

INTERNATIONAL STANDARD

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

(<https://standards.iteh.ai>)
Document Preview

[IEC 63208:2025](https://standards.iteh.ai/catalog/standards/iec/358225d2-dea9-46f0-8912-b7be8bb0f6fc/iec-63208-2025)

<https://standards.iteh.ai/catalog/standards/iec/358225d2-dea9-46f0-8912-b7be8bb0f6fc/iec-63208-2025>



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.

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 It also gives information on projects, replaced and withdrawn publications.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

[IEC 63208:2025](https://standards.iteh.ai/catalog/standards/iec/358225d2-dea9-46f0-8912-b7be8bb0f6fc/iec-63208-2025)

<https://standards.iteh.ai/catalog/standards/iec/358225d2-dea9-46f0-8912-b7be8bb0f6fc/iec-63208-2025>

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

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