Utility and Grid Operator Resources for Future Power Systems Webinar Series

Distribution Cybersecurity: Cybersecurity Considerations of Distributed Resources

Nik Urlaub, Senior Engineer, National Renewable Energy Laboratory (NREL)

NREL Webinar Series

June 10, 2025

In This Presentation

1. Evolving threats to energy infrastructure
- Primary cybersecurity challenges for the future energy systems
- Phases of a successful cyberattack
- History of relevant cyberattack.

2. Understanding distributed energy resources (DERs) and DER systems
- What links DERs and cyber
- Projected future DER system architectures.

3. Standards/guides/policies
- Cybersecurity baselines for electric distribution systems and DERs
- Institute for Electrical and Electronic Engineers (IEEE) 1547.3.

4. Advanced Research on Integrated Energy Systems (ARIES) Platform Overview

Evolving Threats to Energy Infrastructure

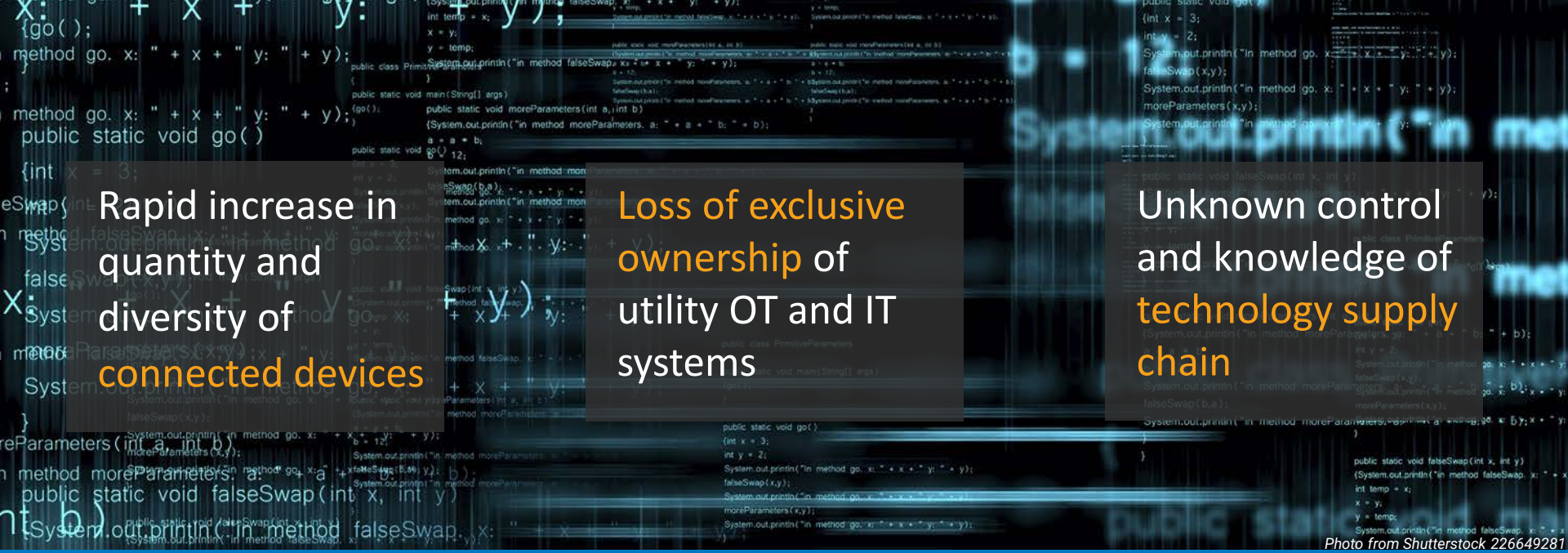
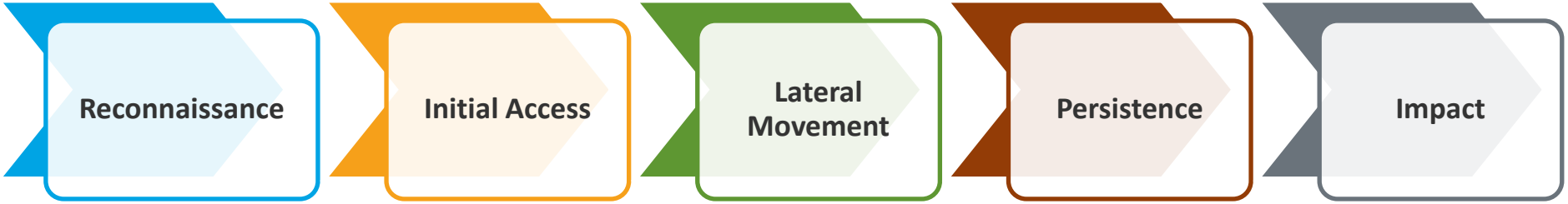


Photo from Shutterstock 226649281

Future Grid Security: Grand Challenges

With potentially orders of magnitude increases in connected devices operating autonomously—the vast majority being customer-owned grid assets—and hardware and software uncertainties for new equipment, cybersecurity for the evolving grid will be critical.

Phases of a Successful Cyberattack



Example: Ukraine December 2015 Power Grid Cyberattack

- Started with a spear-phishing campaign to deliver "BlackEnergy3" malware through malicious email to a Ukrainian electricity distribution company
- Conducted extensive reconnaissance and scanning over several months
- Gained access to Windows Domain Controllers to steal credentials
- Launched attack by sending trip commands to multiple circuit breakers
- Disabled backup power supplies while trying to maintain access for as long as they could
- Launched denial-of-service attack against customer call centers to prevent customers from calling in to report the outage.

Recent Cyberattacks

Photo from Shutterstock 1378498457

December 2015: Hackers compromised information systems of energy distribution companies in Ukraine, shutting off 30 substations and disrupting energy services to 230,000 customers.

December 2016: Industroyer malware was deployed against the Ukrainian transmission operator Ukrenergo. It targeted a transmission substation outside of Kiev and disrupted operation for just over an hour.

August 2017: A sophisticated malware—dubbed Triton, Trisis, or HatMan—compromised Schneider Triconex safety instrumented systems in a Middle Eastern petrochemical facility. The attackers' motives remain unclear, as the breach came to light only after an accidental plant shutdown prompted further investigation.

March 2019: Utah-based renewable energy developer was hit by denial of service. The attack exploited a known vulnerability in firewalls to reboot repeatedly, causing 5-minute interruptions 12-hour period.

Recent Cyberattacks (cont'd)

Photo from Shutterstock 1378498457

February 2021: Damage of SolarWinds attack is unveiled, reporting that up to 18,000 customers from federal agencies and private companies installed updates that left organizations vulnerable to hackers.

February 2022: Denial of service attack against the ViaSat network exploited a VPN appliance misconfiguration, causing loss of remote monitoring of 5,800 ENERCON wind turbines.

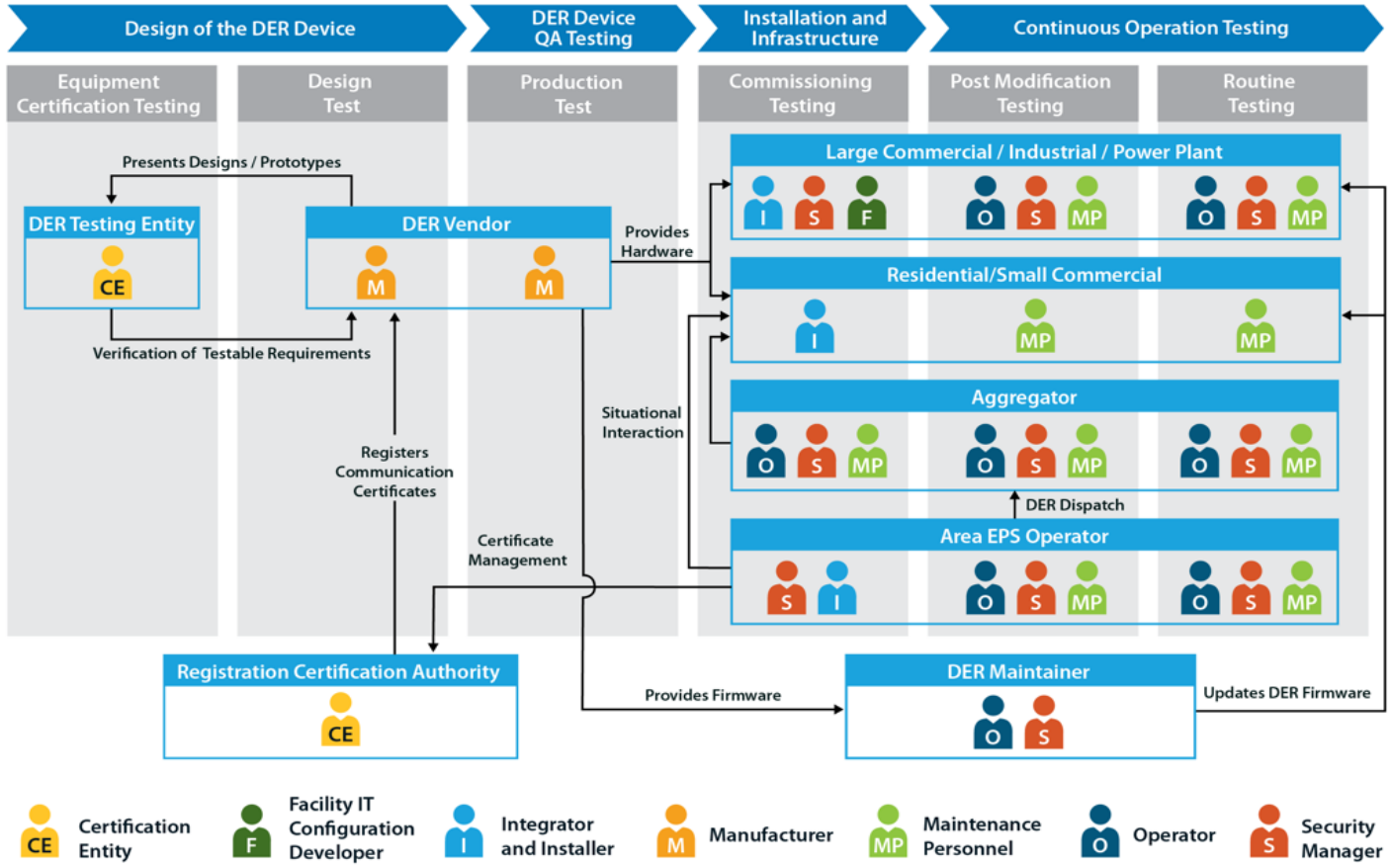
April 2022: Industroyer2 was launched with more configurable mechanisms. It was accompanied by wipers to destroy evidence of attack. However, this time it was discovered before attacks could disrupt power delivery.

May 2023: Twenty-two energy companies in Denmark, including small power and water utilities that operated wind and solar assets, were affected. Unpatched vulnerabilities and zero-day exploits were used. Some organizations were forced to disconnect from the internet and nonessential network connections.

January 2024: In January 2024, the FrostyGoop malware manipulated measurements in ENCO controllers, causing heating outages affecting over 600 apartment buildings in Ukraine during winter.

Understanding DERs and DER Systems

Understanding the Complicated DER Ecosystem



Source: IEEE 1547.3-2023 IEEE Guide for Cybersecurity of Distributed Energy Resources Interconnected with Electric Power Systems. https://ieeexplore.ieee.org/servlet/opac?punumber=10352400

Projected Future DER Systems

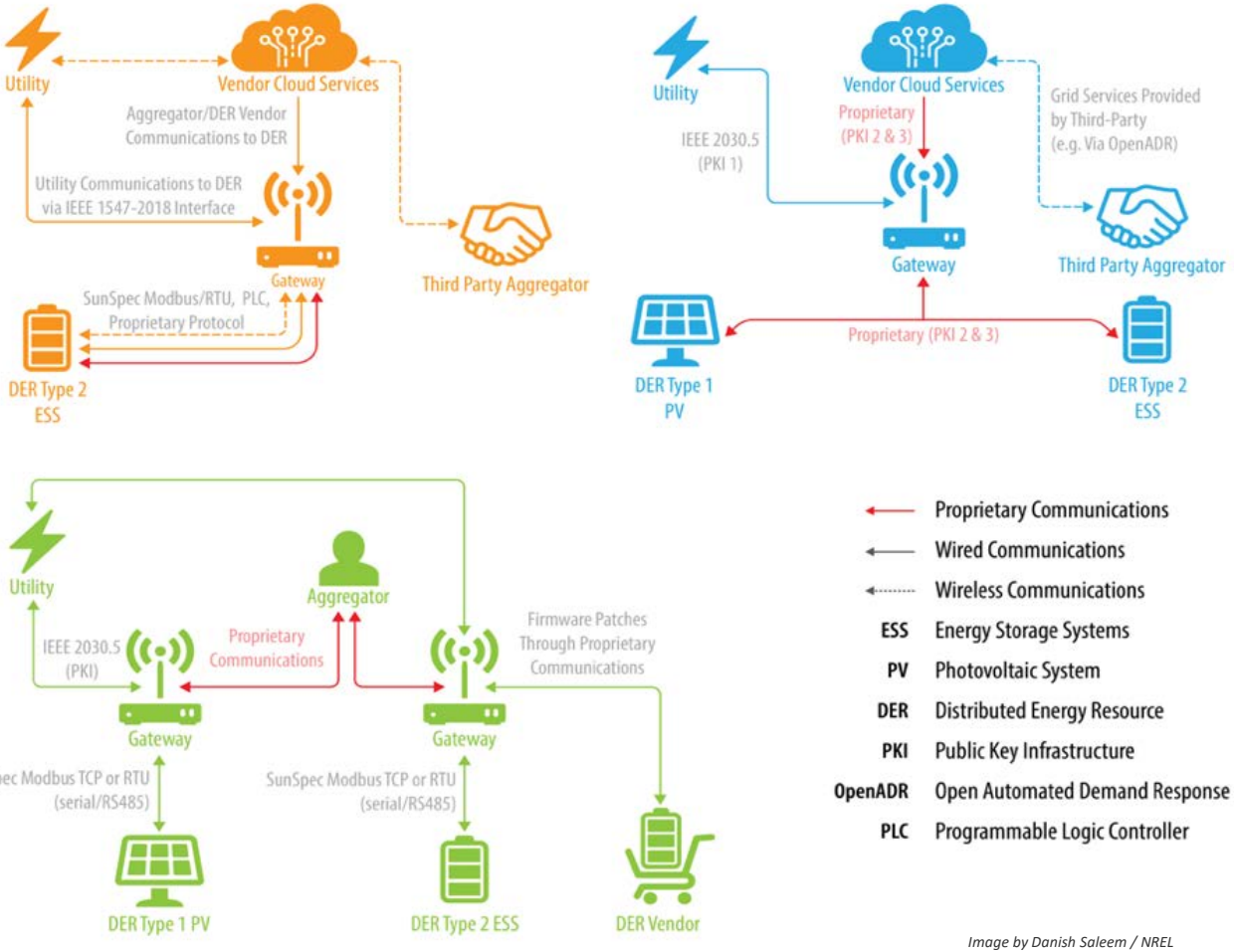


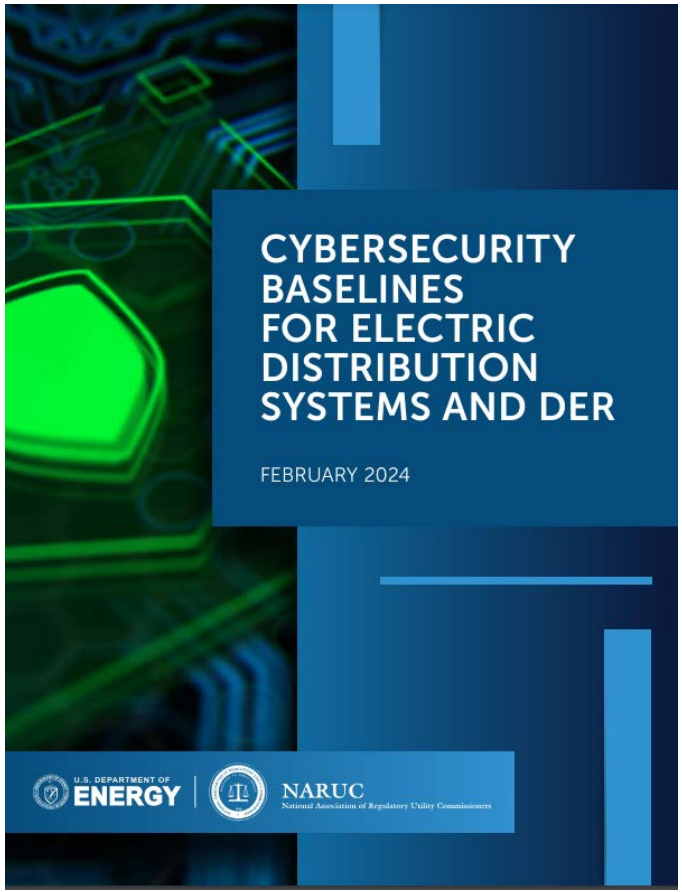
Image by Danish Saleem / NREL

Why Should We Care?

- EIA estimated solar and battery storage make up 81% of new U.S. electric-generating capacity in 2024
- Rooftop and small solar capacity in the US was approximately 53 GW in 2024.
  - This represents about 1/3 of all solar in the US, none of which is required to follow NERC CIP.
  - There is no widely recognized alternative cyber compliance standard for rooftop solar/DER.
- In comparison, the loss of Palo Verde 2,000 MW is the single **largest contingency event**

Standards, Guides, and Policies

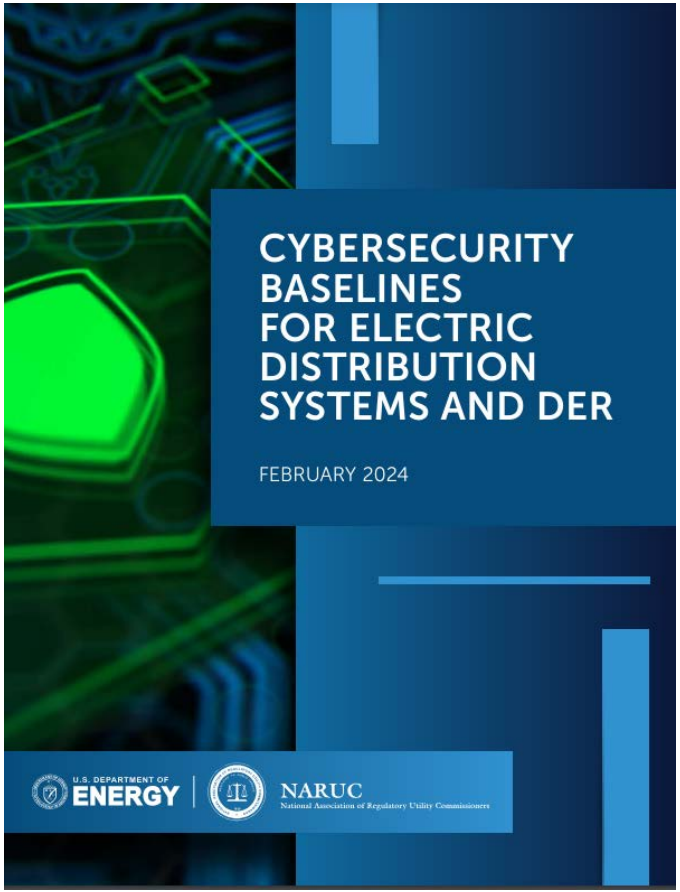
NARUC Cybersecurity Baselines for Electric Distribution Systems and DERs



Background

- The National Association of Regulatory Utility Commissioners (NARUC) collaborated with U.S. Department of Energy (DOE) Office of Cybersecurity, Energy Security, and Emergency Response (CESER) to create cybersecurity baselines for electric distribution systems and DERs.
- These baselines provide vetted recommendations for securing these systems. The interim implementation document focuses on:
  - **Scoping**: Defining which assets, at minimum, should adhere to the baselines based on their risk to the distribution system.
  - **Prioritization**: Identifying the key baselines asset owners/operators should prioritize first.

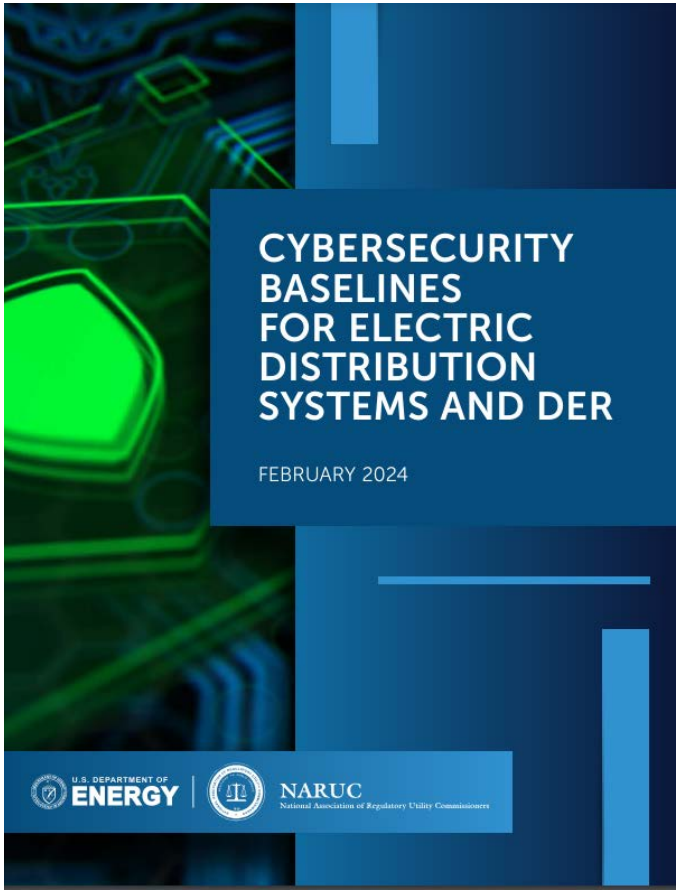
NARUC Cybersecurity Baselines for Electric Distribution Systems and DER



Applicable Systems

- Digital systems or services that directly affect power flow or quality.
- Operator tools for remote monitoring and control of power systems, including transient assets or centralized tools.
- Protective relays tied to power delivery, even if they don't directly alter power flow or quality.
- Automated data exchange systems essential for reliability and power security, including interfaces with battery storage.
- Distributed energy resources (generation, storage, controllable load) and their supporting communication networks.

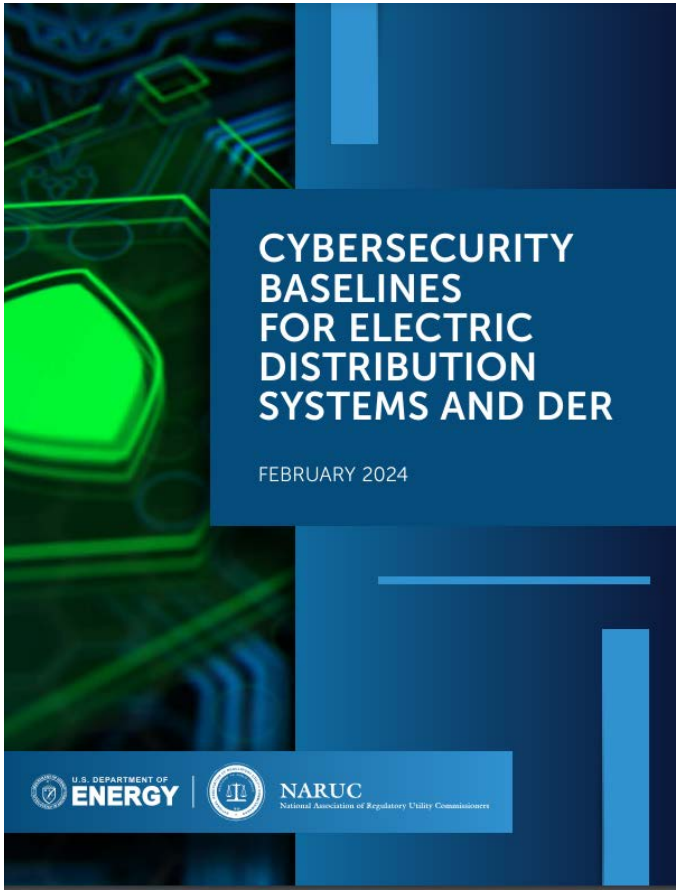
NARUC Cybersecurity Baselines for Electric Distribution Systems and DERs



Priority Baselines for All In-Scope Assets

1.A – Asset Inventory	**1.B** – Organizational Cybersecurity Leadership	**1.C** – OT Cybersecurity Leadership
1.D – Improving IT and OT Cybersecurity Relationships	**1.E** – Mitigating Known Vulnerabilities	**2.A** – Changing Default Passwords
2.B – Password Management	**2.D** – Revoking Credentials for Departing Employees	**2.E** – Separating User and Privileged Accounts

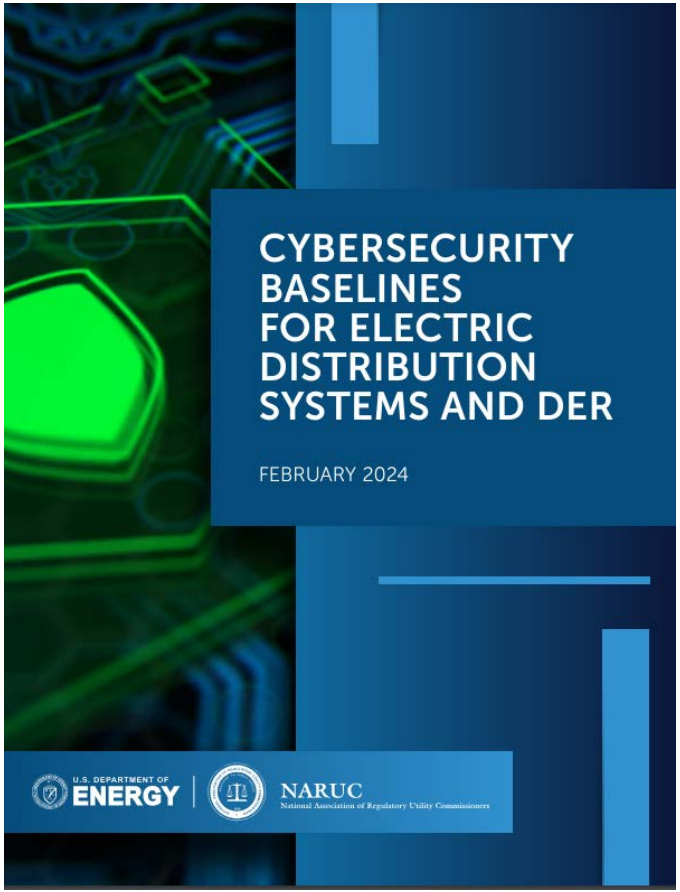
NARUC Cybersecurity Baselines for Electric Distribution Systems and DERs



Priority Baselines for All In-Scope Assets

- **2.F** – Network Segmentation
- **2.H** – Phishing-Resistant Multifactor Authentication
- **2.I** – Basic Cybersecurity Training
- **2.P** – Document & Maintain Network Topology
- **2.R** – System Backups
- **2.W –** No Exploitable Services on the Internet
- **2.X** – Limit OT Connections to Public Internet
- **5.A** – Incident Planning and Preparedness

NARUC Cybersecurity Baselines for Electric Distribution Systems and DERs



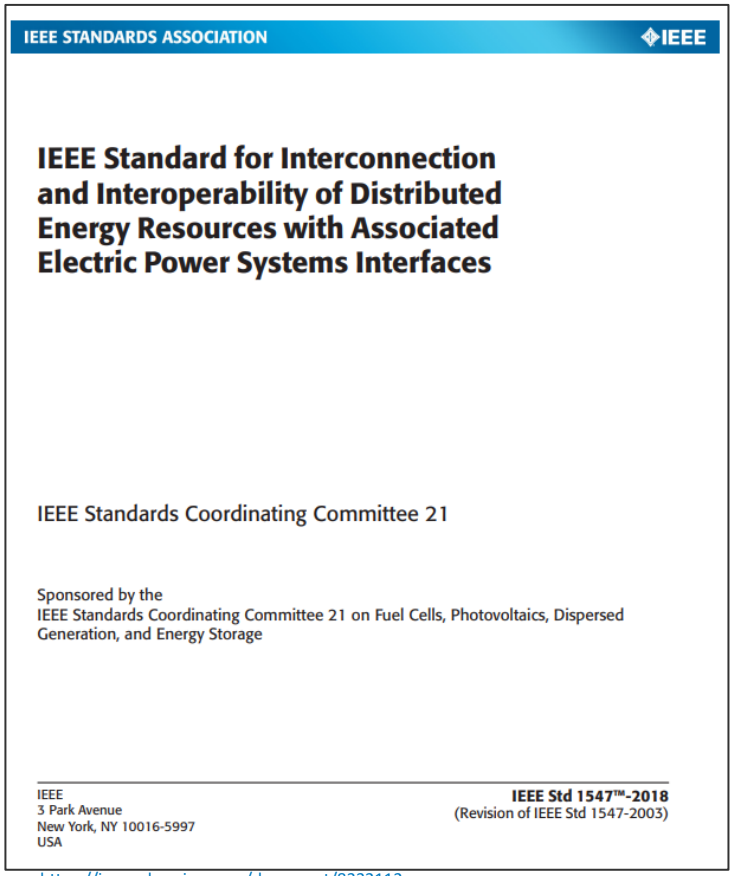
Extra Priority Baselines for In-Scope DER Assets

- **1.F** – Third-Party Validation of Cybersecurity Control Effectiveness
- **1.I** – Vendor/ Supplier Cybersecurity Requirements
- **2.T** – Log Collection
- **2.U** – Secure Log Storage
- **2.V** – Prohibit Connection of Unauthorized Devices
- **4.A** – Incident Reporting

IEEE 1547 Series: Interconnecting Distributed Resources with Electric Power Systems

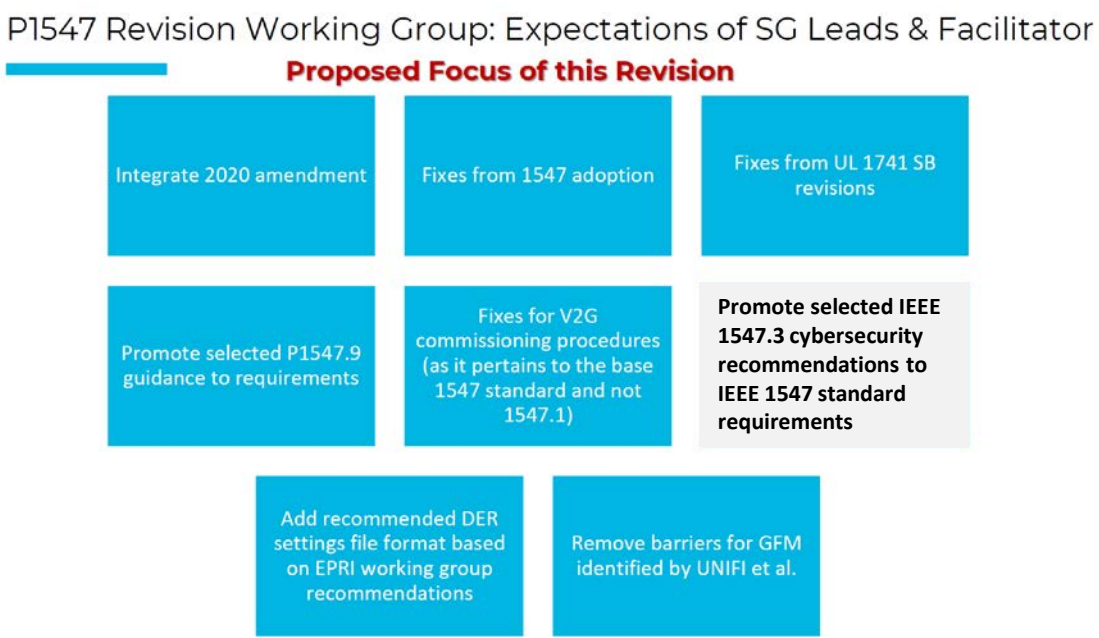
"This standard provides interconnection and interoperability technical and test specifications and requirements for distributed energy resources (DERs). Additionally, several annexes are included in this standard that provide additional material for informative purposes, but are not required to be used in conjunction with this standard."

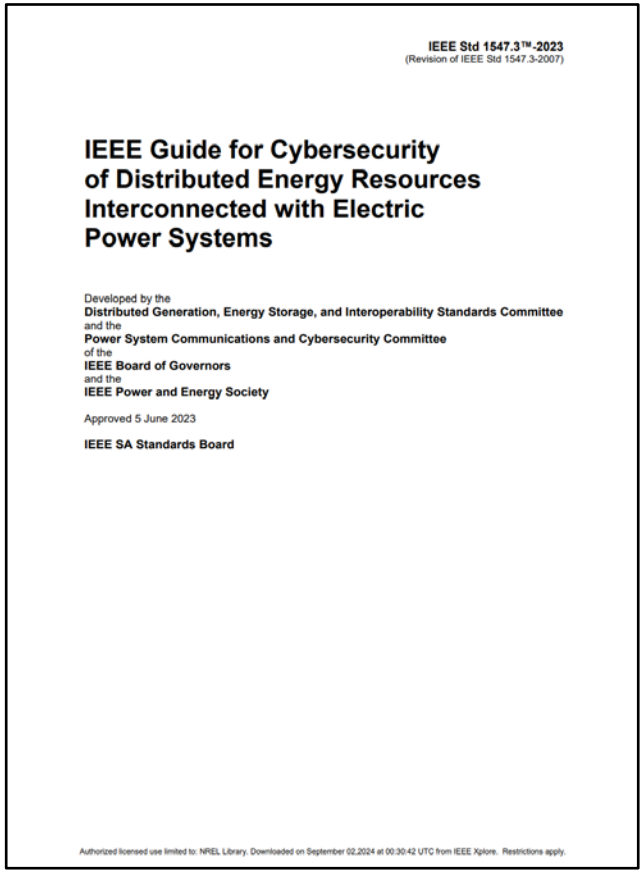
- **IEEE 1547.1-2020** - Describes the testing of the interconnection to determine whether it conforms to standards.
- **IEEE 1547.2-2023** - Provides a technical background on the standard.
- **IEEE 1547.3-2023** - Details cybersecurity guidelines.
- **IEEE 1547.4-2011** - Guide for the design, operation, and integration of conforming systems.
- **IEEE 1547.6-2011** - Describes practices for secondary network interconnections.
- **IEEE 1547.7-2013** - Provides distribution impact studies for distributed resource interconnection.
- **IEEE P1547.9-2022** - Details energy storage guidelines.



https://ieeexplore.ieee.org/document/8332112

IEEE 1547.3: Cybersecurity Guide for DERs




IEEE Std 1547.3™-2023
(Revision of IEEE Std 1547.3-2007)

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

Developed by the
Distributed Generation, Energy Storage, and Interoperability Standards Committee
and the
Power System Communications and Cybersecurity Committee
of the
IEEE Board of Governors
and the
IEEE Power and Energy Society

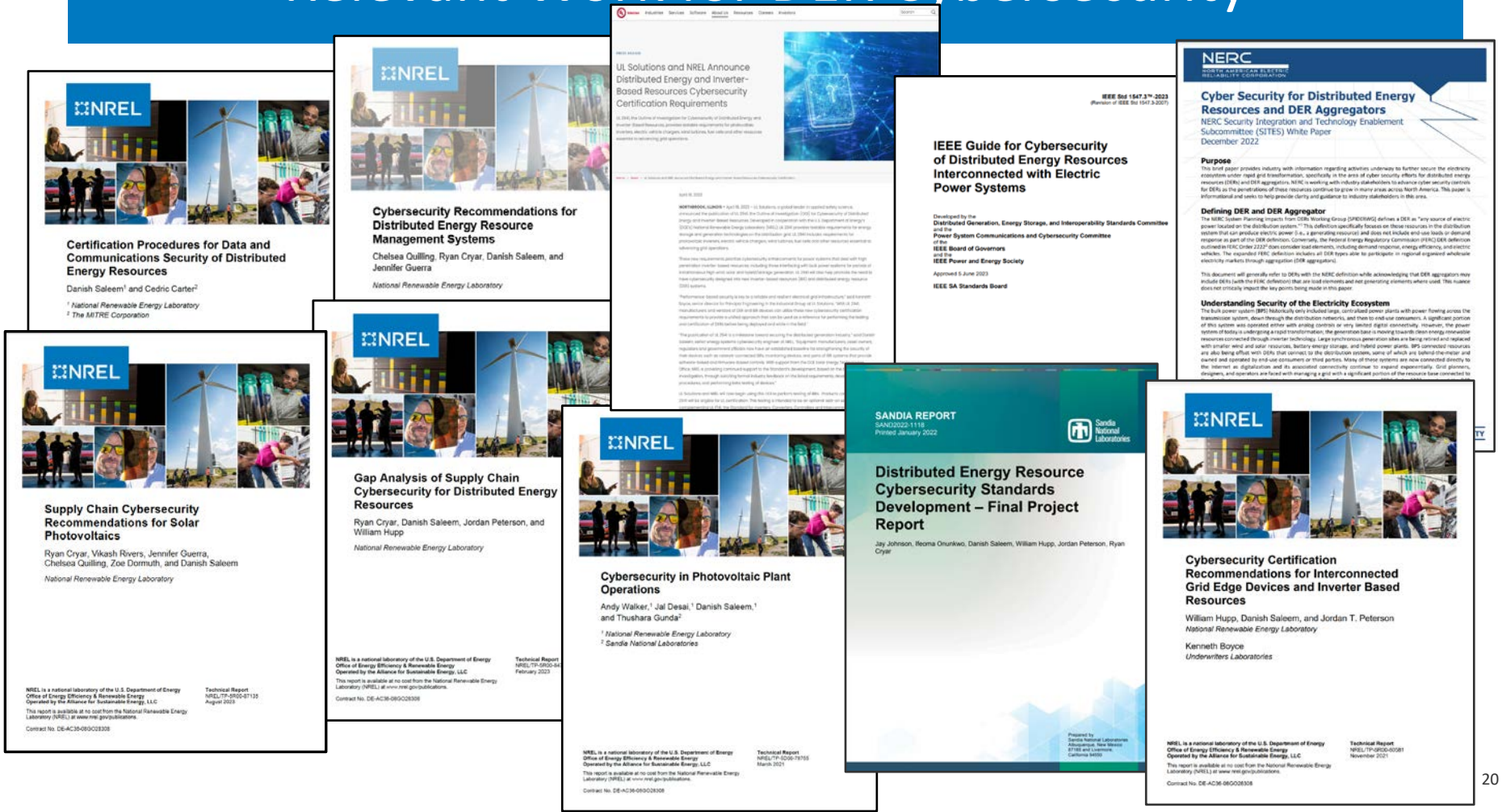
Approved 5 June 2023

IEEE SA Standards Board

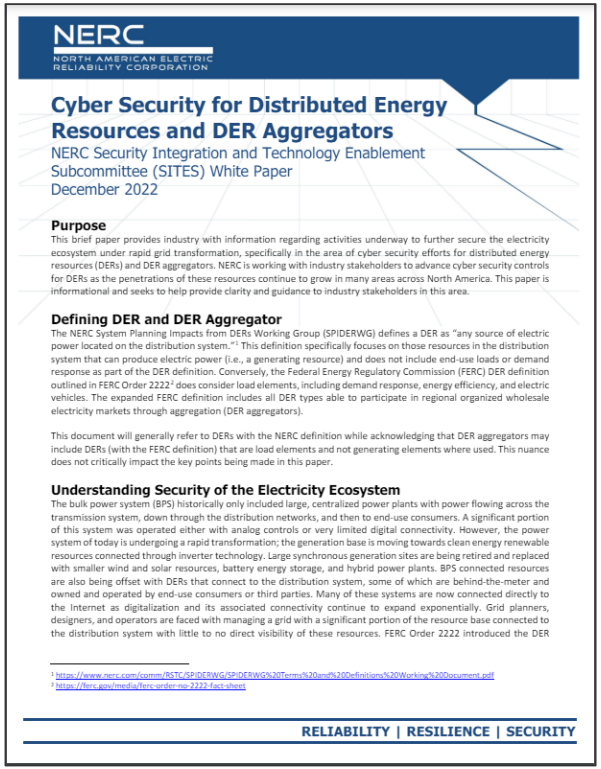
- IEEE 1547.3 cybersecurity guide was published in December 2023 after being approved by the working group and standards coordination committee.
- It was added to the IEEE 1547 standard revision timeline.

https://ieeexplore.ieee.org/document/10352402/keywords#keywords

Relevant Work for DER Cybersecurity



Guidance for DER Cybersecurity



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.

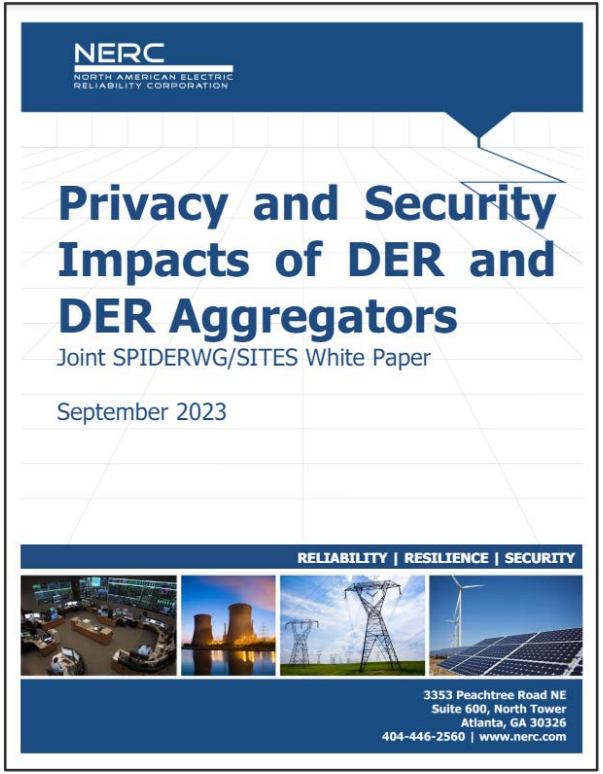
Understanding Security of the Electricity Ecosystem

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

https://www.nerc.com/comm/RSTC_Reliability_Guidelines/White_Paper_Cybersecurity_for%20DERs_and_DER_Aggregators.pdf .



NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Privacy and Security Impacts of DER and DER Aggregators

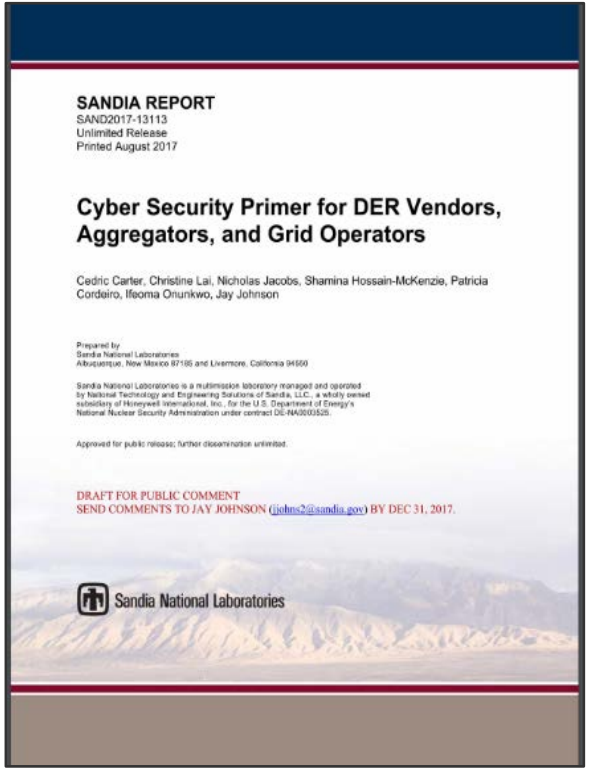
Joint SPIDERWG/SITES White Paper

September 2023

RELIABILITY | RESILIENCE | SECURITY

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

https://www.nerc.com/comm/RSTC_Reliability_Guidelines/JointWhitePaper_PrivacyAndSecurityImpactsOfDERAggregators.pdf.



SANDIA REPORT
SAND2017-13113
Unlimited Release
Printed August 2017

Cyber Security Primer for DER Vendors, Aggregators, and Grid Operators

Cedric Carter, Christine Lai, Nicholas Jacobs, Shamina Hossain-McKenzie, Patricia Cordeiro, Ifeoma Onunkwo, Jay Johnson

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

Sandia National Laboratories is a multimission 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-NA0003525.

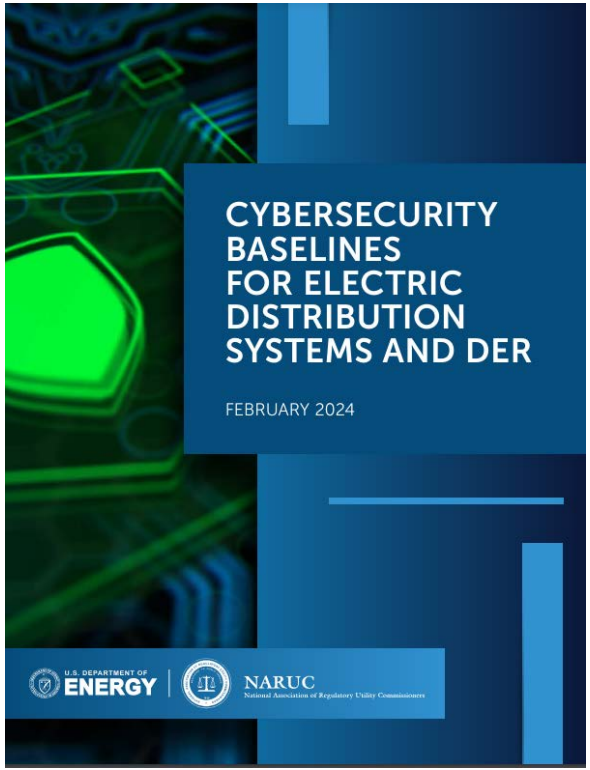
Approved for public release; further dissemination unlimited.

DRAFT FOR PUBLIC COMMENT
SEND COMMENTS TO JAY JOHNSON (johns2@sandia.gov) BY DEC 31, 2017.

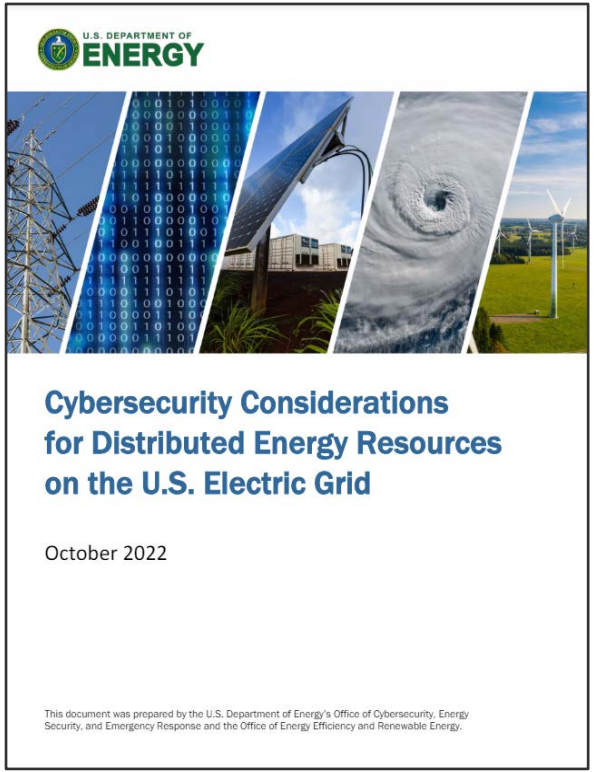
Sandia National Laboratories

https://www.osti.gov/servlets/purl/1761987/

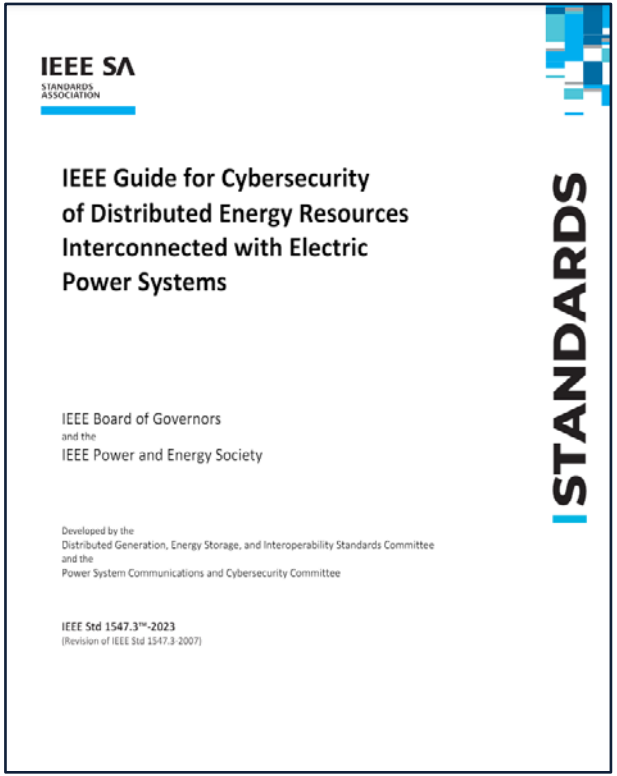
Guidance for DER Cybersecurity (cont'd)



https://www.naruc.org/core-sectors/critical-infrastructure-and-cybersecurity/cybersecurity-for-utility-regulators/cybersecurity-baselines/.



https://www.energy.gov/eere/articles/doe-cybersecurity-report-provides-recommendations-secure-distributed-clean-energy.



https://ieeexplore.ieee.org/document/10352402.

ARIES Overview

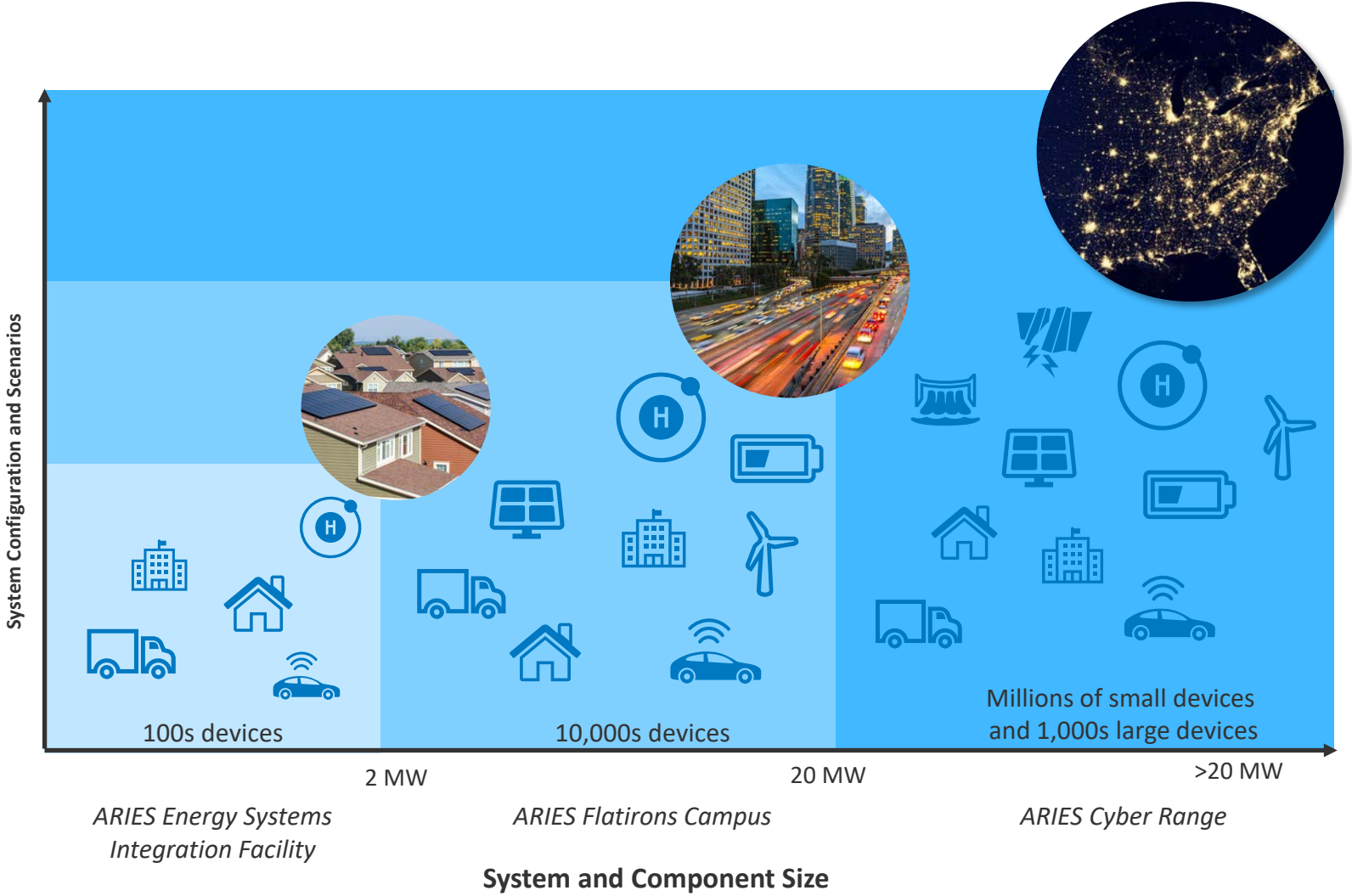
ARIES by NREL

ESIF – 2 MW

FC – 20 MW

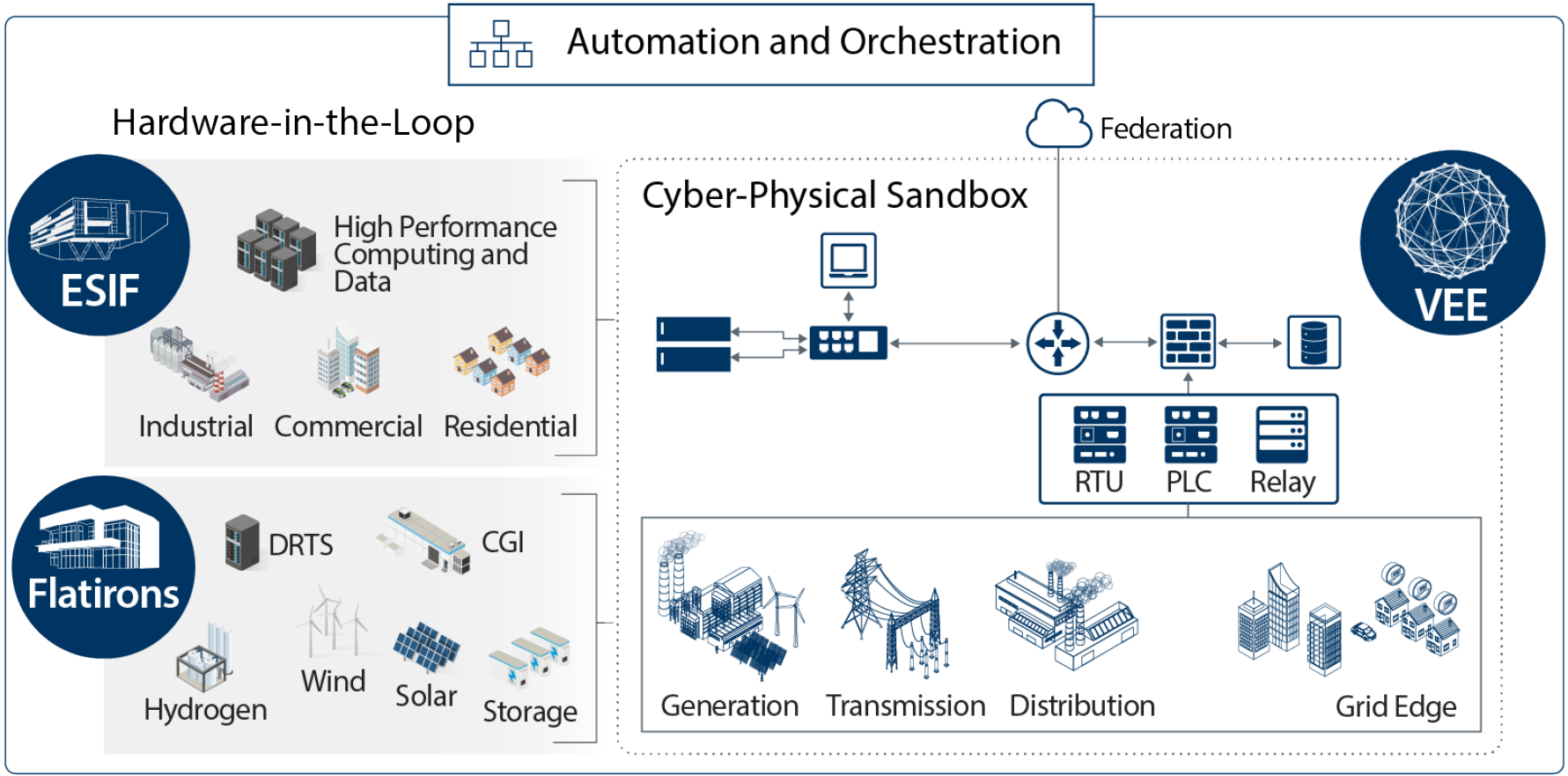
Cyber Range – Scale

ARIES Scale

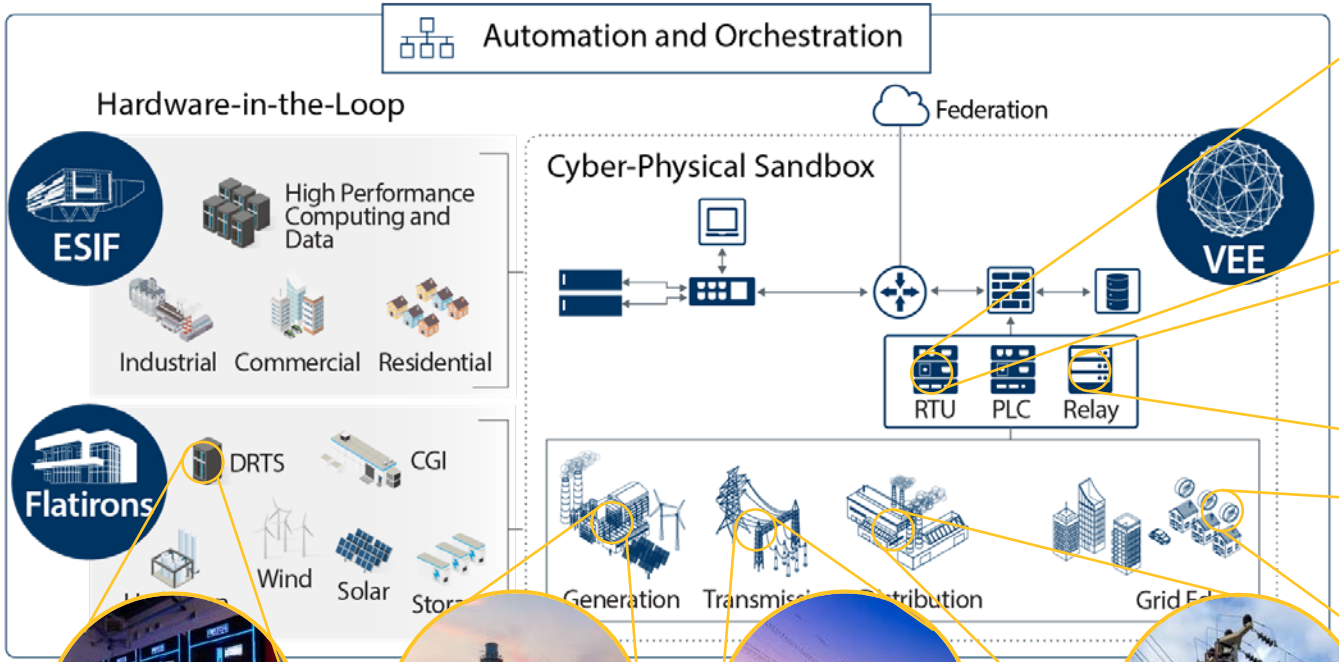


ARIES by NREL

ARIES Cyber Range



ARIES Cyber Range



RTU

Relay

Smart Meter

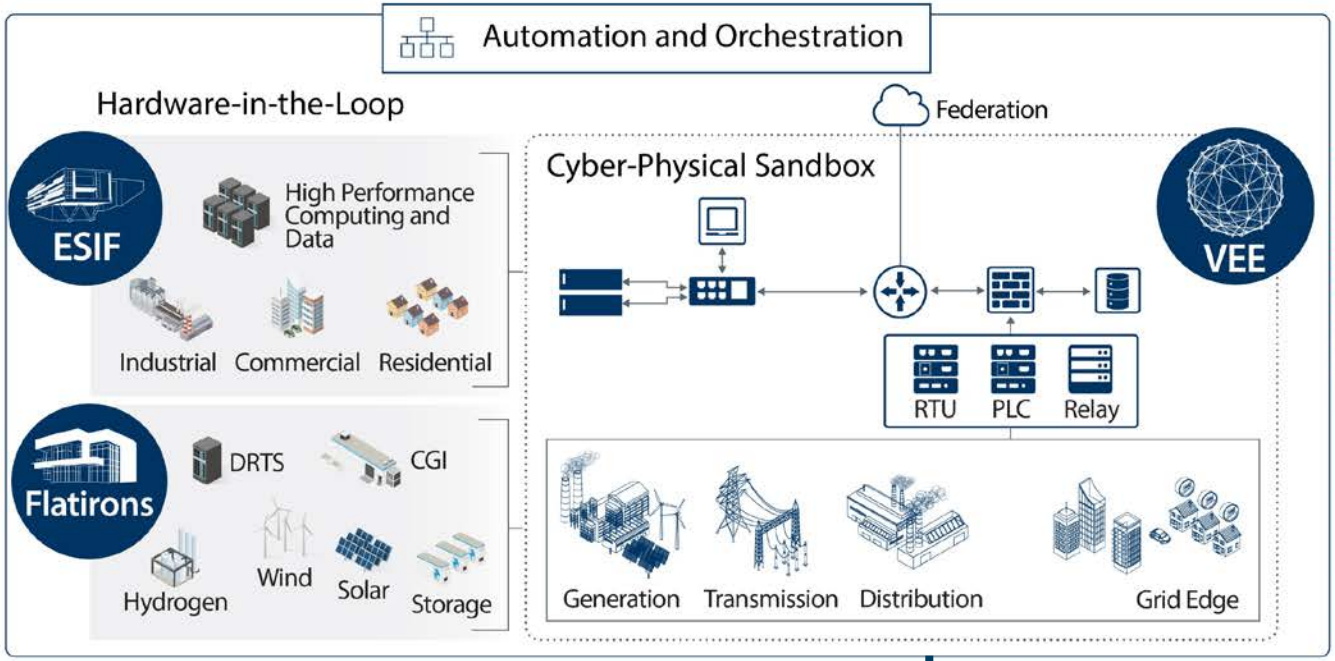
DRTS

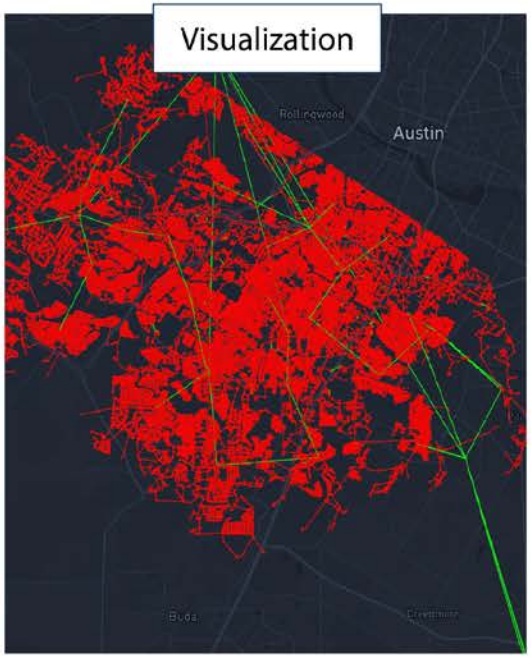
Generation

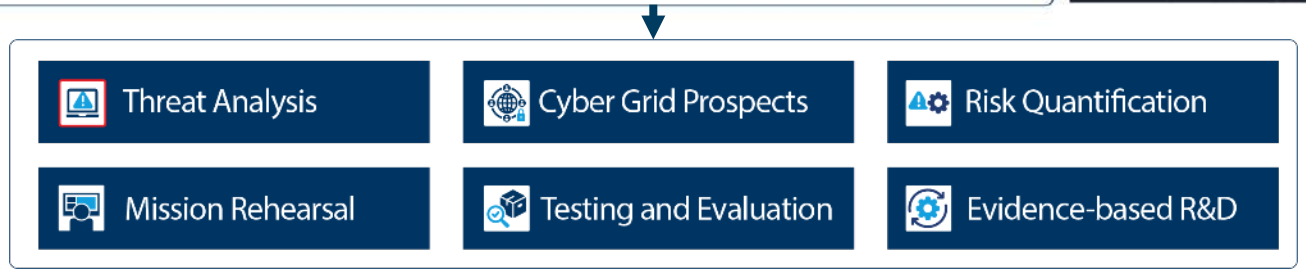
Transmission

Distribution

ARIES Cyber Range







A Unique, World-Class Capability

- Emulates **millions of diverse, distributed devices** in minutes
- Integrates **full-scale power system hardware** across ARIES
- Leverages **industry-validated**, high-fidelity reference architectures
- Deploys **threat-to-consequence modeling** for all-hazards analysis
- Federates **public cloud infrastructure**
- Yields **unmatched visualizations** showing cyber-physical interactions

References

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*
- **IEEE 1547.3:** *Cybersecurity Guide for DER Interconnected with Electric Power Systems*
- **UL 2941:** *Cybersecurity Certification Standard for Distributed Energy and Inverter-Based Resources*

Relevant Cybersecurity Event References

- *https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01*
- *https://www.dragos.com/resources/whitepaper/crashoverride-analyzing-the-malware-that-attacks-power-grids/*
- https://www.dragos.com/resources/whitepaper/anatomy-of-an-attack-detecting-and-defeating-crashoverride/
- *https://cyberscoop.com/spower-power-grid-cyberattack-foia/*
- *https://www.congress.gov/crs-product/IN11559*
- *https://www.viasat.com/perspectives/corporate/2022/ka-sat-network-cyber-attack-overview/*
- *https://cloud.google.com/blog/topics/threat-intelligence/sandworm-disrupts-power-ukraine-operational-technology/*
- *https://www.securityweek.com/22-energy-firms-hacked-in-largest-coordinated-attack-on-denmarks-critical-infrastructure/*

Links to NREL Resources

- ***Certification Procedures for Data and Communications Security of Distributed Energy Resources***
  - *https://www.nrel.gov/docs/fy19osti/73628.pdf*
- ***Cybersecurity Guidance for Distributed Energy Resource Management Systems (DERMS)***
  - *https://www.nrel.gov/docs/fy23osti/87289.pdf*
- **Supply Chain Cybersecurity Recommendations for Solar Photovoltaics**
  - *https://www.nrel.gov/docs/fy23osti/87135.pdf*
- ***Gap Analysis of Supply Chain Cybersecurity for Distributed Energy Resources***
  - *https://www.nrel.gov/docs/fy23osti/84752.pdf*
- ***Cybersecurity in Photovoltaic Plant Operations***
  - *https://www.nrel.gov/docs/fy21osti/78755.pdf*
- ***Cybersecurity Certification Recommendations for Interconnected Grid Edge Devices and Inverter Based Resources***
  - *https://www.nrel.gov/docs/fy22osti/80581.pdf*
- ***ARIES Cyber Range Details***
  - https://www2.nrel.gov/security-resilience/cyber-range

Thank You

www.nrel.gov

Let’s work together! Nik.Urlaub@nrel.gov

NREL/PR-5T00-94352

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 Policy. 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.