IEC 63208

Edition 1.0 2025-08

INTERNATIONAL STANDARD

NORME INTERNATIONALE

Low-voltage switchgear and controlgear and their assemblies - Security requirements

Appareillages et ensembles d'appareillages à basse tension - Exigences de sécurité

ICS 29.130.20

ISBN 978-2-8327-0604-6

IEC 63208:2025-08(en-fr)

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 It also gives information on projects, replaced and withdrawn publications.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, graphical symbols and the glossary. 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 22 500 terminological entries in English and French, with equivalent terms in 25 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, symboles graphiques et le glossaire. 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 22 500 articles terminologiques en anglais et en français, ainsi que les termes équivalents dans 25 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

CONTENTS

FOREWORD....8
INTRODUCTION....10
1 Scope....12
2 Normative references....13
3 Terms, definitions and abbreviated terms....13
3.1 Terms and definitions....13
3.2 Abbreviated terms....19
4 General....20
5 Security objectives....20
6 Security lifecycle management....20
6.1 General....20
6.2 Security risk assessment....22
6.2.1 General....22
6.2.2 Relationship between safety and security....23
6.2.3 Impact assessment....24
6.2.4 Security risk assessment result....24
6.3 Response to security risk....24
6.4 Security requirement specification....25
6.5 Roles and responsibilities....25
6.6 Important data....26
6.7 Control system architecture....26
6.7.1 Control system....26
6.7.2 Levels of communication functionalities....26
6.7.3 Levels of connectivity....28
6.7.4 Exposure levels of equipment....30
6.7.5 Equipment security levels....30
6.7.6 Security protection profile....31
7 Security requirements....32
7.1 General....32
7.2 Physical access and environment....32
7.2.1 PA – Physical access and environment requirement....32
7.2.2 Physical access and environment rationale....32
7.2.3 PA-e – Physical access and environment enhancement....33
7.2.4 Physical access and environment typical implementation....34
7.3 Equipment requirement....34
7.3.1 General....34
7.3.2 FR 1 – Identification and authentication control....35
7.3.3 FR 2 – Use control....39
7.3.4 FR 3 – System integrity....44
7.3.5 FR 4 – Data confidentiality....50
7.3.6 FR 5 – Restricted data flow....51
7.3.7 FR 6 – Timely response to events....51
7.3.8 FR 7 – Resource availability....52
8 Instructions for installation, operation and maintenance....55
8.1 User instruction requirement....55
8.2 User instruction enhancement....56

8.3 User instruction implementation 56
9 Conformance verification and testing 57
9.1 General 57
9.2 Design documentation 57
9.3 Physical access 57
9.3.1 Verification of physical access and environment 57
9.3.2 Verdict criterion 57
9.3.3 Physical access and environment enhancement 57
9.3.4 Verdict criterion 57
9.4 FR 1 – Identification and authentication control 57
9.4.1 CR 1.1 – Human user identification and authentication 57
9.4.2 CR 1.2 – Software and equipment identification and authentication 58
9.4.3 CR 1.5 – Authenticator management 58
9.4.4 CR 1.7 – Strength of password-based authentication 59
9.4.5 CR 1.8 – Public key infrastructure certificates 59
9.4.6 CR 1.9 – Strength of public key-based authentication 60
9.4.7 CR 1.10 – Authenticator feedback 60
9.4.8 CR 1.11 – Unsuccessful login attempts 60
9.4.9 CR 1.14 – Strength of symmetric key-based authentication 61
9.5 FR 2 – Use control 61
9.5.1 CR 2.1 – Authorisation enforcement 61
9.5.2 CR 2.2 – Wireless use control 61
9.5.3 EDR 2.4 – Mobile code 62
9.5.4 CR 2.5 – Session lock 62
9.5.5 CR 2.6 – Remote session termination 62
9.5.6 CR 2.7 – Concurrent session control 63
9.5.7 CR 2.8 – Auditable events 63
9.5.8 CR 2.9 – Audit storage capacity 63
9.5.9 CR 2.10 – Response to audit processing failures 64
9.5.10 CR 2.11 – Timestamps 64
9.5.11 CR 2.12 – Non-repudiation 65
9.5.12 EDR 2.13 – Use of physical diagnostic and test interfaces 65
9.6 FR 3 – System integrity 65
9.6.1 CR 3.1 – Communication integrity 65
9.6.2 EDR 3.2 – Protection from malicious code 66
9.6.3 CR 3.3 – Security functionality verification 66
9.6.4 CR 3.4 – Software and information integrity 66
9.6.5 CR 3.5 – Input validation 67
9.6.6 CR 3.6 – Deterministic output 67
9.6.7 CR 3.7 – Error handling 67
9.6.8 CR 3.8 – Session Integrity 67
9.6.9 CR 3.9 – Protection of audit information 68
9.6.10 EDR 3.10 – Support for updates 68
9.6.11 EDR 3.11 – Physical tamper resistance and detection 68
9.6.12 EDR 3.12 – Provisioning product supplier roots of trust 69
9.6.13 EDR 3.13 – Provisioning asset owner roots of trust 69
9.6.14 EDR 3.14 – Integrity of the boot process 69
9.7 FR 4 – Data confidentiality 70
9.7.1 CR 4.1 – Information confidentiality 70

9.7.2 CR 4.3 – Use of cryptography 70
9.8 FR 6 – Timely response to events 70
9.8.1 CR 6.1 – Audit log accessibility 70
9.9 FR 7 – Resource availability 71
9.9.1 CR 7.1 – Denial of service protection 71
9.9.2 CR 7.2 – Resource management 71
9.9.3 CR 7.3 – Control system backup 71
9.9.4 CR 7.4 – Control system recovery and reconstitution 72
9.9.5 CR 7.6 – Network and security configuration settings 72
9.9.6 CR 7.7 – Least functionality 72
9.9.7 CR 7.8 – Control system inventory 72
Annex A (informative) Cybersecurity and electrical system architecture 74
A.1 General 74
A.2 Typical architecture involving switchgear, controlgear and their assembly 74
A.2.1 Building 74
A.2.2 Manufacturing 75
Annex B (informative) Use case studies 77
B.1 General 77
B.2 Use case 1 – Protection against Denial of Service (DoS) attack 78
B.3 Use case 2 – Protection against unauthorised modification of sensing device 79
B.4 Use case 3 – Protection against unauthorised modification of wireless equipment 80
B.5 Use case 4 – Protection against threat actor remotely taking control of a "managing" intelligent assembly 81
Annex C (informative) Development methods of cybersecurity measures 82
Annex D (informative) Security related instructions in the product documentation 83
D.1 General 83
D.2 Risk assessment and security planning 83
D.2.1 Risk assessment 83
D.2.2 Security plan 83
D.3 Recommendations for design and installation of the system integrating switchgear, controlgear and their assemblies 84
D.3.1 General access control 84
D.3.2 Recommendations for local access 84
D.3.3 Recommendations for remote access 85
D.3.4 Recommendations for firmware upgrades 86
D.3.5 Recommendations for the end of life 86
D.4 Instructions for an assembly 86
Annex E (normative) Security protection profile of soft-starter and semiconductor controller 87
E.1 Introduction 87
E.1.1 Security protection profile reference 87
E.1.2 Target of evaluation overview 87
E.1.3 General mission objectives 88
E.1.4 Features 88
E.1.5 Product usage 88
E.1.6 Users 88
E.2 Assumptions 89
E.3 Conformance claims and conformance statement 89

E.4 Security problem definition 89
E.4.1 Critical assets of the environment 89
E.4.2 ToE critical assets 90
E.4.3 Threat modelFR 7 – Resource availability 90
E.5 Security objectives 91
E.6 Security requirements 91
E.6.1 Security functional requirements 91
E.6.2 Security assurance requirements 91
Annex F (normative) Security protection profile of network connected motor starter 92
F.1 Introduction 92
F.1.1 Security protection profile reference 92
F.1.2 Target of evaluation overview 92
F.1.3 General mission objectives 93
F.1.4 Features 93
F.1.5 Product usage 93
F.1.6 Users 93
F.2 Assumptions 94
F.3 Conformance claims and conformance statement 94
F.4 Security problem definition 94
F.4.1 Critical assets of the environment 94
F.4.2 ToE critical assets 95
F.4.3 Threat model 95
F.5 Security objectives 96
F.6 Security requirements 96
F.6.1 Security functional requirements 96
F.6.2 Security assurance requirements 96
Annex G (normative) Security protection profile of circuit-breaker 97
G.1 Introduction 97
G.1.1 Security protection profile reference 97
G.1.2 Target of evaluation overview 97
G.1.3 General mission objectives 98
G.1.4 Features 98
G.1.5 Product usage 98
G.1.6 Users 98
G.2 Assumptions 99
G.3 Conformance claims and conformance statement 99
G.4 Security problem definition 99
G.4.1 Critical assets of the environment 99
G.4.2 ToE critical assets 100
G.4.3 Threat model 100
G.5 Security objectives 101
G.6 Security requirements 101
G.6.1 Security functional requirements 101
G.6.2 Security assurance requirements 101
Annex H (normative) Security protection profile of transfer switch equipment 102
H.1 Introduction 102
H.1.1 Security protection profile reference 102
H.1.2 Target of evaluation overview 102
H.1.3 General mission objectives 103

H.1.4 Features 103
H.1.5 Product usage 103
H.1.6 Users 103
H.2 Assumptions 104
H.3 Conformance claims and conformance statement 104
H.4 Security problem definition 104
H.4.1 Critical assets of the environment 104
H.4.2 ToE critical assets 105
H.4.3 Threat model 105
H.5 Security objectives 106
H.6 Security requirements 106
H.6.1 Security functional requirements 106
H.6.2 Security assurance requirements 107
Annex I (normative) Security protection profile for wireless controlgear with its communication interface 108
I.1 Introduction 108
I.1.1 Security protection profile reference 108
I.1.2 Target of evaluation overview 108
I.1.3 General mission objectives 109
I.1.4 Features 109
I.1.5 Product usage 109
I.1.6 Users 109
I.2 Assumptions 109
I.3 Conformance claims and conformance statement 110
I.4 Security problem definition 110
I.4.1 Critical assets of the environment 110
I.4.2 ToE critical assets 110
I.4.3 Threat model 111
I.5 Security objectives 111
I.6 Security requirements 112
I.6.1 Security functional requirements 112
I.6.2 Security assurance requirements 112
Annex J (informative) Equipment requirements by level of exposure 113
Annex K (informative) Bridging references to cybersecurity management systems 115
Annex L (informative) Mapping of provisions to the essential cybersecurity requirements of the European Cyber Resilient Act Annexes 120
Bibliography 123

Figure 1 – Standard landscape 11
Figure 2 – Example of physical interfaces of an embedded device in an equipment which can be subject to an attack 22
Figure 3 – Example of relation between security and safety 23
Figure 4 – Control system architecture with switchgear and controlgear 27
Figure 5 – Control system connectivity level C1 28
Figure 6 – Control system connectivity level C2 28
Figure 7 – Control system connectivity level C3 28
Figure 8 – Control system connectivity level C4 29
Figure 9 – Control system connectivity level C5 29

Figure 10 – Structure of a security protection profile 31
Figure 11 – Example of security instruction symbol 56
Figure A.1 – Building electrical architecture 75
Figure A.2 – Industrial plants 76
Figure E.1 – Machinery control architecture 87
Figure F.1 – Machinery control architecture 92
Figure G.1 – Circuit-breaker in its environment 97
Figure H.1 – Functional units of the transfer switch equipment 102
Figure I.1 – Machinery control architecture 108

Table 1 – Potential attack levels 21
Table 2 – Typical threats 21
Table 3 – Impact evaluation 24
Table 4 – Roles related to security responsibilities 25
Table 5 – Level of exposure of an equipment 30
Table 6 – Equipment security level 31
Table 7 – Physical access related requirement references 33
Table 8 – Physical access enhancement related requirement references 33
Table B.1 – List of actors 77
Table B.2 – Base line requirement 77
Table B.3 – Security problems of use cases 77
Table E.1 – Security requirements for the critical assets of the environment 89
Table E.2 – Security requirements for the critical assets 90
Table E.3 – Security functional requirements 91
Table F.1 – Security requirements for the critical assets of the environment 95
Table F.2 – Security requirements for the critical assets 95
Table F.3 – Security functional requirements 96
Table G.1 – Security requirements for the critical assets of the environment 100
Table G.2 – Security requirements for the critical assets 100
Table G.3 – Security functional requirements 101
Table H.1 – Security requirements for the critical assets of the environment 105
Table H.2 – Security requirements for the critical assets 105
Table H.3 – Security functional requirements 106
Table I.1 – Security requirements for the critical assets of the environment 110
Table I.2 – Security requirements for the critical assets 111
Table I.3 – Security functional requirements 112
Table J.1 – Equipment requirements by level of exposure 113
Table K.1 – Useful security standards 115
Table K.2 – Contribution of switchgear, controlgear and their assemblies to ISO and IEC horizontal security framework 117
Table K.3 – Mapping to other security framework 118
Table K.4 – Requirements for IACS not relevant for switchgear, controlgear and their assemblies 118

Table K.5 – Requirements for IoT device not relevant for switchgear, controlgear and their assemblies 119
Table L.1 – Mapping to the essential cybersecurity requirements of the CRA Annex I 120

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

Low-voltage switchgear and controlgear and their assemblies - Security requirements

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) IEC draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). IEC takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, IEC had not received notice of (a) patent(s), which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at https://patents.iec.ch. IEC shall not be held responsible for identifying any or all such patent rights.

IEC 63208 has been prepared by IEC technical committee 121: Switchgear and controlgear and their assemblies for low voltage. It is an International Standard.

This first edition cancels and replaces the first edition IEC TS 63208 published in 2020. This edition constitutes a technical revision.

This edition includes the following significant technical changes with respect to the previous edition:

a) Risk assessment: Attack levels, impact assessment, relationship with safety;
b) Risk objectives: Determination of the equipment security level;
c) Countermeasures referring to IEC 62443-4-2;
d) Conformance verification and testing;
e) Security protection profiles.

The text of this International Standard is based on the following documents:

Draft	Report on voting
121/221/FDIS	121/230/RVD

Full information on the voting for its approval can be found in the report on voting indicated in the above table.

The language used for the development of this International Standard is English.

This document was drafted in accordance with 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/publications.

The committee has decided that the contents of this document will remain unchanged until the stability date indicated on the IEC website under webstore.iec.ch in the data related to the specific document. At this date, the document will be

- reconfirmed,
- withdrawn, or
- revised.

INTRODUCTION

The growing use of data communication capabilities by switchgear, controlgear and their assemblies (called "equipment" in this document) automatically increases cybersecurity risks. In addition, information technology is more often interconnected to and even integrated into industrial systems which therefore increase this risk.

Very often, switchgear such as circuit-breakers, or controlgear such as overload relays or proximity switches, are equipped with data communication interface. They can be connected to a logic controller or remote display, with local and remote connectivity for giving access to data such as settings, actual power supply values, monitoring data, data logging, control and firmware update.

For these typical applications of electrical distribution and machinery, minimum cybersecurity requirements are necessary for maintaining an acceptable level of safety integrity of the main functions for equipment, with or without data communication capability. These requirements are intended to limit the vulnerability of the data communication interfaces. To keep the largest freedom of innovation, the relevant requirements for a defined application are determined preferably by a systematic risk assessment approach.

The intention of this document is to:

1) provide minimum sets of cybersecurity requirements called security protection profiles for equipment to mitigate the likelihood of unintended operation and loss of protective functions in the context of electrical distribution installations and control systems of machinery;
2) provide the test methods for verifying the implementation of the cybersecurity countermeasure within the equipment;
3) provide guidance to avoid impairing the main function of the equipment, in all operating modes, as a consequence of the implementation of security countermeasures.

This document gives guidance on countermeasures applicable to the design of the equipment (hardware, firmware, network interface, access control, system) and on additional countermeasures to be considered for the implementation and instruction for use.

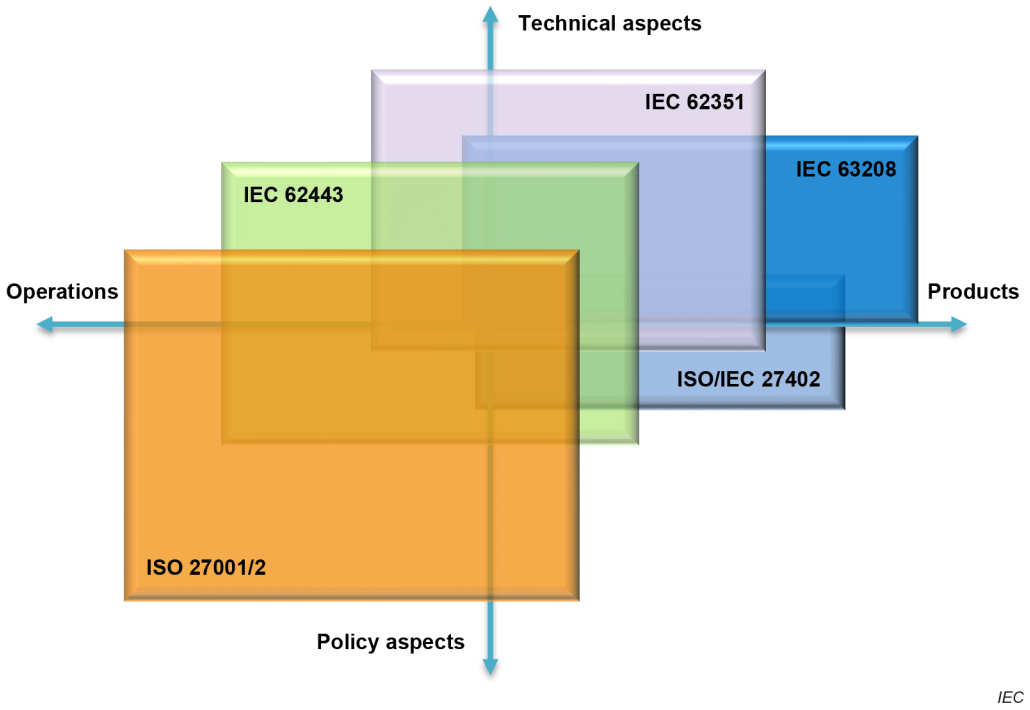

Figure 1 – Standard landscape

Figure 1 positions the landscape of the standards considered in this document with respect to governance and policy aspects, cybersecurity operation aspects, technical details and product requirements. ISO/IEC 27001 and its family of standards are used in many organisations for managing the cybersecurity of information systems and general business. The cybersecurity of industrial control systems is more focussed on maintaining the integrity and the availability of its main functions. IEC 62443 is currently specialised on the generic requirements for process automation system at activity levels 2 and 3 of IEC 62264-1. This document considers the use of the equipment in the activity level 1 of IEC 62264-1 with the cybersecurity of electrical distribution boards and machinery with secured power control and control switching end components. As an example, the principle of systematic and uniformed Security Level requirements SL-1 to SL-4 of IEC 62443-4-2 for the automation components of a control system in a process zone is not relevant for switchgear, controlgear and their assemblies because of their associated cybersecurity risks mainly depending on their limited levels of functionality and their wide possible levels of exposure. Consequently, this document provides minimum cybersecurity requirements depending on these conditions.

This document uses relevant references to the base security publication ISO/IEC 27001 for general aspects and for consistency with the cybersecurity management system of IT systems, to the sector specific standard IEC 62443 for managing aspects related to OT systems, to ISO/IEC 27402 for IoT functionalities and to the applicable security techniques from IEC 62351 (all parts).

Product specific requirements are given in the form of security protection profiles (6.7.6) by category of equipment. Their structure is following Annex B of ISO/IEC 15408-1:2022 and their content can include additional requirements to IEC 62443 standards.

NOTE These product security protection profiles are not equivalent to IEC 62443 security profile defined by IEC TS 62443-1-5 which are limited to the existing content of IEC 62443 standards.

The content of this document is intended to be referenced by product standards.

1 Scope

This document applies to the main functions of switchgear and controlgear and their assemblies, called equipment, in the context of operational technology (OT 3.1.34). It is applicable to equipment with wired or wireless data communication means and their physical accessibility, within their limits of environmental conditions. It is intended to achieve the appropriate physical and cybersecurity mitigation against vulnerabilities to security threats.

This document provides requirements on the appropriate:

– security risk assessment to be developed including the attack levels, the typical threats, the impact assessment and the relationship with safety;
– levels of exposure of the communication interface and the determination of the equipment security level;
– assessment of the exposure level of the communication interfaces;
– assignment of the required security measures for the equipment;
– countermeasures for the physical access and the environment derived from ISO/IEC 27001;
– countermeasures referring to IEC 62443-4-2 with their criteria of applicability;
– user instructions for installation, operation and maintenance;
– conformance verification and testing, and
– security protection profiles by family of equipment (Annex E to Annex I).

In particular, it focuses on potential vulnerabilities to threats resulting in:

– unintended operation, which can lead to hazardous situations;
– unavailability of the protective functions (overcurrent, earth fault, etc.);
– other degradation of main function.

It also provides guidance on the cybersecurity management with the:

– roles and responsibilities (Table 4);
– typical architectures (Annex A);
– use cases (Annex B);
– development methods (Annex C);
– recommendations to be provided to users and for integration into an assembly (Annex D);
– bridging references to cybersecurity management systems (Annex K).

This document does not cover security requirements for:

– information technology (IT);
– industrial automation and control systems (IACS), engineering workstations and their software applications;
– critical infrastructure or energy management systems;
– network device (communication network switch or virtual private network terminator), or
– data confidentiality other than for critical security parameters;
– design lifecycle management. For this aspect, see IEC 62443-4-1, ISO/IEC 27001 or other security lifecycle management standards.

This document, as a product security publication, follows IEC Guide 120.

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.

IEC 60364-7-729, *Low-voltage electrical installations - Part 7-729: Requirements for special installations or locations - Operating or maintenance gangways*

IEC 60947-1:2020, *Low-voltage switchgear and controlgear - Part 1: General rules*

IEC 61439-1:2020, *Low-voltage switchgear and controlgear assemblies - Part 1: General rules*

IEC 62443-3-2:2020, *Security for industrial automation and control systems - Part 3-2: Security risk assessment for system design*

IEC 62443-4-1:2018, *Security for industrial automation and control systems - Part 4-1: Secure product development lifecycle requirements*

IEC 62443-4-2:2019, *Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components*

IEC TS 62443-6-2:2025, *Security for industrial automation and control systems - Part 6-2: Security evaluation methodology for IEC 62443-4-2*

ISO/IEC 27001:2022, *Information security, cybersecurity and privacy protection - Information security management systems – Requirements*
ISO/IEC 27001:2022/AMD1:2024

ISO/IEC 27005:2022, *Information security, cybersecurity and privacy protection - Guidance on managing information security risks*

ISO/IEC 27402:2023, *Cybersecurity - IoT security and privacy - Device baseline requirements*

SOMMAIRE

AVANT-PROPOS....8
INTRODUCTION....10
1 Domaine d'application....12
2 Références normatives....13
3 Termes, définitions et abréviations....13
3.1 Termes et définitions....13
3.2 Abréviations....20
4 Généralités....21
5 Objectifs de sécurité....21
6 Gestion du cycle de vie de la sécurité....21
6.1 Généralités....21
6.2 Appréciation du risque pour la sécurité....23
6.2.1 Généralités....23
6.2.2 Relation entre sécurité et sécurité humaine....24
6.2.3 Appréciation de l'impact....25
6.2.4 Résultat de l'appréciation du risque pour la sécurité....25
6.3 Réponse au risque pour la sécurité....26
6.4 Spécification des exigences de sécurité....26
6.5 Rôles et responsabilités....26
6.6 Données importantes....27
6.7 Architecture du système de commande....27
6.7.1 Système de commande....27
6.7.2 Niveaux des fonctionnalités de communication....28
6.7.3 Niveaux de connectivité....30
6.7.4 Niveaux d'exposition de l'équipement....32
6.7.5 Niveaux de sécurité de l'équipement....32
6.7.6 Profil de protection de la sécurité....33
7 Exigences de sécurité....34
7.1 Généralités....34
7.2 Accès physique et environnement....34
7.2.1 PA – Exigence relative à l'accès physique et à l'environnement....34
7.2.2 Justification pour l'accès physique et l'environnement....34
7.2.3 PA-e – Amélioration des accès physiques et de l'environnement....35
7.2.4 Mise en œuvre type de l'accès physique et de l'environnement....36
7.3 Exigences relatives à l'équipement....37
7.3.1 Généralités....37
7.3.2 FR 1 – Contrôle d'identification et d'authentification....38
7.3.3 FR 2 – Contrôle d'utilisation....42
7.3.4 FR 3 – Intégrité du système....47
7.3.5 FR 4 – Confidentialité des données....53
7.3.6 FR 5 – Transfert de données limité (RDF)....54
7.3.7 FR 6 – Réponse appropriée aux événements....55
7.3.8 FR 7 – Disponibilité des ressources....55
8 Instructions d'installation, de fonctionnement et de maintenance....59
8.1 Exigences relatives aux instructions pour l'utilisateur....59
8.2 Amélioration des instructions pour l'utilisateur....60

8.3 Mise en œuvre des instructions pour l'utilisateur 60
9 Vérification et essais de conformité 60
9.1 Généralités 60
9.2 Documentation de conception 60
9.3 Accès physique 61
9.3.1 Vérification de l'accès physique et de l'environnement 61
9.3.2 Critère de décision 61
9.3.3 Amélioration des accès physiques et de l'environnement 61
9.3.4 Critère de décision 61
9.4 FR 1 – Contrôle d'identification et d'authentification 61
9.4.1 CR 1.1 – Identification et authentification d'un utilisateur humain 61
9.4.2 CR 1.2 – Identification et authentification des logiciels et équipements 62
9.4.3 CR 1.5 – Gestion d'authentifiant 62
9.4.4 CR 1.7 – Force de l'authentification par mot de passe 63
9.4.5 CR 1.8 – Certificats d'infrastructure à clés publiques 63
9.4.6 CR 1.9 – Force de l'authentification par clé publique 63
9.4.7 CR 1.10 – Retour de l'authentifiant 64
9.4.8 CR 1.11 – Tentatives infructueuses de connexion 64
9.4.9 CR 1.14 – Force de l'authentification par clés symétriques 64
9.5 FR 2 – Contrôle d'utilisation 65
9.5.1 CR 2.1 – Mise en œuvre d'autorisation 65
9.5.2 CR 2.2 – Contrôle d'utilisation sans fil 65
9.5.3 EDR 2.4 – Code mobile 65
9.5.4 CR 2.5 – Verrouillage de session 66
9.5.5 CR 2.6 – Fermeture de la session à distance 66
9.5.6 CR 2.7 – Contrôle de sessions simultanées 67
9.5.7 CR 2.8 – Événements auditables 67
9.5.8 CR 2.9 – Capacité de stockage des données d'audit 67
9.5.9 CR 2.10 – Réponse aux défaillances de traitement des audits 68
9.5.10 CR 2.11 – Horodatages 68
9.5.11 CR 2.12 – Non-répudiation 69
9.5.12 EDR 2.13 – Utilisation d'interfaces physiques de diagnostic et d'essai 69
9.6 FR 3 – Intégrité du système 69
9.6.1 CR 3.1 – Intégrité de la communication 69
9.6.2 EDR 3.2 – Protection contre les programmes malveillants 70
9.6.3 CR 3.3 – Vérification de la fonctionnalité de sécurité 70
9.6.4 CR 3.4 – Intégrité des logiciels et des informations 70
9.6.5 CR 3.5 – Validation d'entrée 71
9.6.6 RC 3.6 – Sortie déterministe 71
9.6.7 CR 3.7 – Traitement des erreurs 71
9.6.8 CR 3.8 – Intégrité de la session 72
9.6.9 CR 3.9 – Protection des informations d'audit 72
9.6.10 EDR 3.10 – Support pour les mises à jour 72
9.6.11 EDR 3.11 – Résistance aux violations physiques et détection 73
9.6.12 EDR 3.12 – Fourniture des racines de confiance du fournisseur de produit 73
9.6.13 EDR 3.13 – Fourniture des racines de confiance du propriétaire d'actif 73
9.6.14 EDR 3.14 – Intégrité du processus d'amorçage 74
9.7 FR 4 – Confidentialité des données 74

9.7.1 CR 4.1 – Confidentialité des informations 74
9.7.2 CR 4.3 – Utilisation de la cryptographie 74
9.8 FR 6 – Réponse appropriée aux événements 75
9.8.1 CR 6.1 – Accessibilité au journal d'audit 75
9.9 FR 7 – Disponibilité des ressources 75
9.9.1 CR 7.1 – Protection contre le refus de service 75
9.9.2 CR 7.2 – Gestion des ressources 75
9.9.3 CR 7.3 – Sauvegarde du système de commande 76
9.9.4 CR 7.4 – Reprise et reconstitution du système de commande 76
9.9.5 CR 7.6 – Paramètres de configuration du réseau et de la sécurité 76
9.9.6 CR 7.7 – Fonctionnalité minimale 77
9.9.7 CR 7.8 – Inventaire des composants du système de commande 77
Annexe A (informative) Cybersécurité et architecture des systèmes électriques 78
A.1 Généralités 78
A.2 Architecture type comprenant des appareillages et ensembles d'appareillages 78
A.2.1 Bâtiment 78
A.2.2 Installation de fabrication 79
Annexe B (informative) Études de cas d'utilisation 81
B.1 Généralités 81
B.2 Cas d'utilisation 1 – Protection contre les attaques par déni de service (DoS) 82
B.3 Cas d'utilisation 2 – Protection contre les modifications non autorisées d'un dispositif de détection 83
B.4 Cas d'utilisation 3 – Protection contre les modifications non autorisées d'un équipement sans fil 84
B.5 Cas d'utilisation 4 – Protection contre les agents menaçants qui prennent le contrôle à distance d'un ensemble intelligent "de gestion" 85
Annexe C (informative) Méthodes de développement de mesures de cybersécurité 87
Annexe D (informative) Instructions relatives à la sécurité dans la documentation du produit 88
D.1 Généralités 88
D.2 Appréciation du risque et planification de la sécurité 88
D.2.1 Appréciation du risque 88
D.2.2 Plan de sécurité 89
D.3 Recommandations pour la conception et l'installation du système intégrant des appareillages et ensembles d'appareillages 89
D.3.1 Contrôle d'accès général 89
D.3.2 Recommandations pour l'accès local 89
D.3.3 Recommandations pour l'accès à distance 90
D.3.4 Recommandations pour les mises à niveau du microprogramme 91
D.3.5 Recommandations pour la fin de vie 91
D.4 Instructions pour un ensemble 91
Annexe E (normative) Profil de protection de la sécurité d'un démarreur progressif et d'un contrôleur à semiconducteurs 92
E.1 Introduction 92
E.1.1 Référence du profil de protection de la sécurité 92
E.1.2 Vue d'ensemble de la cible d'évaluation 92
E.1.3 Objectifs généraux de la mission 93
E.1.4 Caractéristiques 93
E.1.5 Utilisation du produit 93

E.1.6 Utilisateurs 93
E.2 Hypothèses 94
E.3 Revendications de conformité et déclaration de conformité 94
E.4 Définition du problème de sécurité 94
E.4.1 Actifs essentiels de l'environnement 94
E.4.2 Actifs essentiels de la ToE 95
E.4.3 Modèle de menaces 95
E.5 Objectifs de sécurité 96
E.6 Exigences de sécurité 96
E.6.1 Exigences fonctionnelles de sécurité 96
E.6.2 Exigences d'assurance de sécurité 97
Annexe F (normative) Profil de protection de la sécurité d'un démarreur de moteur raccordé au réseau 98
F.1 Introduction 98
F.1.1 Référence du profil de protection de la sécurité 98
F.1.2 Vue d'ensemble de la cible d'évaluation 98
F.1.3 Objectifs généraux de la mission 99
F.1.4 Caractéristiques 99
F.1.5 Utilisation du produit 99
F.1.6 Utilisateurs 99
F.2 Hypothèses 100
F.3 Revendications de conformité et déclaration de conformité 100
F.4 Définition du problème de sécurité 100
F.4.1 Actifs essentiels de l'environnement 100
F.4.2 Actifs essentiels de la ToE 101
F.4.3 Modèle de menaces 101
F.5 Objectifs de sécurité 102
F.6 Exigences de sécurité 102
F.6.1 Exigences fonctionnelles de sécurité 102
F.6.2 Exigences d'assurance de sécurité 103
Annexe G (normative) Profil de protection de la sécurité d'un disjoncteur 104
G.1 Introduction 104
G.1.1 Référence du profil de protection de la sécurité 104
G.1.2 Vue d'ensemble de la cible d'évaluation 104
G.1.3 Objectifs généraux de la mission 105
G.1.4 Caractéristiques 105
G.1.5 Utilisation du produit 105
G.1.6 Utilisateurs 105
G.2 Hypothèses 106
G.3 Revendications de conformité et déclaration de conformité 106
G.4 Définition du problème de sécurité 106
G.4.1 Actifs essentiels de l'environnement 106
G.4.2 Actifs essentiels de la ToE 107
G.4.3 Modèle de menaces 107
G.5 Objectifs de sécurité 108
G.6 Exigences de sécurité 108
G.6.1 Exigences fonctionnelles de sécurité 108
G.6.2 Exigences d'assurance de sécurité 109
Annexe H (normative) Profil de protection de la sécurité d'un commutateur de transfert 110

H.1 Introduction 110
H.1.1 Référence du profil de protection de la sécurité 110
H.1.2 Vue d'ensemble de la cible d'évaluation 110
H.1.3 Objectifs généraux de la mission 111
H.1.4 Caractéristiques 111
H.1.5 Utilisation du produit 111
H.1.6 Utilisateurs 112
H.2 Hypothèses 112
H.3 Revendications de conformité et déclaration de conformité 112
H.4 Définition du problème de sécurité 113
H.4.1 Actifs essentiels de l'environnement 113
H.4.2 Actifs essentiels de la ToE 113
H.4.3 Modèle de menaces 114
H.5 Objectifs de sécurité 114
H.6 Exigences de sécurité 115
H.6.1 Exigences fonctionnelles de sécurité 115
H.6.2 Exigences d'assurance de sécurité 115
Annexe I (normative) Profil de protection de la sécurité pour un appareillage de commande sans fil avec son interface de communication 116
I.1 Introduction 116
I.1.1 Référence du profil de protection de la sécurité 116
I.1.2 Vue d'ensemble de la cible d'évaluation 116
I.1.3 Objectifs généraux de la mission 117
I.1.4 Caractéristiques 117
I.1.5 Utilisation du produit 117
I.1.6 Utilisateurs 117
I.2 Hypothèses 117
I.3 Revendications de conformité et déclaration de conformité 118
I.4 Définition du problème de sécurité 118
I.4.1 Actifs essentiels de l'environnement 118
I.4.2 Actifs essentiels de la ToE 119
I.4.3 Modèle de menaces 119
I.5 Objectifs de sécurité 120
I.6 Exigences de sécurité 120
I.6.1 Exigences fonctionnelles de sécurité 120
I.6.2 Exigences d'assurance de sécurité 121
Annexe J (informative) Exigences relatives à l'équipement par niveau d'exposition 122
Annexe K (informative) Établissement de références aux systèmes de management de la cybersécurité 124
Annexe L (informative) Mapping avec les dispositions relatives aux exigences essentielles de cybersécurité des annexes du règlement européen sur la cyberrésilience 130
Bibliographie 133

Figure 1 – Paysage normatif 11
Figure 2 – Exemple d'interfaces physiques d'un dispositif intégré dans un équipement pouvant faire l'objet d'une attaque 23
Figure 3 – Exemple de relation entre sécurité et sécurité humaine 24
Figure 4 – Architecture du système de commande avec appareillages 29

Figure 5 – Niveau de connectivité C1 du système de commande 30
Figure 6 – Niveau de connectivité C2 du système de commande 30
Figure 7 – Niveau de connectivité C3 du système de commande 30
Figure 8 – Niveau de connectivité C4 du système de commande 31
Figure 9 – Niveau de connectivité C5 du système de commande 31
Figure 10 – Structure d'un profil de protection de la sécurité 33
Figure 11 – Exemple de symbole d'instruction de sécurité 60
Figure A.1 – Architecture électrique d'un bâtiment 79
Figure A.2 – Installations industrielles 80
Figure E.1 – Architecture de commande des machines 92
Figure F.1 – Architecture de commande des machines 98
Figure G.1 – Disjoncteur dans son environnement 104
Figure H.1 – Unités fonctionnelles d'un commutateur de transfert 110
Figure I.1 – Architecture de commande des machines 116

Tableau 1 – Niveaux d'attaque potentielle 22
Tableau 2 – Menaces types 22
Tableau 3 – Évaluation de l'impact 25
Tableau 4 – Rôles relatifs aux responsabilités en matière de sécurité 26
Tableau 5 – Niveau d'exposition d'un équipement 32
Tableau 6 – Niveau de sécurité de l'équipement 33
Tableau 7 – Références aux exigences relatives à l'accès physique 35
Tableau 8 – Références aux exigences relatives à l'amélioration de l'accès physique 35
Tableau B.1 – Liste des acteurs 81
Tableau B.2 – Exigence de référence 81
Tableau B.3 – Problèmes de sécurité des cas d'utilisation 82
Tableau E.1 – Exigences de sécurité applicables aux actifs essentiels de l'environnement 95
Tableau E.2 – Exigences de sécurité applicables aux actifs essentiels 95
Tableau E.3 – Exigences fonctionnelles de sécurité 96
Tableau F.1 – Exigences de sécurité applicables aux actifs essentiels de l'environnement 101
Tableau F.2 – Exigences de sécurité applicables aux actifs essentiels 101
Tableau F.3 – Exigences fonctionnelles de sécurité 103
Tableau G.1 – Exigences de sécurité applicables aux actifs essentiels de l'environnement 107
Tableau G.2 – Exigences de sécurité applicables aux actifs essentiels 107
Tableau G.3 – Exigences fonctionnelles de sécurité 108
Tableau H.1 – Exigences de sécurité applicables aux actifs essentiels de l'environnement 113
Tableau H.2 – Exigences de sécurité applicables aux actifs essentiels 113
Tableau H.3 – Exigences fonctionnelles de sécurité 115
Tableau I.1 – Exigences de sécurité applicables aux actifs essentiels de l'environnement 118
Tableau I.2 – Exigences de sécurité applicables aux actifs essentiels 119

Tableau I.3 – Exigences fonctionnelles de sécurité 120
Tableau J.1 – Exigences relatives à l'équipement par niveau d'exposition 122
Tableau K.1 – Normes de sécurité utiles 124
Tableau K.2 – Contribution des appareillages et ensembles d'appareillages au cadre de sécurité horizontal de l'ISO et de l'IEC 126
Tableau K.3 – Mapping avec un autre cadre de sécurité 127
Tableau K.4 – Exigences pour les IACS non pertinentes pour les appareillages et ensembles d'appareillages 127
Tableau K.5 – Exigences pour les dispositifs IdO non pertinentes pour les appareillages et ensembles d'appareillages 129
Tableau L.1 – Mapping avec les exigences essentielles de cybersécurité de l'Annexe I du CRA 130

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

Appareillages et ensembles d'appareillages à basse tension - Exigences de sécurité

AVANT-PROPOS

1) La Commission Électrotechnique 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. À 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'IEC attire l'attention sur le fait que la mise en application du présent document peut entraîner l'utilisation d'un ou de plusieurs brevets. L'IEC ne prend pas position quant à la preuve, à la validité et à l'applicabilité de tout droit de brevet revendiqué à cet égard. À la date de publication du présent document, l'IEC n'avait pas reçu notification qu'un ou plusieurs brevets pouvaient être nécessaires à sa mise en application. Toutefois, il y a lieu d'avertir les responsables de la mise en application du présent document que des informations plus récentes sont susceptibles de figurer dans la base de données de brevets, disponible à l'adresse https://patents.iec.ch. L'IEC ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets.

L'IEC 63208 a été établie par le comité d'études 121 de l'IEC: Appareillages et ensembles d'appareillages basse tension. Il s'agit d'une Norme internationale.

Cette première édition annule et remplace la première édition de l'IEC TS 63208 parue en 2020. Cette édition constitue une révision technique.

Cette édition inclut les modifications techniques majeures suivantes par rapport à l'édition précédente:

a) appréciation du risque: niveaux d'attaque, appréciation de l'impact, relation à la sécurité humaine;
b) objectifs de risque: détermination du niveau de sécurité de l'équipement;

c) contre-mesures en référence à l'IEC 62443-4-2;

d) vérification et essais de conformité;

e) profils de protection de la sécurité.

Le texte de cette Norme internationale est issu des documents suivants:

Projet	Rapport de vote
121/221/FDIS	121/230/RVD

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à son approbation.

La langue employée pour l'élaboration de cette Norme internationale est l'anglais.

Ce document a été rédigé selon les Directives ISO/IEC, Partie 2, il a été développé 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/publications.

Le comité a décidé que le contenu de ce document ne sera pas modifié avant la date de stabilité indiquée sur le site web de l'IEC sous webstore.iec.ch dans les données relatives au document recherché. À cette date, le document sera

- reconduit,
- supprimé, ou
- révisé.

INTRODUCTION

L'utilisation croissante des capacités de communication de données par les appareillages et ensembles d'appareillages (appelés "équipement" dans le présent document) augmente automatiquement les risques de cybersécurité. En outre, les technologies de l'information étant plus souvent interconnectées et même intégrées à des systèmes industriels, ce risque est encore amplifié.

Très souvent, les appareillages de commutation, tels que les disjoncteurs, ou les appareillages de commande, tels que les relais de surcharge ou les détecteurs de proximité, sont équipés d'une interface de communication de données. Ils peuvent être connectés à un contrôleur logique ou à un affichage distant, avec une connectivité locale et à distance pour donner l'accès à des données telles que les réglages, les valeurs d'alimentation réelles, les données de surveillance, la journalisation des données, le contrôle et la mise à jour des microprogrammes.

Pour ces applications types de la distribution électrique et des machines, des exigences minimales en matière de cybersécurité sont nécessaires pour maintenir un niveau acceptable d'intégrité de sécurité humaine des fonctions principales de l'équipement, avec ou sans capacité de communication de données. Ces exigences visent à limiter la vulnérabilité des interfaces de communication de données. Pour maintenir la plus grande liberté d'innovation, les exigences pertinentes pour une application définie sont préférentiellement déterminées par une approche systématique d'appréciation du risque.

Le présent document a pour objet de:

1) fournir des ensembles minimaux d'exigences de cybersécurité, appelés profils de protection de la sécurité de l'équipement, afin d'atténuer la vraisemblance d'un fonctionnement non souhaitable et d'une perte de fonctions de protection dans le contexte des installations de distribution électrique et des systèmes de commande de machines;
2) fournir les méthodes d'essai pour vérifier la mise en œuvre de la contre-mesure de cybersécurité au sein de l'équipement;
3) fournir des recommandations pour éviter de compromettre la fonction principale de l'équipement, dans tous les modes de fonctionnement, à la suite de la mise en œuvre de contre-mesures de sécurité.

Le présent document fournit des recommandations sur les contre-mesures applicables à la conception de l'équipement (matériel, microprogramme, interface réseau, contrôle d'accès, système) et les contre-mesures supplémentaires à prendre en compte pour la mise en œuvre et les instructions pour l'utilisateur.

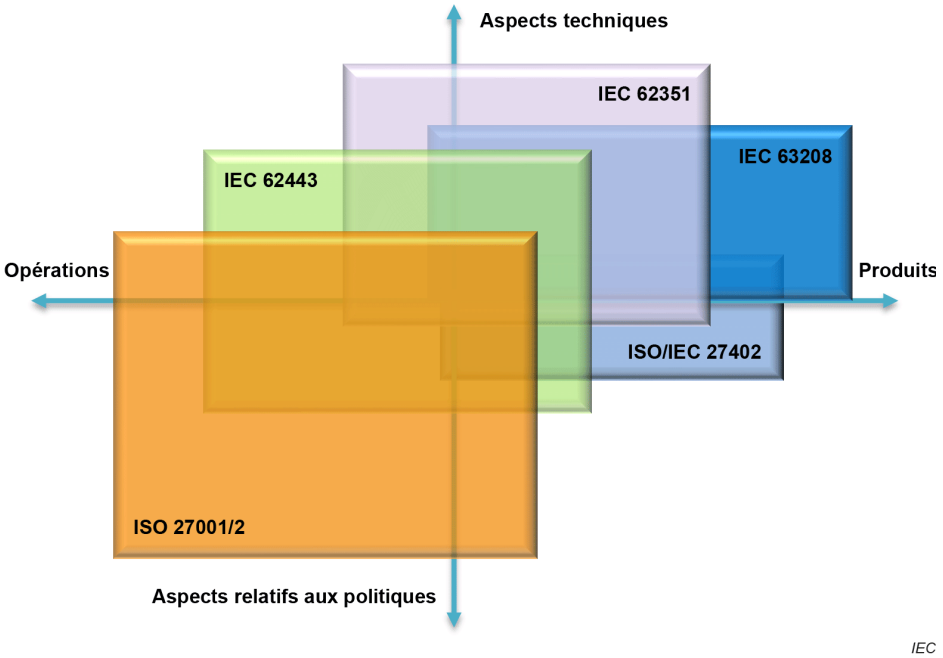

Figure 1 – Paysage normatif

La Figure 1 représente le paysage des normes prises en compte dans le présent document en ce qui concerne les aspects relatifs à la gouvernance et aux politiques, les aspects relatifs aux opérations de cybersécurité, les détails techniques et les exigences du produit. L'ISO/IEC 27001 et sa famille de normes sont utilisées dans de nombreux organismes pour gérer la cybersécurité des systèmes d'information et des activités commerciales en général. La cybersécurité des systèmes de commande industrielle est davantage axée sur le maintien de l'intégrité et de la disponibilité de ses fonctions principales. L'IEC 62443 est actuellement spécialisée sur les exigences génériques applicables à un système d'automatisation de processus aux niveaux d'activité 2 et 3 de l'IEC 62264-1. Le présent document traite de l'utilisation de l'équipement au niveau d'activité 1 de l'IEC 62264-1, en ce qui concerne la cybersécurité des tableaux de distribution électrique et des machines équipées de composants d'extrémité de commutation de commande et de commande d'alimentation sécurisés. À titre d'exemple, le principe des exigences relatives aux niveaux de sécurité systématique et uniforme SL-1 à SL-4 de l'IEC 62443-4-2 pour les composants d'automatisation d'un système de commande dans une zone de procédé n'est pas pertinent pour les appareillages et ensembles d'appareillages en raison des risques de cybersécurité associés, et qui dépendent principalement de leurs niveaux limités de fonctionnalité et de leurs niveaux d'exposition étendus potentiels. Par conséquent, le présent document fournit des exigences minimales de cybersécurité en fonction de ces conditions.

Le présent document utilise les références pertinentes à la publication de base sur la sécurité ISO/IEC 27001 pour les aspects généraux et la cohérence avec le système de management de la cybersécurité des systèmes de technologie de l'information, à la norme sectorielle IEC 62443 pour la gestion des aspects relatifs aux systèmes OT, à l'ISO/IEC 27402 pour les fonctionnalités IdO, ainsi qu'aux techniques de sécurité applicables de l'IEC 62351 (toutes les parties).

Les exigences spécifiques au produit sont données sous la forme de profils de protection de la sécurité (6.7.6) par catégorie d'équipement. Leur structure suit l'Annexe B de l'ISO/IEC 15408-1:2022, et leur contenu peut inclure des exigences qui s'ajoutent à celles des normes IEC 62443.

NOTE Ces profils de protection de la sécurité des produits ne sont pas équivalents au profil de sécurité de l'IEC 62443 défini par l'IEC TS 62443-1-5, qui est limité au contenu actuel des normes IEC 62443.

Le contenu du présent document est destiné à être référencé par les normes de produits.

1 Domaine d'application

Le présent document s'applique aux fonctions principales des appareillages et ensembles d'appareillages, appelés équipements, dans le contexte de la technologie d'exploitation (OT, 3.1.34). Il s'applique aux équipements équipés de moyens de communication de données filaires ou sans fil, ainsi qu'à leur accessibilité physique, dans les limites de leurs conditions d'environnement. Il a pour objet d'assurer l'atténuation appropriée de la sécurité physique et de la cybersécurité contre les vulnérabilités aux menaces à la sécurité.

Le présent document fournit des exigences sur les aspects appropriés suivants:

– l'appréciation du risque pour la sécurité à élaborer, y compris les niveaux d'attaque, les menaces types, l'appréciation de l'impact et la relation à la sécurité humaine;
– les niveaux d'exposition de l'interface de communication et la détermination du niveau de sécurité de l'équipement;
– l'évaluation du niveau d'exposition des interfaces de communication;
– l'attribution des mesures de sécurité exigées pour l'équipement;
– les contre-mesures pour l'accès physique et l'environnement selon l'ISO/IEC 27001;
– les contre-mesures en référence à l'IEC 62443-4-2, avec leurs critères d'applicabilité;
– les instructions pour l'utilisateur concernant l'installation, le fonctionnement et la maintenance;
– la vérification et les essais de conformité; et
– les profils de protection de la sécurité par famille d'équipements (de l'Annexe E à l'Annexe I).

En particulier, il met l'accent sur les vulnérabilités potentielles aux menaces entraînant:

– un fonctionnement non souhaitable, qui peut conduire à des situations dangereuses;
– une indisponibilité des fonctions de protection (surintensité, défaut de terre, etc.);
– toute autre dégradation de la fonction principale.

Il fournit également des recommandations concernant le management de la cybersécurité, avec:

– les rôles et responsabilités (Tableau 4);
– les architectures types (Annexe A);
– les cas d'utilisation (Annexe B);
– les méthodes de développement (Annexe C);
– les recommandations à fournir aux utilisateurs et à intégrer à un ensemble (Annexe D);
– l'établissement de références aux systèmes de management de la cybersécurité (Annexe K).

Le présent document ne fournit aucune exigence de sécurité en ce qui concerne:

– les technologies de l'information (TI);
– les systèmes d'automatisation et de commande industrielles (IACS, *Industrial Automation And Control Systems*), les postes de travail d'ingénierie et leurs applications logicielles;
– les systèmes de management des infrastructures essentielles ou de l'énergie;
– les dispositifs de réseau (commutateur de réseau de communication ou terminaison de réseau privé virtuel); ou
– la confidentialité des données autre que pour les paramètres de sécurité critiques;
– la gestion du cycle de vie de la conception. Pour cet aspect, voir l'IEC 62443-4-1, l'ISO/IEC 27001 ou d'autres normes de gestion du cycle de vie de la sécurité.

Le présent document, en tant que publication sur la sécurité des produits, suit le Guide 120 de l'IEC.

2 Références normatives

Les documents suivants sont cités dans le texte de sorte qu'ils constituent, pour tout ou partie de leur contenu, des exigences du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

IEC 60364-7-729, *Installations électriques à basse tension - Partie 7-729: Règles pour les installations et emplacements spéciaux - Passages d'entretien ou de service*

IEC 60947-1:2020, *Appareillage à basse tension - Partie 1: Règles générales*

IEC 61439-1:2020, *Ensembles d'appareillage à basse tension - Partie 1: Règles générales*

IEC 62443-3-2:2020, *Sécurité des systèmes d'automatisation et de commande industrielles - Partie 3-2: Évaluation des risques de sécurité pour la conception des systèmes*

IEC 62443-4-1:2018, *Sécurité des automatismes industriels et des systèmes de commande - Partie 4-1: Exigences relatives au cycle de développement de produit sécurisé*

IEC 62443-4-2:2019, *Sécurité des systèmes d'automatisation et de commande industrielles - Partie 4-2: Exigences de sécurité technique des composants IACS*

IEC TS 62443-6-2:2025, *Security for industrial automation and control systems – Part 6-2: Security evaluation methodology for IEC 62443-4-2* (disponible en anglais seulement)

ISO/IEC 27001:2022, *Sécurité de l'information, cybersécurité et protection de la vie privée - Systèmes de management de la sécurité de l'information - Exigences*
ISO/IEC 27001:2022/AMD1:2024

ISO/IEC 27005:2022, *Sécurité de l'information, cybersécurité et protection de la vie privée - Préconisations pour la gestion des risques liés à la sécurité de l'information*

ISO/IEC 27402:2023*, Cybersécurité - Sécurité et protection de la vie privée pour l'IdO - Exigences de base relatives aux dispositifs*