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

STEVE A. BUKOWSKI PhD, PE
Senior Research, Idaho National Laboratory

KATHERINE A. HOVLAND
Intern, Idaho National Laboratory

SEAN MORASH
EnerNex

AARON F. SNYDER PHD
EneNex

NEIL PLACER
EnerNex

JAKE P. GENTLE
Program Manager, Idaho National Laboratory

RESILIENCE FRAMEWORK
FOR ELECTRIC ENERGY DELIVERY SYSTEMS

INL/EXT-21-62326
Revision 1
July 2021

Idaho National Laboratory

DISCLAIMER

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
- Bret Barker

Microgrids, Infrastructure Resilience, and Advanced Controls Launchpad (MIRACL) partners
- Sandia National Laboratory
- Pacific Northwest National Laboratory
- National Renewable Energy Laboratory

AUTHORS

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

STEVE A. BUKOWSKI PhD, PE, Senior Research
Idaho National Laboratory

KATHERINE A. HOVLAND, Intern
Idaho National Laboratory

JAKE P. GENTLE, Program Manager
Idaho National Laboratory

SEAN MORASH
EnerNex

AARON F. SNYDER PhD
EneNex

NEIL PLACER
EnerNex

Idaho National Laboratory | Idaho Falls, Idaho 83415 | www.inl.gov

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

SUMMARY

The intent of this document is to introduce a framework that will enable more thoughtful and deliberate consideration of resilience as it relates to electrical energy delivery systems (EEDS), with specific application to distributed wind systems. The need for this framework was established in a previous report from Idaho National Laboratory (INL), *Distributed Wind Resilience Metrics for Electric Energy Delivery Systems*, where definitions of resilience and resilience of EEDS were developed and a critical characteristic of resilience for EEDS, the distinctiveness quality, was identified.[1] This distinctiveness quality reflects the difficulty in applying resilience metrics broadly to the widely varied risk perception of stakeholders and stakeholder groups, the varied range of potential consequences to a system based upon events, and the large set of potential mitigation strategies. Development of resilience metrics, and more specifically distributed wind resilience metrics, must come from a resilience process that addresses this distinctiveness quality and is separate from well-established reliability processes. These two factors are the primary drivers demonstrating the need to establish a resilience methodology that can be applied to any electrical energy delivery system, any set of stakeholders, and any set of events.

This framework is proposed under the Department of Energy (DOE) Wind Energy Technologies Office (WETO) Microgrids, Infrastructure Resilience, and Advanced Controls Launchpad (MIRACL) project. While the focus of this project is on distributed wind, INL believes resilience is best evaluated at a system level. As such, the 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. With this broad view, it is also possible to apply this framework to systems without distributed wind.

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 usually 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 from different motivating factors.

In this document, the definition of resilience for EEDS as previously identified in the 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."[1] 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 across the time stages. At the lower level the process steps are described, which correspond to implementing practices for resilience in each of the core functions. This tiered breakdown is shown in Figure 1.

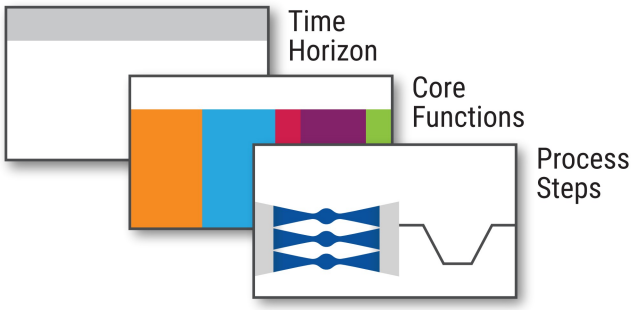

Figure 1. INL resilience framework three-tiered approach

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 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. This framework document intentionally emphasizes the planning stage to highlight the overarching theme that the planning stage heavily impacts those that follow.

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

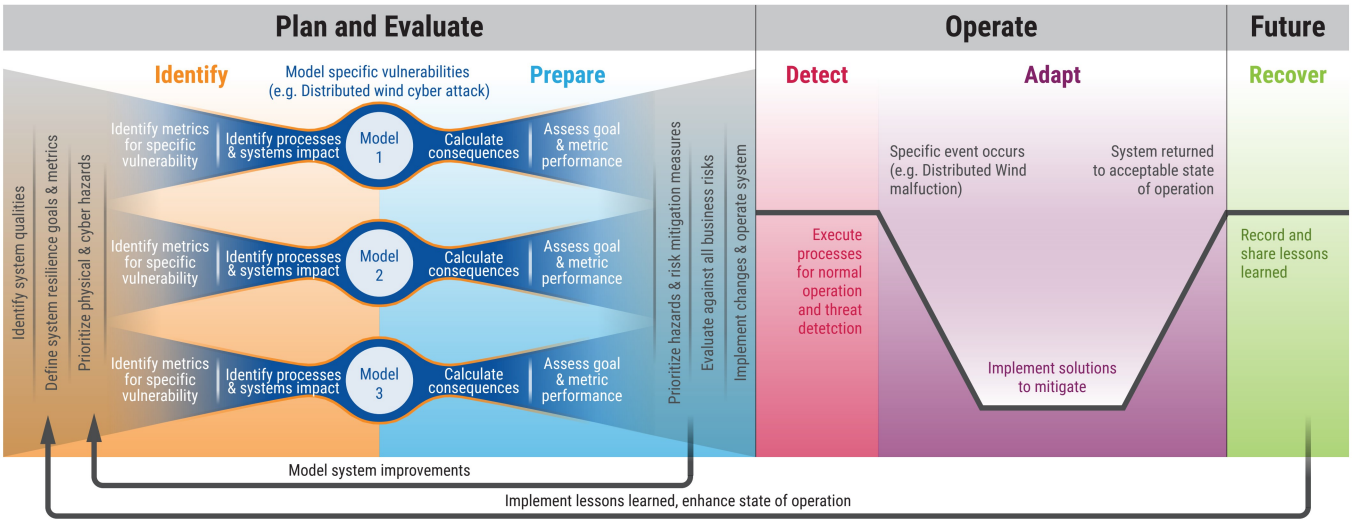

Figure 2. INL resilience framework

The core functions in the framework are 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.[2] Using a structure similar to the NIST framework makes it recognizable and familiar and provides 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. The details of this tiered approach are shown in Figure 2. 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 for identifying, assessing, and mitigating 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.

As the framework is applied to distributed wind, it is important to note that the considerations that shape the framework from a broader EEDS perspective also apply to distributed wind. While the concept of resiliency is not new, its application to the electric grid is neither standardized nor well-defined, and there is little-to-no guidance on how to evaluate resilience specifically for distributed wind systems. This document provides a framework for evaluating 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.

Within this document, the framework emphasizes the planning stage before applying the framework to a utility planner considering multiple investments. While there are already extensive processes 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 creates a process for the model-informed consideration of each hazard.

[2] *"Framework for Improving Critical Infrastructure Cybersecurity," National Institute of Standards and Technology, April 2018. Available: https://doi.org/10.6028/NIST.CSWP.04162018*

CONTENTS

1.0 INTRODUCTION

The intent of this document is to provide a resilience framework for electrical energy delivery systems which can be applied to distributed wind. However, the framework is not limited by application to any resource or system. This framework defines steps to a cyclical process similar in mechanism to both cybersecurity and risk frameworks while providing a common set of language and processes for all stakeholders involved.

One important characteristic of resilience is the unique needs and perspectives of different systems, geographies, resources, stakeholders, perceived risks, and consequences, which we term the **distinctiveness property**. This distinctiveness property drives the requirement to have a resilience framework or methodology that can be implemented for different types of systems. The process or methodology should be cyclic. Recognizing that 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 pace for its distinctiveness property. These constraints have all been taken under consideration during the development of this framework.

1.1 DEFINING RESILIENCE

INL performed an extensive literature review to explore the current state of resiliency work related to electric energy.[1] Industry, regulatory, and national laboratory work was taken under consideration, and a need was identified for a methodology to examine threats, consequences, risks, and, ultimately, mitigation efforts to improve resiliency. The work done to identify existing work and gaps that need to be filled resulted in the following definition of resiliency for Electric Energy Delivery Systems (EEDS):

> *"The resilience of an EEDS is described as a characteristic of the people, assets, and processes that make up the EEDS and its 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."*

A few important components of this definition to highlight include:

- Resilience is a characteristic of a system. There are proposed advanced metrics and indices, discussed in detail in the INL review that can help measure resilience, as well as metrics related to individual components that can help measure the resilience characteristic.
- Resilience is defined with respect to a particular EEDS and its associated people, assets, and processes. It is necessary to appropriately identify all the related components of the system to say anything meaningful about its resilience. To make an analysis consumable, it may be valuable to decompose the more complex system into generic subsystems. However, defining resilience for a generic system without some specifications made does not hold much value.
- Resilience is defined with respect to disruptive events, also referred to as disturbances or hazards. For example, a system that is resilient against fuel shortages may not be resilient against hurricanes. However, a system has some level of overall resilience when evaluated with regard to how the system performs against a certain subset of pre-identified relevant hazards.
- Resilience is focused on the recognition of impact and response to disturbances, not on the properties of the disturbances themselves. By focusing on awareness and response, a system's resilience characteristic can be evaluated against a range of events across time. This also allows for assessment of preparedness for a given event. If a system is prepared for an event, it will likely be more resilient against that event.

- An "acceptable state of operation" does not mean that the system returns to operating exactly as it did before the disruptive events. For example, a system may experience a transmission line outage and switch to localized backup power provided by batteries fed by solar farms. The state of operation is acceptable because customers did not experience an interruption in service, but the operation is very different from the starting condition. The long-term goal of the system should be to reach a state of operation more robust than the starting point. This may be by incorporating lessons learned into operational processes or by making changes or fixes to enhance system resilience. If a system accomplishes this, it is truly resilient.
- The resilience cycle is made of five main functions, as called out in the definition: identify, prepare for, detect, adapt to, and rapidly recover from disruptive events. Detect is not explicitly named in the definition, but it is a critical part of the adapt function. To mitigate consequences during the adapt function, operators must successfully detect the disturbance and implement the correct response plan.

1.2 INTENT OF THE FRAMEWORK

This framework is chiefly intended for regulators, investors, utility planners, engineers, operators, customers, or other stakeholders who need to define, evaluate, or set standards for the resilience of a system. The interests and goals for each of these stakeholders may be different, but the framework is designed to be flexible and to adapt to the priorities identified by the stakeholder using the framework. For example, regulators may use the framework to help establish new processes for their jurisdictions, and consumer advocates and environmental groups may use the framework to participate in prioritization and goal-setting activities. No matter who is leading the resilience planning efforts, this document helps to outline the considerations and processes associated with long-term resilience planning. In the remainder of the document, we use the term stakeholder generically, with the understanding that specific groups will apply the steps that are most relevant for their interests.

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 improvement. It can be used as a key part of the process for identifying, assessing, and managing risks. One benefit from the framework is a systemic prioritization of improvement plans. Using the framework to guide resilience management, stakeholders can:

The framework is intended to be extensible and applicable to a variety of systems, yet customizable to value the goals and metrics appropriate for a given system's distinct characteristics, drivers, and values.

The framework is also extensible and applicable on a smaller scale as stakeholders think through the planning and operations of their EEDS. The same core functions that apply to large systems are important on a small scale. EEDS are often interconnected such that the resilience of one subsystem impacts the larger system. The framework can also be used in this context as stakeholders evaluate how their system fits in the larger context of the EEDS. To that end, Section 5 offers an example of how a system with distributed wind might implement the framework.

1.3 RELATED WORKS

Due to the distinctiveness property of distributed wind systems, it is difficult to define an all-encompassing framework that is specific enough to be useful for planning and decision making, but general enough to encompass the uniqueness of different systems. The IEEE Power and Energy Society (PES) Technical Report, Resilience Framework, Methods, and Metrics for the Electricity Sector, describes this issue:

> *"The development of metrics and a framework for evaluating resilience involves a multi-dimensional exercise with high complexity levels across multiple industry sectors, given the interdependencies among the various infrastructure sectors. The core of the issue is that there are numerous parameters or events associated with resilience."* [3]

In that same document, the task force discusses the similarities and differences between quantitative frameworks, qualitative frameworks, and all-hazards frameworks and their associated qualities. The framework defined in this document best aligns with the all-hazards category but recognizes key benefits of using both qualitative and quantitative metrics at different steps of the process and intentionally incorporates them. As suggested in the IEEE document, we adopt a risk-management perspective.

The North American Electric Reliability Corporation (NERC), while tasked with ensuring the reliability of the grid, has also examined how resilience is already built into their mission, and what they can do to better support resilience efforts.[4] The NERC Reliability Issue Steering Committee (RISC) created a framework that is broken down into four key constructs: robustness, resourcefulness, rapid recovery, and adaptability. This aligns with our operational stage of resilience but does not take the planning and continuous development aspects into account, nor does it provide specific steps to help stakeholders evaluate and improve their resilience position.

Additional academic research examines existing qualitative and quantitative frameworks and presents their own. The resilience evaluation framework from Bie et al. aligns with the planning stage that we present.[5] It specifically aligns with our framework's risk analysis strategy. This is one of the most valuable parts of a resilience framework, and we recommend their work to help create mitigation strategies. However, it fails to move the user into the operational stage and incorporate lessons learned from real scenarios back into the planning stage. Another work which does incorporate the iterative process is the framework defined by Toroghi and Thomas. In this framework, the concept of resilience is applied with four dimensions: robustness, redundancy, resourcefulness, and rapidity plus the adaptation capacity of the system to its new environment, post-incident, which they call the "readjust-ability capacity."[6] The readjust-ability capacity aligns with the iterative nature of our framework, but the focus is primarily on the operational stage.

Sandia National Laboratories also presents a framework that emphasizes the planning stage.[7] The Sandia National Laboratories research not only aligns with our framework, but also takes a similar approach of presenting process steps. The multi-laboratory Grid Modernization Laboratory Consortium (GMLC) project has expanded on this framework and also defines a hazard-based approach. They have developed a "hybrid approach combining multi-criteria decision analysis (MCDA) and performance-based techniques to propose a comprehensive resilience metrics capability that integrates both the technical characteristics of the grid and its operating environment."[8] While this hybrid approach is similar to ours, the two techniques they discuss focus on the planning stage. We aim to build on this work by building out the process steps in more detail and linking them to the operational and future stages.

[3] *IEEE Power and Energy Society, Resilience Framework, Methods, and Metrics for the Electricity Sector, IEEE PES-TR83, Oct. 2020.*

[4] *NERC, "Reliability Issues Steering Committee Report on Resilience," North American Electric Reliability Corporation, November 2018.*

[5] *Z. Bie, Y. Lin, G. Li and F. Li, "Battling the Extreme: A Study on the Power System Resilience," in Proceedings of the IEEE, Vol. 105, No. 7, pp. 1253–1266, July 2017, doi: 10.1109/JPROC.2017.2679040.*

[6] *S. Toroghi and V. Thomas, "A framework for the resilience analysis of electric infrastructure systems including temporary generation systems," Reliability Engineering & System Safety, Vol. 202, October 2020.*

[7] *J. P. Watson, et. al, Conceptual Framework for Developing Resilience Metrics for the Electricity, Oil, and Gas Sectors in the United States, Sandia Report SAND2014-18019, September 2015.*

[8] *F. Petit, V. Vargas, and J. Kavicky, "Grid Modernization: Metrics Analysis (GMLC1.1) – Resilience," Grid Modernization Laboratory Consortium, Reference Document volume 3, April 2020.*

Another national laboratory resilience approach is the National Renewable Energy Laboratory (NREL) research adapting simulation models for resilience analysis.[9] In this approach, a scenario is chosen, this scenario is simulated and evaluated with resilience metrics, optimization techniques are considered, and through an iterative process, decisions on investments are made. This approach corresponds to the bow-tie analysis step of our planning stage, and many of the tools described in this report may be useful.

The research described represents the work that is most relevant to ours, but there is much more research examining resilience in different contexts. One study found that among 100 resilience works analyzed, 52 assess the "resist" function, 77 the "restabilize," 54 the "rebuild," and only 16 the "reconfigure" function.[10] While not exactly correlated, these functions align with the core functions in our framework. The evaluation found emphasis in research on the "resist" phase, including pre-event, but "rebuild" and "reconfigure" functions have been much less investigated. They note that only six studies analyze all four of the resilience functions they define, and only three of these use a quantitative approach, signaling the difficulty to comprehensively quantify resilience and the need to focus on the "reconfigure" function, which in our framework we refer to as the future stage. They also found that many resilience studies only consider situations where disruptions cause drops in performance, and do not consider the likelihood of such events. The risk approach adopted in the planning stage of our framework accounts for the likelihood analysis.

Another study evaluating multiple resilience framework proposes five indicators for evaluating a resilience model: catering to different stakeholders, intervening in development phases, dedicating to certain stressors and failures, taking into account interdependencies, and involving socio-economic characteristics.[11] Our framework performs well against all of these indicators, particularly the first three.

A common theme among the existing frameworks for EEDS is that they cover one, but not multiple, of the resilience stages that we have identified. The few that do cover multiple stages stay at a conceptual and abstract level rather than teaching users how to actually evaluate resilience through the full lifecycle of the system.[12,13] While there is alignment between existing work and our framework within individual stages, existing frameworks do not cover the full lifetime of system resilience though planning, operational deployment, and consistent improvements for the future at a level of detail useful for evaluation. We are filling a gap in research by creating a resilience framework for EEDS that considers multiple stages of resilience, helping stakeholders manage the resilience of their systems throughout the system's lifecycle. Additionally, our approach with three tiers of abstraction allows stakeholders to look at their system's resilience from a high level but also breaks down the process for evaluating and implementing resilience solutions into steps that are easy to follow and apply.

1.4 OUTLINE

This document is broken up according to the three tiers of abstraction that define the framework. The first describes the broadest categories of resilience, distinguished by the three different stages. The next describes the core functions of resilience, which widely encapsulate the actions required for a lifecycle of resilience. The core functions are then broken down into individual process steps that walk a user through the actions needed to evaluate and maintain resilience in each core function. Finally, we present a case study that shows an example of how the framework can be used to make decisions and evaluate resilience benefits in a system.

[9] *C. Murphy, E. Hotchkiss, K, Anderson, C. Barrows, S. Cohen, S. Dalvi, N. Laws, J. Maguire, G. Stephen, and E. Wilson, Adapting Existing Energy Planning, Simulation, and Operational Models for Resilience Analysis, National Renewable Energy Laboratory, NREL/TP-6A20-74241, February 2020.*

[10] *P. Gasser, P. Lustenberger, M. Cinelli, W. Kim, M. Spada, P. Burgherr, S. Hirschberg, B. Stojadinovic, and T. Sun, "A review on resilience assessment of energy systems," Sustainable and Resilient Infrastructure, Taylor & Francis, 2019, DOI: 10.1080/23789689.2019.1610600*

[11] *J. Wang, W. Zuo, L. Rhode-Barbarigos, X. Lu, J. Wang, Y. Lin, "Literature review on modeling and simulation of energy infrastructures from a resilience perspective," Reliability Engineering and System Safety, Vol. 183, pp. 360-373, March 2019. DOI: 10.1016/j.ress.2018.11.029.*

[12] *H. Weise, et al. "Resilience trinity: safeguarding ecosystem functioning and services across three different time horizons and decision contexts," OIKOS, Vol. 129, No. 4, pp. 445–456, April 2020.*

[13] *G. Kandaperumal, A. Srivastava, "Resilience of the electric distribution systems: concepts, classification, assessment, challenges, and research needs," IET Smart Grid, Vol. 3, No. 2, pp. 133-143, April 2020.*

2.0 STAGES OF RESILIENCE

Evaluating a system's resilience is a continual process; however, three stages can be defined to assist in considering this event-based paradigm, as seen in Figure 3.

2.1 PLANNING

During the planning stage, stakeholders consider their system and the potential hazards that it might encounter. They prioritize hazard scenarios and evaluate their system with regard to the breadth and depth of high-priority hazards. Using a hazard-based risk assessment, stakeholders can identify mitigations that will reduce the impact of the greatest risks and implement or make allocations for those mitigation measures. It is practically impossible to test and model all possible scenarios for weather-related events, cyber events, and other types of disturbances. However, through stakeholder input and hazard prioritizations, resilience can be evaluated for a system in certain resilience scenarios.

Systems will be evaluated with regard to high-risk events. Infrastructure may suffer similar consequences (e.g., lines broken, poles damaged, fires) while the locations may differ. Mitigating the impact of these hazards may entail an analysis of critical load support with compromised infrastructure (e.g., portable generators, multi-fuel generators, more circuit reconfiguration equipment). In a weather-based event, the utility will put into place the people, processes, and systems they consider necessary to mitigate that hazard.

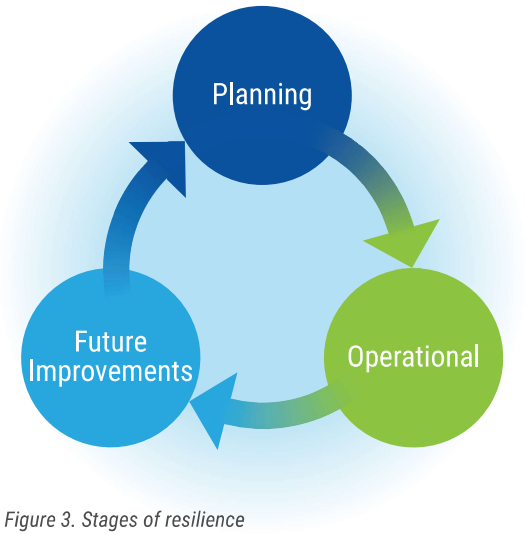

Figure 3. Stages of resilience

Hazards of human origin (i.e., cyber or physical attacks) should also be evaluated as part of the planning stage. Stakeholders should consider different risks and consequences, and plan for unknown vulnerabilities, which can lead to potentially high-impact consequences. For cyber hazards, the utility can engage specialized third parties to examine and test the system to expose risks. Results can then be used to improve the capabilities of the system.

This type of planning differs from traditional reliability planning in that it considers high-impact, potentially long-duration consequences. It also differs from other long-term planning in that the planning stage of this framework focuses on a new characteristic of the system (resilience). Therefore, the planning stage also prioritizes resilience measures with respect to quantifiable metrics and with regard to all other risks. One example of how this stage is needed for distributed wind is that the siting process for distributed wind is not as well developed as it is for bulk wind. If planners considering installing distributed wind spend more time evaluating different potential locations, they can pick the site that would provide the most resilience benefits for the overall system.

The planning stage considers the realm of potential risks, prioritizes mitigation plans, and makes periodic investments. Further, the planning stage includes reconsideration of the involved people, processes, systems, and infrastructure. The end of the planning stage calls for implementing changes in the system, which begins the operational stage.

2.2 OPERATIONAL

In the operational stage, stakeholders are expected to maintain agreed-upon service levels facing any number of risks, expected or unexpected. This is the most "hands-on" portion of resilience as many decisions are needed in very short time frames to maintain system viability. When a hazard event occurs, the people, processes, and systems detect the event, and then react to the extent of their capabilities.

In the operational stage, operators are expected to maintain agreed-upon service levels facing any number of hazard scenarios, planned or unplanned. This is the most hands-on portion of resilience as many decisions are needed in very short time frame to maintain system viability. When a hazard occurs, the people, processes, and systems detect the event and then react to the extent of their capabilities. We employ the resilience trapezoid model to consider different phases of operational resilience in response to a disturbance. Because neither set of risks (cyber or physical) can be completely accounted for, the concept of deterministic degradation to new operating points is critical to keep as an operational philosophy. In other words, the path that failure takes can impact the level of resilience. After recovering to an acceptable operating point, the return to a high-performance state and the impact of the event can be analyzed in the future stage.

2.3 FUTURE

The future stage focuses on implementing changes to improve system resilience over time. This can involve direct work in the operational world to make repairs, upgrade components after they failed, or make immediate changes to standard processes. It also involves the combination of planning efforts and leveraging lessons learned to create future resilience. It is critical to account for new technology and improved workflows, understanding how to pace investments in resilience, and when to make those investments operational. An example is the communications network with sensors and controls to commission a fault location, isolation, and service restoration (FLISR) program for critical, high-priority circuits. Those circuits need a hazard evaluation and some level of hardening before advanced FLISR operations should be considered.

Adjusting the future should begin immediately post-event as an operational "lessons learned debriefing" to identify improvement for the next planning cycle and set of scenarios. The lessons learned should then be turned into changes and improvements to reduce the consequences if a similar event should happen again. This can include decisions like keeping more spare parts available, changing operational processes, or replacing aging or broken components to reduce the likelihood of failures in the future.

3.0 CORE FUNCTIONS OF RESILIENCE

We define five core functions of resilience that make it possible to monitor resilience through the stages of resilience described above. These are:

- Identify
- Prepare
- Detect
- Adapt
- Recover.

The core functions of resilience bring the stages one step closer to a practical stepped framework. These core functions affect the entire lifecycle of a system, from identification of the components of the system to planning the installation of new subsystems, and ultimately through the processes used to retire system components. The five functions fit into the broader stages of resilience, as shown in Figure 4. The identify and prepare functions fall under the planning and evaluation stage. The end of the prepare function calls for implementing changes in the system, which begins the operational stage. The detect and adapt functions fall under the operational stage of resilience. Finally, the recover function takes the system into the future stage of resilience. Descriptions of each function are presented in detail below.

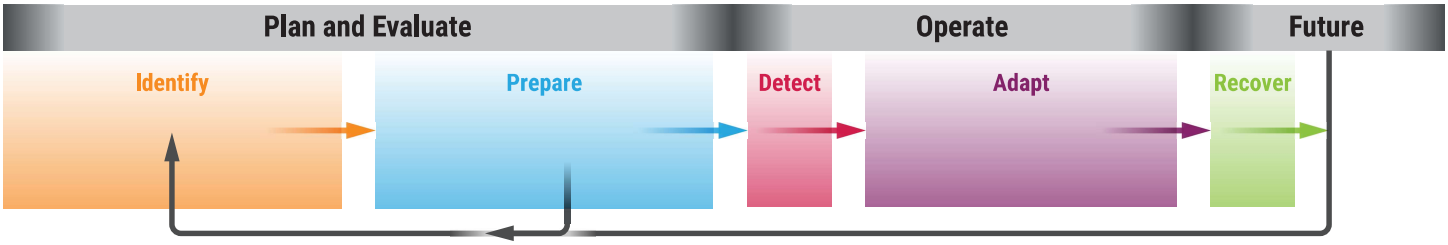

Figure 4. Core functions of resilience

3.1 IDENTIFY

The identify function helps stakeholders assess and develop an understanding of their system resilience relative to potential disturbances to EEDS and associated people, assets, data, and capabilities. The first step in identification is for stakeholders to identify the key properties of their system and their goals with respect to resilience. This might be facilitated by asking the "what if" questions by different stakeholders, including specific events, chain of events, or risks that can help develop resilience scenarios. These priorities and scenarios will look different in every system. To formulate reasonable and applicable goals, stakeholders must also identify the system qualities that are key to defining their system. After defining their goals and the system, the stakeholders should identify the scenarios that are most applicable to their resiliency goals. For example, in an isolated grid, scenarios that impact the cost or obstruction of fuel delivery for thermal generation may significantly impact the EEDS. To identify these events, a full threat evaluation or event analysis with a prioritization of those deemed most important can help support this effort.

For each of the events or threats that are identified as critical, stakeholders should perform risk assessments using a modified bow-tie method of evaluation.[14,15] Unlike a generic threat assessment bow-tie, which focuses on the multiple components that could lead to an event or threat, the left side of our version of the bow-tie focuses on qualifying the factors that will affect and will be affected by the event. The goal of establishing an evaluation of risk to the event or threat is to be able to provide a corresponding prioritization with other business risks, ultimately providing a basis to make investment decisions.

The identify function will include identifying metrics that are applicable to each scenario assessed. Some metrics may be common across all areas, while others may be specific to individual events. The threat assessment will include identifying the processes that are impacted

[14] *Wolters Kluwer, "The bowtie method," CGE Risk, Available: https://www.cgerisk.com/knowledgebase/The_bowtie_method*

[15] *B. Hancock, "The Bow-Tie Analysis: A Multipurpose ERM Tool," NC State Poole College of Management, 2016.*

by the event and modeling the impact on each of those processes. The consequences should be evaluated using the previously identified metrics. Finally, for each scenario the performance of the system should be evaluated with respect to the identified resilience goals.

3.2 PREPARE

The prepare function begins to overlap with the identify function as risks are assessed. The prepare function covers evaluating the results from the threat assessment or event analysis and developing solutions to the system or processes as needed to best mitigate the highest risks. As the consequences from the assessment are evaluated, key factors that could mitigate the consequences should be noted. Assessing the performance against resilience goals gives key insight into which high-priority events or threats need more attention, so that if they occur, the consequences are not as severe.

After evaluating each event individually, the events should be compared against one another and against all business risks to prioritize the most important threats and the corresponding mitigation measures. These mitigations, which may include things like updating emergency response plans or adding additional infrastructure or resources, should be implemented on the real system.

It is worthwhile to iteratively step through the identify and prepare functions to ensure that the proposed mitigations have the intended effect when events that threaten resilience occur. Another way to use this function is to compare different system improvements or mitigation measures. Stakeholders can perform threat analysis of the system under the same resilience scenario with different upgrades in place and evaluate which one best meets the resiliency goals.

The bulk of this report will focus on how to use the identify and prepare functions to evaluate resiliency from a planning perspective.

3.3 DETECT

In the detect function, the system detects disturbances and begins mitigating their impact. The ability to successfully perform this function relies on identification of the potential event and preparation for it (the first two functions). There may be broad categories of scenarios that can be detected by the same mechanisms (i.e., multiple scenarios may cause low-voltage events, but the low voltage can be detected by supervisory control and data acquisition (SCADA) systems no matter how the event started). However, there are also events that require particular awareness of the event. For example, detecting a ransomware attack requires the information technology (IT) tools that can detect when this malware is present.

Another aspect of the detect function is the ability to perform normal operations. Detection needs to happen simultaneously with regular actions and monitoring. Many detection mechanisms may be already built in as part of normal monitoring actions, but stakeholders should ensure that these mechanisms can also be used to detect and alert operators to disruptive events.

3.4 ADAPT

In the adapt function, stakeholders will continue to apply mitigations. The adapt function includes properties like graceful descent to a degraded state, mitigating effects so that the degraded state is less severe, quick responses to limit the time spent in a degraded state, and methods to bring the system back to an acceptable state of operation.

The adapt stage is where all the plans for resiliency are enacted. Emergency operation plans are executed, repair crews are deployed as necessary, and ideally, backup systems prevent the system from feeling the impact of the threat or disturbance. The adapt function uses human assets, equipment, and technology to aid the execution of the response plan. The system should ideally be able to adapt even to scenarios that it has not experienced before.

We consider the adapt function to cover the initial steps of system restoration. The system may stay in a partially restored state that maintains an acceptable level of performance for an extended period of time while measures are taken to restore the system fully. Another way to frame this is to say that often the adapt function includes actions taken on the seconds-to-hours time scale, and the recover function includes actions taken on the days-to-months time scale.

3.5 RECOVER

The recover function brings the system back up to full levels of performance and incorporates lessons learned. At the end of the recover function, the system should be more resilient than it was before, either by reaching a more efficient state of operation, or simply by building lessons learned into emergency response procedures so that if the event reoccurs, the system spends less time in a degraded state. A key part of the recover function is the return to the identify stage, where the iterative identify and prepare steps should be executed to check if the system responded as expected to the resilience scenario, and how to improve performance next time.

4.0 FRAMEWORK PROCESS

So far, we have discussed the stages and core functions of resilience. To make this framework more actionable, we also define process steps. Stakeholders can walk through these steps to assess their resilience and improve their position over time. The full framework is provided in Figure 5 below. The following sections describe the framework process in detail.

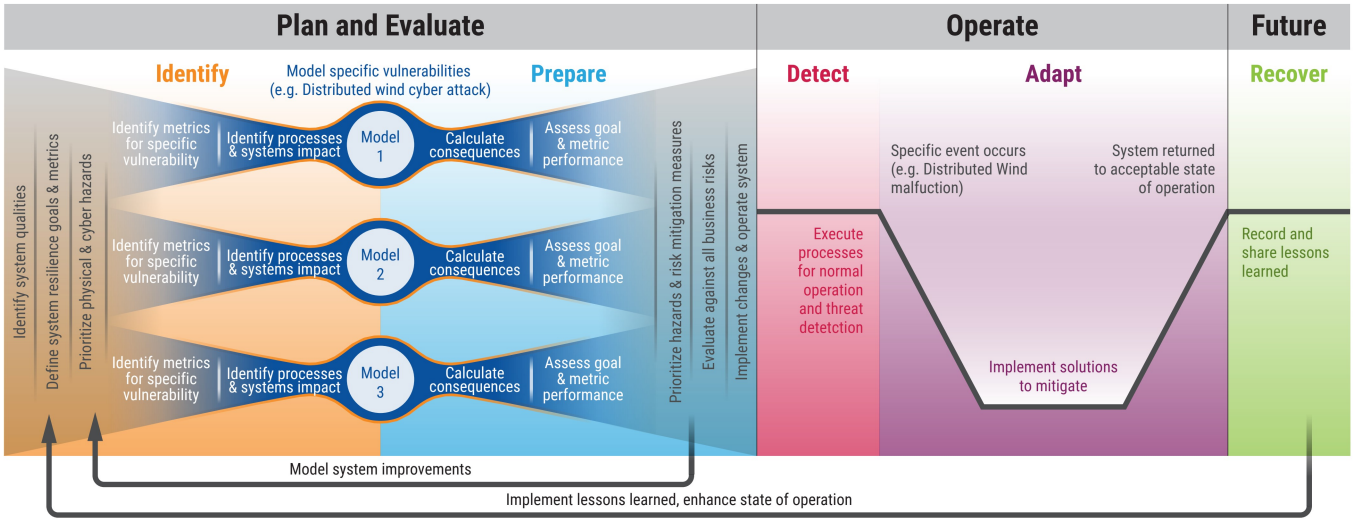

Figure 5. Detailed resilience framework view.

4.1 PLANNING

The key to this framework is effective planning. Through effective planning, stakeholders prepare themselves for risks such that they can improve the resilience of their system, either by reducing the event impact or by rapidly recovering from the disruptive event. The planning process is iterative and includes a feedback loop from real-world experiences. It is intended that this process is undertaken every few years to ensure that identified threats, system characteristics, and metrics of evaluation are still appropriate.

We have modeled the planning process in Figure 6 below. This bow-tie method allows the user to work through broad strokes of the system, narrow focus onto specific resilience scenarios, and then work back through the broader context of the system and associated business risks. The bow-tie method is used across industries to show links between sources of risk and consequences. The bow-tie method traditionally builds from a "cause-event-consequence" diagram to show the multiple causes and consequences stemming from a single event. We have adjusted this method to a planning context and expanded the method to show that the consequences of an event include changing the system over time, rather than simply the near-term impact of the event.

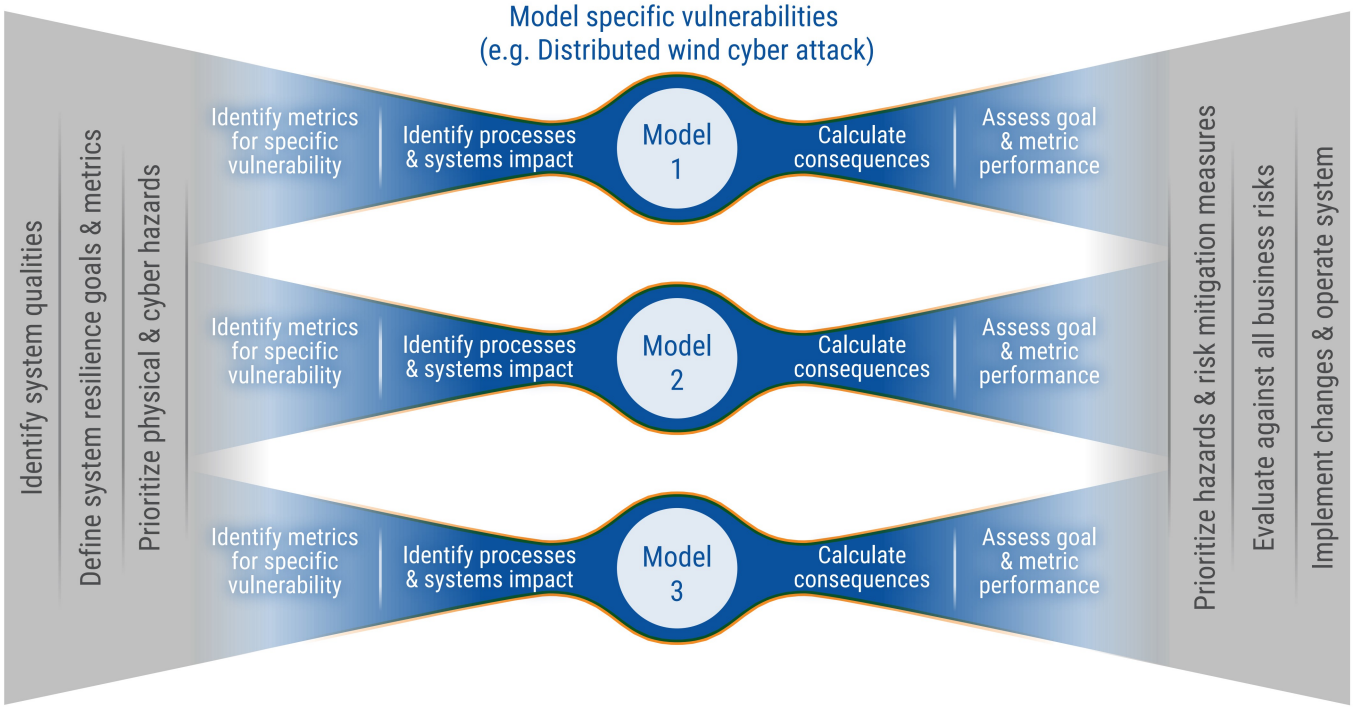

Figure 6. Nested planning bowtie.

4.1.1 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 boundaries, electric boundaries, relevant time periods, or even components. An off-grid distributed wind system might include an entire circuit. A behind-the-meter distributed wind system might only need to define the specifics of everything behind the meter but may still need to take into the account the status of the interconnected distribution feeder. A distribution-tied distributed wind system may need to consider a broader area. However, in each of these configurations of distributed wind systems, it will be important to note the characteristics of the turbine and the controller, including what ancillary services it can provide, what weatherization packages it is outfitted with, and what its physical limitations with respect to external conditions are (wind, temperature, etc.). Each system is unique; therefore, it must be fully defined before the resilience of a system and the relevant resilience scenarios can be uniquely defined.

Appropriately identifying the system characteristics will help to inform subsequent steps, including risk prioritization, modeling the system, and even operating the system. The definition of an acceptable state of operation following a disruptive event should also be defined at this stage. System characteristics may be unknown, which indicates that a potential resilience investment is to improve observability of system.

4.1.2 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. They should identify what they wish to achieve with their system before appropriate metrics and models can be determined and before investments can be made.

Stakeholders may have multiple and competing resilience goals, but these goals should be ranked so that options can be compared. The goals may be defined in terms of broad, general outcomes. Future steps will help narrow unresolved questions and ultimately identify any investments that should be made to achieve the goal.

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 hazard, 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.

In particular, metrics should cover the following criteria, adapted from Watson et al.[16]

Quantitative:

> The metrics should be measurable and useful for data analytics to educate investment decisions.

Extensible:

> The metrics should be scalable to reflect different time periods, electrical landscapes, and geographical areas. The metrics should be valid across a wide range of technologies.

Comparable:

> Applying the same metric across different scenarios (e.g., before and after enhancements, under different operating conditions) should provide valuable information.

Actionable:

> Metrics should be useful for decision-making. Decisions of interest include system planning, operational decisions, and policy-making.

Understandable:

> Metrics should be readily understandable by different audiences.

Risk-based:

> The metrics should relate to particular risks that are relevant to the system. The metrics may relate to a specific disturbance or to potential consequences.

Time-sensitive:

> The metrics should reflect consequences that occur at different time scales, and should consider the recovery period, either directly or indirectly.

Confidence-ranked:

> The metrics should have an associated level of confidence. The uncertainty associated with a metric value will help inform decisions based upon that metric.

Data-driven:

> The metrics selected should be informed by real data from the system. If data to support a certain metric is unavailable, the necessary measurement infrastructure must be added, or confidence in the metric will suffer.

The INL report on resilience metrics discusses in more detail the individual and combined metrics that may be most useful for evaluating resilience of distributed wind systems.[1] A summary of common metrics that are applicable to systems with distributed wind is presented in Figure 7.

The purpose of this step is to define the ideal outcomes of the operational stage, but it is useful to also include goals for the planning and recovery stages.

[16] *Watson, J.-P., R. Guttromson, C. Silva-Monroy, R. Jeffers, K. Jones, J. Ellison, and L. T. Walker,* Conceptual Framework for Developing Resilience Metrics for the Electricity and Gas Sectors in the United States*, Albuquerque, New Mexico: Sandia National Laboratories, 2015*

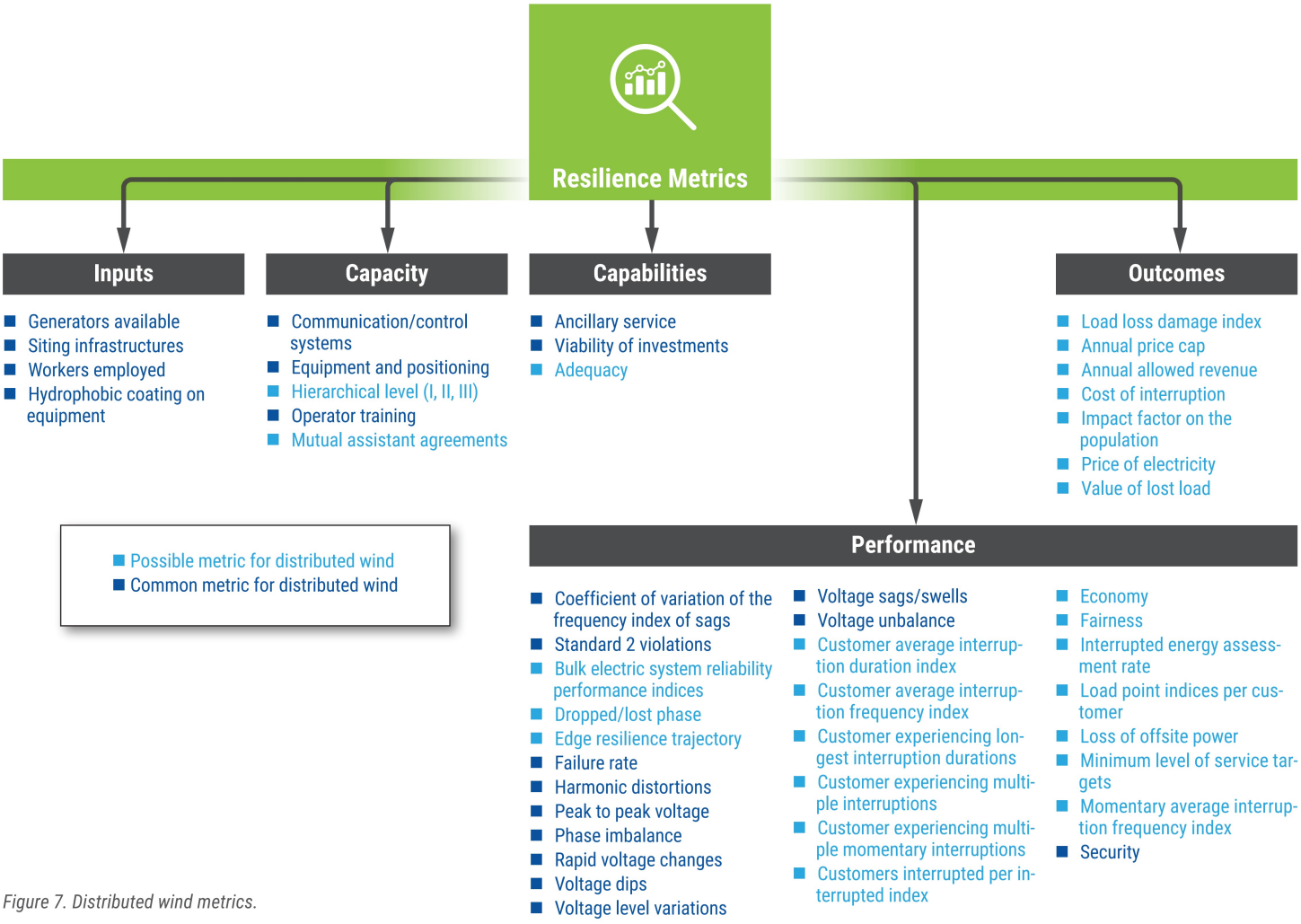

Figure 7. Distributed wind metrics.

4.1.3 PRIORITIZE PHYSICAL AND CYBER HAZARDS

Stakeholders should work together to prioritize physical and cyber 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. Examples of scenarios under consideration may include a severe winter storm, a hurricane, a fuel shortage, a ransomware attack, a downed transmission line, or a cybersecurity advanced persistent threat (APT) with the capability to cause cascading outages. There may be hazards that are specific to distributed wind systems, such as turbines failing to provide ancillary services that are required of them. However, it is more likely that the initial hazard assessment will be more focused on external events due to climate, weather, or manmade threats than failure modes of individual components.

After stakeholders understand the possible threats to a system, the risk of these threats should guide prioritization. Whether it is a physical or cyber hazard, the calculation shown in Figure 8 is helpful in considering risk assessments.

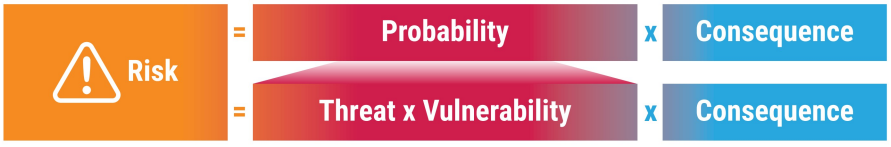

Figure 8. Components of risk.

Risk can be considered the probability (or likelihood) times the consequence (or impact). In this manner, a high-impact but unlikely event can be ranked 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 cyber 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. Consequence may be assessed in terms of public safety, physical damage to infrastructure or equipment, stability of a power system, or ability of a system to provide its intended services. Duration of the consequence should also be considered, as it is a key resilience characteristic.

Hazard prioritization is critical to understanding the system requirements, modeling strategy, and ultimately in developing mitigation plans.

4.1.4 BOW-TIE ANALYSIS OF SPECIFIC HAZARDS

Now that 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 of the system to fully understand system preparedness.

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. Whereas a power system metric may be to measure how many customers remain supplied with power, a metric for a phishing email scenario could be the percentage of stakeholders who fall victim to the scheme.

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. For instance, reacting to a hazard may require a particular process that does not currently exist. Conversely, there may be known vulnerabilities on the system (e.g. wooden pole infrastructure) that may need to be modeled for further investigation.

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 the humans, processes, technology, and infrastructure fare in a mock event.

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?

Finally, for each scenario, performance should be evaluated by considering if goals were met and if metrics were within acceptable ranges. Stakeholders may ask themselves if 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?

The framework can be used to analyze potential investment options. In this case, the bow-tie analysis should be performed for with and without the proposed investment, or with each of the potential investment options, for each hazard. For example, if a utility is considering installing a distributed wind system to support an existing local grid, they should consider their primary hazard assessments both with and without the distributed wind system. By doing this, the resilience benefits from the new investment can be evaluated.

4.1.5 PRIORITIZE RISK MITIGATION MEASURES

Based on the outcomes of the modeling, risk mitigation measures should be prioritized. Perhaps the system performed well against the highest priority scenario, but additional measures are needed to protect the system against the third-highest priority scenario. A single risk may have multiple mitigation options, and those options themselves may mitigate multiple risks. For instance, a distributed wind system may be tied to a distribution system with aging wooden pole infrastructure. To mitigate the potential impact of a hurricane, the pole infrastructure may be upgraded. Alternatively, the pole infrastructure could be replaced with an underground system that also protects against wildlife disrupting the circuit. For the distributed wind system itself, nacelle heaters may make the system more resilient against cold weather storms, and conducting regular cybersecurity audits that include measures like changing passwords and reviewing access control

lists may make the system more resilient against cyberattacks from both internal and external sources. Risk mitigation measures should include cost estimations and effectiveness metrics that evaluate the efficacy of a mitigation measure against a given risk.

At a system level, the outcome of this step may be deciding whether to move forward with a potential investment after running a hazard analysis with and without the potential investment. For example, a utility may decide that installing a distributed wind system provides enough ancillary services to reduce their risk of system instability, and thus provides significant resilience benefits. At a component level, the outcomes of the bow-tie analysis may suggest the need for mitigations measures. For example, a distributed wind system may need nacelle heaters or heated blades installed to mitigate effects from an extreme winter storm. Or, the same system may need firewalls installed, passwords changed, and role-based access control implemented to mitigate the likelihood of a cyberattack affecting the turbine controls.

At this stage, it may be tempting to completely reprioritize based on the outcome of modeling exercises. However, care should be taken to continue to treat high-priority scenarios as such—just because the system was resilient with respect to the highest priority scenario today does not mean it will remain so as the system changes and the risk evolves. Reprioritization and updated modeling and analysis should be performed based on the best judgement of those involved; the framework is intended to be iterative and incorporate inputs as they are known.

This reprioritization and iteration through the planning stage pits top-down framing and against bottom-up analysis. The framework attempts to utilize both to inform the answer planning and operating of the system. Whereas a top-down framing may identify cybersecurity hazards, the bottom-up analysis may show that the system is following best practices of cybersecurity but is lacking in physical infrastructure investments due to decades of underfunding. The risks and measures identified to mitigate them should balance all information available, including the top-down prioritizations identified early by stakeholders and the bottoms-up modeling outcomes.

4.1.6 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. For example, risk mitigation measures identified in the previous step may include upgrading an aging wind turbine with a new system outfitted with the capability to provide more ancillary services and adding a new small gas plant to keep up with growing demand. 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. There can be compromises made at this stage too, for example using the opportunity of upgrading the wind turbine to install a turbine of larger capacity in addition to the new control functions, thereby reducing the load pressure and eliminating the need to build a new gas plant. Decision makers take the prioritized resilience measures and determine what can be done with regard to other business constraints (i.e., resources, budget, feasibility).

This step is where a detailed cost analysis may occur. There are financial tradeoffs 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.

4.1.7 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.

4.2 OPERATIONAL

The operational stage of resilience borrows the resilience trapezoid that was defined in "Distributed Wind Resilience Metrics for Electric Energy Delivery Systems" and is adapted in Figure 9 below. The operational stage covers the core functions of detect and adapt.

4.2.1 OPERATE AND MONITOR

Successful resilience operation begins before a disruptive event occurs. Stakeholders should establish processes for normal operation and incorporate strategies for hazard detection identified in their planning processes. Some events, such as weather disturbances, may be obvious, while a cyberattack may require diligent monitoring to identify. For most parts of a system, the infrastructure to operate and monitor will come standard. However, there may need to be some actions taken to make sure that the appropriate parties have access to the data they need. This could involve configuring a distributed wind system to output its current measurement of the speed and direction of wind at nacelle height in addition to the current power production. This system may also require a historian to be set up to log the data for later analysis. The owner of the wind turbine must also ensure that third-party operators, such as a utility or distribution operator, have access to the data they need, like power production and availability, while also ensuring that no unnecessary remote control abilities are shared.

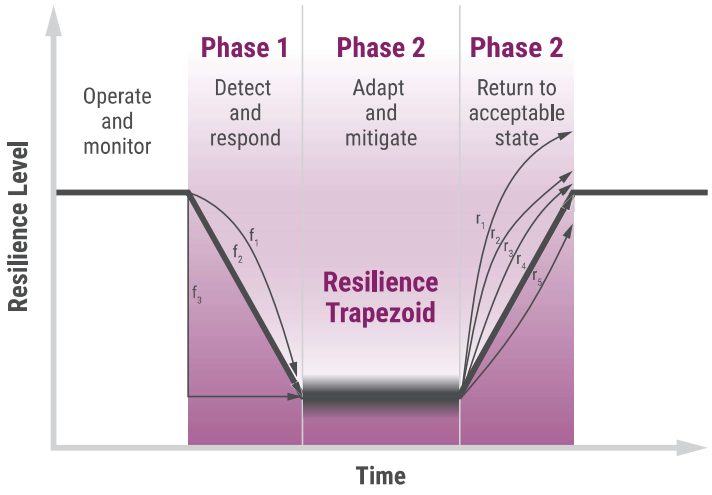

Figure 9. Resilience Trapezoid.

4.2.2 DETECT AND RESPOND TO DISTURBANCES

When a disturbance occurs, the system should have the instrumentation to detect the hazard, and the detection process should be as robust as possible. Detection can occur at any point during the disturbance, but early detection may help lead to an improved response.

Once a system has detected the disruptive event, it can respond. Successful planning can impact the path that the system takes to a failed state. Within Figure 9, the path f1 shows a graceful degradation that is possible because there is an immediate detection and response to the hazard, such as a distributed wind system that is acting as spinning reserve recognizing that there is a drop in voltage signaling a loss in power production. The wind system may then halt power curtailment or reconnect to the system to provide the backup power needed and prevent customers from experiencing a loss in service. The path f3 is a brittle degradation that would put more stress on the system and may be the result of a hazard that the system was not instrumented to detect. For example, an undetected advanced cyberattack has the potential to immediately cut power to customers.

Ideally, response strategies for the given disruptive event were already developed in the planning stage and can be executed immediately after the hazard is detected. This can include simple controls like nacelle heaters turning on when a low-temperature threshold is exceeded to ensure that oil for the turbine does not freeze. Successful detection can also affect the extremity of the failed state; the detection and response to an event can have a significant effect on the overall impact of the event. This concept is represented as the gradient of possible values for the failed state at the bottom of the trapezoid.

4.2.3 IMPLEMENT SOLUTIONS TO MITIGATE

This step occurs after the initial detection and immediate response has taken place and focuses on the solutions that can mitigate the impact of a disturbance. This can include preventing the system from experiencing cascading failures, shortening the duration of the failed state, and beginning a recovery process. This step should include continued implementation of pre-planned response plans, but it may also require dynamic responses to changing conditions that may or may not fall precisely within the scope of the hazards that were modeled during the prepare stage.

4.2.4 RETURN TO ACCEPTABLE OPERATIONS

The recovery process begins once solutions have been initialized to help the system recover and continues until the system returns to an acceptable state of operation. This does not require that the system return to the same state as before the disruptive event. Instead, the system should reach an accepted level of normalcy as defined by stakeholders. As with the degradation process, the return process can take one of many paths. A recovery path such as r1 in Figure 9 represents the system rapidly recovering from the hazard, and potentially returning to a state better than the one it started in. This is the ideal path but may not be readily possible. A recovery path such as r5 represents the system taking longer to recover, and potentially returning to a state not as resilient as the one it started in, but one that bears some semblance to normalcy. Although Figure 9 presents the recovery paths on the same time interval, this is not necessarily the case for a real system, but it helps visualize the comparison of different paths. Also note that in real systems, this return to acceptable operations will likely be more of a step process than a smooth transition.

4.3 CHANGING THE FUTURE THROUGH AN ITERATIVE PROCESS

Once an acceptable state of operation has been reached, stakeholders can shift focus to returning the system to full performance and to improving its resilience to better prepare for future events.

4.3.1 RESTORE AND IMPROVE

A key aspect of resilience is that it should encourage continuous improvement. A truly resilient system will not stop the recovery process when an acceptable state of operation is achieved. We emphasize that the initial goal is to return the system to an acceptable state, but the long-term goal is to use any disturbances as an opportunity to patch weaknesses in the system, make process improvements, and achieve a higher level of operational resilience to better prepare the system for the next disturbance. For example, this could include refining low-voltage ride-through settings for a distributed wind system that disconnected during a low-voltage event and contributed to cascading outages, but had it instead been programmed to ride-through the disturbance for an additional 100 ms, the system would have recovered the voltage. This step is particularly applicable to hazards that were previously unseen or were not well considered during the planning stage.

4.3.2 INCORPORATE LESSONS LEARNED

As part of the recover core function, stakeholders should record and share lessons learned across the system and with external parties to the extent possible. By reflecting upon system performance with respect to an event, the system can ultimately recover to an enhanced state of operation. While that may not occur within the immediate operational timeframe associated with a given event recovery, the longer-term lens allows the system to recover and enhance resilience over time.

Rather than maintaining the system and remaining vulnerable to a specific resilience scenario, this framework emphasizes an evolution of the system over time. Stakeholders should implement lessons learned, both to the system and to the planning process. Implementing lessons learned is not just patching the vulnerability that has been exposed, but also patching the planning processes that led to the event and associated impact. Processes to be improved could appear throughout the framework: from a failure to identify or a mis-prioritization of hazards, to an inaccurate model that did not capture the preparedness of a system, to a detection and adaption real-world process that did not flow as designed, to a recovered state of operation that was insufficient. Opportunities for improvement should be assessed at all levels.

4.3.3 RE-EVALUATE THE PLANNING STAGE

The planning process itself has an iterative component wherein mitigation measures are assessed for their efficacy. The recursive process outlined here is aimed at mitigating future events through continued planning that incorporates operational realities as they occur. The lessons learned from the operational stage should be used in the future, particularly in planning for the next event.

Stakeholders should develop strategic schedules for their resilience planning cycles but remain flexible to adapt those schedules as events necessitate re-evaluation of system characteristics, risks, and potential mitigation measures. For example, a given system may have a plan to re-evaluate their resilience plans every 3 years, but the impact of an unexpected flood event may require an off-cycle iteration to protect against future flood events.

5.0 IMPLEMENTATION EXAMPLE: FRONT-OF-THE-METER DISTRIBUTED WIND

This section provides a brief example of how the framework is intended to be used. The scope of the example is limited, but it is a valuable exercise to walk through the framework process. We focus on the planning stage of resilience. This is where most stakeholders will find the framework most useful, and where the majority of time should be spent to improve operational resilience.

In this example, we consider a front-of-the-meter deployment of distributed wind. Cindy is a planner for a utility co-op that is considering installing a few 100 kW wind turbines. In recent years, the co-op has seen rising transmission congestion, which is raising energy costs for their customers, and building transmission is impractical for the rural co-op. They have also seen more severe thunderstorms in the last few years, and the engineers are concerned that their aging infrastructure is not well equipped to withstand more and more of these storms. Additionally, the board is concerned by a growing number of cyberattacks against the power industry and wants to make sure the co-op's systems are secure. Cindy has been tasked with evaluating the resilience benefit to their system if the turbines are installed. She is going to use the INL resilience framework to study this problem.

1. Identify System Characteristics

The electric cooperative that Cindy works for currently provides electricity to over 4,000 miles of energized line in a 3,000 square mile region. They have more than 200,000 member-consumers. Approximately 70% of their electricity comes from coal-fired power plants. Natural gas accounts for 20%, hydropower 6%, and solar 4% of generated electricity. If the proposed wind turbines are installed, they will account for 5% of the total generation capacity. The turbines would be installed near the local hospital and municipal buildings. These buildings are designated as critical load, and although they have backup diesel generators in the case of an outage, the backup capacity is relatively low.

2. Define System Resilience Goals and Metrics

Cindy meets with engineers and leadership and considers the concerns of the board to identify the primary goals of the electric cooperative: to provide continuous power to as many consumers as possible during the severe summer thunderstorms, and to ensure that the system will not experience operational impact from a cyberattack. Cindy also knows that keeping power on for critical loads is more important than the overall value of load lost. After consulting the "Distributed Wind Resilience Metrics for Electric Energy Delivery Systems" report, she chooses the following metrics to evaluate for the system regardless of the hazard:

- Backup generation available
- Key replacement equipment stockpile
- Ancillary services provided
- Failure Rate
- Rapid voltage changes, voltage level variations, voltage unbalance
- Average customer interruption duration index (CAIDI)
- Load loss damage index
- Critical load identification
- Cost of interruption.

These metrics are specific and backed by data that the co-op already collects. Many are quantitative, but there are some qualitative aspects as well (such as the ancillary services provided and equipment and positioning). These metrics can be adjusted for different time periods and will help Cindy decide whether or not the distributed wind turbines are a good investment.

3. Prioritize Physical and Cyber Hazards

Cindy knows that there is a nearly endless list of potential natural, physical, and cyber hazards that she could consider. However, based on the resilience goals she has identified, she wants to focus on three hazard scenarios:

a. Thunderstorm with severe damage without wind turbines

b. Thunderstorm causing severe damage with wind turbines

c. Cyber-physical mode change attack against distributed wind turbines.

Since the thunderstorm hazard is one that is both increasing in frequency (likelihood) and could have severe consequences, it is a high-risk hazard.

Cindy feels that hackers are unlikely to target her small co-op, but she refers to the "INL Distributed Wind Cybersecurity Guide" and learns that attacks against the energy sector are increasing overall.[17] Some types of attacks may not be targeted at a particular organization, but rather just at equipment that has known vulnerabilities. In fact, there is an argument that a hacker might indeed target a smaller electric organization with attacks like ransomware because they believe that the smaller organizations may not be well prepared for a cyberattack and their assets may not be well defended. Co-ops still have a duty to provide continuous power to their consumers, so if they are hit with ransomware that affects their operational capabilities, they may have to pay the ransom to get systems back online as quickly as possible. Even if the likelihood of this happening to Cindy's co-op is still perceived as relatively low, the consequence may be high, so Cindy decides that this hazard is worth evaluating in detail.

4. Bow-tie Analysis of Specifics Hazards:

a. Thunderstorm with severe damage without wind turbines

Figure 10 summarizes the findings from the bow-tie analysis on the case of a thunderstorm that takes down transmission lines connecting two key coal plants to the system.

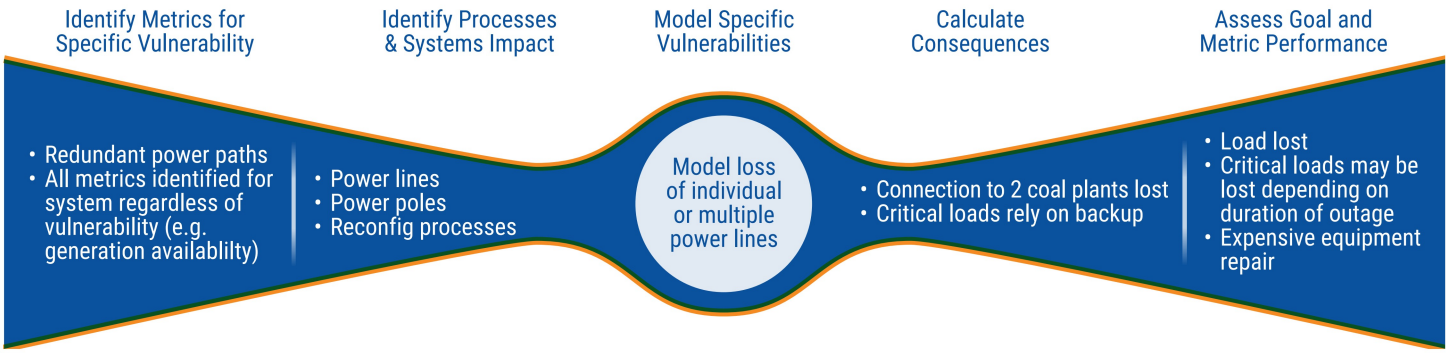

Figure 10. Thunderstorm bow-tie analysis.

[17] *J. Gentle, M. Culler, B. Smith, F. Cleveland, S. Morash, "Cybersecurity Guide for Distributed Wind," Idaho National Laboratory, INL/EXT-21-62264, forthcoming*

Not many metrics are beyond the system-level metrics already identified that are needed to classify this case. Cindy adds a study of redundant power lines to her existing metrics. The assets most at risk during a severe thunderstorm are distribution lines and towers, so she asks the engineers to model outages to these components. Their results show that due to the failure rate of the current equipment and storm risks, the system could lose the connection to two small coal plants. Some customers lose power until the co-op can reconfigure the system to serve the area. Reconfiguration here involves manual switching to import power from adjacent areas while the distribution lines are repaired and the original source of power is restored. Unfortunately, the reconfiguration is only capable of serving part of the outage area. Critical loads like the hospital and municipal buildings rely on their backup generators, but if repairs take too long, the buildings may run out of power. The repairs to the existing equipment combined with the value of load lost makes this an expensive hazard.

b. Thunderstorm causing severe damage with wind turbines.

Figure 11 describes the same scenario as above, but with the proposed wind turbines installed.

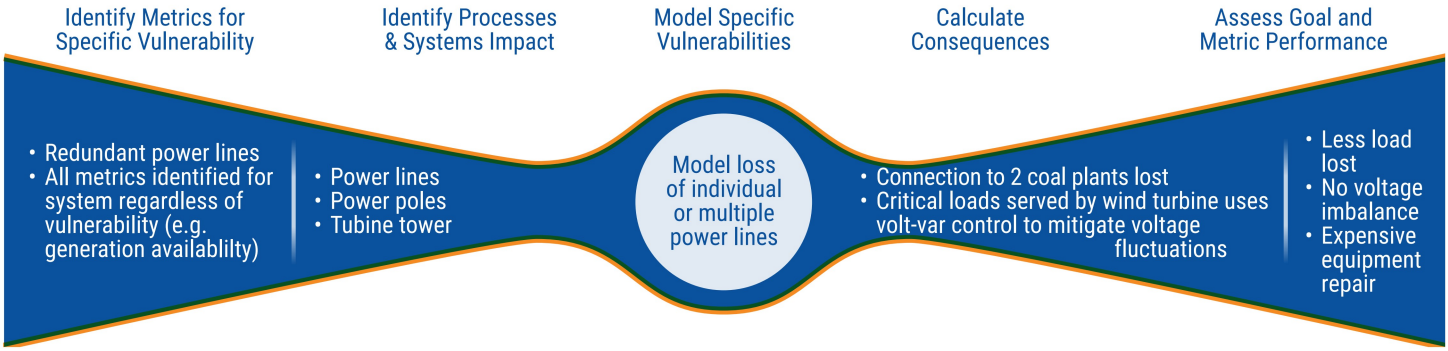

Figure 11. Thunderstorm with wind turbine bow-tie analysis.

In this scenario, the ties to the coal plants are still lost, but wind power can serve much of the local load and supplement the backup generators to ensure they do not run out of power. For completeness, Cindy also models the impacts to a turbine tower during a severe storm but finds that even if power is curtailed to protect against overspeed conditions, the equipment itself is not damaged. During the storm, when the lines go down, the Volt-VAR function of the turbines is able to react quickly and manage voltage fluctuations. Equipment repair may still be costly, but the value of lost load is much less than the previous scenario.

c. Cyber-physical mode change attack against distributed wind turbines

Figure 12 summarizes the findings from the bow-tie analysis on the case of a ransomware attack on the co-op that targets industrial control systems.

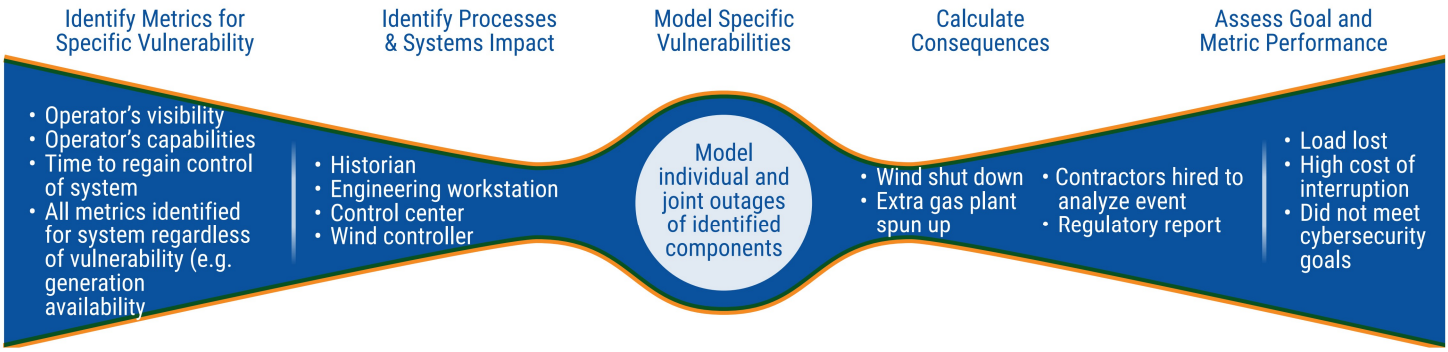

Figure 12. Cyber threat bow-tie analysis.

The metrics relevant for this specific case revolve around whether the system can still be safely operated, if there is operational capability but lack of visibility, or total loss of operational capability. Past attacks indicate that systems including the data historian, an engineering workstation, a control center computer, or even the wind turbine controller could be compromised with ransomware. A successful ransomware attack may not directly compromise the components that generate or deliver power, but if there is a sufficient lack of visibility into the system, either by compromising the historian, engineering workstation, or control center assets, then the system cannot be operated safely. Since safety is the number one priority, the co-op is forced to shut down parts of their system until they can pay for the ransomware to be removed. This is a costly attack, both in the financial costs to pay off the hacker and in the costs and indirect inputs of shutting power off for an hours-to-days time period.

5. Prioritize Hazards and Risk Mitigation Measures

Cindy examines the results from the bow-tie analysis of all the modeled hazards. She sees that the case of a severe thunderstorm with no wind installed has greater consequences than the thunderstorm with wind. She still feels that a cyberattack is unlikely but is surprised by the high impact if a ransomware attack were to occur.

It is clear that adding the wind turbines will help mitigate the thunderstorm hazard and allow the co-op to delay investments in upgrades for a few more years. Cindy wants to make sure that if the turbines are installed, cybersecurity risks are mitigated. She recommends implementing the best practices defined in the INL Distributed Wind Cybersecurity Guide and a comprehensive red team analysis of their system.

6. Evaluate Against All Business Risks

There are costs associated with installing the wind turbines, implementing the cybersecurity best practices, and hiring a team to perform a red team analysis of their systems. However, the alternative to maintain resilience against thunderstorms is to take on system upgrades now that were not planned for another 5-10 years. Some of these changes would need to be implemented before the next storm season, and the added rush would increase the cost. A business case for investing in the turbines will create long-term energy cost savings as well as extend the timeline for performing necessary upgrades.

Although there are cybersecurity risks associated with distributed energy resources (DER) and wind turbines in particular, the recommended implementation of best practices will benefit the whole system, not just the new wind connections. Hiring a penetration testing team is cost-prohibitive for the co-op at this time, but Cindy finds an industrial cybersecurity consultant that they can hire for a short term to help make sure the recommended cybersecurity practices are implemented correctly.

7. Implement Changes and Operate System

Cindy knows that resilience planning is an iterative process, so she wants to make sure that the mitigations she is proposing will improve the system's resilience position.

The system qualities, resilience goals, and identification of hazards steps remain the same at this point. She has the engineering team rerun the cybersecurity bow-tie analysis assuming a stronger security posture, and they are confident that hiring the consultant to help implement best practices will make it more difficult for a ransomware attacker to gain foothold in their critical systems.

Cindy gives the recommendation to install the wind turbines. A year later, the turbines are up and running. She follows up shortly after to make sure that the consultant was hired to help with cybersecurity practices. Her team tells her that the process was successful, and they found many devices on the system that were using default passwords or passwords that were stored in plaintext by the operators. The consultant informed them that even making simple changes to the passwords could help protect them against unauthorized access. The consultant also helped the team ensure that all remote connections to devices were secure.

Cindy checks back in on the project after the most recent storm season. She learns that there were a few line outages during the season, but that power quality was maintained at a higher level than previous years. Inspection of the data revealed that the voltage support provided by the wind turbines helped maintain power quality.

6.0 CONCLUSION

The INL resilience framework is intended to provide a cyclical process for evaluating resilience and building resilience into a system. It provides a roadmap for stakeholders to walk through the process for their own systems and assets, and it frames this roadmap under the core functions of resilience that have been identified through extensive review of literature. The three-tiered approach of resilience stages, resilience core functions, and resilience process steps helps stakeholders understand how evaluations of resilience can change across different stages of a system's lifecycle. We emphasize the first stage, planning, as it is the stage where users make the decisions that will have the greatest impact on the operational stage. Effective planning creates resilient systems.

The implementation example presents a brief demonstration of how to use the framework by applying it to a system with distributed wind. We describe an example system with specific characteristics. We use stakeholder-defined resilience goals to identify hazards, analyze them using the bow-tie method, and develop effective mitigation strategies. As in the rest of this document, the emphasis is on the planning phase and on the cyclical process. Within the planning stage itself, we demonstrate how a user can revisit earlier process steps after reaching the first round of conclusions from the hazard analysis. This cycle can be repeated multiple times before any operational changes are implemented. We also demonstrate how the cyclical process continues after the changes or mitigations have been implemented. There should be regular check-ups on the efficacy of the resilience measures in place, with opportunities to revisit the planning stage, as necessary. This resilience framework can be applied to a variety of systems and applications and serve as a valuable tool to strengthen the resilience of systems with distributed wind, and any EEDS.

ACRONYMS

APT	Advanced Persistent Threat
CAIDI	Consumer Average Interruption Duration Index
EEDS	Electric Energy Delivery System
FLISR	Fault Location, Isolation, and Service Restoration
GMLC	Grid Modernization Laboratory Consortium
IEEE	Institute of Electrical and Electronics Engineers
INL	Idaho National Laboratory
IT	Information Technology
MCDA	Multi-Criteria Decision Analysis
MIRACL	Microgrid, Infrastructure Resilience, and Advanced Controls Launchpad
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
NREL	National Renewable Energy Laboratory
PES	Power and Energy Society (of IEEE)
RISC	Reliability Issue Steering Committee
SCADA	Supervisory Control and Data Acquisition

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

STEVE A. BUKOWSKI PhD, PE
Senior Research, Idaho National Laboratory

KATHERINE A. HOVLAND
Intern, Idaho National Laboratory

SEAN MORASH
EnerNex

AARON F. SNYDER PHD
EneNex

NEIL PLACER
EnerNex

JAKE P. GENTLE
Program Manager, Idaho National Laboratory

RESILIENCE FRAMEWORK
FOR ELECTRIC ENERGY DELIVERY SYSTEMS

INL/EXT-21-62326
Revision 1
July 2021

Idaho National Laboratory