associated with increasing the capacity. This is in part due to the size and variability of the charging resource (the distributed wind plants). No matter the storage capacity, if there is more energy produced by the wind than there is consumed by the load, then the battery will not charge. The biggest benefit of the larger storage capacity was seen when it was able to reach a full charge, thus providing power for a longer period of time as it discharged.

REFERENCES

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

[4] *U.S. Presidential Policy Directive 21,* 2013.

[5] M. J. Culler, S. A. Bukowski, K. A. Hovland, S. Morash, A. F. Snyder, N. Pacer and J. P. Gentle, "Resilience Framework for Electric Energy Delivery Systems," Idaho National Laboratory, Idaho Falls, ID, 2021. Forthcoming.

[6] J. Reily, A. Orrell, B. Naughton and J. Gentle, "MIRACL Reference Systems and Q4 Technical Report Summary," National Renewable Energy Laboratory, Golden, CO, 2020.

[7] S. A. Bukowski, M. J. Culler, J. P. Gentle, J. C. Bell, C. R. Riger and E. Bukowski, "Distributed Wind Resilience Metrics for Electic Energy Delivery Systems: Comprehensive Literature Review," Idaho National Laboratory, Idaho Falls, ID, 2021.

[8] National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity," National Institute of Standards and Technology, 2018.

[9] National Rural Electic Cooperative Association (NRECA), "Distributed Wind Case Study: Iowa Lakes Electric Cooperative," NRECA Research, 2021.

[10] American Clean Power Association, "Clean Power Iowa," American Clean Power Association, Washington, DC, 2021.

[11] U.S. Energy Information Administration, "Iowa State Profile and Energy Estimates Analysis," U.S. Energy Information Administration, 17 June 2021. [Online]. Available: https://www.eia.gov/state/analysis.php?sid=IA. [Accessed 14 July 2021].

[12] S. Provus, "CDFA Spotlight: Overview of Clean Renewable Energy Bonds (CREBs)," Council of Development Finance Agencies, [Online]. Available: https://www.cdfa.net/cdfa/cdfaweb.nsf/0/07C139CF31F69946882579360063E011.

[13] *Iowa Chapter 476B Wind Energy Production Tax Credit.*

[14] T. Hussong, *2011 Wind Cooperative of the Year Award,* Estherville, IA: Iowa Lakes Electric Cooperative, 2012.

[15] GE Energy, "1.5 MW Wind Turbine," GE Energy, 2009.

[16] NC Clean Energy Technology Center DSIRE, "Alternative Energy Law (AEL)," NC State Universtiy, June 2018. [Online]. Available: https://programs.dsireusa.org/system/program/detail/265.

[17] Iowa Environmental Council, "Iowa's Road to 100% Renewable," Iowa Environmental Council, Des Moines, IA, 2020.

[18] The White House, "Executive Order on Tackling the Climate Crisis at Home and Abroad," The White House, 27 January 2021. [Online]. Available: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/01/27/executive-order-on-tackling-the-climate-crisis-at-home-and-abroad/. [Accessed 10 August 2021].

[19] North American Electric Reliability Corporation, "Definition of "Adequate Level of Reliability"," North American Electric Reliability Corporation, Princeton, NJ, 2007.

[20] U.S. Department of Energy Office of Energy Efficiency and Renewable Energy (EERE), "Roadmap for Wind Cybersecurity," U.S. Department of Energy Office of Energy Efficiency and Renewable Energy (EERE), Washington, DC, 2020.

[21] Cybersecurity and Infrastructure Security Agency, "Rising Ransomware Threat to Operational Technology Assets," Cybersecurity and Infrastructure Security Agency, Washington, DC, 2021.

[22] R. Walton, "Utilities face growing ransomware threat as hackers improve strategy, execution," UtilityDive, 26 August 202. [Online]. Available: https://www.utilitydive.com/news/utilities-face-growing-ransomware-threat-as-hackers-improve-strategy-execu/583818/. [Accessed 5 August 2021].

[23] T. Seals, "Ransomware Attacks Hit Major Utilities," Threat Post, 5 February 2021. [Online]. Available: https://threatpost.com/ransomware-attacks-major-utilities/163687/. [Accessed 5 August 2021].

[24] W. Turton and K. Mehrotra, "Hakcers Breached Colonial Pipeline Using Compromised Password," Bloomberg, 4 June 2021. [Online]. Available: https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password. [Accessed 5 August 2021].

[25] J. Fruhlinger, "Ransomware explained: How it works and how to remove it," CSO Online, 19 June 2020. [Online]. Available: https://www.csoonline.com/article/3236183/what-is-ransomware-how-it-works-and-how-to-remove-it.html. [Accessed 5 August 2021].

[26] Cybersecurity & Infrastructure Security Agency, "Securtiy Tip (ST08-001) Using Caution with USB Drives," Department of Homeland Security, 15 November 2019. [Online]. Available: https://us-cert.cisa.gov/ncas/tips/ST08-001. [Accessed 5 August 2021].

[27] M. Genet, "Independence still sorting out 'ransomware' attack," The Examiner, 14 December 2020. [Online]. Available: https://www.examiner.net/story/news/2020/12/14/cybersecurity-independence-missouri-ransomware/6544587002/. [Accessed 5 August 2021].

[28] The Associated Press, "Ransomware attack strikes rural Alabama utility service," AL.com, 6 July 2021. [Online]. Available: https://www.al.com/news/2021/07/ransomware-attack-strikes-rural-alabama-utility-service.html. [Accessed 5 August 2021].

[29] A. Zabetian-Hosseini, A. Mehrizi-Sani and C.-C. Liu, "Cyberattack to Cyber-Physical Model of Wind Farm SCADA," in *44th Annual Conference of the IEEE Industrial Electronics Society*, Washington, DC, 2018.

[30] J. Staggs, D. Ferlemann and S. Shenoi., "Wind Farm Security: Attack Surface, Targets, Scenarios and Mitigation," *International Journal of Critical Infrastructure Protection,* vol. 17, pp. 3-14, 2017.

[31] J. Yan, C.-C. Liu and M. Govindarasu., "Cyber Intrusion of Wind Farm SCADA System and Its Impact Analysis," in *2011 IEEE/PES Power Systems Conference and Exposition*, Phoenix, AZ, 2011.

[32] R. Davidson, "AWEA 2018: Increase in cyber security attacks 'inevitable', expert warns," Wind Power Monthly, 2018 8 May. [Online]. Available: https://www.windpowermonthly.com/article/1464061/awea-2018-increase-cyber-security-attacks-inevitable-expert-warns. [Accessed 9 August 2021].

[33] Interview by Jack Rysider, "Episode 22: Mini Sotries: Vol 1," Darknet Diaries (audio blog), 15 September 2018. [Online]. Available: https://darknetdiaries.com/episode/22/..

[34] B. Sobczak, "First-of-a-kind U.S. grid cyberattack hit wind, solar," E&E News, Politico Pro, 31 October` 2019. [Online]. Available: https://subscriber.politicopro.com/article/eenews/1061421301.

[35] S. Lyngaas, "Utah renewables compnay was hit by rare cyberattack in March," CyberScoop, 31 October 2019. [Online]. Available: https://www.cyberscoop.com/spower-power-grid-cyberattack-foia/.

[36] M. Korolov, "Telephonic DoS a smokescreen for cyberattack on Ukrainian utility," CSO Online, 25 January 2016. [Online]. Available: https://www.csoonline.com/article/3025798/telephonic-dos-a-smokescreen-for-cyberattack-on-ukrainian-utility.html.

[37] K. Mongird, V. Viswanathan, J. Alam, C. Vartanian, V. Sprenkle and R. Baxter, "2020 Grid Energy Storage Technology Cost and Performance Assessmetn," U.S. Department of Energy, 2020.

[38] T. Brewster, "Hundreds Of Wind Turbines And Solar Systems Wide Open To Easy Exploits," Forbes, 2015 12 June. [Online]. Available: https://www.forbes.com/sites/thomasbrewster/2015/06/12/hacking-wind-solar-systems-is-easy/. [Accessed 9 August 2021].

[39] L. M. Jenkins, "Worldwide Denial-of-Service Cyberattacks on Utilities Up Seven-Fold This Summer, Data Shows," Morning Consult, 27 August 2020. [Online]. Available: https://morningconsult.com/2020/08/27/cyber-attacks-gas-electric-utilities-data/. [Accessed 2021 August 2021].

[40] S. Newman, "Lessons Learned from a DoS Attack Against a U.S. Power Utility," Coreo, 24 September 2019. [Online]. Available: https://www.corero.com/blog/lessons-learned-from-a-dos-attack-against-a-u-s-power-utility/. [Accessed 10 August 2021].

[41] L. Fimia, "Protecting Energy and Utility Companies from DDoS Attacks," Active Reach, 12 June 2019. [Online]. Available: https://activereach.net/newsroom/blog/protecting-energy-and-utility-companies-from-ddos-attacks/. [Accessed 10 August 2021].

APPENDIX A
Scenario Setup

Page intentionally left blank

APPENDIX A
Scenario Setup

In all of our resilience scenarios, we consider one full year of operation. We use data collected at each of the 14 separate wind turbines collected from July 2020 to June 2021. Although there is some aggregate wind production data available from other years, we focus on this time period because we have wind production and speed, temperature, and alert data from each individual turbine available.

To run our resilience scenarios, we assume that wind turbine production matches what was provided by ILEC. We do not have real load data to pair with the production data, so we use synthetic data (see below). We assume that any additional power needed to meet the load is imported from Corn Belt transmission system (if available). We assume that any excess wind produced exceeding the load is sold back to Corn Belt.

We do not have enough communication system information to accurately model the source, spread, or most likely targets of cyberattacks, so the discussion around these hazards is primarily qualitative, based on events and research from across the world.

A-1. LOAD MODELING

The loads were generated synthetically by the National Renewable Energy Laboratory. The Lakota loads were taken in the range of 6–7 MW, and the Superior loads were taken in the range of 7–8 MW. The loads follow general annual trends, with peak energy use in the summer.