

© Copyright SEK Svensk Elstandard. Reproduction in any form without permission is prohibited.

Kopplingsapparater och kopplingsutrustningar för lågspänning – Fordringar på cybersäkerhet

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

Som svensk standard gäller europastandarden EN IEC 63208:2025. Den svenska standarden innehåller den officiella engelska språkversionen av EN IEC 63208:2025.

Nationellt förord

Europastandarden EN IEC 63208:2025

består av:

- **europastandardens ikraftsättningsdokument**, utarbetat inom CENELEC
- **IEC 63208, First edition, 2025 - Low-voltage switchgear and controlgear and their assemblies - Security requirements**

utarbetad inom International Electrotechnical Commission, IEC.

ICS 29.130.20

Denna standard är fastställd av SEK Svensk Elstandard,
som också kan lämna upplysningar om **sakinnehållet** i standarden.
Postadress: Box 1042, 172 21 Sundbyberg
Telefon: 08 - 444 14 00.
E-post: sek@elstandard.se. Internet: elstandard.se

Standarder underlättar utvecklingen och höjer elsäkerheten

Det finns många fördelar med att ha gemensamma tekniska regler för bl a mätning, säkerhet och provning och för utförande, skötsel och dokumentation av elprodukter och elanläggningar.

Genom att utforma sådana standarder blir säkerhetsfordringar tydliga och utvecklingskostnaderna rimliga samtidigt som marknadens acceptans för produkten eller tjänsten ökar.

Många standarder inom elområdet beskriver tekniska lösningar och metoder som åstadkommer den elsäkerhet som föreskrivs av svenska myndigheter och av EU.

SEK är Sveriges röst i standardiseringsarbetet inom elområdet

SEK Svensk Elstandard svarar för standardiseringen inom elområdet i Sverige och samordnar svensk medverkan i internationell och europeisk standardisering. SEK är en ideell organisation med frivilligt deltagande från svenska myndigheter, företag och organisationer som vill medverka till och påverka utformningen av tekniska regler inom elektrotekniken.

SEK samordnar svenska intressenters medverkan i SEKs tekniska kommittéer och stödjer svenska experters medverkan i internationella och europeiska projekt.

Stora delar av arbetet sker internationellt

Utformningen av standarder sker i allt väsentligt i internationellt och europeiskt samarbete. SEK är svensk nationalkommitté av International Electrotechnical Commission (IEC) och Comité Européen de Normalisation Electrotechnique (CENELEC).

Standardiseringsarbetet inom SEK är organiserat i referensgrupper bestående av ett antal tekniska kommittéer som speglar hur arbetet inom IEC och CENELEC är organiserat.

Arbetet i de tekniska kommittéerna är öppet för alla svenska organisationer, företag, institutioner, myndigheter och statliga verk. Den årliga avgiften för deltagandet och intäkter från försäljning finansierar SEKs standardiseringsverksamhet och medlemsavgift till IEC och CENELEC.

Var med och påverka!

Den som deltar i SEKs tekniska kommittéarbete har möjlighet att påverka framtida standarder och får tidig tillgång till information och dokumentation om utvecklingen inom sitt teknikområde. Arbetet och kontakterna med kollegor, kunder och konkurrenter kan gynnsamt påverka enskilda företags affärsutveckling och bidrar till deltagarnas egen kompetensutveckling.

Du som vill dra nytta av dessa möjligheter är välkommen att kontakta SEKs kansli för mer information.

SEK Svensk Elstandard

Box 1042
172 21 Sundbyberg
Tel 08-444 14 00
elstandard.se

ICS 29.130.20

English Version

**Low-voltage switchgear and controlgear and their assemblies -
Security requirements
(IEC 63208:2025)**

Appareillages et ensembles d'appareillages à basse tension
- Exigences de sécurité
(IEC 63208:2025)

Niederspannungsschaltgeräte und deren Niederspannungs-
Schaltgerätekombinationen - Security Aspekte
(IEC 63208:2025)

This European Standard was approved by CENELEC on 2025-09-26. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and the United Kingdom.



European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

European foreword

The text of document 121/221/FDIS, future edition 1 of IEC 63208, prepared by TC 121 "Switchgear and controlgear and their assemblies for low voltage" was submitted to the IEC-CENELEC parallel vote and approved by CENELEC as EN IEC 63208:2025.

The following dates are fixed:

- latest date by which the document has to be implemented at national (dop) 2026-10-31 level by publication of an identical national standard or by endorsement
- latest date by which the national standards conflicting with the (dow) 2028-10-31 document have to be withdrawn

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CENELEC shall not be held responsible for identifying any or all such patent rights.

Any feedback and questions on this document should be directed to the users' national committee. A complete listing of these bodies can be found on the CENELEC website.

Endorsement notice

The text of the International Standard IEC 63208:2025 was approved by CENELEC as a European Standard without any modification.

In the official version, for Bibliography, the following notes have to be added for the standard indicated:

IEC 60204-1:2016	NOTE Approved as EN 60204-1:2018
IEC 60364-1	NOTE Approved as HD 60364-1
IEC 60364-4-41	NOTE Approved as HD 60364-4-41
IEC 60364-4-43	NOTE Approved as HD 60364-4-43
IEC 60870-5 (series)	NOTE Approved as EN 60870-5 (series)
IEC 60947-2	NOTE Approved as EN IEC 60947-2
IEC 60947-4-1	NOTE Approved as EN IEC 60947-4-1
IEC 60947-4-2	NOTE Approved as EN IEC 60947-4-2
IEC 60947-4-3	NOTE Approved as EN IEC 60947-4-3
IEC 60947-5-1	NOTE Approved as EN IEC 60947-5-1
IEC 60947-5-2	NOTE Approved as EN IEC 60947-5-2
IEC 60947-5-3	NOTE Approved as EN 60947-5-3
IEC 60947-5-5	NOTE Approved as EN 60947-5-5
IEC 60947-5-7	NOTE Approved as EN IEC 60947-5-7
IEC 60947-6-1	NOTE Approved as EN IEC 60947-6-1

IEC 60947-6-2	NOTE	Approved as EN IEC 60947-6-2
IEC 61439-1:2020	NOTE	Approved as EN IEC 61439-1:2021 (not modified)
IEC 61508-2	NOTE	Approved as EN 61508-2
IEC 61439-2	NOTE	Approved as EN IEC 61439-2
IEC 62061	NOTE	Approved as EN IEC 62061
IEC 62264-1	NOTE	Approved as EN 62264-1
IEC 62351 (series)	NOTE	Approved as EN IEC 62351 (series)
IEC 62351-5	NOTE	Approved as EN IEC 62351-5
IEC 62351-6	NOTE	Approved as EN IEC 62351-6
IEC 62351-8	NOTE	Approved as EN IEC 62351-8
IEC 62351-9	NOTE	Approved as EN IEC 62351-9
IEC 62443 (series)	NOTE	Approved as EN IEC 62443 (series)
IEC 62443-2-1	NOTE	Approved as EN IEC 62443-2-1
IEC 62443-2-4	NOTE	Approved as EN IEC 62443-2-4
IEC 62443-3-3:2013	NOTE	Approved as EN IEC 62443-3-3:2019 (not modified)
IEC 62559-2:2015	NOTE	Approved as EN 62559-2:2015 (not modified)
IEC/TR 63069	NOTE	Approved as CLC IEC/TR 63069
IEC/TR 63201:2019	NOTE	Approved as CLC IEC/TR 63201:2020 (not modified)
ISO/IEC 15408-1:2022	NOTE	Approved as EN ISO/IEC 15408-1:2023 (not modified)
ISO/IEC 15408-2:2022	NOTE	Approved as EN ISO/IEC 15408-2:2023 (not modified)
ISO/IEC 27000:2018	NOTE	Approved as EN ISO/IEC 27000:2020 (not modified)
ISO/IEC 27002:2022	NOTE	Approved as EN ISO/IEC 27002:2022 (not modified)
ISO/TS 14441:2013	NOTE	Approved as CEN ISO/TS 14441:2013 (not modified)

Annex ZA (normative)

Normative references to international publications with their corresponding European publications

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.

NOTE 1 Where an International Publication has been modified by common modifications, indicated by (mod), the relevant EN/HD applies.

NOTE 2 Up-to-date information on the latest versions of the European Standards listed in this annex is available here: www.cencenelec.eu.

<u>Publication</u>	<u>Year</u>	<u>Title</u>	<u>EN/HD</u>	<u>Year</u>
IEC 60364-7-729	-	Low-voltage electrical installations - Part 7-729: Requirements for special installations or locations - Operating or maintenance gangways	HD 60364-7-729	-
IEC 60947-1	2020	Low-voltage switchgear and controlgear - Part 1: General rules	EN IEC 60947-1	2021
IEC 61439-1	2020	Low-voltage switchgear and controlgear assemblies - Part 1: General rules	EN IEC 61439-1	2021
IEC 62443-3-2	2020	Security for industrial automation and control systems - Part 3-2: Security risk assessment for system design	EN IEC 62443-3-2	2020
IEC 62443-4-1	2018	Security for industrial automation and control systems - Part 4-1: Secure product development lifecycle requirements	EN IEC 62443-4-1	2018
IEC 62443-4-2	2019	Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components	EN IEC 62443-4-2	2019
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	EN ISO/IEC 27001	2023
+ A1	2024		+ A1	2024
ISO/IEC 27005	2022	Information security, cybersecurity and privacy protection - Guidance on managing information security risks	EN ISO/IEC 27005	2024
ISO/IEC 27402	2023	Cybersecurity - IoT security and privacy - Device baseline requirements	-	-



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



THIS PUBLICATION IS COPYRIGHT PROTECTED
Copyright © 2025 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, 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.

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.....	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.

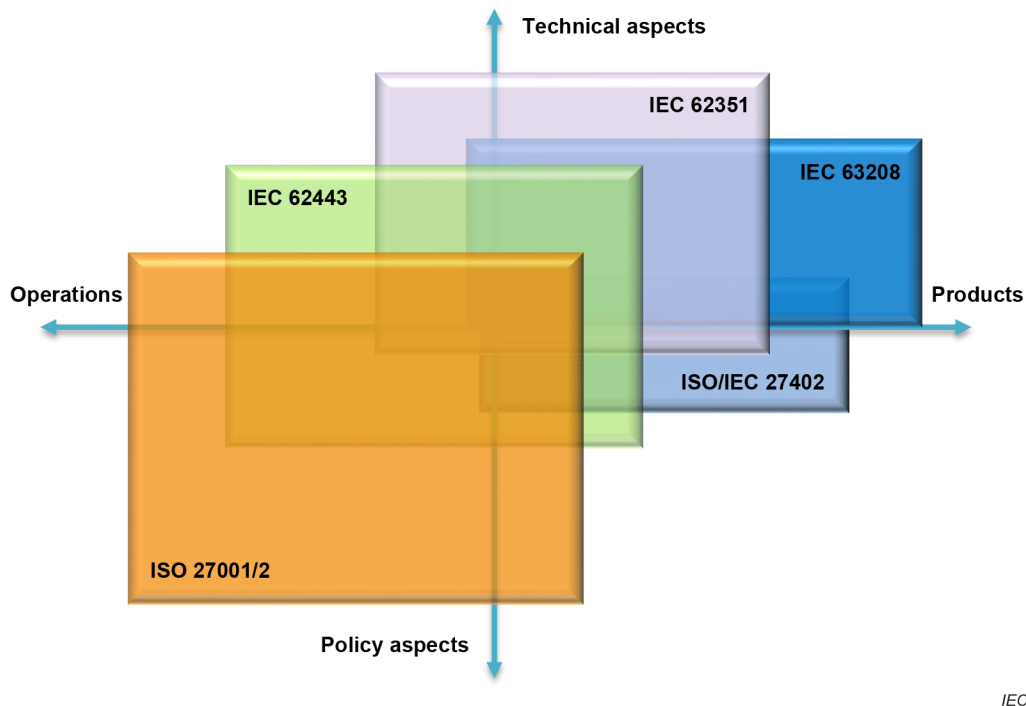


Figure 1 – Standard landscape

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*