NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

# Cyber Security for Distributed Energy Resources and DER Aggregators

NERC Security Integration and Technology Enablement Subcommittee (SITES) White Paper
December 2022

## Purpose

This brief paper provides industry with information regarding activities underway to further secure the electricity ecosystem under rapid grid transformation, specifically in the area of cyber security efforts for distributed energy resources (DERs) and DER aggregators. NERC is working with industry stakeholders to advance cyber security controls for DERs as the penetrations of these resources continue to grow in many areas across North America. This paper is informational and seeks to help provide clarity and guidance to industry stakeholders in this area.

## Defining DER and DER Aggregator

The NERC System Planning Impacts from DERs Working Group (SPIDERWG) defines a DER as "any source of electric power located on the distribution system."[1] This definition specifically focuses on those resources in the distribution system that can produce electric power (i.e., a generating resource) and does not include end-use loads or demand response as part of the DER definition. Conversely, the Federal Energy Regulatory Commission (FERC) DER definition outlined in FERC Order 2222[2] does consider load elements, including demand response, energy efficiency, and electric vehicles. The expanded FERC definition includes all DER types able to participate in regional organized wholesale electricity markets through aggregation (DER aggregators).

This document will generally refer to DERs with the NERC definition while acknowledging that DER aggregators may include DERs (with the FERC definition) that are load elements and not generating elements where used. This nuance does not critically impact the key points being made in this paper.

## Understanding Security of the Electricity Ecosystem

The bulk power system (BPS) historically only included large, centralized power plants with power flowing across the transmission system, down through the distribution networks, and then to end-use consumers. A significant portion of this system was operated either with analog controls or very limited digital connectivity. However, the power system of today is undergoing a rapid transformation; the generation base is moving towards clean energy renewable resources connected through inverter technology. Large synchronous generation sites are being retired and replaced with smaller wind and solar resources, battery energy storage, and hybrid power plants. BPS connected resources are also being offset with DERs that connect to the distribution system, some of which are behind-the-meter and owned and operated by end-use consumers or third parties. Many of these systems are now connected directly to the Internet as digitalization and its associated connectivity continue to expand exponentially. Grid planners, designers, and operators are faced with managing a grid with a significant portion of the resource base connected to the distribution system with little to no direct visibility of these resources. FERC Order 2222 introduced the DER

[1] https://www.nerc.com/comm/RSTC/SPIDERWG/SPIDERWG%20Terms%20and%20Definitions%20Working%20Document.pdf
[2] https://ferc.gov/media/ferc-order-no-2222-fact-sheet

aggregator, which will be another entity in the electricity ecosystem that will play a key reliability and security role moving forward.

This paper focuses on the security aspects of the overall electricity ecosystem. The NERC Critical Infrastructure Protection (CIP) standards apply only to bulk electric system (BES) cyber systems and their associated BES cyber assets as outlined in the currently effective version of NERC CIP-002.[3] In general, the NERC CIP standards are not applicable to systems or assets connected to the distribution system. Historically, this has not been a significant risk since those systems did not have a significant impact on the overall BPS or BES. However, the changing nature of the resource mix, the potential security risks posed through DER aggregation, and the absence of regulatory standards could all present significant risks to the BPS if not properly mitigated.

Therefore, it is important to understand how the various cyber security standards, requirements, practices, and industry efforts are working together in order to secure the overall electricity ecosystem now and moving forward. Equipment needs to be built with secure technological capabilities and with suitable equipment certifications. Operational risk assessments (and mitigations) are needed to secure these systems in real-time.

## Background on IEEE 1547-2018 Standard and Linkage to UL Listing

IEEE 1547, *Standard for Interconnection and Interoperability of Distributed Energy Resources with Associated Electric Power Systems Interfaces*, was completely overhauled with the revision that was published in 2018 (IEEE 1547-2018).[4] The update to the standard focused on the technical specifications, testing, and interoperability between distribution providers and DERs; it did not include cyber security requirements for DERs. IEEE 1547.3-2007, *IEEE Guide for Monitoring, Information Exchange, and Control of Distributed Resources Interconnected with Electric Power Systems*, was originally focused on interoperability, monitoring, information exchange, and DER control but initially did not include any considerations for cyber security. The IEEE P1547.3 working group is currently revising the guide, now titled *IEEE Draft Guide for Cybersecurity of Distributed Energy Resources Interconnected with Electric Power Systems*, to focus directly on cyber security measures and controls for DERs. IEEE standards are wholly voluntary and must be put into effect by a certifying organization or other Authority Governing Interconnection Requirements (AGIR).

IEEE 1547-2018 is being implemented across North America by AGIRs (e.g., state public utility commissions, regional system operators, and distribution entities). Entities can ensure that equipment being manufactured complies with the requirements of IEEE 1547-2018 based on the conformance testing procedures outlined in IEEE 1547.1-2020. This standard specifies the type, production, commissioning, period tests, and evaluations that shall be performed to confirm that equipment conforms to IEEE 1547-2018. Underwriters Laboratories (UL) 1741, *Standard for Inverters, Converters, Controllers and Interconnection System Equipment for Use with Distributed Energy Resources*, is primarily a safety standard that certifies equipment pass the tests outlined in IEEE 1547.1. This enables manufacturers to certify that commercially available DERs meet the requirements of IEEE 1547-2018. **Figure 1** shows a high-level illustration of the overall process.

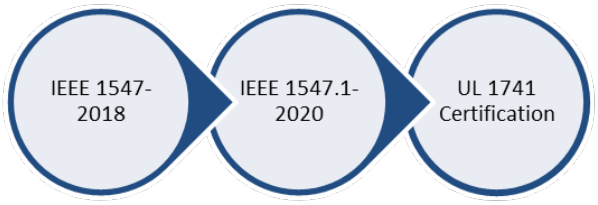


**Figure 1: IEEE 1547-2018 Standard to UL 1741 Certification**

[3] https://www.nerc.com/pa/Stand/Reliability%20Standards/CIP-002-5.1a.pdf
[4] https://standards.ieee.org/ieee/1547/5915/

## Cyber Security Certification Standards Efforts

Many cyber security standards, guides, and recommended practices exist today. Each has its strengths and weaknesses. Some in-depth documents are written for product types outside of the Renewables space, whereas some documents written for Renewable Energy technology do not incorporate mandatory language for certification. To this extent, for certification purposes, there are no standards and test procedures available with a complete list of detailed auditable requirements. Since the cyber security features are spread out over multiple guides and standards, there is a need to conjoin applicable materials to produce a single standard with requirements and testable items that covers the full scope of DER cyber security certification in an understandable format for industry stakeholders. In general, these standards and guides are used to complement each other, however the standards-development effort will also filter out contradicting, outdated, or compromised technology requirements. By thorough filtering and selection, as well as stakeholder input, the requirements and testable items are defined. A national or international cyber security certification standard can aid industry stakeholders to evaluate and validate the cyber security posture of their DER or IBR devices before they are connected to the electric grid. A unified standard will not only facilitate robust cyber security within the electric grid, it will also ensure the concept of security by design is being implemented beginning at the device level for new DER systems.

### Roadmap for UL Cyber Security Certification Standard

Drafting consensus-based cyber security certification standards requires effective industry leadership and regular participation from stakeholders. UL intends to make use of the best practices in existing DERs and industrial cyber security bodies of knowledge to create a standard intended specifically for certification by UL as an independent and accredited third-party laboratory (see **Figure 2**).[5] UL plans to offer this cyber security certification service in addition (or as a stand-alone service) to its existing electrical safety certification services. An initial draft of the new UL standard is expected to be available for circulation among interested experts in 2022. Feedback will be gathered and suggested changes incorporated during Q3/Q4 of 2022 with publication of a UL standard by year's end. NREL and UL can streamline this effort by using in-house expertise, state-of-the-art testing facilities, and by engaging industry experts to participate in the associated UL Standards Technical Panel. UL will begin offering cyber security evaluations and certifications upon publication.[6] This cyber security standard certification will advance the security by design principle for the next generation of technologies and will be applicable to both distributed generation and storage technologies. In 2023, UL will take the further step of assembling a standing committee of industry experts to provide ongoing input for continuous improvement and potential submission to the American National Standard Institute (ANSI) to become and accredited ANSI standard. **Figure 3** illustrates this process.

[5] https://www.nrel.gov/docs/fy22osti/81827.pdf
[6] https://www.ul.com/news/ul-and-nrel-announce-cybersecurity-testing-recommendations-distributed-energy-resources-and

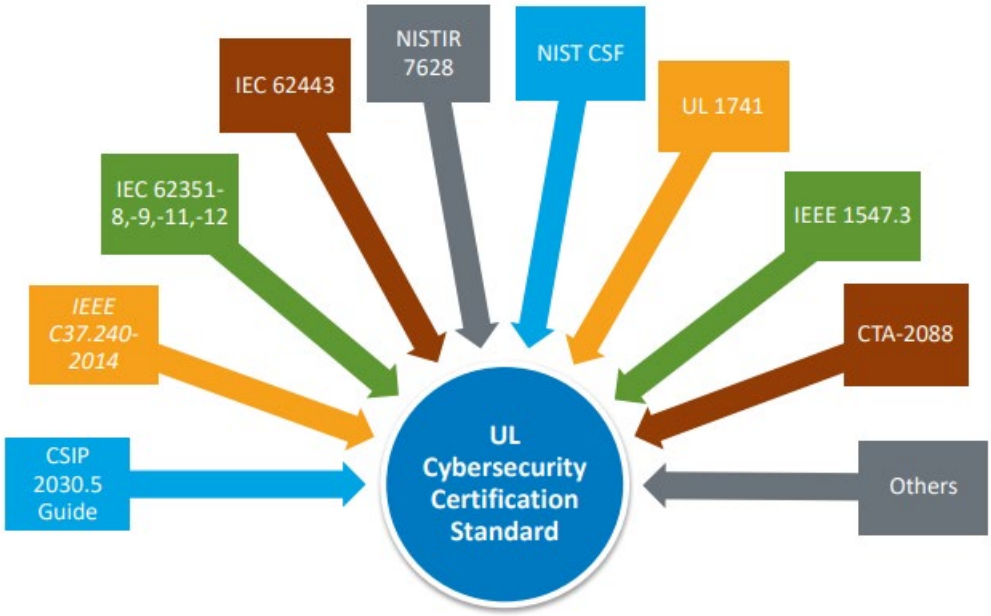


**Figure 2: Inputs to UL Cyber Security Certification Standard [Source: NREL]**

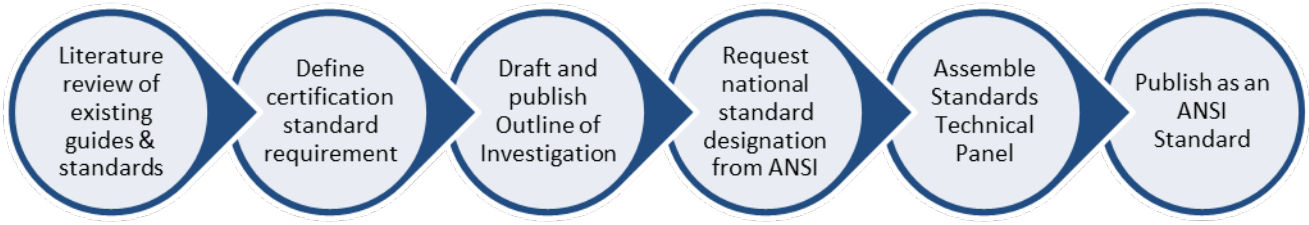


**Figure 3: Process to UL Certification and ANSI Status**

## Operational Security Posture of DERs

UL cyber security certification will help ensure that future DERs being installed on the grid will have security incorporated into the equipment by design. This process ensures that an adequate level of security features and controls are integrated into these system components during manufacturing and that they are tested and ready to be enabled by the user. However, these features need to be utilized to ensure a strong security posture across the entire electricity ecosystem during real-time operations. The certification of equipment capabilities and security features does not ensure that those systems are installed and operated with these security features utilized (see **Figure 4**). Simply having the security control functions present in the equipment does not guarantee that the controls are enabled and configured. For example, a device-level firewall that is not enabled or enabled without proper settings does not achieve the intended security objective for real-time operations. This presents BPS risk and is further reinforced by the fact that some DER classes are owned by end-use consumers (e.g., rooftop solar PV systems) and connected directly to the Internet. Often, this equipment is not intended to be programmatically accessed, configured, or otherwise alerted by the consumer from a security perspective. Additional mitigations are required.

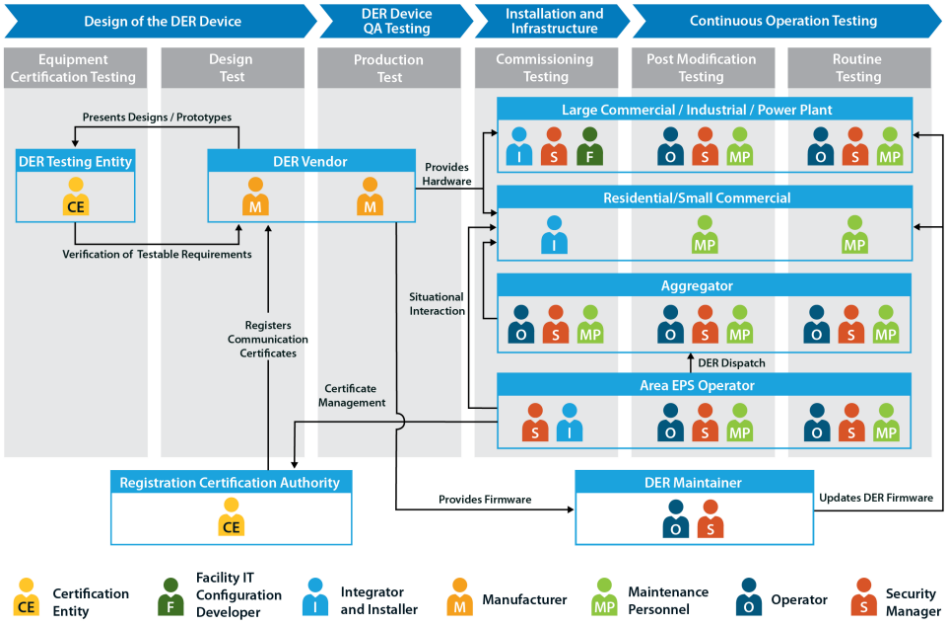


**Figure 4: Roles and Responsibilities for DER Cyber Security [Source: NREL][7]**

The NERC CIP standards ensure that registered entities meet minimum requirements for BES cyber systems and can demonstrate compliance by those systems operationally; however, those standards and associated requirements are generally not applicable to entities or asset owners on the distribution system. Therefore, these systems pose a potential security risk for secure delivery of generation to end-use loads and could lead to vulnerabilities being exploited, potentially affecting many aggregated assets during an inevitable attack from cyber threat actors.[8]

Including DER assets (and asset owners) within the NERC CIP standards construct is not an effective short-term solution to this problem due to the scale and magnitude of assets and owner/operators of DERs. DER devices should be certified and tested so that the equipment is capable of enhanced security measures. AGIRs should ensure that these functions are configurable post-installation, and the specific security controls and implementations should be engineered to mitigate known and potential threats to the electric sector by utilizing a risk-based approach. NERC will work with industry groups (e.g., the National Association of Regulatory Utility Commissioners), distribution providers, and other key stakeholders to help support the operational security of DERs moving forward.

## Cyber Security Risks of the DER Aggregator

Introduced in FERC Order No. 2222, the DER aggregator is a market entity that is able to collect and aggregate multiple DER owners and leverage their collective capacity in order to participate in an electrical wholesale market. The DER aggregator will typically use existing communication networks to provide telemetry and other information from the DER to the DER aggregator and up to the independent system operator/regional transmission organization. Those communications networks are likely owned by third-parties and many individual DERs are likely Internet-connected and accessed through routable protocols. ***The reliability and cyber security risks posed by the DER aggregator are not the same as those posed by individual DERs since the potential compromise of a DER Aggregator could have a significantly greater aggregate impact to the BPS. The compromise of any one DER is likely to have a minimal impact on the BPS; however, the compromise of a DER aggregator could affect hundreds or thousands of individual assets controlled by a centralized DER aggregator.***

[7] https://www.nrel.gov/docs/fy22osti/81827.pdf
[8] https://csrc.nist.gov/glossary/term/threat_actor

DER aggregators have a unique role in the system and they have no standardized cyber security requirements pertaining to their function in the electricity sector. Additionally, they are not anticipated to incorporate as a "control center" in the traditional sense. The system they bid into is operated by and secured by the market operator (ISO/RTO), and their operating signals are for non-owned equipment that previous sections of this paper have described as moving towards an enhanced cyber security posture through UL certification. However, the interfaces they connect across and infrastructure they use to monitor and control their equipment are likely to be conventional Enterprise information technology (IT) equipment protected under an IT security program. Such security controls may be lacking in the operational technology (OT) environment.

If compromised, the DER aggregator can impact a large amount of electrical assets (in MVA). The possible inclusion of cyber security certification of the equipment under a DER aggregator's control should not be viewed as ensuring proper security controls are in place for the DER aggregator's OT systems. Device level UL certification is a good first step, but DER aggregators should adopt an OT cyber security program that includes security controls that address the risks associated to their unique role in a secure electric infrastructure.

Currently available reference material can be used to assist both OEM's of DER technologies[9] and DER aggregators[10] in securing devices as well as communications used for monitoring and control of DERs. Additionally, the update to IEEE 1547.3 with guidelines on DER cyber security is available as draft.[11]

## Recommended Industry Actions Moving Forward

The following are recommended actions that NERC and its stakeholders should take to support a secure electricity ecosystem with increasing levels of DERs (generation), load-side flexible resources, and DER aggregators:

- **DER Cyber Security Certification:** NERC and industry stakeholders should actively support DER cyber security certification initiatives and provide expertise related to BPS impacts of growing DERs and the introduction of the DER aggregator. Efforts such as those pursued by UL to ensure that future DER equipment is designed, tested, and commercially installed with sufficient cyber security controls in place will help secure the overall electricity ecosystem. Without necessary cyber security controls designed in to the components and systems, security risks could be introduced and expensive and/or less effective bolt-on security measures could be necessary in the future.
- **Cyber Security in Distribution Interconnection Requirements:** Similar to how the AGIR establishes necessary equipment performance specifications in IEEE 1547, the AGIR could also be responsible for establishing requirements that ensure newly interconnection DERs are equipped and operationally configured with specific cyber security controls in place. This will require modifications to the IEEE 1547 standard to ensure that cyber security is included in the standards body rather than as an informational guide (i.e., focusing on including some or all aspects of the IEEE 1547.3 guide into the main body of the IEEE 1547 standard).
- **DER Aggregator Registration:** NERC and industry stakeholders have acknowledged that the concept of the DER aggregator is not presently addressed in NERC registration criteria, constituting a reliability and security gap if DER aggregators start actively controlling and operating significant amounts of DERs. In aggregate, these resources will have an impact on the BES. The NERC Reliability and Security Technical Committee and its stakeholder groups should determine the extent of DER aggregator participation in wholesale electricity markets today and in the future and identify possible reliability and security risks these entities could pose if

[9] https://www.nist.gov/itl/applied-cybersecurity/nist-cybersecurity-iot-program/nistir-8259-series
[10] https://csrc.nist.gov/publications/detail/sp/1800-32/final
[11] https://standards.ieee.org/ieee/1547.3/10173/

compromised. NERC will assess these reliability and security impacts and determine if the DER aggregator should be included as a NERC registered entity under certain situations.

- **Proactive Understanding of DER and DER Aggregator Cyber Security Risks:** Industry stakeholders should actively engage in understanding the risk posed with growing levels of DERs and the introduction of DER aggregators. Cyber security risks exist throughout the product lifecycle: equipment design, testing, commissioning, and operation. Understanding the aggregate risks posed by DERs and DER aggregators and how to mitigate them will better posture the BPS for reliable operation of DERs.