U.S. DEPARTMENT OF ENERGY

Cybersecurity Considerations for Distributed Energy Resources on the U.S. Electric Grid

October 2022

This document was prepared by the U.S. Department of Energy's Office of Cybersecurity, Energy Security, and Emergency Response and the Office of Energy Efficiency and Renewable Energy.

TABLE OF CONTENTS

1 Summary

To address the impacts of climate change, the U.S. electric grid will be undergoing significant changes by integrating clean energy resources such as solar and wind. These efforts will be accelerated with the recent passage of the Infrastructure Investment and Jobs Act[1] and the Inflation Reduction Act.[2] Furthermore, electric customers will continue to adopt intelligent energy devices, including smart lighting and thermostats, which will be able to communicate with rooftop solar, electric vehicles, and more. These efforts will be critical for combating climate change and providing resilience benefits before, during, and after major events. However, as the U.S. electric grid undergoes these changes, it will be important to ensure that cybersecurity is incorporated into new devices, systems, and infrastructure and that "security by design" is a core component of these systems.

As such, this report provides an overview of cybersecurity considerations that should be considered by the electric sector, including utilities and distributed energy resources (DER) operators, providers, integrators, developers, and vendors (collectively, "the DER industry"), as well as policymakers as we embark on this transformational change to the U.S. electric grid. This report is not meant to be a comprehensive review of cybersecurity considerations in the DER industry, but rather encourage a dialogue and further conversations between industry and government stakeholders.

The DER industry must partner with energy sector and government efforts to address these challenges over the next decade. This means ensuring that new controls and software interfaces for these smart devices are cybersecure and standardized to mitigate emerging cyber risks. Securing DER also will require addressing the varying ways that DER operate, including their different controls and the fact that owner/operator entities do not have a defined role in securing the grid. Other challenges in addressing DER include assessing how DER cyberattacks could affect grid operations, creating a DER trust model, and extending supply chain security efforts to include DER.

Existing cybersecurity standards and best practices, such as multifactor authentication, endpoint detection and response, encryption, and a skilled and empowered security team, may need to be refined for specific DER deployment use cases. When implementing cybersecurity requirements, grid and DER planners should build cyber defenses with the goal of surviving an attack while maintaining critical functionality. Future DER systems must be designed, built, and operated in an enforced zero-trust model where data is validated using cryptographically secure mechanisms informed by standards, testing, and vulnerability assessments.

Broad industry involvement is key to the development, approval, and implementation of robust DER cybersecurity standards. The U.S. Department of Energy (DOE) will continue to engage DER operators; vendors; developers; owners; aggregators; utilities; and other Federal, state, and local partners to ensure the wide adoption of the standards and best practices. DOE also will move beyond compliance

[1] Infrastructure Investment and Jobs Act, Pub. L. 117-58. https://www.congress.gov/bill/117th-congress/house-bill/3684/text

[2] Inflation Reduction Act of 2022, Pub. L. 117-169 https://www.congress.gov/bill/117th-congress/house-bill/5376/text

by working with university, National Laboratory, and industry researchers on next generation DER defenses, including cyber by design, to ensure security in a decarbonized grid.

2 Acknowledgments

DOE's Office of Cybersecurity, Energy Security, and Emergency Response and the Office of Energy Efficiency and Renewable Energy led the development of this report. DOE would like to acknowledge the National Renewable Energy Laboratory and Sandia National Laboratories for their significant contributions as well.

The final version of this report is the sole responsibility of DOE. The participation of external reviewers does not imply that they, or their respective organizations, either agree or disagree with the findings of this report.

3 Introduction

Over the coming decades, electric customers will continue adopting intelligent energy devices, from smart lighting and thermostats to electric vehicles and rooftop solar photovoltaics.[3] Taken together, these distributed energy resources (DER) offer homes and businesses more choices and control of their energy; encourage clean energy practices to combat climate change; and provide resilience benefits before, during, and after major disaster events. When coupled with energy storage, DER can provide emergency power during grid outages to support community resilience.

Definition of DER

Definitions of DER have varied widely; however, for this report, DER are small-scale power generation, flexible load, or storage technologies (typically from 1 kilowatt to 10,000 kilowatts) that can provide an alternative to, or an enhancement of, the traditional electric power system.

These can be located on an electric utility's distribution system, a subsystem of the utility's distribution system, or behind a customer's meter. They may include electric storage, variable generation, distributed generation, demand response, energy efficiency, thermal storage, or electric vehicles and their charging equipment. The main focus of this report is DER from solar, renewables, and battery storage.

However, the high deployment of solar energy and other DER pose emerging cybersecurity challenges for the electric grid. DER already provide many automated features and their deployment is coupled with transitioning to a digitally interconnected power grid. Cyber attackers frequently evolve their techniques to attack information and operational technology systems.

Addressing cybersecurity challenges over the next decade must be a key priority for the DER industry, which include both utilities and DER owners, operators, developers, software and hardware vendors, and aggregators. The goal is to mitigate current risks to the energy grid and to be prepared for the threats and vulnerabilities of the future. These mitigations form the base of a new framework for defining the defensive posture of the future grid.

3.1 Report Purpose and Scope

This report intends to explain the high-level cybersecurity challenges associated with grid modernization, DER deployment, cybersecurity trends, and the potential risks to the electric grid over the next 10 years. It focuses on DER connected at the distribution level that are smaller than 20 megawatts and often installed behind a customer's meter. The report describes various approaches for the assessment of DER cybersecurity risks and provides recommendations on how to incorporate cybersecurity best practices and minimum requirements for DER deployment. Supplemental technical information supporting the main report, such as DER grid support functions and threat scenarios, is provided in Appendices A and B, respectively.

[3] *See* National Renewable Energy Laboratory (2018). Electrification Futures Study: Scenarios of Electric Technology Adoption and Power Consumption for the United States. https://www.nrel.gov/docs/fy18osti/71500.pdf

See also U.S. Department of Energy, Office of Energy Efficiency and Renewable Energy. (September 2021). Solar Futures Study. https://www.energy.gov/sites/default/files/2021-09/Solar%20Futures%20Study.pdf

3.2 The Department of Energy's Approach to DER Cybersecurity Challenges

The U.S. Department of Energy's (DOE) Office of Cybersecurity, Energy Security, and Emergency Response (CESER) is prioritizing advanced cyber discovery, vulnerability assessment, and rapid risk mitigation.[4] CESER leads work on security and resilience with utility and electric sector engagement with partnerships among a broad set of stakeholders, including all levels of government, private industry, and academia. CESER also works with DOE's Office of Electricity and DOE's Office of Energy Efficiency and Renewable Energy (EERE). Electric utilities also are concerned about cybersecurity threats to electric power infrastructure and are taking action to improve the cybersecurity of their equipment. DOE's EERE also has made it a priority to accelerate cybersecurity research and development to strengthen EERE technologies and systems that are critical to renewable energy, manufacturing, buildings, and transportation—all of which are increasingly interconnected and vulnerable to cyberattack.[5]

State, local, tribal, and territorial entities have a role in ensuring that utilities, renewables developers, and DER aggregators operating in their jurisdictions are incentivized, required, or encouraged to address cybersecurity concerns. This interaction is much the same as they would incentivize, require, or encourage sidewalks, proper watershed construction, anti-pollution efforts, and other public good requirements.

CESER has partnered with EERE, in particular the Solar Energy Technologies Office, to assess and address the emerging cybersecurity challenges from solar and other DER. A cyberattack on today's DER may have a limited, local impact on grid operations; however, as more solar and other DER are connected to the grid that are dependent upon digital communications and controls, the risk of cyberattack rises with the potential for a broader impact. In some regions with high solar and DER deployment, cybersecurity has already become a high-priority issue for grid planners and operators. The tipping point for each locality will differ; however, all providers of DER infrastructure and services should be aware of and plan for this eventuality as a threat to their business models.

Finally, DOE Secretary Jennifer M. Granholm has asked CESER to coordinate cybersecurity across the applied energy and science offices within the Department to ensure that cybersecurity is included from ideation to deployment in the relevant research, development, and deployment efforts occurring to accelerate clean energy systems in the United States.

---

[4] CESER. (2021). CESER Blueprint, January 2021.
https://www.energy.gov/sites/prod/files/2021/01/f82/CESER%20Blueprint%202021.pdf

[5] U.S. Cyberspace Solarium Commission Report. March 2020.
https://www.cybersolarium.org/reports-and-white-papers
[Direct Link to report: http://www.fdd.org/wp-content/uploads/2020/03/CSC-Final-Report.pdf]
[Full report MD5: 75ad4a1adcfe304a03ffb1f916b0d6a8]

4 Trends in Grid Transformation and Securing Distributed Energy

As noted in the North American Electric Reliability Corporation's (NERC) 2020 Long-Term Reliability Assessment, the electric grid is undergoing significant, rapid transformation.[6] Transformation trends include deploying smart grid technologies; supporting more engaged customers; promoting affordable grid modernization; addressing environmental goals; and redefining how the electric system is designed, built, and operated. The deployment of variable generation, primarily wind and solar, is leading this transformation and is associated with retiring conventional generation such that transmission grids are fundamentally planned and operated differently, a move from the physics of large spinning generation to power systems dominated by inverter-based resources (IBR). Energy storage, frequently coupled with wind and solar, is also just starting to be extensively deployed. This is in contrast to nearly the entire history of the electric grid, where little to no electricity was stored.

NERC Long-Term Reliability Assessment (2020)

NERC's 2020 Long-Term Reliability Assessment does not assess reliability impacts due to physical and cyber risk but does highlight the power system transformation that is underway and presenting different reliability challenges for grid planners and operators:

"The electricity sector is undergoing significant changes that are unprecedented in both transformational nature and rapid pace. Such extraordinary evolution presents new challenges and opportunities for reliability, resilience, and security. Advances in technology, customer preferences, policies, and market forces are altering the generation resource mix and challenging the conventional understanding of the reliability role of baseload power that was traditionally provided by large, centralized generating units. While efforts are underway to address these risks, the management of reliability, resilience, and security will require increased focus by all.

The addition of variable energy resources, primarily wind and solar, and the retirement of conventional generation is fundamentally changing how the [bulk power system] is planned and operated. Resource planners must consider greater uncertainty across the resource fleet as well as uncertainty in electricity demand that is increasingly being affected by demand-side resources. As a result, reserve margins and capacity-based estimates can give a false sense of comfort and need to be supplemented with energy adequacy assessments. Energy assessments are key to understanding the reliability needs of a future [bulk power system] and are presented in [the Long-Term Reliability Assessment] report."

While much of this transformation is occurring on the transmission and sub-transmission scale, significant change is occurring at the grid edge with home and business owners installing DER. DER deployment is expected to grow from approximately 90 gigawatts (GW) today to approximately 380 GW by 2025.[7] Nearly half of DER today are solar photovoltaic (PV) systems, with millions of PV arrays atop homes across the country.

[6] North American Electric Reliability Corporation. (December 2020). 2020 Long-Term Reliability Assessment. https://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/NERC_LTRA_2020.pdf

[7] For example, Wood Mackenzie predicts that DER capacity will reach 387 GW by 2025. https://www.woodmac.com/news/editorial/der-growth-united-states/

DER present emerging cybersecurity challenges for the reliability of the electric power grid, and a key challenge is that utilities do not own and often do not directly operate them. Historically, utilities were the primary entity for securing the electric power grid. As DER connect to the grid, the emerging DER industry also will bear responsibility for securing the DER they manufacture, deploy, maintain, and operate. As many DER industry members have not been part of the historical partnerships and oversight that operated and maintained the power grid, electric power reliability, and security requirements, the responsibility needs to be established for this emerging industry.

In addition to this grid transformation, the rapid evolution of ransomware threats, converging information technology (IT) and operations technology (OT) systems, increasing cloud-based communication and control systems, and expanding automation to remove a human operator-in-the-loop also create new cybersecurity challenges. For example, the capability to provide autonomous grid support functions[8] will be required within the next 2 to 3 years on new solar and DER, with the larger scale solar and wind installations already being designed for remote or autonomous operations today.

Securing DER deployment in the future may make communities more resilient, efficient, and effective as consumers and producers of energy. However, deploying insecure DER introduces risks to these net community benefits and also may present a risk to the electric power grid. DER deployed without security could slow the goal of combating climate change and impact the reliable supply of energy.

4.1 A Digital-Controlled Electric Power Resource

Most DER, such as solar photovoltaic systems, battery energy storage, and variable speed pumps and motors, are different from traditional generation in one essential way—they consist of solid-state inverters that produce output in sync with the grid. These inverters use software and power electronics to identify the state of the grid, determine the best signal fit for the situation, and distribute power at that best signal. Because the response is software-driven and digital-controlled, output power is configurable. Energy storage, for instance, can be configured to inject and absorb real and reactive power to provide essential reliability services.

These benefits come with responsibilities as well. While the proper application of these capabilities can provide reliability and stability improvements, the improper application (such as from a cyberattack) could provide reliability and stability declines.

DER are subject to the performance requirements of the Institute of Electrical and Electronics Engineers (IEEE) Standard 1547-2018, and each DER is certified for conformity to interconnect with the grid. Large IBR that are connected to transmission and sub-transmission systems will be subject to the new IEEE Standard P2800—the IEEE Draft Standard for Interconnection and Interoperability of Inverter-Based Resources Interconnecting with Associated Transmission Electric Power Systems.

DER location in the distribution grid permits a response to local grid events with local changes, offering unparalleled ability to provide grid reliability. These capabilities and the response to grid conditions generally are based on the grid support functionality defined in IEEE Standard 1547 for DER.

[8] Institute of Electrical and Electronics Engineers (IEEE) Standard 1547-2018 requires DER to actively support voltage and frequency. DER must ride-through abnormal voltage or frequency events. Appendix A in this report includes high-level descriptions of these capabilities.

DER and large IBR differ from traditional generation because the physics involved with delivering power to the grid for each are entirely different. Traditional generation uses a direct magnetic coupling with a large rotating turbine to generate synchronized output. The physics of this connection have been part of power engineering design since alternating current generators were commercialized in the 1880s.

Modern control and protection systems evolved around these rotating generators, fueled by 130 years of investment by government, utility, and scientific interest in making electricity more reliable, safe, and cost-effective. The behavior of this system is well understood, and the physics have self-correcting properties when paired with the generator's control system. Generators that begin to exhibit suboptimal behavior are corrected by the rest of the grid, by their own rotating electromagnetics, or by being taken offline by protection mechanisms. Rooted in well-defined physics and generic models, these behavioral rules govern the electric power grid.

DER and large IBR, such as wind and solar, are replacing traditional generation, with enhanced performance[9] due to their solid-state power electronics and software control capabilities. This permits them to be used in unique ways to address specific electric system problems, coupled with their location in the distribution grid. This also means that traditional assumptions regarding grid physics will become less valid as IBR and DER adoption increases. IBR and DER's lack of spinning mass and behavior rooted in power electronics and software means that new control and stability[10] assumptions will be required in routine power studies conducted by utilities. DER deployment is coupled with transitioning to a digital power grid, and the underlying software requires cybersecurity and standardization to mitigate the risks associated with software enterprises.

4.2 A Focus on Grid Automation

A grid that is heavily diffused with DER will behave significantly different from a traditional grid. Traditional grids are primarily built to be supplied from the bulk transmission system, supplying power to consumers of electric power at the edge of the grid. This greatly simplifies the design of these grids as they essentially operated as one-way streets where the power only flows down from the larger system into the smaller distribution systems.

However, DER now supply energy from the edge of the grid throughout the local distribution grid and even up into the transmission grid. This results in new two-way streets with the associated additional complexity from figurative stop signs, streetlights, and lane markers. This level of electrical bidirectionality requires new designs, controls, and protection schemes at the distribution level where they did not exist before.

To automate this bidirectional power flow, grid operators are starting to deploy new grid technology, from smarter transformers to advanced distribution management systems, which include the ability to dispatch DER.

---

[9] National Renewable Energy Laboratory. (March 2017). Demonstration of Essential Reliability Services by a 300-MW Solar Photovoltaic Power Plant. https://www.nrel.gov/docs/fy17osti/67799.pdf

[10] *See, for instance,* Hatziargyriou, Nikos, et al. "Definition and classification of power system stability revisited & extended." IEEE Transactions on Power Systems. (2020). doi: 10.1109/TPWRS.2020.3041774

In terms of reliability, the most important change likely will be the addition of adaptive protection to distribution grid planning and design activities, where the protection mechanisms are designed and built to coordinate between each other to better react to the more numerous conditions found in DER grids. Where utilities anticipate (or where aggregators and owners specify) DER will be deployed, new studies will reveal the extent of the automation and protection additions. Securing high-level grid automation systems will require cyber defenses to maintain these capabilities when many DER could be compromised.

4.3 New Roles for a New Market

As part of the transition to a more DER-based power grid, new players will be entering the electric power business. DER aggregators, owners, and vendors are expected to play a greatly expanded role in how resources are operated, maintained, and connected to the larger power grid.

The recent Federal Energy Regulatory Commission Order 2222 aims to enable DER aggregators to compete in all regional organized wholesale electric markets.[11] This differs from traditional power market operations, where utilities and independent power producers are the primary competitors in power markets. These new DER roles are built on a core realization that future DER installations may defer or mitigate expensive grid upgrades but could be more numerous than traditional generation. These DER installations will be managed in a different manner from traditional power operations due to their dispersed nature, resulting in a heavy reliance on telecommunications for remote control and monitoring (and very likely the internet).

For example, fixing software on a traditional generator is a complex, multistage process handled by the generator's owner. Testing, evaluation, and risk management are all necessary to ensure that the generator continues to operate, and the fix is generally handled on-site by responsible personnel at a time of their choosing. Only the on-site systems must be patched, and personnel are available to fix any issues discovered during the patching process with regard to directly handling the systems themselves.

In contrast, if an aggregator determines that a software fix is necessary on DER systems, they must apply that fix to hundreds or thousands of different systems in many places, which is costly and requires many personnel. The software patch process likely will resemble a cellular carrier releasing a fix for customer phone operating systems. The aggregator may need to interface with numerous DER owners/operators to apply that fix and work out an appropriate plan with the grid operator to ensure reliability during the process, especially if it involves a percentage of failed updates that may cause loss of power output. A DER owner/operator may have their own requirements for their installations as well, requiring negotiation with the aggregator. Lastly, the software fix is likely produced by the DER vendor, who may have or want capability for mass system updates outside the direct control of aggregators and owners/operators.

[11] U.S. Department of Energy (DOE) Electricity Advisory Committee. (April 2021). FERC Order 2222, Recommendations for the U.S. Department of Energy—Outline. https://www.energy.gov/sites/default/files/2021-04/EAC%20FERC%20Order%202222%20Recommendations_Approved.pdf

Coordination and cooperation between these roles are vital for maintaining grid reliability, as a poorly executed mass update could impact the reliability of electric power for customers if it interrupts, changes its response/characteristics, or affects a significant output from DER. Securely patching DER will likewise be needed to mitigate supply chain cyberattacks. And all these operations will require cybersecurity measures to ensure that attackers cannot arbitrarily update DER systems, in large part because updates have become a vector for compromise.

4.4 Cybersecurity Trends

The past 20 years have seen the threat from malicious cyber attackers increase substantially, powered by new incentives for conducting attacks, such as drawing a ransom payment. Financial and political incentives for cyberattacks provide malicious groups with motivation to improve their tactics, identify new valuation schemes, and develop new tools to extort victims. This trend in malicious activity is unlikely to abate and likely will see an increase over the next two decades.

The overall expansion of the cybersecurity threat is a rising tide for all sectors; however, it is especially important to the energy sector.[12] Numerous critical infrastructures and citizens rely on the electric power grid for their products, services, and everyday life, and this reliance results in the consequences of cyberattacks on electric power infrastructure reaching farther than the immediate consumers of the electricity.

4.4.1 Cyberattacks at the Grid-Supply Scale

The future of DER on the electric grid will involve hundreds of thousands of distributed resources providing many thousands of megawatts, all operated by an overarching system that interfaces with hierarchical grid operations. Today, cyber compromise of a single or even multiple DER is inconvenient to the owner/operator of that resource, but generally does not register to a grid operator concerned with orders of magnitude more resource supply.[13] However, if a cyberattack could affect many thousands or more DER or the overarching systems controlling DER, then such an attack would reach a level that concerns grid operators. While that attack capability and potential impact are currently low for most regions,[14] the trendline for cyber attackers is that they increase their capabilities over time and target new systems in novel ways.

[12] Annual Threat Assessment of the U.S. Intelligence Community. U.S. Director of National Intelligence, 9 Apr. 2021. https://www.dni.gov/files/ODNI/documents/assessments/ATA-2021-Unclassified-Report.pdf

[13] A trend demonstrating greater renewables and DER importance is already being expressed in areas of North Carolina and California, which have high renewables penetration relative to conventional generation. See North American Electric Reliability Corporation. (December 2020). 2020 Long-Term Reliability Assessment. Potential Demand and Resource Challenges for System Operators, pp. 45–46, and the Regional Assessment Dashboard cards. https://www.nerc.com/pa/RAPA/ra/Reliability%20Assessments%20DL/NERC_LTRA_2020.pdf

[14] Impact depends on a variety of factors. While generally the impact is low in North America, there are areas that may have DER installations that exceed peak load in certain circumstances and/or that are sourced from a small number of DER vendors, increasing the potential impact from DER cyberattacks.

Grid owners and operators have several reasons to be concerned from a cybersecurity perspective, most reasons are directly tied to the number of DER and the total amount of power that can be influenced by a cyberattack. While the critical number varies depending on the size of DER installations, real-time load conditions on the grid, the number and geographical distribution of those installations, and the communication/trust relationships, approximately 30% of DER deployment relative to peak load begins to show infrequent but potential grid-level consequences.[15]

At these moderate deployment levels and to disrupt grid operations, DER cyberattacks would have to be coordinated with periods when the compromised DER could cause grid equipment to operate outside of its intended range. Power flow studies are used to analyze these conditions. DER cyber risk studies must consider the opportunities for and threat of attackers compromising a portion of DER relative to current load conditions and other non-compromised DER and grid resources. Developing the scope, method, and results for cyber risk studies associated with DER are a priority area of study.

The list of potential attack vectors for DER below is not exhaustive. Other more common attack vectors, such as phishing, ransomware, denial-of-service, Trojan horses, data-in-flight and man-in-the-middle attacks, malicious rootkit attacks, and zero-day exploits, also could contribute as links in a long attack chain that result in DER compromise.

- DER ransomware – Attackers take control of DER components and encrypt or disrupt operational software until a ransom is paid. While this attack on a single DER may be a financial frustration to a DER owner, it is not likely to be noticed by a grid operator. However, an attack on large percentages of DER systems or a DER aggregator could have the potential to disrupt grid operations.
- DER supply chain compromise – An attack on an aggregator, vendor, or other responsible party could influence the operations of DER that take direction or receive updates from that responsible party.
- DER botnet – An attack or series of attacks infecting enough DER with malware to enable the attacker to create unanticipated power swings, cause outages, or contribute to grid instability on a larger scale than previously possible.
- DER worm – An attack on a DER system might start with a single DER but could propagate to higher level systems belonging to a grid operator or aggregator or laterally to other DER systems, giving the attacker more influence over supervisory controls than exploitation of a single DER. A DER worm, for instance, may enable an attacker to compromise an aggregator's distributed energy resource management system (DERMS). The compromised DERMS may then send out a false grid services command to the uncompromised DER and instigate power instability issues.

[15] It is useful to think of high DER penetration in terms of the ratio of instantaneous DER generation to instantaneous load (e.g., a grid that gets 15% of its annual generation from rooftop solar may, on a lightly loaded fall day, see solar generation exceed 50% of instantaneous load). Note that minimum load is typically 30% of peak load. This percentage could be higher or lower depending on load conditions and the specific power system. *See* McAllister, Richard, David Manning, Lori Bird, Michael Coddington, and Christina Volpi. (2019). New Approaches to Distributed PV Interconnection: Implementation Considerations for Addressing Emerging Issues. Golden, CO: National Renewable Energy Laboratory. NREL/TP-6A20-72038. https://www.nrel.gov/docs/fy19osti/72038.pdf

These attacks are illustrative of the potential for compromised DER to affect grid operations. A sufficiently large DER cyberattack could disrupt grid conditions and even trigger grid protection that could cause a localized, temporary blackout. Qualifying DER attack assessments involves analyzing industrial control system kill chain tactics and techniques that extend to supervisory systems for the DER aggregator and utility.

The potential for these types of attacks is best evaluated by identifying high-level security objectives, identifying potential security threats, and then looking at the attack vectors through a combination of assessing the attack likelihood and opportunity[16] combined with its potential impact. (See Appendix B in this report for DER threat scenarios.) The combination of likelihood and opportunity with potential impact will help define high-, medium-, and low-risk cyberattack scenarios. Given that energy systems are critical infrastructure, impacts will need to be evaluated for broader societal implications, such as safety (e.g., workforce, public, ecological), reputational (loss of trust and loss of confidence), financial (e.g., economic, consumer and business burden, utility financials), operational (e.g., grid operations, other generation), and critical infrastructure resiliency (e.g., bulk power system, major blackout, cascading effects on other sectors such as transportation or food supply).

To evaluate the risks for a DER cyberattack, understanding the grid architecture and DER aggregator security posture is crucial. Compromised access to DER may, for example, allow malware movement within a DER system, or allow compromise to affect the aggregator via upstream communications. This level of access could be used by attackers to manipulate area power system controls, similar to the 2016 attack in Ukraine (although, in that case, not through DER).[17] Poorly secured DER could serve as an entry point to manipulate wider grid operation systems, either DER aggregator control systems or even a utility's control systems. Understanding this architecture, seen in Figure 1, highlights the DER cybersecurity stakeholders to consider for securing end-to-end DER systems.

4.4.2 Implied Trust Collides with Attacker Ingenuity

In electric power control systems today, an implied trust relationship is common for the communications infrastructure. If industrial systems can talk to one another, they trust each other to provide accurate information and commands. Attackers who have inserted themselves into this trust relationship can poison these systems, causing them to act counter to reliability and resilience requirements.

[16] This report uses attack "opportunity" in combination with likelihood because cyberattacks take advantage of vulnerabilities in systems and people, and do not adhere to a statistical model of likelihood alone (such as with a tornado, or other natural disaster) because targeting is conducted by the attacker.

[17] In December 2016, Russian nation-state cyber attackers infiltrated several power-utility networks in Ukraine, accessed power systems and devices, and turned off power to many electric power customers by the deployment of specialized malware. *See* Cybersecurity and Infrastructure Security Agency. (February 25, 2016). ICS Alert (IR-ALERT-H-16-056-01): Cyber-Attack Against Ukrainian Critical Infrastructure. https://us-cert.cisa.gov/ics/alerts/IR-ALERT-H-16-056-01

The implied trust relationship is not a good model for DER systems. The sheer scale of DER deployment, the wide range of communications options, and the level of access required by various stakeholders will show implied trust does not scale in a resilient manner for DER. Compromises to an implied trust relationship are difficult to discern or reliably block.

To meet grid modernization requirements, information received by a DER system needs to be acted upon in real time due to the physics of electricity and the variability of supply associated with many DER. Given the potential for large DER deployments in the future, there likely is limited capability for human intervention in this process, making the fast transfer of data and automated action on that data a high priority. The trust required between elements of a DER system would be a situation ripe for abuse by an attacker if built on the current grid operations implied trust model.

Figure 1[18] shows DER communications architecture, where DER may communicate directly with the utility DER control server (shown with blue lines) or via public internet/cloud communications (shown with purple lines) that may or may not go through a DER aggregator. The DER communications domain is shown in orange. If aggregators are used, their operational systems domain is shown in green, and the utility's grid operations systems are shown in blue.

To be resilient against attacks, DER systems should be designed, built, and operated by means of an enforced zero-trust model, where data and commands are validated using cryptographically secure mechanisms informed by standards, testing, and vulnerability assessment. DER deployments adhering to zero-trust principles would take specified action only when that direction was based on verified input, otherwise it would fall back on local control algorithms. Access to influence DER systems is denied by default and is explicitly granted to those who hold the responsibility and accountability for managing and operating the system.

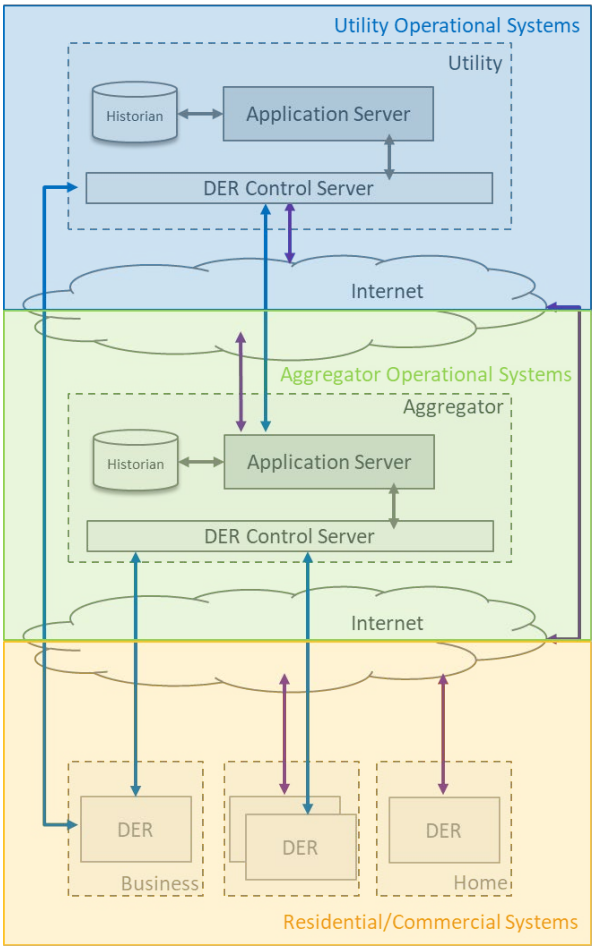

Figure 1. High-Level DER Communications Infrastructure

[18] Figure from NREL and SETO Presentation, Cybersecurity of DER Systems – Cybersecurity Training for State Commissions. https://www.nrel.gov/docs/fy22osti/80666.pdf

4.4.3 Cybersecurity Threats as a Design Consideration

The energy sector has seen an increase in the frequency and severity of cyberattacks that are largely independent of historical DER deployment. Advanced attackers are already capable and resourced for current power grid systems and are anticipated to add to their capability with DER understanding. There is a converging risk associated with sophisticated attacks on power grid systems and expansion of the attack surface that DER requires. Understanding and addressing that risk are critical to establishing defense systems for the modern grid.

It is cheaper and more effective to design cybersecurity measures early in the process rather than experience the consequences of inadequate security and fix things later. As seen in Figure 2, security is the foundation for critical energy infrastructure, and DER must contribute to a more secure and resilient grid. The electric grid is a set of interconnected machines managed by professional operators, and DER connected at the grid edge also must align to wide-area power system reliability, safety, and security operations requirements. Measured defenses also must consider tiered requirements as balancing risk with the potential impact from compromise will be an essential industry concern.

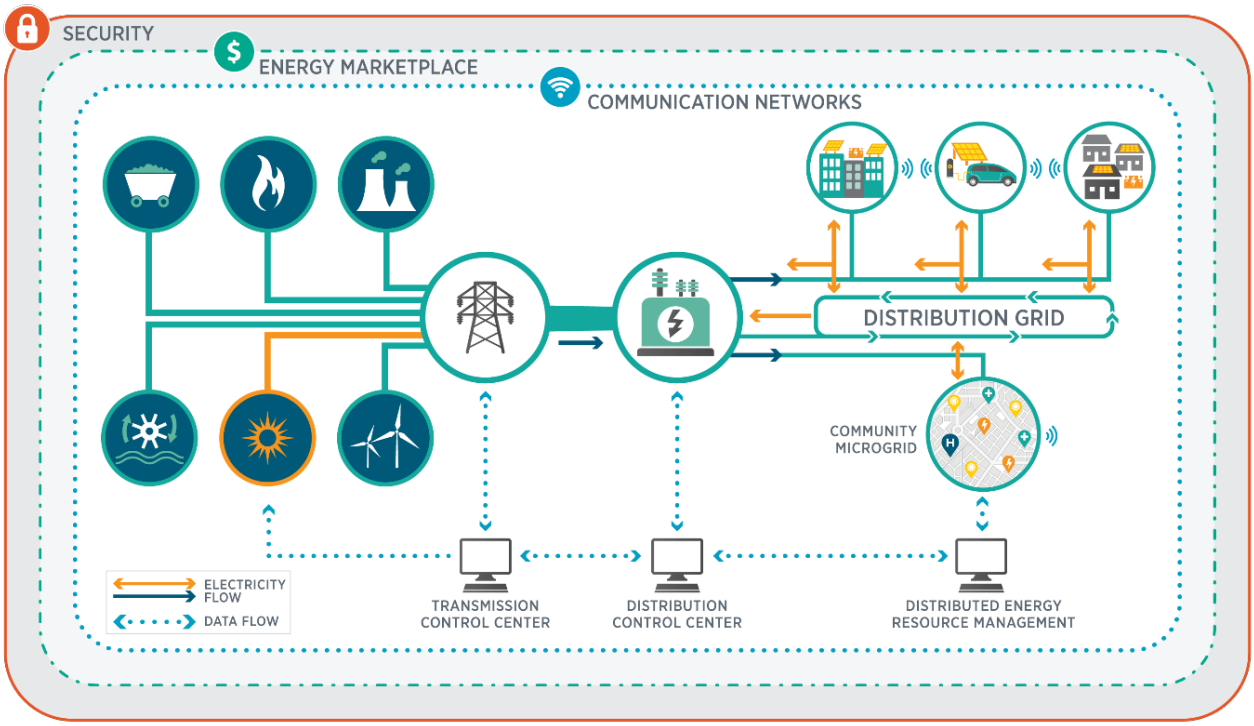

Figure 2. DER Are Interconnected to the Grid and Built from a Security Foundation[1]

4.4.4 Experimentation and Exploitation of Operational Technology

Another industry trend is increased attacker experimentation and exploitation targeting OT systems. For example, advanced attackers shut down power grids in Ukraine by manual means in December 2015 and by specialized malware targeting electric substations in December 2016.[19] In 2017, an attacker was discovered interfacing directly with the industrial systems responsible for petrochemical safety in Saudi Arabia to install malicious software that would permit undetectable alterations.[20] The malicious modifications, dubbed the TRITON/TRISYS malware, were found only when the attacker inadvertently triggered the safety system, leading to an investigation that identified the malware.

Attacker Sophistication and Threat Model

Neither levels of attacker sophistication nor detailed threat profiles are covered in this report. This report uses generalities and trends to describe the threat anticipated to emerge over the next 20 years rather than exact descriptions of specific threats to power systems and grids. This approach permits DOE to summarize the landscape for planning; however, more detailed DER threat models are needed. A threat model incorporates attacker resources, capabilities, and commitments relative to their intensity, stealth, applied time, expert personnel, IT knowledge, and power systems knowledge. Without models to use as a basis for security design, threats could emerge that leverage security weaknesses in DER and utility systems for high impact. (See Appendix B in this report for DER threat scenarios.)

Traditional attack vectors, such as insider threats, poor data security, and access controls, are relevant to new grid technologies. In addition, distribution rooftop solar and other DER present new attack potential, can aggregate to magnitudes like traditional resources, and will challenge traditional cyber defense postures through their administration by many different parties.

4.4.5 Supply Chain Threats

As cybersecurity defenses have evolved over the past 20 years, attackers have changed their tactics at the same rate. Many private and public sector entities have good security practices, including the use of perimeter defenses, defense in depth, and ubiquitous monitoring. In response, attackers have shifted focus to the suppliers of hardware and software for these entities, seeking to add backdoor capabilities that permit unauthorized access and control. In these watering hole attacks, perpetrators leverage trusted supplier relationships to plant backdoors, weaken security measures, and change the underlying functionality of legitimate software to suit their needs.

---

[19] *See* Cybersecurity and Infrastructure Security Agency. (February 25, 2016). ICS Alert (IR-ALERT-H-16-056-01): Cyber-Attack Against Ukrainian Critical Infrastructure. https://us-cert.cisa.gov/ics/alerts/IR-ALERT-H-16-056-01

[20] TRISIS Malware – Analysis of Safety System Targeted Malware, version 1.20171213. Dragos. https://www.dragos.com/wp-content/uploads/TRISIS-01.pdf

Supply chain attacks will continue to be a major theme in cybersecurity. An attacker also could compromise a development environment to taint new software as it comes out of production or compromise authorized updates for software or hardware already deployed.[21] Or an advanced attacker, for instance, may add a chip onto the printed circuit board design that duplicates data in memory and sends it to the attacker, giving the attacker credentials and login data to the compromised devices.

Much like the broader internet-of-things devices, when these attacks are smaller in scale and impact, they are a mere annoyance. However, assuming large-scale DER deployment and sufficient aggregate or supervisory control risks, trust in supply chain hardware and software partners will be necessary.

SolarWinds Attack

In December 2020, law enforcement and private sector security professionals identified an advanced supply chain compromise affecting the SolarWinds Orion series of products. Orion is a network monitoring and asset management software used by thousands of companies to manage their networks and systems.

The attacker compromised SolarWinds as early as March 2020, inserting backdoor code into a digitally signed component of the Orion software. This backdoor code contacted web-based servers controlled by the attacker. This compromised the SolarWinds development system, which was altered to add the backdoor code at a process step that would result in SolarWinds cryptographically signing to the authenticity of the maliciously modified code.

This sophisticated supply chain attack by an advanced adversary affected at least nine Federal agencies and ~100 private sector companies. The attackers leveraged this access to burrow into victim networks with more advanced tools, gaining additional access to privileged documents and emails, and installing additional remote command capabilities outside the initial Orion vector. The impact of the SolarWinds compromise is still being assessed; however, it will be a case study for supply chain attackers for years to come.

As DER deployments grow, securing them will require methods and ways of understanding the supply chain associated with their creation; development of standards to secure that supply; and assurances that suppliers, aggregators, and utilities are assigned the appropriate responsibility and accountability for securing their hardware and software. Supply chain standards are the main driver for assigning this responsibility and accountability.

4.4.6 Threat Stratification and Speed of Compromise

Not all cybersecurity threats are equal; threat groups have varied funding and levels of technical sophistication. While some operate at very high levels of competence and targeting, others conduct their operations quickly and cheaply by leveraging the exploits, tactics, and control mechanisms used (and often discarded) by higher caliber attackers. This trend is particularly prevalent in ransomware activities, where lower tier attackers will leverage a recently exposed exploit to gain a foothold and

[21] Supply Chain Compromise. Alert: APT Compromise of Government Agencies, Critical Infrastructure and Private Sector Organizations. Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/supply-chain-compromise

spread within an entity's network. These lower tier attackers then sell that access to parties interested in greater profit, greater impact, or other motivations.

Retooled exploits and tactics are usually known to defenders, who rapidly develop and deploy countermeasures against them. These reused components have a limited shelf life, and attackers must use them quickly. Attack groups have become extremely good at swiftly incorporating new exploits and tactics into their development processes, allowing them to use retooled exploits and tactics before any defenders can react.[22]

WannaCry Attack

WannaCry was a massive cyberattack launched in May 2017 that encrypted victims' data for ransom. WannaCry leveraged several exploits and hacking tools released by a hacking group called the ShadowBrokers. The ShadowBrokers release included highly effective zero-day exploits and persistence tools believed to be stolen from a well-financed state actor. WannaCry attackers leveraged "EternalBlue," a highly effective exploit against Microsoft® Windows® Server Message Block 1 (SMB1), a protocol that shares files over a network to access them among the clients in an effective manner. The attackers retooled it for their system in a little less than a month in a worldwide attack believed to have compromised 200,000 systems, encrypting victim data for ransom.

While a patch was available for the core EternalBlue vulnerability, many system owners did not apply the patch fast enough. Victims were shown an ominous red ransomware note on their desktop with a BitCoin address to pay a $300 to $600 ransom. Defenders were fortunate that a security researcher in the United Kingdom discovered a kill switch that disabled the encryption portion of the malware, limiting the damage.

If this trend continues, lower tier attackers may apply lessons learned in successful energy sector attack operations for their ransomware actions on critical infrastructure.

5 Conclusion and Recommendations

The electric grid is undergoing an unprecedented, swift transformation to DER deployment, empowering customers with more choices and control of the energy. This transformation is driven by technological advancement and environmental goals such as decarbonization. It is creating market forces for critical infrastructure investments. Wind and solar energy are leading this transformation, fundamentally changing how the electric grid is planned and operated, as well as the electric loads themselves (such as from electric transportation). Meanwhile, DER can diversify grid energy resources and, through microgrids, make the power system more resilient by maintaining critical power during faults on the grid, extreme weather, or even cyberattacks.

In parallel to the grid transformation, economy-wide cyberattacks have steadily increased over the course of two decades. Attackers are evolving their practices and capabilities against new technology faster, and malicious actors are positioned well to enter DER energy systems. DER deployment is coupled with transitioning to a software-defined power grid, and software requires cybersecurity and standardization to mitigate the risks associated with software enterprises. While traditional attack

[22] Alert (TA17-132A): Indicators Associated With WannaCry Ransomware. May 12, 2017. Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/uscert/ncas/alerts/TA17-132A

vectors, such as insider threats, poor data security, and access controls, are relevant to new grid technologies, distribution rooftop solar and large-wattage, customer-owned devices present new attack potential, can aggregate to magnitudes like traditional resources, and will challenge traditional cyber defense postures through their administration by many different parties.

The confluence of these two major forces requires investment, attention, and active development to ensure the reliability of electric power systems and to safeguard the Nation's critical infrastructure. Compared with past energy sector cyber enhancements, securing DER will require addressing the differences between DER and traditional electric power systems.

Nowadays, cyberattacks on DER are largely limited given that many parts of the country are just starting to see significant DER growth. However, future DER deployments will need to incorporate cybersecurity best practices and meet minimum requirements. Defending against emerging DER cybersecurity threats should be based not only on direct business risk, but also on the risk to the wider public interests balanced against cost and complexity. Greater attention also is needed to assess how DER cyberattacks could affect grid operations, create a DER trust model, and extend trust to include the DER supply chain.

Best practices for cybersecurity include multifactor authentication, endpoint detection and response, encryption, and a skilled and empowered security team. Many cybersecurity standards do exist; however, they may need refinement to address specific DER deployment use cases. Resources for development and harmonization for secure DER scenarios include the following:

- The North American Electric Reliability Corporation's (NERC) Critical Infrastructure Protection Standards
- The National Institute of Standards and Technology's (NIST) Framework for Improving Critical Infrastructure Cybersecurity (NIST 2018)
- The Cybersecurity and Infrastructure Security Agency's Securing Industrial Control Systems: A Unified Initiative FY 2019–2021
- The draft IEEE Standard 1547.3 for DER cybersecurity interconnected with electric power systems
- If approved, an IEEE P2800 standard for securing IBR interconnected with transmission electric power systems
- NERC's Reliability and Security Technical Committee working groups
- The Sandia/SunSpec DER cybersecurity working group
- The International Electrotechnical Commission's (IEC) standards, especially the IEC 62351 standards for securing power system communications
- IEEE 2030 standards, especially the 2030.5 standard for smart energy profile application protocol
- NIST SP 800-82, Guide to Industrial Control Systems Security
- V2G – Bidirectional V2G SAE Suite 3778 (New SAE 3000 Series of V2G)
- NIST SP800-213, IoT Device Cybersecurity Guidance for the Federal Government
- The U.S. DOE Office of Scientific and Technical Information's Cyber Security Primer for DER Vendors, Aggregators, and Grid Operators (SAND2017-13113)

When applying these cybersecurity requirements, grid and DER planners should build cyber defenses around the goal of surviving an attack while maintaining critical functionality. The underlying principles for action may include:

- **Implementing best practices** and meeting minimum security requirements in alignment with the controls and practices in the NIST Cybersecurity Framework and/or NERC's Critical Infrastructure Protection standards.
  - Specify DER security requirements and harmonize them for practical DER use in a risk-based and cost-effective manner.
  - Temper the use of these practices with the understanding that DER networks and systems are fundamentally different from their forebearers.
  - Ensure effective testing and conformity to ensure that DER meet these requirements.
- **DER entities and utilities implementing good governance** to improve their defense-in-depth posture. They should design security into their systems from the beginning and make security a priority for all employees, suppliers, and customers. Utilities should support the DER industry on improved systems governance and be responsible for the system-of-systems risks with overall accountability for the power system withstanding an attack.
  - Understand, codify, and enforce the roles and responsibilities of each entity involved in the DER ecosystem.
  - Enhance firmware security via code signing, secure patching, and software bills of materials verification.
  - Test and enumerate software/hardware bills of materials to identify vulnerabilities in code that could be exploited.
  - Monitor communications and events associated with DER, enhancing anomaly detection and moving toward verified DER control requests.
  - Use cryptographically secure communications protocols and methods of storing and distributing keys.
  - Apply certificates to authenticate communications and use of the certificates for DER power system interconnection.
  - Implement effective access control mechanisms for both individuals and entities.
- **Industry incentivizing cyber resilience** by going beyond standards to actively detect threats with autonomous mitigation techniques and moving to zero-trust architectures for securing critical DER operations under attack.

Future DER systems must be designed, built, and operated in an enforced zero-trust model where data are validated using cryptographically secure mechanisms informed by standards, testing, and vulnerability assessments. DOE and industry efforts that support the creation of an enforced trust model include:

- Publishing and implementing the draft IEEE Standard 1547.3 DER cybersecurity guidelines currently under development. As part of implementation, the industry also will need to determine and apply testing and conformity requirements.

- Advising or participating in Federal and state activities to identify DER cyber risks. Regulator advice will be critical for clarifying roles and responsibilities.
    - Beyond Federal efforts, DOE engages energy officials and regulators through the State, Local, Tribal, and Territorial Program.
    - For assessing emerging DER cybersecurity risks, DOE is co-funding the National Association of State Energy Officials and National Association of Regulatory Utility Commissioners solar cybersecurity project, Enabling Solar Cybersecurity Solutions Through State Energy Office and Public Utility Commission Engagement with Private Sector Partners.
- Using cryptographically secure mechanisms to verify commands and data, such as those envisioned by the Secure SCADA Protocol for the 21st Century program.[23]
- Analyzing supply chain risks, especially through hardware and software trust platforms and robust assessment of software bills of materials.
- Assessing readiness through an adversarial testing process run by cybersecurity professionals, exemplified by CESER's Cyber Testing for Resilient Industrial Control Systems (CyTRICS™) program. CyTRICS is intended to evaluate hardware, software, and firmware in energy sector systems and provide guidance on ensuring the security of the product development infrastructure.
- Designing secure systems from the ground up, incorporating cybersecurity lessons learned and cyber-informed engineering[24] practices that result in resilient systems engineered to reduce cyber risk.
- Training the next generation of cyber guardians. DOE is supporting this through the SunSpec Cyberguardians and science, technology, engineering, and mathematics (STEM) Warriors program, which concentrate on providing opportunities to military veterans and young professionals.[25]

Broad industry involvement is key to the development, approval, and implementation of robust DER cybersecurity standards, trust models, and best practices that would raise the bar for foundational DER defenses. DOE will continue to engage DER vendors, owners, operators, aggregators, and utilities, as well as Federal, state, local, tribal, and territorial energy officials and regulators to ensure wide adoption of the standards and best practices. DOE also will move beyond compliance by working with university, National Laboratory, and industry researchers on next generation DER defenses to ensure security in a decarbonized grid.

[23] Secure SCADA Protocol for the 21st Century. https://www.energy.gov/sites/default/files/2018/12/f58/LLNL%20-%20Secure%20SCADA%20Protocol%20%28SSP-21%29.pdf

[24] Cyber-Informed Engineering (CIE). https://inl.gov/cie/

[25] *See* PROJECT PROFILE: SunSpec Alliance (FY2018 Workforce Initiatives). U.S. Department of Energy. https://www.energy.gov/eere/solar/project-profile-sunspec-alliance-fy2018-workforce-initiatives

6 Appendices

6.1 Appendix A: Autonomous Distributed Energy Resources' Grid Support Functions

Distributed energy resources (DER), such as rooftop solar photovoltaic systems, battery energy storage, and even backup natural gas generation, will be required to follow the latest Institute of Electrical and Electronics Engineers (IEEE) Standard 1547-2018. States are rapidly adopting this standard, which includes the next generation of DER requirements to connect to the electric grid safely and reliably. IEEE Standard 1547 defines the functional requirements for DER and applies to all equipment connecting to the electric grid distribution system, regardless of the equipment's type or size.

As noted in Figure 3, grid support functions from DER have evolved from DER disconnecting from the grid during abnormal power system events to now being required to ride-through these events and continue to actively support voltage and frequency stability within limits.

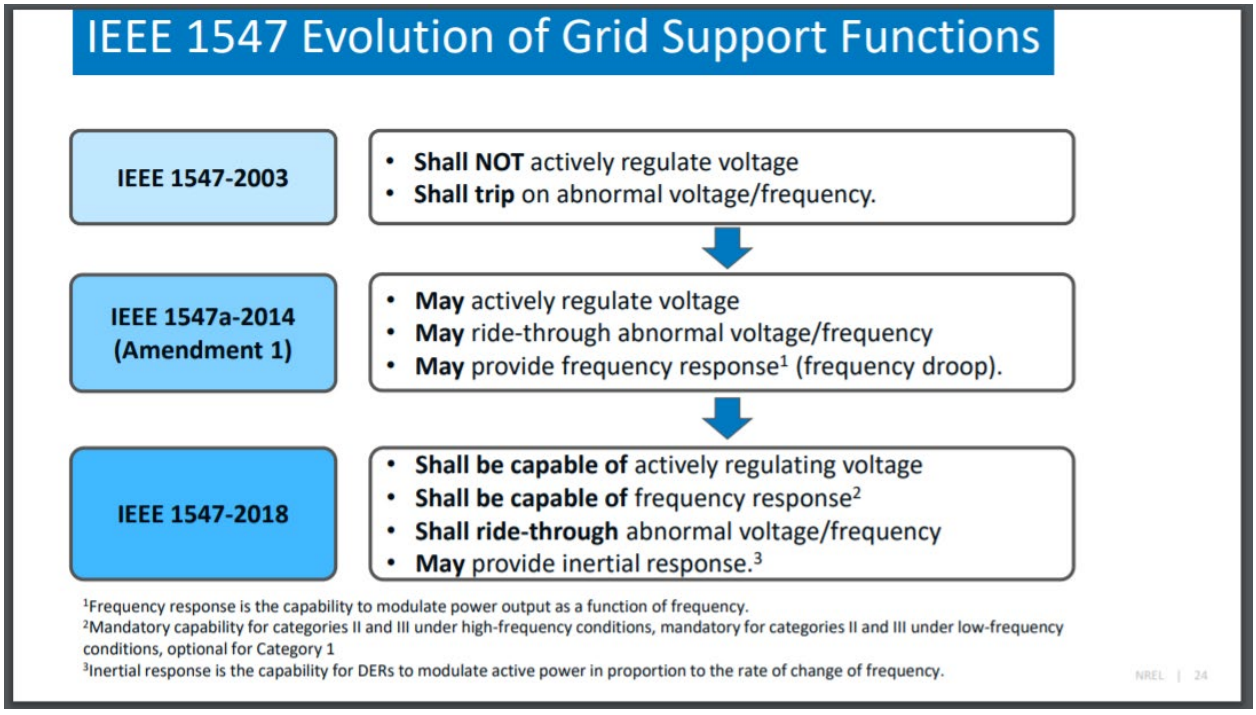

Figure 3. DER Grid Support Functions[26]

[26] Figure from National Renewable Energy Laboratory. (2019). Highlights of IEEE Standard 1547-2018. https://www.nrel.gov/docs/fy20osti/75436.pdf

See also https://www.nrel.gov/grid/ieee-standard-1547

Range conditions can cause abnormal events on the grid, from weather and wildlife to aging equipment and security events. If lightning, for instance, hits a transmission line, the grid's protection equipment would normally clear that fault but a very brief spike in frequency or voltage may occur. DER will need to ride-through that disturbance event to help keep the grid's frequency and voltage within its proper range. This disturbance only lasts a few seconds, so DER must respond automatically within the same period to support the grid.

If DER did not have these grid support functions and were deployed with the legacy requirements, nearby DER disconnecting during a fault would make the disturbance even worse. If there were many DER disconnecting, this may cause cascading failures and produce widespread outages. IEEE Standard 1547-2018 grid support requirements ensure that DER ride-through these abnormal grid conditions and support area grid reliability.

6.2 Appendix B: Distributed Energy Resources Threat Scenarios

A valuable tool when developing standards for more traditional engineered systems are case studies, where failures and successes are analyzed for commonalities, controls are developed to counteract those common failures, and tests can be developed to ensure that the controls address the problems encountered. These are valuable for probabilistic events; however, cybersecurity threats are based on human decisions and ingenuity. With this in mind, understanding the threat faced provides a similar background to a case study, and expanding that threat into scenarios provides similar value to design activities.

The following generic threat scenarios on DER can inform designers working on standards and systems.

6.2.1 DER Aggregate Capacity Cybersecurity Risks

A single and limited attack on one DER (i.e., lacking DER worm propagation) is not likely to cause wider issues on the grid. Attacking enough DER occurs when a proportion—or aggregate capacity as a DER botnet—of infected grid resources would significantly disrupt wider grid operations, either causing power quality issues or possibly even rolling or cascading outages. The aggregate capacity of these compromised DER poses a risk to the reliability of the area power system. Based on sufficiently compromised DER relative to grid load conditions, examples of DER botnet attacks include malicious DER configuration or patching, manipulating DER ride-through and trip thresholds, inducing power system oscillations, and other aggregate DER attack vectors.

Smaller devices, especially adjustable facility loads and smartphone-enabled home automation devices, are internet of things (IoT) devices. This report does not focus on the security of IoT technologies, which generally do not contribute energy to the power system.[27] However, IoT systems and devices should align with the cybersecurity requirements for DER if the aggregation of the IoT technologies could cause

[27] Controllable loads—having remote access and a configurable state—are outside of the scope of the Institute of Electrical and Electronics Engineers (IEEE) Standard 1547. As such, future standards will need to align DER and controllable loads requirements for power system reliability, plus include cybersecurity to merge DER and Internet of things (IoT) security requirements. For instance, this may include harmonizing requirements and certification for IEEE Standard 1547 and the Open Automated Demand Response devices and extending to all DER and controllable loads.

power quality or stability issues on the grid. Even today, compromised IoT devices (dubbed "botnets" by cybersecurity professionals) have reached into the millions—a volume of compromise that underscores the threat to future DER installations that leverage similar technology. More research is necessary to gauge the impact of IoT.

6.2.2 Malicious DER Configuration or Compromised Patching

DER could be attacked by maliciously configuring them during factory shipment or installation or during patching. This is a hybrid attack category given the supply chain dimensions; however, it is being highlighted as a DER botnet risk because compromised configurations are not high-risk issues for the grid until an aggregate number start to impact power stability margins. Compromised DER settings could obscure the actual operational state of DER and, in sufficient number, cause grid voltage and current violations. Attacker execution of compromised configurations also would lead to DER not responding to distributed energy resource management system (DERMS) control requests and impacting DER provision of grid services. Table 1 summarizes this general DER misconfiguration attack.

Table 1. Attack Summary for Malicious DER Configuration or Compromised Patching

Intended Consequences	General grid disruption by intentionally misconfiguring DER to obscure their operation mode.
Category of Systems/Devices Compromised	General configurable DER.
Attack Surface and Technique	**DER vendor, owner, operator, or aggregator that misconfigures DER during factory shipment, installation, servicing, or pushing a compromised patch:** General misconfiguration issues either obscure the actual operating state of DER and/or cause DER to operate counter to grid operator commands.
Number of Systems/Devices That Need To Be Compromised in a Successful Attack	The number of devices varies according to the average and instantaneous percentage of DER penetration relative to composite load during abnormal grid operations. At higher levels of penetration, lower percentages of DER compromise could achieve an area blackout.
Result	The most impactful result of this type of attack would be a cascading loss of power and a complete blackout. At lower levels of compromise, the attack could cause load shedding or a local blackout in response to over/undervoltage or frequency. In the extreme case of a blackout, the duration of the outage would depend, in part, on the ability of the system to execute a black start.
Cyber Vulnerabilities Exploited	DER firmware and configuration settings could be compromised through poor supply chain security.

6.2.3 Manipulating DER Ride-Through and Trip Thresholds

This attack is a more specific variety of the general DER misconfiguration attack. This attack leverages the new, required grid support functionality defined in IEEE Standard 1547-2018, where DER must have adjustable voltage and frequency ride-through and expanded trip settings. Ride-through requirements ensure that DER continue to add power to the grid to help stabilize grid frequency and voltage to ensure sufficient power flow. This new power system requirement contrasts with legacy DER, which tripped offline during such abnormal events.

Table 2 summarizes the DER ride-through and trip attack, which would cause DER to disconnect from the grid during events when they should remain connected.

Table 2. Attack Summary for Manipulating DER Trip Thresholds

Intended Consequences	Create instability in the grid by intentionally causing DER to disconnect from the grid during events when they should remain connected.
Category of Systems/Devices Compromised	DER that support frequency ride-through and voltage ride-through settings with remote communication access and software/firmware-defined ride-through settings.
Attack Surface and Technique	**DER aggregator systems or their DER-to-utility communications networks:** Changing the over/underfrequency ride-through settings of many advanced DER or changing the over/undervoltage ride-through settings of many advanced DER. Once the DER settings are changed, the attacker simply waits for a grid disturbance (fault or loss of generation) to cause widespread DER tripping. (Note: A more sophisticated attack also might cause such a trip, but this extra effort would represent a higher threat profile.)
Number of Systems/Devices That Need To Be Compromised in a Successful Attack	The number of devices varies according to the average and instantaneous percentage of DER penetration relative to composite load during abnormal grid operations. At higher levels of penetration, lower percentages of DER compromise could achieve an area blackout.
Result	The most impactful result of this type of attack would be a cascading loss of power and a complete blackout. At lower levels of compromise, the attack could cause load shedding or a local blackout in response to over/undervoltage or frequency. In the extreme case of a blackout, the duration of the outage would depend, in part, on the ability of the system to execute a black start.
Cyber Vulnerabilities Exploited	DER firmware settings could be compromised through a communications network belonging either to the aggregator, the utility, or the DER vendor. Malicious firmware could be inserted through a compromised DER vendor or aggregator.

6.2.4 DER Control Systems Cybersecurity Risks

Access to DER upstream communications and control of DERMS systems could allow attackers to directly manipulate wide-area power system devices, constituting a DER worm attack. Compromised DER-to-aggregator, aggregator-to-utility, or DER-to-utility communications may manipulate wide-area DERMS control via spoofing or man-in-the-middle attacks. Another vector is when the DER worm attack successfully infiltrates the DERMS control systems application itself, again manipulating its wide-area control requests and potentially compromising its entire DER fleet.

Poorly protected communications networks may, for instance, propagate malware via lateral movement vectors to widely disrupt communications or even access the systems control applications. Because the systems control applications coordinate and dispatch many DER and interface with other grid operational control technologies, systems attacks can cause widespread issues. For DER, today's systems controls suffer from implicit trust concerns, where DER lack sophistication to verify commands and ensure integrity. Example DER control system attacks include disrupting adaptive protection, spoofing DER data, and issuing malicious DERMS control requests.

6.2.5 Disrupting Adaptive Protection

Grid protection systems (e.g., fuses, relays, circuit breakers) will need to be upgraded as more inverter-based resources (IBR) connect to the grid and for distribution protection as more DER connect to the grid. IBR and inverter-based DER provide substantially different fault currents. Thus enhanced protection is being piloted today for adaptive settings. The aggregate contribution of many DER scattered throughout the distribution grid could reduce the fault current level sufficiently to desensitize traditional overcurrent relays, trigger overcurrent protection, trigger protection device maloperation, or alter fault detection.

A traditional setting works when there are few DER and when fault characteristics are still dominated by traditional rotating generation. Adaptive settings will be needed for periods when a high proportion of generation is from IBR, plus DER could change and reverse power flow that likewise would require adaptive settings. Adaptive protection may inherently include communication-based modes and would thus expand the attack surface in parallel with DER deployments.

Because adaptive protection will be deployed as more DER are installed, attackers who are able to compromise utility communications or even access grid operations applications could target adaptive protection to specifically trigger instability associated with DER settings. Table 3 summarizes adaptive protection attacks.

Table 3. Attack Summary for Disrupting Adaptive Protection

Intended Consequences	Compromise grid protection coordination.
Category of Systems/Devices Compromised	Adaptive protection devices with communication-enabled setpoints.
Attack Surface and Technique	**Utility protection controls:** The attacker manipulates the trip settings of protection devices and/or the coordination management system in a way that leaves some devices desensitized to faults in their protection area, leading to larger outages and noncleared faults. The attacker also can cause the outage of a large portion of the distribution system by modifying the trip settings of a protection device. Because DER are so fast-acting, interaction with misconfigured protection could quickly lead to power instabilities and localized backouts.
Number of Systems/Devices That Need To Be Compromised in a Successful Attack	The number of protection devices that need to be compromised for a successful attack depends on the location and the operating conditions of the system at the time of the attack. A carefully planned attack on one protection device by an attacker who knows the topology and loading profile of the system can lead to significant load going unserved.
Result	The most impactful result of this type of attack would be causing a substation protection device to trip unnecessarily, leading to an outage. Also, modifying the settings on a set of protection devices can result in inappropriate settings in other coordinated protection devices.
Cyber Vulnerabilities Exploited	Protection devices could be compromised through the adaptive protection communications network.
Threat Profile	Given that protection devices may have minimum and maximum allowed trip settings based on their ratings, randomly altering protection settings may not easily yield a widespread outage. The attacker must know the topology of the system and estimate the operating conditions at the time of the attack to be successful.
Severity of Impact	Attackers can cause outages, leaving portions of the system without power for minutes to hours. In the case of non-cleared faults, equipment damage can occur.

6.2.6 Spoofing DER Data and Man-in-the-Middle Attacks

As more DER are deployed, they likely will be used as ubiquitous grid sensors. DER measurements, for instance, may be used to calculate distribution current and voltage at feeder buses to help determine system loads, which may be included in transmission decisions. Therefore, falsifying the data from these devices will impact monitoring and state estimation systems and lead to poor automated or human-controlled decisions. Falsifying data during natural disasters or other periods of stress (e.g., peak load) on a system could lead to more drastic failures. This type of attack corresponds to upstream DER

communications network attacks that aim to impact DERMS, distribution management systems, or energy management system and other grid operator controls. Table 4 summarizes spoofing and man-in-the-middle attacks.

Table 4. Attack Summary for Spoofing DER Data and Man-in-the-Middle Attacks

Intended Consequences	Spoofed data could cause unnecessary changes to power system operations manually or through an automated system. Conversely, falsified data could mask risky power system operations when a change should occur (e.g., masking a fault as normal conditions). Both scenarios could cause grid instability or loss of power.
Category of Systems/Devices Compromised	Data originating from DER devices, aggregators, utility sensors, and supervisory control and data acquisition (SCADA) systems.
Attack Surface and Technique	**DER communications:** The attacker can perform a man-in-the-middle attack by address resolution protocol, spoofing endpoints on the network so that data can be modified, injected, or dropped into the communications channel.
Number of Systems/Devices That Need To Be Compromised in a Successful Attack	The number of systems/devices that need to be compromised will vary depending on the network configuration and decision points. The communication streams to and from the aggregator would be a point of interest. Compromising individual endpoints would accomplish the same goal but would require more end devices to be compromised for widespread damage to occur.
Result	The most impactful result of this type of attack would be if the data falsification causes faults to persist and grid instability or large-scale outages, depending on the number of devices compromised relative to load. Data falsification also could cause a grid operator or automated system to perform an action that should not be performed. For example, if the data incorrectly suggested that a portion of the grid had islanded, control systems may de-energize that portion of the grid.
Cyber Vulnerabilities Exploited	DER endpoints, SCADA systems, DER communications, aggregators, utilities, and sensor data would be vulnerable if the firmware update status data are compromised and a man-in-the-middle attack injects, modifies, or drops communications.
Threat Profile	The attacker would need a presence on the network and to correctly manipulate communications from several vantage points simultaneously to produce the intended malicious results. This would require considerable skill, effort, and access points within the network.
Severity of Impact	Falsified data can result in loss of power and equipment damage if they cause an operator to initiate an outage when none is needed or fail to initiate an outage when one is needed. In the case of load shedding, portions of the system would be without power for minutes to hours.

6.2.7 Issuing Malicious DERMS Control Requests

Compromised DER-to-aggregator, aggregator-to-utility, or DER-to-utility communications may give DER worm attackers lateral movement access to DERMS control systems. Another vector is when the attack successfully infiltrates the DERMS control systems application itself (e.g., via supply chain, backdoors), again manipulating its wide-area control requests and potentially compromising its entire DER fleet. Table 5 summarizes issuing malicious DERMS control requests.

Table 5. Attack Summary for Malicious DERMS Control Requests

Intended Consequences	DERMS control systems issue DER commands that induce instability and a potential loss of power.
Category of Systems/Devices Compromised	DER data originating from DER devices, aggregators, utility sensors, and SCADA systems.
Attack Surface and Technique	**DER communications and DERMS systems:** The attacker leverages a poorly protected DER communications network to propagate and laterally move access to the aggregator or utility DERMS system, now directly compromising its wide-area control.
Number of Systems/Devices That Need To Be Compromised in a Successful Attack	Poor protective technology for DER communications security may serve as an entry point for attacker lateral movement to widely disrupt communications or generally access systems control applications. Because the systems control applications coordinate and dispatch many DER, plus interface with other grid operational controls technologies, systems attacks can cause widespread issues.
Result	The most impactful result of this type of attack would be, under large DER deployment scenarios, malicious DERMS commands causing DER to initiate power system instabilities or area outages, depending on the proportion of DER to traditional assets and load.
Cyber Vulnerabilities Exploited	Unsecured ports/services on DER devices are exposed on public communications, poor firewall configuration, physical access to unprotected interfaces, remote access, bypassed DERMS authentication systems, escalating privileges, and so forth.
Threat Profile	The attacker would need a presence on the network and to correctly infiltrate upstream systems. This would require considerable skill, effort, and access within the network.
Severity of Impact	Attacked DERMS could issue corrupted commands causing power system instability or power losses, leaving portions of the system without power for minutes to hours.

6.2.8 Hybrid DER Aggregate and Systems Risks

Hybrid DER aggregate and systems risks highlight how some attacks involve more than one tactic to impact critical grid operations. These multiple attack vectors require identifying DER or systems vulnerabilities that can disrupt grid operations. An important hybrid attack vector to prepare for is a compromised DER preventing a black start.

During a black start, small regions of minimal generation and loads are brought online to slowly reenergize the rest of the system. During that time, the energized regions are very susceptible to disruption and collapse due to weak grid conditions. In future power systems, DER may provide black start capabilities to the power system.

The concept of using many DER at the distribution level for a black start is challenging because the devices are mixed with load. It would not be possible to energize a distribution system without bringing online uncontrolled local loads, such as air conditioning, refrigeration, and lighting, on the same circuit. Extensive use of DER for a black start is therefore also probably coupled with developing networked or ad hoc microgrids combined with extensive controllable loads.

During a conventional black start, where restoration is driven primarily by large, central generation, the grid is already in a weakened state and cannot absorb disruptions as well as it can during normal operations. Maliciously operated DER could therefore have a greater than normal impact on the black start. The primary risks are that (1) DER could be manipulated to change the generation or load in a destabilizing way, and (2) DER could be manipulated to change reactive power contributions that cause overvoltage or undervoltage protection devices to trip. Normally, when there is a sizeable number of online generators, reactive power controllers are plentiful and finely tuned adjustments are possible. However, this is not the case during a black start. For this reason, malicious reactive power control of DER could make it significantly harder for grid operators to stably return the system to full operation. Table 6 summarizes a scenario where corrupted DER prevent a black start.

Table 6. Attack Summary for DER Preventing a Black Start

Intended Consequences	Disrupt or prevent a black start by manipulating DER end devices.
Category of Systems/Devices Compromised	DER end devices that contribute to generation and load.
Attack Surface and Technique	**DER and DER aggregators:** An attacker with control of DER devices (e.g., through vulnerable software, insider access, denial of service, man-in-the-middle, supply chain) can cycle them to create instability early in the black start when stable generation is critical. Also, if DER are relied on to assist with a black start, the attacker could prevent those DER from re-energizing the grid.
Number of Systems/Devices That Need To Be Compromised in a Successful Attack	The set of devices controlled by cycling DER power will vary depending on the black start process; however, it would be limited to the portions of the system used as early loads. If the early load regions are unstable, it could cause another collapse.
Result	If an attacker is controlling DER end devices, it may continuously cause black start failures. Also, if systems are energized out of order or if DER are maliciously controlled to generate or absorb significant quantities of reactive power, it may cause voltage collapse.
Cyber Vulnerabilities Exploited	DER end devices could be compromised through a variety of DER or DERMS attack vectors, such as supply chain interferences that provide a backdoor for adversary control; DER software/firmware compromised to allow remote access by an adversary; compromise of the control network belonging either to the aggregator, the utility, or the DER vendor; and man-in-the-middle attack to manipulate data and communications.
Threat Profile	While large numbers of DER end devices could be compromised using IoT attack methodologies, correctly manipulating the DER devices to continuously cause black start failures would require considerable skill and effort. Moreover, this attack could be carried out only after widespread blackout has already occurred for another reason.
Severity of Impact	Outages could be extended indefinitely if DER are maliciously controlled to disrupt black starts.