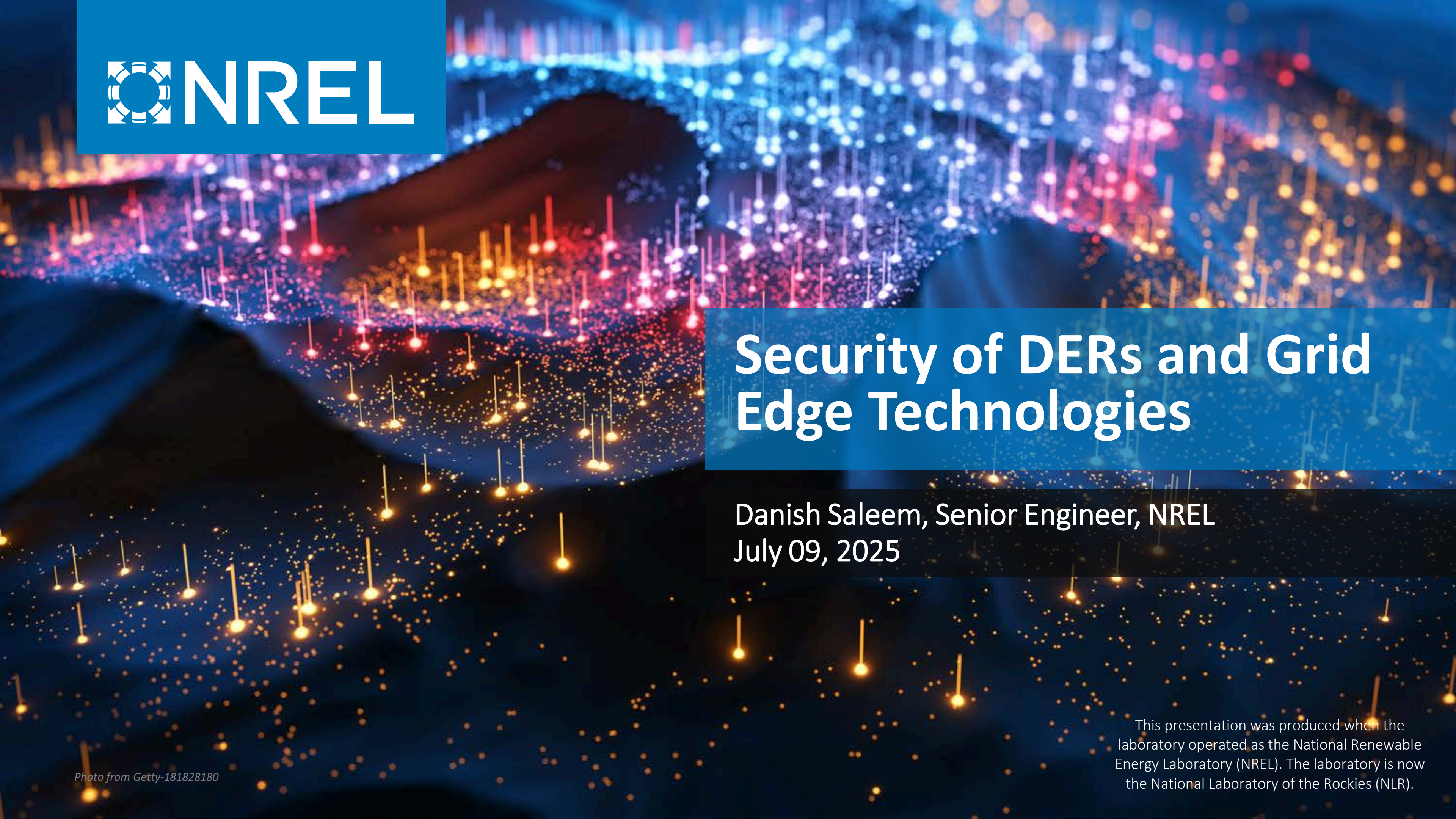
DISCLAIMER



NREL

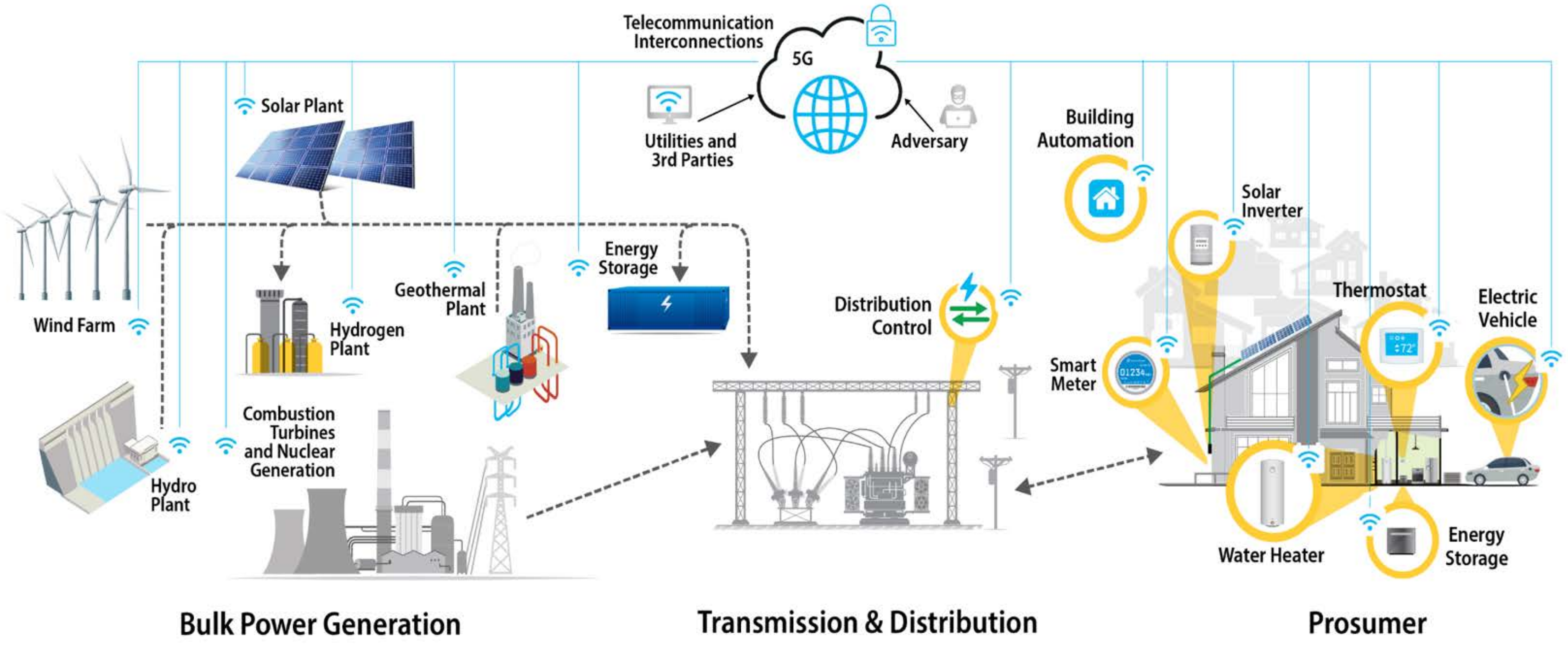
Security of DERs and Grid Edge Technologies

Danish Saleem, Senior Engineer, NREL
July 09, 2025

Photo from Getty-181828180

In this Presentation

- Introduction
  - A New Frontier
  - Cybersecurity Grand Challenges
  - IBRs vs DERs
- What happens if:
  - Threats and Consequence
  - Simulating Cyber-Attack on Transmission and Distribution Systems
- Security through standards
  - Evolution of Standards
  - Standards library
  - Cybersecurity certification and guide
- Shared responsibility model

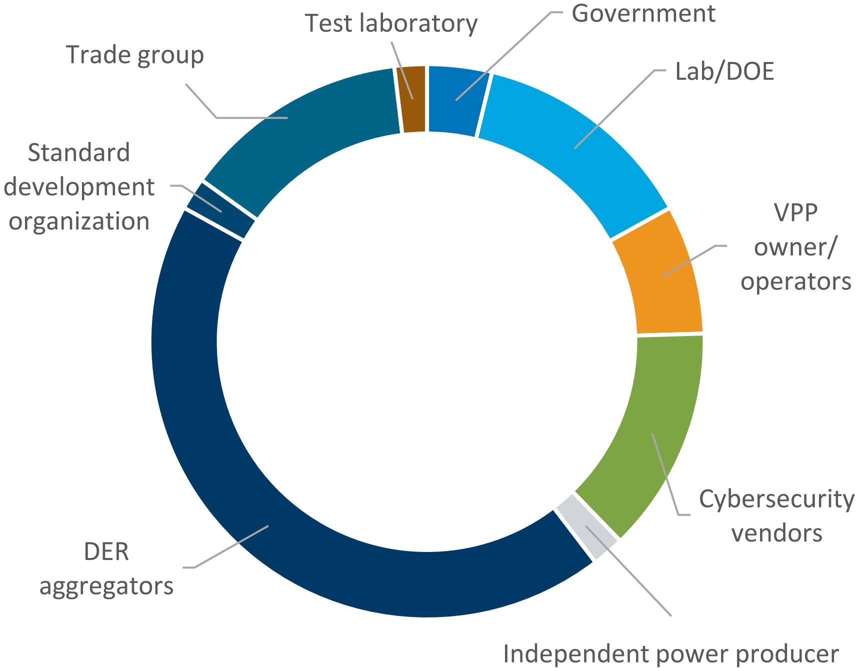


A New Frontier:

The grid is evolving to become more distributed, intelligent, and complex.

- This modernization drives new utility business models with a growing number of non-utility stakeholders playing an active role in energy markets and providing grid services.
- Coupled with aging infrastructure, the risks of emerging energy systems to disruption are not yet well understood.

New and Diverse Stakeholders



EXAMPLE OF STAKEHOLDERS

(not an exhaustive list)

- EDF Power Solutions
- Enphase
- Itron, Inc
- Dragos Inc
- NextEra Energy, Inc.
- Axio
- Xcel Energy
- GridSecurity Inc.
- Hawaii State Energy Office
- United Power
- RMI/Virtual Power Plant Partnership (VP3)
- Duke Energy
- DER Security
- Berkshire Hathaway Energy
- Yaskawa Solectria Solar
- Department of Energy
- Ava Community Energy
- Portland General Electric
- CNK Solutions
- UL.LLC
- UL Solutions
- Tesla
- National Association of Regulatory Utility Commissioners
- EnergyHub
- OptimusCloud
- Southern California Edison
- NRECA
- Olivine
- Burns & McDonnell Engineering
- SEIA
- E-ISAC / NERC
- Edison Electric Institute
- SolarEdge
- Utilidata
- Idaho National Laboratory
- LADWP

Rapid increase in the quantity and diversity of connected devices

No standardized ownership models for aggregated DER Systems

Evolving cybersecurity threats challenging grid reliability

Lack of a national standard with industry trust and consensus

Different approaches for managing risk, establishing accountability, and handling data

Cybersecurity Grand Challenges

Wide variations in technologies, standards, and regulations present a major challenge for applying consistent and interoperable cybersecurity policies at the national level. It is imperative to understand and visualize the risks to better understand cascading failures in the future electric grid.

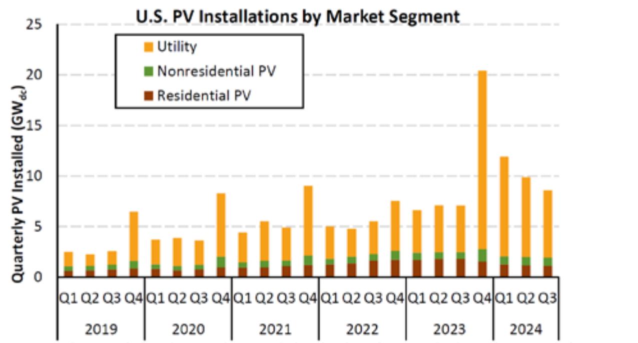
Photo from Adobe Stock

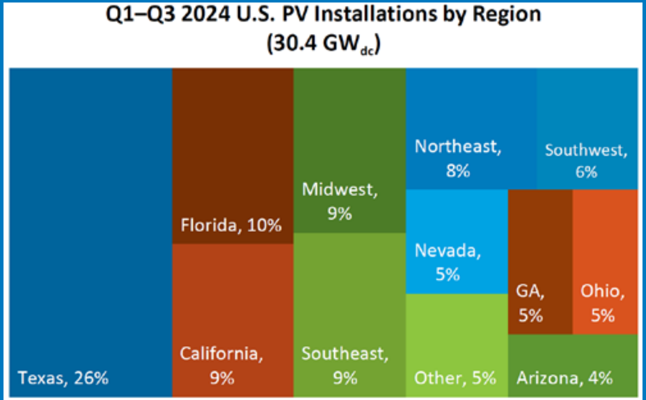
Essential DER and Cybersecurity Terms

- **Distributed Energy Resources (DERs)** – DERs are controllable grid-edge devices, including generation resources (wind, solar), storage (battery, hydrogen), and energy management systems (demand response, building load controllers) that are typically connected to the distribution grid behind a customer's meter
- **Virtual Power Plants (VPP)** – VPPs are aggregations of DERs that can balance electrical loads and provide utility-scale and utility-grade grid services like a traditional power plant. They enable smaller energy resources to participate in energy markets and provide grid services as aggregated entities, which would otherwise not be feasible.
- **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.
- **Utility** –The entity responsible for electricity distribution and grid management. They can leverage DERs or VPPs to enhance grid reliability and resilience. Utilities
- **Internet of Things (IoT) devices vs DERs** – DERs are subject to performance requirements of 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.




What links DER and Cyber? *Interconnection*

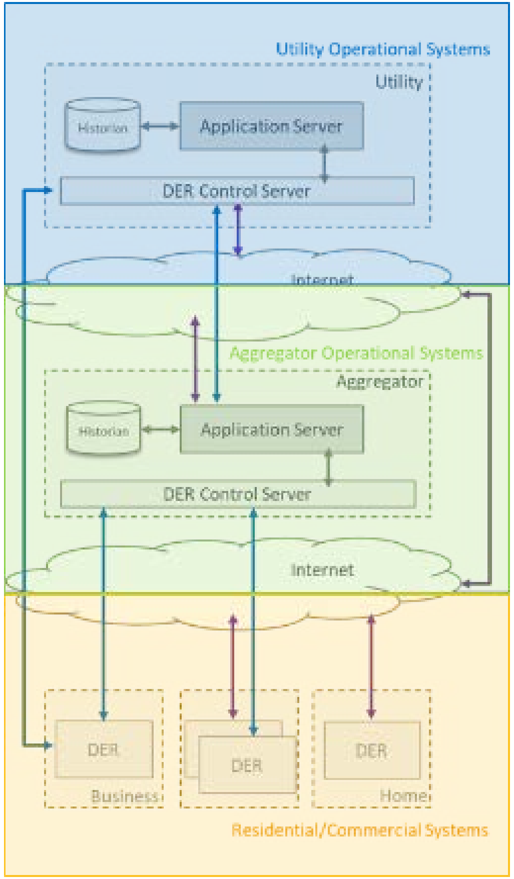




Source: Wood Mackenzie/SEIA, U.S. Solar Market Insight: Q4, 2024

- Interconnection standard
  - Provide a transparent and efficient means to connect generations sources to electric power systems
  - Maintain safety, reliability, power quality, and <u>*security*</u> of electric power systems
- IEEE 1547 was revised in 2018 for grid support capabilities from DERs.
  - But there are no "shall have" cybersecurity requirements.
- IEEE 1547.3 is a draft guideline with "may have" cyber requirements
- UL 2941 is the cybersecurity certification standard for DERs that provides testable requirements for device-level cybersecurity

Understanding DER Systems Roles is Critical



- **Utility Systems** need operational data from devices they do not own and operate
- **DER Aggregators** are becoming 3rd party grid services providers, sending control requests to DERs
- **Customers** are not skilled at securing their DER devices

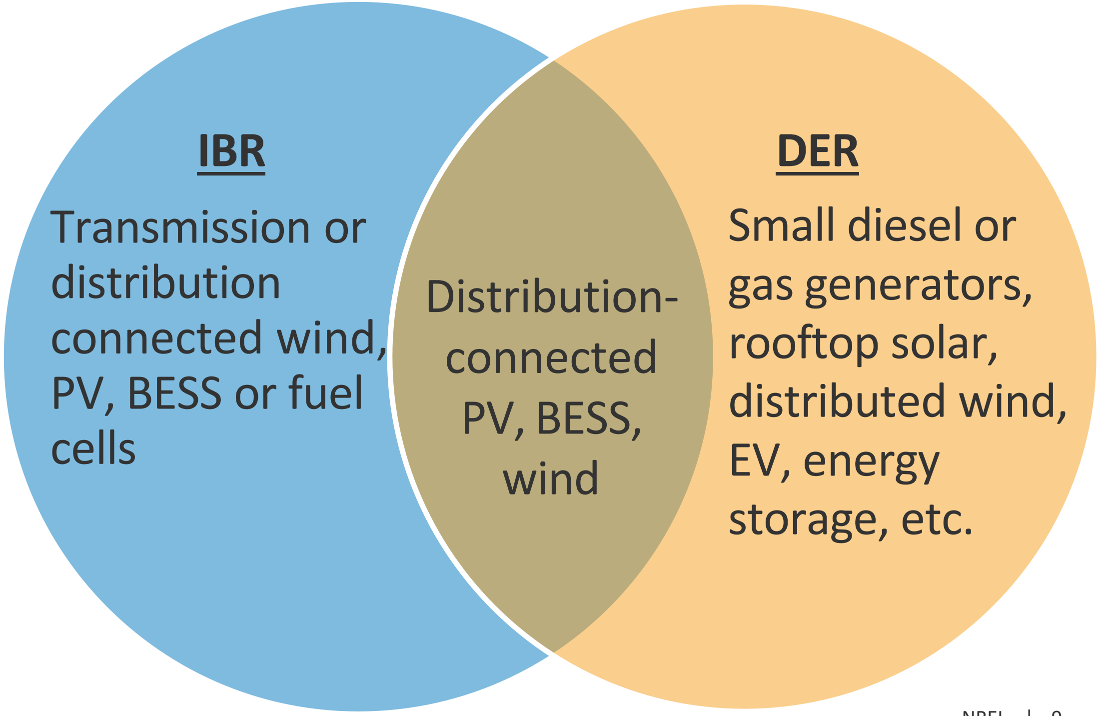
IBR versus DER: What's the difference?

- Inverter-based resource (IBR) refers to **power electronic converter-interfaced generation and storage resources** that can be connected to the electric power system (transmission, sub-transmission, or distribution system) and consists of one or more IBR unit(s) operated as a single resource at a common point of interconnection (in NERC terms)

- Distributed Energy Resources (DERs) refers to **controllable generation, storage, or load devices that are interconnected specifically to the distribution system** (in the IEEE 1547 terms), behind a customer's meter.

- Many DERs are IBRs, including the most common types: PV, battery

Examples of IBRs and DERs



In this Presentation

- Introduction
  - A New Frontier
  - Cybersecurity Grand Challenges
  - IBRs vs DERs
- What happens if:
  - Threats and Consequence
  - Simulating Cyber-Attack on Transmission and Distribution Systems
- Security through standards
  - Evolution of Standards
  - Standards library
  - Cybersecurity certification and guide
- Shared responsibility model

What Happens If...?

We have grid-scale models of power flow, but not of operational risk (cyber or all-hazard)

Questions yet to be answered:

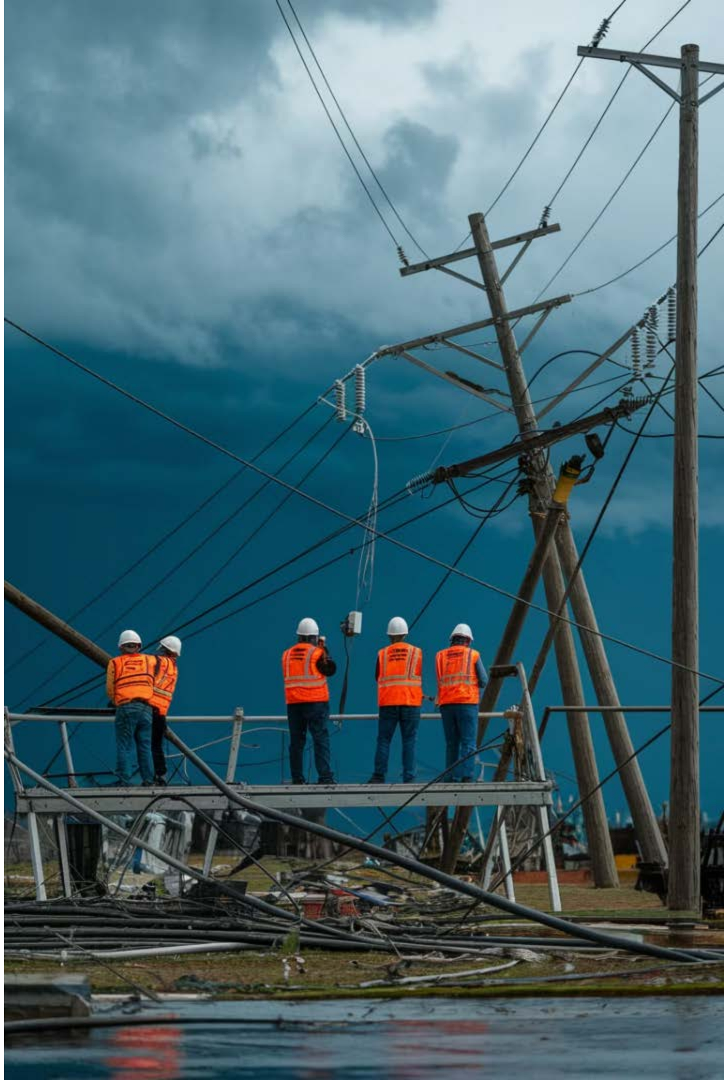
What is the national exposure ?

What would a CrowdStrike event look like for DERs ?

Can we endure instant load shedding of foreign-controlled crypto-mining data centers, regionally or nationally?

How does pending legislation change the risk calculus?

Grid-scale rapid risk simulation would enable forward-looking risk response at the national level

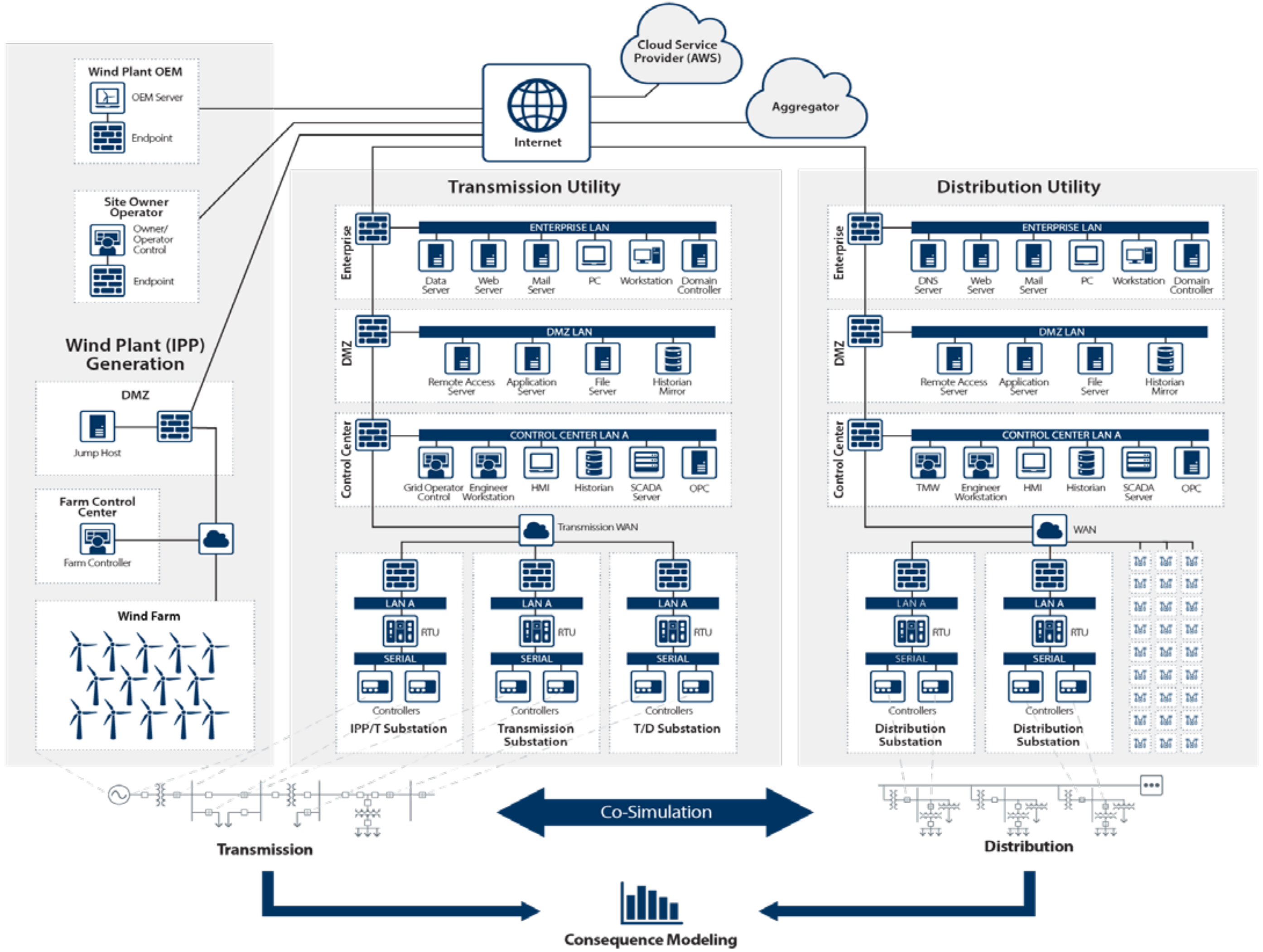


Phases of a Successful Cyberattack

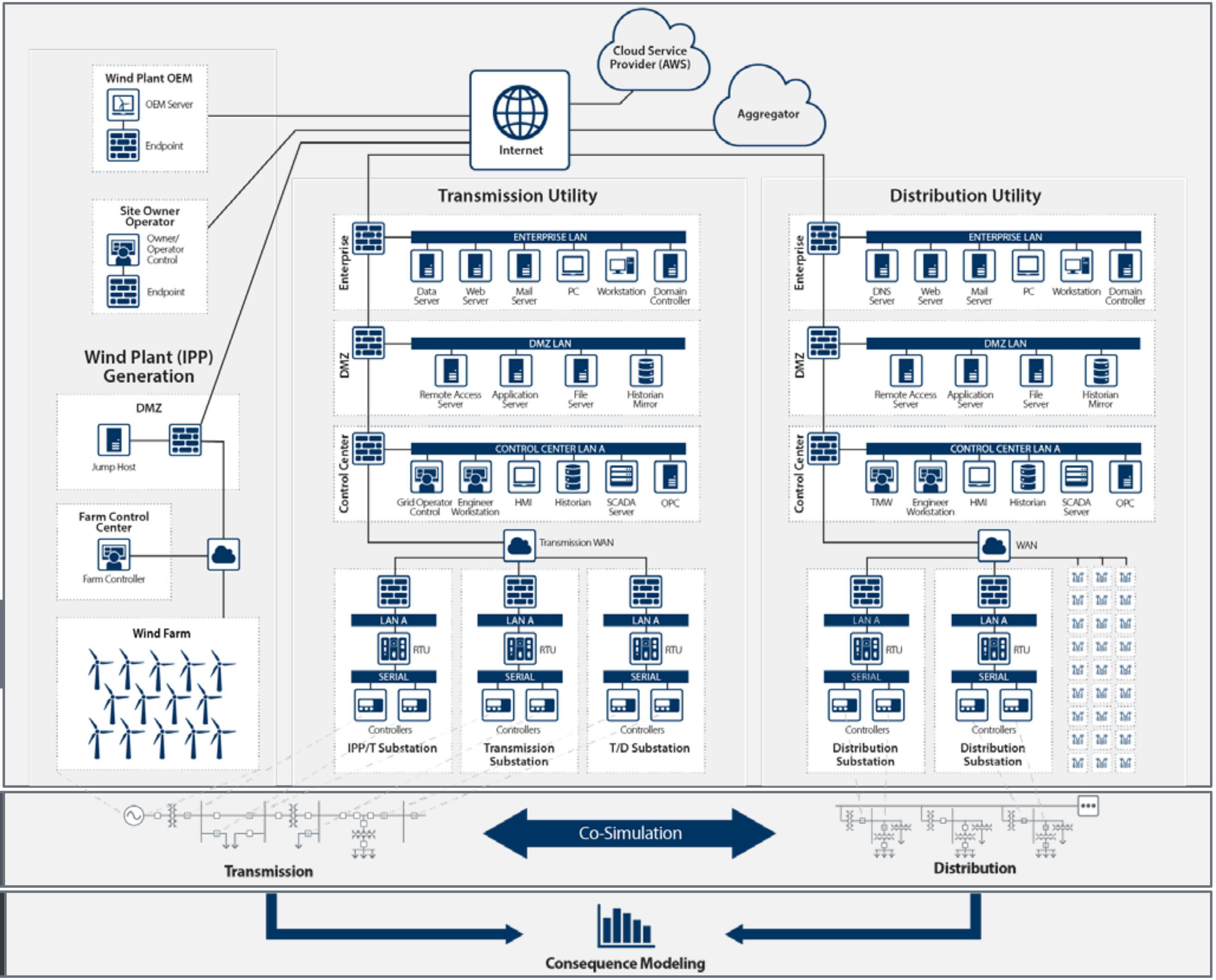
<u>Example</u>: <u>Ukraine Power Grid Cyber-Attack</u>

- Started with a spear-phishing campaign to deliver “BlackEnergy3” malware through malicious email to 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 simultaneous 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.

NREL ARIES Cyber Range Environment



Environment Details



CYBER RANGE

POWER SYSTEM ANALYSIS & PLANNING

CONSEQUENCE & IMPACTS ANALYSIS

Cyber Threat Details

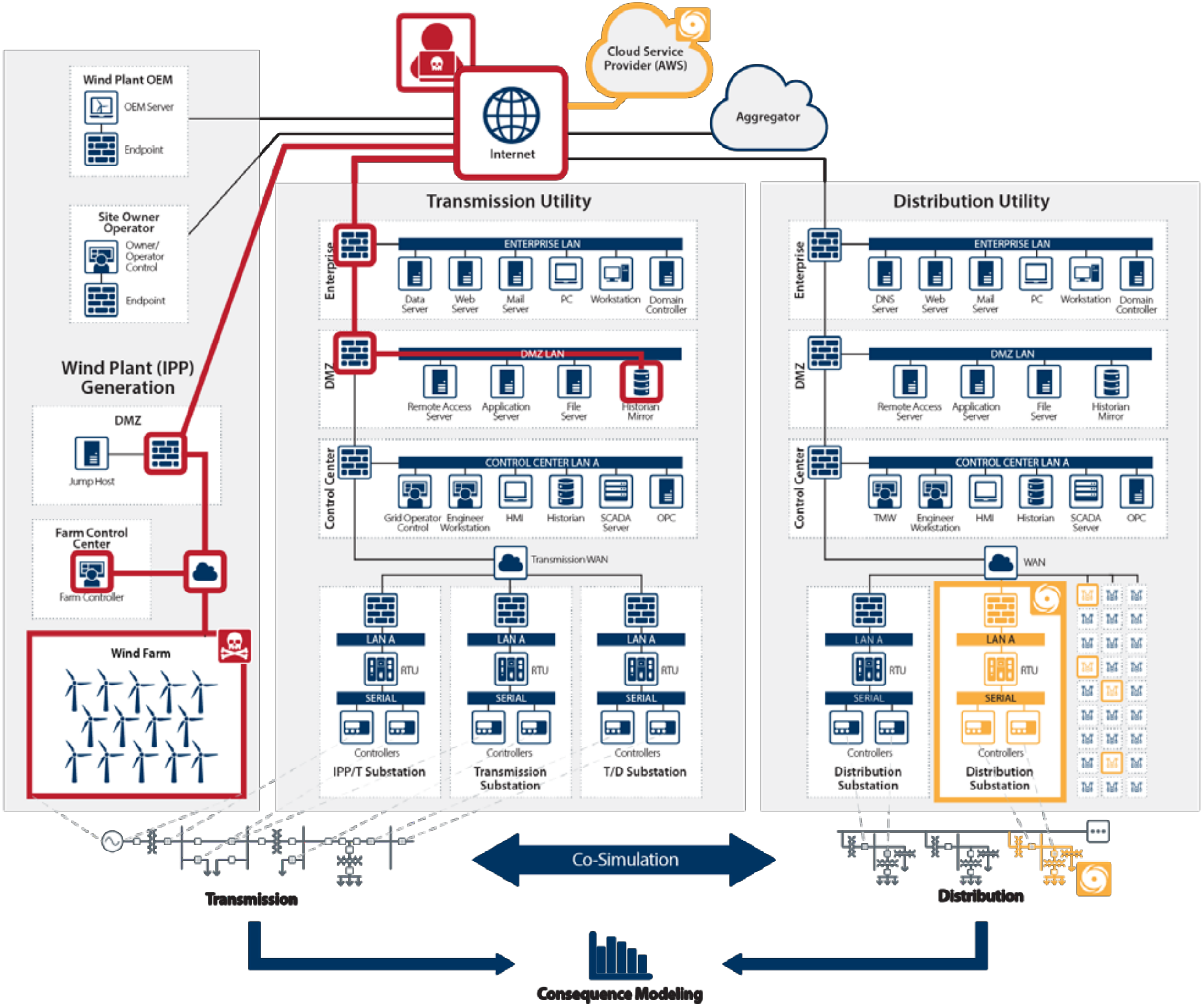
Cyber-Attack on Transmission

Nation State actors and TTPs modeled

Prepositioned access

Pivoting via **living off the land** (LOTL) techniques

CRASHOVERRIDE attack on wind plant

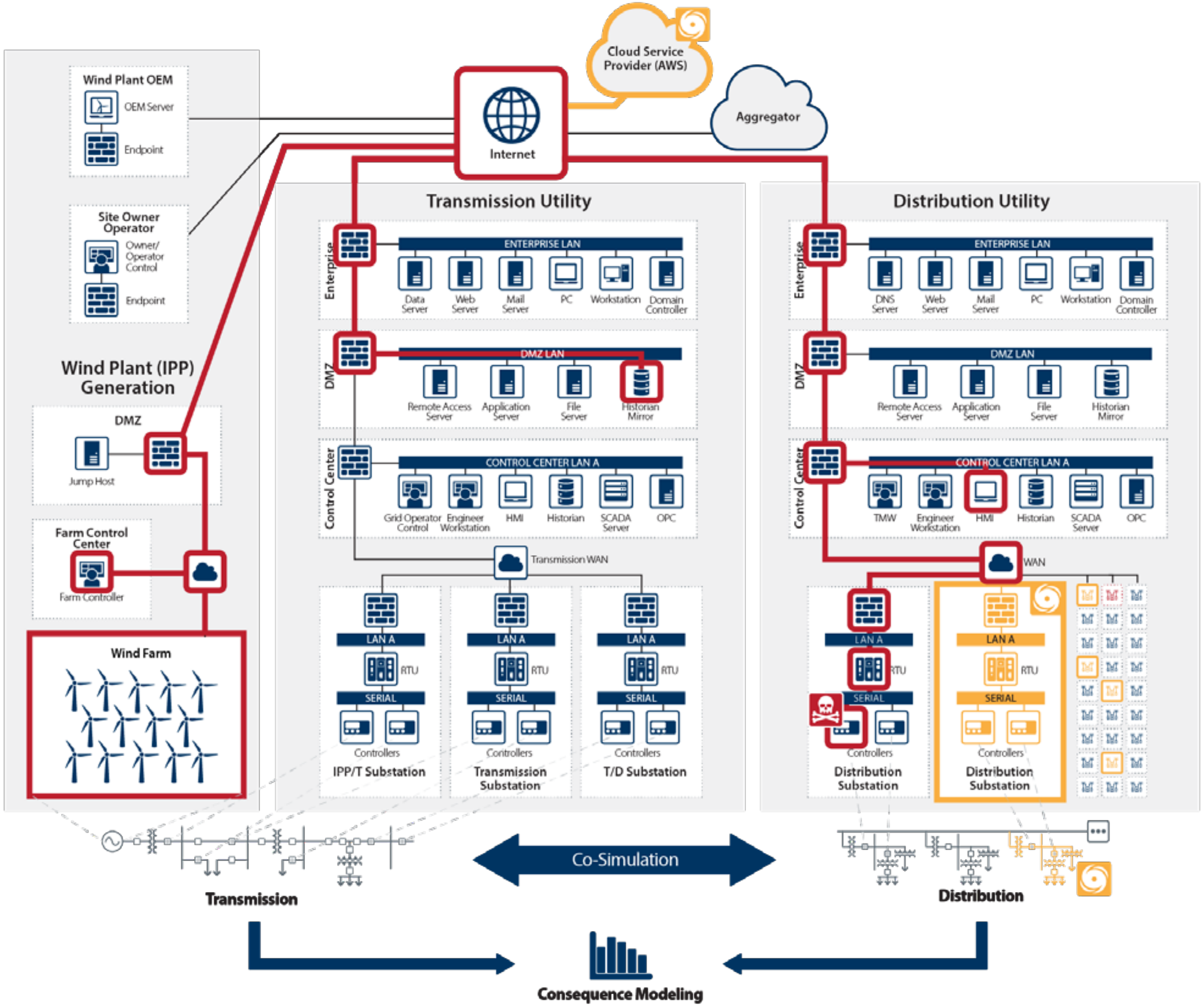


Cyber Threat Details

Cyber-Attack on Distribution

Prepositioned access

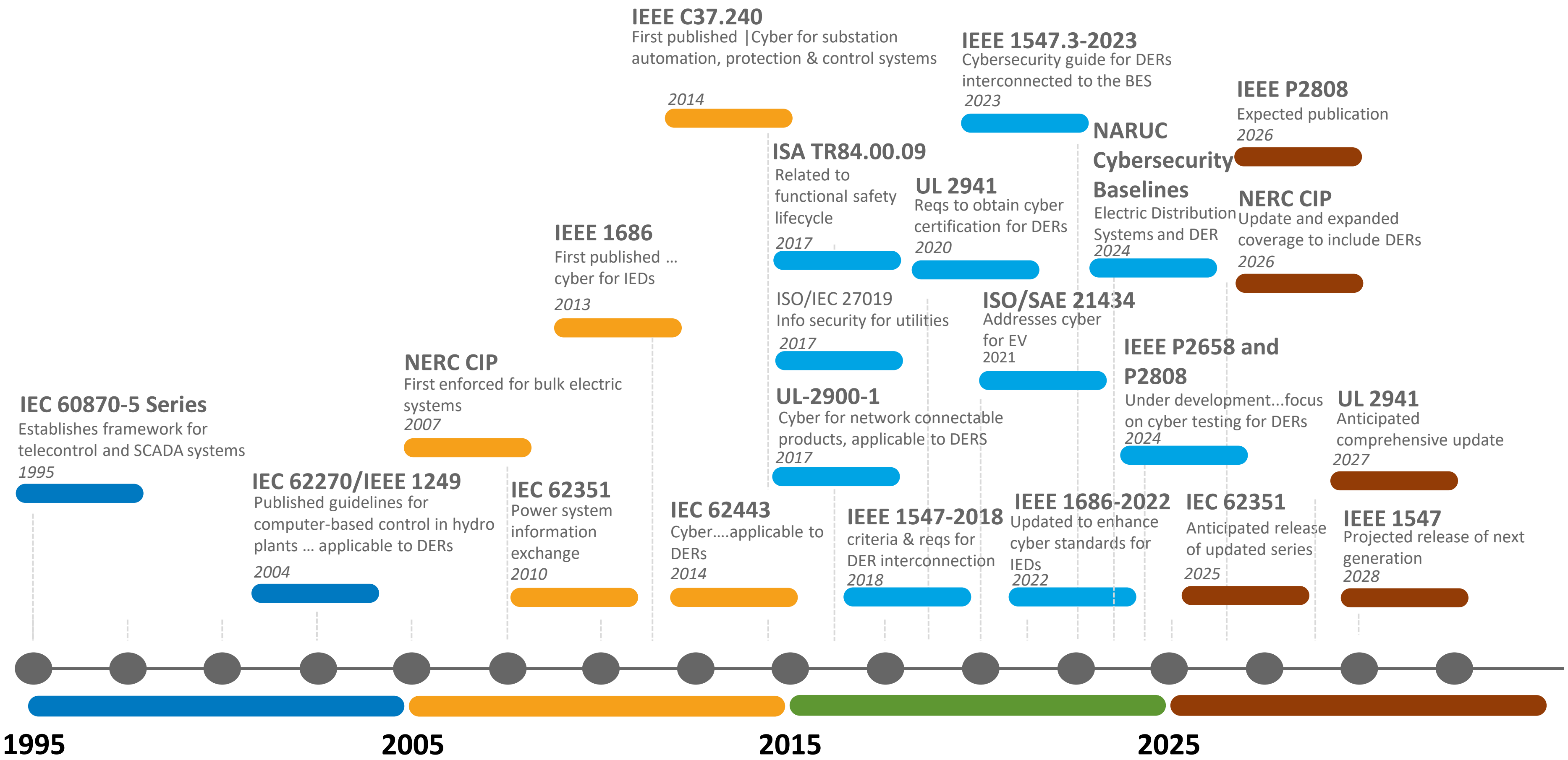
FrostyGoop malware used to affect substation equipment



In this Presentation

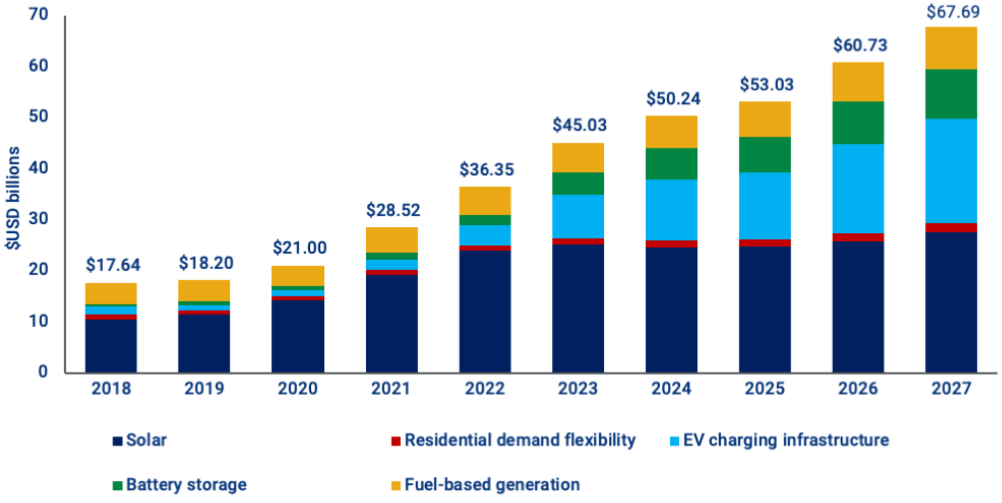
- Introduction
    - A New Frontier
    - Cybersecurity Grand Challenges
    - IBRs vs DERs
- What happens if:
    - Threats and Consequence
    - Simulating Cyber-Attack on Transmission and Distribution Systems
- Security through standards
    - Evolution of Standards
    - Cybersecurity certification and guide
    - Standards library
- Shared responsibility model

Evolution of Standards



Need for Cybersecurity Standards Education

By 2027, the US DER market will likely reach $68 billion per year



Source: Wood Mackenzie Grid Edge US Distributed Solar and Energy Storage Service
https://www.woodmac.com/news/opinion/transformation-distributed-energy-resource-market/

- The growth of DERs necessitates a closer look at cybersecurity standards
- Adoption challenges for newer standards or guides such as IEEE 1547.3-2023 or UL 2941
- Complexity in implementing comprehensive frameworks (e.g., ISA/IEC 62443)
- Diverse DER technologies such as solar, energy storage, wind, EV charging infrastructure, controllable loads, hydrogen fuel cells, etc.
- Integration challenges with legacy systems
- Lack of harmonization between existing standards and/or regulatory requirements

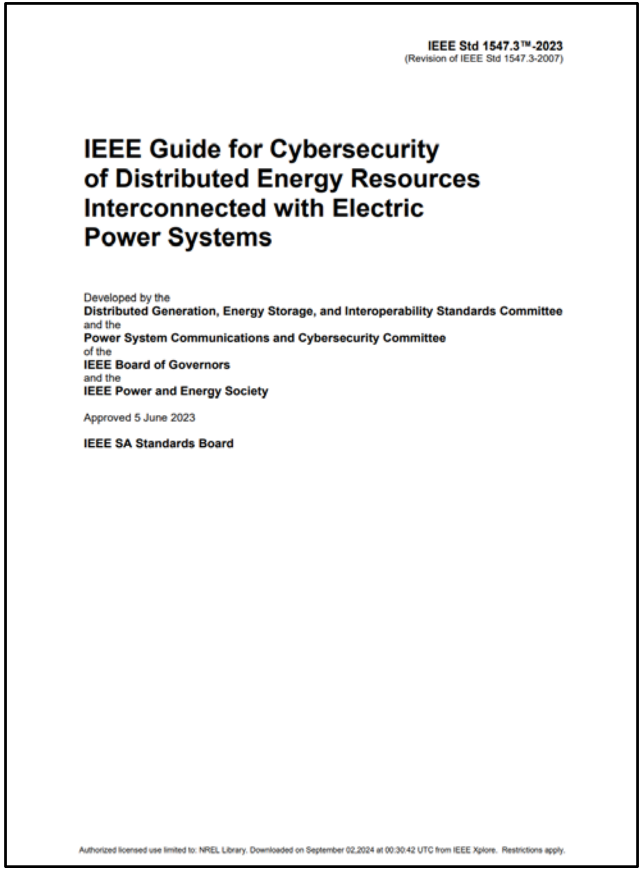
UL 2941: Cybersecurity Certification Standard

IEEE 1547.3: Cybersecurity Guide

P1547 Revision Working Group: Expectations of SG Leads & Facilitator

Proposed Focus of this Revision

- Integrate 2020 amendment
- Fixes from 1547 adoption
- Fixes from UL 1741 SB revisions
- Promote selected P1547.9 guidance to requirements
- Fixes for V2G commissioning procedures (as it pertains to the base 1547 standard and not 1547.1)
- **Promote selected IEEE 1547.3 cybersecurity recommendations to IEEE 1547 standard requirements**
- Add recommended DER settings file format based on EPRI working group recommendations
- Remove barriers for GFM identified by UNIFI et al.


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

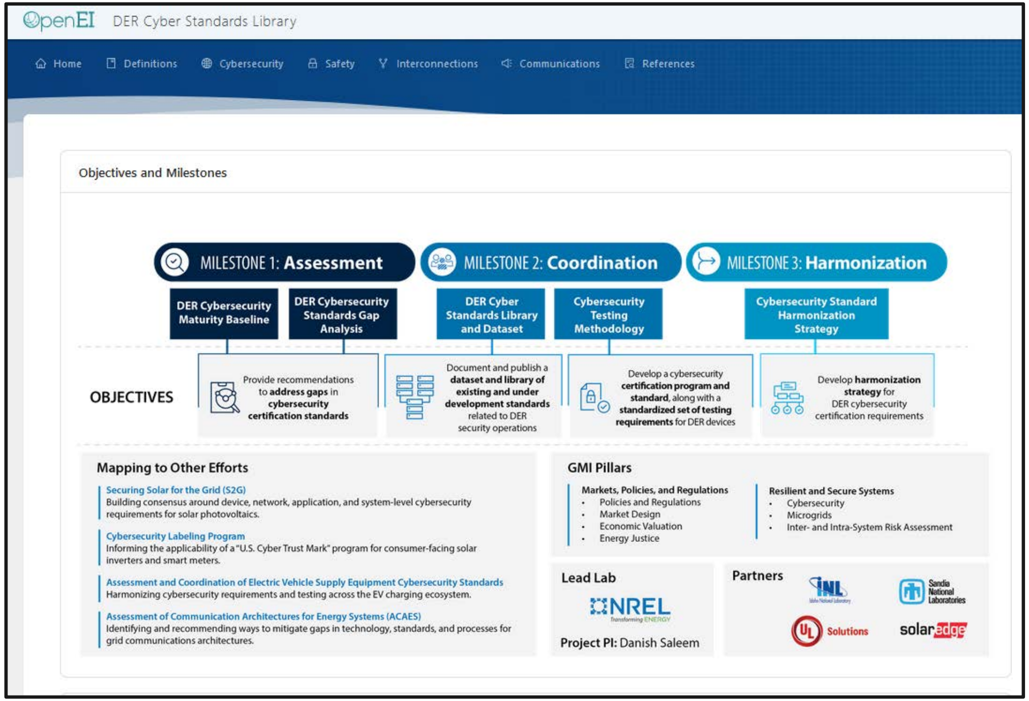
IEEE SA Standards Board

- Published in December 2023
- Passed the ballot and approved by the WG and coordination committee.
- Added to the IEEE 1547 standard revision timeline.

	IEEE 1547.3	UL 2941	IEC 62443
Scope	Cybersecurity, monitoring, information exchange, and control for distributed energy resources (DER) interconnected with electric power systems	Cybersecurity certification for DER devices (e.g., inverters, storage, EV chargers)	Cybersecurity for industrial automation and control systems (IACS), including OT and ICS environments
Industry Focus	Electric power systems, DERs, utilities, aggregators	DER manufacturers, vendors, grid interconnection	Industrial, manufacturing, critical infrastructure, utilities
Framework Type	Guideline for secure interoperability and communication	Testable requirements for device-level cybersecurity	Comprehensive, lifecycle-based, risk-driven standards series
Security Levels	Not explicitly defined; focuses on best practices and controls	Not explicitly defined; focuses on meeting baseline device security	Four defined levels (SL1–SL4), based on threat sophistication and risk
Key Concepts	Secure communication, data integrity, role-based access control, protocol-agnostic	Secure firmware/software, network hardening, vulnerability mitigation	Zones & conduits, defense-in-depth, risk management, shared responsibility, security lifecycle
Certification	No formal certification; implementation is voluntary	Certification required for DER devices (complements UL 1741)	Conformity assessment and product/system certification available
Coverage	All DERs (solar, wind, storage, fuel cells, EVs, etc.) connected to electric grids	DER devices (PV inverters, batteries, wind, EV chargers, etc.)	All automation and control systems, including SCADA, DCS, PLCs, and supporting networks
Approach	System-level guidance for utilities/operators, protocol-agnostic	Device-level requirements for manufacturers and vendors	Risk-based, organizational and technical controls, policies, and procedures

Standards Library

- Provides a comprehensive platform for accessing and managing standards related to DERs.
- Integrates a wide range of guidelines, reports, and documents crucial for maintaining secure, efficient, and effective communication, cybersecurity, and safety within DER systems.
- Designed to support aggregators, VPP owner/operators, installers, utilities, researchers, developers, and other DER industry stakeholders.



https://apps.openei.org/der-cyber-standards/

Key Standards Analyzed

Cybersecurity

- IEC 60870-5 Series
- IEC 62270/IEEE 1249
- IEC 62351
- IEEE 1547.3
- IEEE C37.240
- IEEE P2658
- IEEE P2808
- ISA TR84.00.09
- ISA/IEC 62443
- ISO/IEC 27019:2017
- ISO/SAE 21434:2021
- NERC-CIP
- UL 2900-1
- UL 2941

Safety

- IEC 61400-2:2013
- IEC 62109-1:2010
- IEC 62109-2:2011
- IEC 62109-3:2020
- IEC 62116
- IEE 2030.2-1
- NFPA
- UL 9540

Interconnections

- IEC 61850-7-4
- IEC 61850-8-1
- ANSI/ISA 95
- IEC 61850-8-2
- IEEE 1547-2018
- IEEE 1547.1-2020
- IEEE 1547.2
- IEEE 1547.4
- IEEE 1547.9-2022
- IEEE 1815-2012
- IEEE 1815.2
- IEEE 2030.7
- IEEE P2800
- IEEE P2800.2
- MESA DEV/SPEC
- UL 1741

Communication

- IEC 61850-8-1
- ANSI C12.18/21/22
- ANSI/ASHRAE 135
- BS EN 13757 Fam
- BS EN 50090 Fam
- CAN FD 1.0
- Device Net
- EPSG DS 301
- ETSI – TS 104 001
- FTP
- HTTPS
- IEC 60870-5-101/103/104
- IEC 60870-6
- IEC 61158 Fam
- IEC 61400-25
- IEC 61850 Series
- IEC 61968
- IEC 61970
- IEC 62351
- IEC 62443
- IEC 62746
- IEC TR 61850-7-510
- IEC TR 61859-90-7
- IEC TR 62351-90-3

Communication

- IEEE 1588
- IEEE 1703
- IEEE 1815 (DNP3)
- IEEE 2030.11
- IEEE 2030.5
- IEEE 1547.9
- IEEE P2418.5
- ISO 16484-5
- ISO/IEC 14543-3
- ISO/IEC 14908
- ITU-T G.9903
- ITU-T Y.4480
- MQTT
- MODBUS
- OCPP 2.1
- OPC
- OpenADR
- Profibus
- Profinet
- REST
- RFC 778
- SEPA DERMS
- TCP/IP
- UDP
- Zigbee

DER Testing, Certification, and Commissioning

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

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

What is impact of creating a DER specific cybersecurity certification standard?

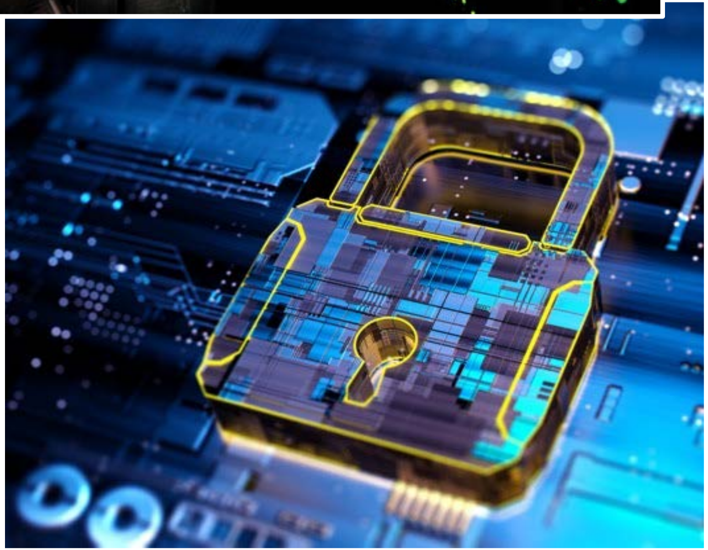
- Ensures DER devices have all five pillars of cybersecurity: confidentiality, integrity, availability, authentication and non-repudiation
- Mandates DER devices pass cybersecurity certification to introduce a minimum level of cybersecurity to the electric grid, to prevent future cyberattacks and strengthen overall electric power system cybersecurity posture
- Creates an environment where the baseline security posture of the DER industry will be elevated

How can utilities support cybersecurity for DERs?

- Support cyber risk mitigation and resiliency
- Support and promote the implementation of best practices and cybersecurity polices with good governance, such as NIST CSF and/or NERC CIP
- Coordinate within state government and across the public-private nexus
- Respond to a cyberattack affecting energy infrastructure through consequence management as part of all-hazards energy assurance
- Contribute and/or actively support the development of DER cybersecurity certification standards and other relevant industry efforts

Recommended General Cybersecurity Policies

1. Isolate internal and external communication from each other.
2. Use of signature and context-based firewalls, gateways, and secured ports to separate the security domains. Consider disabling unused ports and services.
3. Use of authentication to ensure correct identities of personnel, customers, and vendors.
4. Use of Transport Layer Security to ensure encryption, authentication, and data integrity.
5. Use of intrusion detection systems and/or intrusion prevention systems to monitor communication network traffic.
6. Validation of all application software patches and software data updates with roll-back capabilities (if applicable).
7. Use of role-based access control for all communications, human-machine interface, and other places as appropriate.



NOTE: This is not an exhaustive and should not be treated as such

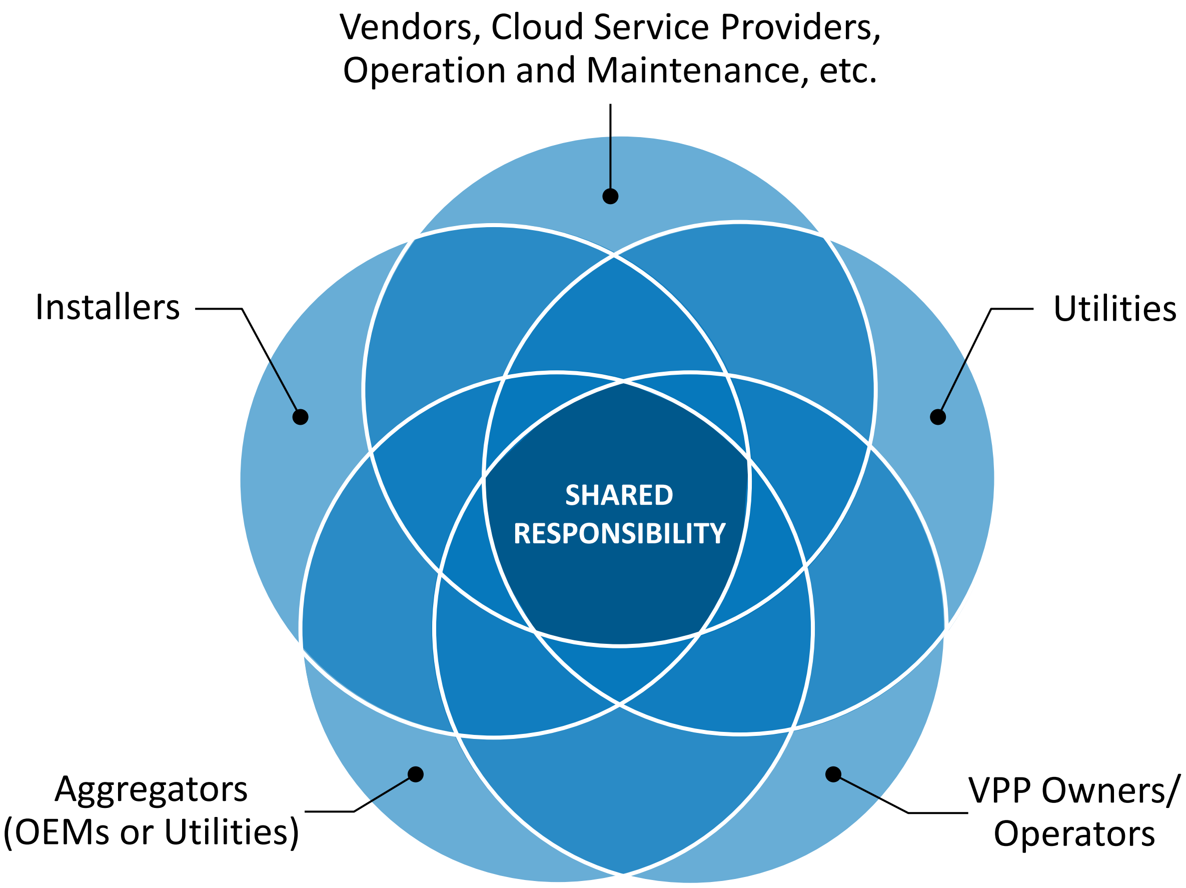
In this Presentation

- Introduction
  - A New Frontier
  - Cybersecurity Grand Challenges
  - IBRs vs DERs
- What happens if:
  - Threats and Consequence
  - Simulating Cyber-Attack on Transmission and Distribution Systems
- Security through standards
  - Evolution of Standards
  - Cybersecurity certification and guide
  - Standards library
- Shared responsibility model

Cybersecurity is a Shared Responsibility

GOALS of COLLABORATION

- Mitigate risks through collective defense.
- Adopt unified cybersecurity controls.
- Enhance grid reliability and resilience.
- Facilitate collaboration and actionable strategies.



Thank You!

NLR/PR-5T00-95917

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 National Renewable Energy Laboratory (NREL). 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.

NREL