NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Privacy and Security Impacts of DER and DER Aggregators

Joint SPIDERWG/SITES White Paper

September 2023

RELIABILITY | RESILIENCE | SECURITY

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Table of Contents

Preface ... iii

Executive Summary ... iv

Introduction ... v

Intended Audience ... v

Definitions ... v

IEEE 1547-2018 ... vi

UL Solutions Standard 2941 ... vi

Regional Autonomy and Network Architecture ... vi

Chapter 1: Security Controls Available to DER and DER Aggregators ... 1

Network and Protocol Security ... 2

Internal Network Security Monitoring ... 4

Interactive Remote Access Controls ... 5

Data Management and Access Controls ... 6

DER Gateways ... 7

Carrier Controls Inherent in Communication ... 9

Chapter 2: Current Distribution Security Landscape of DERs and DER Aggregators ... 10

Differentiation of Utility-scale DER versus Retail-scale DER landscape ... 11

Distribution Management Systems and Emerging Distribution Landscape Considerations ... 11

Security posture of DER Aggregators ... 12

Confidentiality of Data at the DER and DER Aggregator ... 12

Chapter 3: NERC Standards, Relationships, Security Standards, Frameworks, or Alternatives in the Area ... 13

BES Cyber Asset ... 14

Limitations on Assessment and Applicability of DER, DER Aggregators, or other Distribution Entities ... 14

BES Impact Test and Meaning ... 15

Security Standards, Frameworks, or Alternatives in this Area ... 15

National and International Lessons Learned ... 16

Chapter 4: Conclusions and Recommendations to DER and DER Aggregators ... 18

State Coordination of Implementation of Recommendations ... 19

Data Confidentiality ... 20

Data Integrity ... 20

Data Availability ... 20

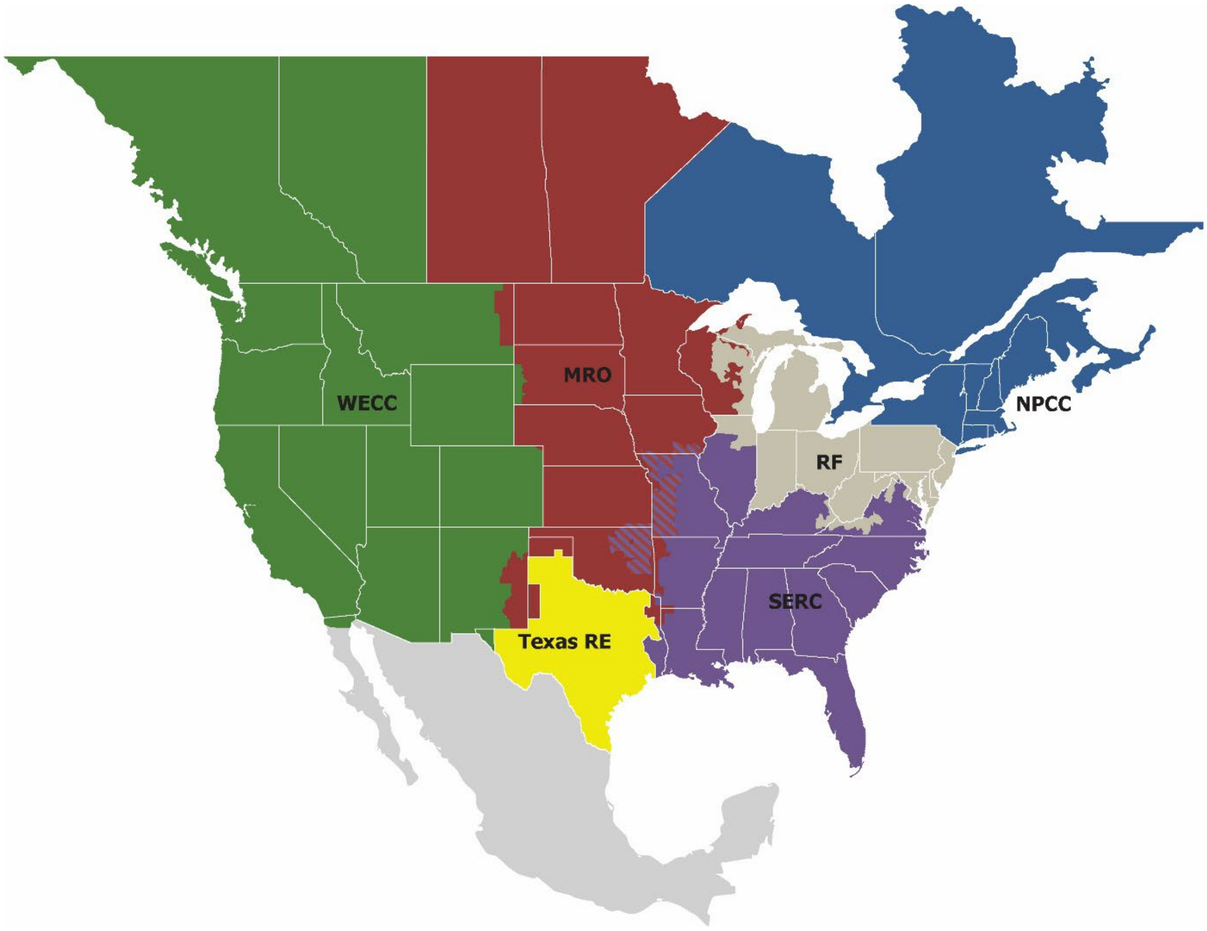
Chapter 5: Contributors ... 21

Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of NERC and the six Regional Entities, is a highly reliable, resilient, and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security
Because nearly 400 million citizens in North America are counting on us

The North American BPS is made up of six Regional Entities as shown on the map and in the corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one Regional Entity while associated Transmission Owners/Operators (TO/TOPs) participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	WECC

Executive Summary

The Federal Energy Regulatory Commission (FERC) approved Order No. 2222, which enabled distributed energy resources (DERs) to participate in wholesale electric markets[1] through a DER aggregator that interfaces with Independent System Operators (ISO) and Regional Transmission Operators (RTO). These ISO/RTOs are generally registered as the Balancing Authorities (BAs) and Reliability Coordinators (RC) in their respective Interconnections. The NERC System Planning Impacts from the DER Working Group (SPIDERWG) and the Security Integration and Technology Enablement Subcommittee (SITES) have both authored white papers[2] analyzing the bulk system reliability and security implications of the DER aggregator; however, no NERC industry stakeholder group has explored the technical aspects of security controls for these grid functions with their systems. This paper focuses solely on the security controls available to DERs and DER aggregators and provides recommendations[3] in order to maintain the reliability of the BPS.

This paper explores the technical facets of security controls available to DERs and DER aggregators and provides examples of potential attacks that can be mitigated through the implementation of those security controls. It also provides an overview of the security posture for the distribution landscape (particularly for DERs and DER aggregators) and correlations to relevant NERC Reliability Standards. The Bulk Electric System (BES) cyber asset 15-minute impact test is compared to DERs and DER aggregators to understand their potential impact to the BPS. Furthermore, privacy concerns are covered related to the confidentiality of user data for DER owners as such data may be the target of a malicious actor. This paper will also provide high-level recommendations to DERs and/or DER aggregators on security controls or other risk mitigation measures.

[1] FERC Order 2222 is available here: https://www.ferc.gov/sites/default/files/2020-09/E-1_0.pdf

[2] The SPIDERWG white paper *BPS Reliability Perspectives for Distributed Energy Resource Aggregators* is available here: https://www.nerc.com/comm/RSTC_Reliability_Guidelines/SPIDERWG_White_Paper_-_BPS_Persepectives_on_DER_Aggregator_docx.pdf and the SITES white paper *Cyber Security for Distributed Energy Resources and DER Aggregators* is available here: https://www.nerc.com/comm/RSTC_Reliability_Guidelines/White_Paper_Cybersecurity_for%20DERs_and_DER_Aggregators.pdf.

[3] This paper does not provide Compliance Implementation Guidance related to the CIP standards. Rather, security controls are presented at a high level, and the functional interplay between DER, DER aggregators, and other entities is considered in the context of security and security controls.

Introduction

Intended Audience

This paper is intended for the following NERC Registered entities, external stakeholders, and broader groups:

- Planning Coordinators (PC)
- Transmission Planners (TP)
- TOPs
- Distribution Providers (DP)
- DER owners, aggregators, and developers
- ISOs/RTOs (i.e., the BAs and RCs)

This paper includes recommendations to DER owners, DER aggregators, and NERC registered entities as they assess or analyze their security and privacy-protective posture. The complexity of managing the security and privacy of these systems is further compounded by the increasing DER penetrations. This paper is not intended to alter the DP's interconnection requirements nor to alter the electrical specifications to produce DER equipment. Rather, this paper is seeking to recommend security measures or requirements that improve the electrical ecosystem's security posture.

Definitions

To clarify terms and definitions to accurately scope what constitutes resources in a DER aggregator versus the SPIDERWG set of terms, the following main points should be noted:

- The SPIDERWG "DER" definition[4] of "any Source of Electric Power located on the Distribution system" is the preferred definition for discussing reliability concerns. The following is additional context:
  - This is different from the definition of DER in the FERC order, which is "a source or sink of power that is located on the distribution system, any subsystem thereof, or behind a customer meter."[5] Namely, the reliability-focused (i.e., SPIDERWG) definition focuses on generation only while the FERC definition includes load.
  - This is also slightly different from current discussions in Project 2022-02,[6] which is attempting to consolidate definitions and avoid the addition of many new terms. The Project 2022-02 definitions are not currently approved at the time of this document's publication.
- FERC Order 2222 introduces the definition of "DER aggregator," which (for this paper) is the entity[7] that controls the aggregation of generation (i.e., DERs) and load end-use devices.
  - The DER aggregator may have control over both load and generation, and it may control existing demand response programs.
- Both definitions include inverter-based resources (IBR) and non-IBR generation. For example, a 1 MW Solar PV plant and a 500 kW steam cogeneration facility would both be DERs if they are distribution connected.

[4] The SPIDERWG terms and definitions, including DER, Source of Electric Power, and Distribution System are available here: https://www.nerc.com/comm/RSTC/SPIDERWG/SPIDERWG%20Terms%20and%20Definitions%20Working%20Document.pdf

[5] Taken from FERC Order 2222 on page 85. Available here: https://www.ferc.gov/sites/default/files/2020-09/E-1_0.pdf

[6] Project 2022-02 website is located here: https://www.nerc.com/pa/Stand/Pages/Project2022-02ModificationstoTPL-001-5-1andMOD-032-1.aspx

[7] Furthermore, there are various names for the entities that control and aggregate DERs besides the DER aggregator. Examples include virtual power plant or emergency load reduction programs (excluded demand response). For this paper, DER aggregator and these other entities are synonymous as they functionally aggregate DERs (i.e., generation) on the distribution system.

DER management system (DERMS) and virtual power plant (VPP) control schemes will likely have different communications architecture.[8] For this paper, the terms DER aggregator, VPP, and utility systems that manage the control of DER are equivalent, and recommendations to a DER aggregator apply to these entities as well. However, each has a specific architecture that require different attack surface evaluations. Since this paper is a reliability-focused discussion on the privacy and security impacts of DERs and DER aggregators, it uses the SPIDERWG set of definitions. In instances where the load portion of a DER aggregator is relevant the load will be separated from generation by using terms like "DERs and load".

IEEE 1547-2018

The latest update to IEEE 1547-2018[9] makes it possible for the utility, or any other entity, to deploy DERMS and cohesively monitor and manage the diverse mix of DER technologies[10] and brands being deployed today. Utilities and third-party aggregators are deploying DERMS, making them an integral part of system operations. However, the large and diverse number of DERs, their evolving capabilities, and their continuous interconnection and retirement pose significant challenges to security and reliability of the DER ecosystem. Standardization efforts like IEEE 1547-2018 make DER integration practical by keeping DER operational functions simple and leaving more complex operational functions to the control and integration systems (i.e., DERMS or VPP). The standard also only dictates the communication protocols and intentionally left cybersecurity out of scope.

UL Solutions Standard 2941

UL Solutions announced the publication of UL 2941,[11] the *Outline of Investigation for Cybersecurity of Distributed Energy and Inverter-Based Resources*, developed in cooperation with National Renewable Energy Laboratory (NREL). The requirements will provide a single unified approach for testing and certification of DERs in advance of the anticipated rapid deployment.[12]

These new requirements prioritize cyber security enhancements for power systems technologies, particularly for inverter-based resources and DERs. UL 2941 is anticipated to promote the cyber security of new IBR and DER systems.[13] The standard outlines various testing needed to pass in order to achieve certification.

Regional Autonomy and Network Architecture

In the context of DER aggregators, security includes availability. The electric power system is designed with the ability for given area to isolate from surrounding areas for reliability purposes. For example, it may be possible for a given BA to maintain service within its footprint when a blackout is occurring in adjacent areas. As DERs become more common, there is increased potential for power system operability at local levels.

For regional power systems to operate, both the energy and the communication systems involved must be available. If DERs play a role of any significance, then the communication networks that manage DERs must remain functional. This can be an issue for some communication architectures. Grid equipment is integrated via networks that remain available when the local area is operating, but DERs within the area may not be available if they are managed via systems or networks in some other location where operation has been interrupted. For example, if a DER aggregator operates DERs in the Western Interconnection, then it isn't practical for the associated control system to have dependencies in a different system, such as the Eastern Interconnection.

[8] Primarily that utility implemented DERMS will likely have direct control and on-premises security controls while VPPs are more inclined to utilize cloud solutions for their security controls.

[9] IEEE 1547-2018 is available here: https://standards.ieee.org/standard/1547-2018.html

[10] E.g., Battery Energy Storage, Solar Photovoltaic, or synchronous DERs.

[11] Available here: https://www.shopulstandards.com/ProductDetail.aspx?productId=UL2941_1_O_20230113

[12] https://www.nrel.gov/docs/fy23osti/84709.pdf

[13] https://www.ul.com/news/ul-solutions-and-nrel-announce-distributed-energy-and-inverter-based-resources-cybersecurity

Chapter 1: Security Controls Available to DERs and DER Aggregators

The draft *IEEE P1547.3 Guide for Cybersecurity of Distributed Energy Resources Interconnected with Electric Power Systems,*[14] currently out for industry comments, provides guidance and recommendations for cyber security practices and controls to ensure secure communication of DER protocols (e.g., IEEE Std 1815, IEEE Std 2030.5, SunSpec Modbus, and IEC 61850) specified in the IEEE 1547-2018.

The P1547.3 guide includes considerations relating to the following cyber security topics:

- Risk assessment and management
- Communication network engineering
- Access control
- Data security
- Security management
- Coping and recovering from security events
- Testing and commissioning for cyber security and conformance with the IEEE P1547.3.

Though not exhaustive, the following sections provide a high-level overview of security controls available to DER devices and installation sites, DER aggregators and their control systems. **Figure 1.1** graphically shows the new communication pathways (in red) introduced with the addition of the DER aggregator to the electric ecosystem. Although their equipment, such as DER gateways, may be at the DER site, the DER aggregator logically sits at the T-D Interface and may communicate its DER control capabilities to the ISOs and RTOs (i.e., the BAs and RCs), who may then determine the utilization of those capabilities in coordination with distribution system operators. The DER aggregator issues operating commands to the DERs it manages as well as communicates necessary information with the additional key entities in the ecosystem. These new communication pathways necessitate a thorough understanding of associated risks and the available mitigating controls essential to protecting data security, privacy, and grid reliability.

[14] IEEE P1547.3 website: https://sagroups.ieee.org/scc21/standards/ieee-std-1547-3-2007-revision-in-progress/

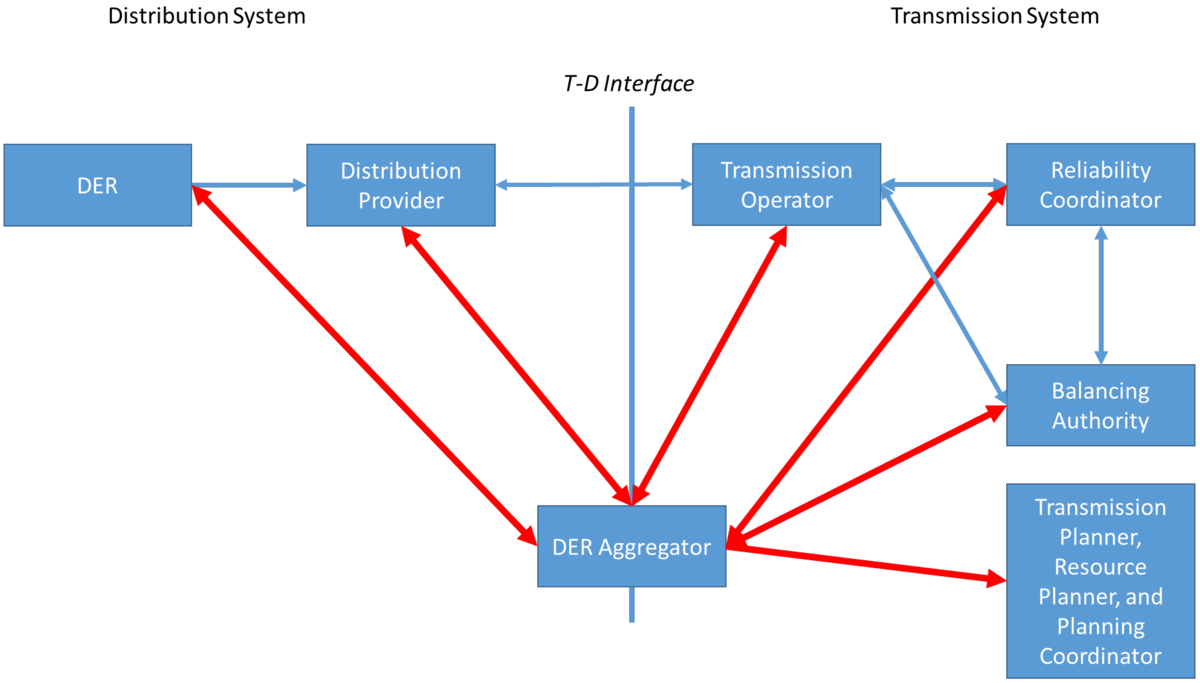


Figure 1.1: High-level Diagram of Added Communication for DER, DER aggregators, and the BES[15]

Network and Protocol Security

DERs, DER aggregators, and utility networks should be separated based on ownership, control capabilities, and trust relationships within specific implementations. The increased attack surface stemming from the connection of numerous DERs demands network architectures[16] that do not rely on implicit trust relationships. In the event of a single device or entire network segment compromise, proper network segmentation and additional security controls should ensure the continued operation of other segments.

Securely designed network architecture for DERs and DER aggregators may include the following:

- **Demilitarized zones, subnets, and VLANs**: These logical network segments isolate sensitive or critical systems from other parts of the networks; they establish security zones based on criticality of assets or operations and limit unauthorized access and potential damage from cyber attacks.
- **Intrusion prevention systems and intrusion detection systems:** These systems enable comprehensive visibility into network traffic through the monitoring and detection of suspicious activity or potential threats. Passively and continuously scanning and analyzing network traffic for known common vulnerabilities and exposures in addition to abnormal patterns these systems can identify and prevent potential cyber threats and enhance overall network security. This type of technology can be deployed in the demilitarized zone of the network to segment operational networks from business networks in and between subnets and VLANs for "East-West" protection.
- **Absence of implicit trust relationships:** Network architectures should be designed without assumptions of trust between connected devices or systems, minimizing the potential for unauthorized access and lateral movement of attackers within the network.

[15] Note that attacks scenarios can target communications outside of those highlighted in the Figure 1.1. For instance, original equipment manufacturer to DER communication as well as DERs directly to the RCs or BAs.

[16] This includes architectures that are centrally-managed and contain source-traceable components. Implicit trust can be designed out of an architecture and implicit trust should not be assumed even when an entity owns all components of the architecture.

- **Secure network boundaries:** Firewalls control incoming and outgoing network traffic based on predetermined rules while data diodes ensure one-way data flow that add layers of protection to network boundaries.
- **Strong encryption:** Implementing advanced encryption algorithms, such as Advanced Encryption Standard,[17] Elliptic Curve Cryptography, and Rivest-Shamir-Adleman,[18] ensures the confidentiality and integrity of sensitive data transmitted across networks.
- **Secure Protocols:** Communication protocols with built-in security features ensures the safe and reliable exchange of information between DER devices and control systems such as DNP3-SA.[19] These protocols incorporate robust authentication, encryption, forward-secrecy,[20] and non-repudiation, providing a strong foundation for secure DER communication.
- **Authentication:** Robust authentication mechanisms (e.g., digital certificates, public key Infrastructure, phishing-resistant multi-factor authentication) validate the identities of devices and users.
- **Authorization:** Implementing access control policies based on the "least privilege" principle ensures that users and devices have the minimum necessary access rights, limiting the potential impact of compromised credentials.
- **Virtual private networks (VPN):** VPNs create secure and encrypted connections over public networks (i.e., the internet) that protect data transmission from eavesdropping and tampering.
- **Efficient logging and alerting:** Security information and event management systems collect, analyze, and correlate log data from various network devices that generate alerts for potential security incidents and facilitating timely response.
- **Hardened networking equipment:** Applying security technical implementation guide recommendations ensures that networking equipment adheres to industry-standard security practices and reduce vulnerabilities and attack surfaces.

Besides isolating networks based on trust relationships and ownership, DER aggregator and utility networks should also be segregated within their internal networks (e.g., isolating corporate networks from industrial control systems). Implementations and specific security controls will depend on the use cases for a given DERMS. Isolated networks can range from decentralized VPP architectures, centralized distribution utility DERMS, or hybrid implementations. In addition, these networks should be securely segmented from other networks, including corporate networks. Insufficiently segmented networks with weak or lax security controls could enable cyber attacks to spread across multiple systems and network segments. DER endpoints,[21] being the most vulnerable links in these networked systems, present a higher risk of targeted attacks, such as DERs and DER gateways. **Figure 1.2** shows an example network architecture of a DER-managing entity controlling both small-scale DERs and utility level DERs. **Figure 1.2** highlights the effective use of network segmentation and firewalls to establish security zones, providing network boundaries to deploy further security controls.

[17] 100 bits or above should be used to be secure.

[18] 2,048 bits or above should be used to be secure.

[19] Other secure protocols exist. This is used as an example of one such secure protocol.

[20] Forward secrecy methods implemented within protocols ensures that past communication sessions cannot be decrypted if either session or private keys are compromised.

[21] Endpoints of a security system are where the "door meets the outside" for any given system. These are access points designed in system architecture and are frequently targeted by malicious actors. See here for a panel that discusses more of the reasons why endpoints are vulnerable: https://webinars.govtech.com/Closing-the-Endpoint-Security-Gap-in-State-and-Local-Government-102979.html#:~:text=According%20to%20intelligence%20firm%20IDC,and%20administrative%20passwords%2C%20and%20more.

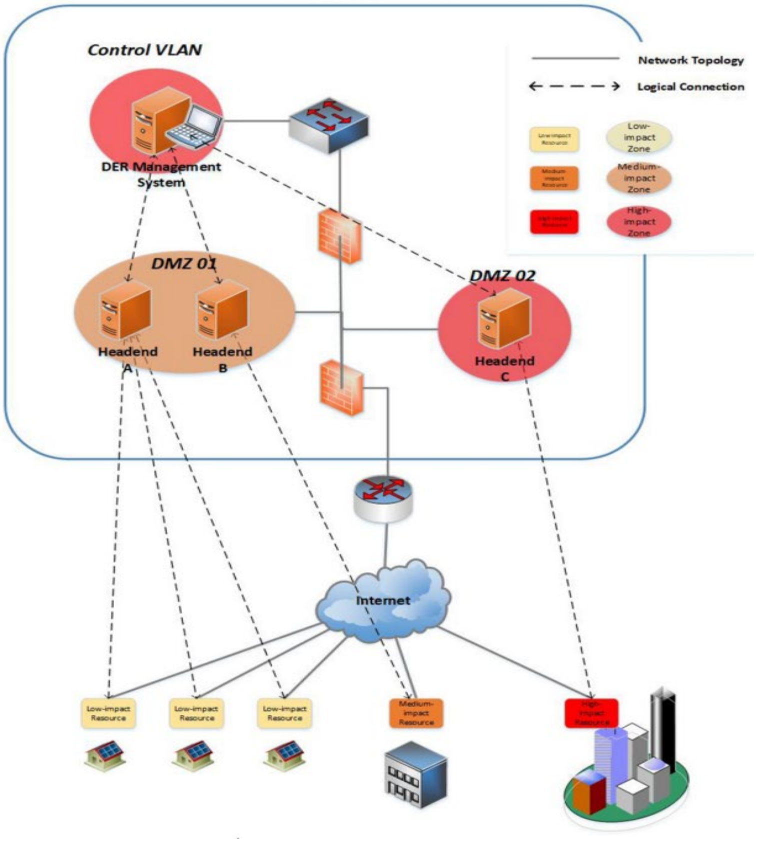


Figure 1.2: Example DER Managing Utility Architecture [Source: EPRI]

In general, network and protocol security are fundamental to proper cyber security practices. As such, the types of threats and adversary tactics they mitigate are diverse and numerous.

Internal Network Security Monitoring

Internal network security monitoring (INSM) controls are available for all networks involved, potentially including owners of the DER network,[22] the DER aggregator's network, a utility's network, or an original equipment manufacturer's (OEM) network. INSM monitors the traffic flowing internal throughout the network and provides alerts when suspect traffic is detected. These solutions include network mapping, vulnerability management, anomaly detection, logging, and alerting when malicious traffic is detected. Some INSM implementation may also block network communications to and from suspected compromised nodes. Proper patching and updates to malicious code signatures or heuristic detection schemes are critical to assure effectiveness of these network-based security controls.

Monitoring and logging are a prerequisite for any automated prevention or response-based controls, including access control lists, endpoint security, and security orchestration tools. In addition, the monitoring controls and their associated logs and reports facilitate security event triage and are key components[23] of security incident response activities. Their monitoring and alert data can also be sent to security information and event management solutions for security operations center analysts and/or handled by managed security service providers.

[22] It is not expected that residential DER owners would implement advanced controls beyond the default configuration at the time of their DER installation.

[23] Due to their pivotal nature, these controls will be required for high impact or medium impact with external routable connectivity control centers in the NERC CIP standards per FERC Order 887. Text available here: https://www.ferc.gov/media/e-1-rm22-3-000

Complete INSM solutions can be implemented for greater network visibility, but limitations in architecture, bandwidth, or device capabilities may preclude the monitoring of 100% of all network segments. This monitoring is analogous to the current and voltage relaying equipment[24] typically found on the electrical monitoring equipment in substations; however, these controls can take some automated action to mitigate against specific traffic. The following malicious activities can typically be detected by successful implementations of INSM:

- Active scanning of networks by malicious actors
- Lateral movement between internal network nodes, such as servers and workstations, and DER endpoints
- Download of known malware
- Command and control traffic
- Communications parameters and malformed packets
- New devices connecting to networks
- Weak and cleartext passwords
- Appliance usage and health logs
- Threat intelligence indicators of compromise (e.g., malicious IP addresses)

In general, INSM defends against internal reconnaissance, lateral movement within the network, and malware deployment to reduce the severity from incidents and compromise. Additionally, should a malicious actor compromise a DER or DER aggregator network, INSM may be able to detect outbound command and control communications, which is a prerequisite for a coordinated attack utilizing many compromised DER devices.

Interactive Remote Access Controls

Physical access to the DER site by the utility or DER aggregator is typically unlikely outside of routine meter reads and similar calls. Consequently, DER gateway communication interfaces will need to facilitate remote access capability to perform routine patching, firmware updates, or even the altering inverter settings. Any remote access[25] (and the communications network required to facilitate it) introduces a credible attack vector to the DER, gateway, and DER aggregator ecosystem. The absence of security controls, improperly configured and maintained security controls, or vulnerabilities at the DER site or within a DER aggregator's network could be exploited. Securely implemented and maintained remote access is critical for DER aggregators, utilities, and OEMs to service and manage DERs.

Remote access may require software and certain functionality on both sides of the communication link. Thus, security controls may exist on the utility network, DER aggregator network, or on the DER device or DER gateway in order to provide remote access capability in a secure manner. A simple but inadequate form of a security control authentication credentials;[26] more sophisticated remote access control mechanisms are needed. Secure remote access technologies include the following:

- VPNs using encrypted tunnels for network traffic
- Network access controls limiting device connections to authorized and accessed[27] devices

[24] As substation circuit breakers requires the voltage and current waveforms in order to isolate faults from the system. As such, more complex security solutions require monitoring and logging to perform their objective.

[25] Programmatic or interactive

[26] Another mitigation example is adding a timeout session of remote access.

[27] Assessed in this context means assessing the security posture of the device prior to it being allowed access to network resources. Security posture assessment may include firmware patch level, antivirus version, hardening level, MAC address, or other criteria used to assess the security "health" of the device.

- Phishing-resistant multi-factor authentication (MFA)[28] for interactive remote access
- Certificate based authentication for programmatic application access or system-to-system access
- Zero trust architectures requiring constant re-authentication and re-authorization
- Secure protocols

These methods are essential for securing remote access, a high-demand function for the current digitalized landscape. With an increasing number of access points through remote DER connections, secure networks are paramount to facilitating DER adoption and management through DER aggregator and utility systems. While the implementation and specific functionality of a technology will determine the vulnerability to particular threats and attacks, secure remote access implementations can generally mitigate the following types of malicious activities:

- Unauthorized external remote access
- Man-in-the-middle attacks
- Remote system discovery and reconnaissance
- Compromised trust relationships

Any security controls improperly configured or unpatched systems for vulnerabilities may allow attackers to circumvent remote access controls. Thus, the above mitigations support proper cyber-hygiene and a defense-in-depth approach. Both are important to balance the need for remote access with the security risk.

Data Management and Access Controls

Data, particularly at the DER aggregator level, can scale exponentially. Data management policies that address storage, transit, use, and retention measures are essential to ensuring the establishment of a holistic data management program.[29] Data management and access controls secure the access and management functions of data. Applied to DER and DER aggregators, these controls limit the credentials of who can read, write, and transfer data from a particular entities network. At the DER device level, these functions are broad per 1547-2018, particularly Clause 10 language, which allows for wide read, write, and transfer capabilities inherent in the DER equipment itself. Other device standards, like UL2941, are more specific in their requirement language for data storage and data transit. As stated above, 1547-2018 requires that DERs support necessary monitoring and management at the local interface and does not specify cyber security at this interface. With this, DER aggregators and DER owners need to implement these cyber security controls on their respective networks.

The controls themselves reside in the privileges granted to users to read, write, extract, and otherwise alter the data on the DER, DER aggregator, or other entity's network. Best practice security controls include storage, extraction, and deletion policies for data. These practices are particularly useful when exchanging equipment at the DER aggregator level that may have private information stored about the DER it controls or even for DER owners that exchange devices to wipe the private information stored locally. Effective implementations ensure the security and privacy of data as well as mitigate against IT sourced attacks on OT equipment in this environment. Specific attacks mitigated by data management and access controls could include the following:

- Credential harvesting or access
- Privilege escalation

[28] *Implementing Phishing-Resistant MFA*. CISA: October 2022. https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf

[29] Some data management policies allow for off-site, on-site, or hybrid approaches to manage data. Cloud security practices are important once data management and access controls include off-site or hybrid data management solutions.

- Account manipulation
- Data deletion, encoding, obfuscation, or manipulation
- Cryptographic (private) key exfiltration

Data management controls can further mitigate against data exfiltration or ransomware by a malicious actor. Privilege escalation is a common technique in the cyber criminal's toolbox, allowing the individual or malware to overcome a number of inhibiting controls to access data. Controls, such as data loss prevention, intrusion detection systems/intrusion prevention systems, and endpoint security, provide a greater assurance to detect or prevent the exfiltration or malicious encryption of data.

DER Gateways

DERs face a broad range of local threats and vulnerabilities thatare presently outside of utility responsibility and control. For example, a DER can have a variety of interfaces in addition to the standardized one, including those used for aggregators, owners, and OEM management. Each of these interfaces present a potential backdoor to the DER, any local networks, and the upstream managing entity's systems. IEEE 1547-2018 requires one open standard interface but does not prohibit these other interfaces. There are currently no specifications or requirements that apply to other DER interfaces. IEEE 1547-2018 does not specify cyber security requirements for DER and its local interfaces because they are generally untrusted systems to the DER managing entity[30] due to these risk exposures.

Key Takeaway:
Although endpoint controls may be applied to the DER to accomplish security objectives, these controls are not guaranteed to be adequately maintained over their lifetimes, and existing DERs may not be technically equipped to accommodate them. DER gateways are required to mitigate the lack of endpoint controls on the DER devices and to ensure secure interoperability with upstream managing entities. Alternatively, endpoint controls on the DER devices may accomplish some of the same security objectives.

Furthermore, current compliance and certification frameworks are limited in their scope of enforcement[31] to ensure that necessary security controls are adequately met among DER owners. In the absence of enforceable requirements at all DER interfaces, managing entities cannot establish assurances that critical security controls use for secure communications, including certificate management, private key protection, firewall policies, user access control, and other device-specific security features that are routinely reviewed and maintained over the DER's lifetime. This gap presents a challenge for managing entities where the integrity and availability of data and functionalities cannot be fully established for communications to the DER, where risk exposures[32] are much broader. This gap exposes all interfacing parties to a variety of attack scenarios against communications critical for grid interoperability, including the following:

- **Man-in-the-Middle:** Data that is supposed to flow only between a managing entity and the DER flows through a middle node that reads or modifies data before it is sent on its way.
- **Denial of Service:** A group of compromised DERs deliberately overload upstream managing systems with useless traffic and the resource-exhausted network or managing system cannot perform its functions. Alternatively, a certificate expires on the DER and prevents the managing system from accessing it. In both cases, this could impact a power system operator trying to control the power system.

[30] The special case exception to this is when the DER managing entity is also the DER manufacturer.
[31] Due to the voluntary nature of the IEEE Standards, and the varying nature of the regulatory framework for the local distribution of energy. Furthermore, it is not feasible to require action at the DER Owner level for their networks.
[32] This is especially true for cases where DERs integrate using public, internet-based networks.

- **Replay:** A command being sent from the managing entity to the DER is copied by an attacker. This command is then used at some other time to cause unexpected actions performed by the DER.
- **Malware**: An attacker adds malware to a DER, allowing it to propagate upstream to the managing entity.

DER gateways can serve as local platforms that house features and functions important to the DER managing entity, but they can also perform several important perimeter security functions that prevent these attack scenarios. This local platform physically resides at the DER site and includes a wired, physical interface that establishes a private connection to the DER through the gateway though the definition is still under revision in IEEE as defined by IEEE 1547.

Placing security requirements for DER gateways assumes that there are deficiencies in DERs and establishes a higher degree of trust in the communications to and from DER sites to protect critical utility systems, such as DERMS and advanced distribution management systems, from internal and external threats. These requirements include translating the DER's communication to trusted transport layer security (or similar) communications, implementing data access rights through role-based controls, configuring network access control and segmentation through firewall policy, performing network and application-layer monitoring for threats, and verifying firmware updates through signature-based methods. Because these and other security features are implemented on a gateway that is owned, implemented, maintained, and certified by the managing entity rather than the DER-owner or manufacturer, managing entities can ensure secure integration over public, untrusted networks with its DERMS or other management software operations.

Firmware updates are necessary to maintain security. For example, mobile phones, browsers, and computer operating systems are engineered with great attention to security, and yet frequently updated due to discovered vulnerabilities. It is not practical to expect that a DER managing entity could or would update firmware in a customer's DER for several reasons:

- The system is made up of a broad diversity of makes, models and vintages.
- Only the manufacturers of each DER can produce a new/patched code.
- The manufacturer of DER's may not be in business or supporting the models in the field and are not required by interconnection agreements to provide future updates.
- Manufacturers may not have a network path or connection to reach the DER to perform an update.
- There may be risk of harming (i.e., rendering unusable) a device when updating its code.

However, DER managing entities may readily maintain the firmware of DER gateways that may be of consistent design and under their direct control. For example, firmware updates are commonly pushed to thousands of utility supervisory control and data acquisition radios, millions of AMI meters, etc. Furthermore, complete systems of DER gateways and the communication networks they use can be retired and replaced, when necessary, but it is not practical to force the retirement of a customer's DER.

A new IEEE recommended practice, the *IEEE P1547.10 Recommended Practice for Distributed Energy Resource Gateway Platforms,*[33] is currently under development with contributions from several stakeholder groups (e.g., DER and DER gateway developers, owners, and operators, software producers, distribution and transmission system planners and operators, certification providers). The purpose of this project is to maintain coherency between the family of P1547.x and P2030.x standards as well as other related projects for DERs and DERMS within the evolving smart grid interoperability reference model with a focus on DER gateway platforms. The recommended practices

[33] PAR available at https://development.standards.ieee.org/myproject-web/app - viewpar/13494/9866

within P1547.10 will enable utilities deploying DERMS and other DER integration systems to integrate DER with grid edge intelligence, while allowing DER devices to serve their core functions, focused on simplicity, interoperability, and long-term stability. The scope of IEEE P1547.10 includes gateway platform functions and communications, including operational procedures and data collection recommendations. Additionally, recommended procedures for cyber security, centralized manageability, monitoring, grid edge intelligence and control, multiple entities management, error detection and mitigation, events tracking, and notification, communication protocol translation, and communication network performance monitoring. **Figure 3.1** illustrates the use of DER gateways. As indicated by the dashed lines, the gateways are physically at the DER site but are part of the aggregation/management system as shown by the coloring.

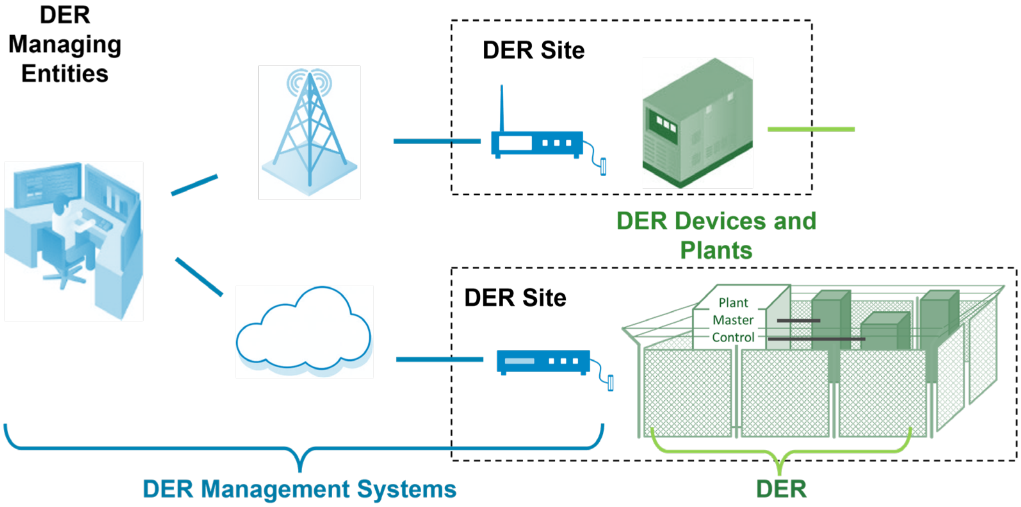


Figure 1.3: Example DER Gateway interface [Source: EPRI]

Carrier Controls Inherent in Communication

Many of the communications channels anticipated for information sharing between DERs and DER aggregators may traverse fiber networks using TCP/IP protocols. Devices (e.g., DER inverters or DER aggregator control centers) using routable protocols over fiber networks, including some private fiber networks, will have a carrier entity install and maintain these communication lines. Entities should ensure that business agreements with third-party carriers of these fiber networks ensure security controls are implemented.

Chapter 2: Current Distribution Security Landscape of DER and DER Aggregators

As evidenced in recent presentations[34] to SPIDERWG and SITES, the distribution landscape is primarily supported by equipment standardization with little to no standard design criteria about specific hardware, technologies, and engineering. This practice is in an effort to ensure that non-engineering technicians can install cost-effective solutions geared towards mitigating commonly reported customer problems within the affected portion of the distribution system. From a cyber security perspective, this may seem to involve major interoperability challenges that would need solid endpoint controls to limit access to the centralized ecosystem. Specific security requirements, however, are left up to each distribution entity's regulatory and corporate bodies to enable specific security controls for DERs. Additionally, FERC Order 2222 does not require any specific security protections to enable the participation of DERs in the wholesale ISO/RTO markets. Thus, SPIDERWG and SITES reviewed all available information on the distribution system and characterized a few main points, summarized below.

Telecommunications Networks: Distribution utilities use a combination of private fiber connections, public internet fiber connections, and radio communication interfaces for their monitoring and switching action. Utility-level DERs are more likely to emulate BPS architectures by using private networks for communication back to their shared locally geographic control centers. Most concerning, however, are geographically decentralized residential and commercial DERs utilizing public networks (i.e., the internet). Commonly, these connections do not use the IEEE 1547-2018 specified interface but a variety of other interfaces for which there is presently no requirements at all. Accordingly, adding cyber security requirements to the IEEE 1547-2018 standard interface would have no effect.

Public internet access for DERs utilizes Wi-Fi and cellular 4G/5G wireless networks, which are susceptible to interception and require strong encryption and authentication. Wired Ethernet and fiber-optic networks can be compromised through physical access or device vulnerabilities at the site of the DER endpoint. In some cases, private networks between the DER aggregator and their controlled DERs are achieved over the internet through the use of VPNs. Such communication offers increased security if the communication is properly terminated for remote sessions. Regardless of the medium for access, the use of public internet leaves both DER and DER aggregator control systems more exposed to remote attacks from anywhere on the globe. To ensure the resilience and stability of residential and commercial DER ecosystems, it is crucial to implement comprehensive security measures tailored to the specific requirements of each telecommunication network.

Electrical Protection Measures: It is still a common practice to use fuse-based protection in most distribution networks; some distribution entities may use more advanced solid state relay protection. In these instances, the protection seeks to limit backfeed to the transmission system or to enhance a secondary area network scheme's ability to recover from fault. The distribution system is thus much more fuse-based, providing single-use protection that is not present in the same ways or same densities on the transmission grid.

Distribution Entities Reliance on Equipment Standardization: With the need to lower cost to their consumers, distribution companies rely on turnkey solutions that are based on standard designs when upgrading or fixing a circuit. This allows the distribution system to be reconfigured by non-engineering staff and field crews while still maintaining high levels of reliability (e.g., using proven designs to limit the system average interruption frequency index and the system average interruption duration index)

Lack of Distribution System Design Security Integration: Rather than installing security protections, distribution companies rely on well-run line crews to recover the system and restore damaged equipment by using local spare equipment. As distribution poles and associated equipment are relatively cheap, some perceive this as a cost-

[34] In particular the presentations at the SPIDERWG February 2023 meeting. Available here: https://www.nerc.com/comm/RSTC/SPIDERWG/SPIDERWG_Presentations.pdf

effective solution to the security challenge posed by overhead distribution. However, the proliferation of DERs, the upward trend of cyber attacks against both internet of things and industrial control systems, and the potential for aggregate attack against DER ecosystems are changing these perspectives.

The common distribution system does not currently have a robust set of security requirements and controls to protect it from malicious activity. Rather, the system is currently designed around quick response to equipment damage (e.g., due to tree limbs, downed distribution poles, or other faults) and reconfiguration to maintain a high degree of reliability to their system. Current research and scenario development[35] to secure the distribution system and DERs at large is progressing rapidly, especially by review of equipment standards and implementing security controls. This research is leading to improved equipment-level standards so distribution entities can use standard equipment when integrating DERs into their system. For example, UL Solutions is seeking to investigate a way to certify the functional requirements of secure communication to limit the impact of a security compromise of a single DER at an equipment level. These updates to equipment standards and the certification of distribution equipment are anticipated to maintain the current distribution paradigm and enhance it to support a strong security posture.

Differentiation of Utility-Scale DERs versus Retail-Scale DERs landscape

The security posture between utility-scale DERs (U-DER) and retail-scale DERs (R-DER) can differ. The retail-scale may not have a private fiber connection to the utility itself and can use public networks for communication. Furthermore, the DER owners of R-DER are not able to practically acquire, implement, and maintain the above security controls and as such have no requirements to do so. In the utility-scale side there is a higher likelihood that the connection will be over a private network to the utility and may already have a small attack surface and stronger security controls inherent to the design. These end-use devices will then move towards having fewer recommended additional controls for managers of U-DERs than for management of R-DER devices. Namely, R-DER devices are assumed untrustworthy as a default. However, these categorizations do not alter the current distribution landscape as the same equipment standardization will likely be used to electrically connect both U-DERs and R-DERs to the distribution system. These categorizations are important when considering the "trustworthiness" of a type of communication and for producing standardized designs to incorporate U-DERs, R-DERs, or a combination of both into the distribution system. DER aggregators in particular should implement and maintain security controls that allow for strong protection against attack through the DER it controls regardless of U-DER or R-DER classification.

Distribution Management Systems and Emerging Distribution Landscape Considerations

Currently, efforts are ongoing to implement DERMS at various entities. These systems have functional specifications housed in the IEEE 2030.11-2021,[36] which is a guide that houses the various configurations and required functions of such a management system. Such a guide allows the functions of the DERMS to exist within an entity's premises, off-site at a cloud-based system, or a hybrid solution that interplays between the two. As stated in the guide, "it is possible to deploy a DERMS in an off-site location where the infrastructure is provided by a third-party computer hosting provider." While 2030.11 lists the various common communication protocols and concepts required to be addressed, it does not directly address the cyber security requirements of a DERMS. Rather, the guide provided other referenced material (e.g., IEEE C37.240-2014[37]) and allows the integrator of a DERMS to determine the exact cyber security requirements. The guide lists that the security of data in such deployments should be reviewed and include the following:

- Security of data in transit between on-site and off-site locations
- Security of data at the off-site locations

[35] One example of the research into recommendations and test cases for cyber security scenarios pertaining to DERs is available here: https://www.osti.gov/biblio/1832209

[36] Available here: https://ieeexplore.ieee.org/document/9447316

[37] Available here: https://standards.ieee.org/ieee/C37.240/5029/

- Security of requests sent from the off-side location to the external internet
- Backups of off-site data
- Hosting service availability

In such instances, the ongoing implementation of a DERMS will have direct tie-ins to the ongoing evaluation of cloud-hosted services and the security requirements of such applications. Most utilities at this time do not have a DERMS and likely lack the sufficient infrastructure to fully utilize a DERMS should they choose to do so. Utilities looking to implement a DERMS in order to manage and dispatch DERs should have stringent specification for cybersecurity requirements when using off-site hosting services as part of their DERMS. Furthermore, DER aggregators are assumed to require a DERMS or similar management system in order to accomplish their goal and should also require stringent cybersecurity requirements when implementing any functions of a DERMS off-site. As a first step, requiring strong cybersecurity controls as part of their service agreements with the off-site hosting service can initiate a bilateral agreement with the off-site hosting service in order to secure the DERMS from malicious interaction.

Security Posture of DER Aggregators

DER aggregators are relatively new entities to the ecosystem of aggregate control of multiple end-use devices to participate in wholesale ISO/RTO markets. The ISO/RTOs consist of the PCs, BAs, and RCs of the transmission system while the DER aggregator is a middle entity that constitutes a pathway for previously independently controlled DER assets. A DER aggregator currently does not have security requirements relative to the risk-impact it has on the bulk system nor does it have OT security requirements outside of those required by regulators over the DER aggregator. As such, the NERC SPIDERWG and SITES have assumed the following with respect to the DER aggregator:

- The DER aggregator will act to protect itself against common information technology (IT) attacks targeting personal data required to award bids.
- The protections on a DER aggregator's IT software will not allow operation technology (OT) compromise by an IT intrusion.
- The DER aggregator has minimal OT security and relies on the utility (i.e., ISO/RTOs) to dictate the required security controls on the aggregator and the DER it controls.
- The DER aggregator will use cloud solutions for their DER management due to the amount of data to process.

Confidentiality of Data at the DER and DER Aggregator

In order to conduct a proper study of the electrical impact of DER and DER aggregators, specific electrical models need to be developed and shared to represent the aggregate impact DERs have on the BPS. SPIDERWG has multiple reliability guidelines associated with the model development of aggregate DERs; however, the representation of a DER aggregator can vary; DERs should be represented with the impact they have on load flow and transient stability. As with bulk-connected resources, some information may be tied to confidential agreements between OEMs or owners, and data sharing of that confidential data is not allowed. This requirement to represent the end-use electrical equipment to study impact of aggregate DERs[38] does not require the type of data typically secured under confidential and private agreements between the DER owner, manufacturer, DER aggregator, or the utility. Entities handling DER information (e.g., TPs, PCs, DPs) should ensure that the security controls they have in place include proper data management and access controls to ensure the sharing of required modeling data can occur while maintaining a high level of confidence in the privacy-protective treatment of end-user data.

[38] Operated under a DER aggregator or in independent operation.

Chapter 3: Review of Standards, Frameworks, and Alternatives

As both DER aggregators and DERs do not have a NERC registered entity category that directly covers their applicability to NERC Reliability Standards, SPIDERWG, and SITES identified similarities where the privacy and security practices of DERs and DER aggregators may need to be examined to determine any future applicability to NERC Reliability Standards, especially concerning whether DERs or DER aggregators provide BES reliability operating services. These services are typically assessed for any impact over a 15-minute time frame. The **Table 3.1** is from CIP-002-5.1a,[39] which can help relate the electrical function provided by a registered entity and what has been identified to have a grid reliability impact. SPIDERWG and SITES note that the DER aggregator can provide some of these functions for the DER it controls in some instances; however, the capacity of the DER aggregator in a particular area can determine if the service has an impact on BES reliability operating services.

Table 3.1: Impact of Registered Entity and Associated Reliability Functions

Entity Registration	RC	BA	TOP	TO	DP	GOP	GO
Dynamic Response		X	X	X	X	X	X
Balancing Load and Generation	X	X	X	X	X	X	X
Controlling Frequency		X				X	X
Controlling Voltage			X	X	X		X
Managing Constraints	X		X			X	
Monitoring and Control			X			X	
Restoration			X			X	
Situation Awareness	X	X	X			X	
Inter-Entity coordination	X	X	X	X		X	X

In Order No. 2222 Paragraph 130, FERC specified that RTO/ISOs must "…allow distributed energy resources to provide all services that they are technically capable of providing through aggregation." If capable, the DER aggregator's DER aggregations may begin providing services that resemble BES reliability operating services. To determine whether DER aggregator cyber assets meet the definition of BES cyber assets, new and improved models for simulating a DER aggregator's impact on the Bulk Electric System will be required. Without accurate development of electrical models[40] that represent the control behavior pertinent to the functions above, completing the impact test of whether control of the asset may materially impact the bulk system requires engineering judgement. For instance, if DER aggregators are providing frequency regulation (balancing supply and demand on the electric system by changing energy injection or energy withdrawal within seconds), then the impact of rendering the DER aggregator's DER aggregation cyber asset "unavailable, degraded, or misused" within 15 minutes on the BA area should be carefully studied. A DER aggregator providing 1 MW of frequency regulation compared to a DER aggregator providing 100 MW of frequency regulation will clearly have a different level of impact on the BPS (i.e., to area control error).

[39] CIP-002-5.1a is available here: https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-002-5.1a.pdf

[40] These models can take on a variety of data sources, the most common software platforms that represent the Bulk Electric System are positive sequence models. Models here include load flow and transient dynamic representations of the behavior exhibited by DER and DER aggregator actions. Current SPIDERWG modeling documents exist for DER operating independently of a DER aggregator. It is available here: https://www.nerc.com/comm/Pages/Reliability-and-Security-Guidelines.aspx

BES Cyber Asset

The BES Cyber Asset definition can be found at the NERC Glossary of Terms and defines when Cyber Assets become BES Cyber Assets. When DER aggregators contain assets that act as a BES Cyber Asset, they should take appropriate action based on how such assets may materially affect the Reliable Operation of the Bulk Power System

Key Takeaway:
When DER aggregators contain assets that act as a BES Cyber Asset, they should take appropriate action based on how such assets may materially affect the Reliable Operation of the Bulk Power System

Limitations on Assessment and Applicability of DER, DER Aggregators, or other Distribution Entities

The *NERC Rules of Procedure* Appendix 5B's material impact test[41] defines the way in which a potentially compromised asset in the generation, transmission, or distribution of energy can impact the BES. The materials impact test questions are as follows:

- "Is the entity specifically identified in the emergency operation plans and/or restoration plans of an associated Reliability Coordinator, Balancing Authority, Generator Operator or Transmission Operator?
- Will intentional or inadvertent removal of an Element owned or operated by the entity, or a common mode failure of two Elements as identified in the Reliability Standards (for example, loss of two Elements as a result of a breaker failure), lead to a reliability issue on another entity's system (such as a neighboring entity's Element exceeding an applicable rating, or loss of non-consequential load due to a single contingency)? Conversely, will such contingencies on a neighboring entity's system result in issues for Reliability Standards compliance on the system of the entity in question? Appendix 5B – Statement of Compliance Registry Criteria (Revision 7) 8
- Can the normal operation, misoperation or malicious use of the entity's cyber assets cause a detrimental impact (e.g., by limiting the operational alternatives) on the operational reliability of an associated Balancing Authority, Generator Operator or Transmission Operator?
- Can the normal operation, misoperation, or malicious use of the entity's Protection Systems (including UFLS, UVLS, Special Protection System, Remedial Action Schemes and other Protection Systems protecting BES Facilities) cause an adverse impact on the operational reliability of any associated Balancing Authority, Generator Operator or Transmission Operator, or the automatic load shedding programs of a PC or TP (UFLS, UVLS)?"[42]

As seen by the language above, NERC identifies the material impact on the BPS through an element's ability to affect the operational state and functions performed by a BA, GOP, or TOP. A few other questions focus on distribution-enabled relaying (i.e., under frequency load shedding (UFLS) and under voltage load shedding) that DERs and DER aggregators may more strongly impact depending on feeder configuration and the specific implementation[43] of a PC's UFLS program. Many of these questions do not currently apply to OEM interactions for proprietary connections to the asset but instead deal with the element's electric impact on the BPS. Proprietary connections are allowable per 1547-2018 at the local DER interface, allowing for the DER device to be compromised and possibly leading to misoperation or malicious use if unprotected. Thus, it is important to represent the potential impact of these devices in studies that assess the performance of the BPS, including the applicable level these assets reach in NERC's

[41] Available here: https://www.nerc.com/FilingsOrders/us/RuleOfProcedureDL/Appendix%205B.pdf

[42] Taken from the NERC Rules of Procedure Appendix 5B. Available here: https://www.nerc.com/FilingsOrders/us/RuleOfProcedureDL/Appendix%205B.pdf

[43] SPIDERWG has drafted a reliability guideline on this topic, which is available here: https://www.nerc.com/comm/RSTC_Reliability_Guidelines/Recommended_Approaches_for_UFLS_Program_Design_with_Increasing_Penetrations_of_DERs.pdf

Reliability Standard CIP-002-5.1a. A thorough understanding of the interaction between DERs, DER aggregators, and utility systems is required to appropriately categorize these devices with the impact test.

BES Impact Test and Meaning

DER aggregators may potentially meet the material impact test as per the "BES Cyber Asset" definition as part of the NERC *Glossary of Terms*[44] and through the understanding of the control of assets the DER aggregator has in its system. SPIDERWG and SITES do not anticipate that any one DER outage will have the size and impact that can adversely affect the operational reliability of any associated BA, GOP, TOP, RC, or other NERC entity. Rather, the aggregate impact of DERs onto the BPS can affect the performance of the bulk system during grid disturbances. SPIDERWG has developed reliability guidelines[45] to address the modeling and verification of DERs in bulk system studies and is currently drafting guidance[46] on the studies performed that incorporate these aggregate models. Furthermore, the SITES has also identified[47] that the individual DER under malicious control has a different impact than the DER aggregator. Depending on the size[48] and control mechanisms in place, a DER aggregator may reach a level of BES impact. The SPIDERWG and SITES recommend further analysis in this area to determine the impact of a DER aggregator (or similar entity) has on the BES.

Security Standards, Frameworks, and Alternatives

Outside of the NERC CIP standards, other governmental and national labs have provided frameworks to categorize multiple aspects of a strong security posture for the electric ecosystem. Other cybersecurity forums have also provided certification, tests, and other communication protocols that enhance the efficacy of modern security controls. In some instances, these alternatives can include resilience focused projects that do not fully rely on security controls, akin to how many distribution companies have "hot swappable" equipment. Some of these alternatives include the following:

- The Cybersecurity Capability Maturity Model,[49] which is a tool for organizations to evaluate cybersecurity capabilities for IT and OT environments
- The Distributed Energy Resource Cybersecurity Framework[50] by NREL, which is a tool designed specifically to evaluate the cybersecurity posture of DERs for the U.S. federal government
- Idaho National Lab's Standards to Secure Energy Infrastructure,[51] which allows for quick searches of applicable standards or guidance material in this area
- Underwriter Laboratory Cybersecurity Assurance Program,[52] which offers a suite of tools, testing, and certifications (e.g., UL 2941[53]) to manage and apply commercially available cyber security capabilities
- Sunspec's Cybersecurity Certification Program,[54] which also seeks to certify functions for DERs, particularly for compliance to IEEE 2030.5

[44] Glossary of terms here: https://www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf

[45] The SPIDERWG reliability guidelines are available here: https://www.nerc.com/comm/Pages/Reliability-and-Security-Guidelines.aspx

[46] See SPIDERWG Work Plan, available here: https://www.nerc.com/comm/RSTC/SPIDERWG/SPIDERWG%20Work%20Plan.pdf

[47] Identified in *Cyber Security for Distributed Energy Resources and DER Aggregators*, available here: https://www.nerc.com/comm/RSTC_Reliability_Guidelines/White_Paper_Cybersecurity_for%20DERs_and_DER_Aggregators.pdf

[48] For reference, the CIP-002-5.1a Medium impact threshold for generator control centers is 1,500 MW of active power resources and 1,000 MVAR of reactive power resources

[49] Available here: https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2

[50] Available here: https://dercf.nrel.gov/

[51] Available as part of the Office of Cybersecurity, Energy Security, and Emergency Response here: https://energyicsstandards.inl.gov/

[52] Available here: https://www.ul.com/services/ul-cybersecurity-assurance-program-ul-cap

[53] Standard available here: https://www.shopulstandards.com/ProductDetail.aspx?productId=UL2941_1_O_20230113

[54] Available here: https://sunspec.org/sunspec-cybersecurity-certification-work-group/

- Sandia National Lab's Recommendations for Distributed Energy Resource Access Control,[55] which provides a framework to minimize the risk of unauthorized access to DER systems.
- The National Institute of Standards and Technology's set of protocol[56] standards, which define information system security practices.

Many of these alternatives are self-answered questionnaires that highlight areas of improvement for an organization to build new capabilities or leverage existing technology to improve their cyber security postures. As such, SPIDERWG and SITES encourage DER owners, DER aggregators, and similar entities to leverage these more exhaustive tools in addition to the recommendations found in this paper.

Market rules may also offer an avenue for enhanced cyber security measures for DERs as they dictate the participation requirements for each participant in the energy market. It is outside the scope of this paper to evaluate particular markets for their structure or adequacy in meeting cybersecurity objectives; however, market rules that specify heightened cyber security postures for all participants may be an avenue to ensure DERs and DER aggregators maintain cyber security practices in both the IT and OT environments. ISOs and RTOs are encouraged to incorporate reliability-focused security practices in their rules such that the reliable operation of the BPS is not compromised by latent or unknown security threat by the participants of the electric market. Utilities are likewise recommended to ensure proper cyber security hygiene when integrating command and control over DERs into their distribution control centers or DERMS.[57]

Sponsored certification programs reach a sort of standardization depending on the test bed and protocol. One example from the NREL aims to provide testing and certification procedures[58] for common cyber security controls. Additionally, NREL is also working to build a framework[59] that identifies the common threats against DERs in order to standardize incident response and other key players in securing the DER landscape.

National and International Lessons Learned

Current efforts to aggregate DER control and dispatch include the PG&E VPP pilot project[60] with Tesla to leverage distribution-connected battery energy storage systems during times of high peak demand. At the time of this paper, these efforts have led to many thousands of end-users supplying a peak power output of nearly 30 MW of generation during times of high strain on the grid. Internationally, vehicle-to-grid initiatives that aggregate the ability for electric vehicles to discharge when called upon by the system operator have had some success in the European Union. One of the European Union's vehicle-to-grid VPP programs is looking to a pilot project[61] to provide short-term frequency response to grid disturbances with strong collaboration between the grid operator and the VPP operator. These pilot projects have the same structural compositions seen by DER aggregators.

Furthermore, it is known that many cyber security recommendations, standards, and frameworks speak to a limited scope of applicable assets, threats, and known threat actors. In areas like DERs and the distribution system security

[55] Available here: https://www.osti.gov/biblio/1765273

[56] Primarily NIST's *Security and Privacy Controls for Information Systems and Organizations*, available here: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final, and their Technical Note 2182, available here: https://nvlpubs.nist.gov/nistpubs/TechnicalNotes/NIST.TN.2182.pdf.

[57] A DER Management System is identified in the IEEE 2030.X family of standards. Particularly 2030.11-2021, which can be found here: https://standards.ieee.org/ieee/2030.11/7259/

[58] Available here: https://www.nrel.gov/docs/fy22osti/80581.pdf

[59] Available here: https://www.nrel.gov/docs/fy20osti/75044.pdf. Other work by NREL includes supply chain concerns (https://www.nrel.gov/docs/fy23osti/84752.pdf) and measuring framework compliance by an emulated environment (https://www.nrel.gov/docs/fy23osti/84079.pdf)

[60] Information related to this pilot program can be found on PG&E's website for the Emergency Load Reduction Program. Available here: https://elrp.olivineinc.com/

[61] Information for this one particular project is available here: https://www.next-kraftwerke.com/products/balancing-energy. For this pilot, available lessons learned can be found at the integrating German utility, available here: https://www.amprion.net/

landscape, many of these frameworks are vague in their applicability to the threats facing DERs, DER aggregators, and the distribution system at large. This is largely due to inherent assumptions, a lack of threat information sharing, and assumed minimal threat of distribution facilities.

Entities that lack specific threat information sharing have found that technical design specifications and framework adaptations improve the overall reliability of their system. To improve the reliability of the entire electric ecosystem, this should also include threats facing the distribution system. Current advancements in this area include specifying technical security requirements[62] that historically have not existed for DERs.

[62] One example of these specifications comes from NREL. Their report on functional specifications is available here: https://www.nrel.gov/docs/fy22osti/79974.pdf

Chapter 4: Conclusions and Recommendations to DER and DER Aggregators

While there are a variety of security controls available to DER aggregators and owners, some controls are better suited at the end-user device (i.e., the DER) or at the entity that controls aggregate DERs (e.g., DER aggregator or VPP). The types of security controls, types of mitigated attack, implementation notes and recommended entity for these security controls are summarized in Table 4.1. This table is a summary of the information contained in the above sections. Furthermore, DER aggregators implementing a DERMS all or in-part at an off-site hosting service should ensure that strong cyber security requirements are in the service agreement, including similar or greater protection than at their own premises.

Table 4.1: Security Control Recommendations

Security Control	Types of Attacks Mitigated by Proper Control Implementation	Applicable Entitles	Implementation Notes
Internal Network Security Monitoring	Phishing, Active Scanning, Gathering Victim Network or Organization Information, Malware Deployment	DER Aggregators	INSM alerts and logs may be inputs for other activities, such as automated responses, forensics, or incident response.
DER Gateways	Man in the Middle, Malware Deployment, Denial Of Service, and Replay Attacks	DER Aggregators**	DER gateways are currently under development for technical specification and may change per IEEE P1547.10 outcomes.
Remote Access Controls	Unauthorized External Remote Access, Trusted Relationship Compromises, Remote System Discovery, and Most Forms of Reconnaissance	All Entities*	DER aggregators in particular should enable strong remote access security controls on the DERs they control.
Data Management and Access Controls	Credential Harvesting or Access, Privilege Escalation, Account Manipulation; and a Broad Set of Data Deletion, Encoding, Obfuscation, or Manipulation	DER Aggregators**	These controls can also be used to mitigate privacy concerns by end-users as well as their intended security functions.
Network and Protocol Security	a Majority of Current and Future Cyber Security Threats	DER Aggregators	Certain endpoints in the chosen DER aggregator's environment may not support all desired protocols. The implementation of these controls may be software-based, specifically for cloud implemented controls.

* denotes that a DER owner's implementation of the control doesn't need to be as sophisticated as DER aggregators or utilities
** denotes that, while DER aggregators are applicable, the control may require DER owner coordination to implement

The SPIDERWG and SITES joint team has developed recommendations for the ISO/RTOs (collectively registered as BAs and RCs), DER aggregators, and DERs in order to enhance the security posture of the electric ecosystem. Cyber attacks that utilize simple social engineering or other low-level tactics can readily compromise credentials, making security controls based on credentials alone insufficient. DERs constitute a large attack surface with potentially thousands of entry points into a network, so the compromise of any one side of a communications network can allow for interconnected networks to also become compromised, potentially facilitating malware propagation and malicious actor lateral movement (e.g., DER devices, DER aggregator networks, and utility networks). With an ever increasing number of DER access points, robust security controls are high priority to ensure the security of the electric grid.

To that end, SPIDERWG and SITES jointly developed the following high-level recommendations for the ISO/RTOs:

- ISOs/RTOs should ensure that their market rules do not prohibit entities from enhancing their cyber security posture beyond a minimum level of protection.
- ISOs/RTOs should also explore and consider market rule enhancements that encourage participants to incorporate cyber security best practices while not imposing a risk to the reliable operation of the BES. This is part of proper cyber hygiene for entities.

SPIDERWG and SITES also jointly developed the following high-level recommendations for DER aggregators:

- DER aggregators should implement proper data management and access controls for its network in order to assure confidentiality of private data as well as mitigate against specific cyber attacks. DER aggregators should start by performing a privacy impact assessment[63] and implement the necessary data management and access controls identified as needed from the assessment.
- DER aggregators should implement strong network access controls, particularly for remote access, and require multi-factor authentication for remote access of their network and applications.
- DER aggregators should implement strong internal controls, such as intrusion detection systems, so they are notified of a compromise and can take proper actions to mitigate it.
- DER aggregators should ensure endpoint controls, such as through DER gateways, are deployed at DER sites where a gap exists.

Furthermore, SPIDERWG and SITES jointly developed the following high-level recommendations for DERs:

- DER owners should ensure they wipe personal information from old hardware and, to the degree possible, implement data management and access control to their network. In particular, U-DERs should implement strong access controls.
- DER owners should understand agreements with DER aggregators, including the criteria for the proper use and handling of their personal data, including data exchanged with third-parties and requirements related to the DER owner's prior consent.
- U-DERs should implement network access controls as much as possible, particularly for remote access. For programmatic remote access, public key infrastructure through a DERMS or other management system by the utility should be enabled.

State Coordination of Implementation of Recommendations

FERC Order 2222 does not specify requirements for cyber security and data privacy. Rather the order recommends that "… that RTOs/ISOs coordinate with distribution utilities and relevant electric retail regulatory authorities (e.g., state PUCs) to establish protocols for sharing metering and telemetry data, and that such protocols minimize costs and other burdens and address concerns raised with respect to privacy and cybersecurity." Due to the various

[63] These assessments evaluate the data exchange and storage that may potentially hold energy consumption data that infers customer behaviors or personally identifiable information. Common assessment tools also include follow-up recommendations based on the identified risk exposure in the assessment.

jurisdictions on utility procedures and security measures, strong collaboration and coordination among transmission and distribution entities is highly recommended.

The overall security posture of the BPS can be impacted by the potential security risks associated with DERs or DER aggregators, and SPIDERWG and SITES recommend that DER aggregators register for NERC standards applicability when they act as BES cyber assets that can impact the reliability of the BES. The recommendations above should be coordinated with appropriate and open stakeholder engagement where the security measures and controls are agreed on for the local distribution system. These entities can assist in building the design basis threat or other risk assessment that prioritize the most effective security controls to mitigate their anticipated threats. State coordination is a high priority where DER-site-specific physical security measures are identified.

In general, the key risk considerations in this broader coordination effort[64] include data privacy for both personal and market data, data integrity among entities, and data availability.

Data Confidentiality

Per FERC Order 2222, RTOs/ISOs must revise their tariffs such that DER aggregators provide "a list of the individual resources in its aggregation, necessary information that must be submitted for individual DERS, and retain performance data for individual DERs." Entities participating in energy markets must be aware of data privacy regulations, understand the potential impact to customer privacy in the event of data-loss-events, and ensure both technical and procedural controls are implemented for data transparency and protection for consumer data. The recommended coordination should identify these and similar confidentiality requirements, especially as they relate to protecting against a widespread DER compromise.

Data Integrity

Entities should coordinate development of cyber security criteria for DER systems and communication protocols used for interoperability and data exchanges, include NIST-approved cryptographic suites and protocols to protect against data manipulation, and establish protocols to ensure adequacy of security control implementations. Testing standards for DER systems and communication protocols should also be included in the implementation of recommendations.

Data Availability

Risk assessment methodologies need to be created in order to evaluate a grid entity's role in the electric sector and the associated security control and redundancy measures these roles must adopt and maintain. These measures can account for various financial, safety, reliability, privacy considerations that result from cyber attacks against the entity's systems and data.

[64] Additional resources on how this participation in markets can be influenced by DER aggregators is available at here: EPRI, DER Aggregation Participation in Electricity Markets: EPRI Collaborative Forum Final Report and FERC Order 2222 Roadmap, Palo Alto, 3002020599

Chapter 5: Contributors

NERC wishes to thank the following subject matter experts for contributing to this document. NERC also wishes to thank NREL and EPRI for their contributions and review of the white paper.

Name	Entity
John Biasi	Burns and McDonnell
Dan Kopin	VELCO
Jens Boemer	EPRI
Jose Cordova	EPRI
Xavier Francia	EPRI
Abrez Mondal	EPRI
John Schmall (SPIDERWG vice chair)	ERCOT
Shayan Rizvi (SPIDERWG chair)	NPCC
Shannon Mickens	SPP
Morgan King	WECC
Nick Hatton	WECC
Sam Chanoski	INL
Karl Perman	CIP Corps
Jordan Petersen	NREL
Danish Salem	NREL
Ryan Cyar	NREL
Tom Hofstetter	NERC
Dan Goodlett	NERC
Larry Collier (SITES Coordinator)	NERC
JP Skeath (SPIDERWG Coordinator)	NERC