

GUIDE



Security aspects – Guidelines for their inclusion in publications





THIS PUBLICATION IS COPYRIGHT PROTECTED
Copyright © 2018 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 Central Office
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 corrigenda or an amendment might have been published.

IEC Catalogue - webstore.iec.ch/catalogue

The stand-alone application for consulting the entire bibliographical information on IEC International Standards, Technical Specifications, Technical Reports and other documents. Available for PC, Mac OS, Android Tablets and iPad.

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 It also gives information on projects, replaced and withdrawn publications.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 also once a month by email.

Electropedia - www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing 21 000 terms and definitions in English and French, with equivalent terms in 16 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary

67 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

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.

GUIDE



Security aspects – Guidelines for their inclusion in publications

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 35.030

ISBN 978-2-8322-5827-9

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

CONTENTS

FOREWORD.....	4
INTRODUCTION.....	6
1 Scope.....	7
2 Normative references	7
3 Terms and definitions	7
4 Guide to terminology	9
4.1 General.....	9
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	10
5 Categorisation of publications.....	11
5.1 Overview.....	11
5.2 Publication type	11
5.2.1 General	11
5.2.2 Base security publications	12
5.2.3 Group security publications	12
5.2.4 Product security publications	13
5.2.5 Guidance security publications	13
5.2.6 Test security publications	13
5.2.7 Relationship between types of security publications.....	13
5.3 Application domain.....	13
5.4 Content.....	14
5.5 User/target group.....	14
5.6 Developing security publications	14
5.6.1 Base security publications	14
5.6.2 Group security publications	15
5.6.3 Product security publications	15
5.6.4 Guidance security publications and test security publications	15
6 Mapping/overview of publications	16
6.1 General.....	16
6.2 List of relevant publications.....	16
6.3 Domain table chart.....	16
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 base security publications	21
7.4.2 Consider conformity assessment when writing standards.....	21
7.4.3 Lifecycle approach.....	22
7.4.4 Holistic system view	22
7.4.5 Vulnerability handling	23
7.4.6 Defence-in-depth	23
7.4.7 Security management	23

7.4.8 Supply chain..... 23

7.4.9 Consider greenfield and brownfield..... 24

7.4.10 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 26

Bibliography..... 27

Figure 1 – Possible categorization of publications 11

Figure 2 – Types of publications 12

Figure 3 – Publications and application domains..... 16

Figure 4 – Example of security requirements, threats, and possible attacks 17

Figure 5 – Decision flow chart..... 19

Figure 6 – Interrelation between functional safety and security 20

Figure 7 – Example of security management cycle for an organization..... 22

Figure 8 – Selected measures for defence-in-depth strategy..... 23

Figure 9 – Possible impact of security risk(s) on the safety-related control system..... 25

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 first 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 is a non-mandatory guide in accordance with SMB Decision 136/8.

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

DV	Report on voting
C/2086/DV	C/2113A/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.

This document has been drafted in accordance with the ISO/IEC Directives, Part 2.

A bilingual version of this publication may be issued at a later date.

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/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 guide, the term “committee”, includes technical committees, subcommittees and system committees. The term “publication” includes “standard”, “technical report”, “technical specification” and “guide”.

National laws (legislation and regulation) may override 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 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 “cyber security”.

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

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*

3 Terms and definitions

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

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

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

3.1

accountability

property of a system (including all of its system resources) that ensures that the actions of a system entity may 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, 2.3]

3.3

authentication

provision of assurance that a claimed characteristic of an entity is correct

[SOURCE: ISO/IEC 27000:2016, 2.7]