# IEC GUIDE 120

Edition 2.0 2023-10
REDLINE VERSION

# GUIDE

colour
inside

## Security aspects – Guidelines for their inclusion in publications

IECNORM.COM : Click to view the full PDF of IEC GUIDE 120:2023 RLV

**THIS PUBLICATION IS COPYRIGHT PROTECTED**
**Copyright © 2023 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 It also gives information on projects, replaced and withdrawn publications.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.

IECNORM.COM : Click to view the full PDF of IEC GUIDE 120:2023 RLV

IEC®

# IEC GUIDE 120

Edition 2.0 2023-10
REDLINE VERSION

# INTERNATIONAL STANDARD

colour inside

IECNORM.COM : Click to view the full PDF of IEC GUIDE 120:2023 RLV

## Security aspects – Guidelines for their inclusion in publications

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 35.030 ISBN 978-2-8322-7676-1

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

® Registered trademark of the International Electrotechnical Commission

## CONTENTS

IECNORM.COM : Click to view the full PDF of IEC GUIDE 120:2023 RLV

IECNORM.COM : Click to view the full PDF of IEC GUIDE 120:2023 RLV

INTERNATIONAL ELECTROTECHNICAL COMMISSION

____________

# SECURITY ASPECTS – GUIDELINES FOR THEIR INCLUSION IN PUBLICATIONS

## 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.

**This redline version of the official IEC Standard allows the user to identify the changes made to the previous edition IEC Guide 120:2018. A vertical bar appears in the margin wherever a change has been made. Additions are in green text, deletions are in strikethrough red text.**

IECNORM.COM : Click to view the full PDF of IEC GUIDE 120:2023 RLV

This second edition of IEC Guide 120 has been prepared, in accordance with ISO/IEC Directives, Part 1, Annex A, by the Advisory Committee on Information security and data privacy (ACSEC).

This second edition cancels and replaces the first edition published in 2018.

The main changes with respect to the previous edition are as follows:

a) The terminology of IEC Guide 120 has been aligned with the terminology of IEC Guide 108:2019.

The text of this Guide is based on the following documents:

| Draft | Report on voting |
|---|---|
| SMBNC/39/DV | SMBNC/47/RV |

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

The language used for the development of this Guide is English.

This publication has been drafted in accordance with the 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/standardsdev/publications.

**IMPORTANT – The 'colour inside' logo on the cover page of this publication 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.**

IECNORM.COM : Click to view the full PDF of IEC GUIDE 120:2023 RLV

# INTRODUCTION

The increasing complexity and connectivity of systems, products, processes and services entering the market requires that the consideration of security aspects be given a high priority. Inclusion of security aspects in standardization provides protection from and response to risks of unintentionally and intentionally caused events that can disrupt the functionality and operation of products and systems.

When preparing publications, committees should ensure that relevant resilience requirements applicable to their application domain are included. Security aspects will in many cases play a role in achieving resilience directed standards.

In this document, the term "committee", includes technical committees, subcommittees and systems committees. The term "publication" includes "International Standard", "Technical Report", "Technical Specification" and "Guide".

National ~~laws (legislation and regulation) may override~~ legal and regulatory requirements can exist that impact the general application of publications.

NOTE Publications can deal exclusively with security aspects or can include clauses specific to security.

IECNORM.COM : Click to view the full PDF of IEC GUIDE 120:2023 RLV

# SECURITY ASPECTS – GUIDELINES FOR THEIR INCLUSION IN PUBLICATIONS

## 1 Scope

This document provides guidelines on the security ~~topics to be covered~~ aspects included in IEC publications, and ~~aspects of~~ how to implement them. These guidelines can be used as a checklist for the combination of publications used in implementation of systems.

This document includes what is often referred to as "cybersecurity".

This document excludes non-electrotechnical aspects of security such as societal security, except where they directly interact with electrotechnical security.

NOTE The IEC Standardization Management Board (SMB) has decided that Guides such as this one can have mandatory requirements which shall be followed by all IEC committees developing technical work that falls within the scope of the Guide, as well as guidance which may or may not be followed. Any mandatory requirements in this Guide are identified by the use of "shall". Statements that are only for guidance are identified by using the verb "should". (See ISO/IEC Directives, IEC Supplement:2021, A.1.1.)

## 2 Normative references

~~The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.~~

~~ISO/IEC Directives Part 2:2018, *Principles and rules for the structure and drafting of ISO and IEC documents*~~

There are no normative references in this document

## 3 Terms and definitions

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

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

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

**3.1**
**accountability**
property of a system (including all of its system resources) that ensures that the actions of a system entity ~~may~~ can be traced uniquely to that entity, which can be held responsible for its actions

[SOURCE: IEC TS 62443-1-1:2009, 3.2.3]

IECNORM.COM : Click to view the full PDF of IEC GUIDE 120:2023 RLV

**3.2**
**attack**
attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset

[SOURCE: ISO/IEC 27000:~~2016~~2018, 3.2]

**3.3**
**authentication**
provision of assurance that a claimed characteristic of an entity is correct

[SOURCE: ISO/IEC 27000:~~2016~~2018, 3.5]

**3.4**
**authorization**
right or permission that is granted to a system entity to access a system resource

[SOURCE: IEC TS 62443-1-1:2009, 3.2.14]

**3.5**
**availability**
property of being accessible and usable upon demand by an authorized entity

[SOURCE: ISO/IEC 27000:~~2016~~2018, 3.7]

**3.6**
**confidentiality**
property that information is not made available or disclosed to unauthorized individuals, entities, or processes

[SOURCE: ISO/IEC 24767-1:2008, 2.1.2]

**3.7**
**functional safety**
part of the overall safety that depends on functional and physical units operating correctly in response to their inputs

[SOURCE: IEC 60050-351:2013, 351-57-06]

**3.8**
**harm**
injury or damage to the health of people, or damage to property or the environment

[SOURCE: ISO/IEC Guide 51:2014, 3.1]

**3.9**
**integrity**
property of accuracy and completeness

[SOURCE: ISO/IEC 27000:~~2016~~2018, 3.36]

**3.10**
**non-repudiation**
ability to prove the occurrence of a claimed event or action and its originating entities

[SOURCE: ISO/IEC 27000:~~2016~~2018, 3.48]

IECNORM.COM : Click to view the full PDF of IEC GUIDE 120:2023 RLV

**3.11**
**risk**
combination of the probability of occurrence of harm and the severity of that harm

Note 1 to entry: The probability of security risks often cannot be determined in the same way as the probability of safety hazards based on statistical analysis.

[SOURCE: IEC 60050-351:2013, 351-57-03, modified – Note 1 to entry has been added.]

**3.12**
**safety**
freedom from risk which is not tolerable

[SOURCE: ISO/IEC Guide 51:2014, 3.14]

**3.13**
**security**
condition that results from the establishment and maintenance of protective measures that ensure a state of inviolability from hostile acts or influences

Note 1 to entry: Hostile acts or influences could be intentional or unintentional.

Note 2 to entry: In actual usage, "security" and "cybersecurity" are often used interchangeably, even if technically, "cybersecurity" can be considered different from "security". However, this document does not make distinction between these terms.

[SOURCE: IEC TS 62351-2:2008, 2.2.173, modified – Notes 1 and 2 to entry have been added.]

**3.14**
**security control**
~~measure (including process, policy, device, practice or other action) which modifies security risk or use~~

measure which modifies security risk or use

Note 1 to entry: A security control can be a process, policy, device, practice or other action.

**3.15**
**security service**
mechanism used to provide confidentiality, data integrity, authentication, or non-repudiation of information

[SOURCE: IEC TS 62443-1-1:2009, 3.2.115]

**3.16**
**threat**
potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm

[SOURCE: IEC TS 62443-1-1:2009, 3.2.125]

**3.17**
**vendor**
manufacturer or distributor of a product

[SOURCE: IEC 62337:2012, 3.12, modified – In the definition, "piece of equipment/ instrument/package unit" has been replaced with "product".]

IECNORM.COM : Click to view the full PDF of IEC GUIDE 120:2023 RLV

**3.18**
**vulnerability**
flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy

Note 1 to entry: This definition of vulnerability should not be confused with the term vulnerability when used in the context of general risk management, where it encompasses the notion of possibility of exposition to a risk.

[SOURCE: IEC TR 62918:2014, 3.16, modified – Note 1 to entry has been added.]

# 4 Guide to terminology

## 4.1 General

There are already many security-related terms and definitions in existing publications. Therefore, before defining a new term, existing terms and definitions should be checked first. Primary recommended sources are shown in 4.2 and they should be used in preference to the other relevant sources shown in 4.3. If no appropriate term and definition is found in those sources, either modify an existing one or define a new one.

Definitions in this document are not intended to be generic ones but only apply to this document.

The ISO/IEC Directives Part 2:~~2018~~2021, Clause 16, defines how the terms and definitions in IEC publications are drafted.

NOTE The same term ~~might~~ can have different definitions depending on the context in which it is used, or different terms ~~might~~ can be used for the same or similar meaning in different application domains.

## 4.2 Primary recommended sources

The primary recommended sources are

a) IEC 60050 (all parts) (IEV) [1][1],

a) IEC Glossary [2], and

b) ISO/IEC JTC 1/SC 27 SD6 [3],

where IEC 60050 and the IEC Glossary should be used in preference.

IEC 60050 provides representative definitions to more than 20 000 terms, organized by subject areas in IEC. The IEC Glossary is a compilation of electrotechnical terms extracted from the "Terms and definitions" clause in existing IEC publications.

If no appropriate term or definition is found in the two sources above, ISO/IEC JTC 1 SC 27 SD6, which covers more security-related terms and definitions, should be consulted.

NOTE Application-domain specific terms developed by IEC committees are also considered to be primary sources. These can be searched using the web page of the IEC Glossary.

## 4.3 Other relevant sources

### 4.3.1 General

There are a variety of resources available which focus on certain application domains of electrotechnology such as energy, building, healthcare, and transportation.

[1] Numbers in square brackets refer to the Bibliography.

IECNORM.COM : Click to view the full PDF of IEC GUIDE 120:2023 RLV

This includes application-domain independent sources (4.3.2) and application-domain specific sources (4.3.3).

### 4.3.2 Other application-domain independent sources

- IETF RFC 4949 [4];
- NISTIR 7298 [5];
- IEEE, Standards Glossary [6];
- ITU, ITU Terms and Definitions [7].

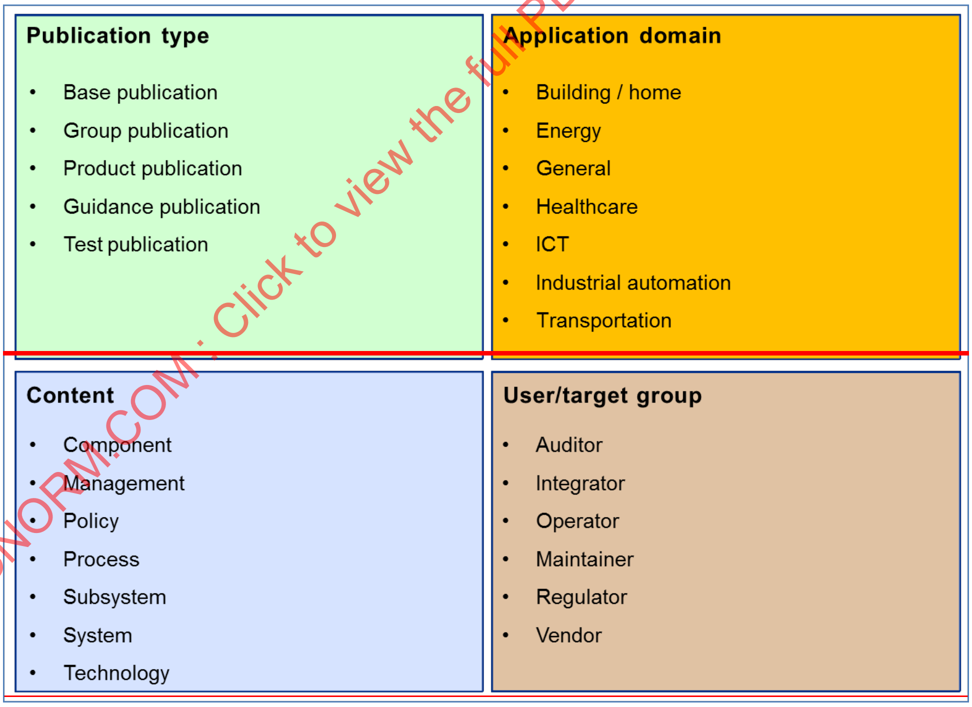
### 4.3.3 Other application-domain specific sources

- Healthcare: HL7, Glossary Of Acronyms, Abbreviations and Terms Related To Information Security In Healthcare Information Systems [8].
- Nuclear: IAEA, Nuclear Security Series Glossary [9].
- Energy: IEA, Glossary [10].

## 5 Categorization of publications

### ~~5.1 Overview~~

~~There are several different ways in which security publications can be categorised. Four possible aspects for the categorization are shown in Figure 1. Publications can belong to more than one category. Each category is identified by combination types of each aspect.~~



**Publication type**

- Base publication
- Group publication
- Product publication
- Guidance publication
- Test publication

**Application domain**

- Building / home
- Energy
- General
- Healthcare
- ICT
- Industrial automation
- Transportation

**Content**

- Component
- Management
- Policy
- Process
- Subsystem
- System
- Technology

**User/target group**

- Auditor
- Integrator
- Operator
- Maintainer
- Regulator
- Vendor

~~Figure 1 – Possible categorization of publications~~

### ~~5.2 Publication type~~

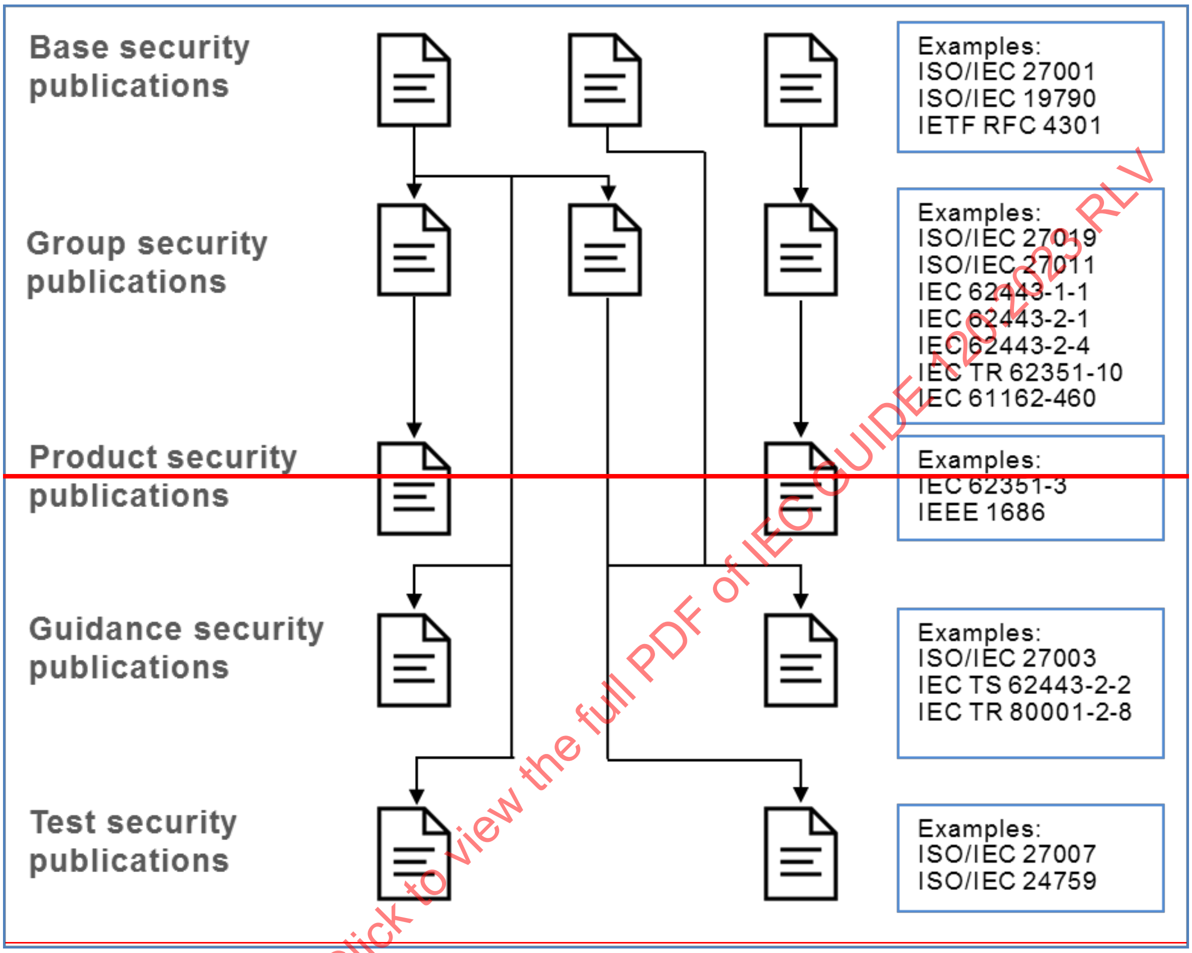
#### ~~5.2.1 General~~

~~Publications for security can be categorised as one of the five types listed below, as shown in Figure 2:~~

- ~~base security publication;~~

IECNORM.COM : Click to view the full PDF of IEC GUIDE 120:2023 RLV

- ~~group security publication;~~
- ~~product security publication;~~
- ~~guidance security publication;~~
- ~~test security publication.~~



~~NOTE The examples listed in Figure 2 are not exhaustive.~~

~~**Figure 2 – Types of publications**~~

### ~~5.2.2 Base security publications~~

~~Base security publications are publications that define some aspect of security, in a generic manner.~~

~~Base security publications deal with fundamental concepts, principles and requirements with regard to general security aspects applicable to a wide range of products and systems. Horizontal standards dealing with security, as defined in IEC GUIDE 108 [14], are base security publications.~~

### ~~5.2.3 Group security publications~~

~~Group security publications show how to apply security in one of the application domains. To do this, they may reference or customise base security publications. They are equivalent to group publications as defined in IEC GUIDE 104 [13] for safety applications.~~

~~Group security publications may be applicable to many products or systems, or families of similar products or systems.~~

IECNORM.COM : Click to view the full PDF of IEC GUIDE 120:2023 RLV

~~Group security publications are sometimes referred to as sector-specific security publications.~~

### ~~5.2.4 Product security publications~~

~~Product security publications define how to apply base security publications or group security publications for a particular type of product. They ensure that different products can interact or interoperate securely, and can be controlled and managed in a uniform manner.~~

~~Product security publications should as far as possible define their requirements by reference to base security publications and group security publications.~~

~~NOTE In this context, the term product includes items such as process, service, installation, and combinations thereof.~~

### ~~5.2.5 Guidance security publications~~

~~Guidance security publications should not contain requirements. They explain how to implement base publications, and group or product publications.~~

~~In some application areas, guidance publications are not used. Instead necessary guidance information is provided through informative annexes within the relevant requirements standard.~~

### ~~5.2.6 Test security publications~~

~~Test security publications define ways to determine that the requirements of base publications, and group or product publications have been correctly implemented.~~

~~Test publications typically have a specialised audience and often make reference to conformity assessment. They may define or identify reference implementations that can be used to determine correct implementation through successful interoperation.~~

### ~~5.2.7 Relationship between types of security publications~~

~~The relationship between these different types of publications is shown in Figure 2. There is an equivalent figure for safety publications in Annex B of IEC GUIDE 104:2010 [13].~~

### 5.1 Overview

There are several different ways in which security publications can be categorized. Five possible classes for the categorization are considered as shown in Table 1:

- Publication categories;
- Publication types;
- Application domain;
- Content;
- User or target group;

Publications can belong to more than one class.

This document provides complementary information to IEC Guide 108 when referring to horizontal security publications.

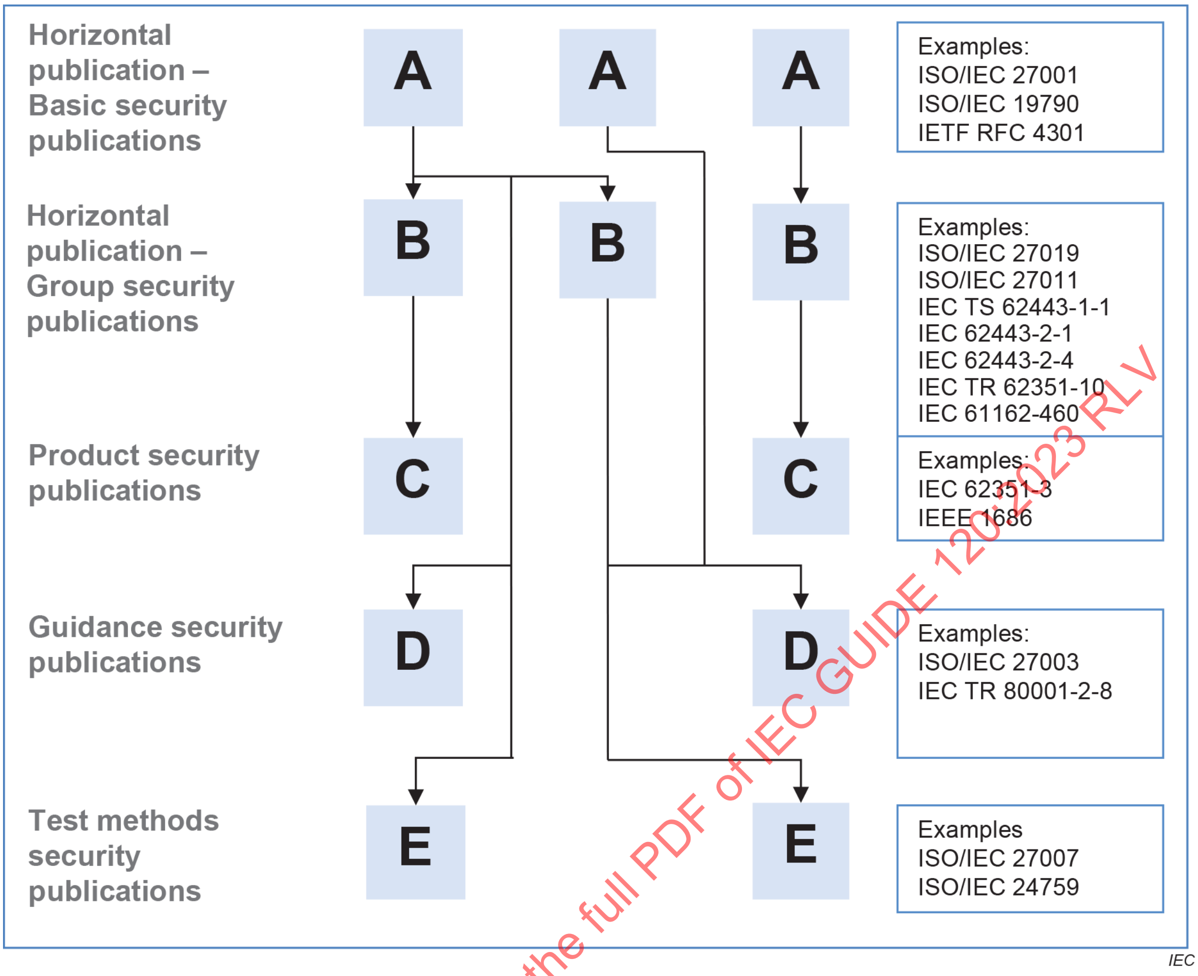
IECNORM.COM : Click to view the full PDF of IEC GUIDE 120:2023 RLV

**Table 1 – Possible categorization of publications**

| | |
|---|---|
| **Publication categories** | Horizontal publication – Basic security publications (applicable to any domain)<br>Horizontal publication – Group security publications (applicable to one or several specified domains)<br>Product security publications |
| **Publication types** | Guidance security publications (which could be horizontal publications or not)<br>Test methods security publications (which could be horizontal publications or not)<br>Configuration |
| **Application domain** | • Building<br>• Energy<br>• General<br>• Healthcare<br>• ICT<br>• Industrial automation<br>• Transportation |
| **Content** | • Component<br>• Management<br>• Policy<br>• Process<br>• Subsystem<br>• System<br>• Technology |
| **User or target group** | • Auditor<br>• Integrator<br>• Operator<br>• Maintainer<br>• Regulator<br>• Vendor |

Figure 1 shows some examples of security publications listed according to the proposed classes.

IECNORM.COM : Click to view the full PDF of IEC GUIDE 120:2023 RLV



NOTE The examples listed in Figure 1 are not exhaustive.

**Figure 1 – Examples of publications according to different categorization classes**

IECNORM.COM : Click to view the full PDF of IEC GUIDE 120:2023 RLV

## 5.2 Publication categories

### 5.2.1 General

"Publication categories" stems from IEC Guide 108:2019 and extends the definition of the different categories proposed for horizontal publications to fully consider the security aspect context. The publication categories considered in this document are:

- Horizontal publication – Basic security publications (applicable to any domain);
- Horizontal publication – Group security publications;
- Product security publications.

### 5.2.2 Horizontal publication – Basic security publications (applicable to any domain)

"Horizontal publication – Basic security publications" deal with fundamental concepts, principles and requirements with regard to general security aspects applicable to a wide range of products and systems, and are applicable to any domain.

### 5.2.3 Horizontal publication – Group security publications

"Horizontal publication – Group security publications" show how to apply security in one of the application domains. To do this, they may reference or customize existing "Horizontal publication – Basic security publications".

"Horizontal publication – Group security publications" may be applicable to many products or systems, or families of similar products or systems.

"Horizontal publication – Group security publications" can be referred to as sector-specific security publications.

#### 5.2.4 Product security publications

"Product security publications" define how to apply "Horizontal publication – Basic security publications" or "Horizontal publication – Group security publications" for a particular type of product. They ensure that different products can interact or interoperate securely, and can be controlled and managed in a uniform manner.

"Product security publications" should as far as possible define their requirements by reference to "Horizontal publication – Basic security publications" or "Horizontal publication – Group security publications".

NOTE In this context, the term "product" includes items such as process, service, installation, and combinations thereof.

### 5.3 Publication types

#### 5.3.1 General

"Publication types" stems from IEC Guide 108:2019 and extends the definition of the different types proposed for horizontal publications to fully consider the security aspect context. The proposed types considered in this document are:

- Guidance security publications;
- Test methods security publications.

#### 5.3.2 Guidance security publications

"Guidance security publications" should not contain requirements. They explain how to implement "Horizontal publication – Basic security publications", "Horizontal publication – Group security publications" or product security publications.

In some application areas, guidance security publications are not used. Instead, necessary guidance information is provided through informative annexes within the relevant requirements standard.

#### 5.3.3 Test methods security publications

"Test methods security publications" define ways to determine that the requirements of "Horizontal publication – Basic security publications", and "Horizontal publication – Group security publications" or product security publications have been correctly implemented.

Test methods security publications typically have a specialized audience and often make reference to conformity assessment. They may define or identify reference implementations that can be used to determine correct implementation through successful interoperation.

### 5.4 Application domain

Publications for security can also be categorized according to their intended domain of application. This ~~may~~ can be a sector of economic or industrial activity, a type of market, or an area of application.

Some examples of application domains are listed below, as shown in Figure 1:

- building~~/home~~;

IECNORM.COM : Click to view the full PDF of IEC GUIDE 120:2023 RLV

- energy;
- general;
- healthcare;
- ICT;
- industrial automation;
- transportation.

In many cases an application domain will have an associated IEC committee responsible for the development of publications for that domain. This committee should accept responsibility for the development of the associated security publications.

Such committees will normally be able to define relevant threat models and security use cases independently, but ~~may~~ it is possible that they will need to seek advice from the committees responsible for ~~base security publications~~ "Horizontal publication – Basic security publications" in configuring or customizing those ~~base~~ basic security publications when referenced.

### 5.5 Content

Publications for security can also be grouped by their type of content.

Some examples of possible groups are listed below, as shown in Figure 1:

- component;
- management;
- policy (not in IEC);
- process;
- subsystem;
- system;
- technology.

For example, electrotechnical standards for information security management include the ~~generic~~ "Horizontal publication – Basic security publications" standard ISO/IEC 27001 [11] (developed by ISO/IEC JTC 1/SC 27), but also the sector-specific standards ISO/IEC 27019 [12] (developed by ISO/IEC JTC 1/SC 27), IEC 62443-2-1 [13] (developed by IEC TC 65) and IEC 62645 [14] (developed by IEC SC 45A).

### 5.6 User~~/ or~~ target group

Publications for security can also be grouped by their intended audience. Some examples of possible user groups are listed below, as shown in Figure 1:

- auditor;
- integrator;
- operator;
- maintainer;
- regulator;
- vendor.

IECNORM.COM : Click to view the full PDF of IEC GUIDE 120:2023 RLV

## 5.7 Developing security publications

### 5.7.1 ~~Base~~ Basic security publications

Many ~~base security publications~~ "Horizontal publication – Basic security publications" were originally developed by government, consortia or specialist commercial organizations. Most of these have been subsequently formalized into international or other generally accepted technological standards. IEC committees should reference the public form of these standards if one exists. The rules for referencing non ISO and IEC standards from within ISO and IEC publications are specified in 10.2 of ISO/IEC Directives Part 2:~~2018~~2021.

Within ISO/IEC joint technical committees, ~~base security publications~~ "Horizontal publication – Basic security publications" defining security controls are prepared by ISO/IEC JTC 1/SC 27~~,~~ ~~IT security techniques~~. Other IEC committees should not attempt to develop such ~~generic~~ basic security controls as they are unlikely to have the necessary level of generic security expertise and information. If an IEC committee identifies a need for a new publication of this type, it should supply the relevant use case to JTC 1/SC 27 and request it to prepare an appropriate publication.

It is left open to IEC committees to define security publications for their own domain to address

- relevant terminology,
- common threats and attacks,
- security design philosophy or such related issues, and
- common technical requirements (such as interoperability).

### 5.7.2 Horizontal publication – Group security publications

"Horizontal publication – Group security publications" will normally be domain-specific publications.

~~Group security publications~~ Horizontal publication – Basic security publications will normally be developed within one IEC committee, but may have application in areas beyond the scope of that committee. Normally, the domain committee will retain responsibility for publications development and maintenance, but should take account of other known use cases and requirements of wider use.

~~Group security publications~~ Horizontal publication – Basic security publications should build upon basic security services as defined in appropriate ~~base security publications~~ "Horizontal publication – Basic security publications", but may be parameterized or configured to reflect the intended field of application. This includes identifying specific threats, types of attack and consequences that apply to the intended field of application.

IEC committees should not attempt to restrict the applicability of "Horizontal publication – Group security publications" without good reason. This will enable developers of compliant products and systems to offer them for use elsewhere. However, ~~group security publications~~ "Horizontal publication – Basic security publications" should clearly identify any assumptions or limitations concerning their applicability in order to minimize the potential for misuse.

Where necessary, IEC committees developing "Horizontal publication – Group security publications" should consult or work collaboratively with the originators of the ~~base~~ basic security publications that they reference.

IECNORM.COM : Click to view the full PDF of IEC GUIDE 120:2023 RLV

### 5.7.3 Product security publications

Product security publications should normally be produced by the IEC committee that deals with the aspects of that type of product or series of products. Product security publications will often only deal with the product's interaction with its environment, referencing ~~generic base or group publications~~ "Horizontal publication – Basic security publications" or "Horizontal publication – Group security publications" to define internal behaviour.

### 5.7.4 Guidance security publications and test security publications

These publications should be produced by the IEC committee responsible for ~~the base, group~~ "Horizontal publication – Basic security publications", "Horizontal publication – Group security publications" or product security publication to which these publications refer. Assistance should be sought from specialist committees dealing with conformity assessment if applicable.

Committees should consider whether it is more effective to deal with guidance and test aspects of a publication through body text or annexes to the main specification, rather than by separate publications or parts of publications. There are benefits and drawbacks in both approaches.

Committees referencing guidance publications or annexes should take care not to create normative references to guidance information. In normative publications, references to guidance information should appear in the bibliography.

## 6 Mapping and overview of publications

### 6.1 General

ACSEC has developed and maintains up to date a set of files for use by IEC committees, in order to provide a global vision of the landscape of standardization in security.

These files are accessible from the Supporting Documents~~/Support Documents webpage from~~ section of the ACSEC dashboard on the IEC website [15].

ACSEC invites all IEC committees developing, revising or withdrawing publications involving security aspects or requirements to notify ACSEC so that these files can be updated.

### 6.2 List of relevant publications

The list of publications provides useful information for each identified publication:

- committee;
- publication reference;
- publication title;
- security relevance;
- type of publication, see 5.3;
- application domain, see 5.4;
- content, see 5.5;
- user~~/~~ or target group, see 5.6;
- link to the IEC webstore.

This list will help publication writers in identifying existing publications, in order to avoid duplication of work and favour consistency and coherence.

IECNORM.COM : Click to view the full PDF of IEC GUIDE 120:2023 RLV

### 6.3 Domain table chart

Figure 2 illustrates the principle of the application-domain table chart, which indicates in which application domains the publications produced by a body are applied or will be applied in the future. This will help publication users to identify committees or publications or both which could play a role in the dedicated application domain.

| | Building automation | Energy | Healthcare | Home automation | ICT | Industrial automation | Nuclear | Transportation |
|---|---|---|---|---|---|---|---|---|
| IEC TC X | a | a | | | | m | | |
| IEC TC Y | a | m | a | a | a | d | a | a |
| IEC TC Z | a | | m | d | | | | |

**Key**

m main domain: primary area of application for the publications of the committee.

a further application: secondary areas of application for the publications of the committee.

d under development: potential future areas of application for the publications of the committee.

**Figure 2 – Publications and application domains**

## 7 Considerations for publications development

### 7.1 Practical considerations for publication writers

IEC publications should be clear, concise, consistent and complete, and should be written in line with ISO/IEC Directives, Part 2. Publication writers should have in mind that security of systems relies on security risk assessment and management. Therefore, security considerations in publications should sometimes be formulated as recommendations to allow the applicability of the security considerations to different systems belonging to the scope of the publication. For example, interoperability between systems can require that product security publications specify requirements instead of recommendations.

Moreover, security considerations in publications should not specify any particular or commercial solution to address requirements, but should adopt a generic approach to provide security recommendations.

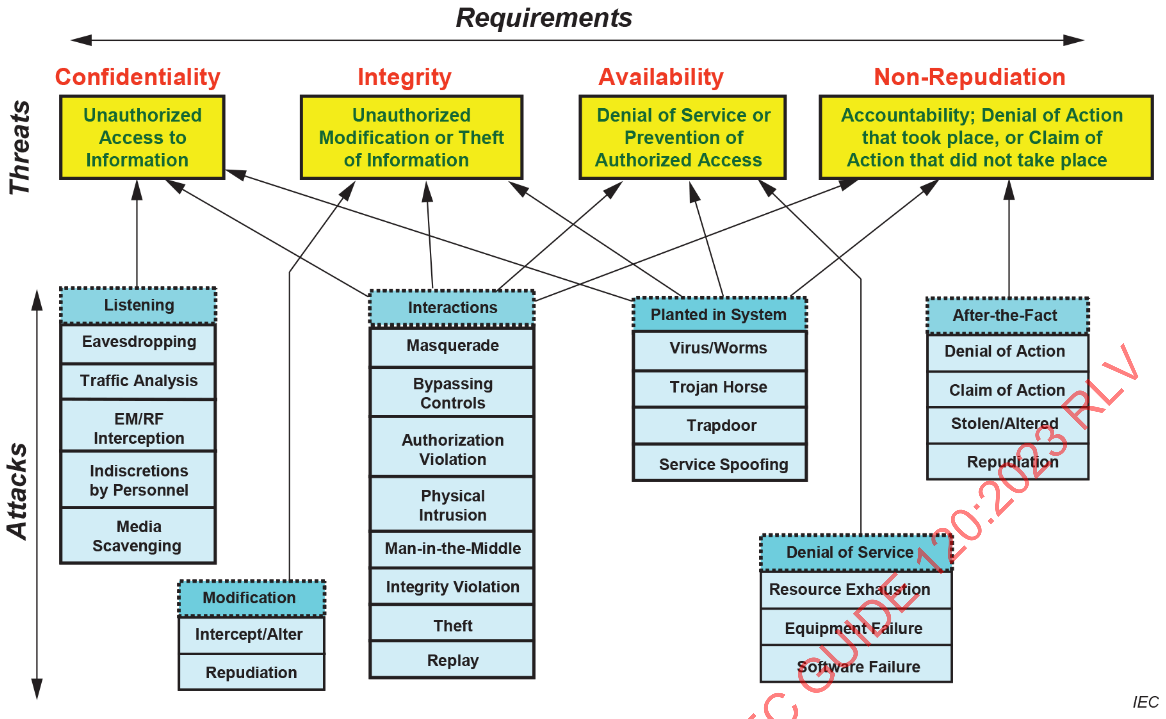
Where appropriate, security considerations should be included in specific clauses in the IEC publication.

Security research and technology is developing rapidly; as a result, any publication should be reviewed on a regular basis to ensure that it is current with technology and threat landscape.

### 7.2 Development process of security in publications

Figure 3 gives an example of the relationships between security requirements, threats, and attacks.

IECNORM.COM : Click to view the full PDF of IEC GUIDE 120:2023 RLV



SOURCE: IEC TS 62351-1:2007, Figure 1.

Figure 3 – Example of security requirements, threats, and possible attacks

~~ACSEC recommends that:~~

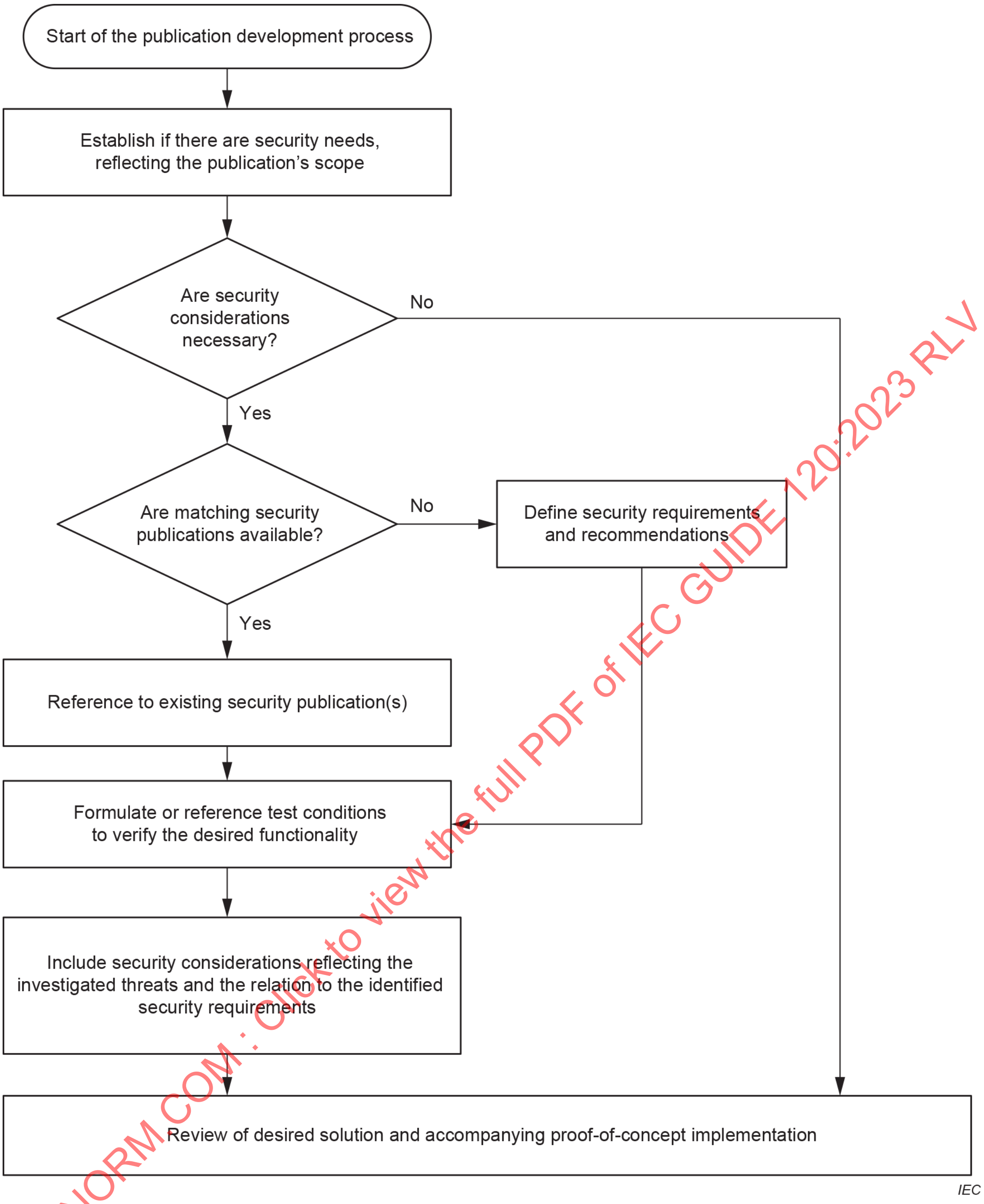
Security issues should be considered from the start of the publication development process. It should be checked whether security is to be considered (see Figure 4) in terms of mandatory requirements or recommendations.

Security considerations (including acceptable risk if appropriate) should be addressed by a risk based approach (see, for example, ISO 31000 [16] as a generic approach, and ISO/IEC 27005 [17] as a common IT security approach).

NOTE Risk based approach does not imply risk assessment.

If security aspects to be addressed in the publication have been identified, it should be determined whether existing publications can be referenced (see 6.2). If no suitable publication exists, the identified security provisions should be developed.

IECNORM.COM : Click to view the full PDF of IEC GUIDE 120:2023 RLV


Start of the publication development process
Establish if there are security needs, reflecting the publication's scope
Are security considerations necessary?
No
Yes
Are matching security publications available?
No
Define security requirements and recommendations
Yes
Reference to existing security publication(s)
Formulate or reference test conditions to verify the desired functionality
Include security considerations reflecting the investigated threats and the relation to the identified security requirements
Review of desired solution and accompanying proof-of-concept implementation
IEC

IECNORM.COM : Click to view the full PDF of IEC GUIDE 120:2023 RLV

**Figure 4 – Decision flow chart**

The guidelines listed below elaborate the flow chart and provide further recommendations for covering security considerations in publications as appropriate (partly from IEC TS 62351-1 [18]).

a) Consider the relevance of security aspects to the subject of the publication and identify the security needs.

b) If no specific considerations are necessary for the publication, consider documenting the rationale. If specific considerations are required, do not re-invent requirements or solutions if they can be found in well-established publications. Instead, use normative references to publications as much as possible, with the selection of alternatives or options normatively stated.

c) If existing publications do not provide a solution to the identified threats and risks, additional security requirements or recommendations or both should be defined.

d) To ensure that the specified security measures address the identified threats, formulate or reference test conditions that can help the user of the publication to verify the desired functionality. Therefore, it is recommended that a well described set of tools and documentation methods be set in place. These will assist in conformity assessment, see 7.4.2.

e) Include security considerations reflecting the investigated threats and the relation to the identified security requirements.

### 7.3 Interrelation between functional safety and security

Security is expected to protect functional safety, for example from interference or unauthorized modification.

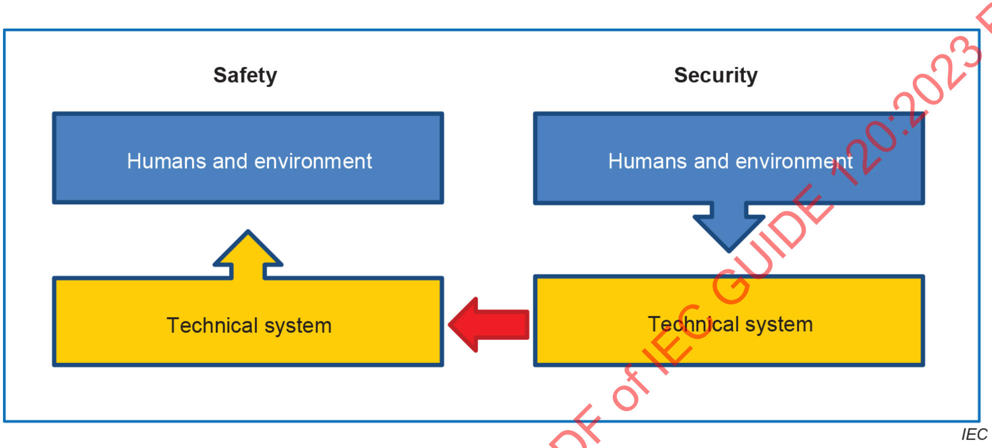


**Figure 5 – Interrelation between functional safety and security**

In Figure 5, there is an inverse direction of impact when safety and security aspects are compared. In functional safety, humans and the environment are potentially harmed by failure of the technical system. For security, the technical system is the potentially harmed target of disturbance by intended or accidental attacks carried out by humans or originating from the environment. The security of a technical system ~~might~~ can impact safety, and loop back to harm humans, property or the environment. The increase of connected components and systems is not only increasing the complexity of this "system of systems" but also raises concerns with respect to the safety impact due to security issues.

To ensure proper security and safety features are implemented in the system, both safety and security risk analysis should be performed.

Safety and security sometimes have conflicting requirements. For instance, information on a system is expected to be protected from access by anyone who cannot authenticate themselves to the system, but for safety reasons a break-glass function is required. For medical equipment, this is to allow access to the system and data in emergency cases where authentication is not possible when for instance domain servers are down or when emergency medical staff do not have the credentials to access the medical system but require immediate access to treat a patient.

Principles for interrelation between security and functional safety are as follows:

- security controls should not affect functional safety (e.g. no change of existing proof of functional safety);
- in particular, security controls should not affect the performance of functional safety measures beyond an acceptable level (e.g. integrity of data relevant for functional safety);
- functional safety measures should be designed in a way that they are reasonably protected from failures of security controls (e.g. update of vulnerable software without re-validation);

IECNORM.COM : Click to view the full PDF of IEC GUIDE 120:2023 RLV

- in particular, security controls should mitigate identified hazards caused by security threats in order to achieve the requested level of safety. See also 7.5.3.

Security and safety risk assessments can assist in determining where the two fields conflict and which requirements prevail. A security risk assessment can also assist in determining if a threat could be a potential cause for a hazard. It is valuable to have safety experts joining a security risk assessment. Safety lifecycle management is often reasonably stable as it is driven by the discovery of failures whereas security lifecycle management requires continuous updates and changes to the system to mitigate new vulnerabilities, threats and changes in the threat landscape. These security updates can have an impact on safety and as a result often require re-validation and certification of the system when the configuration has changed. Combination of activities addressing safety and security is not recommended, due to their different needs throughout the product or service lifetime.

Security measures should not be defined by the publication writers for safety systems, as security is considered to be ~~an own~~ a separate domain within standardization. However, informative references to security publications ~~can~~ may be made.

### 7.4 Specific requirements

#### 7.4.1 Relationship with ~~base security publications~~ "Horizontal publication – Basic security publications"

Existing ~~base~~ security publications are listed in the Supporting Documents section of the ACSEC dashboard [15].

Publication writers should identify particular clauses or subclauses of the applicable ~~base security publications~~ "Horizontal publication – Basic security publications" that address their specific security aspects.

#### 7.4.2 Consider conformity assessment when writing standards

Conformity assessment provides the ability to evaluate and assess that specified requirements relating to a product, process, service, person, system or body are fulfilled. ~~Pursuant to~~ Clause 33 of ISO/IEC Directives Part 2:~~2018~~2021 requires that IEC publications ~~should~~ be written in accordance with the "neutrality principle", such that conformity can be assessed by a first party, second party, or third party.

IEC standards that contain requirements should always be developed in such a way that conformity assessment is possible. IEC standards and other normative specifications that do not contain requirements are used to supplement testable standards and are not intended to be used as primary elements in a conformity assessment programme.

Test security standards that are used for conformity assessment should adhere to the following criteria:

a) technical requirements should be as technology neutral as possible;

b) technical requirements should provide the ability to be evaluated, assessed or "tested" in a repeatable and reproducible manner;

c) technical requirements should avoid "industry accepted" terms unless they denote what is considered industry accepted in a clause of the standard;

d) technical requirements that require an audit or assessment of an organization or process should provide the expected criteria for assessment.

When any conformity assessment body develops operational documents to manage the ability for third party conformity assessment, it is important that the requirements are developed to remove as much ambiguity or interpretation as possible. Hence, the requirements in the standard should be clear to the user of the standard so the market can develop and design products or processes to meet the requirements found in the standard.

IECNORM.COM : Click to view the full PDF of IEC GUIDE 120:2023 RLV

Conformity assessment groups can develop guidance documents for further clarity of the conformity assessment programme; however, as illustrated in 5.7.4, it is more effective to deal with guidance and test aspects of a standard through annexes to the main specification rather than by guidance documents from the conformity assessment body.

One other consideration is to reference ~~and/~~or otherwise utilize the content of ISO/IEC 17007 [19] that is suitable for use for conformity assessment.

### 7.4.3 IEC Horizontal security functions and Group security functions

The assignment of horizontal functions is defined in IEC Guide 108:2019. In the aspect of security, the assignment of horizontal functions is the responsibility of the Advisory Committee on Information security and data privacy (ACSEC), subject to confirmation by the SMB (Standardization Management Board).

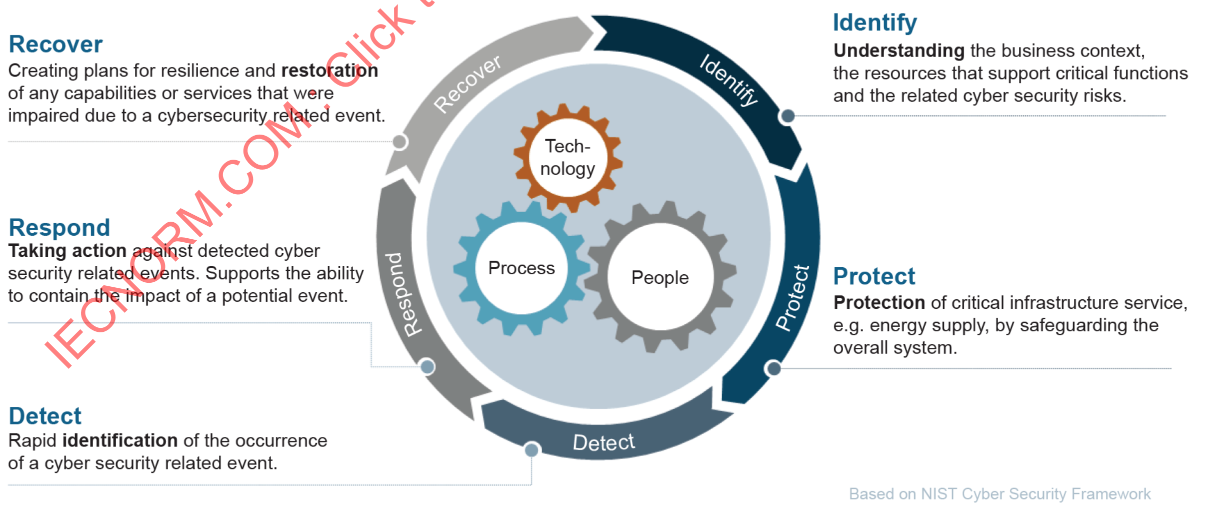
### 7.4.4 Lifecycle approach

The threat landscape changes continuously. Stringent security requirements, elaborate security risk assessments and exhaustive security testing during design and development can greatly reduce security risks. Security risks can change due to newly discovered vulnerabilities and changes in the threat landscape.

Security should be considered from the conceptual phase up to and including disposition; this includes the use of secure software development processes, change control, patch management, security monitoring and incident handling throughout the entire lifecycle of the system.

The security management cycle should include ongoing monitoring and remediation, see Figure 6.

A periodical revision of the publication should be considered to address new threats or deprecate old technologies and consider new technologies.


Recover
Creating plans for resilience and **restoration** of any capabilities or services that were impaired due to a cybersecurity related event.
Identify
**Understanding** the business context, the resources that support critical functions and the related cyber security risks.
Respond
**Taking action** against detected cyber security related events. Supports the ability to contain the impact of a potential event.
Protect
**Protection** of critical infrastructure service, e.g. energy supply, by safeguarding the overall system.
Detect
Rapid **identification** of the occurrence of a cyber security related event.
Recover
Identify
Protect
Detect
Respond
Tech-nology
Process
People

Based on NIST Cyber Security Framework

IEC

**Figure 6 – Example of security management cycle for an organization**

IECNORM.COM : Click to view the full PDF of IEC GUIDE 120:2023 RLV

### 7.4.5 Holistic system view

Security should envision the entire environment in which the systems are being used and not in isolation as each interconnected component on a system or in a network architecture could impose a risk to, or rely on the protection of another component on that system or network. For example, a vulnerability in a mobile application ~~might~~ can expose a threat vector to a cloud solution where the backend is hosted.

Security risk assessments should cover both component level and the entire system perspective. The holistic view is needed to identify conflicts, overlaps and gaps, and to ensure complete coverage.

### 7.4.6 Vulnerability handling

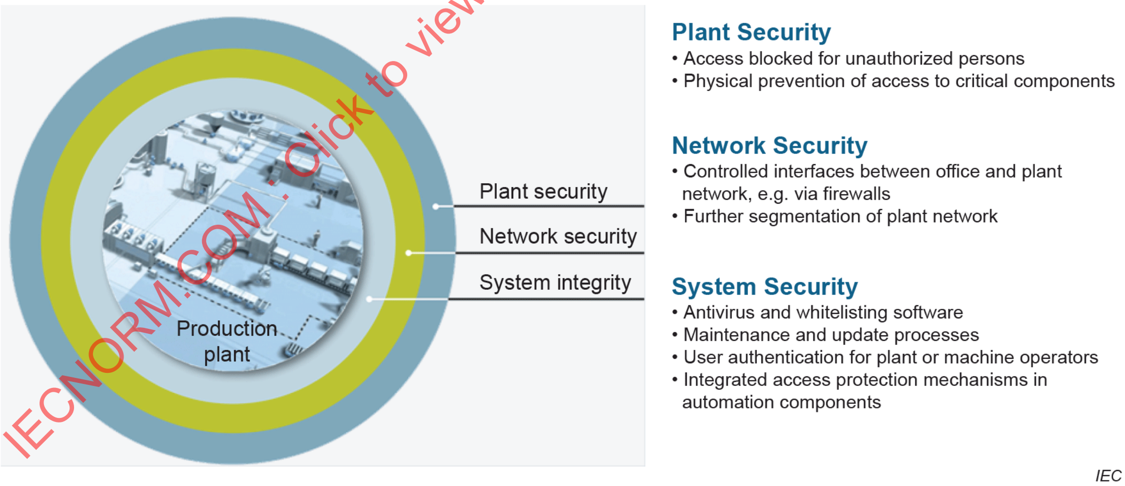
The close cooperation between vendors and their customers, security researchers and national security centres is essential to reveal and appropriately address newly discovered vulnerabilities in released products. The increase of the number of stakeholders involved in complex infrastructures such as cloud applications requires a structured approach towards a coordinated vulnerability management.

Publications should not contain requirements that unnecessarily impede such coordination.

### 7.4.7 Defence-in-depth

A defence-in-depth security architecture is based on the idea that any one point of protection can, and probably will, be defeated. It implies layers of security and detection, even on single systems.

Security measures are organized in a set of layers, each building a distinct barrier against an attack. These are called lines of defence, see Figure 7.



**Plant Security**
- Access blocked for unauthorized persons
- Physical prevention of access to critical components

**Network Security**
- Controlled interfaces between office and plant network, e.g. via firewalls
- Further segmentation of plant network

**System Security**
- Antivirus and whitelisting software
- Maintenance and update processes
- User authentication for plant or machine operators
- Integrated access protection mechanisms in automation components

**Figure 7 – Selected measures for defence-in-depth strategy**

### 7.4.8 Security management

The security management system preserves the security objectives by applying a risk management process. It provides confidence to interested parties that security risks are adequately managed within the context of the organization.

Regulators may mandate their own generic security framework.

IECNORM.COM : Click to view the full PDF of IEC GUIDE 120:2023 RLV

### 7.4.9 Supply chain

Suppliers can have either a direct or indirect access to the systems of the acquirer, or will provide elements (software, hardware, processes, or human resources) that will be involved in information processing. Acquirers can also have physical and/or logical access to the information of the supplier when they control or monitor production and delivery processes of the supplier.

### 7.4.10 Consider greenfield and brownfield

#### 7.4.10.1 General

When drafting security-related publications, ~~one has~~ it is valuable to consider that publication users ~~might~~ can face brownfield (existing system) or greenfield (newly designed system) scenarios, which makes a difference in security design needs.

#### 7.4.10.2 Greenfield

In a greenfield scenario, offering a high degree of freedom in engineering a "to-build" plant or system, the major focus will be on security by design. Following such design-based thinking, attention should be given to

- thorough risk analysis based on experience of comparable plants and systems,
- dimensioning for future upgrades during lifetime operation,
- consideration of expected future requirements,
- remote security monitoring, and
- remote software update capabilities.

#### 7.4.10.3 Brownfield

For a brownfield scenario, limiting the publications user and security design engineering to an "as-is" design of an existing plant or system, additional guidance should be given on

- criteria for the analysis and assessment of existing architectures to address security risks,
- criteria for a conscious "re-use/upgrade or swap/replace" decision,
- identification of limitations when deciding for upgrade/re-use,
- migration aspects for both "upgrade" and "replace" options, and
- identification of the remaining risk.

In any case, due to the high dynamics in the security threats, much attention ~~has~~ needs to be ~~spent~~ paid to backwards compatibility and future flexibility.

### 7.4.11 Use of term integrity

The definition of integrity in this document should not be confused with the term integrity used in "safety integrity" (as in IEC 61508 (all parts)) and in dependability publications. This is a different property from the one used in functional safety. Publications should clarify which definition they use.

## 7.5 Security risk assessment

### 7.5.1 General

Publications for technical system design, implementation and operation should include security risk assessment as a requirement, if appropriate.

IECNORM.COM : Click to view the full PDF of IEC GUIDE 120:2023 RLV

Any security risk assessment can be relevant for safety-related applications or non-safety-related applications. However, security risk assessment methods are different from those used for safety risk assessment.

The iterative process of security risk assessment and security risk mitigation is essential to achieve or guarantee a defined secure state during the overall lifecycle.

It is necessary to identify the security objectives during the security risk assessment.

Security risk assessment should

- address the identified security objectives, for example authentication, authorization, accountability, non-repudiation, integrity, confidentiality and availability, and
- identify the major threats and failure scenarios for each of the requirements applicable to the document's focus area, including assessing their likelihood and their potential impacts.

As a consequence, security policies and procedures should be developed for all target groups covered in the publication, see 5.6.

Security risk assessment is further explained, for example, in IEC~~/ISO~~ 31010 [20].

### 7.5.2 Iterative process of security risk assessment and risk mitigation

Publication writers should determine the extent to which the iterative process of security risk assessment and risk mitigation can be included as a requirement within the publication. This ~~might~~ can include guidance for the publication user when performing a security risk assessment to identify additional product or system specific risks.

The security risk assessment should use the latest version of the publication, and should be carried out, at least

- at each lifecycle phase by the designer of a product or system and the end user of this product or system, and
- at regular intervals or whenever triggered (e.g. when new security vulnerabilities become known), to identify new threats and vulnerabilities of the product or system.

Security risk assessment cannot override mandatory requirements for security protection, for example by regulation or customer requirement.

### 7.5.3 Maintaining safe operation

Maintaining safe operation is one of the overall security objectives of all control systems, see Figure 8.

Security risks will be evaluated by using a security risk assessment in order to identify the security objectives and to derive security measure(s).

IECNORM.COM : Click to view the full PDF of IEC GUIDE 120:2023 RLV

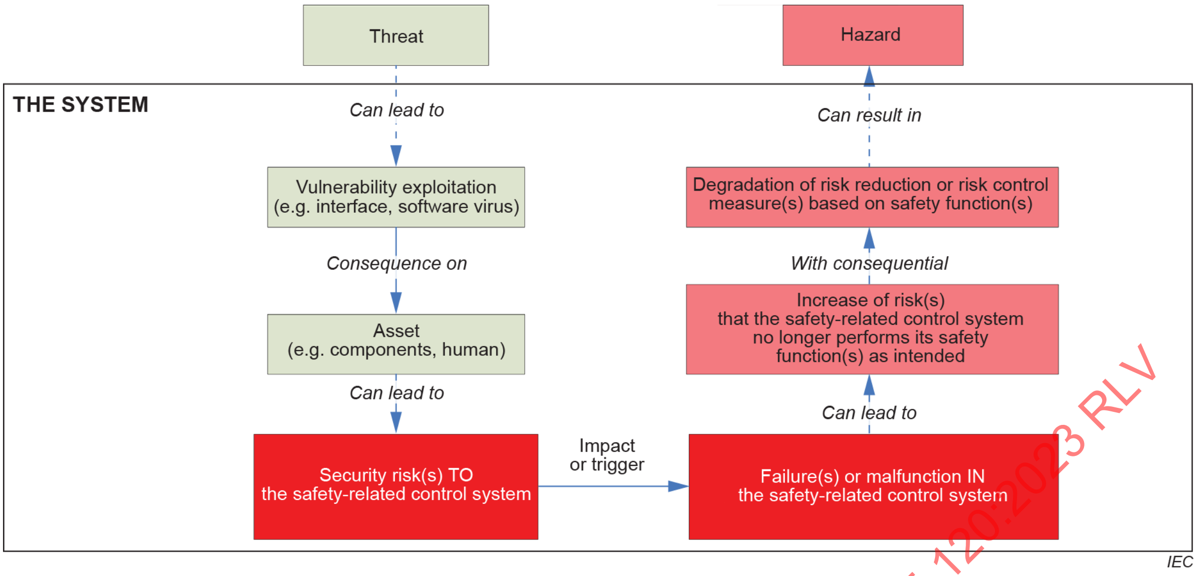

Threat
Hazard
THE SYSTEM
Can lead to
Can result in
Vulnerability exploitation (e.g. interface, software virus)
Degradation of risk reduction or risk control measure(s) based on safety function(s)
Consequence on
With consequential
Asset (e.g. components, human)
Increase of risk(s) that the safety-related control system no longer performs its safety function(s) as intended
Can lead to
Can lead to
Security risk(s) TO the safety-related control system
Impact or trigger
Failure(s) or malfunction IN the safety-related control system
IEC

**Figure 8 – Possible impact of security risk or risks on the safety-related control system**

IECNORM.COM : Click to view the full PDF of IEC GUIDE 120:2023 RLV

### 7.5.4 Scenario analysis

Scenario analysis ~~may~~ can be used to develop models of potential threats and identify their associated risk.

Publications incorporating security aspects should provide guidance on scenario analysis where appropriate.

Scenario analysis as defined, for example, in IEC~~/ISO~~ 31010 [20] includes the established techniques of threat modelling.

### 7.5.5 Security risk mitigation strategy

All products and systems are inherent to some level of security risk. However, the security risk should be reduced to an appropriate secure level.

A security risk mitigation strategy should consider the following options depending on the environment (e.g. location and organization):

a) design the security risk out (avoid);

b) reduce the security risk (limit);

c) accept the security risk;

d) transfer or share the security risk (to a third entity).

As a consequence, there is a need to define an appropriate secure level, in particular when developments, both in technology and in knowledge, can lead to economically feasible improvements to attain the minimum security risk.

Publications incorporating security aspects should provide guidance on achieving acceptable secure level by an adequate risk mitigation strategy.

### 7.5.6 Validation

Publications should include guidance to validate the implemented security risk mitigation strategy and security measures including

- their effectiveness, as well as their testability,
- the security risk assessment strategy (procedure) that has been followed, and
- the documentation of the outcome of the security risk assessment.

IECNORM.COM : Click to view the full PDF of IEC GUIDE 120:2023 RLV

# Bibliography

[1] IEC 60050 (all parts), *International Electrotechnical Vocabulary (IEV)*, available at <http://www.electropedia.org>

[2] IEC Glossary. available at <http://std.iec.ch/glossary>

[3] ISO/IEC JTC 1/SC 27, Standing Document SD6, *Glossary of IT Security Terminology*

[4] INTERNET ENGINEERING TASK FORCE (IETF) RFC 4949: *Internet Security Glossary, Version 2*, available at <https://tools.ietf.org/html/rfc4949>

[5] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) NISTIR 7298 Revision 2, *Glossary of Key Information Security Terms*, available at <https://dx.doi.org/10.6028/NIST.IR.7298r3>

[6] INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS (IEEE), *Standards Glossary,* available at <https://www.standardsuniversity.org/article/standards-glossary/>

[7] INTERNATIONAL TELECOMMUNICATION UNION (ITU). *ITU Terms and Definitions,* available at <https://www.itu.int/ITU-R/go/terminology-database>

[8] HEALTH LEVEL SEVEN (HL7), Secure Transactions Special Interest Group. *Glossary Of Acronyms, Abbreviations and Terms Related To Information Security In Healthcare Information Systems*. July 1999, available at <https://www.hl7.org/documentcenter/public/wg/secure/GLOSSARY2.rtf>

[9] INTERNATIONAL ATOMIC ENERGY AGENCY (IAEA), *Nuclear Security Series Glossary*, available at <https://www.iaea.org/resources/nuclear-security-series>

[10] INTERNATIONAL ENERGY AGENCY (IEA). *Glossary*

[11] ISO/IEC 27001, *Information security, cybersecurity and privacy protection – Information security management systems – Requirements*

[12] ISO/IEC 27019, *Information technology – Security techniques – Information security controls for the energy utility industry*

[13] IEC 62443-2-1, *Industrial communication networks – Network and system security – Part 2-1: Establishing an industrial automation and control system security program*

[14] IEC 62645, *Nuclear power plants – Instrumentation, control and electrical power systems – Cybersecurity requirements*

[15] IEC ACSEC dashboard available at <https://www.iec.ch/acsec/supportingdocuments>

[16] ISO 31000, *Risk management – Guidelines*

[17] ISO/IEC 27005, *Information security, cybersecurity and privacy protection – Guidance on managing information security risks*

[18] IEC TS 62351-1:2007, *Power systems management and associated information exchange – Data and communications security – Part 1: Communication network and system security – Introduction to security issues*

IECNORM.COM : Click to view the full PDF of IEC GUIDE 120:2023 RLV

[19] ISO/IEC 17007, *Conformity assessment – Guidance for drafting normative documents suitable for use for conformity assessment*

[20] IEC 31010, *Risk management – Risk assessment techniques*

[21] IEC 61508 (all parts), *Functional safety of electrical/electronic/programmable electronic safety-related systems*

[22] IEC 62337:2012, *Commissioning of electrical, instrumentation and control systems in the process industry – Specific phases and milestones*

[23] IEC TS 62351-2:2008, *Power systems management and associated information exchange – Data and communications security – Part 2: Glossary of terms*

[24] IEC TS 62443-1-1:2009, *Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models*

[25] IEC TR 62918:2014, *Nuclear power plants – Instrumentation and control important to safety – Use and selection of wireless devices to be integrated in systems important to safety*

[26] IEC Guide 104:2019, *The preparation of safety publications and the use of basic safety publications and group safety publications*

[27] IEC Guide 108:2019, *Guidelines for ensuring the coherence of IEC publications – Horizontal functions, horizontal publications and their application*

[28] ISO/IEC 24767-1:2008, *Information technology – Home network security – Part 1: Security requirements*

[29] ISO/IEC 27000:2018, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*

[30] ISO/IEC 27002, *Information security, cybersecurity and privacy protection – Information security controls*

[31] ISO/IEC 27009, *Information security, cybersecurity and privacy protection – Sector-specific application of ISO/IEC 27001 – Requirements*

[32] ISO/IEC 27036-1, *Cybersecurity – Supplier relationships – Part 1: Overview and concepts*

[33] ISO/IEC 27036-2, *Cybersecurity – Supplier relationships – Part 2: Requirements*

[34] ISO/IEC 27036-3, *Information technology – Security techniques – Information security for supplier relationships – Part 3: Guidelines for information and communication technology supply chain security*

[35] ISO/IEC 27036-4, *Information technology – Security techniques – Information security for supplier relationships – Part 4: Guidelines for security of cloud services*

[36] ISO/IEC 29100, *Information technology – Security techniques – Privacy framework*

[37] ISO/IEC 29101, *Information technology – Security techniques – Privacy architecture framework*

IECNORM.COM : Click to view the full PDF of IEC GUIDE 120:2023 RLV

[38] ISO/IEC 29115, *Information technology – Security techniques – Entity authentication assurance framework*

[39] ISO/IEC 29191, *Information technology – Security techniques – Requirements for partially anonymous, partially unlinkable authentication*

[40] ISO/IEC Guide 51:2014, *Safety aspects – Guidelines for their inclusion in standards*

[41] ISO/IEC Directives Part 2:2021, *Principles and rules for the structure and drafting of ISO and IEC documents*

[42] NIST SP 800-53, *Security Controls and Assessment Procedures for Federal Information Systems and Organizations*

___

IECNORM.COM : Click to view the full PDF of IEC GUIDE 120:2023 RLV

IECNORM.COM : Click to view the full PDF of IEC GUIDE 120:2023 RLV

# IEC GUIDE 120

Edition 2.0 2023-10

# GUIDE

# GUIDE

colour inside

## Security aspects – Guidelines for their inclusion in publications

## Aspects liés à la sûreté – Lignes directrices pour les inclure dans les publications

IECNORM.COM : Click to view the full PDF of IEC GUIDE 120:2023 RLV

## CONTENTS

IECNORM.COM : Click to view the full PDF of IEC GUIDE 120:2023 RLV

IECNORM.COM : Click to view the full PDF of IEC GUIDE 120:2023 RLV

INTERNATIONAL ELECTROTECHNICAL COMMISSION

____________

# SECURITY ASPECTS – GUIDELINES FOR THEIR INCLUSION IN PUBLICATIONS

## 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.

This second edition of IEC Guide 120 has been prepared, in accordance with ISO/IEC Directives, Part 1, Annex A, by the Advisory Committee on Information security and data privacy (ACSEC).

This second edition cancels and replaces the first edition published in 2018.

The main changes with respect to the previous edition are as follows:

a) The terminology of IEC Guide 120 has been aligned with the terminology of IEC Guide 108:2019.

IECNORM.COM : Click to view the full PDF of IEC GUIDE 120:2023 RLV

The text of this Guide is based on the following documents:

| Draft | Report on voting |
|---|---|
| SMBNC/39/DV | SMBNC/47/RV |

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

The language used for the development of this Guide is English.

This publication has been drafted in accordance with the 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/standardsdev/publications.

**IMPORTANT – The 'colour inside' logo on the cover page of this publication 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.**

IECNORM.COM : Click to view the full PDF of IEC GUIDE 120:2023 RLV

# INTRODUCTION

The increasing complexity and connectivity of systems, products, processes and services entering the market requires that the consideration of security aspects be given a high priority. Inclusion of security aspects in standardization provides protection from and response to risks of unintentionally and intentionally caused events that can disrupt the functionality and operation of products and systems.

When preparing publications, committees should ensure that relevant resilience requirements applicable to their application domain are included. Security aspects will in many cases play a role in achieving resilience directed standards.

In this document, the term "committee", includes technical committees, subcommittees and systems committees. The term "publication" includes "International Standard", "Technical Report", "Technical Specification" and "Guide".

National legal and regulatory requirements can exist that impact the general application of publications.

NOTE Publications can deal exclusively with security aspects or can include clauses specific to security.

IECNORM.COM : Click to view the full PDF of IEC GUIDE 120:2023 RLV

# SECURITY ASPECTS – GUIDELINES FOR THEIR INCLUSION IN PUBLICATIONS

## 1 Scope

This document provides guidelines on the security aspects included in IEC publications, and how to implement them. These guidelines can be used as a checklist for the combination of publications used in implementation of systems.

This document includes what is often referred to as "cybersecurity".

This document excludes non-electrotechnical aspects of security such as societal security, except where they directly interact with electrotechnical security.

NOTE The IEC Standardization Management Board (SMB) has decided that Guides such as this one can have mandatory requirements which shall be followed by all IEC committees developing technical work that falls within the scope of the Guide, as well as guidance which may or may not be followed. Any mandatory requirements in this Guide are identified by the use of "shall". Statements that are only for guidance are identified by using the verb "should". (See ISO/IEC Directives, IEC Supplement:2021, A.1.1.)

IECNORM.COM : Click to view the full PDF of IEC GUIDE 120:2023 RLV

## 2 Normative references

There are no normative references in this document.

## 3 Terms and definitions

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

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

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

**3.1**
**accountability**
property of a system (including all of its system resources) that ensures that the actions of a system entity can be traced uniquely to that entity, which can be held responsible for its actions

[SOURCE: IEC TS 62443-1-1:2009, 3.2.3]

**3.2**
**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]

**3.3**
**authentication**
provision of assurance that a claimed characteristic of an entity is correct

[SOURCE: ISO/IEC 27000:2018, 3.5]

**3.4**
**authorization**
right or permission that is granted to a system entity to access a system resource

[SOURCE: IEC TS 62443-1-1:2009, 3.2.14]

**3.5**
**availability**
property of being accessible and usable upon demand by an authorized entity

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

**3.6**
**confidentiality**
property that information is not made available or disclosed to unauthorized individuals, entities, or processes

[SOURCE: ISO/IEC 24767-1:2008, 2.1.2]

**3.7**
**functional safety**
part of the overall safety that depends on functional and physical units operating correctly in response to their inputs

[SOURCE: IEC 60050-351:2013, 351-57-06]

**3.8**
**harm**
injury or damage to the health of people, or damage to property or the environment

[SOURCE: ISO/IEC Guide 51:2014, 3.1]

**3.9**
**integrity**
property of accuracy and completeness

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

**3.10**
**non-repudiation**
ability to prove the occurrence of a claimed event or action and its originating entities

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

**3.11**
**risk**
combination of the probability of occurrence of harm and the severity of that harm

Note 1 to entry: The probability of security risks often cannot be determined in the same way as the probability of safety hazards based on statistical analysis.

[SOURCE: IEC 60050-351:2013, 351-57-03, modified – Note 1 to entry has been added.]

IECNORM.COM : Click to view the full PDF of IEC GUIDE 120:2023 RLV

**3.12**
**safety**
freedom from risk which is not tolerable

[SOURCE: ISO/IEC Guide 51:2014, 3.14]

**3.13**
**security**
condition that results from the establishment and maintenance of protective measures that ensure a state of inviolability from hostile acts or influences

Note 1 to entry: Hostile acts or influences could be intentional or unintentional.

Note 2 to entry: In actual usage, "security" and "cybersecurity" are often used interchangeably, even if technically, "cybersecurity" can be considered different from "security". However, this document does not make distinction between these terms.

[SOURCE: IEC TS 62351-2:2008, 2.2.173, modified – Notes 1 and 2 to entry have been added.]

**3.14**
**security control**
measure which modifies security risk or use

Note 1 to entry: A security control can be a process, policy, device, practice or other action.

**3.15**
**security service**
mechanism used to provide confidentiality, data integrity, authentication, or non-repudiation of information

[SOURCE: IEC TS 62443-1-1:2009, 3.2.115]

**3.16**
**threat**
potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm

[SOURCE: IEC TS 62443-1-1:2009, 3.2.125]

**3.17**
**vendor**
manufacturer or distributor of a product

[SOURCE: IEC 62337:2012, 3.12, modified – In the definition, "piece of equipment/ instrument/package unit" has been replaced with "product".]

**3.18**
**vulnerability**
flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy

Note 1 to entry: This definition of vulnerability should not be confused with the term vulnerability when used in the context of general risk management, where it encompasses the notion of possibility of exposition to a risk.

[SOURCE: IEC TR 62918:2014, 3.16, modified – Note 1 to entry has been added.]

IECNORM.COM : Click to view the full PDF of IEC GUIDE 120:2023 RLV

# 4 Guide to terminology

## 4.1 General

There are already many security-related terms and definitions in existing publications. Therefore, before defining a new term, existing terms and definitions should be checked first. Primary recommended sources are shown in 4.2 and they should be used in preference to the other relevant sources shown in 4.3. If no appropriate term and definition is found in those sources, either modify an existing one or define a new one.

Definitions in this document are not intended to be generic ones but only apply to this document.

The ISO/IEC Directives Part 2:2021, Clause 16, defines how the terms and definitions in IEC publications are drafted.

NOTE The same term can have different definitions depending on the context in which it is used, or different terms can be used for the same or similar meaning in different application domains.

## 4.2 Primary recommended sources

The primary recommended sources are

a) IEC 60050 (all parts) (IEV) [1][1],

b) IEC Glossary [2], and

c) ISO/IEC JTC 1/SC 27 SD6 [3],

where IEC 60050 and the IEC Glossary should be used in preference.

IEC 60050 provides representative definitions to more than 20 000 terms, organized by subject areas in IEC. The IEC Glossary is a compilation of electrotechnical terms extracted from the "Terms and definitions" clause in existing IEC publications.

If no appropriate term or definition is found in the two sources above, ISO/IEC JTC 1 SC 27 SD6, which covers more security-related terms and definitions, should be consulted.

NOTE Application-domain specific terms developed by IEC committees are also considered to be primary sources. These can be searched using the web page of the IEC Glossary.

## 4.3 Other relevant sources

### 4.3.1 General

There are a variety of resources available which focus on certain application domains of electrotechnology such as energy, building, healthcare, and transportation.

This includes application-domain independent sources (4.3.2) and application-domain specific sources (4.3.3).

### 4.3.2 Other application-domain independent sources

- IETF RFC 4949 [4];
- NISTIR 7298 [5];
- IEEE, Standards Glossary [6];
- ITU, ITU Terms and Definitions [7].

[1] Numbers in square brackets refer to the Bibliography.

IECNORM.COM : Click to view the full PDF of IEC GUIDE 120:2023 RLV

### 4.3.3 Other application-domain specific sources

- Healthcare: HL7, Glossary Of Acronyms, Abbreviations and Terms Related To Information Security In Healthcare Information Systems [8].
- Nuclear: IAEA, Nuclear Security Series Glossary [9].
- Energy: IEA, Glossary [10].

# 5 Categorization of publications

## 5.1 Overview

There are several different ways in which security publications can be categorized. Five possible classes for the categorization are considered as shown in Table 1:

- Publication categories;
- Publication types;
- Application domain;
- Content;
- User or target group;

Publications can belong to more than one class.

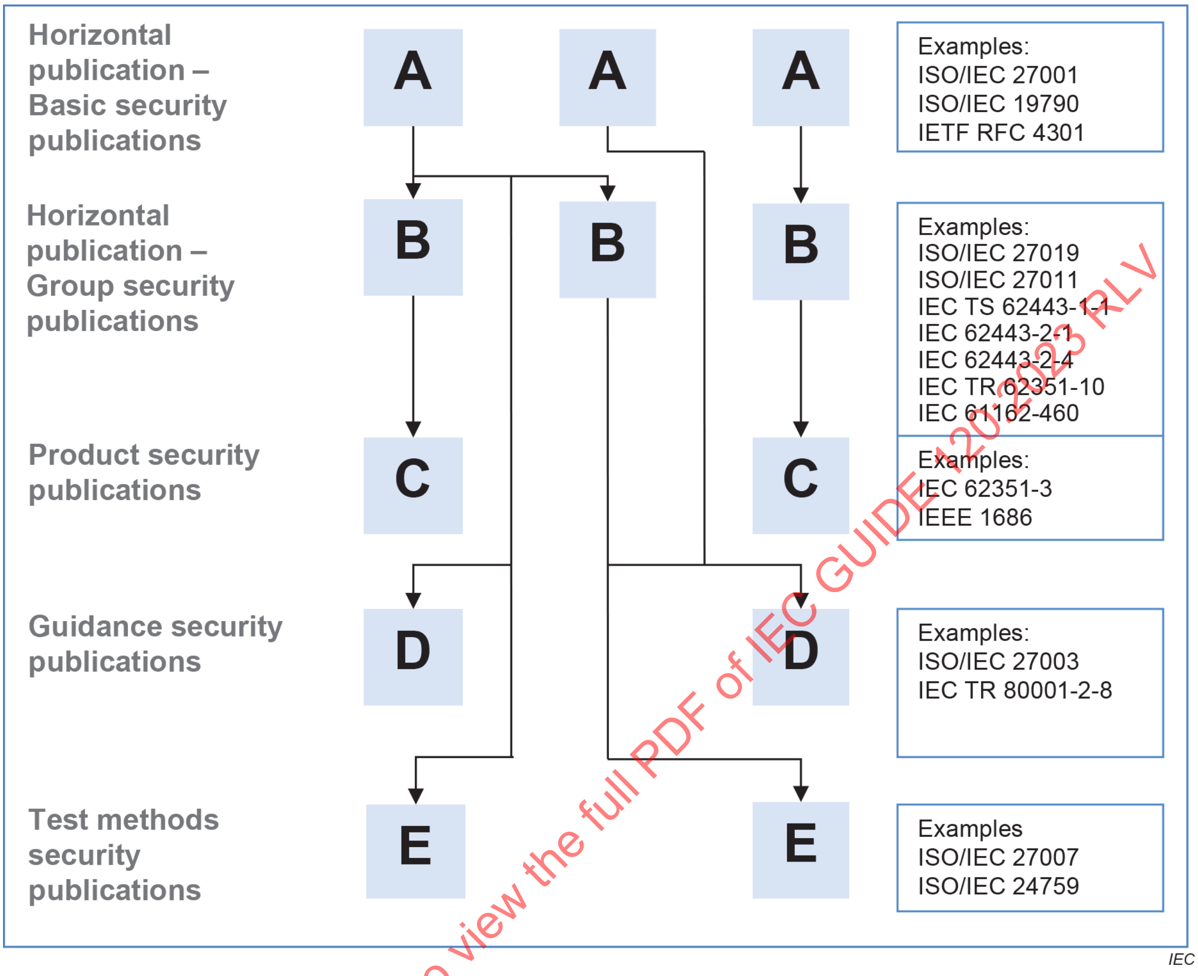
This document provides complementary information to IEC Guide 108 when referring to horizontal security publications.

**Table 1 – Possible categorization of publications**

| | |
|---|---|
| **Publication categories** | Horizontal publication – Basic security publications (applicable to any domain)<br>Horizontal publication – Group security publications (applicable to one or several specified domains)<br>Product security publications |
| **Publication types** | Guidance security publications (which could be horizontal publications or not)<br>Test methods security publications (which could be horizontal publications or not)<br>Configuration |
| **Application domain** | • Building<br>• Energy<br>• General<br>• Healthcare<br>• ICT<br>• Industrial automation<br>• Transportation |
| **Content** | • Component<br>• Management<br>• Policy<br>• Process<br>• Subsystem<br>• System<br>• Technology |
| **User or target group** | • Auditor<br>• Integrator<br>• Operator<br>• Maintainer<br>• Regulator<br>• Vendor |

IECNORM.COM : Click to view the full PDF of IEC GUIDE 120:2023 RLV

Figure 1 shows some examples of security publications listed according to the proposed classes.



NOTE The examples listed in Figure 1 are not exhaustive.

**Figure 1 – Examples of publications according to different categorization classes**

## 5.2 Publication categories

### 5.2.1 General

"Publication categories" stems from IEC Guide 108:2019 and extends the definition of the different categories proposed for horizontal publications to fully consider the security aspect context. The publication categories considered in this document are:

- Horizontal publication – Basic security publications (applicable to any domain);
- Horizontal publication – Group security publications;
- Product security publications.

### 5.2.2 Horizontal publication – Basic security publications (applicable to any domain)

"Horizontal publication – Basic security publications" deal with fundamental concepts, principles and requirements with regard to general security aspects applicable to a wide range of products and systems, and are applicable to any domain.

IECNORM.COM : Click to view the full PDF of IEC GUIDE 120:2023 RLV

### 5.2.3 Horizontal publication – Group security publications

"Horizontal publication – Group security publications" show how to apply security in one of the application domains. To do this, they may reference or customize existing "Horizontal publication – Basic security publications".

"Horizontal publication – Group security publications" may be applicable to many products or systems, or families of similar products or systems.

"Horizontal publication – Group security publications" can be referred to as sector-specific security publications.

### 5.2.4 Product security publications

"Product security publications" define how to apply "Horizontal publication – Basic security publications" or "Horizontal publication – Group security publications" for a particular type of product. They ensure that different products can interact or interoperate securely, and can be controlled and managed in a uniform manner.

"Product security publications" should as far as possible define their requirements by reference to "Horizontal publication – Basic security publications" or "Horizontal publication – Group security publications".

NOTE In this context, the term "product" includes items such as process, service, installation, and combinations thereof.

## 5.3 Publication types

### 5.3.1 General

"Publication types" stems from IEC Guide 108:2019 and extends the definition of the different types proposed for horizontal publications to fully consider the security aspect context. The proposed types considered in this document are:

- Guidance security publications;
- Test methods security publications.

### 5.3.2 Guidance security publications

"Guidance security publications" should not contain requirements. They explain how to implement "Horizontal publication – Basic security publications", "Horizontal publication – Group security publications" or product security publications.

In some application areas, guidance security publications are not used. Instead, necessary guidance information is provided through informative annexes within the relevant requirements standard.

### 5.3.3 Test methods security publications

"Test methods security publications" define ways to determine that the requirements of "Horizontal publication – Basic security publications", and "Horizontal publication – Group security publications" or product security publications have been correctly implemented.

Test methods security publications typically have a specialized audience and often make reference to conformity assessment. They may define or identify reference implementations that can be used to determine correct implementation through successful interoperation.

IECNORM.COM : Click to view the full PDF of IEC GUIDE 120:2023 RLV

### 5.4 Application domain

Publications for security can also be categorized according to their intended domain of application. This can be a sector of economic or industrial activity, a type of market, or an area of application.

Some examples of application domains are listed below, as shown in Figure 1:

- building;
- energy;
- general;
- healthcare;
- ICT;
- industrial automation;
- transportation.

In many cases an application domain will have an associated IEC committee responsible for the development of publications for that domain. This committee should accept responsibility for the development of the associated security publications.

Such committees will normally be able to define relevant threat models and security use cases independently, but it is possible that they will need to seek advice from the committees responsible for "Horizontal publication – Basic security publications" in configuring or customizing those basic security publications when referenced.

IECNORM.COM : Click to view the full PDF of IEC GUIDE 120:2023 RLV

### 5.5 Content

Publications for security can also be grouped by their type of content.

Some examples of possible groups are listed below, as shown in Figure 1:

- component;
- management;
- policy (not in IEC);
- process;
- subsystem;
- system;
- technology.

For example, electrotechnical standards for information security management include the "Horizontal publication – Basic security publications" standard ISO/IEC 27001 [11] (developed by ISO/IEC JTC 1/SC 27), but also the sector-specific standards ISO/IEC 27019 [12] (developed by ISO/IEC JTC 1/SC 27), IEC 62443-2-1 [13] (developed by IEC TC 65) and IEC 62645 [14] (developed by IEC SC 45A).

### 5.6 User or target group

Publications for security can also be grouped by their intended audience. Some examples of possible user groups are listed below, as shown in Figure 1:

- auditor;
- integrator;
- operator;
- maintainer;

- regulator;
- vendor.

## 5.7 Developing security publications

### 5.7.1 Basic security publications

Many "Horizontal publication – Basic security publications" were originally developed by government, consortia or specialist commercial organizations. Most of these have been subsequently formalized into international or other generally accepted technological standards. IEC committees should reference the public form of these standards if one exists. The rules for referencing non ISO and IEC standards from within ISO and IEC publications are specified in 10.2 of ISO/IEC Directives Part 2:2021.

Within ISO/IEC joint technical committees, "Horizontal publication – Basic security publications" defining security controls are prepared by ISO/IEC JTC 1/SC 27. Other IEC committees should not attempt to develop such basic security controls as they are unlikely to have the necessary level of generic security expertise and information. If an IEC committee identifies a need for a new publication of this type, it should supply the relevant use case to JTC 1/SC 27 and request it to prepare an appropriate publication.

It is left open to IEC committees to define security publications for their own domain to address

- relevant terminology,
- common threats and attacks,
- security design philosophy or such related issues, and
- common technical requirements (such as interoperability).

### 5.7.2 Horizontal publication – Group security publications

"Horizontal publication – Group security publications" will normally be domain-specific publications.

Horizontal publication – Basic security publications will normally be developed within one IEC committee, but may have application in areas beyond the scope of that committee. Normally, the domain committee will retain responsibility for publications development and maintenance, but should take account of other known use cases and requirements of wider use.

Horizontal publication – Basic security publications should build upon basic security services as defined in appropriate "Horizontal publication – Basic security publications", but may be parameterized or configured to reflect the intended field of application. This includes identifying specific threats, types of attack and consequences that apply to the intended field of application.

IEC committees should not attempt to restrict the applicability of "Horizontal publication – Group security publications" without good reason. This will enable developers of compliant products and systems to offer them for use elsewhere. However, "Horizontal publication – Basic security publications" should clearly identify any assumptions or limitations concerning their applicability in order to minimize the potential for misuse.

Where necessary, IEC committees developing "Horizontal publication – Group security publications" should consult or work collaboratively with the originators of the basic security publications that they reference.

IECNORM.COM : Click to view the full PDF of IEC GUIDE 120:2023 RLV

### 5.7.3 Product security publications

Product security publications should normally be produced by the IEC committee that deals with the aspects of that type of product or series of products. Product security publications will often only deal with the product's interaction with its environment, referencing "Horizontal publication – Basic security publications" or "Horizontal publication – Group security publications" to define internal behaviour.

### 5.7.4 Guidance security publications and test security publications

These publications should be produced by the IEC committee responsible for "Horizontal publication – Basic security publications", "Horizontal publication – Group security publications" or product security publication to which these publications refer. Assistance should be sought from specialist committees dealing with conformity assessment if applicable.

Committees should consider whether it is more effective to deal with guidance and test aspects of a publication through body text or annexes to the main specification, rather than by separate publications or parts of publications. There are benefits and drawbacks in both approaches.

Committees referencing guidance publications or annexes should take care not to create normative references to guidance information. In normative publications, references to guidance information should appear in the bibliography.

IECNORM.COM : Click to view the full PDF of IEC GUIDE 120:2023 RLV

## 6 Mapping and overview of publications

### 6.1 General

ACSEC has developed and maintains up to date a set of files for use by IEC committees, in order to provide a global vision of the landscape of standardization in security.

These files are accessible from the Supporting Documents section of the ACSEC dashboard on the IEC website [15].

ACSEC invites all IEC committees developing, revising or withdrawing publications involving security aspects or requirements to notify ACSEC so that these files can be updated.

### 6.2 List of relevant publications

The list of publications provides useful information for each identified publication:

- committee;
- publication reference;
- publication title;
- security relevance;
- type of publication, see 5.3;
- application domain, see 5.4;
- content, see 5.5;
- user or target group, see 5.6;
- link to the IEC webstore.

This list will help publication writers in identifying existing publications, in order to avoid duplication of work and favour consistency and coherence.

### 6.3 Domain table chart

Figure 2 illustrates the principle of the application-domain table chart, which indicates in which application domains the publications produced by a body are applied or will be applied in the future. This will help publication users to identify committees or publications or both which could play a role in the dedicated application domain.

| | Building automation | Energy | Healthcare | Home automation | ICT | Industrial automation | Nuclear | Transportation |
|---|---|---|---|---|---|---|---|---|
| IEC TC X | a | a | | | | m | | |
| IEC TC Y | a | m | a | a | a | d | a | a |
| IEC TC Z | a | | m | d | | | | |

**Key**

m main domain: primary area of application for the publications of the committee.

a further application: secondary areas of application for the publications of the committee.

d under development: potential future areas of application for the publications of the committee.

**Figure 2 – Publications and application domains**

IECNORM.COM : Click to view the full PDF of IEC GUIDE 120:2023 RLV

## 7 Considerations for publications development

### 7.1 Practical considerations for publication writers

IEC publications should be clear, concise, consistent and complete, and should be written in line with ISO/IEC Directives, Part 2. Publication writers should have in mind that security of systems relies on security risk assessment and management. Therefore, security considerations in publications should sometimes be formulated as recommendations to allow the applicability of the security considerations to different systems belonging to the scope of the publication. For example, interoperability between systems can require that product security publications specify requirements instead of recommendations.

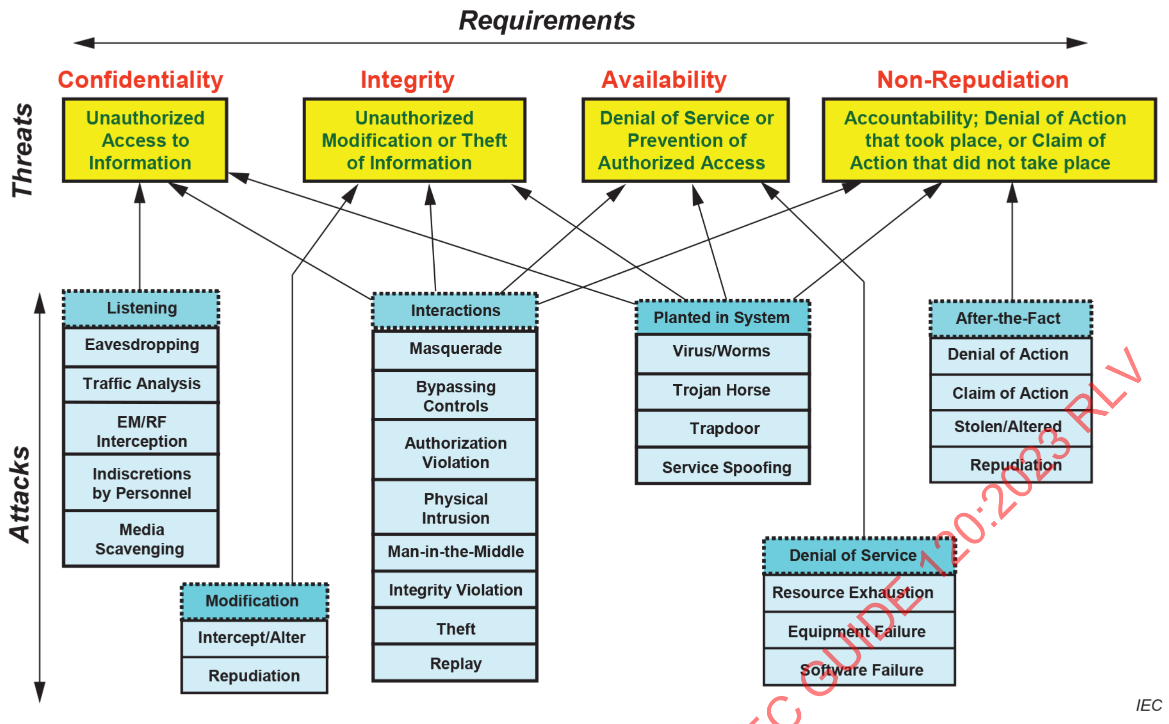
Moreover, security considerations in publications should not specify any particular or commercial solution to address requirements, but should adopt a generic approach to provide security recommendations.

Where appropriate, security considerations should be included in specific clauses in the IEC publication.

Security research and technology is developing rapidly; as a result, any publication should be reviewed on a regular basis to ensure that it is current with technology and threat landscape.

### 7.2 Development process of security in publications

Figure 3 gives an example of the relationships between security requirements, threats, and attacks.



SOURCE: IEC TS 62351-1:2007, Figure 1.

**Figure 3 – Example of security requirements, threats, and possible attacks**

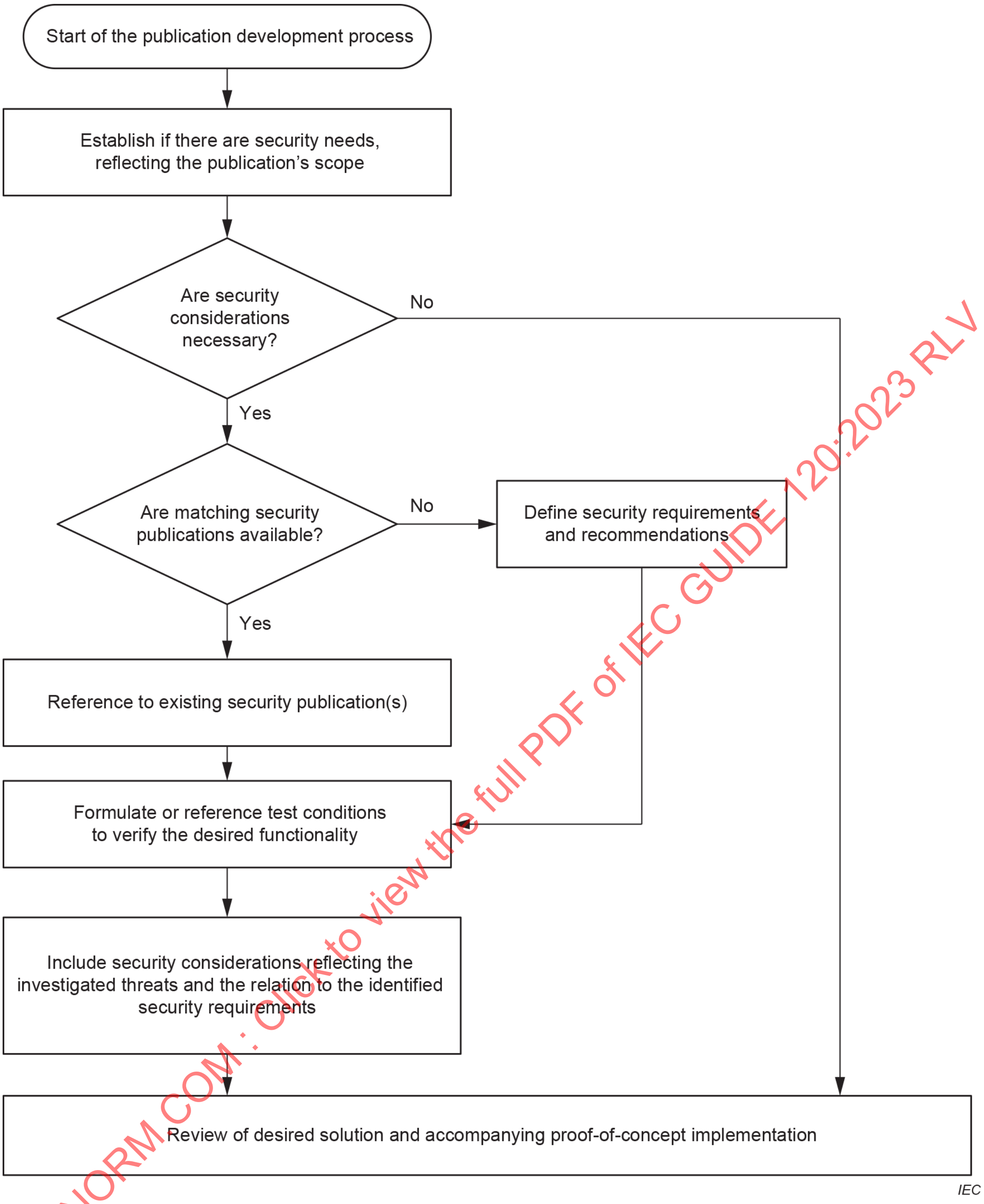
Security issues should be considered from the start of the publication development process. It should be checked whether security is to be considered (see Figure 4) in terms of mandatory requirements or recommendations.

Security considerations (including acceptable risk if appropriate) should be addressed by a risk based approach (see, for example, ISO 31000 [16] as a generic approach, and ISO/IEC 27005 [17] as a common IT security approach).

NOTE Risk based approach does not imply risk assessment.

If security aspects to be addressed in the publication have been identified, it should be determined whether existing publications can be referenced (see 6.2). If no suitable publication exists, the identified security provisions should be developed.

IECNORM.COM : Click to view the full PDF of IEC GUIDE 120:2023 RLV


Start of the publication development process
Establish if there are security needs, reflecting the publication's scope
Are security considerations necessary?
No
Yes
Are matching security publications available?
No
Define security requirements and recommendations
Yes
Reference to existing security publication(s)
Formulate or reference test conditions to verify the desired functionality
Include security considerations reflecting the investigated threats and the relation to the identified security requirements
Review of desired solution and accompanying proof-of-concept implementation
IEC

IECNORM.COM : Click to view the full PDF of IEC GUIDE 120:2023 RLV

**Figure 4 – Decision flow chart**

The guidelines listed below elaborate the flow chart and provide further recommendations for covering security considerations in publications as appropriate (partly from IEC TS 62351-1 [18]).

a) Consider the relevance of security aspects to the subject of the publication and identify the security needs.

b) If no specific considerations are necessary for the publication, consider documenting the rationale. If specific considerations are required, do not re-invent requirements or solutions if they can be found in well-established publications. Instead, use normative references to publications as much as possible, with the selection of alternatives or options normatively stated.

c) If existing publications do not provide a solution to the identified threats and risks, additional security requirements or recommendations or both should be defined.

d) To ensure that the specified security measures address the identified threats, formulate or reference test conditions that can help the user of the publication to verify the desired functionality. Therefore, it is recommended that a well described set of tools and documentation methods be set in place. These will assist in conformity assessment, see 7.4.2.

e) Include security considerations reflecting the investigated threats and the relation to the identified security requirements.

### 7.3 Interrelation between functional safety and security

Security is expected to protect functional safety, for example from interference or unauthorized modification.

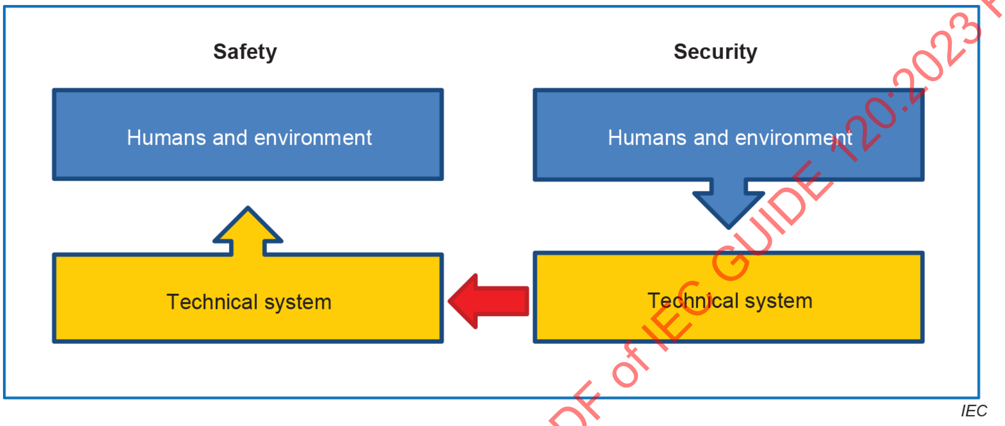


**Figure 5 – Interrelation between functional safety and security**

In Figure 5, there is an inverse direction of impact when safety and security aspects are compared. In functional safety, humans and the environment are potentially harmed by failure of the technical system. For security, the technical system is the potentially harmed target of disturbance by intended or accidental attacks carried out by humans or originating from the environment. The security of a technical system can impact safety, and loop back to harm humans, property or the environment. The increase of connected components and systems is not only increasing the complexity of this "system of systems" but also raises concerns with respect to the safety impact due to security issues.

To ensure proper security and safety features are implemented in the system, both safety and security risk analysis should be performed.

Safety and security sometimes have conflicting requirements. For instance, information on a system is expected to be protected from access by anyone who cannot authenticate themselves to the system, but for safety reasons a break-glass function is required. For medical equipment, this is to allow access to the system and data in emergency cases where authentication is not possible when for instance domain servers are down or when emergency medical staff do not have the credentials to access the medical system but require immediate access to treat a patient.

Principles for interrelation between security and functional safety are as follows:

- security controls should not affect functional safety (e.g. no change of existing proof of functional safety);
- in particular, security controls should not affect the performance of functional safety measures beyond an acceptable level (e.g. integrity of data relevant for functional safety);
- functional safety measures should be designed in a way that they are reasonably protected from failures of security controls (e.g. update of vulnerable software without re-validation);

IECNORM.COM : Click to view the full PDF of IEC GUIDE 120:2023 RLV

- in particular, security controls should mitigate identified hazards caused by security threats in order to achieve the requested level of safety. See also 7.5.3.

Security and safety risk assessments can assist in determining where the two fields conflict and which requirements prevail. A security risk assessment can also assist in determining if a threat could be a potential cause for a hazard. It is valuable to have safety experts joining a security risk assessment. Safety lifecycle management is often reasonably stable as it is driven by the discovery of failures whereas security lifecycle management requires continuous updates and changes to the system to mitigate new vulnerabilities, threats and changes in the threat landscape. These security updates can have an impact on safety and as a result often require re-validation and certification of the system when the configuration has changed. Combination of activities addressing safety and security is not recommended, due to their different needs throughout the product or service lifetime.

Security measures should not be defined by the publication writers for safety systems, as security is considered to be a separate domain within standardization. However, informative references to security publications may be made.

## 7.4 Specific requirements

### 7.4.1 Relationship with "Horizontal publication – Basic security publications"

Existing security publications are listed in the Supporting Documents section of the ACSEC dashboard [15].

Publication writers should identify particular clauses or subclauses of the applicable "Horizontal publication – Basic security publications" that address their specific security aspects.

### 7.4.2 Consider conformity assessment when writing standards

Conformity assessment provides the ability to evaluate and assess that specified requirements relating to a product, process, service, person, system or body are fulfilled. Clause 33 of ISO/IEC Directives Part 2:2021 requires that IEC publications be written in accordance with the "neutrality principle", such that conformity can be assessed by a first party, second party, or third party.

IEC standards that contain requirements should always be developed in such a way that conformity assessment is possible. IEC standards and other normative specifications that do not contain requirements are used to supplement testable standards and are not intended to be used as primary elements in a conformity assessment programme.

Test security standards that are used for conformity assessment should adhere to the following criteria:

a) technical requirements should be as technology neutral as possible;

b) technical requirements should provide the ability to be evaluated, assessed or "tested" in a repeatable and reproducible manner;

c) technical requirements should avoid "industry accepted" terms unless they denote what is considered industry accepted in a clause of the standard;

d) technical requirements that require an audit or assessment of an organization or process should provide the expected criteria for assessment.

When any conformity assessment body develops operational documents to manage the ability for third party conformity assessment, it is important that the requirements are developed to remove as much ambiguity or interpretation as possible. Hence, the requirements in the standard should be clear to the user of the standard so the market can develop and design products or processes to meet the requirements found in the standard.

IECNORM.COM : Click to view the full PDF of IEC GUIDE 120:2023 RLV

Conformity assessment groups can develop guidance documents for further clarity of the conformity assessment programme; however, as illustrated in 5.7.4, it is more effective to deal with guidance and test aspects of a standard through annexes to the main specification rather than by guidance documents from the conformity assessment body.

One other consideration is to reference or otherwise utilize the content of ISO/IEC 17007 [19] that is suitable for use for conformity assessment.

### 7.4.3 IEC Horizontal security functions and Group security functions

The assignment of horizontal functions is defined in IEC Guide 108:2019. In the aspect of security, the assignment of horizontal functions is the responsibility of the Advisory Committee on Information security and data privacy (ACSEC), subject to confirmation by the SMB (Standardization Management Board).

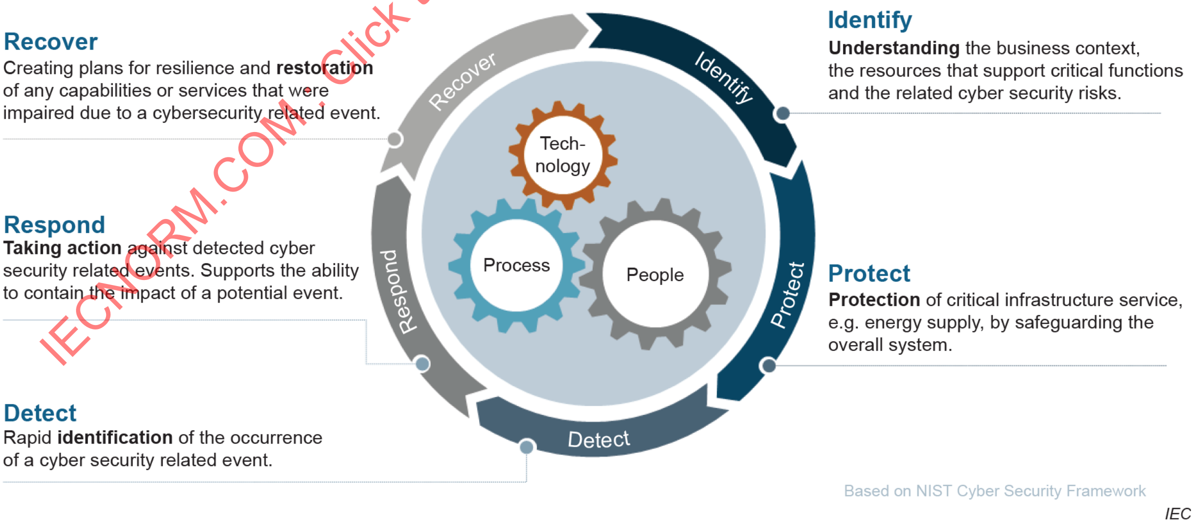
### 7.4.4 Lifecycle approach

The threat landscape changes continuously. Stringent security requirements, elaborate security risk assessments and exhaustive security testing during design and development can greatly reduce security risks. Security risks can change due to newly discovered vulnerabilities and changes in the threat landscape.

Security should be considered from the conceptual phase up to and including disposition; this includes the use of secure software development processes, change control, patch management, security monitoring and incident handling throughout the entire lifecycle of the system.

The security management cycle should include ongoing monitoring and remediation, see Figure 6.

A periodical revision of the publication should be considered to address new threats or deprecate old technologies and consider new technologies.



**Recover**
Creating plans for resilience and **restoration** of any capabilities or services that were impaired due to a cybersecurity related event.

**Identify**
**Understanding** the business context, the resources that support critical functions and the related cyber security risks.

**Respond**
**Taking action** against detected cyber security related events. Supports the ability to contain the impact of a potential event.

**Protect**
**Protection** of critical infrastructure service, e.g. energy supply, by safeguarding the overall system.

**Detect**
Rapid **identification** of the occurrence of a cyber security related event.

Based on NIST Cyber Security Framework

IEC

**Figure 6 – Example of security management cycle for an organization**

IECNORM.COM : Click to view the full PDF of IEC GUIDE 120:2023 RLV

### 7.4.5 Holistic system view

Security should envision the entire environment in which the systems are being used and not in isolation as each interconnected component on a system or in a network architecture could impose a risk to, or rely on the protection of another component on that system or network. For example, a vulnerability in a mobile application can expose a threat vector to a cloud solution where the backend is hosted.

Security risk assessments should cover both component level and the entire system perspective. The holistic view is needed to identify conflicts, overlaps and gaps, and to ensure complete coverage.

### 7.4.6 Vulnerability handling

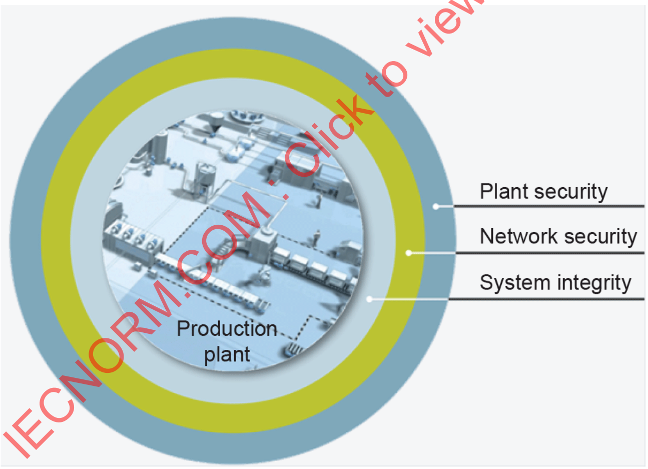
The close cooperation between vendors and their customers, security researchers and national security centres is essential to reveal and appropriately address newly discovered vulnerabilities in released products. The increase of the number of stakeholders involved in complex infrastructures such as cloud applications requires a structured approach towards a coordinated vulnerability management.

Publications should not contain requirements that unnecessarily impede such coordination.

### 7.4.7 Defence-in-depth

A defence-in-depth security architecture is based on the idea that any one point of protection can, and probably will, be defeated. It implies layers of security and detection, even on single systems.

Security measures are organized in a set of layers, each building a distinct barrier against an attack. These are called lines of defence, see Figure 7.



**Plant Security**
- Access blocked for unauthorized persons
- Physical prevention of access to critical components

**Network Security**
- Controlled interfaces between office and plant network, e.g. via firewalls
- Further segmentation of plant network

**System Security**
- Antivirus and whitelisting software
- Maintenance and update processes
- User authentication for plant or machine operators
- Integrated access protection mechanisms in automation components

**Figure 7 – Selected measures for defence-in-depth strategy**

### 7.4.8 Security management

The security management system preserves the security objectives by applying a risk management process. It provides confidence to interested parties that security risks are adequately managed within the context of the organization.

Regulators may mandate their own generic security framework.

IECNORM.COM : Click to view the full PDF of IEC GUIDE 120:2023 RLV

#### 7.4.9 Supply chain

Suppliers can have either a direct or indirect access to the systems of the acquirer, or will provide elements (software, hardware, processes, or human resources) that will be involved in information processing. Acquirers can also have physical and/or logical access to the information of the supplier when they control or monitor production and delivery processes of the supplier.

#### 7.4.10 Consider greenfield and brownfield

##### 7.4.10.1 General

When drafting security-related publications, it is valuable to consider that publication users can face brownfield (existing system) or greenfield (newly designed system) scenarios, which makes a difference in security design needs.

##### 7.4.10.2 Greenfield

In a greenfield scenario, offering a high degree of freedom in engineering a "to-build" plant or system, the major focus will be on security by design. Following such design-based thinking, attention should be given to

- thorough risk analysis based on experience of comparable plants and systems,
- dimensioning for future upgrades during lifetime operation,
- consideration of expected future requirements,
- remote security monitoring, and
- remote software update capabilities.

##### 7.4.10.3 Brownfield

For a brownfield scenario, limiting the publications user and security design engineering to an "as-is" design of an existing plant or system, additional guidance should be given on

- criteria for the analysis and assessment of existing architectures to address security risks,
- criteria for a conscious "re-use/upgrade or swap/replace" decision,
- identification of limitations when deciding for upgrade/re-use,
- migration aspects for both "upgrade" and "replace" options, and
- identification of the remaining risk.

In any case, due to the high dynamics in the security threats, much attention needs to be paid to backwards compatibility and future flexibility.

#### 7.4.11 Use of term integrity

The definition of integrity in this document should not be confused with the term integrity used in "safety integrity" (as in IEC 61508 (all parts)) and in dependability publications. This is a different property from the one used in functional safety. Publications should clarify which definition they use.

### 7.5 Security risk assessment

#### 7.5.1 General

Publications for technical system design, implementation and operation should include security risk assessment as a requirement, if appropriate.

IECNORM.COM : Click to view the full PDF of IEC GUIDE 120:2023 RLV

Any security risk assessment can be relevant for safety-related applications or non-safety-related applications. However, security risk assessment methods are different from those used for safety risk assessment.

The iterative process of security risk assessment and security risk mitigation is essential to achieve or guarantee a defined secure state during the overall lifecycle.

It is necessary to identify the security objectives during the security risk assessment.

Security risk assessment should

- address the identified security objectives, for example authentication, authorization, accountability, non-repudiation, integrity, confidentiality and availability, and
- identify the major threats and failure scenarios for each of the requirements applicable to the document's focus area, including assessing their likelihood and their potential impacts.

As a consequence, security policies and procedures should be developed for all target groups covered in the publication, see 5.6.

Security risk assessment is further explained, for example, in IEC 31010 [20].

### 7.5.2 Iterative process of security risk assessment and risk mitigation

Publication writers should determine the extent to which the iterative process of security risk assessment and risk mitigation can be included as a requirement within the publication. This can include guidance for the publication user when performing a security risk assessment to identify additional product or system specific risks.

The security risk assessment should use the latest version of the publication, and should be carried out, at least

- at each lifecycle phase by the designer of a product or system and the end user of this product or system, and
- at regular intervals or whenever triggered (e.g. when new security vulnerabilities become known), to identify new threats and vulnerabilities of the product or system.

Security risk assessment cannot override mandatory requirements for security protection, for example by regulation or customer requirement.

### 7.5.3 Maintaining safe operation

Maintaining safe operation is one of the overall security objectives of all control systems, see Figure 8.

Security risks will be evaluated by using a security risk assessment in order to identify the security objectives and to derive security measure(s).

IECNORM.COM : Click to view the full PDF of IEC GUIDE 120:2023 RLV

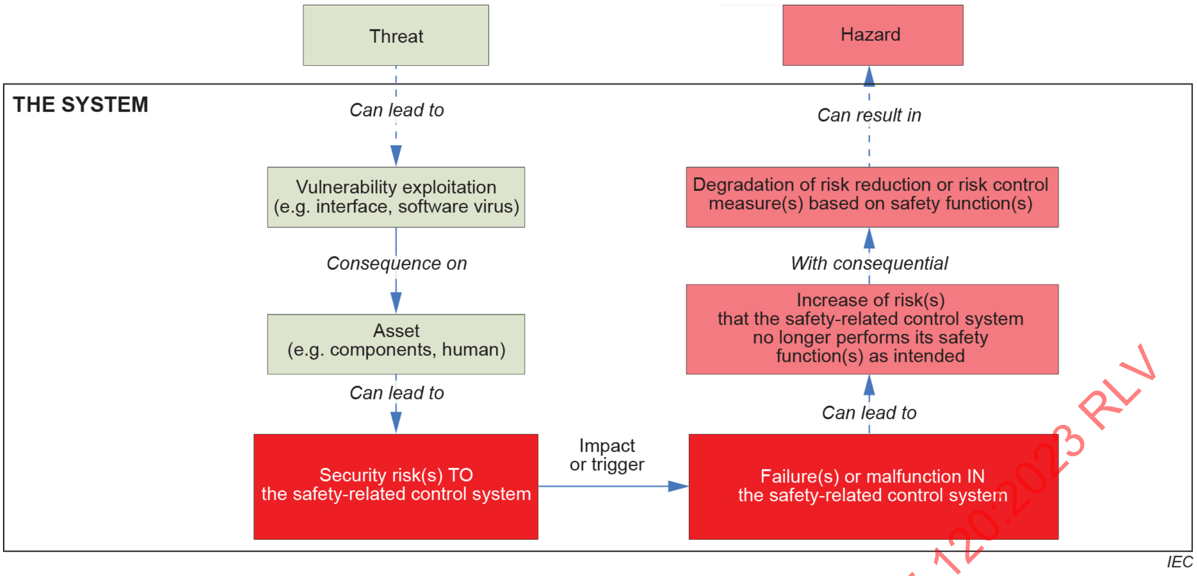

Threat
Hazard
THE SYSTEM
Can lead to
Can result in
Vulnerability exploitation
(e.g. interface, software virus)
Degradation of risk reduction or risk control measure(s) based on safety function(s)
Consequence on
With consequential
Asset
(e.g. components, human)
Increase of risk(s) that the safety-related control system no longer performs its safety function(s) as intended
Can lead to
Can lead to
Security risk(s) TO the safety-related control system
Impact or trigger
Failure(s) or malfunction IN the safety-related control system
IEC

**Figure 8 – Possible impact of security risk or risks on the safety-related control system**

### 7.5.4 Scenario analysis

Scenario analysis can be used to develop models of potential threats and identify their associated risk.

Publications incorporating security aspects should provide guidance on scenario analysis where appropriate.

Scenario analysis as defined, for example, in IEC 31010 [20] includes the established techniques of threat modelling.

### 7.5.5 Security risk mitigation strategy

All products and systems are inherent to some level of security risk. However, the security risk should be reduced to an appropriate secure level.

A security risk mitigation strategy should consider the following options depending on the environment (e.g. location and organization):

a) design the security risk out (avoid);

b) reduce the security risk (limit);

c) accept the security risk;

d) transfer or share the security risk (to a third entity).

As a consequence, there is a need to define an appropriate secure level, in particular when developments, both in technology and in knowledge, can lead to economically feasible improvements to attain the minimum security risk.

Publications incorporating security aspects should provide guidance on achieving acceptable secure level by an adequate risk mitigation strategy.

IECNORM.COM : Click to view the full PDF of IEC GUIDE 120:2023 RLV

### 7.5.6 Validation

Publications should include guidance to validate the implemented security risk mitigation strategy and security measures including

- their effectiveness, as well as their testability,
- the security risk assessment strategy (procedure) that has been followed, and
- the documentation of the outcome of the security risk assessment.

IECNORM.COM : Click to view the full PDF of IEC GUIDE 120:2023 RLV

# Bibliography

[1] IEC 60050 (all parts), *International Electrotechnical Vocabulary (IEV)*, available at <http://www.electropedia.org>

[2] IEC Glossary. available at <http://std.iec.ch/glossary>

[3] ISO/IEC JTC 1/SC 27, Standing Document SD6, *Glossary of IT Security Terminology*

[4] INTERNET ENGINEERING TASK FORCE (IETF) RFC 4949: *Internet Security Glossary, Version 2*, available at <https://tools.ietf.org/html/rfc4949>

[5] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) NISTIR 7298 Revision 2, *Glossary of Key Information Security Terms*, available at <https://dx.doi.org/10.6028/NIST.IR.7298r3>

[6] INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS (IEEE), *Standards Glossary,* available at <https://www.standardsuniversity.org/article/standards-glossary/>

[7] INTERNATIONAL TELECOMMUNICATION UNION (ITU). *ITU Terms and Definitions,* available at <https://www.itu.int/ITU-R/go/terminology-database>

[8] HEALTH LEVEL SEVEN (HL7), Secure Transactions Special Interest Group. *Glossary Of Acronyms, Abbreviations and Terms Related To Information Security In Healthcare Information Systems*. July 1999, available at <https://www.hl7.org/documentcenter/public/wg/secure/GLOSSARY2.rtf>

[9] INTERNATIONAL ATOMIC ENERGY AGENCY (IAEA), *Nuclear Security Series Glossary*, available at <https://www.iaea.org/resources/nuclear-security-series>

[10] INTERNATIONAL ENERGY AGENCY (IEA). *Glossary*

[11] ISO/IEC 27001, *Information security, cybersecurity and privacy protection – Information security management systems – Requirements*

[12] ISO/IEC 27019, *Information technology – Security techniques – Information security controls for the energy utility industry*

[13] IEC 62443-2-1, *Industrial communication networks – Network and system security – Part 2-1: Establishing an industrial automation and control system security program*

[14] IEC 62645, *Nuclear power plants – Instrumentation, control and electrical power systems – Cybersecurity requirements*

[15] IEC ACSEC dashboard available at <https://www.iec.ch/acsec/supportingdocuments>

[16] ISO 31000, *Risk management – Guidelines*

[17] ISO/IEC 27005, *Information security, cybersecurity and privacy protection – Guidance on managing information security risks*

[18] IEC TS 62351-1:2007, *Power systems management and associated information exchange – Data and communications security – Part 1: Communication network and system security – Introduction to security issues*

IECNORM.COM : Click to view the full PDF of IEC GUIDE 120:2023 RLV

[19] ISO/IEC 17007, *Conformity assessment – Guidance for drafting normative documents suitable for use for conformity assessment*

[20] IEC 31010, *Risk management – Risk assessment techniques*

[21] IEC 61508 (all parts), *Functional safety of electrical/electronic/programmable electronic safety-related systems*

[22] IEC 62337:2012, *Commissioning of electrical, instrumentation and control systems in the process industry – Specific phases and milestones*

[23] IEC TS 62351-2:2008, *Power systems management and associated information exchange – Data and communications security – Part 2: Glossary of terms*

[24] IEC TS 62443-1-1:2009, *Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models*

[25] IEC TR 62918:2014, *Nuclear power plants – Instrumentation and control important to safety – Use and selection of wireless devices to be integrated in systems important to safety*

[26] IEC Guide 104:2019, *The preparation of safety publications and the use of basic safety publications and group safety publications*

[27] IEC Guide 108:2019, *Guidelines for ensuring the coherence of IEC publications – Horizontal functions, horizontal publications and their application*

[28] ISO/IEC 24767-1:2008, *Information technology – Home network security – Part 1: Security requirements*

[29] ISO/IEC 27000:2018, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*

[30] ISO/IEC 27002, *Information security, cybersecurity and privacy protection – Information security controls*

[31] ISO/IEC 27009, *Information security, cybersecurity and privacy protection – Sector-specific application of ISO/IEC 27001 – Requirements*

[32] ISO/IEC 27036-1, *Cybersecurity – Supplier relationships – Part 1: Overview and concepts*

[33] ISO/IEC 27036-2, *Cybersecurity – Supplier relationships – Part 2: Requirements*

[34] ISO/IEC 27036-3, *Information technology – Security techniques – Information security for supplier relationships – Part 3: Guidelines for information and communication technology supply chain security*

[35] ISO/IEC 27036-4, *Information technology – Security techniques – Information security for supplier relationships – Part 4: Guidelines for security of cloud services*

[36] ISO/IEC 29100, *Information technology – Security techniques – Privacy framework*

[37] ISO/IEC 29101, *Information technology – Security techniques – Privacy architecture framework*

IECNORM.COM : Click to view the full PDF of IEC GUIDE 120:2023 RLV

[38] ISO/IEC 29115, *Information technology – Security techniques – Entity authentication assurance framework*

[39] ISO/IEC 29191, *Information technology – Security techniques – Requirements for partially anonymous, partially unlinkable authentication*

[40] ISO/IEC Guide 51:2014, *Safety aspects – Guidelines for their inclusion in standards*

[41] ISO/IEC Directives Part 2:2021, *Principles and rules for the structure and drafting of ISO and IEC documents*

[42] NIST SP 800-53, *Security Controls and Assessment Procedures for Federal Information Systems and Organizations*

___________

IECNORM.COM : Click to view the full PDF of IEC GUIDE 120:2023 RLV

IECNORM.COM : Click to view the full PDF of IEC GUIDE 120:2023 RLV

## SOMMAIRE

IECNORM.COM : Click to view the full PDF of IEC GUIDE 120:2023 RLV

IECNORM.COM : Click to view the full PDF of IEC GUIDE 120:2023 RLV

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

____________

# ASPECTS LIÉS À LA SÛRETÉ – LIGNES DIRECTRICES POUR LES INCLURE DANS LES PUBLICATIONS

## AVANT-PROPOS

1) La Commission Electrotechnique Internationale (IEC) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de l'IEC). L'IEC a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, l'IEC – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de l'IEC"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'IEC, participent également aux travaux. L'IEC collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.

2) Les décisions ou accords officiels de l'IEC concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de l'IEC intéressés sont représentés dans chaque comité d'études.

3) Les Publications de l'IEC se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de l'IEC. Tous les efforts raisonnables sont entrepris afin que l'IEC s'assure de l'exactitude du contenu technique de ses publications; l'IEC ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.

4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de l'IEC s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de l'IEC dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de l'IEC et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.

5) L'IEC elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de l'IEC. L'IEC n'est responsable d'aucun des services effectués par les organismes de certification indépendants.

6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.

7) Aucune responsabilité ne doit être imputée à l'IEC, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de l'IEC, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de l'IEC ou de toute autre Publication de l'IEC, ou au crédit qui lui est accordé.

8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.

9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de l'IEC peuvent faire l'objet de droits de brevet. L'IEC ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets.

Cette deuxième édition de l'IEC Guide 120 a été établie, selon les Directives ISO/IEC, Partie 1, Annexe A, par le Comité consultatif sur la sécurité de l'information et la confidentialité des données (ACSEC, *Advisory Committee on Information security and data privacy*).

Cette deuxième édition annule et remplace la première édition parue en 2018.

Les principales modifications par rapport à l'édition précédente sont les suivantes:

a) La terminologie de l'IEC Guide 120 a été alignée sur celle de l'IEC Guide 108:2019.

IECNORM.COM : Click to view the full PDF of IEC GUIDE 120:2023 RLV

Le texte du présent Guide est issu des documents suivants:

| Projet | Rapport de vote |
|---|---|
| SMBNC/39/DV | SMBNC/47/RV |

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à l'approbation du présent Guide.

La langue employée pour l'élaboration du présent Guide est l'anglais.

Cette publication a été rédigée selon les Directives ISO/IEC, Partie 2, elle a été développée selon les Directives ISO/IEC, Partie 1 et les Directives ISO/IEC, Supplément IEC, disponibles sous www.iec.ch/members_experts/refdocs. Les principaux types de documents développés par l'IEC sont décrits plus en détail sous www.iec.ch/standardsdev/publications.

**IMPORTANT – Le logo "colour inside" qui se trouve sur la page de couverture de cette publication indique qu'elle contient des couleurs qui sont considérées comme utiles à une bonne compréhension de son contenu. Les utilisateurs devraient, par conséquent, imprimer cette publication en utilisant une imprimante couleur.**

IECNORM.COM : Click to view the full PDF of IEC GUIDE 120:2023 RLV

# INTRODUCTION

La complexité et la connectivité croissantes des systèmes, des produits, des processus et des services qui arrivent sur le marché exigent d'accorder une priorité élevée à la prise en compte des aspects liés à la sûreté. L'inclusion des aspects liés à la sûreté dans la normalisation assure la protection contre les risques d'événements involontairement et volontairement causés qui peuvent perturber la fonctionnalité et le fonctionnement des produits et des systèmes ainsi que la réponse à ces risques.

Lors de l'élaboration des publications, il convient que les comités veillent à inclure les exigences de résilience pertinentes applicables à leur domaine d'application. Dans de nombreux cas, les aspects liés à la sûreté jouent un rôle dans le respect des normes en matière de résilience.

Dans le présent document, le terme "comité" comprend les comités d'études, les sous-comités et les comités des systèmes. Le terme "publication" couvre les Normes internationales, les Rapports techniques, les Spécifications techniques et les Guides.

L'existence d'exigences juridiques et réglementaires nationales peut avoir une incidence sur l'application générale des publications.

NOTE Les publications peuvent traiter exclusivement des aspects liés à la sûreté ou comprendre des articles spécifiques à la sûreté.

IECNORM.COM : Click to view the full PDF of IEC GUIDE 120:2023 RLV

# ASPECTS LIÉS À LA SÛRETÉ – LIGNES DIRECTRICES POUR LES INCLURE DANS LES PUBLICATIONS

## 1 Domaine d'application

Le présent document fournit des lignes directrices concernant les aspects liés à la sûreté inclus dans les publications de l'IEC et la façon de les mettre en œuvre. Les présentes lignes directrices peuvent servir de liste de contrôle pour la combinaison des publications utilisées dans la mise en œuvre des systèmes.

Le présent document couvre ce qui est souvent appelé la "cybersécurité".

Le présent document ne couvre pas les aspects non électrotechniques liés à la sûreté, tels que la sûreté sociétale, sauf s'ils interagissent directement avec la sûreté électrotechnique.

NOTE Le Bureau en charge de la gestion de la normalisation (SMB, *Standardization Management Board*) de l'IEC a décidé que les Guides tels que celui-ci pouvaient comporter des exigences obligatoires qui doivent être appliquées par l'ensemble des comités de l'IEC en charge de travaux techniques relevant du domaine d'application du Guide, ainsi que des recommandations qui peuvent ne pas être suivies. Toutes les exigences obligatoires établies dans le présent Guide sont introduites par le verbe "devoir". Les énoncés fournis uniquement à titre de recommandations sont introduits par la formule "il convient" (voir les Directives ISO/IEC, Supplément IEC:2021, A.1.1).

## 2 Références normatives

Le présent document ne contient aucune référence normative.

## 3 Termes et définitions

Pour les besoins du présent document, les termes et définitions suivants s'appliquent.

L'ISO et l'IEC tiennent à jour des bases de données terminologiques destinées à être utilisées en normalisation, consultables aux adresses suivantes:

- IEC Electropedia: disponible à l'adresse https://www.electropedia.org/
- ISO Online browsing platform: disponible à l'adresse https://www.iso.org/obp

**3.1**
**imputabilité**
propriété d'un système (y compris toutes ses ressources) qui assure que les actions d'une entité du système ne peuvent être imputées qu'à cette entité, qui peut être tenue pour responsable de ses actions

[SOURCE: En anglais, IEC TS 62443-1-1:2009, 3.2.3]

**3.2**
**attaque**
tentative de détruire, de rendre public, de modifier, d'invalider, de voler ou d'utiliser sans autorisation un actif, ou de faire un usage non autorisé de celui-ci

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

IECNORM.COM : Click to view the full PDF of IEC GUIDE 120:2023 RLV

**3.3**
**authentification**
méthode permettant de garantir qu'une caractéristique revendiquée pour une entité est correcte

[SOURCE: ISO/IEC 27000:2018, 3.5]

**3.4**
**autorisation**
droit ou permission accordé(e) à une entité du système pour accéder à une ressource du système

[SOURCE: En anglais, IEC TS 62443-1-1:2009, 3.2.14]

**3.5**
**disponibilité**
propriété d'être accessible et utilisable à la demande par une entité autorisée

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

**3.6**
**confidentialité**
propriété selon laquelle l'information n'est pas rendue disponible ou divulguée à des personnes ou à des entités ou des processus non autorisés

[SOURCE: En anglais, ISO/IEC 24767-1:2008, 2.1.2]

**3.7**
**sécurité fonctionnelle**
partie de la sécurité générale qui dépend des unités fonctionnelles et physiques fonctionnant correctement en réponse à leurs entrées

[SOURCE: IEC 60050-351:2013, 351-57-06]

**3.8**
**dommage**
blessure physique ou atteinte à la santé des personnes, ou atteinte aux biens ou à l'environnement

[SOURCE: ISO/IEC Guide 51:2014, 3.1]

**3.9**
**intégrité**
propriété d'exactitude et de complétude

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

**3.10**
**non-répudiation**
capacité à prouver l'occurrence d'un événement ou d'une action donnée(e) et des entités qui en sont à l'origine

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

IECNORM.COM : Click to view the full PDF of IEC GUIDE 120:2023 RLV

**3.11**
**risque**
combinaison de la probabilité de l'occurrence d'un dommage et de la gravité de ce dommage

Note 1 à l'article: La probabilité des risques pour la sûreté ne peut souvent pas être déterminée de la même manière que la probabilité des dangers pour la sécurité à partir d'une analyse statistique.

[SOURCE: IEC 60050-351:2013, 351-57-03, modifié – La Note 1 à l'article a été ajoutée.]

**3.12**
**sécurité**
absence de risque intolérable

[SOURCE: ISO/IEC Guide 51:2014, 3.14]

**3.13**
**sûreté**
condition qui résulte de l'établissement et du maintien de mesures de protection qui assurent un état d'inviolabilité vis-à-vis d'actes ou d'influences hostiles

Note 1 à l'article: Les actes ou influences hostiles peuvent être intentionnels ou non.

Note 2 à l'article: Dans la pratique, "sûreté" et "cybersécurité" sont souvent utilisés de manière interchangeable, même si techniquement, la "cybersécurité" peut être considérée comme différente de la "sûreté". Toutefois, le présent document n'établit aucune distinction entre ces termes.

[SOURCE: En anglais, IEC TS 62351-2:2008, 2.2.173, modifié – Les Notes 1 et 2 à l'article ont été ajoutées.]

**3.14**
**contrôle de sûreté**
mesure qui modifie le risque pour la sûreté ou l'utilisation

Note 1 à l'article: Un contrôle de sûreté peut être un processus, une politique, un dispositif, une pratique ou tout autre action.

**3.15**
**service de sûreté**
mécanisme utilisé pour fournir la confidentialité, l'intégrité des données, l'authentification ou la non-répudiation des informations

[SOURCE: En anglais, IEC TS 62443-1-1:2009, 3.2.115]

**3.16**
**menace**
possibilité de violation de la sûreté, qui existe en cas de circonstance, de capacité, d'action ou d'événement susceptible de porter atteinte à la sûreté et de causer des dommages

[SOURCE: En anglais, IEC TS 62443-1-1:2009, 3.2.125]

**3.17**
**fournisseur**
constructeur ou distributeur d'un produit

[SOURCE: IEC 62337:2012, 3.12, modifié – Dans la définition, "équipement/instrument/unité autonome" a été remplacé par "produit".]

IECNORM.COM : Click to view the full PDF of IEC GUIDE 120:2023 RLV

**3.18**
**vulnérabilité**
faille ou faiblesse dans la conception, la mise en œuvre ou l'exploitation et la gestion d'un système qui peut être exploitée pour violer la politique de sûreté du système

Note 1 à l'article: Il convient de ne pas confondre cette définition de la vulnérabilité avec le terme "vulnérabilité" utilisé dans le contexte du management du risque général, qui comprend la notion de possibilité d'exposition à un risque.

[SOURCE: En anglais, IEC TR 62918:2014, 3.16, modifié – La Note 1 à l'article a été ajoutée.]

# 4 Guide de la terminologie

## 4.1 Généralités

Les publications existantes comprennent déjà de nombreux termes et définitions relatifs à la sûreté. Par conséquent, avant de définir un nouveau terme, il convient de vérifier en premier lieu les termes et définitions existants. Les principales sources recommandées sont indiquées en 4.2 et il convient de privilégier leur utilisation à celle des autres sources pertinentes indiquées en 4.3. Si aucun terme et aucune définition appropriés ne sont trouvés dans ces sources, modifier une source existante ou en définir une nouvelle.

Les définitions qui figurent dans le présent document ne sont pas des définitions génériques; elles s'appliquent uniquement au présent document.

L'Article 16 des Directives ISO/IEC Partie 2:2021 définit la façon dont les termes et définitions des publications de l'IEC sont rédigés.

NOTE Le même terme peut avoir différentes définitions selon le contexte dans lequel il est utilisé, ou différents termes peuvent être utilisés pour une signification identique ou similaire dans différents domaines d'application.

## 4.2 Principales sources recommandées

Les principales sources recommandées sont

a) l'IEC 60050 (toutes les parties) (IEV) [1][1];

b) le Glossaire de l'IEC [2]; et

c) SD6 de l'ISO/IEC JTC 1/SC 27 [3].

Il convient d'utiliser en priorité l'IEC 60050 et le Glossaire de l'IEC.

L'IEC 60050 fournit des définitions représentatives pour plus de 20 000 termes, organisées par domaines de l'IEC. Le Glossaire de l'IEC est une compilation de termes électrotechniques extraits de l'article "Termes et définitions" des publications existantes de l'IEC.

Si aucun terme ou définition approprié n'est trouvé dans les deux sources ci-dessus, il convient de consulter SD6 de l'ISO/IEC JTC 1/SC 27, qui couvre davantage de termes et définitions relatifs à la sûreté.

NOTE Les termes spécifiques au domaine d'application établis par les comités de l'IEC sont également considérés comme des sources principales. Ceux-ci peuvent être recherchés sur la page Web du Glossaire de l'IEC.

[1] Les chiffres entre crochets renvoient à la Bibliographie.

IECNORM.COM : Click to view the full PDF of IEC GUIDE 120:2023 RLV

### 4.3 Autres sources pertinentes

#### 4.3.1 Généralités

Il existe une variété de ressources qui concernent certains domaines d'application de l'électrotechnologie, tels que l'énergie, le bâtiment, la santé et les transports.

Cela comprend les sources indépendantes du domaine d'application (4.3.2) et les sources spécifiques au domaine d'application (4.3.3).

#### 4.3.2 Autres sources indépendantes du domaine d'application

- IETF RFC 4949 [4];
- NISTIR 7298 [5];
- IEEE, Standards Glossary [6];
- UIT, Termes et définitions de l'UIT [7].

#### 4.3.3 Autres sources spécifiques au domaine d'application

- Santé: HL7, Glossary Of Acronyms, Abbreviations and Terms Related To Information Security In Healthcare Information Systems [8].
- Nucléaire: AIEA, Glossaire de la série sur la sûreté nucléaire [9].
- Energie: AIE, Glossaire [10].

## 5 Catégorisation des publications

### 5.1 Vue d'ensemble

Les publications de sûreté peuvent être classées de différentes manières. Cinq classes possibles pour la catégorisation sont prises en compte, comme cela est indiqué dans le Tableau 1:

- catégories de publications;
- types de publications;
- domaine d'application;
- contenu;
- utilisateur ou groupe cible.

Les publications peuvent appartenir à plusieurs classes.

Le présent document fournit des informations complémentaires à l'IEC Guide 108 lorsqu'il est fait référence à des publications horizontales de sûreté.

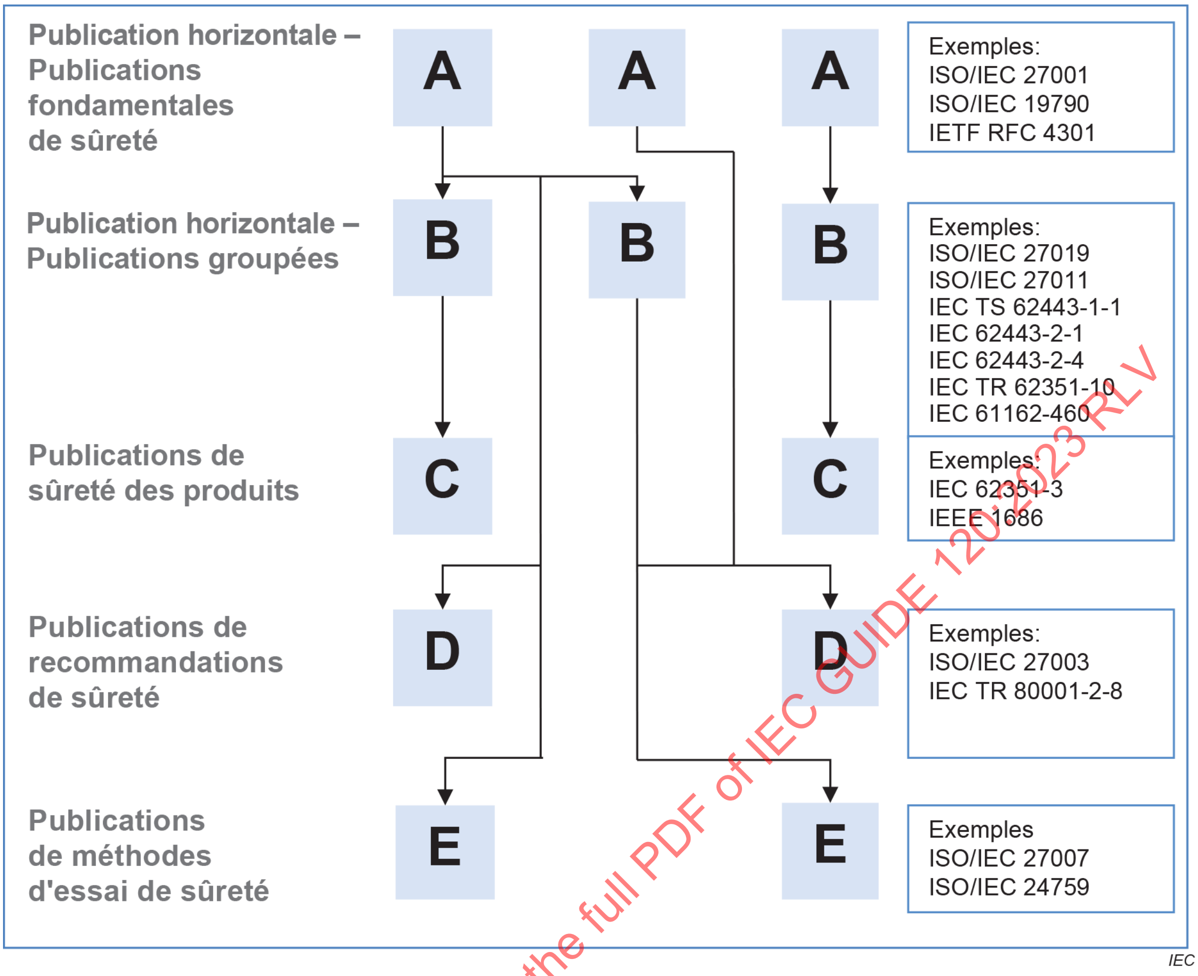
IECNORM.COM : Click to view the full PDF of IEC GUIDE 120:2023 RLV

**Tableau 1 – Catégorisation possible des publications**

| | |
|---|---|
| **Catégories de publications** | Publication horizontale – Publications fondamentales de sûreté (applicables à tous les domaines)<br>Publication horizontale – Publications groupées de sûreté (applicables à un ou plusieurs domaines spécifiés)<br>Publications de sûreté des produits |
| **Types de publications** | Publications de recommandations de sûreté (qui peuvent être des publications horizontales ou non)<br>Publications de méthodes d'essai de sûreté (qui peuvent être des publications horizontales ou non)<br>Configuration |
| **Domaine d'application** | • Bâtiment<br>• Energie<br>• Général<br>• Santé<br>• TIC<br>• Automatisation industrielle<br>• Transports |
| **Contenu** | • Composant<br>• Gestion<br>• Politique<br>• Processus<br>• Sous-système<br>• Système<br>• Technologie |
| **Utilisateur ou groupe cible** | • Auditeur<br>• Intégrateur<br>• Opérateur<br>• Technicien de maintenance<br>• Chargé de la réglementation<br>• Fournisseur |

La Figure 1 donne des exemples de publications de sûreté répertoriées selon les classes proposées.

IECNORM.COM : Click to view the full PDF of IEC GUIDE 120:2023 RLV



NOTE Les exemples de la Figure 1 ne sont pas exhaustifs.

**Figure 1 – Exemples de publications selon différentes classes de catégorisation**

IECNORM.COM : Click to view the full PDF of IEC GUIDE 120:2023 RLV

## 5.2 Catégories de publications

### 5.2.1 Généralités

Les "catégories de publications" proviennent de l'IEC Guide 108:2019 et étendent la définition des différentes catégories proposées pour les publications horizontales afin de tenir pleinement compte du contexte des aspects liés à sûreté. Les catégories de publications prises en compte dans le présent document sont les suivantes:

- Publication horizontale – Publications fondamentales de sûreté (applicables à tous les domaines);
- Publication horizontale – Publications groupées de sûreté;
- Publications de sûreté des produits.

### 5.2.2 Publication horizontale – Publications fondamentales de sûreté (applicables à tous les domaines)

La catégorie "Publication horizontale – Publications fondamentales de sûreté" traite des concepts, principes et exigences fondamentaux en ce qui concerne les aspects généraux liés à la sûreté applicables à un large éventail de produits et de systèmes, et s'applique à tous les domaines.

### 5.2.3 Publication horizontale – Publications groupées de sûreté

La catégorie "Publication horizontale – Publications groupées de sûreté" décrit comment appliquer la sûreté dans l'un des domaines d'application. Pour ce faire, ces publications peuvent faire référence aux publications existantes de la catégorie "Publication horizontale – Publications fondamentales de sûreté" ou adapter celles-ci.

La catégorie "Publication horizontale – Publications groupées de sûreté" peut s'appliquer à de nombreux produits ou systèmes, ou à des familles de produits ou systèmes similaires.

Les publications de la catégorie "Publication horizontale – Publications groupées de sûreté" peuvent être appelée publications sectorielles de sûreté.

### 5.2.4 Publications de sûreté des produits

Les "Publications de sûreté des produits" définissent l'application des publications de la catégorie "Publication horizontale – Publications fondamentales de sûreté" ou "Publication horizontale – Publications groupées de sûreté" pour un type particulier de produit. Ils assurent que différents produits peuvent interagir ou interopérer en toute sécurité, et qu'ils peuvent être contrôlés et gérés de manière uniforme.

Il convient, dans la mesure du possible, que les "Publications de sûreté des produits" définissent leurs exigences en se référant aux publications de la catégorie "Publication horizontale – Publications fondamentales de sûreté" ou "Publication horizontale – Publications groupées de sûreté".

NOTE Dans ce contexte, le terme "produit" englobe des éléments tels que le processus, le service, l'installation, ainsi les combinaisons de ces éléments.

## 5.3 Types de publications

### 5.3.1 Généralités

Les "types de publication" proviennent de l'IEC Guide 108:2019 et étendent la définition des différents types proposés pour les publications horizontales afin de tenir pleinement compte du contexte des aspects liés à sûreté. Les types proposés pris en compte dans le présent document sont les suivants:

- publications de recommandations de sûreté;
- publications de méthodes d'essai de sûreté.

### 5.3.2 Publications de recommandations de sûreté

Il convient que les "Publications de recommandations de sûreté" ne comportent pas d'exigences. Elles expliquent la mise en œuvre des publications de la catégorie "Publication horizontale – Publications fondamentales de sûreté", des publications de la catégorie "Publication horizontale – Publications groupées de sûreté" ou des publications de sûreté des produits.

Dans certains domaines d'application, les publications de recommandations de sûreté ne sont pas utilisées. A la place, les recommandations nécessaires sont fournies par le biais d'annexes informatives dans la norme d'exigences applicable.

### 5.3.3 Publications de méthodes d'essai de sûreté

Les "Publications de méthodes d'essai de sûreté" définissent les moyens qui permettent de déterminer que les exigences des publications de la catégorie "Publication horizontale – Publications fondamentales de sûreté" et de la catégorie "Publication horizontale – Publications groupées de sûreté" ou des publications de sûreté des produits ont été correctement mises en œuvre.

IECNORM.COM : Click to view the full PDF of IEC GUIDE 120:2023 RLV

Les publications de méthodes d'essai de sûreté sont généralement destinées à un public spécialisé et font souvent référence à l'évaluation de la conformité. Elles peuvent définir ou identifier des mises en œuvre de référence qui peuvent être utilisées pour déterminer la mise en œuvre adéquate à travers une interopération réussie.

### 5.4 Domaine d'application

Les publications relatives à la sûreté peuvent également être classées en fonction de leur domaine d'application prévu. Il peut s'agir d'un secteur d'activité économique ou industrielle, d'un type de marché ou d'un champ d'application.

Des exemples de domaines d'application sont donnés ci-dessous (voir Figure 1):

- bâtiment;
- énergie;
- général;
- santé;
- TIC;
- automatisation industrielle;
- transports.

Dans de nombreux cas, un domaine d'application est associé à un comité de l'IEC chargé de l'élaboration des publications pour ce domaine. Il convient que ce comité assume la responsabilité de l'élaboration des publications de sûreté connexes.

Ces comités sont normalement en mesure de définir les modèles de menace pertinents et les cas d'utilisation relatifs à la sûreté de manière indépendante, mais ils peuvent avoir besoin de consulter les comités responsables de la catégorie "Publication horizontale – Publications fondamentales de sûreté" pour configurer ou adapter ces publications fondamentales de sûreté lorsqu'il y est fait référence.

### 5.5 Contenu

Les publications relatives à la sûreté peuvent également être regroupées par type de contenu.

Des exemples de groupes possibles sont donnés ci-dessous (voir Figure 1):

- composant;
- gestion;
- politique (pas dans le cadre de l'IEC);
- processus;
- sous-système;
- système;
- technologie.

Par exemple, les normes électrotechniques relatives aux management de la sécurité de l'information comprennent la norme de la catégorie "Publication horizontale – Publications fondamentales de sûreté" ISO/IEC 27001 [11] (élaborée par le SC 27 du JTC 1 de l'ISO/IEC), mais également les normes sectorielles ISO/IEC 27019 [12] (élaborée par le SC 27 du JTC 1 de l'ISO/IEC), IEC 62443-2-1 [13] (élaborée par le CE 65 de l'IEC) et IEC 62645 [14] (élaborée par le SC 45A de l'IEC).

IECNORM.COM : Click to view the full PDF of IEC GUIDE 120:2023 RLV