



# Path Toward Cybersecurity Standards for Solar PV and Other DERs

Danish Saleem

Cybersecurity Systems Researcher

UL/NREL Cybersecurity Overview of Standards  
and Protocols for CPUC & CA IOUs

01/14/2021

Energy systems across the globe are changing.

Advancements in future systems are needed to ensure the safety, reliability, security, and resilience of those systems.

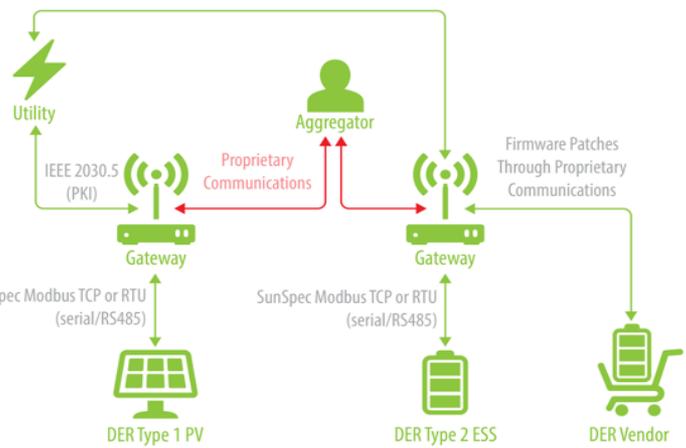
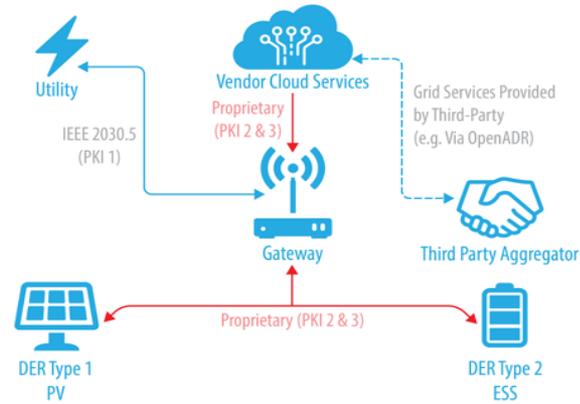
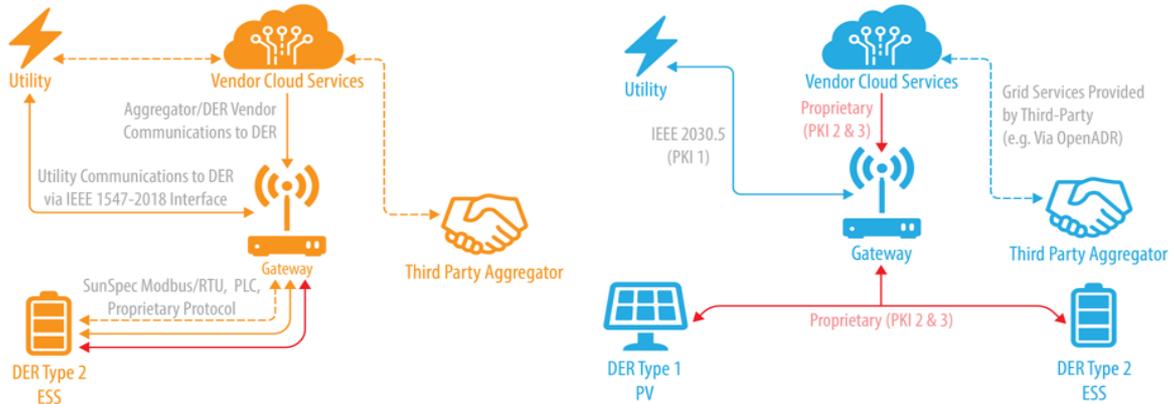


# Grid Security and Reliability Must Keep Pace



To manage, optimize, and secure the future grid, new technologies and control techniques will be required that don't currently exist.

# What Future Distributed Energy Resource (DER) Systems Might Look Like



- ← Proprietary Communications
- ← Wired Communications
- ← Wireless Communications
- ESS Energy Storage Systems
- PV Photovoltaic System
- DER Distributed Energy Resource
- PKI Public Key Infrastructure
- OpenADR Open Automated Demand Response
- PLC Programmable Logic Controller

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

Cybersecurity Information Sharing Act of 2015. S. 754, 114<sup>th</sup> Congress (2015).

# Cybersecurity Standards Initiatives

- IEEE 1547.3 Working Group
  - Provides guidelines for cybersecurity for DERs interconnected with the electric power system
- SunSpec/Sandia National Laboratories working group
  - Six subgroups, each led by different organization
- National Renewable Energy Laboratory/Underwriters Laboratories partnership for establishing certification standards for DERs
- National Association of Regulatory Utility Commissioners and National Association of State Energy Officials partnering with industry to establish cybersecurity advisory team for state solar (CATSS)
- Laboratory Coordination Committee (LCC)



### Certification Procedures for Data and Communications Security of Distributed Energy Resources

Danish Saleem<sup>1</sup> and Cedric Carter<sup>2</sup>

<sup>1</sup> National Renewable Energy Laboratory  
<sup>2</sup> The MITRE Corporation



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  
Contract No. DE-AC36-09OR22499

Technical Report  
NREL/TP-5800-7326  
July 2019



### EPRI SECURITY ARCHITECTURE FOR THE DISTRIBUTED ENERGY RESOURCES INTEGRATION NETWORK

#### RISK-BASED APPROACH FOR NETWORK DESIGN

**EXECUTIVE SUMMARY**

As distributed energy resources (DERs) expand rapidly as a major source of electricity generation and transmission with the grid, the ability to securely monitor and control the operation of the resources to help grid operators and utilities increasingly important to maintain safety, reliability and efficiency of the national grid. Research, development and control of distributed generation require local devices and secure communication protocols, secure and secure connections from the power system, to public or private communication networks. In the meantime, the cyberattacks against the national grid is becoming an area of major concern because intelligence and control. Without adequate cybersecurity protection, energy generation and transmission systems are heavily exposed to cyber threats.

This paper provides a practical set of cybersecurity requirements pertaining to the network components supporting distributed energy resources (DER) communications. The requirements specified herein aim to reduce the cybersecurity risk to the distributed grid in which various DER are connected. The requirements discussed herein do not make any assumption to the communication protocols, particular functional standards, or secure communication methods in terms of their effectiveness in cybersecurity. Further, it is not possible to define the view of the interconnected system, including DER, and it is suggested that they can be provided from cybersecurity.

The scope of this report is limited to network security concerns. The grid is a possible guideline for designing and implementing network infrastructure to help the grid adhere to the National Electrical Security Institute (NESI) standards.

It is important to note that network security solutions address only a portion of the cybersecurity risks associated with DER integration. To protect DER and the connected grid adequately, a more comprehensive cybersecurity strategy needs to be developed and implemented.

**THE RISK-BASED APPROACH FOR NETWORK DESIGN**

The risk-based approach consists of the following:

- DER supporting system, supporting system, or system.
- A system, application, or device used to support the operation of DER in grid services is vulnerable to DER.
- DER supporting system or supporting system. A supporting system specifically used to manage DER. The essential functions of a DER managing system include data acquisition and control.
- Essential network. A sub-communication network that connects critical data to the DER network (EDN), between one network (EDN) or cloud, or the Internet.
- Security. One or more devices or hardware devices where a device in a secure connection with other devices within the same facility has access to and from devices outside the same is considered.

**NETWORK SECURITY REQUIREMENTS**

The general network security requirements described in this section are drawn from various cybersecurity standards available to the industry [1-14].

### IEEE 1547.3

Type of Project: New IEEE  
Standard PAR Request Date:

PAR Approval Date:  
PAR Expiration Date:  
Status: Not approved

11 Project Number: 1547.3  
12 Type of Document: Guide  
13 Life Cycle: Full Use

21 Title: Guide for Cybersecurity of Distributed Energy Resources Interfaces with Associated Electric Power Systems

31 Working Group:

35 Sponsoring Society and Committee: IEEE-SA8B Coordinating Committee SCC21 - Fuel Cells, Photovoltaics, Dispersed Generation, and Energy Storage (SA8B SCC21)

Contact Information for Sponsor  
Chair Name: Janette Sandberg  
Email Address: janette.sandberg@ieee.org  
Phone: 505.612.1519  
Contact Information for Standards Representative  
Michael Kipness

41 Type of Ballot: Individual  
42 Expected Date of submission of draft to the IEEE-SA for Initial Sponsor Ballot: 07/2021  
43 Projected Completion Date for Submittal to RevCom 12/2021  
Note: Usual minimum time between initial sponsor ballot and submission to RevCom is 6 months.

44 Approximate number of people expected to be actively involved in the development of this project: 40  
45 Scope: This document provides guidelines for Cybersecurity of Distributed Energy Resources (DER) interfaces with the Electric Power Systems (EPS).

51 In the completion of this standard dependent upon the completion of another standard:  
52 Purpose: This document provides guidelines for cybersecurity for one or more distributed resources that are interconnected with electric power systems. DER include systems in the areas of fuel cells, photovoltaics, wind turbines, microturbines, other distributed energy sources, and distributed energy storage systems. The revision will focus on updating the guidelines on mitigating cybersecurity risks at the individual DER device level that may be introduced by enabling communication capability at the DER interface, by utilizing the resources and standards that have been developed in the past 10 years.



### SANDIA REPORT

SAND2019-1490  
Unlimited Release  
Printed February 2019

## Recommendations for Data-in-Transit Requirements for Securing DER Communications

Reema Ounakao

This work is primarily under IEEE office review for approval and should not be disseminated outside the working group used a final version has been authorized for release.

Prepared by  
Sandia National Laboratories  
Albuquerque, New Mexico  
87185-1500  
California 94550



### SANDIA REPORT

SAND2019-1490  
Unlimited Release  
Printed February 2019

## Recommendations for Trust and Encryption in DER Interoperability Standards

James Oberl, Patricia Cordeiro, Jay Johnson, Gordon Lum, Tom Tansy, Max Pala, Ronald H.

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

Sandia National Laboratories is a multi-program 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 number DE-NA0003525.

# Cybersecurity Advisory Team for State Solar

- What are the key challenges of PV solar and/or DER cybersecurity?
- Why have these challenges not been addressed to date?
- What would be the ideal solution for addressing solar cybersecurity challenges at the state level?
- What role should state energy officials, public utility commissions, manufacturers, electric utilities, certification labs and standard development organizations take on to address these challenges?



# Relevant Standards and Guides

- **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:** SEP2—Smart Energy Profile 2.0
- **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 (ES-C2M2)
- **DOE/NIST/NERC RMP:** Electricity Subsector Cybersecurity Risk Management Process Guideline
- **IEEE 1547.3:** Guide for Cybersecurity of DERs Interconnected with Electric Power Systems
- **Potential new UL/ISA Standard:** Cybersecurity Certification Standard for DERs

# Basic Cybersecurity Principles

- Recent FERC order 2222 enables DERs to participate alongside traditional resources in regional organized wholesale markets through aggregations.
- The need is to develop intrinsic security design principles for the future grid—a grid that can operate autonomously, with millions of advanced grid devices to support high penetrations of distributed energy resources.
- Future research should focus on how to integrate high penetration levels of DERs seamlessly onto the grid in a secure and reliably manner.

1

**Incorporate security at the design level.**

2

**Advance security updates and vulnerability management.**

3

**Build on proven security measures.**

4

**Prioritize security measures according to potential impact.**

5

**Promote transparency across grid.**

6

**Connect carefully and deliberately.**

# Thank you

---

[www.nrel.gov](http://www.nrel.gov)

**Danish Saleem**

[danish.saleem@nrel.gov](mailto:danish.saleem@nrel.gov) | 720-404-5912

NREL/PR-5R00-78768

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.

