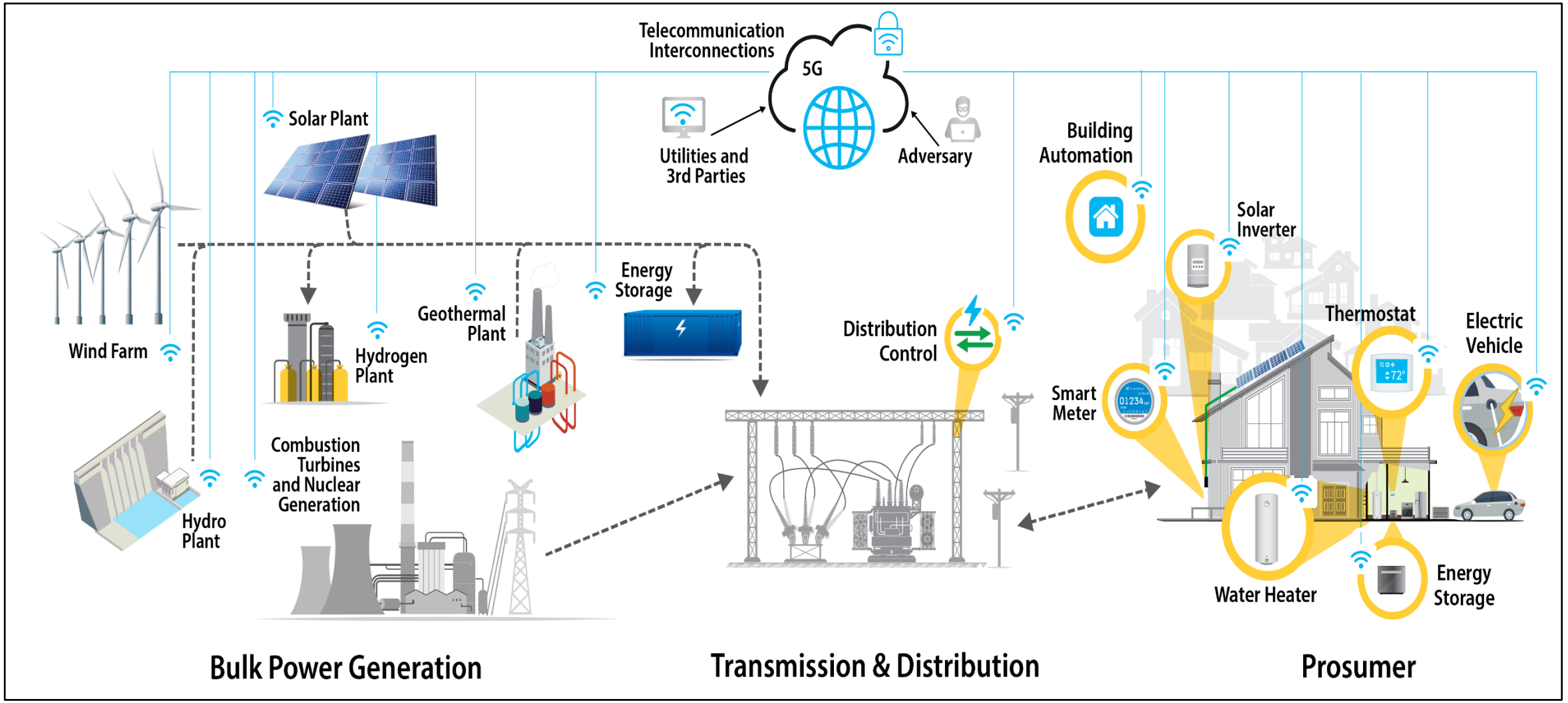
Cybersecurity Standards, Certification, and Best Practices for DERs

DOE Securing Solar for the Grid (S2G) Program

Zoe Dormuth | National Renewable Energy Laboratory

This presentation was produced when the laboratory operated as the National Renewable Energy Laboratory (NREL). The laboratory is now the National Laboratory of the Rockies (NLR).

Understanding DER Systems



Graphic by NREL

Solar Energy Systems

Cybersecurity Future Benefits

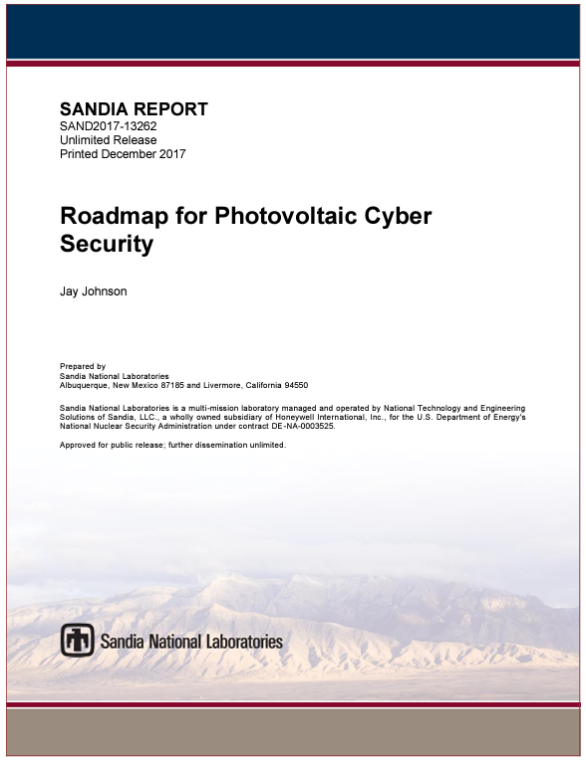
- Reduce reliance on centralized energy generation
- Enhance energy security by diversifying energy sources
- R&D lead to improvements in efficiency, capabilities, integration with other DERs and cybersecurity
- Assess and update cybersecurity standards and establish certification programs
- Develop, refine, improve, and harmonize cybersecurity requirements for DER ecosystem to develop a cohesive security approach across DER environments through standards

Solar Energy Systems

Cybersecurity Risks

- Solar energy systems are increasingly interconnected and remotely accessible
- Data privacy for energy production, consumption patterns, and system health data
- Reliance on components sourced globally
- Integration with the grid opens the attack surface and can disrupt broader energy distribution networks
- Lack of a universal cybersecurity standards for solar energy systems

Relevant Work for Solar Cybersecurity



SANDIA REPORT
SAND2017-13262
Unlimited Release
Printed December 2017

Roadmap for Photovoltaic Cyber Security

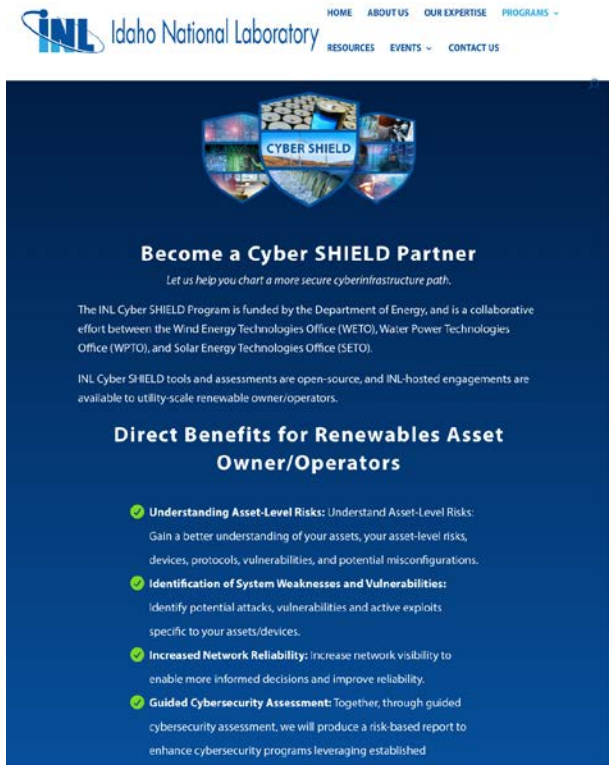
Jay Johnson

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia National Laboratories is a multi-mission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC., a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA-0003525.

Approved for public release; further dissemination unlimited.

Sandia National Laboratories



INL Idaho National Laboratory

HOME ABOUT US OUR EXPERTISE PROGRAMS RESOURCES EVENTS CONTACT US

CYBER SHIELD

Become a Cyber SHIELD Partner

Let us help you chart a more secure cyberinfrastructure path.

The INL Cyber SHIELD Program is funded by the Department of Energy, and is a collaborative effort between the Wind Energy Technologies Office (WETO), Water Power Technologies Office (WPTO), and Solar Energy Technologies Office (SETO).

INL Cyber SHIELD tools and assessments are open-source, and INL-hosted engagements are available to utility-scale renewable owner/operators.

Direct Benefits for Renewables Asset Owner/Operators

- **Understanding Asset-Level Risks:** Understand Asset-Level Risks: Gain a better understanding of your assets, your asset-level risks, devices, protocols, vulnerabilities, and potential misconfigurations.
- **Identification of System Weaknesses and Vulnerabilities:** Identify potential attacks, vulnerabilities and active exploits specific to your assets/devices.
- **Increased Network Reliability:** Increase network visibility to enable more informed decisions and improve reliability.
- **Guided Cybersecurity Assessment:** Together, through guided cybersecurity assessment, we will produce a risk-based report to enhance cybersecurity programs leveraging established

NREL

Cybersecurity in Photovoltaic Plant Operations

Andy Walker,[1] Jal Desai,[1] Danish Saleem,[1] and Thushara Gunda[2]

[1] *National Renewable Energy Laboratory*
[2] *Sandia National Laboratories*

NREL is a national laboratory of the U.S. Department of Energy
Office of Energy Efficiency & Renewable Energy
Operated by the Alliance for Sustainable Energy, LLC

This report is available at no cost from the National Renewable Energy Laboratory (NREL) at www.nrel.gov/publications.

Contract No. DE-AC36-08GO28308

Technical Report
NREL/TP-5D00-78755
March 2021

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

RELIABILITY | RESILIENCE | SECURITY

UL's DER Cybersecurity Certification Program

Outline of Investigation for Cybersecurity of Distributed Energy and Inverter-Based Resources

Cybersecurity Certification Standard – UL 2941

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

PRESS RELEASE

UL Solutions and NREL Announce Distributed Energy and Inverter-Based Resources Cybersecurity Certification Requirements

UL 2941, the Outline of Investigation for Cybersecurity of Distributed Energy and Inverter-Based Resources, provides testable requirements for photovoltaic inverters, electric vehicle chargers, wind turbines, fuel cells and other resources essential to advancing grid operations.

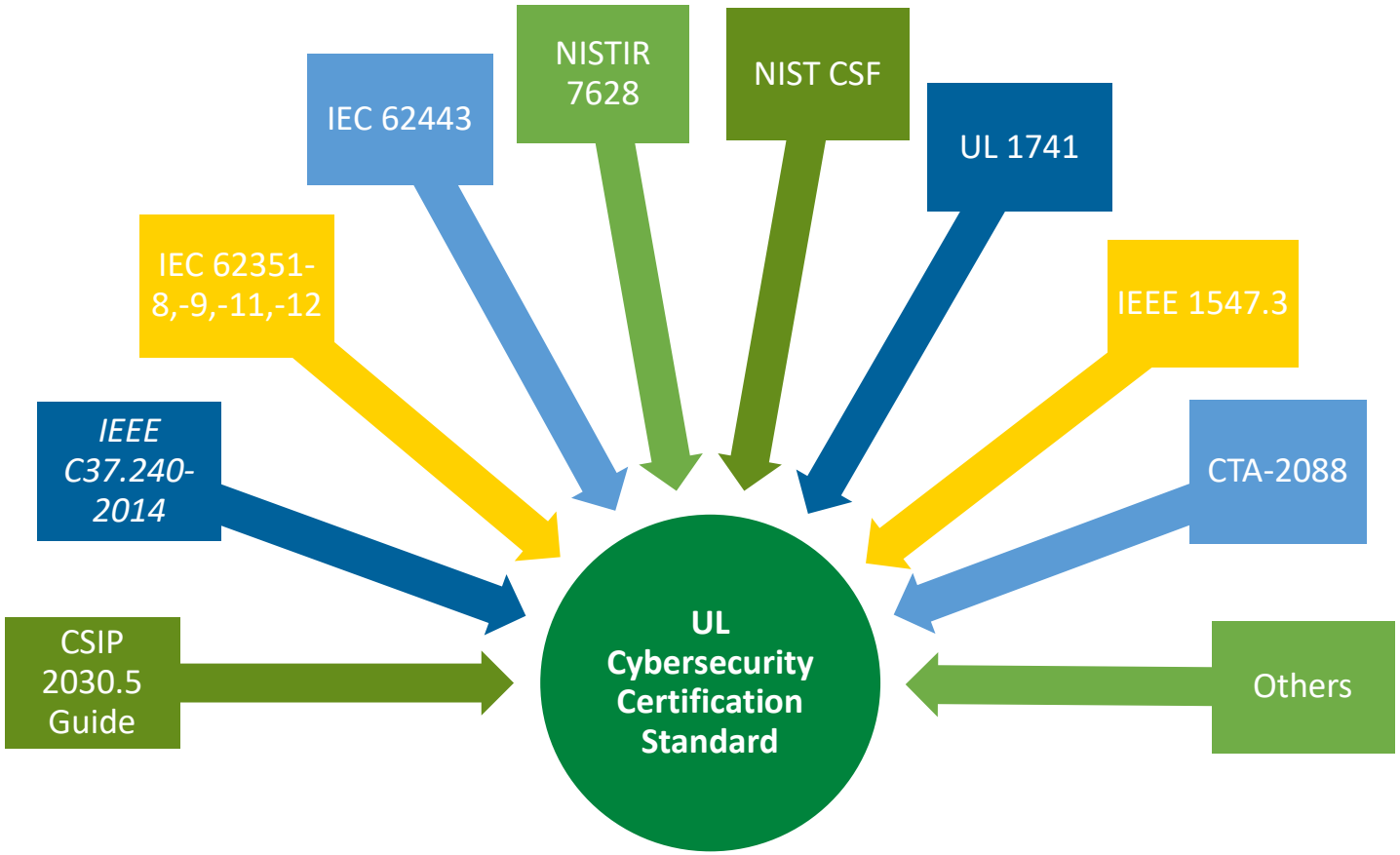
- The requirements provide a single unified approach for testing and certification of DERs
- The certification is applicable to generation and energy storage technologies.
- UL is currently soliciting formal feedback through UL 2941 Technical Committee.
- Planned publication of first version is end of 2024

https://www.nrel.gov/security-resilience/cybersecurity-standards.html

Many Standards and Guides Exist Why a New One?

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”



Benefits of a 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

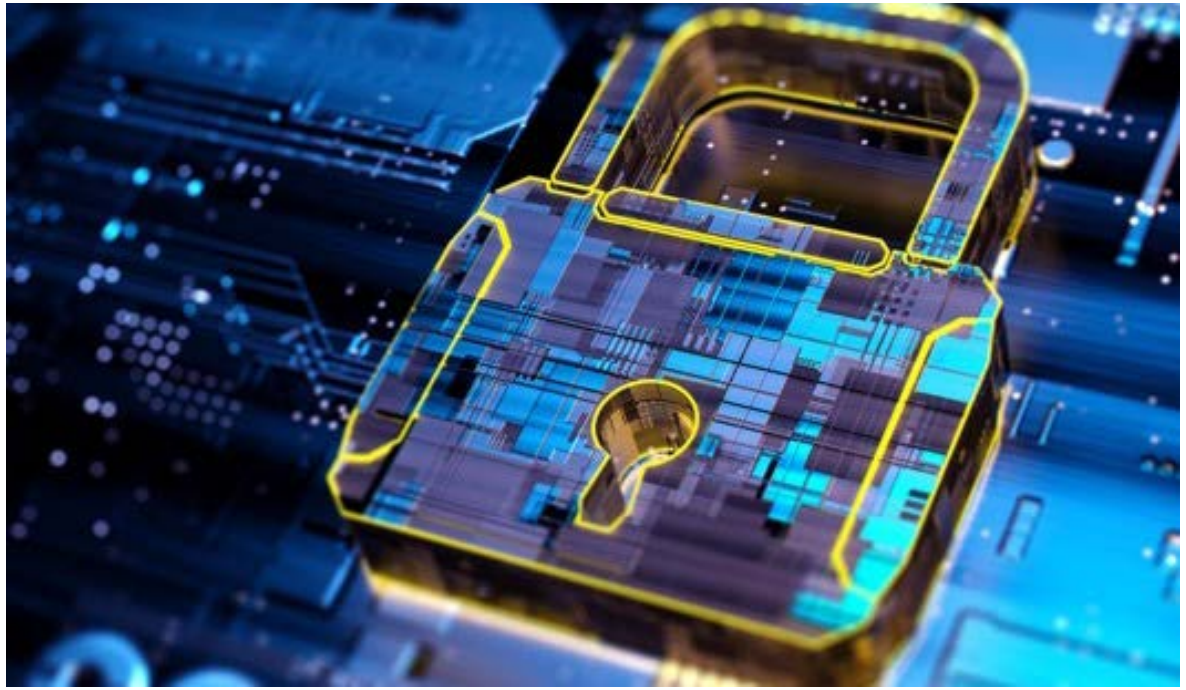
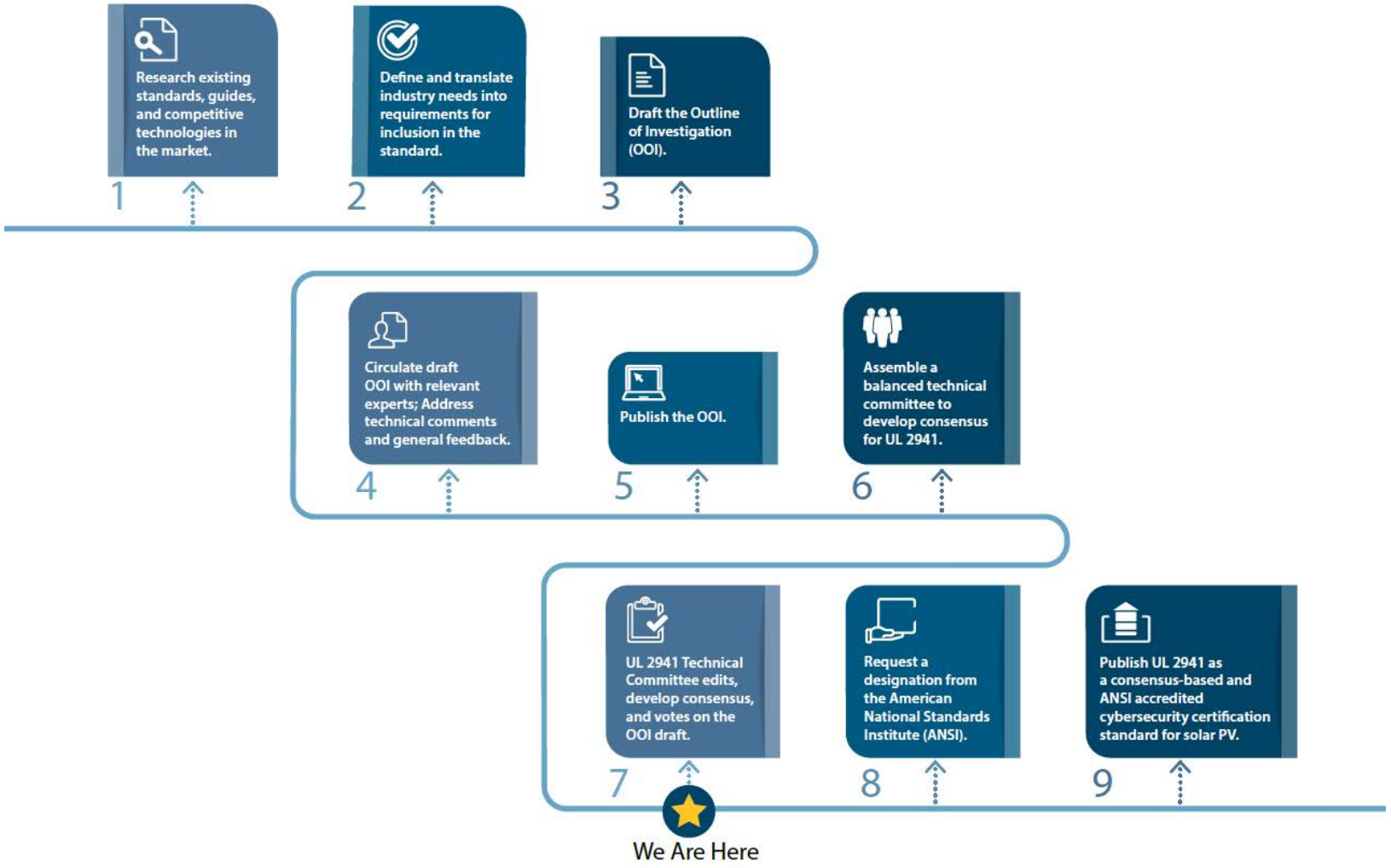


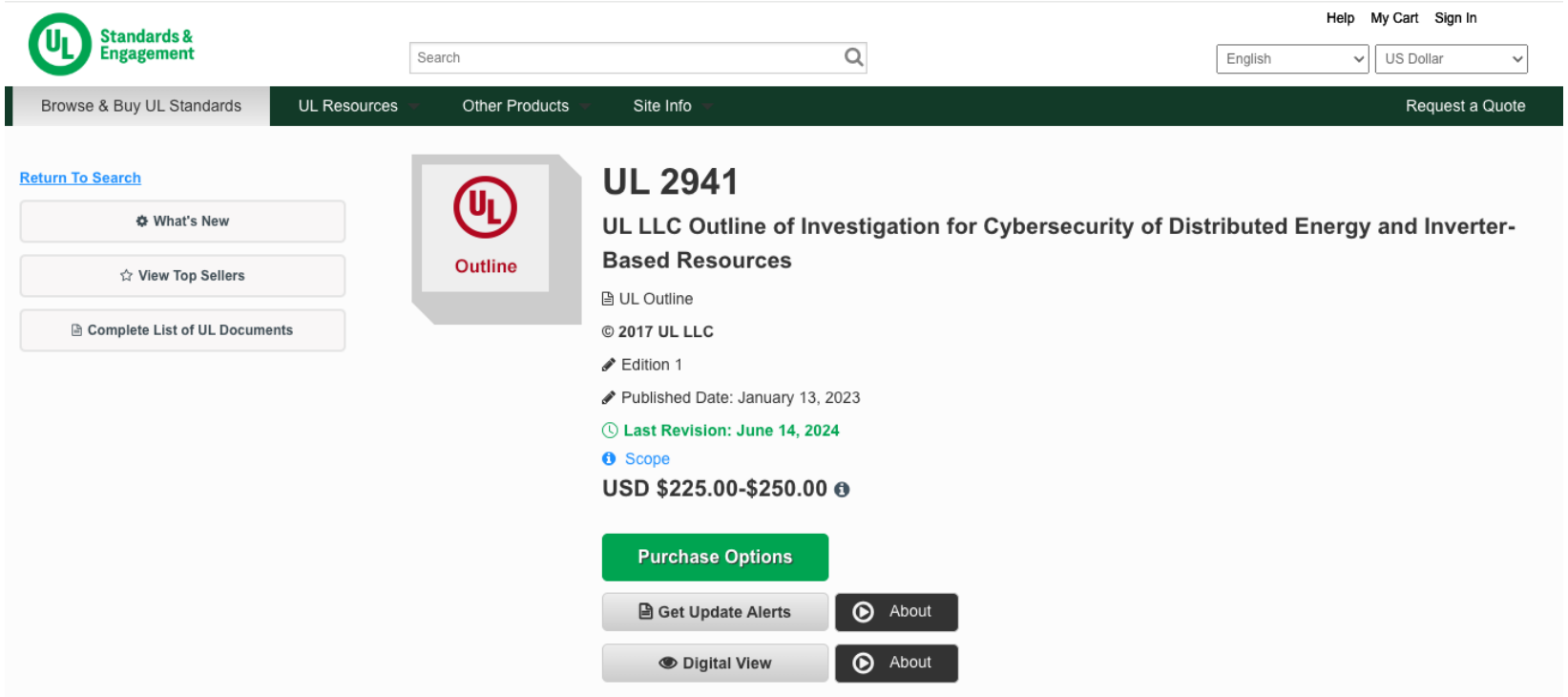
Photo from iStock, 1185245180

UL 2941 Development Timeline



UL 2941 Publication

- The standard is now published.
- Joint effort by UL and NREL (as directed by SETO/DOE).
- We are engaging industry for soliciting formal feedback. Please reach out if you are interested!



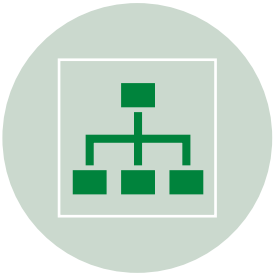
IEEE 1547 Updates

Standard for Interconnecting Distributed Resources with Electric Power Systems

IEEE 1547-2018

The DER Interconnection & Interoperability Standard

Requirements for DERs to support grid stability and resilience, such as voltage and frequency regulation capabilities.



Guidelines for communication between DERs and utility control systems to enable coordinated operation and grid management.

Enhanced testing and certification requirements to ensure compliance with technical specifications and operational standards.

Considerations for cybersecurity to protect against cyber threats targeting interconnected DER systems.

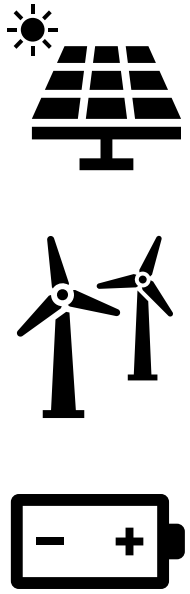
Does not define requirements for cybersecurity

Standards for cybersecurity for “smart energy” systems including DER but not explicitly DER

IEEE 1547.3

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

Fuel cells
Photovoltaics
Wind turbines
Microturbines
Distributed energy sources
Distributed energy storage systems



- Utilities
- DER Owner/Operators
- Aggregators
- Manufacturers
- Integrators

IEEE 1547.3

Motivation

Communication capabilities increase the vulnerability of the power system to cybersecurity events

Discusses key cybersecurity issues and best practices related to DER interconnections with the power system

Provides specific guidance on cybersecurity capabilities of the protocols specified in IEEE 1547-2018

IEEE Std 1815 (DNP3)

IEEE 2030.5

SunSpec Modbus

IEC 61850

IEEE 1547.3

Technical Cybersecurity Recommendations for DER operations

- Risk assessment and management
- Communication network engineering
- Access control
- Data security
- Security Management
- Coping with and recovering from security events

Standards versus Certifications

Sets guidelines, requirements, or specifications by a recognized authority

Provides a framework for best practices

A process through which a third-party organization verifies that a product, service, or system meets specific standards

Provides assurance to consumers, manufacturers, and regulators

Thank you

NLR/PR-5T00-90559

This work was authored by NREL for the U.S. Department of Energy (DOE), operated under Contract No. DE-AC36-08GO28308. Funding provided by the U.S. Department of Energy Office of Energy Efficiency and Renewable Energy Solar Energy Technologies Office. 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.