

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 It also gives information on projects, replaced and withdrawn publications.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

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.