IEC TS 63383

Edition 1.0 2022-11

TECHNICAL SPECIFICATION

colour inside

Cybersecurity aspects of devices used for power metering and monitoring, power quality monitoring, data collection and analysis

iTeh STANDARD PREVIEW
(standards.iteh.ai)
IEC TS 63383:2022
https://standards.iteh.ai/catalog/standards/sist/d4ea4e89-ba2d-4c8a-9988-e5ff8cc1f4de/iec-ts-63383-2022

IEC TS 63383:2022-11(en)

THIS PUBLICATION IS COPYRIGHT PROTECTED
Copyright © 2022 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester. If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

IEC Secretariat
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
info@iec.ch
www.iec.ch

About the IEC
The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications
The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigendum or an amendment might have been published.

IEC publications search - webstore.iec.ch/advsearchform
The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee, …). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished
Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and once a month by email.

IEC Customer Service Centre - webstore.iec.ch/csc
If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: sales@iec.ch.

IEC Products & Services Portal - products.iec.ch
Discover our powerful search engine and read freely all the publications previews. With a subscription you will always have access to up to date content tailored to your needs.

Electropedia - www.electropedia.org
The world's leading online dictionary on electrotechnology, containing more than 22 300 terminological entries in English and French, with equivalent terms in 19 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

iTeh STANDARDS PREVIEW
(standards.iteh.ai)
IEC TS 63383:2022
https://standards.iteh.ai/catalog/standards/sist/d4ea4e89-ba2d-4c8a-9988-e5ff8cc1f4de/iec-ts-63383-2022

IEC TS 63383

Edition 1.0 2022-11

TECHNICAL SPECIFICATION

colour inside

Cybersecurity aspects of devices used for power metering and monitoring, power quality monitoring, data collection and analysis

iTeh STANDARD PREVIEW
(standards.iteh.ai)
IEC TS 63383:2022
https://standards.iteh.ai/catalog/standards/sist/d4ea4e89-ba2d-4c8a-9988-e5ff8cc1f4de/iec-ts-63383-2022

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 17.220.20; 29.240.01

ISBN 978-2-8322-6115-6

Warning! Make sure that you obtained this publication from an authorized distributor.

® Registered trademark of the International Electrotechnical Commission

CONTENTS

FOREWORD 4
INTRODUCTION 6
1 Scope 7
2 Normative references 7
3 Terms, definitions, symbols and abbreviated terms 7
3.1 Definitions related to cybersecurity 7
3.2 Definitions related to devices 11
3.3 Symbols and abbreviated terms 12
4 Security objectives 13
5 Cybersecurity risk assessment (generic approach) 13
5.1 Risk assessment 13
5.2 Risk management 14
5.2.1 General 14
5.2.2 Examples of metrics 14
5.2.3 Examples for prioritization 15
6 Requirements 15
6.1 Overview 15
6.2 Requirements for risk assessment 16
6.3 Requirements for countermeasures 17
6.4 Requirements for testing 17
6.5 Requirements for lifecycle security management 18
6.6 Requirements for instructions of use 18
Annex A (informative) Example of generic risk assessment for PMDs, PQIs, data gateways (DGW), energy data loggers (EDL) and energy servers (ESE) 19
A.1 General 19
A.2 Generic roles 19
A.3 Generic system use-case 19
A.4 Generic functions achieved by devices within a system 20
A.4.1 PMD and PQI devices 20
A.4.2 Data gateways (DGW), energy data loggers (EDL), energy servers (ESE) 21
A.5 Generic assessment of devices within the system 22
A.5.1 Generic list of feared events 22
A.5.2 Generic list of device-feared events 23
A.5.3 Generic list of accesses allowing potential vulnerabilities 25
A.5.4 Generic list of device accesses allowing potential vulnerabilities 26
Annex B (informative) Example of generic countermeasures 27
B.1 General 27
B.2 Recommendations for manufacturers during design phase 27
B.3 Recommendations for manufacturers during manufacturing 27
B.4 Recommendations for manufacturers putting devices on the market 27
B.5 Recommendations for integrators building systems within facilities 27
B.6 Recommendations for commissioning 27
B.7 Recommendations for facility managers operating systems within facilities 28
B.8 Recommendations for facility managers during maintenance 28
B.9 Recommendations for facility managers during de-commissioning 28

iTeh STANDARD PREVIEW
(standards.iteh.ai)
IEC TS 63383:2022
https://standards.iteh.ai/catalog/standards/sist/e4e89-ba2d-4c8a-9982-5ed8cc1f4de/iec-ts-63383-2022

B.10 Recommendations for facility managers during disposal 28
Bibliography 29

Figure 1 – Generic examples for classification of device(s) within an organisational environment 13
Figure 2 – Typical graph of acceptable and non-acceptable risks 15
Figure 3 – Requirements in 5 phases 16
Figure 4 – Examples of device accesses 17
Figure A.1 – Example of generic system use-case 20
Figure A.2 – Example of data processing within DGW, EDL and ESE 22
Figure A.3 – Example of device assets together with its interfaces 26

Table 1 – Example of a simple 3 × 3 risk matrix 15
Table A.1 – Example of generic roles 19
Table A.2 – Kind of data measured by PMD and PQI 21
Table A.3 – Generic device feared events (potential security problems) 23
Table A.4 – Generic device-feared events (security problems) definition 24
Table A.5 – Generic example of device accesses 26

iTeh STANDARD PREVIEW
(standards.iteh.ai)
IEC TS 63383:2022
https://standards.iteh.ai/catalog/standards/sist/d4ea4e89-ba2d-4c8a-9988-e5ff8cc1f4de/iec-ts-63383-2022

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

CYBERSECURITY ASPECTS OF DEVICES USED FOR POWER METERING AND MONITORING, POWER QUALITY MONITORING, DATA COLLECTION AND ANALYSIS

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
IEC TS 63383:2022
https://standards.iteh.ai/catalog/standards/sist/d4ea4e89-ba2d-4c8a-9988-e5ff8cc1f4de/iec-ts-63383-2022

IEC TS 63383 has been prepared by IEC technical committee 85: Measuring equipment for electrical and electromagnetic quantities. It is a Technical Specification.

The text of this Technical Specification is based on the following documents:

Draft	Report on voting
85/832/DTS	85/839/RVDTS

Full information on the voting for its approval can be found in the report on voting indicated in the above table.

The language used for the development of this Technical Specification is English.

This document was drafted in accordance with ISO/IEC Directives, Part 2, and developed in accordance with ISO/IEC Directives, Part 1 and ISO/IEC Directives, IEC Supplement, available at www.iec.ch/members_experts/refdocs. The main document types developed by IEC are described in greater detail at www.iec.ch/publications.

The committee has decided that the contents of this document will remain unchanged until the stability date indicated on the IEC website under webstore.iec.ch in the data related to the specific document. At this date, the document will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

IMPORTANT – The "colour inside" logo on the cover page of this document indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
IEC TS 63383:2022
https://standards.iteh.ai/catalog/standards/sist/d4ea4e89-ba2d-4c8a-9988-e5ff8cc1f4de/iec-ts-63383-2022

INTRODUCTION

This publication can be regarded as a generic document to be referenced for cybersecurity aspects within other TC 85 publications. It contains general information for measuring equipment and related systems used in low-voltage applications for which cybersecurity can be a concern.

The growing use of measuring devices (e.g. power metering and monitoring devices as defined in IEC 61557-12:2018), power quality instruments (defined in IEC 62586-1:2017) and data collection, gathering and analysis devices (e.g. gateways, energy servers, as defined in IEC 62974-1:2017) is being accompanied by a growing increase in cybersecurity risks. This is enhanced by the growing use of interconnected devices in electrical installations.

Thus, maintenance of an acceptable information level for devices and environmental policy should be considered by facility managers to limit the risks. To keep the largest freedom of innovation, good practices when designing devices to withstand cybersecurity threats during its whole lifecycle are preferably based on a risk assessment approach.

This document uses British spelling.

This document follows IEC Guide 120:2018.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
IEC TS 63383:2022
https://standards.iteh.ai/catalog/standards/sist/d4ea4e89-ba2d-4c8a-9988-e5ff8cc1f4de/iec-ts-63383-2022

CYBERSECURITY ASPECTS OF DEVICES USED FOR POWER METERING AND MONITORING, POWER QUALITY MONITORING, DATA COLLECTION AND ANALYSIS

1 Scope

This document deals with cybersecurity related to measuring devices (PMD according to IEC 61557-12 and PQI according to IEC 62586-1) and devices for data collection (devices according to IEC 62974-1) that are intended to be installed in restricted access areas.

This document deals with cybersecurity aspects (e.g. device hardening or device resilience) of device(s) used for power metering and monitoring, power quality monitoring, data collection and analysis, but does not cover requirements for organisational cybersecurity (e.g. end-user security policy).

NOTE Organisational cybersecurity is essential for trustworthy operation of the device(s).

This document is a first attempt to develop awareness by manufacturers and other relevant stakeholders about cybersecurity aspects and provide basic guidance for achieving the appropriate security mitigation against vulnerabilities to security threats:

– in coherence with device/system approaches described in relevant standards such as IEC 62443 (all parts) and ISO/IEC 27001,
– based on generic system use-cases.

This document does not cover billing meters covered by the IEC 62053-2x set of standards.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
IEC TS 63383:2022
https://standards.iteh.ai/catalog/standards/sist/d4ea4e89-ba2d-4c8a-9988-e5ff8cc1f4de/iec-ts-63383-2022

2 Normative references

There are no normative references in this document.

3 Terms, definitions, symbols and abbreviated terms

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at http://www.electropedia.org/
- ISO Online browsing platform: available at http://www.iso.org/obp

3.1 Definitions related to cybersecurity

3.1.1
assets
entities that the owner of a component presumably places value upon

[SOURCE: ISO/IEC 15408-1:2009, 3.1.2, modified – In the definition, "TOE" has been replaced with "component".]

3.1.2
attack
attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset

[SOURCE: ISO/IEC 27000:2018, 3.2]

3.1.3
attack vector
path or means by which an attacker can gain access to a device in order to generate an attack

[SOURCE: ISO/IEC 27032:2012, 4.10, modified – In the definition, "computer or network server" replaced with "device" and "deliver a malicious outcome" with "generate an attack".]

3.1.4
authenticity
property that an entity is what it claims to be

[SOURCE: ISO/IEC 27000:2018, 3.6]

3.1.5
availability
property of being accessible and usable on demand by an authorized entity

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[SOURCE: ISO/IEC 27000:2018, 3.7]

3.1.6
component
smallest selectable set of elements on which requirements may be based

https://standards.iteh.ai/catalog/standards/sist/d4ea4e89-ba2d-4c8a-9988-e5ff8cc1f4de/iec-ts-63383-2022

[SOURCE: ISO/IEC 15408-1:2009, 3.1.12]

3.1.7
confidentiality
property that information is not made available or disclosed to unauthorized individuals, entities, or processes

[SOURCE: ISO/IEC 27000:2018, 3.10]

3.1.8
control
measure that is modifying the risk

Note 1 to entry: Controls include any process, policy, device, practice, or other actions which modify risk.

Note 2 to entry: It is possible that controls do not always exert the intended or assumed modifying effect.

[SOURCE: ISO/IEC 27000:2018, 3.14]

3.1.9
countermeasure
action, device, procedure, or technique that reduces a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken

Note 1 to entry: Other terms such as "measures", "means", "controls" or "mitigations", are also used in other standards instead of "countermeasures".

[SOURCE: IEC TS 62443-1-1:2009, 3.2.33, modified – The Note has been deleted and a new Note to entry has been added.]

3.1.10
cybersecurity
actions required to preclude unauthorized use of, denial of service to, modifications to, disclosure of, loss of revenue from, or destruction of critical systems or informational assets

Note 1 to entry: The objective is to reduce the risk of causing personal injury or endangering public health, losing public or consumer confidence, disclosing sensitive assets, failing to protect business assets or failing to comply with regulations. These concepts are applied to any system in the production process and include both stand-alone and networked components. Communications between systems may be either through internal messaging or by any human or machine interfaces that authenticate, operate, control, or exchange data with any of these control systems. Cybersecurity includes the concepts of identification, authentication, accountability, authorization, availability, and privacy.

[SOURCE: IEC TS 62443-1-1:2009, 3.2.36]

iTeh STANDARD PREVIEW
(standards.iteh.ai)

3.1.11
debug interface
physical interface used by the manufacturer to communicate with the device during development or to perform triage of issues with the device and that is not used as part of the consumer-facing functionality

IEC TS 63383:2022
https://standards.iteh.ai/catalog/standards/sist/d4ea4e89-ba2d-4c8a-9988-e5ff8cc1f4de/iec-ts-63383-2022

EXAMPLE: Test points, UART, SWD, JTAG

[SOURCE: ETSI EN 303 645:2020 V2.1.0]

3.1.12
device hardening
improvement of device ability to withstand a cyberattack by reducing the likelihood of success of an attack

3.1.13
element
indivisible statement of a security need

[SOURCE: ISO/IEC 15408-1:2009, 3.1.24]

3.1.14
event
occurrence or change of a particular set of circumstances

Note 1 to entry: An event can be one or more occurrences and can have several causes.

Note 2 to entry: An event can consist of something not happening.

Note 3 to entry: An event can sometimes be referred to as an "incident" or "accident".

[SOURCE: ISO/IEC 27000:2018, 3.21]

3.1.15
information security
preservation of confidentiality, integrity and availability of information

Note 1 to entry: In addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved.

[SOURCE: ISO/IEC 27000:2018, 3.28]

3.1.16
integrity
property of accuracy and completeness

[SOURCE: ISO/IEC 27000:2018, 3.36]

3.1.17
level of risk
magnitude of a risk expressed in terms of the combination of consequences and their likelihood

[SOURCE: ISO Guide 73:2009, modified – "or combination of risks," has been deleted.]

3.1.18
likelihood
chance of something happening

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[SOURCE: ISO Guide 73:2009]

3.1.19
non-repudiation
ability to prove the occurrence of a claimed event or action and its originating entities

IEC TS 63383:2022
https://standards.iteh.ai/catalog/standards/sist/d4ea4e89-ba2d-4c8a-9988-e5ff8cc1f4de/iec-ts-63383-2022

[SOURCE: ISO/IEC 27000:2018, 3.48]

3.1.20
operational environment
environment in which a component is operated

[SOURCE: ISO/IEC 15408-1:2009, 3.1.48, modified – In the definition, "the TOE" has been replaced with "a component".]

3.1.21
organisational security policy
set of security rules, procedures, or guidelines for an organisation

Note 1 to entry: A policy may pertain to a specific operational environment.

3.1.22
reliability
property of consistent intended behaviour and results

[SOURCE: ISO/IEC 27000:2018, 3.55]

3.1.23
threat
potential cause of an unwanted incident, which can result in harm to a system or organisation

[SOURCE: ISO/IEC 27000:2018, 3.74]