IEC GUIDE 120

Edition 2.0 2023-10
REDLINE VERSION

GUIDE

colour
inside

Security aspects – Guidelines for their inclusion in publications

IEC GUIDE 120:2023-10 RLV(en)

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

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

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

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

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 It also gives information on projects, replaced and withdrawn publications.

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

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

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

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

IEC GUIDE 120

Edition 2.0 2023-10
REDLINE VERSION

GUIDE

colour
inside

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.

CONTENTS

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.

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.

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.

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]

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]

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".]

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.

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].

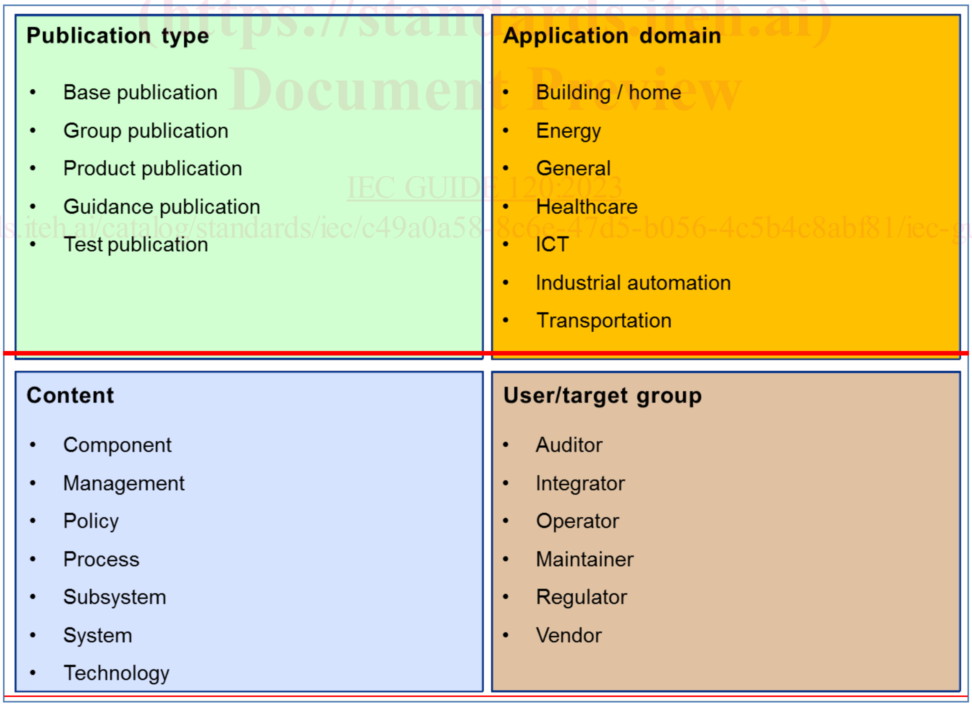
4.3.3 Other application-domain specific sources

- 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**~~

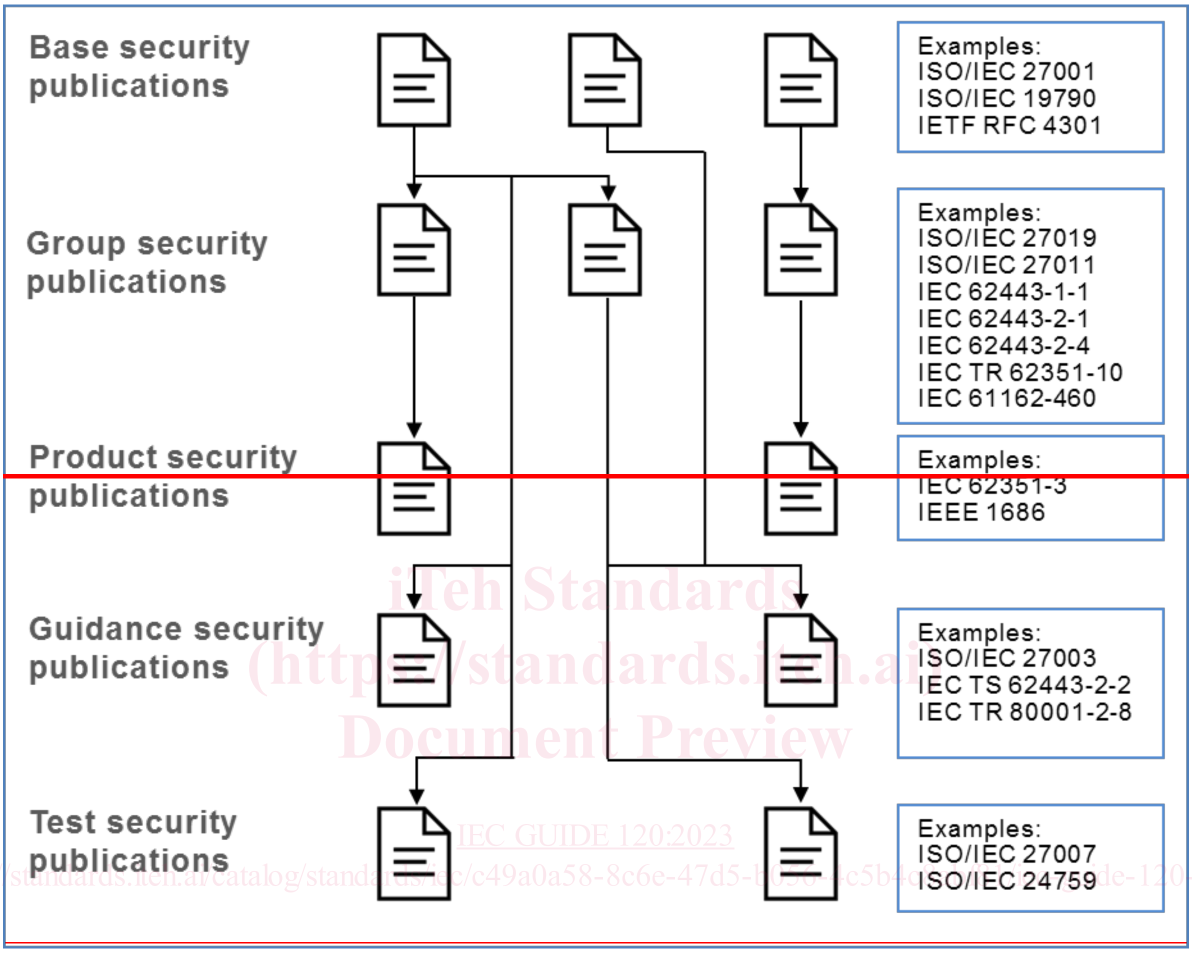
~~5.2 Publication type~~

~~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;~~

- ~~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.~~