IEEE SA
STANDARDS ASSOCIATION

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

STANDARDS

IEEE Board of Governors
and the
IEEE Power and Energy Society

Developed by the
Distributed Generation, Energy Storage, and Interoperability Standards Committee
and the
Power System Communications and Cybersecurity Committee

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



IEEE

AVA Documents
Document Sharing Hub

Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 18:54:43 UTC from IEEE Xplore. Restrictions apply.

Full document details: IEEE 1547.3-2023

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

Documents
Document Sharing Hub

Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 18:54:43 UTC from IEEE Xplore. Restrictions apply.

Full document details: IEEE 1547.3-2023

THIS IS A REDLINE DOCUMENT PRODUCED BY TECHSTREET, AN ASME COMPANY.

This document is intended to provide users with an indication of changes from one edition to the next. It includes a full-text version of the new document, plus an indication of changes from the previous version.

Redlines are designed to save time and improve efficiencies by using the latest software technology to find and highlight document changes. More professionals are using valuable new technologies like redlines, to help improve outcomes in a fast paced global business world.

Because it may not be technically possible to capture all changes accurately, it is recommended that users consult previous editions as appropriate. In all cases, only the current base version of this publication is to be considered the official document.

This Redline is produced solely by Techstreet. IEEE has not prepared this Redline and is not responsible for its accuracy.

445 Hoes Lane, Piscataway, NJ 08854 USA | http://standards.ieee.org | Tel. +1 732-981-0060 Fax +1 732-562-1571
Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 18:54:43 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1547.3-2023

Redline Processing Notes:

1. ~~**Red Text**~~ - Red strikethrough text denotes deletions.

2. **Blue Text** - Blue underlined text denotes modifications and additions.

Documents
Document Sharing Hub

Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 18:54:43 UTC from IEEE Xplore. Restrictions apply.

Full document details: IEEE 1547.3-2023

Abstract: Guidelines for cybersecurity of distributed energy resources (DER) interconnection with electric power systems (EPS) are provided in this guide.

Keywords: cybersecurity, certification, clearing time, codes, commissioning, communications, dc injection, design, diesel generators, dispersed generation, distributed generation, electric distribution systems, electric power systems, energy resources, energy storage, faults, field, flicker, frequency support, fuel cells, generators, grid, grid support, harmonics, IEEE 1547™, induction machines, installation, interconnection requirements and specifications, interoperability, inverters, islanding, microturbines, monitoring and control, networks, paralleling, performance, photovoltaic power systems, point of common coupling, power converters, production tests, quality, power, protection functions, public utility commissions, reclosing coordination, regulations, ride through, rule-making, standards, storage, synchronous machines, testing, trip setting, utilities, voltage regulation, wind energy systems

The Institute of Electrical and Electronics Engineers, Inc.
3 Park Avenue, New York, NY 10016-5997, USA

Copyright © 2023 by The Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 11 December 2023. Printed in the United States of America.

IEEE is a registered trademark in the U.S. Patent & Trademark Office, owned by The Institute of Electrical and Electronics Engineers, Incorporated.

"Modbus" is a registered trademark of Schneider Electric USA, Inc.

PDF: ISBN 979-8-8557-0285-9 STD26596
Print: ISBN 979-8-8557-0286-6 STDPD26596

IEEE prohibits discrimination, harassment, and bullying.
For more information, visit https://www.ieee.org/about/corporate/governance/p9-26.html.
No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher.

Copyright © 2023 IEEE. All rights reserved.

Documents
Document Sharing Hub

Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 18:54:43 UTC from IEEE Xplore. Restrictions apply.

Full document details: IEEE 1547.3-2023

Important Notices and Disclaimers Concerning IEEE Standards Documents

IEEE Standards documents are made available for use subject to important notices and legal disclaimers. These notices and disclaimers, or a reference to this page (https://standards.ieee.org/ipr/disclaimers.html), appear in all standards and may be found under the heading "Important Notices and Disclaimers Concerning IEEE Standards Documents."

Notice and Disclaimer of Liability Concerning the Use of IEEE Standards Documents

IEEE Standards documents are developed within IEEE Societies and subcommittees of IEEE Standards Association (IEEE SA) Board of Governors. IEEE develops its standards through an accredited consensus development process, which brings together volunteers representing varied viewpoints and interests to achieve the final product. IEEE standards are documents developed by volunteers with scientific, academic, and industry-based expertise in technical working groups. Volunteers are not necessarily members of IEEE or IEEE SA and participate without compensation from IEEE. While IEEE administers the process and establishes rules to promote fairness in the consensus development process, IEEE does not independently evaluate, test, or verify the accuracy of any of the information or the soundness of any judgments contained in its standards.

IEEE makes no warranties or representations concerning its standards, and expressly disclaims all warranties, express or implied, concerning this standard, including but not limited to the warranties of merchantability, fitness for a particular purpose and non-infringement IEEE Standards documents do not guarantee safety, security, health, or environmental protection, or guarantee against interference with or from other devices or networks. In addition, IEEE does not warrant or represent that the use of the material contained in its standards is free from patent infringement. IEEE Standards documents are supplied "AS IS" and "WITH ALL FAULTS."

Use of an IEEE standard is wholly voluntary. The existence of an IEEE standard does not imply that there are no other ways to produce, test, measure, purchase, market, or provide other goods and services related to the scope of the IEEE standard. Furthermore, the viewpoint expressed at the time a standard is approved and issued is subject to change brought about through developments in the state of the art and comments received from users of the standard.

In publishing and making its standards available, IEEE is not suggesting or rendering professional or other services for, or on behalf of, any person or entity, nor is IEEE undertaking to perform any duty owed by any other person or entity to another. Any person utilizing any IEEE Standards document, should rely upon their own independent judgment in the exercise of reasonable care in any given circumstances or, as appropriate, seek the advice of a competent professional in determining the appropriateness of a given IEEE standard.

IN NO EVENT SHALL IEEE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO: THE NEED TO PROCURE SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE PUBLICATION, USE OF, OR RELIANCE UPON ANY STANDARD, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE AND REGARDLESS OF WHETHER SUCH DAMAGE WAS FORESEEABLE.

Copyright © 2023 IEEE. All rights reserved.
Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 18:54:43 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1547.3-2023

Translations

The IEEE consensus balloting process involves the review of documents in English only. In the event that an IEEE standard is translated, only the English version published by IEEE is the approved IEEE standard.

Official statements

A statement, written or oral, that is not processed in accordance with the IEEE SA Standards Board Operations Manual shall not be considered or inferred to be the official position of IEEE or any of its committees and shall not be considered to be, nor be relied upon as, a formal position of IEEE. At lectures, symposia, seminars, or educational courses, an individual presenting information on IEEE standards shall make it clear that the presenter's views should be considered the personal views of that individual rather than the formal position of IEEE, IEEE SA, the Standards Committee, or the Working Group. Statements made by volunteers may not represent the formal position of their employer(s) or affiliation(s).

Comments on standards

Comments for revision of IEEE Standards documents are welcome from any interested party, regardless of membership affiliation with IEEE or IEEE SA. However, **IEEE does not provide interpretations, consulting information, or advice pertaining to IEEE Standards documents**.

Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Since IEEE standards represent a consensus of concerned interests, it is important that any responses to comments and questions also receive the concurrence of a balance of interests. For this reason, IEEE and the members of its Societies and subcommittees of the IEEE SA Board of Governors are not able to provide an instant response to comments, or questions except in those cases where the matter has previously been addressed. For the same reason, IEEE does not respond to interpretation requests. Any person who would like to participate in evaluating comments or in revisions to an IEEE standard is welcome to join the relevant IEEE working group. You can indicate interest in a working group using the Interests tab in the Manage Profile & Interests area of the IEEE SA myProject system.[1] An IEEE Account is needed to access the application.

Comments on standards should be submitted using the Contact Us form.[2]

Laws and regulations

Users of IEEE Standards documents should consult all applicable laws and regulations. Compliance with the provisions of any IEEE Standards document does not constitute compliance to any applicable regulatory requirements. Implementers of the standard are responsible for observing or referring to the applicable regulatory requirements. IEEE does not, by the publication of its standards, intend to urge action that is not in compliance with applicable laws, and these documents may not be construed as doing so.

[1] Available at: https://development.standards.ieee.org/myproject-web/public/view.html#landing.
[2] Available at: https://standards.ieee.org/content/ieee-standards/en/about/contact/index.html.

Copyright © 2023 IEEE. All rights reserved.
Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 18:54:43 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1547.3-2023

Data privacy

Users of IEEE Standards documents should evaluate the standards for considerations of data privacy and data ownership in the context of assessing and using the standards in compliance with applicable laws and regulations.

Copyrights

IEEE draft and approved standards are copyrighted by IEEE under U.S. and international copyright laws. They are made available by IEEE and are adopted for a wide variety of both public and private uses. These include both use, by reference, in laws and regulations, and use in private self-regulation, standardization, and the promotion of engineering practices and methods. By making these documents available for use and adoption by public authorities and private users, neither IEEE nor its licensors waive any rights in copyright to the documents.

Photocopies

Subject to payment of the appropriate licensing fees, IEEE will grant users a limited, non-exclusive license to photocopy portions of any individual standard for company or organizational internal use or individual, non-commercial use only. To arrange for payment of licensing fees, please contact Copyright Clearance Center, Customer Service, 222 Rosewood Drive, Danvers, MA 01923 USA; +1 978 750 8400; https://www.copyright.com/. Permission to photocopy portions of any individual standard for educational classroom use can also be obtained through the Copyright Clearance Center.

Updating of IEEE Standards documents

Users of IEEE Standards documents should be aware that these documents may be superseded at any time by the issuance of new editions or may be amended from time to time through the issuance of amendments, corrigenda, or errata. An official IEEE document at any point in time consists of the current edition of the document together with any amendments, corrigenda, or errata then in effect.

Every IEEE standard is subjected to review at least every 10 years. When a document is more than 10 years old and has not undergone a revision process, it is reasonable to conclude that its contents, although still of some value, do not wholly reflect the present state of the art. Users are cautioned to check to determine that they have the latest edition of any IEEE standard.

In order to determine whether a given document is the current edition and whether it has been amended through the issuance of amendments, corrigenda, or errata, visit IEEE Xplore or contact IEEE.[3] For more information about the IEEE SA or IEEE's standards development process, visit the IEEE SA Website.

Errata

Errata, if any, for all IEEE standards can be accessed on the IEEE SA Website.[4] Search for standard number and year of approval to access the web page of the published standard. Errata links are located under the Additional Resources Details section. Errata are also available in IEEE Xplore. Users are encouraged to periodically check for errata.

[3] Available at: https://ieeexplore.ieee.org/browse/standards/collection/ieee.
[4] Available at: https://standards.ieee.org/standard/index.html.

Copyright © 2023 IEEE. All rights reserved.
Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 18:54:43 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1547.3-2023

Patents

IEEE standards are developed in compliance with the IEEE SA Patent Policy.[5]

Attention is called to the possibility that implementation of this standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken by the IEEE with respect to the existence or validity of any patent rights in connection therewith. If a patent holder or patent applicant has filed a statement of assurance via an Accepted Letter of Assurance, then the statement is listed on the IEEE SA Website at https://standards.ieee.org/about/sasb/patcom/patents.html. Letters of Assurance may indicate whether the Submitter is willing or unwilling to grant licenses under patent rights without compensation or under reasonable rates, with reasonable terms and conditions that are demonstrably free of any unfair discrimination to applicants desiring to obtain such licenses.

Essential Patent Claims may exist for which a Letter of Assurance has not been received. The IEEE is not responsible for identifying Essential Patent Claims for which a license may be required, for conducting inquiries into the legal validity or scope of Patents Claims, or determining whether any licensing terms or conditions provided in connection with submission of a Letter of Assurance, if any, or in any licensing agreements are reasonable or non-discriminatory. Users of this standard are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. Further information may be obtained from the IEEE Standards Association.

IMPORTANT NOTICE

Technologies, application of technologies, and recommended procedures in various industries evolve over time. The IEEE standards development process allows participants to review developments in industries, technologies, and practices, and to determine what, if any, updates should be made to the IEEE standard. During this evolution, the technologies and recommendations in IEEE standards may be implemented in ways not foreseen during the standard's development. IEEE standards development activities consider research and information presented to the standards development group in developing any safety recommendations. Other information about safety practices, changes in technology or technology implementation, or impact by peripheral systems also may be pertinent to safety considerations during implementation of the standard. Implementers and users of IEEE Standards documents are responsible for determining and complying with all appropriate safety, security, environmental, health, and interference protection practices and all applicable laws and regulations.

[5] Available at: https://standards.ieee.org/about/sasb/patcom/materials.html.

Copyright © 2023 IEEE. All rights reserved.
Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 18:54:43 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1547.3-2023

Participants

At the time this guide was completed, the 1547.3 Working Group had the following membership:

Anthony Johnson and **Janette Sandberg**, *Chairs*
Benjamin Kazimier and **Danish Saleem**, *Vice Chairs*
Frances Cleveland, *Secretary*

Marelo Algrain
Hauker Asgeirsson
Robert Bridges
Ken Brunkenhoefer
Sean Carr
Nancy Connelly
Ryan Davidson
Mamadou Diong
Benjamin Ealey
Antti Eerola
Robert Fox
Hailegebriel Gashaw
Greg Hasler
Nelson Hastings
Jay Johnson
Yashar Kenarangui
Paul Krell
Brian Lydic
James Mater
Thomas McDermott
Lyman Morikawa
Paul Pierce
Jordan Peterson
Michael Ropp
Kirk Rosener
Nachum Sadan
David Sanchez
Joesph Schaefer
Ronald Shipman
Mark Siira
Mark Smith
Gary Smullin
Wayne Stec
Adam Todorski
Stephen Wurmlinger

The following members of the individual Standards Association balloting group voted on this guide. Balloters may have voted for approval, disapproval, or abstention.

Steven Alexanderson
Mark Baldassari
Gilles Bargone
Paul Barnhart
Thomas Basso
Sebastien Billaut
Sara Biyabani
Thomas Blair
Jens Boemer
James Bougie
Gustavo Brunello
Ted Burse
William Byrd
John Calvin
Paul Cardinal
Sean Carr
Richard Carter
Pin Chang
Ke Chen
Nancy Chilton
Ritwik Chowdhury
Frances Cleveland
Nancy Connelly
Stephen Conrad
Michael Cowan
Ratan Das
Ryan Davidson
Mamadou Diong
Michael Dood
Neal Dowling
Michael Doyle
Ernest Duckworth
Donald Dunn
Benjamin Ealey
Christian Eder
Zakia El Omari
Kevin Fellhoelter
Rafael Garcia
Kamal Garg
Shubhanker Garg
Hailegebriel Gashaw
Jonathan Gay
Michael Geocaris
Jalal Gohari
Sigifredo Gonzalez
Randy Hamilton
Jerry Harness
Kyle Hawkings
Mariana Hentea
David Herrell
Alan Hetzel
Werner Hoelzl
Anderson Hoke
Ali Hooshyar
Doug Houseman
Eric Hubbard
Dmitry Ishchenko
Anthony Johnson
Brian Johnson
Jay Johnson
Rosanna Kallio
Piotr Karocki
John Kay
Aura Lee Keating
Thomas Keels
Yashar Kenarangui
Chad Kennedy
Gregory Kern
Yuri Khersonsky
Taesic Kim
Venkat Reddy Konala
Paul Krell
Marc Lacroix
Mikhail Lagoda
Daniel Lambert
James Lee
Shuhui Li
Brian Lydic
Thomas McDermott
Jeffrey McElray
Hank McGlynn
Anudeep Medam
Ronald Mitchell
Ali Moeini
David Mueller
David Narang
N. Kishor Narang
Alexandre Nassif
Gayle Nelms
Arthur Neubauer
Joe Nims
Matthew Norwalk
Gregory Olson

Copyright © 2023 IEEE. All rights reserved.
Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 18:54:43 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1547.3-2023

Lorraine Padden
Bansi Patel
Marc Patterson
Howard Penrose
Karen Quackenbush
Robert Rallo
Benito Ramos
R. K. Rannow
Lakshman Raut
James Reilly
Miguel Rios Rivera
Charles Rogers
Daniel Sabin
Nachum Sadan
Danish Saleem
Janette Sandberg
Steven Sano
Surya Santoso
Vincent Saporita
William Saylor
Bartien Sayogo
Stefan Schlichting
Christopher Searles
Daniel Seidel
Edward Seiter
Robert Seitz
Ronald Shipman
Mark Siira
P. Sivaraman
Glenn Skutt
Jerry Smith
Gary Smullin
Aaron Snyder
Sachin Soni
Lincoln Sprague
Wayne Stec
Scott Sweat
David Tepen
Michael Thesing
Michael Thompson
Sylvester Toe
Onur Usmen
James Van De Ligt
Benton Vandiver
Rajiv Varma
John Vergis
Alex Waitkus
Keith Waters
Kevin Whitener
Terry Woodyard
Stephen Wurmlinger
Francisc Zavoda

When the IEEE SA Standards Board approved this guide on 5 June 2023, it had the following membership:

David J. Law, *Chair*
Ted Burse, *Vice Chair*
Gary Hoffman, *Past Chair*
Konstantinos Karachalios, *Secretary*

Sara R. Biyabani
Ted Burse
Doug Edward
Ramy Ahmed Fathy
Guido R. Hiertz
Yousef Kimiagar
Joseph L. Koepfinger*
Thomas Koshy
John D. Kulick
Joseph S. Levy
Howard Li
Johnny Daozhuang Lin
Gui Lin
Xiaohui Liu
Kevin W. Lu
Daleep C. Mohla
Andrew Myles
Paul Nikolich
Annette D. Reilly
Robby Robson
Lei Wang
F. Keith Waters
Karl Weber
Philip B. Winston
Don Wright

*Member Emeritus

Copyright © 2023 IEEE. All rights reserved.
Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 18:54:43 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1547.3-2023

Introduction

This introduction is not part of IEEE Std 1547.3-2023, IEEE Guide for Cybersecurity of Distributed Energy Resources Interconnected with Electric Power Systems.

IEEE Std 1547™-2018 defines the interconnection and interoperability requirements for Distributed Energy Resources (DER) connected to the Electric Power System (EPS). Their conformance test procedures and pass/fail criteria are defined in IEEE Std 1547.1™.

IEEE Std 1547.3™ was initially developed to cover interoperability and cybersecurity for the original IEEE 1547-2003, but with the inclusion of interoperability in IEEE Std 1547-2018, interoperability will be covered in IEEE Std 1547.2™. However, IEEE Std 1547-2018 does not define requirements for cybersecurity; various standard development organizations (SDOs) like Underwriters Laboratory (UL), International Standards Organization (ISO), and the International Electrotechnical Commission (IEC) have developed standards for cybersecurity for "smart energy" systems, including DER, but not explicitly for DER meeting the IEEE Std 1547-2018 requirements. The industry is also learning from field and lab experiences; new vulnerabilities and potential threats are being discovered as more DER are evaluated. Therefore, IEEE Std 1547.3 was updated to provide guidance and recommendations by referring to the cybersecurity features available in the protocols specified by IEEE Std 1547-2018 (IEEE Std 1815™, IEEE Std 2030.5™, SunSpec Modbus, and IEC 61850), along with new cybersecurity concepts and technologies that have been developed over recent years. The scope of IEEE Std 1547.3 is, therefore, cybersecurity for the interconnection and interoperability of DER connected to electric power systems. Although not explicitly within the scope of IEEE Std 1547.3, transmission-connected systems, microgrids, electric vehicle charging stations, and off-grid systems could still benefit from the recommendations described in this guide.

Copyright © 2023 IEEE. All rights reserved.

Documents
Document Sharing Hub

Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 18:54:43 UTC from IEEE Xplore. Restrictions apply.

Full document details: IEEE 1547.3-2023

Contents

1. Overview 12
1.1 Scope 12
1.2 Purpose 12
1.3 Need for cybersecurity guidelines for DER 12
1.4 Word usage 13

2. Normative references 13

3. Definitions, acronyms, and abbreviations 14
3.1 Definitions 14
3.2 Acronyms and abbreviations 16

4. Cybersecurity considerations for DER interconnected to the electric power system 18
4.1 Overview 18
4.2 Need for DER cybersecurity guidance 18
4.3 Basics of cybersecurity for “cyber-physical” power systems 23
4.4 Cybersecurity for the DER domain 29
4.5 Elements of NIST Cybersecurity Framework for DER 42

5. Technical cybersecurity recommendations for DER operations 45
5.1 Overview of the structure of this clause 45
5.2 Risk assessment (RA) and management recommendations 46
5.3 Communication network engineering (NE) recommendations 49
5.4 Access control (AC) recommendations 54
5.5 Data security (DS) recommendations 57
5.6 Security management (SM) recommendations 61
5.7 Coping with and recovering from security events recommendations 67

6. Testing and commissioning for cybersecurity and conformance with IEEE Std 1547.3 recommendations 70
6.1 General 70
6.2 Audience description 70
6.3 DER lifecycle testing recommendations 72

Annex A (informative) Bibliography 77

Annex B (informative) Overview of DER communications protocols in IEEE Std 1547 81
B.1 Overview comparison of key DER communication protocols 81
B.2 IEEE Std 1815 (DNP3) 82
B.3 IEC 61850 83
B.4 IEEE Std 2030.5 83
B.5 SunSpec Modbus 85
B.6 MESA-DER and MESA-device specifications 86

Annex C (informative) Overview of other DER-related standards 89
C.1 IEC 60870-5-101 and IEC 60870-5-104 89
C.2 Open Platform Communications United Architecture 89
C.3 IEC 61968-5 90
C.4 OpenADR 2.0 91
C.5 Open Filed Message Bus (FMB) 91
C.6 ASHRAE 201 92

Copyright © 2023 IEEE. All rights reserved.
Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 18:54:43 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1547.3-2023

C.7 ASHRAE 135 92
C.8 IEEE Std 2030.2™ 93
C.9 LonTalk STACK 93

Annex D (informative) Brief descriptions of key cybersecurity standards 94
D.1 ISO/IEC 27000 cybersecurity standards 94
D.2 NIST Cybersecurity Framework 95
D.3 ISO 31000 and ISO 22301 95
D.4 NISTIR 7628 96
D.5 IEC 62443 series for industrial automation 97
D.6 IEC 62351 cybersecurity standards and guidelines for the smart grid 98
D.7 IEC 60870-5-7 Cybersecurity for IEC 60870-5-101/104 applying IEC 62351-5 101
D.8 IEEE Std 1815 (DNP3) Cybersecurity—Secure Authentication Version 5 and Version 6 101
D.9 NERC critical infrastructure protection (CIP) 102
D.10 Internet cybersecurity standards 103
D.11 IEEE Std 1686 107
D.12 IEEE Std C37.240™ 107
D.13 SAE J2931/7 cybersecurity for electric vehicles 108

Annex E (informative) Guideline recommendations based on NIST Cybersecurity Framework 109
E.1 Scope of guidelines 109
E.2 Overview of NIST Cybersecurity Framework 109
E.3 Identify (ID) 112
E.4 Protect (PR) 125
E.5 Detect (DE) 144
E.6 Respond (RS) 154
E.7 Recover (RC) 163

Annex F (informative) DER stakeholder roles and responsibilities recommendations 166
F.1 General 166
F.2 DER manufacturer (StkM) recommendations: DER system design for security and resilience 167
F.3 DER integrator and installer (StkI) recommendations: DER setup for meeting resilience requirements 170
F.4 DER testing (StkT) recommendations: Resilient DER system interconnection testing 171
F.5 DER users (facility/utility/aggregator operators) (StkU) recommendations: access requirements 172
F.6 DER facility ICT configuration (StkC) developer recommendations: Requirements for DER facilities 173
F.7 DER security managers (StkS) recommendations: Alarming, logging, and reporting cybersecurity requirements 175
F.8 DER maintenance personnel (StkE) recommendations: Requirements for DER maintenance, updating and re-testing 175
F.9 DER operator coping action (StkP) recommendations: actions during an attack or failure 176
F.10 DER recovery and analysis action (StkR) recommendations: After an attack or failure 178

Annex G (informative) Cloud computing 179
G.1 Managed hosting of upstream applications 179
G.2 Managed hosting of large-scale upstream applications 179

Annex H (informative) Questionnaire for implementors 180
H.1 What are the functional requirements, configuration, and data flows of your system? (ID.AM, ID.BE, ID.GV) 180
H.2 What are the security requirements for the system? (ID.RA, ID.RM, ID.SC) 180
H.3 How do you handle communication security? (PR.AC, PR.DS, PR.IP) 181
H.4 How do you manage your system? 181

Copyright © 2023 IEEE. All rights reserved.
Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 18:54:43 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1547.3-2023

IEEE Guide for Cybersecurity ~~Monitoring, Information Exchange, and Control~~ of Distributed Energy Resources Interconnected with Electric Power Systems

1. Overview

~~This overview is intended to provide a concise description of the scope, purpose, limitations, and application of this guide. Background information is provided in this clause, and detailed discussions of technical content are provided in the later clauses of this guide. The scope explains what is covered in the guide, the purpose explains why this guide's project is needed, and a subclause on limitations is presented that identifies certain monitoring, information exchange, and control (MIC) aspects not covered in this guide. In other words, the technical boundaries of the guide are discussed in these opening subclauses. Following that, background and introductory information are presented on understanding this guide's general application considerations.~~

1.1 Scope

This document provides guidelines for cybersecurity ~~monitoring, information exchange, and control~~ of distributed energy resources (DER ~~DR~~) interconnection ~~interconnected~~ with electric power systems (EPS~~s~~).

1.2 Purpose

This document provides guidelines for cybersecurity for ~~to facilitate the interoperability of~~ one or more distributed energy resources (DER) that are ~~DR~~ interconnected with electric power system. DER ~~EPSs. It describes functionality, parameters, and methodologies for MIC of DR interconnected with or associated with EPSs. DR technologies~~ include systems in the areas of fuel cells, photovoltaics, wind turbines, microturbines, ~~and~~ other distributed energy sources, and ~~generators as well as~~ distributed energy storage systems interconnected to EPSs at typical primary or secondary distribution voltage levels.

Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 18:54:43 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1547.3-2023

~~This guide documents alternatives for sound practice based on current practice and includes both legacy and new MIC systems.~~

1.3 Need for cybersecurity guidelines for DER

The cybersecurity guidelines outlined in this guide are for utilities, DER owner/operators, aggregators, manufacturers/integrators supporting DER interconnections, and other stakeholders involved in the DER domain.

This guide addresses the broad requirements of cybersecurity, going beyond the "DER interface" covered by the IEEE Std 1547™-2018 interoperability requirements, because security must be "end-to-end," and needs to be applicable for many different system architectures. For this reason, the security items covered in this document are guidelines and recommendations. The recommendations presented in this guide may not include all requirements; it is ultimately the responsibility of users of this document to review the applicability of the recommendations for their specific implementations. Although not explicitly within the scope of this document, transmission-connected systems, microgrids, electric vehicle charging stations, and off-grid systems could still benefit from the recommendations described.

This guide is designed to be used by individuals with different areas of expertise and experience with DER and cybersecurity. Clause 4 is designed to be useful and provide general background information on DER communications and cybersecurity. Clause 5 defines the cybersecurity technical recommendations for DER systems. Clause 6 lists cybersecurity testing recommendations for equipment and systems. The annexes provide additional information on standards and best practices.

Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 18:54:43 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1547.3-2023

1.4 Word usage

The word *shall* indicates mandatory requirements strictly to be followed in order to conform to the standard and from which no deviation is permitted (*shall* equals *is required to*).[6,7]

The word *should* indicates that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others; or that a certain course of action is preferred but not necessarily required (*should* equals *is recommended that*).

The word *may* is used to indicate a course of action permissible within the limits of the standard (*may* equals *is permitted to*).

The word *can* is used for statements of possibility and capability, whether material, physical, or causal (*can* equals *is able to*).

~~1.3 Limitations~~

~~This guide is primarily concerned with MIC between DR units and the outside world. It is not intended for MIC within a device or among the components that make up a DR unit. The data exchanges between the distributed resource controller and equipment or entities internal to the local electric power system are not addressed in this guide. Refer to 1.7 for clarification. The many potential paths of data exchanges among individual stakeholders are also beyond the focus of this document. This guide does not establish requirements for interconnection, protection, safety, or local and area EPS operation functions.~~

[6] The use of the word *must* is deprecated and cannot be used when stating mandatory requirements, *must* is used only to describe unavoidable situations.

[7] The use of *will* is deprecated and cannot be used when stating mandatory requirements, *will* is only used in statements of fact.

Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 18:54:43 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1547.3-2023

This guide does not attempt to judge the economic or technical viability of specific types of DR, but rather presents guidelines for MIC for specific use cases of DR. Market drivers will determine which DR applications become viable in these use cases. Further, it is beyond the scope of this guide to mandate the business or tariff requirements associated with DR interconnected with an electric power system. However, monitoring, information exchange, and control related to such issues and requirements may be satisfied by judicious use of this guide.

The guide provides a description of the MIC characteristics that support DR installations. The guide is intended to aid DR interested entities in the identification of MIC issues and solutions to support DR installations. This guide is not wholly comprehensive of the types of applications or the MIC desires of interested parties.

This guide does not address the MIC within the local EPS. (See Figure 1.) It does not address MIC for protection, and it does not address MIC requirements associated with revenue metering.

The guide is not part of any set of information exchange architecture standards for utility systems. Hence, conforming products to this guide does not guarantee they will be compatible with any utility system information exchange architecture.

Finally, specific hardware and software equipment, products, and services are not the subject of this guide.

1.4 Alternative approaches

This document provides guidelines rather than rigid requirements. This means alternative approaches to good practice are suggested but no clear-cut recommendations are made. This document states approaches relative to MIC for DR in EPSs. Example approaches are given, but there is more than one effective way to accomplish the desired results. One approach or another may be easier to implement in a specific user's DR installation, and it is recognized that the user has a choice.

Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 18:54:43 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1547.3-2023

1.5 Different levels of stakeholder needs

Stakeholder MIC needs vary with DR type, size, ownership, and location. In some situations, only minimal DR communications capabilities will be implemented. Additional capabilities may simply not be needed, or the functional benefit may not justify the expense. In other situations, a more comprehensive set of capabilities will be implemented to meet particular stakeholder needs or because the implementation cost is minimal. Although this document lists many potential MIC capabilities, it is important to remember that a wide range of stakeholder needs exists and that a corresponding range of MIC capabilities would be appropriate in these systems. In general, the size of the DR unit and the complexity of the application situation will help the user determine which MIC capabilities from the most relevant use case in this guide should be applied.

1.6 How to use this document

This guide is intended to help stakeholders in DR installations implement alternative approaches for MIC to support the operation of DR and transactions among stakeholders associated with DR. The reader should become familiar with the overall structure and intent of this guide, especially as discussed in Clause 1 and Clause 4.

Clause 1 provides an overview of the guide. Clause 2 presents references that are indispensable for the application of this guide. Clause 3 presents definitions and acronyms. Clause 4 introduces general technical content and application considerations of MIC of DR. Clause 5 contains basic MIC guidelines that focus on 4.16 of IEEE Std 1547™.[1] Clause 6 and Clause 7 present an in-depth treatment of MIC based on forward-looking approaches. In these clauses, guidelines are given for information modeling of DR interconnection applications. Clause 8 identifies example information technology protocol options and guidelines for protocols for MIC. Clause 9 provides guidelines for security issues for MIC in DR applications.

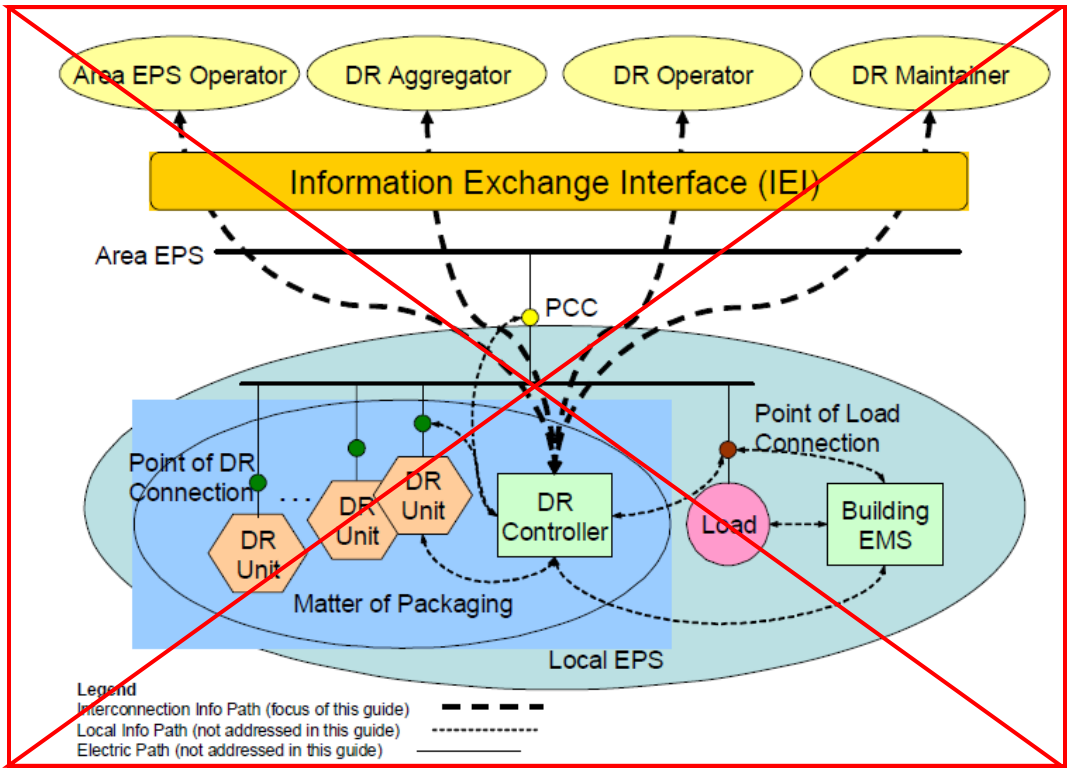
Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 18:54:43 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1547.3-2023

After these clauses, Annex A provides a bibliography. Annex B supports Clause 4 by presenting an annotated list of communications protocols, and Annex C supports this clause by providing additional information about open systems. Annex D is an introduction to business process concepts that supplements Clause 6 and Clause 8. Clause 6 is also supported by Annex E, which provides a use case template, and Annex F, which provides sample use cases. Annex G supplements Clause 7 with sample information exchange agreements (IEAs). Finally, Annex H supports Clause 9 by providing additional information security information.

1.7 IEEE 1547.3 reference diagram for information exchange

Figure 1 provides a reference overview of IEEE 1547.3 guidelines. Its emphasis is conceptual to focus the guidelines on the MIC that are relevant to DR interconnection. The diagram identifies the components that participate in processes of interest. These components are the subjects, or actors, of the process descriptions included in these guidelines. The components in this diagram are consistent with IEEE Std 1547. The new components of the diagram not defined in IEEE Std 1547 are defined in 1.7.1.

Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 18:54:43 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1547.3-2023



(Deleted)

Figure 1—Reference diagram for information exchange

The upper ovals represent the roles of stakeholders who may need to exchange information with the DR system about its interconnection with the area EPS. Other stakeholders are acknowledged as important in the integration of these resources; however, those shown are the subject of the IEEE 1547.3 guidelines (see 1.7.1.2).

The DR units are represented by the hexagons. There may be one or many DR units at a site, but there will be at least one DR controller that performs a monitoring and control function. The DR controller has the intelligence with which to collaborate with stakeholders and site equipment. Note that the DR controller may communicate with these other entities through a communication gateway component; however, for the purposes of the reference diagram, the DR controller subsumes this function. The DR units and controllers can be installed in a variety of configurations. DR units and DR controllers may be packaged together or separately, depending on the business strategy of the manufacturers and the requirements of the clients.

Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 18:54:43 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1547.3-2023

The large circle represents a load. Some loads may be facilities with facility energy management system (EMS) controllers to optimize their operations. A building facility controller is represented as a rectangle and labeled building EMS. Because the focus of the guidelines is on the DR interconnection, coordination of the DR with specific loads on the local EPS may be needed. The building EMS represents the intelligent component for collaboration with the DR controller to enable such interactions as may be needed for combined heat and power applications. The building EMS operator and the DR operator would need to collaborate to ensure appropriate interaction between the DR controller and building EMS for this purpose.

Connections of interest are presented as lines in Figure 1. Solid lines represent electrical connections, and dashed lines represent communication paths. The communication paths are further sub-divided into those that are relevant to the guidelines and those that are acknowledged as important in an installation but are not the focus of this work. Note that communications exist among the stakeholders; however, these are not the subject of these guidelines and, for simplicity, are not shown in the diagram. The heavy dashed lines between stakeholders and the DR controller indicate the focus of these guidelines. The lighter dashed lines are generally required for local monitoring and control of internal device parameters or connection points in the local EPS. They are addressed through various mechanisms (such as standards, de facto standards, and custom implementations) that are generally within the control of the DR site integrator and, therefore, are less relevant to the interconnection with the area EPS and interaction with the DR stakeholders. As noted in 1.3, limitations, local sensing, and control are not the concern of this guide. In addition, the light dashed line between the DR controller and building EMS is included in the diagram to acknowledge that these systems may be integrated at a site to coordinate capabilities such as combined heat and power, but the details of this interaction are not the concern of this guide.

Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 18:54:43 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1547.3-2023

This guide can be thought of in terms of an information exchange interface for the DR device to communicate with remote parties. The information exchange interface could be an actual single point of interface for all remote information flows to and from the device, or it could be an abstraction that represents information flows by multiple, but coordinated, physical media. In either case, this document provides guidance for the information content (e.g., parameters, data, and data rates) that needs to be available at the information exchange interface. The information exchange interface is the information exchange counterpart of the point of common coupling (PCC) in the electrical system.

1.7.1 Diagram terminology

To clarify the terms and concepts in the reference diagram, definitions of the equipment and stakeholder roles follow. The term "role" represents that component of an organization that performs a certain job and interacts with other components in its duties. Organizations can be structured to contain different mixes of roles (e.g., a distribution system company may include area EPS operator (AEPSO), DR operator, and DR maintainer roles). By distinguishing among roles, the information exchange described by these guidelines can be applied to organizations with different combinations of roles. The same holds true for the combinations of equipment components in an installation and the roles they assume.

1.7.1.1 Equipment roles

- **Building EMS:** A system that supervises the scheduling and interaction among all building subsystems (e.g., chillers, boilers, and air handling units) to meet facility needs with appropriate operator input. Building EMSs are also used to optimize building operations, start/stop, and demand control. Other names for these systems include building supervisory control systems, building automation systems, or facility management systems. Building EMSs may need to share information with the DR controller to coordinate supply and demand within a local EPS.

Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 18:54:43 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1547.3-2023

- **DR controller:** A device that manages the moment-by-moment operation of the DR device. These functions include fuel control, machine safety, and electrical protection as well as other functions that need tightly coupled monitoring and control. The DR controller has an interface that handles the slower communications requirements of the stakeholders and coordination with a building EMS. The DR controller can be incorporated into a DR device, or one DR controller may control several DR devices. The DR controller includes the functions of system control, electrical protection, and steady-state control, as described in the Definitions clause of IEEE Std 1547.1™.

- **DR unit:** Per IEEE Std 1547, the DR unit is a source of electric power that is not directly connected to a bulk power transmission system. DR units include both generators and energy storage technologies.

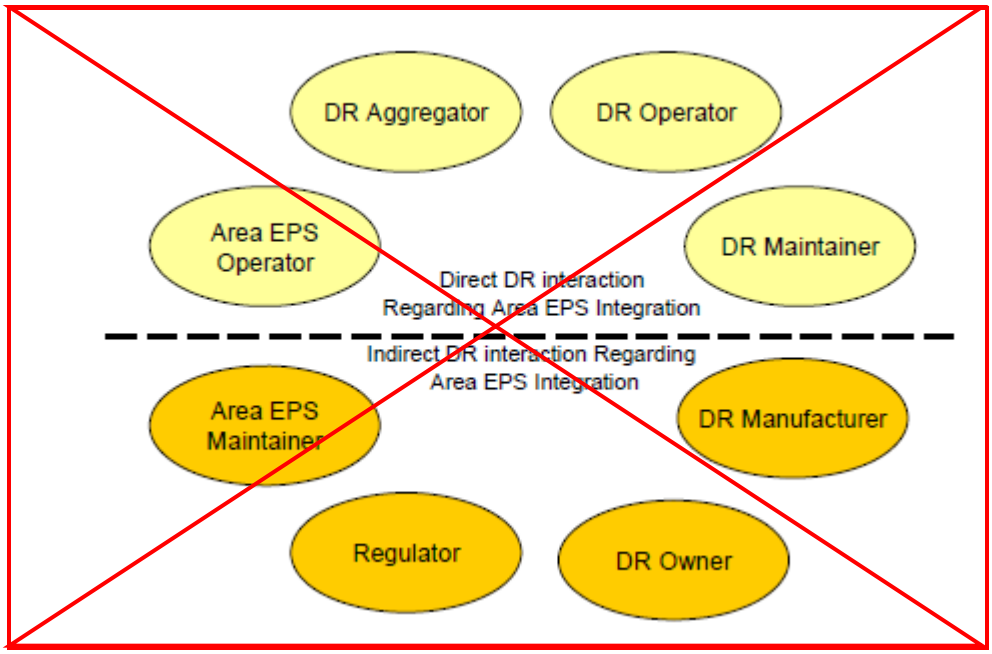
- **Load:** A point of delivery for end-use electrical consumption in the electric system. The load is usually made up of a combination of appliances (e.g., heating, ventilation, and air conditioning; refrigerators; lights; and other electric equipment) that is fed through a single point in the local EPS.

1.7.1.2 Stakeholder roles

The stakeholders with an interest in DR interconnection are people and organizations with complex groupings of responsibilities. Each organization is marked by its particular business strategies and structures, which have the capacity to evolve over time. The predominant roles that stakeholders assume are defined in this subclause. Any stakeholder organization may be composed of one or more of these roles.

The stakeholder roles are distinguished into two categories based on their need for direct interaction with DR systems, as illustrated in Figure 2. Note that many paths of information exchange exist among these roles, but these are beyond the focus of this document.

Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 18:54:43 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1547.3-2023



~~(Deleted)~~

~~Figure 2—Stakeholder roles relevant to DR interconnection~~

~~1.7.1.2.1 Roles with direct interaction~~

~~The following stakeholder roles may have direct communications interactions with DR systems about their interconnection with the area EPS:~~

- ~~**Area electric power system operator (AEPSO):** Responsible for the operations of the area EPS with which the DR is interconnected through the PCC. This operator is concerned with the safe and reliable operation of the distribution system and ensures that any misoperation of the DR will not affect other customers connected to the EPS. The AEPSO may need to interact with the DR unit to monitor its state or ensure its removal from the EPS to protect the safe and reliable operation of the EPS. In some cases, the AEPSO may also own and operate the DR.~~

Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 18:54:43 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1547.3-2023

- **DR aggregator:** Manages distributed electric energy resources that consist of more than one supply source (e.g., for the purpose of marketing energy and ancillary services to clients via the area EPS). The DR aggregator may interact with DR controllers to exchange economic or control information as well as information for contract settlement.

- **DR maintainer:** Maintains a DR unit for safe, reliable operation. The DR maintainer may interact with the DR unit to monitor its behavior, receive reports of problems involving maintenance, or otherwise review its health.

- **DR operator:** Controls the DR operation through local or remote means. It interacts with the DR unit to monitor its status and supervise its control.

1.7.1.2.2 Acknowledged roles without direct interaction

The following roles are acknowledged to play an important part of the successful integration of DR technology with the distribution system. They are distinguished from the roles with direct information exchange interaction because they gather their information needs visually or through others that have information exchange roles with the DR controller.

- **Area EPS maintainer:** Responsible for maintaining the EPS equipment on the area EPS side of the PCC. To safely maintain this equipment, the area EPS maintainer will need to know the operational state of the DR unit from the AEPSO and have visual assurances of important operational characteristics (such as deenergized state).

- **DR manufacturer:** Manufactures, produces, or integrates components that make up all or part of the system referred to as the DR. This includes producers of DR controllers. The DR manufacturer may get diagnostic information from the DR controller through its own diagnostic communication mechanisms or through others, such as the DR maintainer or DR operator, that have information exchange. Manufacturer interfaces may be highly specialized and business sensitive and thus are beyond the focus of these guidelines.

Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 18:54:43 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1547.3-2023

- ~~**DR owner:** Owns in part or whole a DR unit. The DR owner may have no connection with the location or operation of the DR. It interacts with other stakeholder roles (e.g., the DR operator) to verify operations and maintenance aspects performed by the other roles.~~

- ~~**Regulator:** Monitors agreed upon aspects of DR and distribution system operations for proper behavior against established rules. The regulator gathers information through visual means and the records kept by those performing the other stakeholder roles.~~

2. Normative references

The following referenced documents are indispensable for the application of this document (i.e., they must be understood and used, so each referenced document is cited in text and its relationship to this document is explained). For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments or corrigenda) applies.

Barrett, Matthew P., Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 NIST, 2018.[8,9]

IEC 61850-7-420:2021, Basic communication structure—Distributed energy resources and distribution automation logical nodes.[10]

IEC 62351, Power systems management and associated information exchange—Data and communications security.

IEC 62443, Industrial communication networks—Network and system security.

[8] NIST publications are available from the National Institute of Standards and Technology (https://www.nist.gov/).

[9] As of publication, this book can specifically be found at https://www.nist.gov/publications/framework-improving-criticalinfrastructure-cybersecurity-version-11.

[10] IEC publications are available from the International Electrotechnical Commission (https://www.iec.ch) and the American National Standards Institute (https://www.ansi.org/).

Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 18:54:43 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1547.3-2023

IEEE Std 1547™-2018, IEEE Standard for Interconnection and Interoperability of ~~Interconnecting~~ Distributed Energy Resources with Associated Electric Power Systems Interfaces.[11,12] ~~.[2], [3]~~

IEEE Std 1686™-2022, IEEE Standard for Intelligent Electronic Devices Cyber Security Capabilities.

IEEE Std 1815™-2012, IEEE Standard for Electric Power Systems Communications-Distributed Network Protocol (DNP3).

IEEE Std 2030.5™-2018, IEEE Standard for Smart Energy Profile Application Protocol.

ISO/IEC 27000 series, Information technology—Security techniques—Information security management systems—Overview and vocabulary (all that are applicable).[13]

UL 2900-2-2:2016, Software Cybersecurity for Network-Connectable Products, Part 2-2: Particular Requirements for Industrial Control Systems.[14]

~~IEEE Std 1547.1, IEEE Standard for Conformance Tests Procedures for Equipment Interconnecting Distributed Resources with Electric Power Systems.[2,3]~~

[11] The IEEE standards or products referred to in this clause are trademarks owned by The Institute of Electrical and Electronics Engineers, Incorporated.

[12] IEEE publications are available from The Institute of Electrical and Electronics Engineers (https://standards.ieee.org/).

[13] ISO publications are available from the International Organization for Standardization (https://www.iso.org/) and the American National Standards Institute (https://www.ansi.org/).

[14] ANSI publications are available from the American National Standards Institute (https://www.ansi.org/).

~~[2] IEEE publications are available from the Institute of Electrical and Electronics Engineers, 445 Hoes Lane, Piscataway, NJ 08854, USA (http://standards.ieee.org/).~~

~~[3] The IEEE standards or products referred to in this clause are trademarks of the Institute of Electrical and Electronics Engineers, Inc.~~

Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 18:54:43 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1547.3-2023

3. Definitions, ~~and~~ acronyms, and abbreviations

3.1 Definitions

For the purposes of this document ~~guide~~, the following terms and definitions apply. The *IEEE Standards* ~~*Authoritative*~~ *Dictionary Online* ~~*of IEEE Standards, Seventh Edition*~~ [B33][4] should be consulted ~~referenced~~ for terms not defined in this clause.[15]

access control list (ACL): A mechanism that implements access control for a system resource by enumerating the identities of the system entities that are permitted to access the resources.

NOTE—Source: NIST SP 800-82 Rev. 2 [B47].[16]

~~3.1 Definitions~~

~~**3.1.1 actor:** Term used in Unified Modeling Language (UML) to designate the role a human, an application, or a system plays in the function being modeled.~~

~~**3.1.2 aggregation:** A special form of association that specifies a whole-part relationship between the aggregate (whole) and a component part.~~

~~**3.1.3 alarm:** Change-of-state information that is important enough to warrant notifying a person or system.~~

area electric power system (Area EPS): An EPS that serves local EPSs. Note that, typically, an Area EPS has primary access to public rights-of-way, priority crossing of property boundaries, etc., and is subject to regulatory oversight.

[15] *IEEE Standards Dictionary Online* is available at: http://dictionary.ieee.org. An IEEE account is required for access to the dictionary, and one can be created at no charge on the dictionary sign-in page.

~~[4]The numbers in brackets correspond to those of the bibliography in Annex A.~~

[16] [5] Notes in text, tables, and figures of a standard are given for information only and do not contain requirements needed to implement this ~~the~~ standard.

Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 18:54:43 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1547.3-2023

NOTE—Source: IEEE Std 1547 [B21]. [17]

bulk power system (BPS): Any electric generation resources, transmission lines, interconnections with neighboring systems, and associated equipment.

NOTE—Source: IEEE Std 1547 [B21].

commissioning test: A test conducted when the equipment is installed to verify correct operation.

NOTE—Source: IEEE Std 1547 [B21].

cleansed: Process that restores a device by resetting all settings through a factory reset process or some other means.

controllable load: An electric load that may be controlled.

cyber-physical system (CPS): A system that integrates computation with physical processes, in a network manner, whose behavior is defined by both cyber and physical parts of the system.

NOTE—Source: IEEE Std 2660.1™-2020 [B25].

demilitarized zone (DMZ): A perimeter network or screened subnet separating an internal network that is more trusted from an external network that is less trusted.

NOTE—Source: NIST SP 1800-16B [B51].

design test: *See*: **type test**.

~~**3.1.5 association:** The semantic relationship between two or more classifiers that specifies connections among their instances.~~

~~**3.1.6 authorization:** The process of verifying that a user or process has permission to use a resource in the manner requested. To assure security, the user or process also needs to be authenticated before access is granted.~~

[17] Information on references can be found in Clause 2.

Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 18:54:43 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1547.3-2023

3.1.7 class: A description of a set of objects that share the same attributes, operations, methods, relationships, and semantics. A class may use a set of interfaces to specify collections of operations it provides to its environment.

3.1.8 class diagram: A diagram that shows a collection of declarative (static) model elements such as classes and types and their contents and relationships.

3.1.9 collaboration: The specification of how an operation or classifier, such as a use case, is realized by a set of classifiers and associations playing specific roles used in a specific way. The collaboration defines an interaction.

3.1.10 collaboration diagram: A diagram that shows interactions organized around the structure of a model by using either classifiers and associations or instances and links. Unlike a sequence diagram, a collaboration diagram shows the relationships among the instances. Sequence diagrams and collaboration diagrams express similar information but show it in different ways.

3.1.11 command: Controllable point used to change system behavior (enable/disable).

3.1.12 communication security: Protective measures for information transmitted between system components, over telecommunication links, and through networks to provide data confidentiality, integrity, and authenticity.

3.1.13 communications security: The use of administrative, technical, or physical measures to deny unauthorized persons information from a computer or a communications network and ensure the authenticity and integrity of such communications.

3.1.14 compromise: A violation of the security of a system such that an unauthorized disclosure of sensitive information may have occurred.

3.1.15 control: Operational function used to change and modify, intervene, switch, set parameters, and optimize generation.

Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 18:54:43 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1547.3-2023

3.1.16 data integrity: (A) The degree to which a collection of data is complete, consistent, and accurate. (B) The condition or state in which data has not been altered or destroyed in an unauthorized manner.

3.1.17 distributed energy resource: *See:* **distributed resources.**

3.1.18 distributed generation or distributed generator: Electric generation facility connected with an area EPS through a PCC; a sub-set of DR.

3.1.19 distributed resources (DR): Sources of electric power that are not directly connected with a bulk power transmission system. DR include both generation and energy storage technologies.

NOTE DR devices are also widely known as "distributed energy sources" and "distributed energy resources." Both the terms DR and DER are used in other contexts to have a broader meaning than in this guide.[5]

3.1.20 distributed resource aggregator: Manages distributed electric energy resources that consist of more than one supply source for the purpose of marketing energy and ancillary services to clients via the area EPS. The DR aggregator may interact with DR controllers to exchange economic or control information as well as information for contract settlement.

3.1.21 distributed resource controller: A device that manages the moment-by-moment operation of the DR device. These functions include fuel control, machine safety, and electrical protection as well as other functions that need tightly coupled monitoring and control.

3.1.22 distributed resource maintainer: Maintains a DR unit for safe, reliable operation. The DR maintainer may interact with the DR unit to monitor its behavior, receive reports of problems involving maintenance, or otherwise review its health.

3.1.23 distributed resource operator: Controls the DR operation through local or remote means. It interacts with the DR unit to monitor its status and supervise its control.

Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 18:54:43 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1547.3-2023

~~3.1.24~~ ~~**distributed resource owner:** Owns in part or whole a DR unit. The DR owner may have no connection with the location or operation of the DR. It interacts with other stakeholder roles (e.g., the DR operator) to verify operations and maintenance aspects performed by the other roles.~~

distributed energy resources (DER): A ~~**resource unit:** Per~~ source of electric power that is not directly connected to a bulk power ~~transmission~~ system. DER includes ~~DR units include~~ both generators and energy storage technologies capable of exporting active power to an EPS. An interconnection system or a supplemental DER device that is necessary for compliance with IEEE Std 1547.3™ is part of a DER.

NOTE—Controllable loads used for demand response are not included in the definition of DER. Source: IEEE Std 1547 [B21].

~~3.1.26~~ ~~**distributed storage:** An electric storage facility connected with an area electric power system through a PCC; a subset of distributed resources.~~

~~3.1.27~~ ~~**domain:** An area of knowledge or activity characterized by a set of concepts and terminology understood by practitioners in that area.~~

electric power system (EPS): Facilities that deliver electric power to a load. *See also:* **area electric power system (EPS)**; **local electric power system (EPS)**.

NOTE 1— EPS may include generation units.

NOTE 2— Source: IEEE Std 1547 [B21].

gateway [1]: A device or apparatus of a communication network composed of hardware and software that can interconnect with other communication networks using protocols and equipment that can access other systems.

NOTE—Source: IEEE Std 2847™-2021 [B27].

Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 18:54:43 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1547.3-2023

gateway [2]: An intermediate system (interface, relay) that attaches to two (or more) computer networks that have similar functions but dissimilar implementations and that enables either one-way or two-way communication between the networks.

NOTE—Source: NIST SP 800-12 Rev. 1 [B46].

~~**3.1.29 electric power system, area:** *See :* **area electric power system (EPS).**~~

~~**3.1.30 electric power system, local:** *See:* **local electric power system (EPS).**~~

~~**3.1.31 enumeration:** A list of named values used as the range of a particular attribute type. For example, RGB Color = {red, green, blue}. Boolean is a predefined enumeration with values from the set {false, true}.~~

~~**3.1.32 event:** The specification of a significant occurrence that has a location in time and space. In the context of state diagrams, an event is an occurrence that can trigger a transition.~~

~~**3.1.33 extensible markup language:** A specification developed by the World Wide Web Consortium, or W3C (a consortium of organizations that promotes interoperability on the Internet). Extensible Markup Language (XML) is a pared-down version of SGML designed especially for Web documents. It allows designers to create customized tags (data types), which enables the definition, transmission, validation, and interpretation of data among applications and among organizations.~~

~~**3.1.34 function:** A task, usually automated but with possible actions by human users, that is performed in the control center or distributed resource system.~~

~~**3.1.35 generalization:** A taxonomic relationship between a more general element and a more specific element. The more specific element is fully consistent with the more general element and contains additional information. An instance of the more specific element may be used where the more general element is allowed.~~

Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 18:54:43 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1547.3-2023

~~3.1.36 **information:** Content of communication; data and metadata describing data. The material basis is raw data, which is processed into relevant information. distributed resource device information categories include source information (e.g., analogue and state information) and derived information (e.g., statistical and historical information).~~

~~3.1.37 **information exchange:** Communication process between two systems, such as component and actor, with the goal to provide and get relevant information. Requires specific communication functions (services).~~

~~3.1.38 **interaction:** A specification of how stimuli are sent between instances to perform a specific task. The interaction is defined in the context of a collaboration.~~

~~3.1.39 **interaction diagram:** A generic term that applies to several types of diagrams that emphasize object interactions. These include collaboration diagrams and sequence diagrams.~~

~~3.1.40 **interconnection:** The result of adding a distributed resource unit to an area electric power system.~~

interconnection system (ICS): ~~The~~ the collection of all ~~interconnection~~ equipment and functions, taken as a group, used to interconnect a distributed energy resources (DER) ~~resource~~ unit to ~~with~~ an area electric power system (EPS).

NOTE—Source: IEEE Std 1547 [B21].

inverter: A machine, device, or system that changes dc power to ac power.

NOTE—Source: IEEE Std 1547 [B21].

~~3.1.42 **island:** A condition in which a portion of an area electric power system is energized solely by one or more local electric power systems through the associated point of common couplings while that portion of the area electric power system is electrically separated from the rest of the area electric power system.~~

Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 18:54:43 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1547.3-2023

~~3.1.43~~ ~~**islanding:** The process whereby a power system is split into two or more segments, each with its own generation. Islanding is a deliberate emergency measure, the result of automatic protection or control action, or the result of human error.~~

local electric power system (local ~~electric power system (~~EPS): An EPS contained entirely within a single premises ~~premise~~ or group of premises.

NOTE—Source: IEEE Std 1547 [B21].

~~3.1.45~~ ~~**measured value:** A sample of an analog quantity over a specific time period.~~

~~3.1.46~~ ~~**message:** A specification of the conveyance of information from one instance to another, with the expectation that activity will ensue. A message may specify the raising of a signal or the call of an operation.~~

~~3.1.47~~ ~~**monitoring:** An operational function used for local or remote observing of the status and changes of states.~~

~~3.1.48~~ ~~**object:** An entity with a well-defined boundary and identity that encapsulates state and behavior. State is represented by attributes and relationships; behavior is represented by operations, methods, and state machines. An object is an instance of a class.~~

~~3.1.49~~ ~~**ontology:** In the field of information technology, an ontology defines the common words and concepts (the meaning) used to describe and represent an area of knowledge. It is an engineering product that consists of a specific vocabulary used to describe a part of reality, plus a set of explicit assumptions regarding the intended meaning of that vocabulary—in other words, the specification of a conceptualization.~~

~~3.1.50~~ ~~**operational function:** Used by actors for the normal daily operation of devices to obtain information about devices and send instructions to them. Types include monitoring, logging and reporting, data retrieval, and control.~~

~~3.1.51~~ ~~**package:** A general purpose mechanism for organizing elements into groups. Packages may be nested within other packages.~~

Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 18:54:43 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1547.3-2023

~~3.1.52 **parallel operation:** (A) The operation of interconnected power systems in synchronism. (B) The operation of network components—such as lines, transformers, and generators—connected in parallel.~~

~~3.1.53 **personnel security:** Procedures to ensure that personnel with access to sensitive information and critical services have the appropriate authorizations and training.~~

~~3.1.54 **physical security:** The protection of system resources from physical access, tampering, and destruction through the use of barriers, locks, seals, and intrusion detection systems.~~

point of common coupling (PCC): The point of connection between the Area EPS and the local EPS. ~~The point at which a local electric power system is connected with an area electric power system.~~

NOTE—Source: ~~See Figure 1 of~~ IEEE Std 1547 [B21].

point of distributed energy resources connection (PoC): The point where a DER unit is electrically connected in a local EPS.

NOTE—Source: relevant part of definition in IEEE Std 1547 [B20].

production test: A test conducted on every unit of equipment prior to shipment.

NOTE—Source: IEEE Std 1547.1™-2020 [B21].

resilience: The ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruption. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents.

NOTE—Source: NIST SP 800-160 Vol. 2 Rev. 1 [B48].

supplemental DER device: Any equipment that is used to obtain compliance with some or all of the interconnection requirements of IEEE Std 1547™.

tamper detection: The ability of a device to sense an active attempt to compromise device integrity or data associated with the device.

Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 18:54:43 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1547.3-2023

type test: A test of one or more devices manufactured to a certain design to demonstrate, or provide information that can be used to verify, that the design meets the requirements specified in this standard. Syn: **design test**.

NOTE—Source: IEEE Std 1547-2018.

virtual local area network (VLAN): A broadcast domain that is partitioned and isolated within a network at the data link layer. A single physical local area network (LAN) can be logically partitioned into multiple, independent VLANs; a group of devices on one or more physical LANs can be configured to communicate within the same VLAN, as if they were attached to the same physical LAN.

NOTE—Source: NIST SP 1800-15B [B50].

zero-day exploit: The technique or attack a malicious actor deploys to leverage an unknown security vulnerability to gain access into a system.

3.2 Acronyms and abbreviations

AAA	availability, authorization, and accounting
ACL	access control list
AES	advanced data encryption standard
AMI	advanced metering infrastructure
AMP	authority management protocol
API	application programming interface
BPS	bulk power system
C2M2	cybersecurity capability maturity model
CA	certificate authority

Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 18:54:43 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1547.3-2023

CAP	cybersecurity assurance program
CIA	confidentiality, integrity, availability
CPS	cyber-physical system
CPUC	California public utilities commission
CRC	cyclic redundancy checking
CRL	certificate revocation list
CSET	cybersecurity evaluation tool
CSIP	common smart inverter profile
CVE	common vulnerabilities and exposures
DDoS	distributed denial of service
DER	distributed energy resources
DERMS	distributed energy resource management system
DES	data encryption standard
DNP	distributed network protocol
DMZ	demilitarized zone
DNP3	distributed network protocol
DoS	denial of service
DSA	digital signature algorithm
DSS	digital signature standard
ECC	elliptic curve cryptography

Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 18:54:43 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1547.3-2023

EMI	electromagnetic interference
EPS	electric power system
ESS	energy storage system
EUT	equipment under test
FDEMS	facilities
DER	energy management system
FEMS	facility energy management system
FERC	federal energy regulatory commission
FIPS	federal information processing standard
GOOSE	generic object-oriented substation event
HAN	home area network
HIL	hardware-in-the-loop
HMI	human-machine interface
HTTPS	hypertext transfer protocol security
ICS	interconnection system / industrial control system
IDS	intrusion detection system
IEC	international electrotechnical commission
IED	intelligent electronic device
IoT	internet of things
IOU	investor-owned utility

Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 18:54:43 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1547.3-2023

IP	internet protocol
IPS	intrusion prevention system or internet protocol suite
IPSec	internet protocol security
IT	information technology
LAN	local area network
MMS	manufacturing message specification
NAT	network address translation
NISTIR	NIST interagency or internal report
NTP	network time protocol
OCSP	online certificate status protocol
OT	operational technology
PCC	point of common coupling
PCS	power conditioning
PKCS	public-key cryptography standards
PKI	public key infrastructure
PLC	programmable logic controller
PoC	point of [distributed energy resources (DER)] connection
PV	photovoltaic
RBAC	role-based access control
RFC	request for comment

Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 18:54:43 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1547.3-2023

RMP	risk management process
Root-CA	root certificate authority
RTU	remote terminal unit
SA	situational awareness or secure authentication (e.g., DNP-SA)
SCADA	supervisory control and data acquisition
SNMP	simple network management protocol
SP	special publication, from NIST
SRTP	secure real-time transport protocol
SSL	secure socket layer
TCP	transmission control protocol
TLS	transport layer security
TPM	trusted platform module
TTP	tactics-techniques-procedures
UDP	user datagram protocol
VLAN	virtual local area network
VPN	virtual private network
WAN	wide area network
XMPP	eXtensible messaging and presence protocol

Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 18:54:43 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1547.3-2023

4. Cybersecurity considerations for DER interconnected to the electric power system

4.1 Overview

This clause is intended to provide the reader with a basic understanding of cybersecurity concepts and to establish the need for DER cybersecurity guidance. Subclause 4.2 covers the background of interoperability requirements in IEEE Std 1547-2018, and the gap in cybersecurity requirements for DER equipment and networks. Subclause 4.3 introduces the broader concerns associated with cyber-physical systems [also called industrial control systems (ICSs) or operational technology (OT)] as applicable to power systems. Subclause 4.4 focuses on themes associated with DER cybersecurity; and 4.5 introduces the NIST cybersecurity framework, which is used to categorize the recommendations in Clause 5 and Clause 6.

4.2 Need for DER cybersecurity guidance

4.2.1 Electric power system as critical infrastructure

The electric power system is deemed a critical infrastructure because electrical energy is vital to all sectors of society, including the industrial, commercial, and residential domains. But now, due to the increasing numbers and sizes of DER interconnected to the power system, the operation of the power system is being radically restructured and is posing new and complex engineering challenges. At the same time, the increased requirement for data to be exchanged amongst the many DER stakeholders challenges the secure operation of the power system. Cybersecurity is therefore looming as one of key challenges to help ensure the safe and continued operation of this critical cyber-physical system.

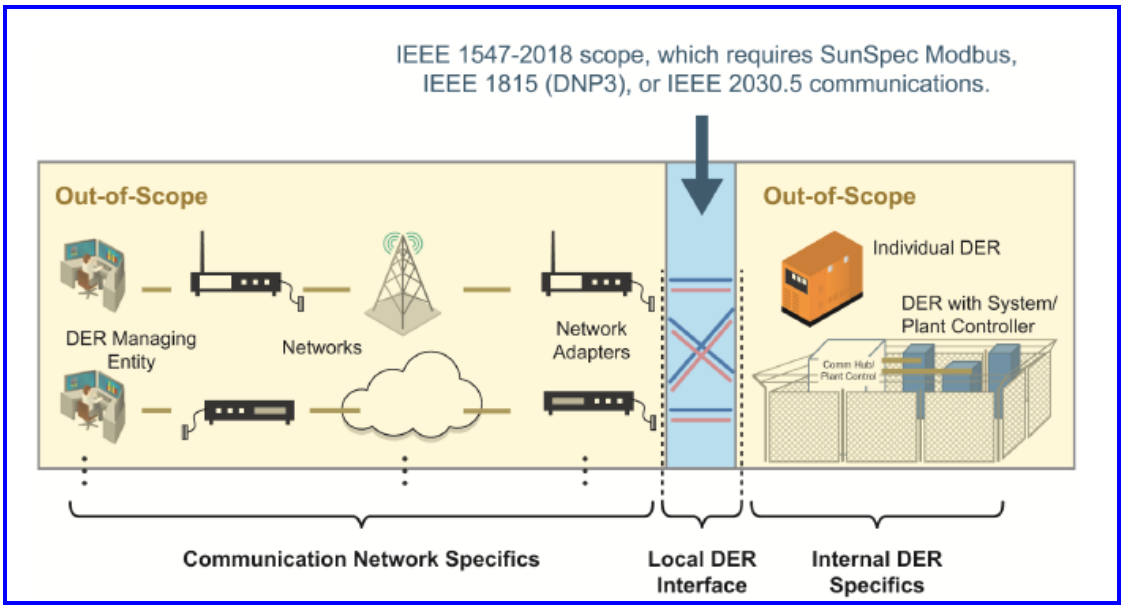
Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 18:54:43 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1547.3-2023

4.2.2 IEEE 1547 interoperability communication implications for DER cybersecurity

IEEE Std 1547-2018 includes interoperable communication requirements for the interconnection of DER to the electric power system in order to provide area electric power system operators, aggregators, and DER operators with greater flexibility for managing and delivering grid services. However, these communication capabilities also increase the vulnerability of the power system to cybersecurity events and now pose a significant risk to the resilience and reliability of the electric grid if DER equipment, particularly in aggregate, is compromised. Yet, IEEE Std 1547-2018 does not define requirements for cybersecurity other than stating, "It is recognized that cybersecurity is a critically important issue for DER deployments connected to broader monitoring and control communications networks." In stating this, it has left the development of cybersecurity recommendations to other efforts.

IEEE Std 1547.3 was initially developed to cover interoperability and cybersecurity for the original IEEE Std 1547-2003. However, the industry is continuously learning from field and lab experiences, while new vulnerabilities and potential threats are being discovered as more DER are interconnected. So, with the revision to IEEE Std 1547-2018, it was determined that the general cybersecurity discussions in IEEE Std 1547.3-2007 were no longer adequate to address present security needs. As a result, this revision of IEEE Std 1547.3 was undertaken to provide cybersecurity guidance and recommendations for communications of DER interconnected to the electric power system as required by IEEE Std 1547-2018, and shown in Figure 1.

Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 18:54:43 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1547.3-2023



(New)

Figure 1 —IEEE Std 1547 scope for interoperability requirements

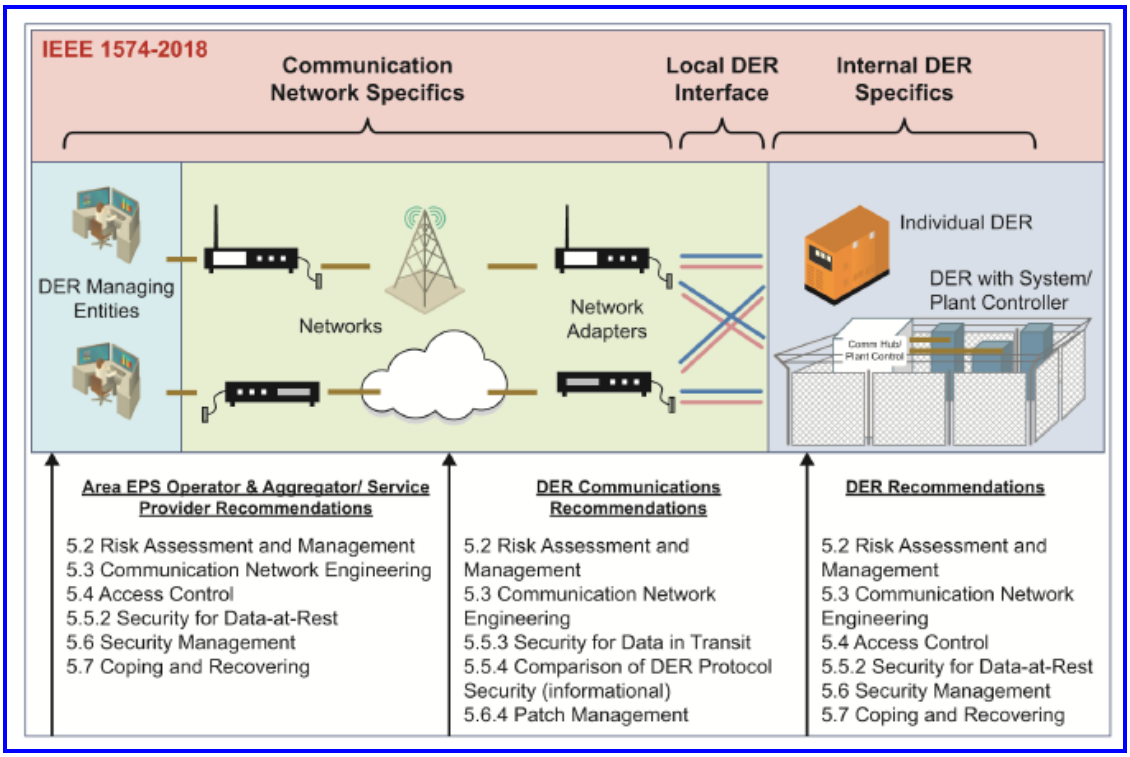
However, although IEEE Std 1547-2018 references only the local DER communication interface, effective cybersecurity needs to be "end-to-end" in order to protect and manage the secure transmission and storage of data. Therefore, cybersecurity applies not only at the local DER interface, but also across the entire communication system to avoid the possibility that compromised data, even if encrypted, can be sent across the interface between a DER facility and power system operations. Although "information security" is a key aspect of cybersecurity, the primary purpose of cybersecurity for any cyber-physical systems is still resilien*ce* to any cyber-caused security problems that impact the safety and reliability of those cyberphysical operations.

So, using this broad cybersecurity scope as a starting point, this document discusses the key cybersecurity issues and best practices related to DER interconnected with the power system and addresses concerns related to the entire DER domain, including recommendations on cybersecurity for functional and interoperability interactions across utility operations, DER facilities, aggregators, vendors, maintenance, and other stakeholders.

Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 18:54:43 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1547.3-2023

To help clarify this extended scope, Figure 2 adds the cybersecurity recommendations from Clause 5 to the interoperability scope diagram from IEEE Std 1547. As can be seen, IEEE Std 1547.3 expands beyond the constrained scope of IEEE Std 1547-2018 to encompass an end-to-end scope, in order to protect the communications and operations of DER equipment, network systems, and operating entities. IEEE Std 1547.3 also provides specific guidance on the cybersecurity capabilities of the protocols specified in IEEE Std 1547-2018 (namely, IEEE Std 1815™, IEEE Std 2030.5™, and SunSpec Modbus, as well as IEC 61850).

This guide applies to all entities operating within the DER communication environment and should be referenced as a best practice to secure DER communications. Applying these recommendations will establish a strong defense-in-depth foundation for DER assets connected to the power system.



(New)

Figure 2 —IEEE Std 1547.3 scope with Clause 5 recommendations

Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 18:54:43 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1547.3-2023

4.2.3 Cybersecurity policies, procedures, and organizational directives

Cybersecurity policies and procedures drive the determination of what cybersecurity techniques and technologies could be used to improve the security of systems. In particular, as described in the NIST Cyber Security Framework, security policies need to cover many aspects of security, including the following:

- **Identify and plan**: Preparing for potential threats and reducing security risks.
- **Protect**: Guarding not only against deliberate security attacks, but also minimizing the more frequent inadvertent security violations.
- **Detect**: Being informed in a timely manner of possible security attacks, including when vulnerabilities are discovered, and the inevitable successful security attacks.
- **Respond**: Determining how to handle and cope with different types of security attacks, including operating the power system in degraded mode.
- **Recover**: Defining stakeholder business continuity planning/disaster recovery (BCP/DR) plans and how best to restore the systems after various types of security compromises.

Security procedures would be implemented to follow the general security policies and provide more precise details on what needs to be done. For instance, the roles of people and systems would be defined, along with their responsibilities and constraints. These procedures would also define exactly who does what, and with which tools before, during, and after security events.

Finally, technology would provide the tools for how best to support the security policies and procedures. Often technologies are expected to be the solution for security, but in reality, they are only as effective as the security policies and procedures behind them. For instance, encryption technology may be used to prevent eavesdropping on messages, but if the contents of the message have already been compromised due to a failed procedure, just encrypting the "bad" message will not prevent the system from operating incorrectly or unsafely.

Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 18:54:43 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1547.3-2023

4.2.4 Cybersecurity challenges for power systems with interconnected DER

Increasing adoption of new technologies to improve operational efficiencies and services to grid modernization expands cybersecurity risks that may have serious impacts on grid operations. Adopting cybersecurity guidelines are necessary measures that enable organizations to identify vulnerabilities and provide mitigations. This is particularly true for the DER implementations, since there is little history in performing risk assessments for these new technologies for wide-spread critical equipment in sites with minimal security, and for cross-organizational security agreements.

Optimal protection against cyber threats includes a comprehensive risk assessment and application of security measures that are best suited for its environment. Resiliency is built-in through modeling cyber threats and consequences as well as developing mitigations that allow the systems to quickly recover from cyber-attacks. When classifying cyber-attacks and defining defense mechanisms for the grid, the network [wide area network (WAN); neighborhood area network (NAN); home area network (HAN)], application, and data are considered (see Rawat and Bajracharya [B6]). The power system communication network protocols include secure requirements to implement data security over DER network communication while ensuring reliable, secure, and real-time information delivery. Grid systems have highly predictable communications, making monitoring much more feasible and, as such, network monitoring is utilized.

Although there is now general consensus that cybersecurity is absolutely needed in power system operations including for interconnected DER, many challenges exist to actually accomplishing this goal. These challenges include the following:

— Integrating DER in power systems is a relatively new process, with many engineering challenges. The response to being asked to include cybersecurity in a project often is “We just need to get this implementation done, then we’ll add cybersecurity” or “we already have usernames and passwords—we really don’t need anything more.”

Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 18:54:43 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1547.3-2023

— The projects and requirements for implementing DER vary between jurisdictions, which makes consistent implementation difficult, including for cybersecurity measures. Although general cybersecurity standards state what to do, few standards exist on how security could actually be implemented.

— Adding cybersecurity is often expected to cause delays in DER projects since there are few cybersecurity experts available or standardized methods for applying cybersecurity to one-off projects.

— The utility cybersecurity experts, even those that are experienced in power system operations, are not experts in DER equipment or DER site security. Their recommendations may be excessive or not applicable. Most utilities struggle to have the necessary skill set for DER security and there is not enough clear direction in the standards for someone other than an expert to install a secure DER.

— There are very few cybersecurity experts in the DER manufacturer domain, and of those, few are experienced in working with power system cybersecurity requirements. For instance, aggregators may be expert at securing their interactions with their own DER, but have rarely needed to interact closely with utility security systems when providing DER data to the utility or receiving commands from the utility.

— Cybersecurity requirements that cross multiple utilities, DER facilities, aggregators, vendors, implementors, and other DER stakeholders are not well understood. Some questions that are often asked but not yet answered include: What are the real threats and vulnerabilities? What are the potential impacts of possible attacks? What are the inadvertent errors, equipment failures, and natural disasters that could impact the utility's power system reliability and safety? How does a cyber threat or attack on one stakeholder affect the other stakeholders? How can cybersecurity requirements be met between stakeholders? How can implementations be assessed and audited across stakeholders?

Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 18:54:43 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1547.3-2023

— Contractual arrangements with DER manufacturers usually do not address cybersecurity, except with "vague words," such as "cybersecurity will be provided." This can lead to future problems, such as how can DER manufacturers securely continue to interact with their own DER for upgrade and maintenance purposes once they are in the field, or how firmware can be updated securely when these issues were not included in the agreements.

— Except for the NERC Critical Infrastructure Protection (CIP) mandates for large power system elements (e.g., generation plants greater than 75 MW), no general cybersecurity enforcement agent yet exists for mandating and auditing the cybersecurity of smaller DER even if in aggregate they may have major power system impacts.

— Without an external enforcement entity covering these smaller DER, individual utilities are having to develop cybersecurity mandates across all relevant stakeholders, which would need to be written in cross-organizational agreements on cybersecurity requirements, testing, verification over time, auditing, and even penalties.

— The communication protocols used for DER interactions, even those with well-defined security standards, are almost never implemented with their security capabilities. Even if they are purchased with their security capabilities, these are rarely enabled. In addition, testing of the security of these protocols is rarely performed and rarely have true testing and certification programs.

— Cloud computing has become increasingly used for certain types of interactions, particularly for applications involving the collection of large amounts of data that can be stored on third party data centers. For use in DER management, cloud computing users include the utility, the DER facility, any aggregator, the vendor, and potentially the settlement and regulatory entities. Cloud security involves both the security policies and practice of the cloud provider and those of the user. The primary cloud services providers are very sensitive to the security needs of their customers and include very rigorous security measures as part of their services. In some situations, cloud infrastructure may lead to challenges in determining where vulnerabilities are and who is responsible for correcting them.

Documents
Document Sharing Hub
Authorized licensed use limited to: Tsinghua University. Downloaded on February 24,2026 at 18:54:43 UTC from IEEE Xplore. Restrictions apply.
Full document details: IEEE 1547.3-2023