

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Cybersecurity Certification Standard for Distributed Energy Resources

Ryan Cryar, Cybersecurity Researcher
National Renewable Energy Laboratory
NERC DER Workshop
December 14th, 2022

RELIABILITY | RESILIENCE | SECURITY



- Why should we care about developing DER cybersecurity certification now?
- Solar is 3% of today's electricity generation
- Rooftop and small solar in the Western Interconnection is approximately 30,000 MW
- This represents about 65% of all solar in the west, none of which is required to follow NERC CIP

A national or international cybersecurity certification standard can aid industry stakeholders to evaluate and validate the cybersecurity posture of the DER devices before they are connected to the electric grid.



Photo by Dennis Schroeder, NREL 22168

CNN

Biden administration says solar energy has the potential to power 40% of US electricity by 2035

Nilsen, Ella. CNN.com, September 8, 2021. [url](#)

Reuters

Solar energy can account for 40% of U.S. electricity by 2035, according to DOE

Volcovici, Valeri. Reuters.com, September 8, 2021. [url](#)

NBC

Nearly half of U.S. electricity could come from solar by 2050, Biden administration

Lederman, Josh. NBC.com, September 8, 2021. [url](#)

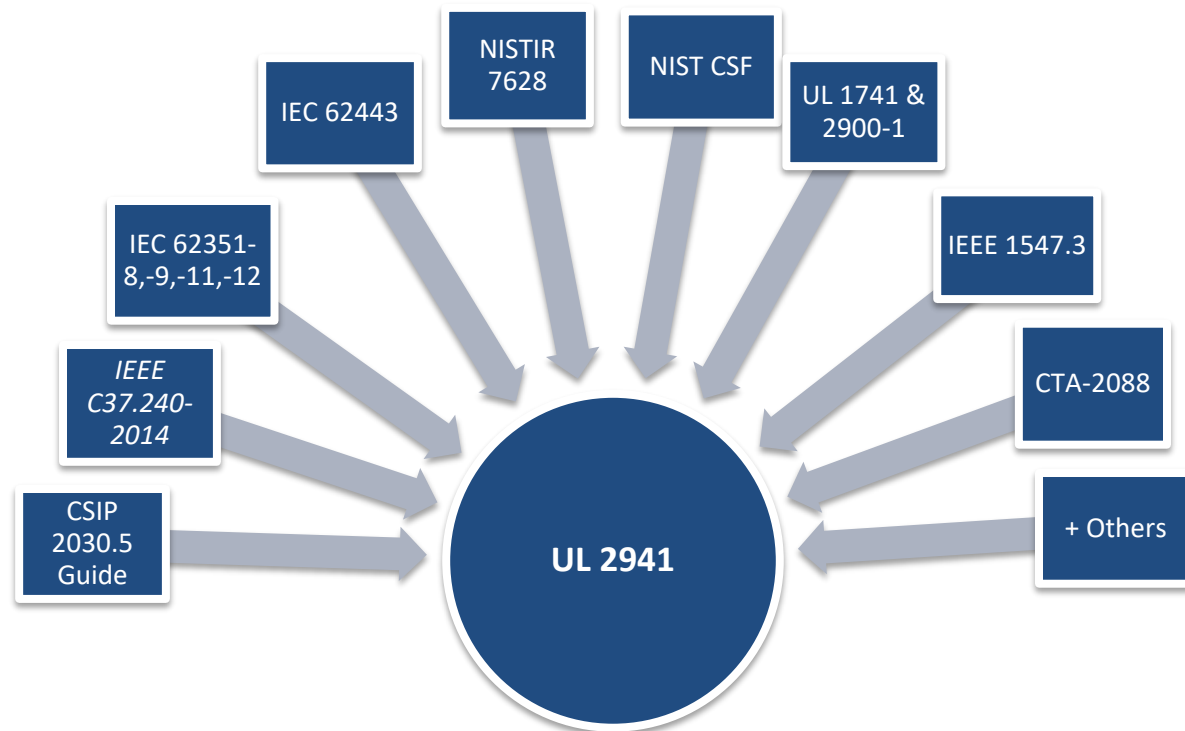
NERC

Variable-energy resources ...continue to be a significant component of new capacity

NREC Planning Committee Meeting, June 6, 2017. [url](#)

The UL cybersecurity certification standard will:

- Build on past work
- Map and leverage security requirements from industry best practices for hardware and software
- Provide an information hub for DER Industry stakeholders
- Establish “Security by Design”
- UL will lead development of the cybersecurity certification standard.



*Note: All these standards serve a different purpose.
The UL cybersecurity certification standard will not replace them by any means.*

PRESS RELEASE

UL and NREL Announce Cybersecurity Testing Recommendations for Distributed Energy Resources and Inverter Based Resources

UL and the National Renewable Energy Laboratory will complete an Outline of Investigation as a precursor to the first cybersecurity certification standard for distributed energy resources.



[Home](#) > [News](#) > [UL and NREL Announce Cybersecurity Testing Recommendations for Distributed Energy Resources and Inverter Based Resources](#)

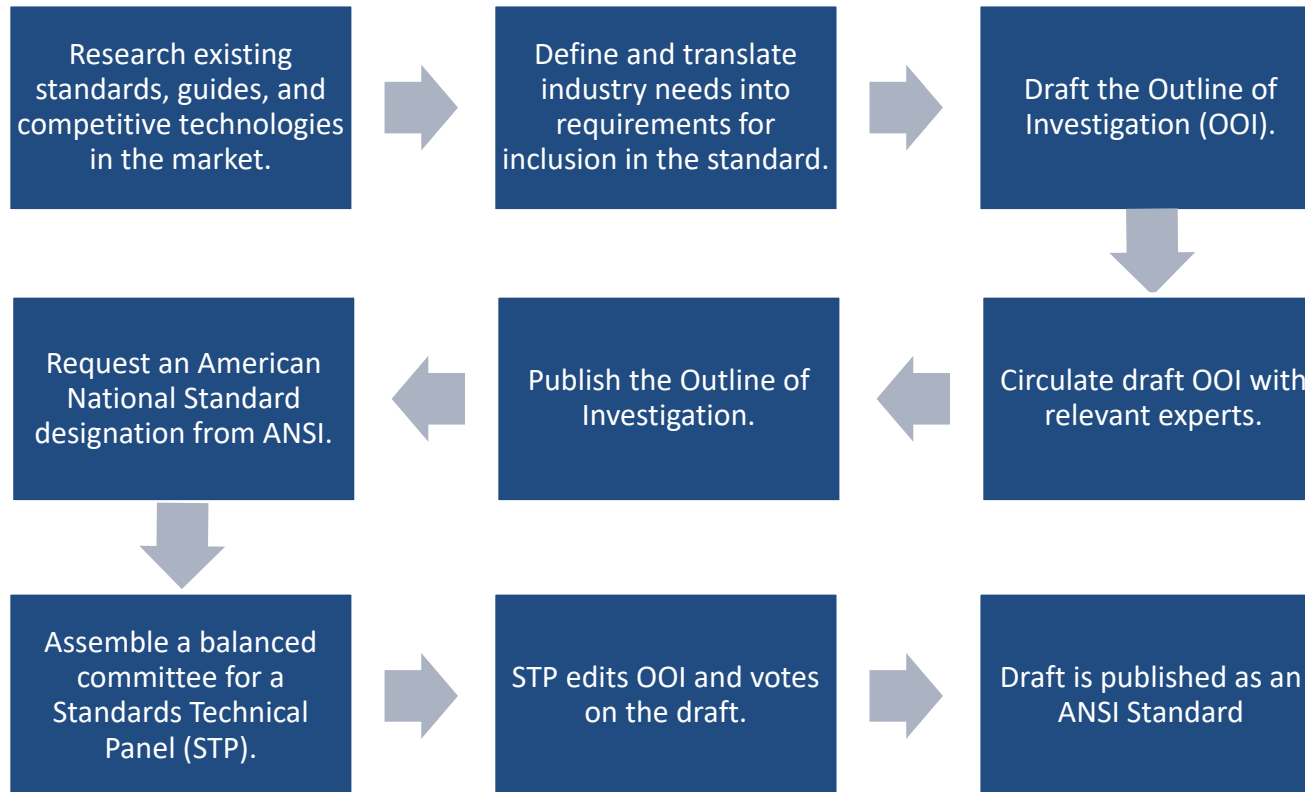
March 7, 2022

NORTHBROOK, Illinois - March 7, 2022 - UL, a global safety science leader, has released a report, co-authored with the U.S. Department of Energy's (DOE's) National Renewable Energy Laboratory (NREL), titled "Cybersecurity Certification Recommendations for Interconnected Grid Edge Devices and Inverter-Based Resources." The report includes recommendations that enable distributed energy resources (DER) and inverter-based resources (IBRs) to maintain a strong cybersecurity posture.

With support from DOE's Solar Energy Technologies Office, UL will continue working with NREL on developing requirements to support cybersecurity certification standards for DERs and IBRs. NREL and UL are currently working on an Outline of Investigation for a standard that will apply to energy storage and generation technologies on the distribution grid, including photovoltaic inverters, electric vehicle chargers, wind turbines, fuel cells and other resources essential to advancing grid operations. These new requirements will prioritize cybersecurity enhancements for power systems dealing with high penetration inverter-based resources, including those interfacing with bulk power systems for periods of instantaneous high wind, solar and hybrid/storage generation. It will also help ensure cybersecurity is designed into new IBR and DER systems.

"Currently, there are no cybersecurity certification requirements to which manufacturers and vendors can certify their DER and IBR devices against an established and widely adopted cybersecurity certification program. The development of these new cybersecurity certification requirements will provide a single unified approach that can be taken as a reference for performing the testing and certification of DERs before being deployed and while in the field," said Kenneth Boyce, senior director for Principal Engineering, Industrial, group at UL. "Drafting comprehensive certification requirements with peer review requires effective leadership and stakeholder participation. We are pleased to be working with NREL in this effort to bring additional performance-based security to electrical grid infrastructure."

- The requirements will provide a single unified approach for testing and certification of DERs in *advance* of deployment.
- The certification will be applicable to generation and energy storage technologies.
- UL and NREL are actively developing the OOI.
- Feedback was received from 10 manufacturers, a few utilities, and three national labs
- Publishing version 1 of OOI by end of year
- In calendar year 2023, will have one more round of formal feedback sonication
- To receive news and information, please visit UL news.



CONTENTS	
INTRODUCTION.....	3
1 Scope.....	3
2 Referenced Publications	3
3 Document Usage.....	4
4 Glossary	4
GENERAL REQUIREMENTS	7
5 Access Control, User Authentication and User Authorization	7
6 Cryptography.....	9
7 Sensitive Data Management	12
8 Security Management.....	15
9 Risk Management.....	17
10 Documentation	19
11 Monitoring.....	21
12 Logging.....	22
13 Product Management	23
14 Time synchronization.....	24
15 Physical anti tamper	25
ANNEX A (INFORMATIVE).....	26

* Draft, subject to change

- Draft v6
- Testable requirements categorized into 11 domains
- Addressed comments from industry, in final reviews for v1
- v1 publication end of December
- Feedback from manufacturers, installers/aggregators, utilities, and national labs
- Controls on public key infrastructure, access control, and remote management
- **UL will serve on the advisory board** and help drive select committees and working groups to advance key cybersecurity objectives.
- **UL's goal** is to structure cybersecurity and promote adoption of the cybersecurity certification standard.



- Ensures DER devices have all five pillars of cybersecurity: confidentiality, integrity, availability, authentication, and non-repudiation
- Supports federal and state mandates
- Establishes security by design in new DER systems
- Creates an environment where the baseline security posture of the DER industry will be elevated



Better coordination between government agencies and industry stakeholders to enhance DER Security.



Acceleration of public awareness, education, and training for stakeholders about risks associated with DERs.



Identification of risks and addition of incentives-based programs to incorporate DER security.



Development of a cybersecurity certification to ensure “security by design” for new DER systems.



Provides a baseline for device-level security and informs the development of a cybersecurity certification standard for DER stakeholders

Provides cybersecurity guidelines for one or more distributed energy resources that are interconnected with electric power system

Provides cybersecurity certification requirements that IBR equipment shall support in a way that the choice of implemented technology is at the manufacturer's decision.

Provides engagement activities to bring together individuals across industry, academia, and government to exchange ideas and learn.



Cybersecurity Certification Recommendations for Interconnected Grid Edge Devices and Inverter Based Resources

William Hupp, Danish Saleem, and Jordan T. Peterson
National Renewable Energy Laboratory

Kenneth Boyce
Eindhoven Laboratories

NREL is a national laboratory of the U.S. Department of Energy Office of Energy Efficiency & Renewable Energy Operated by the National Renewable Energy Laboratory (NREL) at www.nrel.gov/publications. This report is available at no cost from the National Renewable Energy Laboratory (NREL) at www.nrel.gov/publications. Contact: nrel-cc@nrel.gov

1 Draft Guide for Cybersecurity of Distributed Energy Resources Interconnected with Electric Power Systems

1. Overview

1.1 Scope

1 This document provides guidelines for cybersecurity of Distributed Energy Resources (DER) interconnected with Electric Power Systems (EPS).

1.2 Purpose

19 This document provides guidelines for cybersecurity for one or more distributed energy resources (DER) that are interconnected with electric power systems. DER includes systems at the sites of fuel cells, photovoltaics, small hydro, microturbines, other distributed energy resources, and distributed energy storage systems interconnected to EPS in a typical manner in secondary distribution voltage levels.

1.3 Need for cybersecurity guidelines for DER

15 These cybersecurity guidelines are for utilities, DER owner/operators, aggregators, vendors supporting DER, interconnectors, and other stakeholders involved in the DER domain.

17 This document addresses the broad requirements of cybersecurity going beyond the "DER standard" created by the IEEE C62.41-2016 interoperability requirements, because security is not for "just-in-it". For the security, the security issues covered in this document cannot be made secondary but need to be addressed and implemented. These recommendations may set initial or minimum requirements. It is ultimately the responsibility of users of the document to cover the applicability of the recommendations for their specific systems. Although not explicitly within the scope of this document, transmission-connected systems, storage, electric vehicle charging stations, and off-grid systems could still benefit from the recommendations described here.

24 This Guide is designed to be used by individuals with different levels of expertise and experience with DER and cybersecurity. It does it in a designed to be useful and provide general background information on DER communications and cybersecurity. It also defines the (necessary) technical recommendations for DER systems. Class 1 lists cybersecurity using recommendations for equipment and systems. The sections provide additional information on standards and best practices.

30 Specifically, this document covers cybersecurity issues and recommendations, including:

UL and NREL Announce Cybersecurity Testing Recommendations for Distributed Energy Resources and Inverter Based Resources

UL and the National Renewable Energy Laboratory will conduct an Online Investigation as a precursor to the cybersecurity certification standard for distributed energy resources.

WHAT IS NEW?

NORTHWOOD, Illinois—March 8, 2022—UL, a global safety science leader, has released a report, coordinated with the U.S. Department of Energy (DOE) and the National Renewable Energy Laboratory (NREL), titled "Cybersecurity Testing Recommendations for Distributed Energy Resources and Inverter Based Resources." The report includes recommendations for testing distributed energy resources (DER) and inverter based resources (IBR) to the "state-of-the-art" cybersecurity practices.

With support from DOE's Grid Energy Technology Office (GTO), UL will continue working with NREL on developing requirements to support cybersecurity certification standards for DER and IBR, and UL is currently working on a suite of investigation for reports that will assist in energy storage and generation technologies in the distributed and individual generation systems, electric vehicle charging, and various fuel cells and other non-renewable or emerging generation systems. These new requirements will provide cybersecurity requirements for better systems leading to high performance, enhanced safety, and reducing their carbon footprint. This report serves as a guide for manufacturers, high-end users and technology providers. It is also the first cybersecurity report being released by UL and NREL.

"Specifically, this report is cybersecurity certification requirements to which manufacturers and vendors can certify their DER and IBR devices against an established and widely-accepted cybersecurity program." The development of these cybersecurity certification requirements will provide a large initial step that can be taken as a reference for performing the testing and evaluation of DERs that are being developed and sold in the field, and to ensure they meet the requirements for electrical engineering, industrial practices, and cybersecurity certification requirements with power quality requirements related to distribution and protection. This is expected to be working with NREL in the future to bring additional performance based testing to support grid applications."

SunSpec/Sandia DER Cybersecurity Workgroup

DER Cybersecurity Certification Procedure Complete

- Defined standard procedure for DER vulnerability assessments.
- Leads: Danish Saleem (NREL) and Cedric Carter (METE)
- Publication: "Certification Procedures for Data and Communications Security of Distributed Energy Resources"
- Future work: Expected development within UL 2500-2-537

Secure Network Architecture Complete

- Created DER reference architecture best practice.
- Lead: Candice Sullivan (BPA)
- Publication: "EPRI Security Architecture for the Distributed Energy Resources Integration Network: Risk-based Approach for Network Design"
- Future work: Risk-based approach adopted in IEEE 1547.3

Data-in-Flight Requirements Complete

- Encryption, authentication, and key management requirements.
- Lead: Arnon Oranboon (Sandia)
- Publication: "Recommendations for Trust and Encryption in DER Interoperability Standards", another covering Data-in-Flight Requirements document (forthcoming).
- Future work: IEEE 1547.3 update, IEEE 2030.5 revisions.

Access Control Wrapping Up

- DER Role-Based Access Control recommendations.
- Lead: Jay Johnson (Sandia)
- Topics: Access control taxonomy and security models
- Planned Publication: "Recommendations for Distributed Energy Resource Access Control"
- Future work: Add recommendations to IEEE 1547.3 Guide

Patching Requirements Starting!

- Establishing patching guidelines for DER devices and DER networking equipment.
- Starting August-Sept 2020. Lead: TBD
- Topics: Patching update rates, maintenance guidelines, etc.

Utility/Aggregator Auditing Procedure O2 FY21

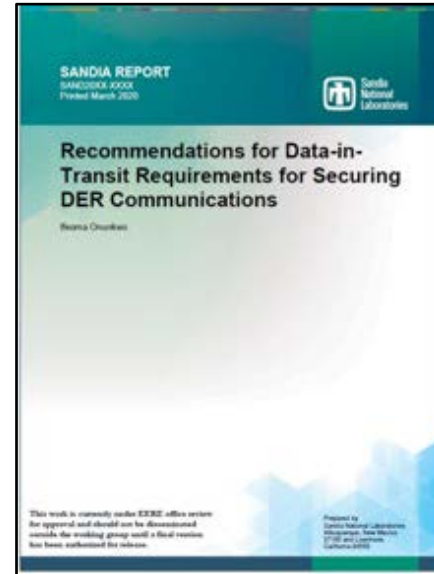
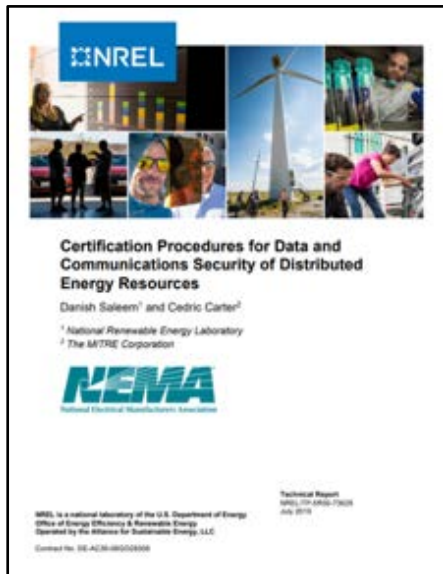
- Creating recommended auditing practices for DER networks.
- Planned for March-April 2021. Lead: TBD
- Topics: Key-by-step auditing procedures for internal or external compliance review. Recommended data for attack forensics.

Provides test cases that can be used to check, verify and validate cybersecurity posture of DERs

Provides practical cybersecurity requirements pertaining to the network components supporting DERs.

Examines the cybersecurity requirements for DER comms protocols, per IEEE 1547-2018 revision

Provides near and long-term recommendations to improve trust and encryption mechanisms for DER comms





- Publish the Outline of Investigation.
- Develop appropriate third-party conformity assessment programs for DER cybersecurity testing and certification.
- Develop white papers, a press release, industry webinars, and related activities to increase awareness.
- Organize and host a DER cybersecurity summit for thought leaders and key stakeholders from national laboratories, utilities, and the energy and renewables industries to establish practical and actionable plans to move forward.



Questions and Answers

Thank you

NREL/PR-5R00-84709

This work was authored by the National Renewable Energy Laboratory, operated by Alliance for Sustainable Energy, LLC, for the U.S. Department of Energy (DOE) under Contract No. DE-AC36-08GO28308. Funding provided by U.S. Department of Energy Office of Solar Energy Technology Office (SETO). The views expressed in the article do not necessarily represent the views of the DOE or the U.S. Government. The U.S. Government retains and the publisher, by accepting the article for publication, acknowledges that the U.S. Government retains a nonexclusive, paid-up, irrevocable, worldwide license to publish or reproduce the published form of this work, or allow others to do so, for U.S. Government purposes.

