

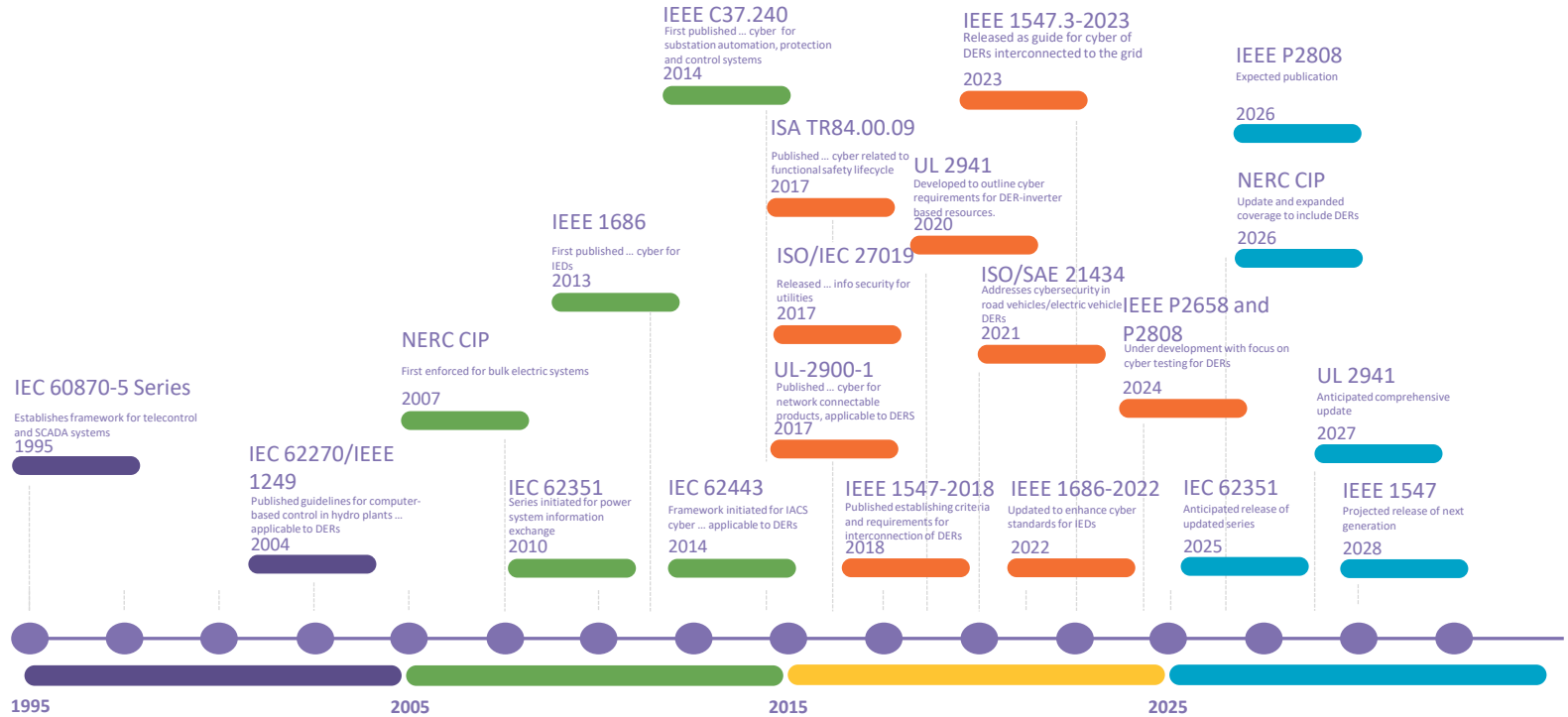
Cybersecurity Standards for Distributed Energy Resources: Gaps and Harmonization Strategy

Charles MaGill
Danish Saleem

January 2025



Evolution of Standards



Why we are here

Growth of Distributed Energy Resources (DERs) from 2018-2027



- The growth of distributed energy resources (DERs) necessitates a closer look at cybersecurity standards
- Task: Conduct a comprehensive gap analysis of existing cybersecurity standards for DERs
- Aim: Identify critical deficiencies and provide actionable recommendations
- Scope: Consider various DER technologies (solar, wind, energy storage, hydrogen fuel cells)
- Importance: Establish robust cybersecurity frameworks for increasingly integrated systems

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



Gaps



Identified Gaps

1. Inadequate coverage of DER-specific cybersecurity challenges
2. Complexity in implementing comprehensive frameworks (e.g., ISA/IEC 62443)
3. Integration challenges with legacy systems
4. Adoption challenges for newer standards (e.g., IEEE 1547.3-2023, UL 2941)
5. Lack of harmonization between standards and regulatory requirements



Gap 1: Inadequate Coverage of DER-Specific Challenges

- Traditional standards were designed for centralized electric systems
- They fail to address:
 - Vulnerability to localized attacks
 - Complexities of securing geographically dispersed systems
 - Bidirectional power flow and communication risks

Technology	Risk	Example	Relative Risk Level
Solar PV Inverters	Data Integrity	-Manipulation of settings to disrupt power or grid stability. -False data injection to mislead grid operators.	High
	Device Control	- Unauthorized control of inverter functions. - Disconnection of inverters from the grid.	High
	Denial of Service	-Flooding inverters with traffic to make unavailable.	Medium
Wind Turbine Controllers	Data Integrity	-Manipulation of parameters (e.g., blade pitch, yaw) to reduce efficiency, cause damage, or disrupt the grid.	High
	Device Control	-Unauthorized access to turbine controls. -Shutting down turbines remotely.	High
	Denial of Service	-Disrupting comms to prevent monitoring and control.	Medium
Energy Storage	Data Integrity	-Falsifying state-of-charge or other battery data. - Manipulating charging/discharging schedules to destabilize the grid or cause financial losses.	High
	Device Control	-Unauthorized control of charging/discharging cycles. -Remotely disabling the ESS.	High
	Denial of Service	-Preventing the ESS from responding to commands.	Medium
Hydrogen	Data Integrity	-Manipulation of fuel cell operating parameters.	Medium
	Device Control	-Unauthorized control of fuel cell output.	Medium
	Denial of Service	-Disrupting communication with fuel cells.	Low/Medium

Source: Thomas, D.-M., A. Sanghvi, M. D. Touhiduzzaman, P. Wand, and T. Reynolds. 2022. NREL Guide to the DER Distributed Energy Resource Risk Management Framework. Golden, CO: NREL. NREL/TP-5R00-81715. <https://www.nrel.gov/docs/fy22osti/81715.pdf>.

Gap 2: Complexity in Implementing Comprehensive Frameworks

- ISA/IEC 62443: Effective but complex for DER systems
- Challenges:
 - Resource-intensive implementation
 - Requires deep technical understanding
 - Difficulty in gaining management support
 - Time-consuming risk assessment process



Gap 3: Integration Challenges With Legacy Systems

- Obsolete protocols and data formats create data silos
- There is a lack of real-time monitoring features
- There is increased vulnerability to attacks
- There is difficulty in complying with current security standards



Gap 4: Adoption Challenges for Newer Standards

- IEEE 1547.3-2023 and UL 2941 are more applicable to DER cybersecurity
- Implementation challenges:
 - Substantial product redesigns are required. This leads to:
 - Increased development costs
 - Extended production timelines
 - Learning curves for industry professionals

Gap 5: Lack of Harmonization

- Fragmented regulatory landscape
- Consequences:
 - Increased compliance burdens
 - Potential security gaps
 - Diverted resources from actual cybersecurity operations
 - Stifled innovation in cybersecurity practices





Harmonization Strategy



Common Goals and Objectives

- Create cohesive DER cybersecurity set of requirements that supports a collective defense
- Ensure the reliable and secure operation of DERs and the electric grid across geographic lines.
- Protect DERs from cyberattacks that could disrupt grid stability, compromise data integrity, or cause physical damage.
- Promote the interoperability of DERs while maintaining cybersecurity.
- Facilitate the secure integration of DERs into various grid architectures and operational environments.
- Protect consumers and their data as a key objective of DER cybersecurity harmonization.






Key Challenges and Barriers

- Varying cybersecurity standards and regulations across different regions and countries.
- Lack of interoperability between different DER technologies and communication protocols.
- Limited resources and expertise for implementing cybersecurity measures, particularly for smaller DER operators.
- Rapid evolution of cyber threats and vulnerabilities, requiring continuous adaptation of security measures.
- Complexities introduced by the involvement of the private sector in DER cybersecurity, including challenges related to international cooperation.

Strategy Execution

- Develop a common set of harmonized cybersecurity requirements and best practices for DERs, drawing from existing standards and frameworks.
- Promote having national DER cybersecurity certification programs to ensure that devices meet minimum security requirements.
- Develop guidelines and training resources to assist DER operators in implementing cybersecurity measures and leverage and promote the library.
- Foster collaboration, outreach and information sharing among stakeholders, including government agencies, industry groups, and research institutions.

Key Stakeholders and Roles

Stakeholder	Role	Examples
 Government Agencies (DOE, CISA, NIST)	Develop and promote cybersecurity standards and policies, provide guidance and resources, and facilitate collaboration.	The DOE funds research on DER cybersecurity and develops cybersecurity guidelines for utilities. CISA provides vulnerability assessments and incident response services. NIST develops cybersecurity frameworks and standards.
 Industry Groups (IEEE, SunSpec Alliance, SEPA)	Develop industry-specific standards and best practices, conduct research, and provide training and education.	The IEEE develops standards for DER interconnection and cybersecurity. The SunSpec Alliance promotes interoperability and security for solar and storage technologies. SEPA provides education and resources on DER cybersecurity best practices.
 DER Operators and Utilities	Implement cybersecurity measures, comply with standards and regulations, and participate in information sharing.	DER operators implement access controls, intrusion detection systems, and security monitoring. Utilities conduct risk assessments and develop incident response plans.
 DER Manufacturers and Vendors	Design and develop secure DER technologies, comply with cybersecurity standards, and provide security updates and support.	Manufacturers incorporate security features into DER devices and conduct vulnerability testing. Vendors provide security patches and updates to address identified vulnerabilities.
 Research Institutions (INL, NREL, Sandia National Laboratories)	Conduct research on DER cybersecurity, develop testing and evaluation methodologies, and provide technical expertise.	National Labs conduct research on DER cybersecurity and develops tools for assessing cybersecurity posture. Additionally, National Labs conduct vulnerability analysis and develops security solutions for DERs.

Roadmap for Execution

- **Phase 1:**
 - Strengthen working group with representatives from key stakeholders.
 - Develop a harmonized set of cybersecurity requirements and best practices for DERs.
 - Finalize and socialize gap analysis and DER standards library and identify areas for harmonization.
- **Phase 2:**
 - Continue socializing gap analysis and DER standards library and identify areas for harmonization.
 - Socialize DER cybersecurity certification program and testing procedures.
 - Create guidelines and training resources for DER operators.
 - Pilot test the harmonized standards and certification program with select DER operators.
- **Phase 3:**
 - Refine the harmonized standards and certification program based on pilot test results.
 - Promote the widespread adoption of the harmonized standards and certification program.
 - Establish a mechanism for ongoing monitoring and evaluation of DER cybersecurity.



Library



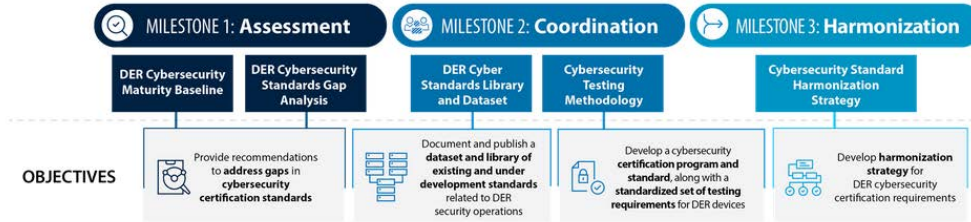
Library

Home Link

OpenEI DER Cyber Standards Library

Home Definitions Cybersecurity Safety Interconnections Communications References

Objectives and Milestones



Mapping to Other Efforts

Securing Solar for the Grid (S2G)
Building consensus around device, network, application, and system-level cybersecurity requirements for solar photovoltaics.

Cybersecurity Labeling Program
Informing the applicability of a "U.S. Cyber Trust Mark" program for consumer-facing solar inverters and smart meters.

Assessment and Coordination of Electric Vehicle Supply Equipment Cybersecurity Standards
Harmonizing cybersecurity requirements and testing across the EV charging ecosystem.

Assessment of Communication Architectures for Energy Systems (ACAES)
Identifying and recommending ways to mitigate gaps in technology, standards, and processes for grid communications architectures.

GMI Pillars

Markets, Policies, and Regulations

- Policies and Regulations
- Market Design
- Economic Valuation
- Energy Justice

Resilient and Secure Systems

- Cybersecurity
- Microgrids
- Inter- and Intra-System Risk Assessment

Lead Lab



Project PI: Danish Saleem

Partners



- Designed to support researchers and developers by providing a comprehensive platform for accessing and managing standards related to DERs.
- Integrates a vast collection of guidelines, reports, and documentation that are essential for ensuring secure, efficient, and effective communication, cybersecurity, and safety in DER systems

THANK YOU

Charlie MaGill

charles.magill@nrel.gov

864-901-2646

NREL/PR-5T00-92844

This work was authored by NREL for the U.S. Department of Energy (DOE), operated under Contract No. DE-AC36-08GO28308. Funding provided by U.S. Department of Energy Office of Cybersecurity, Energy Security, and Emergency Response. 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.



SHAPE THE GRID EDGE

