Cybersecurity Certification Standard for Distributed Energy & Inverter-Based Resources

Danish Saleem, National Renewable Energy Laboratory
Michael Slowinske, UL

NASEO/NARUC Cybersecurity Advisory Team for State Solar (CATSS)
01/24/2022

Presenters

Michael Slowinske

Director of Principal Engineering

UL

- UL is a global safety science company that has certified tens of billions of products.
- UL has expertise in cybersecurity and safety, global standards and frameworks, IoT security solutions, and hardware and software-based security evaluations.
- As an independent, trusted third party, UL will lead the program to develop the cybersecurity certification standard.

Danish Saleem

Senior Energy Systems Cybersecurity Researcher

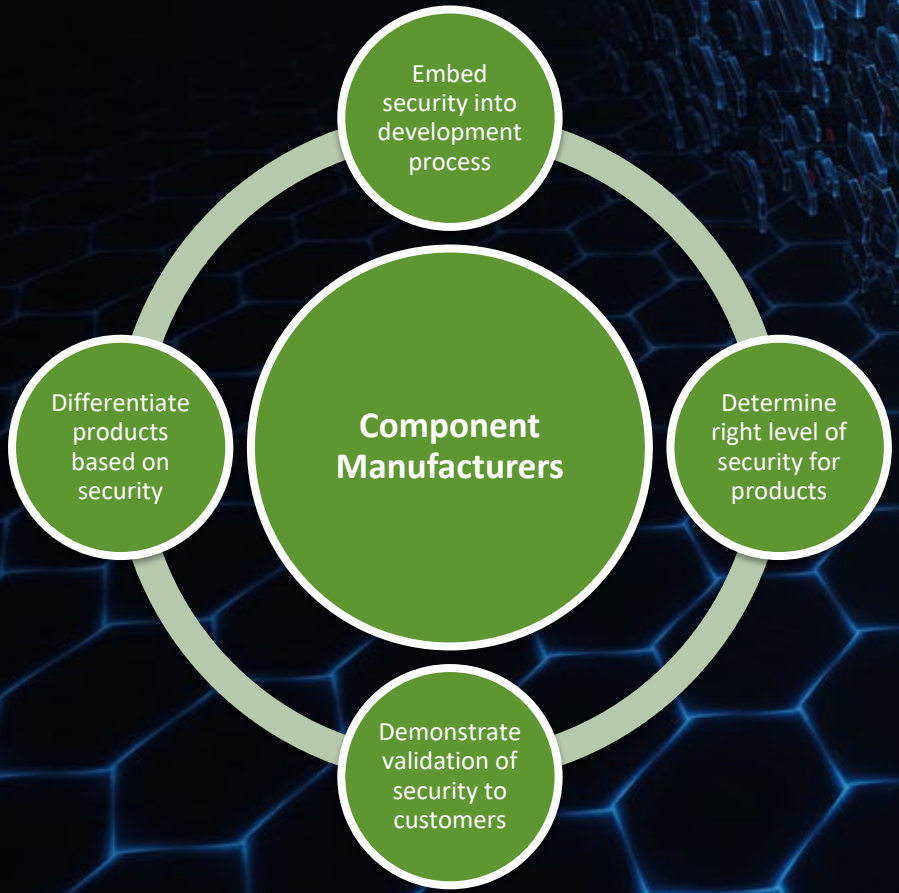
National Renewable Energy Laboratory

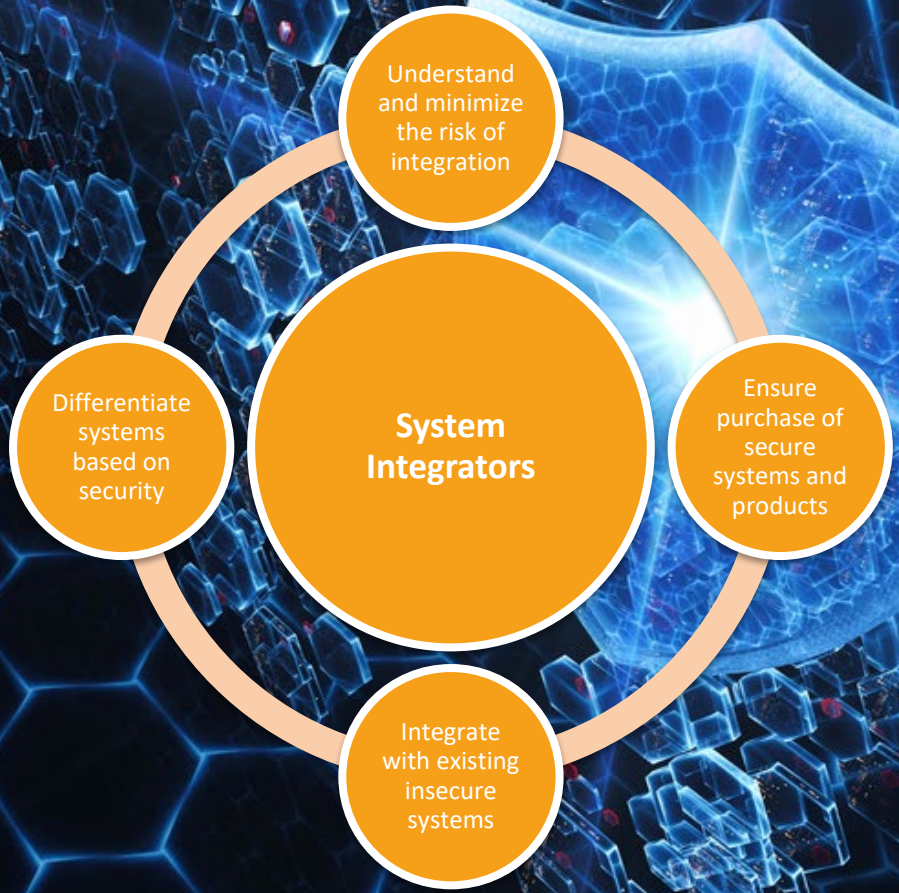
- NREL is a national laboratory of the U.S. Department of Energy, Office of Energy Efficiency and Renewable Energy.
- NREL has about 900 partnerships works with industry, academia and government.
- Researchers at NREL work with utilities, vendors, certification labs, and standard development organizations to research, identify, and establish interoperability and cybersecurity requirements for distributed energy resources.
- NREL is supporting this effort with expertise on integrated energy systems and laboratory evaluation and testing platforms.

Agenda

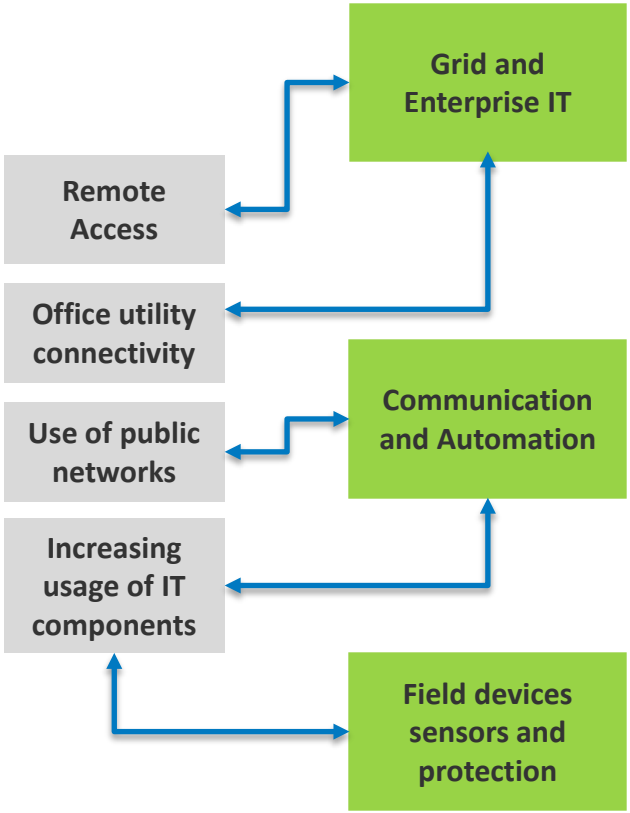
- The new security challenge
- Benefits of a cybersecurity certification standard
- Previous initiatives
- Role of electric utilities and state energy offices
- The UL expertise
- 2023 National Electrical Code (NEC) proposals on cybersecurity
- Process from Outline of Investigation to Certification Standard

Industry Cybersecurity Challenges





The New Security Challenge



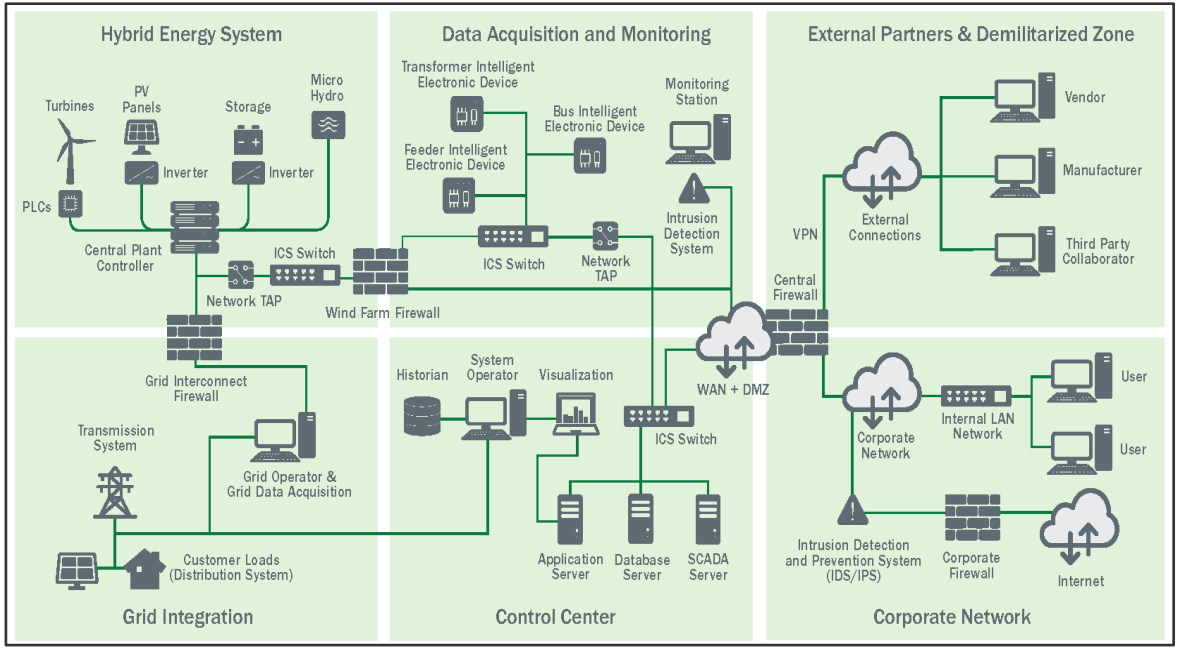
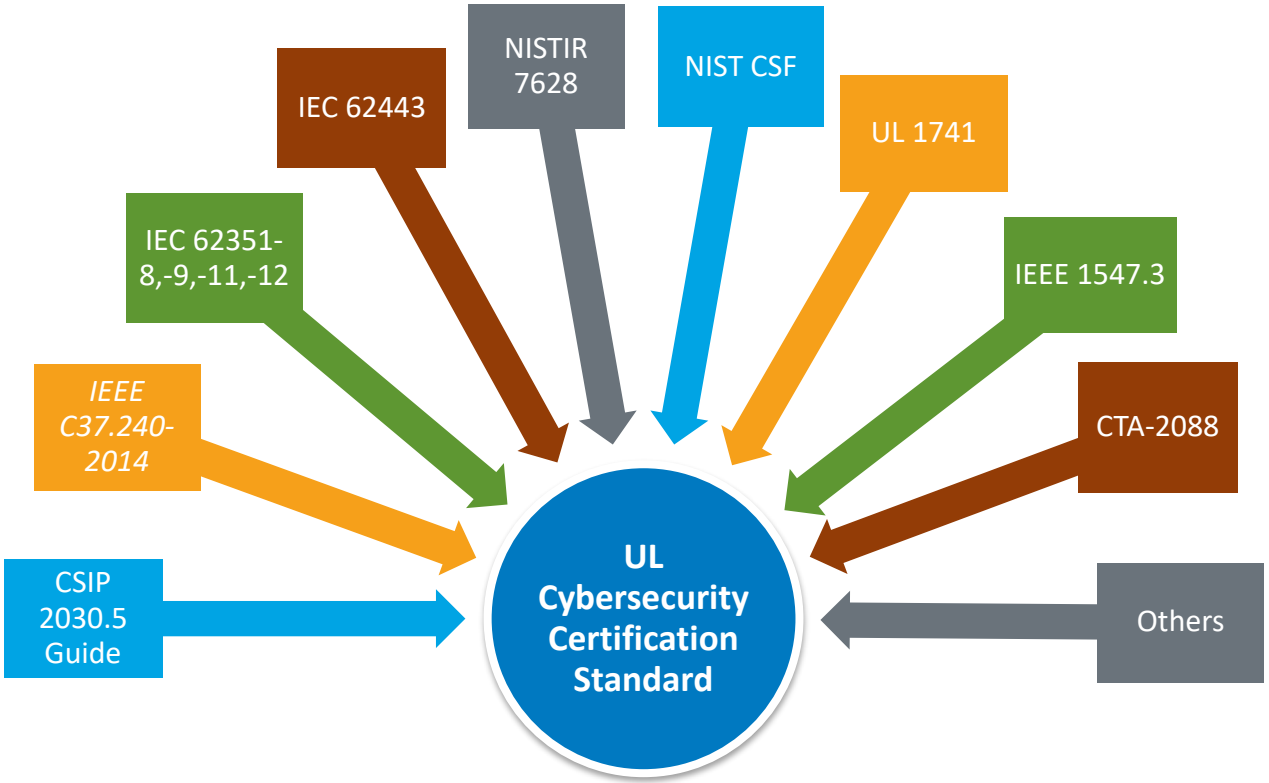


Illustration by Alfred Hicks, NREL

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"



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

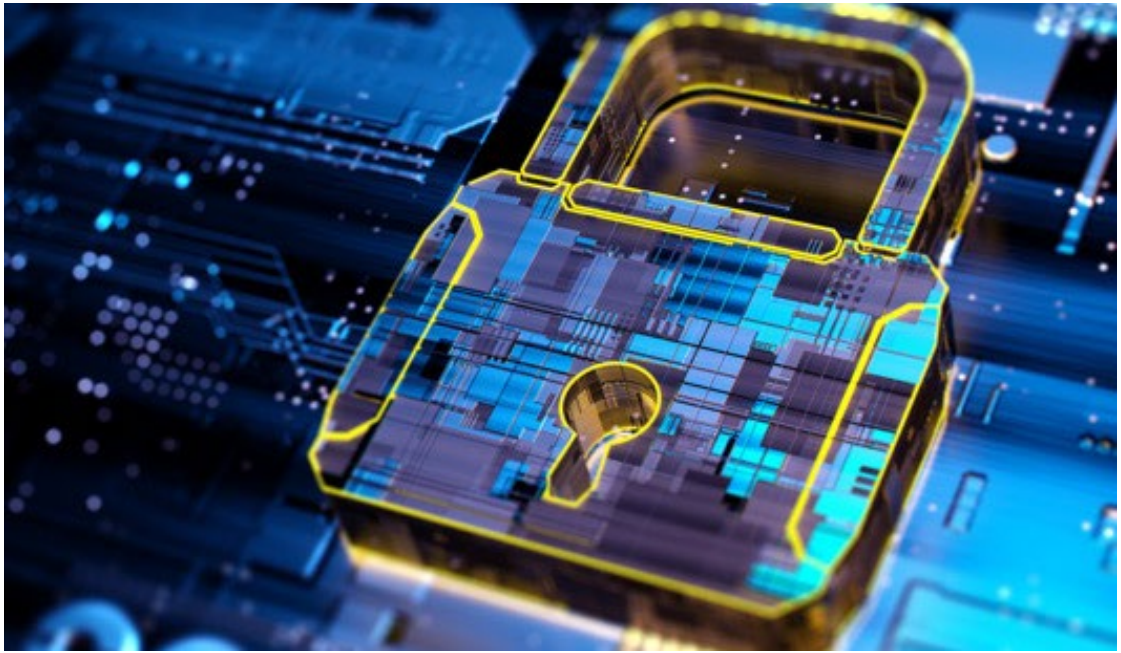


Photo from iStock, 1185245180

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

Cybersecurity Certification – Why Now?

- Why should we care about developing DER/IBR 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

Photo by Dennis Schroeder, NREL 22168

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

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

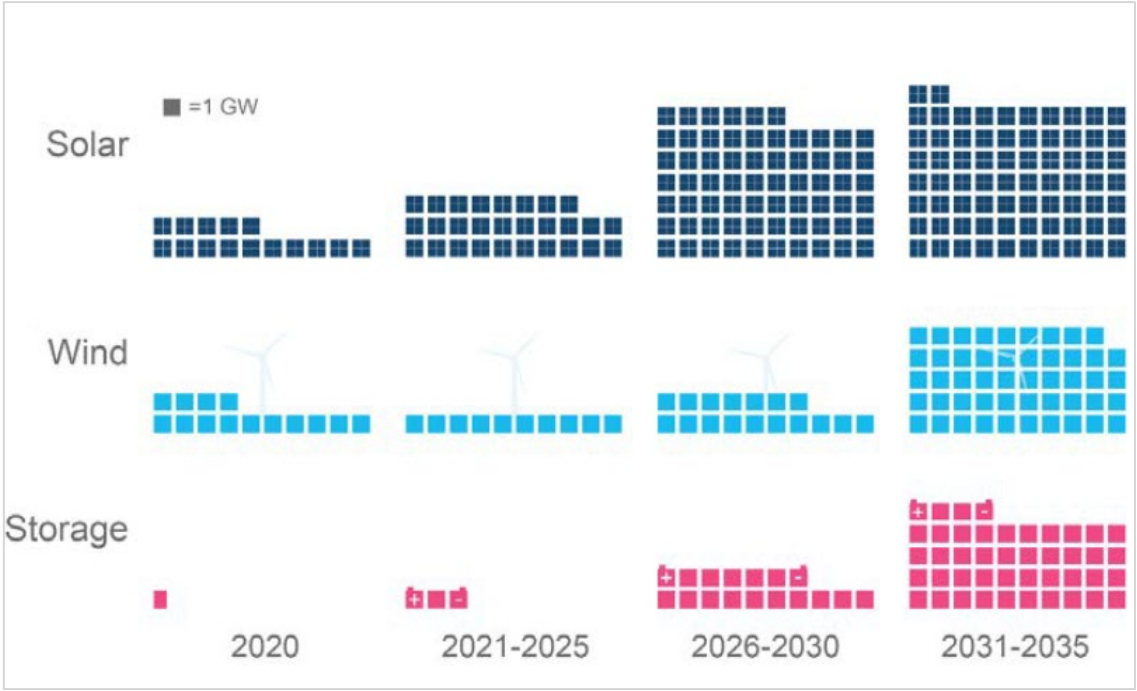
Variable-energy resources ….continue to be a significant component of new capacity

NREC Planning Committee Meeting, June 6, 2017. url

Solar Futures Study

This EERE study explored pathways for solar energy to drive decarbonization of the U.S. electric grid by 2035, weighing factors such as:

- integrating solar onto the electric grid
- synergies between solar and storage
- necessary technological advancements, and
- supply chain and environmental considerations



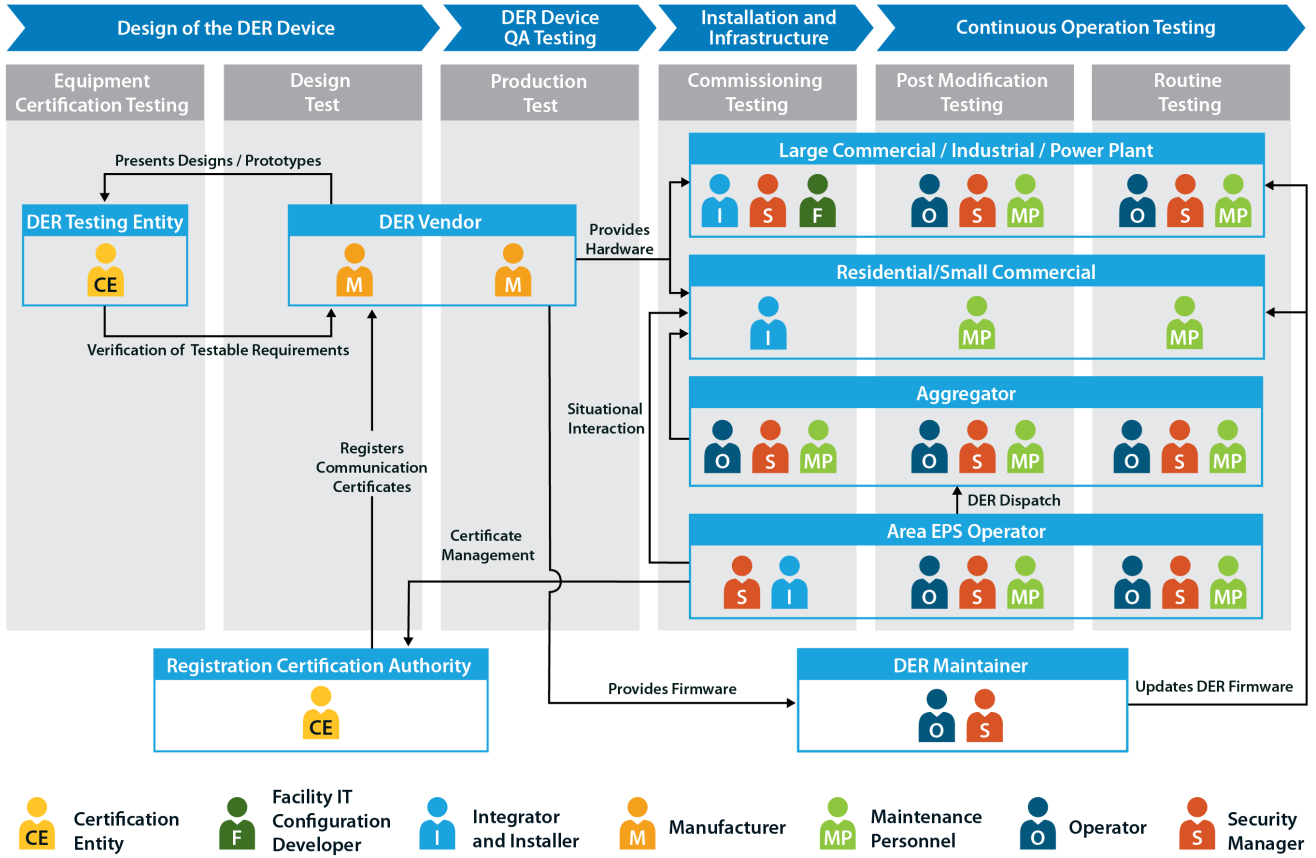
Graphic by Eric O'Shaughnessy, NREL

Solar currently provides 3% (80 GWac) of total U.S. electricity demand. It is estimated to grow to 40% (1,000 GWac) by 2035 and 45% by 2050 (1,600GWac).

Full report: Solar Futures Study report.
DOE Website: https://www.energy.gov/eere/solar/solar-futures-study

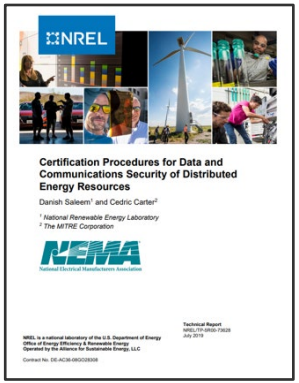
Recommended Cybersecurity Testing and Commissioning

Per IEEE 1547.3, “Testing should be viewed as a risk mitigation activity and should be integrated with the overall cybersecurity risk management framework.”



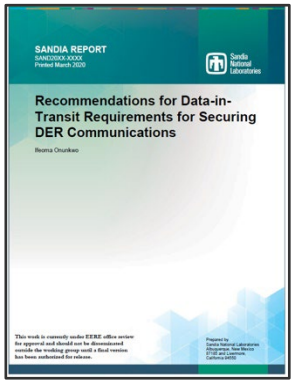
Outcomes of Cybersecurity Standards Initiatives

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

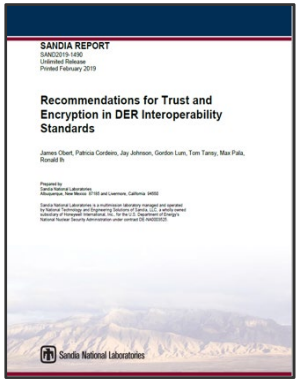


Provides practical cybersecurity requirements pertaining to the network components supporting DERs

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



Provides cybersecurity guidelines for DERs that interconnect with electric power system

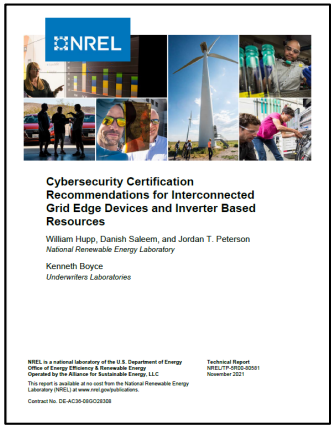
Outcomes of Cybersecurity Standards Initiatives (contd.)

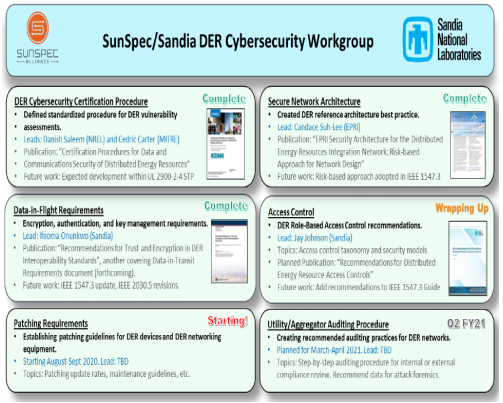
Provides a baseline for device-level security and informs the development of a cybersecurity certification standard for DER stakeholders

Provides certification testing through SunSpec-authorized test labs for product compliancy to CA rule 21 and CSIP standard

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

Provides three-year-long program to prepare industry professionals and military veteran job seekers for the next wave of DER technology

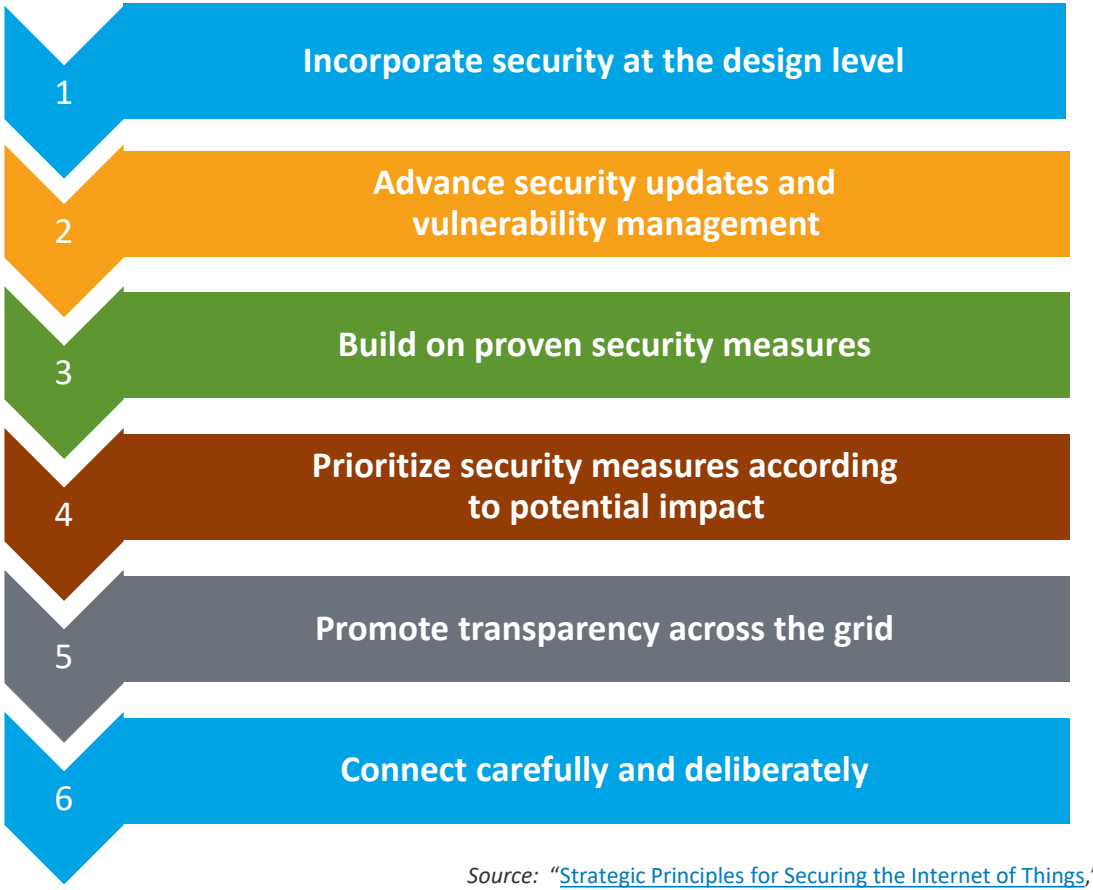




Think Before You Connect

Implement **security by design** and practice basic **cyber hygiene.**

- Change default passwords.
- Use two-factor authentication.
- Install updates, i.e., authentication, TLS1.2 or higher, etc.
- Consider security of underlying infrastructure during patch management or remote connection.
- Monitor both consumer devices and vendor-managed devices.
- If possible, add code-signing and roll-back firmware.
- Use vendors with cyber hygiene.
- DO NOT connect printers or other similar devices to the operations network.



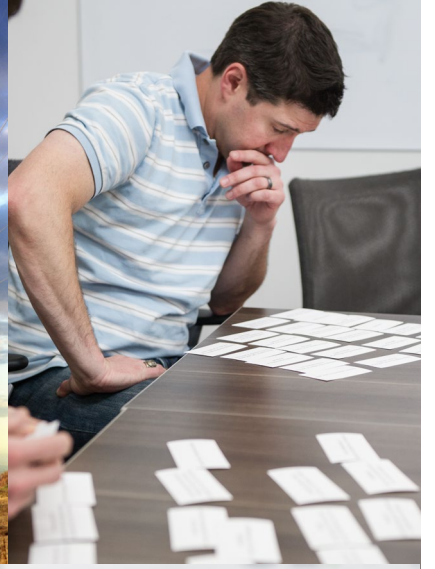
Source: "Strategic Principles for Securing the Internet of Things," U.S. Department of Homeland Security (2016)

Blind spots and challenges for electric utilities

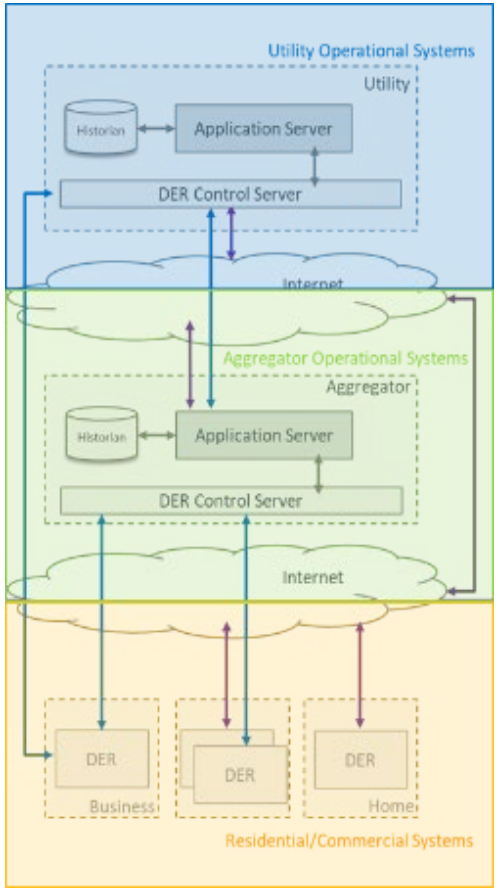
- Lack of visibility into operating assets
- Lack of investment in workforce development
- Lack of security alignment between OT and IT
- Pace of advancements in technology and threats.
- Accessibility of threat and risk information

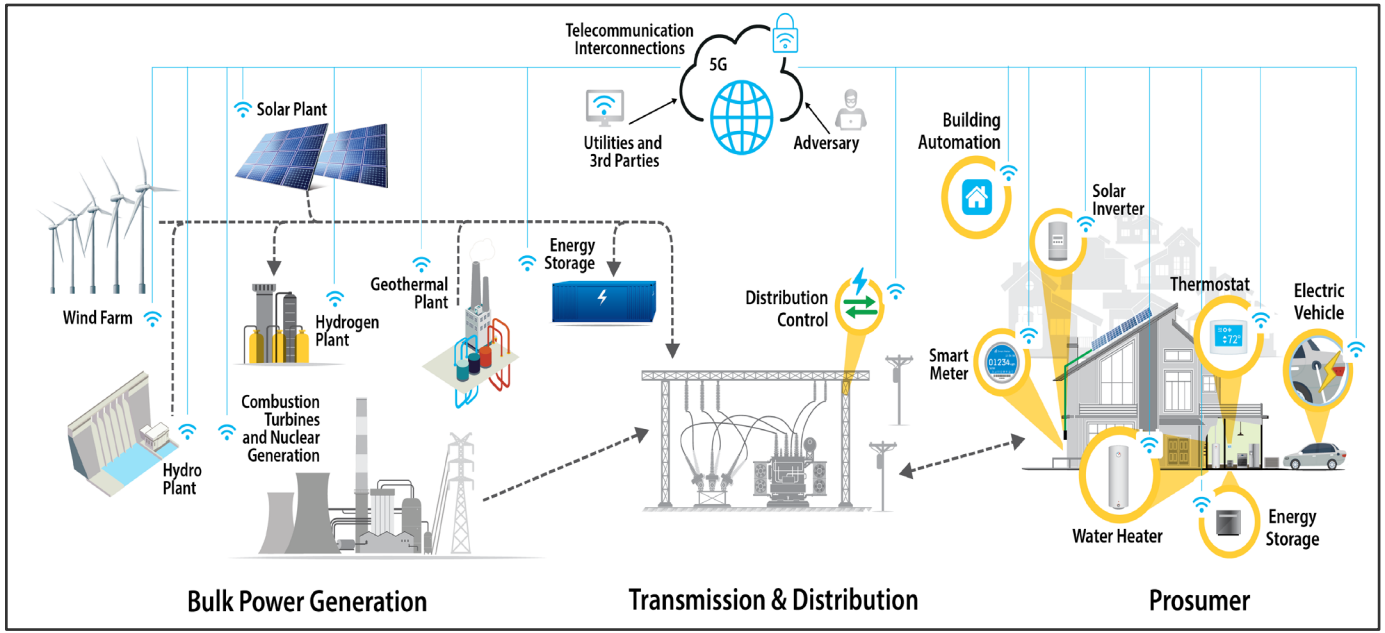
How can state energy offices support cybersecurity standard development efforts?

- Support risk mitigation and resiliency.
- Promote cyber best practices and policies with good governance, such as NIST CSF and/or NERC CIP
- Coordinate within state government.
- Engage across public and private stakeholders.
- Contribute and/or actively support the development of DER cybersecurity certification standards.
- Proactively develop cyberattack response and mitigation plans.



Understanding DER Systems

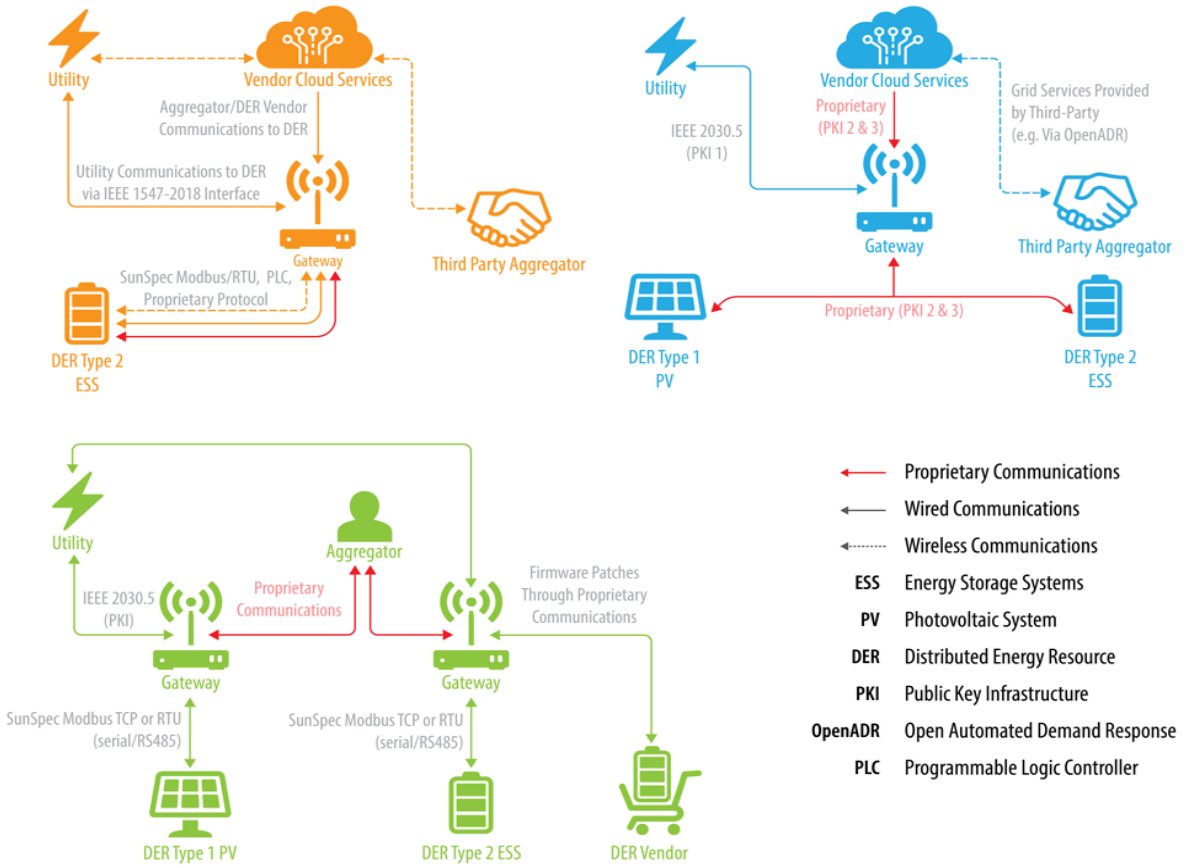




Graphic by Anthony Castellano, NREL

Projected Future DER Systems

The **Cybersecurity Information Sharing Act of 2015** authorizes and encourages private companies to take defensive measures to protect against and mitigate cyber threats.



Graphic by NREL

Source: Cybersecurity Information Sharing Act of 2015. 2015. S. 754, 114th Congress.

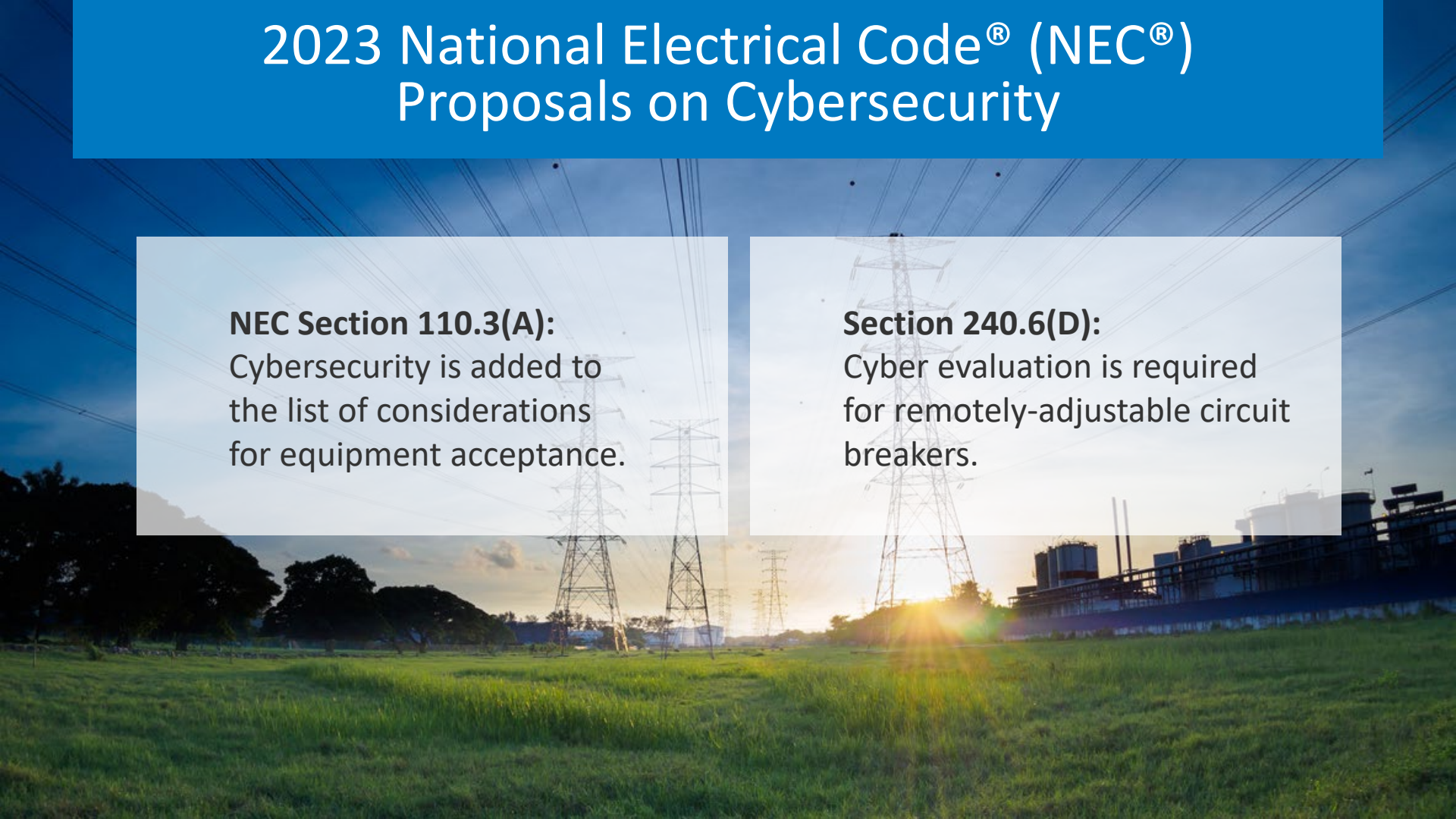
UL will lead development of the cybersecurity certification standard.

As an independent third party, UL will manage the steps to standard development.

The process will be guided by UL expertise in:

- Cybersecurity and safety
- Global standards and frameworks
- IoT security solutions
- Hardware and software-based security evaluations
- Regulated security markets
- Learning and development
- Data insights

2023 National Electrical Code® (NEC®) Proposals on Cybersecurity



NEC Section 110.3(A):
Cybersecurity is added to the list of considerations for equipment acceptance.

Section 240.6(D):
Cyber evaluation is required for remotely-adjustable circuit breakers.

Outline of Investigation (OOI)

- 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.
- **We will welcome participation from industry.**
- To receive news and information, please visit UL news.

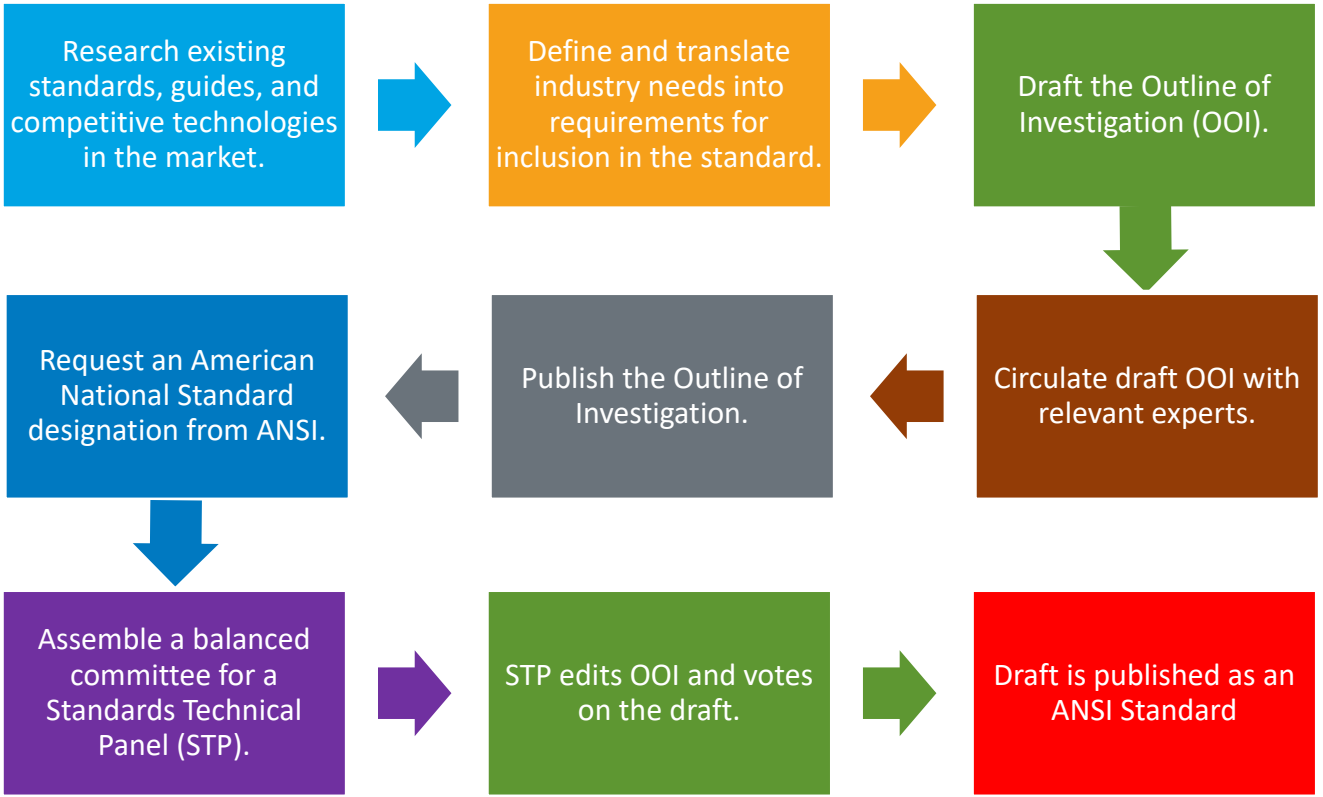
January X, 2022

UL x12345x

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

Issue No: 1

Process from OOI to Certification Standard



UL and ISA

UL is a founding member of the International Society of Automation (ISA) Global Cybersecurity Alliance (ISAGCA), formed in late 2020.

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.

https://www.ul.com/news/ul-joins-isa-global-cybersecurity-alliance-founding-member-advance-industrial-cybersecurity

What Needs To Be Done

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.

Roadmap of Next Steps

- Publish the Outline of Investigation.
- Develop white papers, a press release, industry webinars, and related activities to increase awareness.
- Develop appropriate third-party conformity assessment programs for DER cybersecurity testing and certification.
- 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?

Thank You!

Let’s Work together!

Danish.Saleem@nrel.gov

Michael.Slowinske@ul.com

NREL/PR-5R00-81827

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 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.

Additional Slides

Essential DER and Cybersecurity Terms

Distributed Energy Resources (DERs) - Controllable electric generation, storage, or load devices that are interconnected to the electric grid and typically are behind a customer's meter. DERs are intelligent energy devices, from smart lighting and thermostats, to electric vehicles and rooftop solar photovoltaics.

Inverter Based Resources (IBRs) – Resources that are asynchronously connected to the grid and are either completely or partially interfaced with the BPS through power electronics.

Internet of Things (IoT) devices vs DERs - DERs are subject to performance requirements of the Institute of Electrical and Electronics Engineers, the IEEE 1547-2018 standard, and each DER is certified for conformity to interconnect with the grid. Smaller devices, especially adjustable home or business loads and smart phone-enabled home automation devices, are IoT devices. Harmonizing IoT and DER performance requirements, including cyber, is a challenge.

DER Aggregator - An entity that groups together DER resources for the purposes of operating it as a group for grid services.

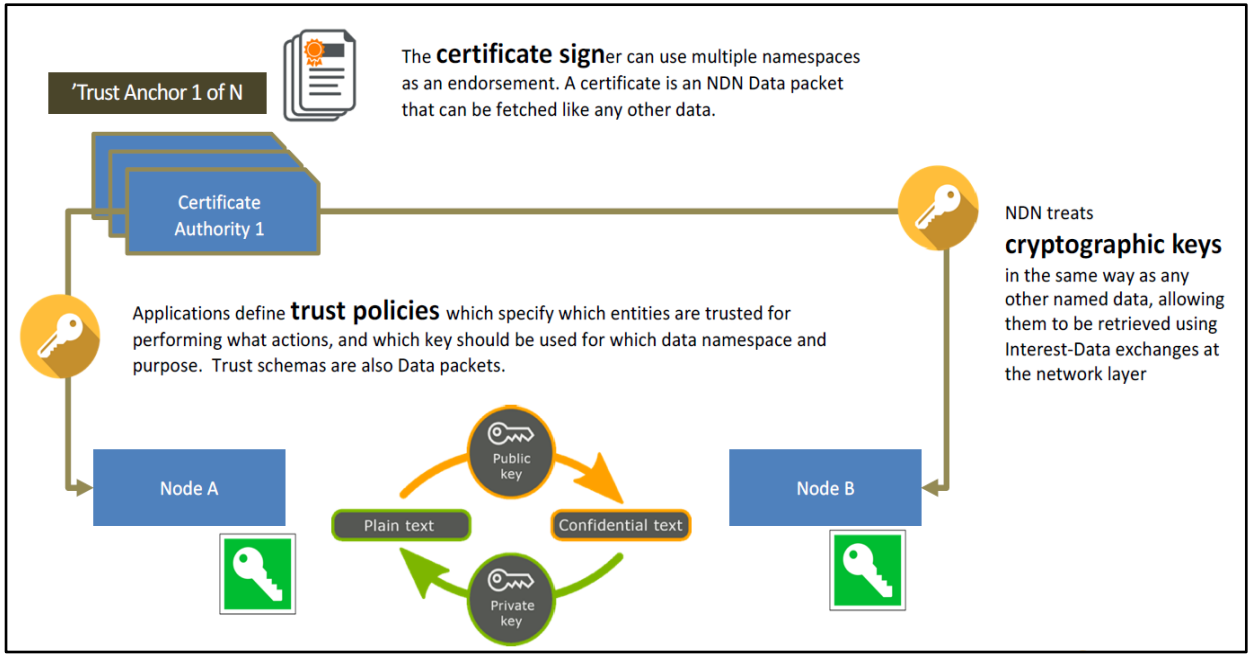
DER Owner/Operators – The entity (or entities) that is responsible for the regular care and maintenance of a particular DER resource or group of resources.

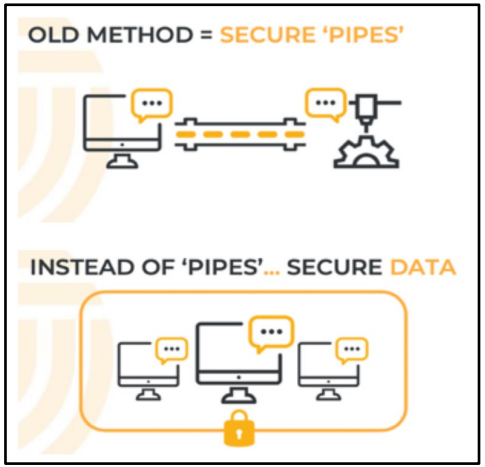
DER Vendor – The entity that originally built the DER resource, or components of the DER resource.

Essential DER and Cybersecurity Terms

Likelihood and Opportunity: Assessment of the “hack value” notion among hackers that something is worth doing.
Vulnerability: Existence of a weakness, design, or implementation error that can lead to an attacker gaining access.
Zero-day attack: An attack that exploits vulnerabilities before the vendor releases a patch for that vulnerability.
DER Ransomware: An attack that takes control of a DER and encrypts its operational software until a ransom is paid. While a financial frustration to the DER owner, a ransomware attack on a single DER is not likely to be noticed by a grid operator.
DER Botnet: An attack infecting enough DER, controlled by the attacker, that enables grid instability at a larger scale than previously possible.
DER Worm: DER attack on a single DER that could propagate to higher level systems belonging to a grid operator or aggregator or laterally to other DER systems.

Emerging Technologies





Named data networking (NDN) is a new Internet architecture that enables secure end-to-end communications without depending on the security or topology of underlying channels.

Instead of defending only data channels, NDN secures the data directly by uniquely naming the data packets and by securely binding those names to the data packets using cryptographic signatures.

Source: https://operantnetworks.com/

Relevant Standards, Guides, and Best Practices

- ***IEEE C37.240-2014 –*** *IEEE Standard Cybersecurity Requirements for Substation Automation, Protection, and Control Systems*
- ***NIST SP 800-82 Revision 2:*** *Guide to Industrial Control Systems (ICS) Security*
- **NIST interagency/internal report 7628:** *Guidelines for Smart Grid Cybersecurity*
- ***NIST Cybersecurity Framework****:*
- ***IEEE 2030.5-2018 –*** *IEEE Standard for Smart Energy Profile Application Protocol*
- ***NERC Reliability Guideline****: Cyber Intrusion Guide for System Operators*
- ***IEC 62351****: Information Security for Power System Control Operations*
- ***IEC 62443****: Industrial Automation and Control Systems Security*
- **DOE/DHS ES-C2M2**: *Electricity Subsector Cybersecurity Capability Maturity Model*
- **DOE/NIST/NERC risk management process**: *Electricity Subsector Cybersecurity Risk Management Process Guideline*
- **SEPA Cybersecurity Working Group:** *Identify and address the gaps and challenges to ensure the security of hardware and software, and to create reference cybersecurity policies.*