

GUIDE

GUIDE



Security aspects – Guidelines for their inclusion in publications

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



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.

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de l'IEC ou du Comité national de l'IEC du pays du demandeur. Si vous avez des questions sur le copyright de l'IEC ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de l'IEC de votre pays de résidence.

IEC Secretariat
3, rue de Varembe
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 It also gives information on projects, replaced and withdrawn publications.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.

A propos de l'IEC

La Commission Electrotechnique Internationale (IEC) est la première organisation mondiale qui élabore et publie des Normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

A propos des publications IEC

Le contenu technique des publications IEC est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

Recherche de publications IEC - webstore.iec.ch/advsearchform

La recherche avancée permet de trouver des publications IEC en utilisant différents critères (numéro de référence, texte, comité d'études, ...). Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

IEC Just Published - webstore.iec.ch/justpublished

Restez informé sur les nouvelles publications IEC. Just Published détaille les nouvelles publications parues. Disponible en ligne et une fois par mois par email.

Service Clients - webstore.iec.ch/csc

Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: sales@iec.ch.

IEC Products & Services Portal - products.iec.ch

Découvrez notre puissant moteur de recherche et consultez gratuitement tous les aperçus des publications. Avec un abonnement, vous aurez toujours accès à un contenu à jour adapté à vos besoins.

Electropedia - www.electropedia.org

Le premier dictionnaire d'électrotechnologie en ligne au monde, avec plus de 22 300 articles terminologiques en anglais et en français, ainsi que les termes équivalents dans 19 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.



Documents

Document Sharing Hub



GUIDE

GUIDE



Security aspects – Guidelines for their inclusion in publications

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

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 35.030

ISBN 978-2-8322-6434-8

Warning! Make sure that you obtained this publication from an authorized distributor.
Attention! Veuillez vous assurer que vous avez obtenu cette publication via un distributeur agréé.

CONTENTS

FOREWORD.....	4
INTRODUCTION.....	6
1 Scope.....	7
2 Normative references	7
3 Terms and definitions	7
4 Guide to terminology	10
4.1 General.....	10
4.2 Primary recommended sources	10
4.3 Other relevant sources.....	10
4.3.1 General	10
4.3.2 Other application-domain independent sources.....	10
4.3.3 Other application-domain specific sources	11
5 Categorization of publications.....	11
5.1 Overview.....	11
5.2 Publication categories.....	12
5.2.1 General	12
5.2.2 Horizontal publication – Basic security publications (applicable to any domain)	12
5.2.3 Horizontal publication – Group security publications	13
5.2.4 Product security publications	13
5.3 Publication types	13
5.3.1 General	13
5.3.2 Guidance security publications	13
5.3.3 Test methods security publications	13
5.4 Application domain.....	14
5.5 Content.....	14
5.6 User or target group.....	14
5.7 Developing security publications	15
5.7.1 Basic security publications.....	15
5.7.2 Horizontal publication – Group security publications	15
5.7.3 Product security publications	16
5.7.4 Guidance security publications and test security publications	16
6 Mapping and overview of publications	16
6.1 General.....	16
6.2 List of relevant publications.....	16
6.3 Domain table chart.....	17
7 Considerations for publications development.....	17
7.1 Practical considerations for publication writers.....	17
7.2 Development process of security in publications	17
7.3 Interrelation between functional safety and security	20
7.4 Specific requirements	21
7.4.1 Relationship with "Horizontal publication – Basic security publications"	21
7.4.2 Consider conformity assessment when writing standards.....	21
7.4.3 IEC Horizontal security functions and Group security functions.....	22
7.4.4 Lifecycle approach.....	22
7.4.5 Holistic system view	23

7.4.6	Vulnerability handling	23
7.4.7	Defence-in-depth	23
7.4.8	Security management	23
7.4.9	Supply chain	24
7.4.10	Consider greenfield and brownfield	24
7.4.11	Use of term integrity	24
7.5	Security risk assessment	24
7.5.1	General	24
7.5.2	Iterative process of security risk assessment and risk mitigation	25
7.5.3	Maintaining safe operation	25
7.5.4	Scenario analysis	26
7.5.5	Security risk mitigation strategy	26
7.5.6	Validation	27
Bibliography		28
Figure 1 – Examples of publications according to different categorization classes		12
Figure 2 – Publications and application domains		17
Figure 3 – Example of security requirements, threats, and possible attacks		18
Figure 4 – Decision flow chart		19
Figure 5 – Interrelation between functional safety and security		20
Figure 6 – Example of security management cycle for an organization		22
Figure 7 – Selected measures for defence-in-depth strategy		23
Figure 8 – Possible impact of security risk or risks on the safety-related control system		26
Table 1 – Possible categorization of publications		11

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.

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 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 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.)

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.]

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.]

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.

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;

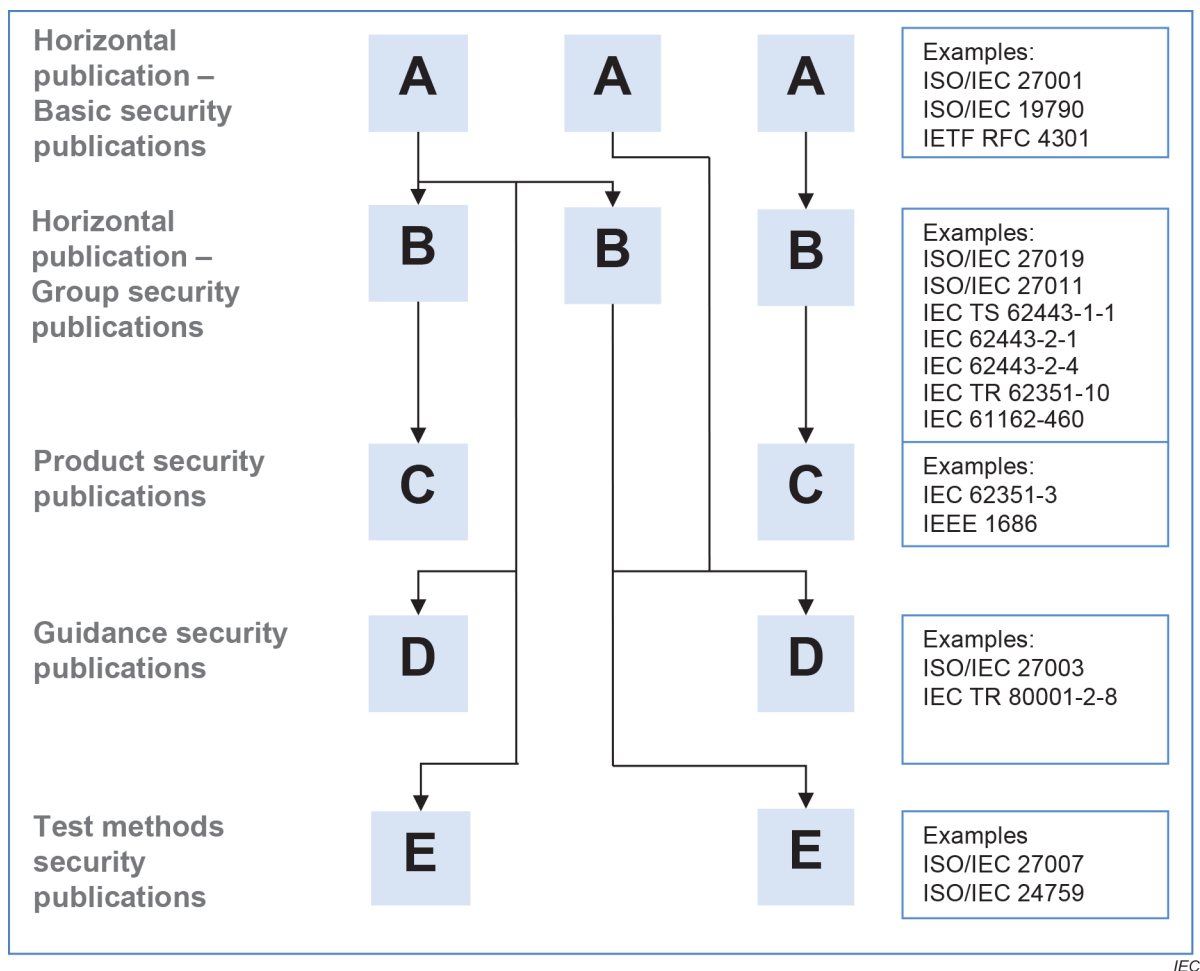
Publications can belong to more than one class.

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

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.

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 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.

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.

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.

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

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.

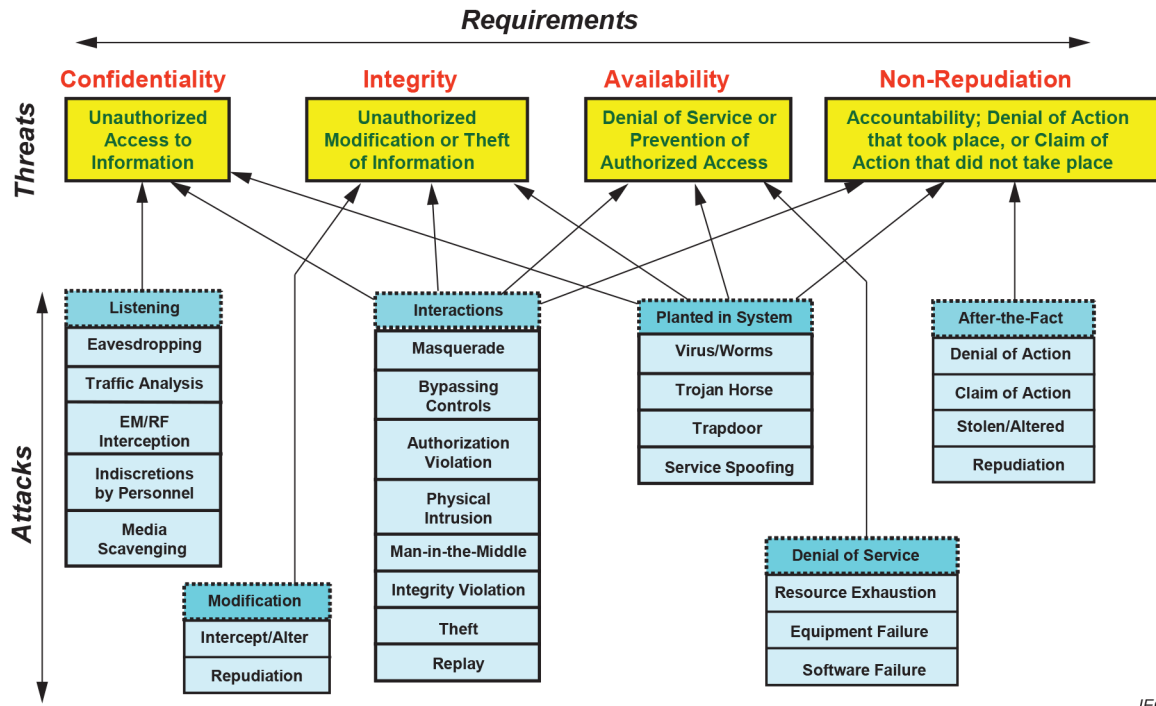
Moreover, security considerations in publications should not specify any particular or commercial solution to address requirements, but should adopt a generic approach to provide security recommendations.

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.



IEC

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

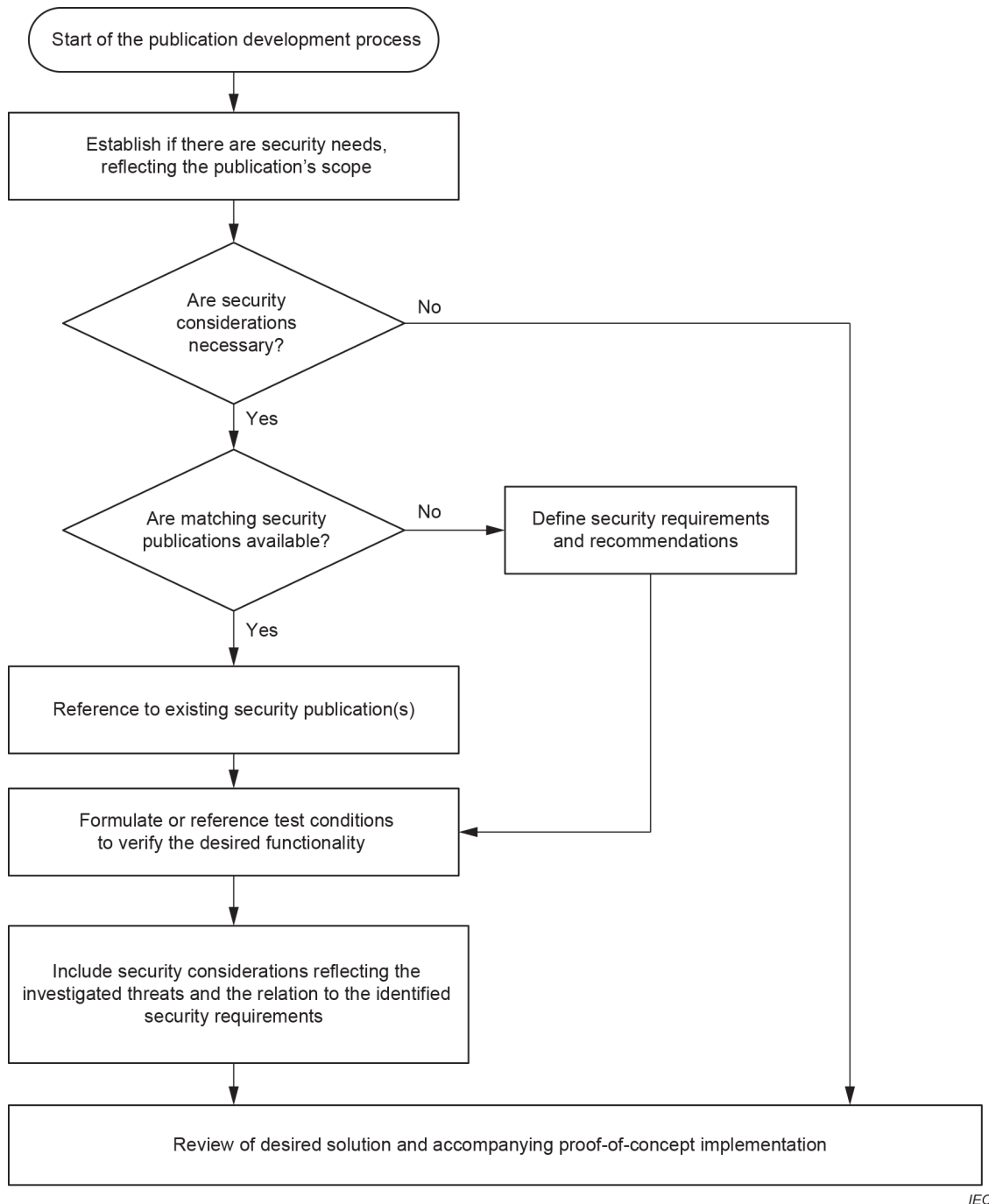
Figure 3 – Example of security requirements, threats, and possible attacks

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.



IEC

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.