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

IEC TS 63383:2022-11(en)

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 It also gives information on projects, replaced and withdrawn publications.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.

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

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.

CONTENTS

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.

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.

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.

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.

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

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

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

[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]

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

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

[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

[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]

3.1.24
vulnerability
weakness of an asset or control that can be exploited by one or more threats

[SOURCE: ISO/IEC 27000:2018, 3.77]

3.1.25
security functionality
combined functionality of all hardware, software, and firmware of a component that is relied upon for the correct enforcement of the cybersecurity properties

[SOURCE: ISO/IEC 15408-1, 3.1.74, modified – In the definition, "must be" has been replaced with "is", "SFRs" has been replaced with "cybersecurity properties", and "TOE" has been replaced with "component".]

3.2 Definitions related to devices

3.2.1
data gateway
DGW
devices in charge of transmission of information between networks in electrical distribution systems of industrial, commercial and similar plants

[SOURCE: IEC 62974-1:2017, 3.2.3]

3.2.2
energy servers
ESE
devices in charge of computation and retention of energy data, relevant variables, and visualisation through a local display or remote access, in electrical distribution systems of industrial, commercial and similar plants

[SOURCE: IEC 62974-1:2017, 3.2.1]

3.2.3
energy data logger
EDL
devices in charge of logging and exporting information to networks, in electrical distribution systems of industrial, commercial and similar plants

[SOURCE: IEC 62974-1:2017, 3.2.2]

3.2.4
I/O data concentrator
IODC
devices for collection of digital and/or analogue energy data in electrical distribution system of industrial, commercial and similar plants

[SOURCE: IEC 62974-1:2017, 3.2.4]

3.2.5
measuring device
device able to measure energy data

[SOURCE: IEC 62974-1:2017, 3.2.5]

3.2.6
power metering and monitoring device
PMD
combination in one or more devices of several functional modules dedicated to metering and monitoring electrical parameters in energy distribution systems or electrical installations, used for applications such as energy efficiency, power monitoring and network performance

Note 1 to entry: Under the generic term "monitoring" are also included functions of recording, alarm management, etc.

Note 2 to entry: These devices can include demand side quality functions for monitoring inside commercial/industrial installations.

[SOURCE: IEC 61557-12:2018, 3.1.1]

3.2.7
power quality instrument
PQI
instrument whose main function is to measure, record and possibly monitor power quality parameters in power supply systems, and whose measuring methods (class A or class S) are defined in IEC 61000-4-30

[SOURCE: IEC 62586-1:2017, 3.1.1]

3.2.8
billing
process that allows energy suppliers or their representatives to invoice their customers according to a defined contract

Note 1 to entry: These applications can be covered by international standards, regulations such as MID in Europe or NMI in Australia, and/or utility specifications.

[SOURCE: IEC TR 63213:2019, 3.2.4]

3.2.9
sub-billing
process that allows a landlord, property management firm, condominium association, homeowner association or other multi-tenant property to spread out invoice over energy users (assign portions of invoice to users), for measured usages or services

Note 1 to entry: This fee is usually combined with other tenant's facility fees.

Note 2 to entry: The landlord does not commit on the quality of the supply.

[SOURCE: IEC TR 63213:2019, 3.2.5]

3.3 Symbols and abbreviated terms

HMI	Human Machine Interface
USB	Universal Serial Bus
NFC	near-field communication
LAN	local area network
WAN	wide area network
JTAG	Joint Test Action Group (IEEE 1149.1)

4 Security objectives

For devices within electrical distribution systems, the overall security objectives are to ensure they operate as designed and configured, provide trustworthy operation of components and avoid system intrusion which could lead to unintended operations.

For trustworthy operation, the main security aspects to be considered should be detailed in terms of what needs to be protected and how this can be achieved:

– all assets can be subject to different threats (see a generic example in Table A.3);

– assets should be protected appropriately against relevant threats (see a generic example in Table A.4).

Figure 1 provides a generic description of devices, using generic terms, and includes 3 examples of construction, also considering the organisational environment (access policy, password management, etc.).

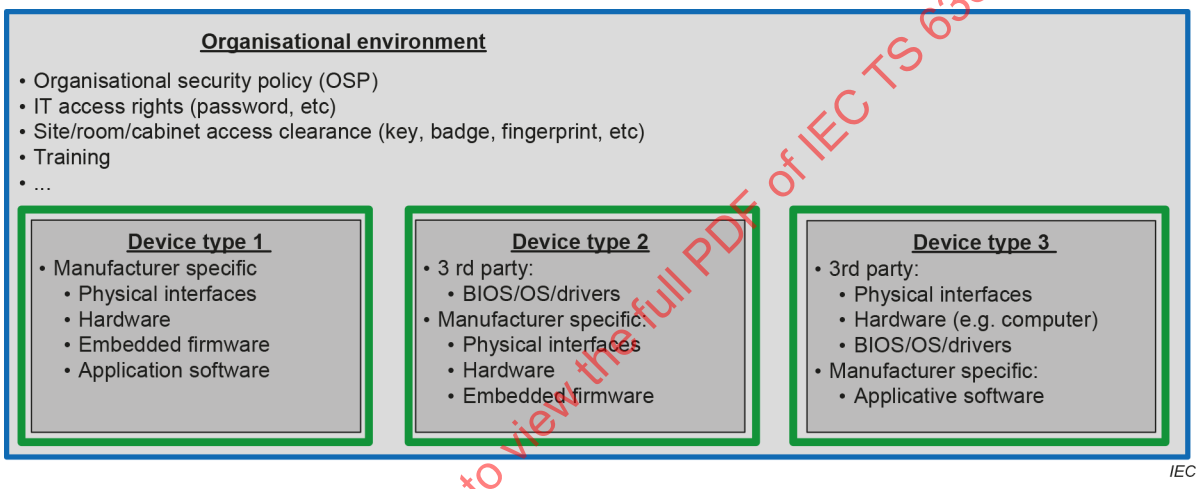

Figure 1 – Generic examples for classification of device(s) within an organisational environment

NOTE Organisational security policy is usually based on an approach specified in standards such as ISO/IEC 27001 and IEC TS 62443-1-1:2009.

Depending on the type of device, the assessment can be different, for example when a component comes from a third-party supplier or is home-made.

5 Cybersecurity risk assessment (generic approach)

5.1 Risk assessment

In general, a generic cybersecurity risk assessment is based on a device for its intended environment. Potential threats and known vulnerabilities should be considered for defining their potential influence and the relevant countermeasures to fulfil the overall security objectives.

NOTE A specific cybersecurity risk assessment is usually conducted by the system integrator and/or facility manager for its operational environment. See Annex B.

All relevant threats and identified vulnerabilities that could affect the trustworthy operation of the device(s) should be considered and documented. Examples of aspects to be considered are:

– data stores and protection;

– interacting external entities;

– internal and external communication protocols implemented in the device;
– interfaces, e.g. accessible physical ports including debug ports;
– circuit board connections such as JTAG connections or debug interfaces which might be used to attack the hardware;
– potential attack vectors including attacks on the hardware, if applicable;
– potential threats, their likelihood, their severity level and possible consequence levels;
– countermeasures for each considered threat;
– security-related issues identified;
– external dependencies in the form of drivers or third-party applications (code that is not developed by the supplier) linked into the application.

The risk assessment should result in the description of:

– the devices under assessment;
– the identified vulnerabilities that could be exploited by threats and result in security risks (including attacks and unintended events resulting from human error);
– the potential consequences resulting from the security risks;
– the countermeasures taken to reduce or manage the threats for each phase of the entire lifecycle.

5.2 Risk management

5.2.1 General

Based on levels of risk acceptance criteria, responses to security risks can be needed to:

– mitigate intolerable security risks by:
  a) designing the security risk out , or
  b) limiting the security risk, or
  c) transferring or sharing the security risk (to another entity);
– or accept the security risk if tolerable.

As a result, a document should be generated describing at least:

– possible consequences, as defined in Table A.4;
– the description of proposed security countermeasure(s);
– possible residual risks.

5.2.2 Examples of metrics

Following the security risk assessment based on threats and vulnerabilities, the levels of risks (combination of likelihood and consequences – see Figure 2) should be determined according to the context.

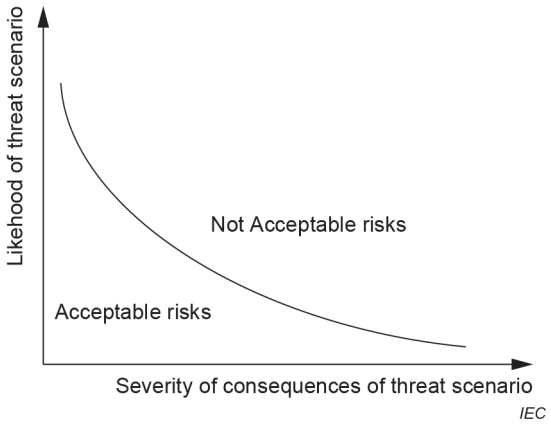

Figure 2 – Typical graph of acceptable and non-acceptable risks

5.2.3 Examples for prioritization

Table 1 shows a simple example of a matrix of possible threat scenarios and associated severity of consequences.

Table 1 – Example of a simple 3 × 3 risk matrix

Likelihood of threat scenario	**Highly likely**	Medium risk	High risk	High risk
	Possible	Low risk	Medium risk	High risk
	Unlikely	Low risk	Low risk	Medium risk
		Negligible	**Moderate**	**Severe**
		Severity of consequences of threat scenarios		

Security countermeasures should be implemented to reduce the risk, according to the level of risk.

6 Requirements

6.1 Overview

The requirements consist of 5 phases, as shown in Figure 3.

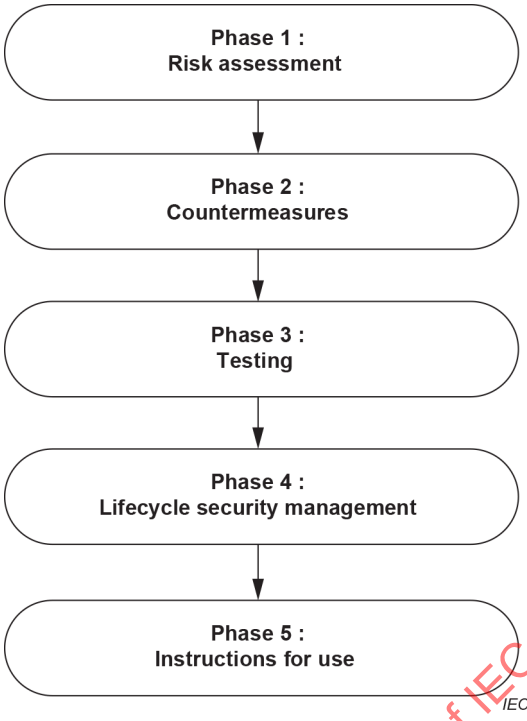

Figure 3 – Requirements in 5 phases

6.2 Requirements for risk assessment

A risk assessment, taking into account assets, threats, accesses and vulnerabilities shall be conducted.

The risk assessment should:

– address the identified security objectives such as integrity, confidentiality and availability;
– identify the threats and assess their level of risk.

Figure 4 provides examples of device accesses (also called "attack surfaces").

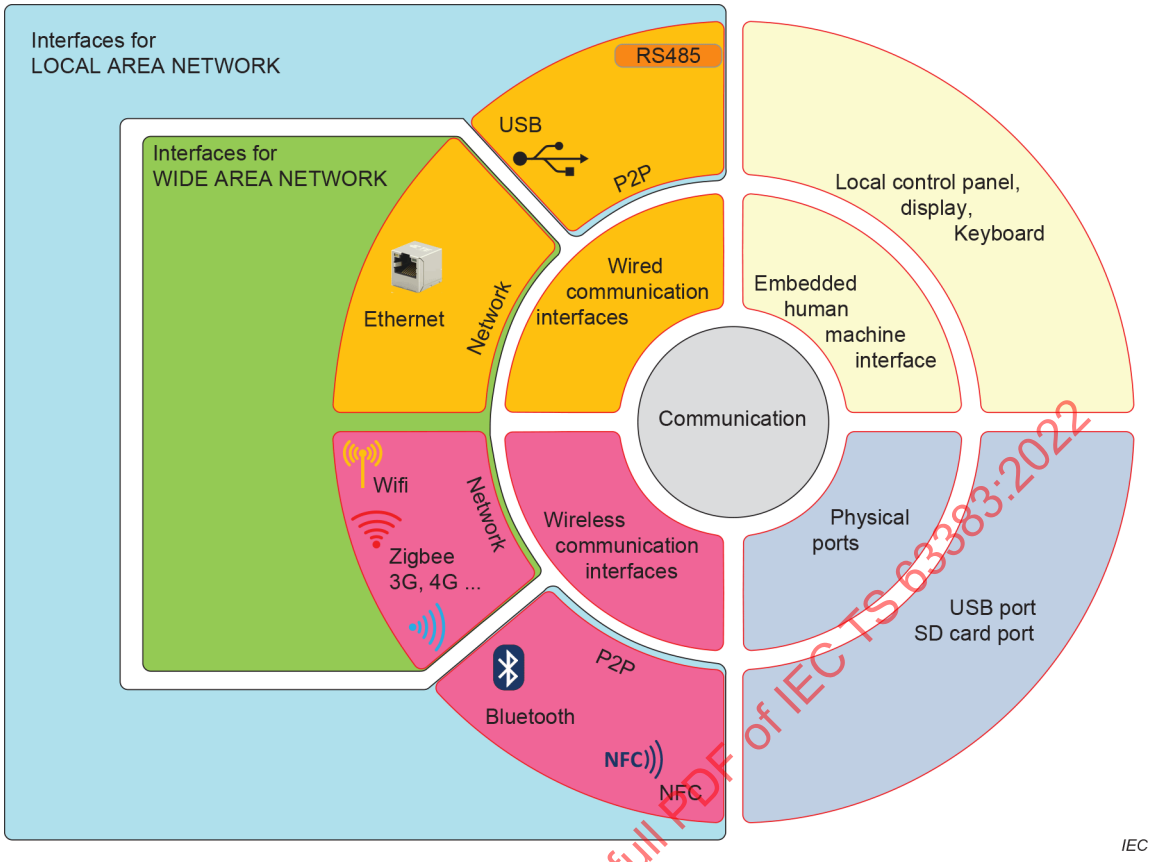

Figure 4 – Examples of device accesses

An example of generic risk assessment for PMD, PQI, energy servers, energy data loggers and energy gateways is described in Annex A.

6.3 Requirements for countermeasures

Based on the results of the risk assessment, the countermeasures should protect the assets taking into consideration the level of risks (see 5.2).

For each identified threat against a given asset:

– a security functionality should be implemented within the device, according to the relevant standard, for example the IEC 62443 series (all parts dealing with devices/components) or ISO/IEC 27402; or

– if the functionality cannot be fulfilled within the device, it should be addressed by countermeasures at an organisational level by a security management system, for example ISO/IEC 27001 or IEC 62443-3-3. This should be documented by the manufacturer.

NOTE In some countries, other standards are also used, such as ETSI EN 303 645 in Europe.

An informative example of countermeasures applied to PMD, PQI, energy servers, energy data loggers and energy gateways is described in Annex B.

6.4 Requirements for testing

To verify that all security functionalities have been implemented, the testing should follow a well-defined and managed process, for example IEC 62443-4-2 or ISO IEC 27402 or a similar standard.

NOTE In some countries, other standards are also used, such as ETSI EN 303 645 in Europe.

6.5 Requirements for lifecycle security management

Protections against security attacks during design, supply chain, manufacturing, delivery, commissioning, maintenance and disposal of the device should be determined based on the results of a risk assessment.

An example of generic countermeasures applied to PMD, PQI, energy servers, energy data loggers and energy gateways is described in Annex B.

6.6 Requirements for instructions of use

Manufacturers should provide all relevant information for installing and configuring the device to reach and maintain the intended security needs. Where functionalities are not implemented within the device, additional organisational countermeasures that might need to be taken, if any, should be documented for a cybersecure integration in the intended systems (e.g. countermeasures during installation, configuration or operation). The same holds true for software upgrades and updates.

Training can also be suggested by the manufacturer.

Annex A
(informative)

Example of generic risk assessment for PMDs, PQIs, data gateways (DGW), energy data loggers (EDL) and energy servers (ESE)

A.1 General

This annex provides a generic assessment that can be used as a template for each assessment for a range of devices.

Clauses A.2 to A.5 provide a generic list of potential assets, threats, feared events, accesses and vulnerabilities, but those lists are not exhaustive.

A.2 Generic roles

Table A.1 provides an example of generic roles. Access mode can be remote or local, or both.

Table A.1 – Example of generic roles

Roles	Description
VIEWER	A viewer can view what objects are present within an intelligent electronic device (IED) by presenting the type and ID of those objects.
OPERATOR	An operator can view what objects and values are present within an IED by presenting the type and ID of those objects as well as perform control actions.
ENGINEER	An engineer can view what objects and values are present within an IED by presenting the type and ID of those objects. Moreover, an engineer has full access to DataSets and Files and can configure the server locally or remotely.
INSTALLER	An installer can view what objects and values are present within an IED by presenting the type and ID of those objects. Moreover, an installer can write files and can configure the server locally or remotely.
SECADM	A security administrator can change subject-to-role assignments (outside the device) and role-to-permission assignment (inside the device) and validity periods; change security setting such as certificates for subject authentication and access token verification
SECAUD	A security auditor can view audit logs
RBACMNT	Role-based access control (RBAC) management can change role-to-permission assignment.
NOTE This description is derived from IEC 62351-8.	

A.3 Generic system use-case

Figure A.1 provides a generic system use-case that is used in this informative annex.

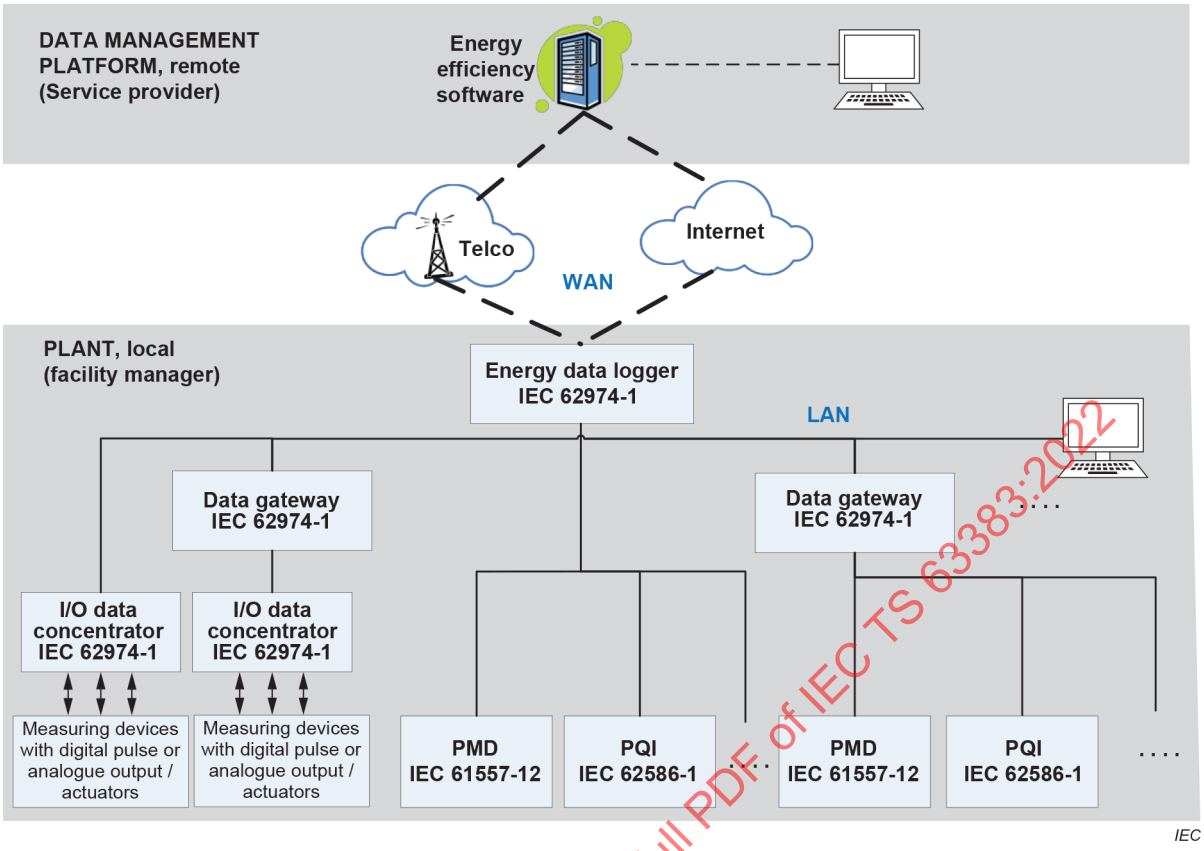

Figure A.1 – Example of generic system use-case

A.4 Generic functions achieved by devices within a system

A.4.1 PMD and PQI devices

Table A.2 shows the different kind of data measured by PMD and PQI.

Table A.2 – Kind of data measured by PMD and PQI

		Kind of device, related standard, and main measurement functions		
		Billing meter (IEC 62053-2x) Energies	**PMD (IEC 61557-12)** Energies + electrical parameters	**PQI (IEC 62586-1)** Power quality parameters
Applications	**Sub applications**			
Billing	Billing	Billing meter	N/A	N/A
Cost management (Part of Energy management)	Sub-billing (tenant billing)	Billing meter when a regulation requests legal metrology	PMD [a], when installed in LV assemblies or panels [c]	N/A
	Utility bill verification	N/A	PMD [a]	N/A
	Cost allocation	N/A	PMD [a]	N/A
Energy efficiency (Part of Energy management)	Energy usage analysis	N/A	PMD [a]	N/A
	Energy performance analysis	N/A	PMD [a]	N/A
Power monitoring	Network & load monitoring	N/A	PMD [a]	N/A
	Demand side power quality	N/A	PMD [a], when features are sufficient, and when installed in LV assemblies or panels [c]	PQI-S or PQI-A [b], when PQ features are requested, or when installed in MV/HV cubicles [d]
Grid power quality	Grid power quality monitoring	N/A	N/A	PQI-S or PQI-A [b]
	Grid power quality compliance	N/A	N/A	PQI-A [b]

[a] PMD-I, PMD-II and PMD-III are three categories of Power Metering and Monitoring Devices (PMD) defined in IEC 61557-12.

[b] PQI-A and PQI-S are two categories of Power Quality Instruments (PQI) defined in IEC 62586-1.

[c] LV assemblies are usually dense and include heating devices, then temperature can go up to 55°C or even 70 °C. See K55 and K70 classes of IEC 61557-12.

[d] MV/HV cubicles are usually subject to harsh EMC environments. See environmental classes of IEC 62586-1.

NOTE N/A stands for Not Applicable. The bolded boxes reflect the applicable cases.

A.4.2 Data gateways (DGW), energy data loggers (EDL), energy servers (ESE)

These devices intend to manage data provided by PMDs and PQIs according to the below Figure A.2 described in IEC 62974-1:

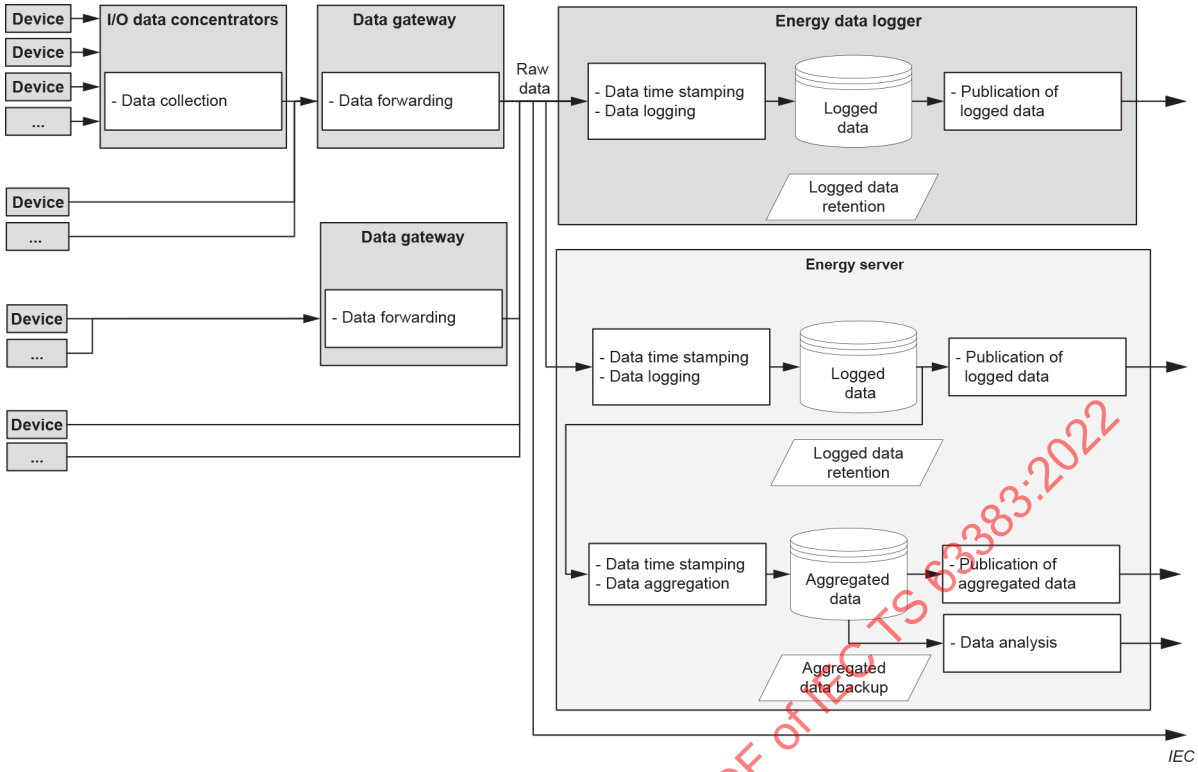

Figure A.2 – Example of data processing within DGW, EDL and ESE

A.5 Generic assessment of devices within the system

A.5.1 Generic list of feared events

A list of examples of feared events (FEIxx, FEAxx, FECxx), resulting from a combination of assets and possible threats is provided in Table A.3. These feared events are further described in Table A.4.

Table A.3 – Generic device feared events (potential security problems)

Generic asset categories	Generic device assets	Generic device threats		
		C [b]	I [b]	A [b]
		Unauthorized access to data	Unwanted change of data	Unwanted change in operations (stop, reboot, ...)
1. Application data (e.g. Measured data)	Sub-billing data	FEC_11	FEI_11	FEA_11
	Cost-management data	FEC_12	FEI_12	---
	Energy efficiency data	---	FEI_13	---
	Power Monitoring data	---	FEI_14	FEA_14
	Grid power quality data	---	FEI_15	---
2. Settings data	End-user settings	---	FEI_21	---
	End-user configuration	---	FEI_22	---
	Time	---	FEI_23	---
3. Security data	Encryption codes and keys, ...	FEC_31	FEI_31	---
	RBAC with passwords and backdoor passwords	FEC_32	FEI_32	---
	Logs	FEC_33	FEI_33	---
	Time stamping functions (for security)	---	FEI_34	---
4. Embedded Firmware or applicative software	Measurement functions	---	FEI_41	---
	Logging functions (storage)	---	FEI_42	---
	Power monitoring functions (including alarming)	---	FEI_43	---
	Time stamping functions (for measurement)	---	FEI_43	---
	By-default settings	---	FEI_44	---
	Display applications with HMI interface	---	FEI_45	---
	Secure reboot capability to ensure unaffected operational system (e.g. to install firmware applications securely, or upload update of firmware into memory)	---	FEI_46	---
5. Third party components	Commercial Operating Systems (for instance Windows or Unix or Linux, ..) running a software on a computer	Assessment needs to be performed by the vendor		
	Commercial embedded Operating Systems running a firmware on a dedicated main Board	Assessment needs to be performed by the vendor		

[a] Security risk assessment should be preferably based on an approach such as in ISO/IEC 27005 and IEC TS 62443-1-1:2009.

[b] C stands for confidentiality; I stands for integrity; A stands for availability, see definitions.

A.5.2 Generic list of device-feared events

This list of device-feared events is provided in Table A.4, resulting from Table A.3.

Table A.4 – Generic device-feared events (security problems) definition

FE n°	Feared event (security problem) description
FEC_11	Sub-billing data can represent the consumption of a facility or of a workshop, then can reflect the activity of a company.
	The loss of confidentiality of sub-billing data can harmfully affect the competitive advantage of an operator via disclosure resulting from unauthorised access.
FEI_11	Sub-billing data can be used for charging fees. Any change in this data leads to customers being over-charged or under-charged.
	The loss of integrity of sub-billing data can harmfully affect the accounting of an operator via unauthorised modification.
FEA_11	Sub-billing data are integrated into the sub-billing calculations of the devices sold. False data can skew these calculations.
	The loss of availability of sub-billing data can harmfully affect the accounting of an operator via unauthorised modification.
FEC_12	Energy cost management data are confidential data and impact the profitability of companies. Analysis of these data provides information on manufacturing processes, for example.
	The loss of confidentiality of cost management data can harmfully affect the competitive advantage of an operator via disclosure resulting from unauthorised access.
FEI_12	Energy cost management data are integrated into the cost calculations of the devices sold. False data can skew these calculations.
	The loss of integrity of cost management data can harmfully affect the accounting of an operator via unauthorised modification.
FEI_13	Energy efficiency data are the basis for calculating the indicators of energy performance actions implemented in organizations. False data can impact these indicators.
	The loss of integrity of energy efficiency data can affect the operations via unauthorised modification.
FEI_14 FEA_14	False alarming outputs from monitoring (based on data) functions or incorrect display of measured values can impact the availability of the installation.
	The loss of integrity or availability of monitoring data can harmfully affect the operations via unauthorised modification.
FEI_15	Grid power quality data have a direct impact on the reliability of the electrical installation. False data can provide production losses.
	The loss of integrity of power quality data can affect the operations via unauthorised modification.
FEI_21	Unwanted change of the end-user setting can result in an unexpected situation.
	The loss of integrity of end-user setting data can harmfully affect the operations via unauthorised modification.
FEI_22	Unwanted change of the end-user configuration can result in an unexpected situation.
	The loss of integrity of end-user configuration can harmfully affect the operations via unauthorised modification.
FEI_23	Unwanted change of the time can result in an unexpected situation.
	The loss of integrity of time can harmfully affect the operations via unauthorised modification.
FEC_31	Access to encryption codes and keys, specifically on private key, compromised confidentiality of all the system. Strategic data can be read.
	The loss of confidentiality of cryptographic data can harmfully affect the competitive advantage of an operator via disclosure resulting from unauthorised access as well as the operations via loss of management capabilities.
FEI_31	Modification of encryption codes and keys can result in a chaotic situation.
	The loss of integrity of cryptographic data can harmfully affect the competitive advantage of an operator.
FEC_32	Fraudulent or accidental access to RBAC with passwords and backdoor passwords can provide a global access to the system and a loss of confidentiality.
	The loss of confidentiality of access control data or the existence of access control backdoors can harmfully affect the operations via unintended authorised access.

FE n°	Feared event (security problem) description
FEI_32	Modification of RBAC with passwords and backdoor passwords can lead to a global system crash (change of administrator password for example).
	The loss of integrity of access control data can harmfully affect the operations via unauthorised modification of access control settings.
FEC_33	Access to logs, specific on system events, provides a loss of confidentiality.
	The loss of confidentiality of logging data can be used for further unauthorised access or modification attempts.
FEI_33	Modification of the recorded events can hide fraudulent access. Integrity of the system can be lost.
	The loss of integrity of logging data can be used to obfuscate unauthorised access or modification attempts.
FEI_34	Change of stamping time can hide fraudulent access and destroy integrity of the measured data (sub-billing function).
	The loss of integrity of time stamping data leads to irregular status regarding operations, reactions, measurements, accounting, etc.
FEI_41	Unwanted change of firmware can affect the quality of measurement functions and cause untimely shutdowns.
	Unauthorized access to firmware can affect the accuracy of measurement functions. If it is access to source code, then it is a catastrophe. This should reasonably not be considered.
FEI_42	Logging functions (storage). Unwanted change of logged information can affect the correct forensic reconstruction of the system's behaviour.
	The loss of integrity of logging data leads to irregular status regarding operational parameters, reactions, measurements etc.
FEI_43	Power monitoring functions (including alarming). Unwanted change of monitored information and the reactions based thereupon can affect the stability of the system's behaviour.
	The loss of integrity of monitoring functions leads to irregular status regarding operational parameters, reactions, measurements etc.
FEI_44	By-default settings. Unwanted change of by-default settings can affect the correct starting point for the reconstruction of the system's configuration.
	The loss of integrity of by-default settings leads to irregular status e.g. after a reset.
FEI_45	Display applications with HMI interface. Unwanted change of displayed information and inappropriate reactions based thereupon can affect the system's intended behaviour.
	The loss of integrity of HMI functions leads to irregular status e.g. after an inappropriate reaction based thereupon.
FEI_46	The loss of integrity of installed firmware leads to irregular status regarding operations, reactions, measurements, accounting etc. Unauthorised FW updates should not be possible.
	Unauthorized access to firmware can affect the accuracy of measurements functions. If it is access to source code, then it is a catastrophe. This should reasonably not be considered.
NOTE The first line represents the operational situation, the second represents the correlation between threats and assets.	

A.5.3 Generic list of accesses allowing potential vulnerabilities

A generic list of device accesses together with the related device vulnerabilities is provided in Figure A.3 and in in Table A.5.