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

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.

® Registered trademark of the International Electrotechnical Commission
Marque déposée de la Commission Electrotechnique Internationale

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

SOMMAIRE

AVANT-PROPOS 34
INTRODUCTION 36
1 Domaine d'application 37
2 Références normatives 37
3 Termes et définitions 37
4 Guide de la terminologie 40
4.1 Généralités 40
4.2 Principales sources recommandées 40
4.3 Autres sources pertinentes 41
4.3.1 Généralités 41
4.3.2 Autres sources indépendantes du domaine d'application 41
4.3.3 Autres sources spécifiques au domaine d'application 41
5 Catégorisation des publications 41
5.1 Vue d'ensemble 41
5.2 Catégories de publications 43
5.2.1 Généralités 43
5.2.2 Publication horizontale – Publications fondamentales de sûreté (applicables à tous les domaines) 43
5.2.3 Publication horizontale – Publications groupées de sûreté 44
5.2.4 Publications de sûreté des produits 44
5.3 Types de publications 44
5.3.1 Généralités 44
5.3.2 Publications de recommandations de sûreté 44
5.3.3 Publications de méthodes d'essai de sûreté 44
5.4 Domaine d'application 45
5.5 Contenu 45
5.6 Utilisateur ou groupe cible 46
5.7 Élaboration des publications de sûreté 46
5.7.1 Publications fondamentales de sûreté 46
5.7.2 Publication horizontale – Publications groupées de sûreté 46
5.7.3 Publications de sûreté des produits 47
5.7.4 Publications de recommandations de sûreté et publications d'essai de sûreté 47
6 Cartographie et vue d'ensemble des publications 47
6.1 Généralités 47
6.2 Liste des publications pertinentes 48
6.3 Graphique comparatif des domaines 48
7 Considérations relatives à l'élaboration des publications 49
7.1 Considérations pratiques pour les rédacteurs de publications 49
7.2 Processus d'élaboration de la sûreté dans les publications 49
7.3 Corrélation entre la sécurité fonctionnelle et la sûreté 53
7.4 Exigences spécifiques 54
7.4.1 Relation avec la catégorie "Publication horizontale – Publications fondamentales de sûreté" 54
7.4.2 Prise en compte de l'évaluation de la conformité lors de la rédaction des normes 54

7.4.3 Fonctions horizontales de sûreté et fonctions groupées de sûreté de l'IEC 55
7.4.4 Approche fondée sur le cycle de vie 55
7.4.5 Vue globale du système 56
7.4.6 Gestion de la vulnérabilité 56
7.4.7 Défense en profondeur 56
7.4.8 Management de la sûreté 57
7.4.9 Chaîne d'approvisionnement 57
7.4.10 Prise en compte des zones vertes et des friches industrielles 57
7.4.11 Utilisation du terme "intégrité" 58
7.5 Appréciation du risque pour la sûreté 58
7.5.1 Généralités 58
7.5.2 Processus itératif d'appréciation du risque pour la sûreté et d'atténuation du risque 59
7.5.3 Maintien du fonctionnement en toute sécurité 59
7.5.4 Analyse de scénarios 59
7.5.5 Stratégie d'atténuation du risque pour la sûreté 60
7.5.6 Validation 60
Bibliographie 61

Figure 1 – Exemples de publications selon différentes classes de catégorisation 43
Figure 2 – Publications et domaines d'application 48
Figure 3 – Exemple d'exigences de sûreté, de menaces et d'attaques possibles 50
Figure 4 – Diagramme de décision 52
Figure 5 – Corrélation entre la sécurité fonctionnelle et la sûreté 53
Figure 6 – Exemple de cycle de management de la sûreté pour une organisation 56
Figure 7 – Sélection de mesures pour une stratégie de défense en profondeur 57
Figure 8 – Incidence possible du ou des risques pour la sûreté sur le système de contrôle relatif à la sécurité 59

Tableau 1 – Catégorisation possible des publications 42

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.

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.

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.

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.