



**SLOVENSKI STANDARD**  
**oSIST prEN IEC 63208:2024**

**01-oktober-2024**

---

**Stikalne in krmilne naprave ter njihovi sestavi za uporabo pri nizki napetosti -  
Varnostni vidiki**

Switchgear and controlgear and their assemblies for low voltage - Security aspects

Appareillages et ensembles d'appareillages basse tension - Aspects de sécurité

**Ta slovenski standard je istoveten z: prEN IEC 63208:2024**

---

**ICS:**

29.130.20 Niskonapetostne stikalne in krmilne naprave Low voltage switchgear and controlgear

**oSIST prEN IEC 63208:2024**

**en**





# 121/172/CDV

## COMMITTEE DRAFT FOR VOTE (CDV)

PROJECT NUMBER: <b>IEC 63208 ED1</b>	
DATE OF CIRCULATION: <b>2024-08-30</b>	CLOSING DATE FOR VOTING: <b>2024-11-22</b>
SUPERSEDES DOCUMENTS: <b>121/167/CD, 121/170/CC</b>	

IEC TC 121: SWITCHGEAR AND CONTROLGEAR AND THEIR ASSEMBLIES FOR LOW VOLTAGE	
SECRETARIAT: France	SECRETARY: Mr Michaël LAHEURTE
OF INTEREST TO THE FOLLOWING COMMITTEES: TC 17, SC 22G, TC 23, TC 44, TC 65, TC 94, SC 121A, SC 121B	HORIZONTAL FUNCTION(S):
ASPECTS CONCERNED:	
<input checked="" type="checkbox"/> SUBMITTED FOR CENELEC PARALLEL VOTING  <b>Attention IEC-CENELEC parallel voting</b> The attention of IEC National Committees, members of CENELEC, is drawn to the fact that this Committee Draft for Vote (CDV) is submitted for parallel voting. The CENELEC members are invited to vote through the CENELEC online voting system.	<input type="checkbox"/> NOT SUBMITTED FOR CENELEC PARALLEL VOTING

oSIST prEN IEC 63208:2024

<https://standards.iteh.ai/catalog/standards/sist/8975dc46-8e94-4809-87c4-e7123b9ab3bc/osist-pren-iec-63208-2024>

This document is still under study and subject to change. It should not be used for reference purposes.

Recipients of this document are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Recipients of this document are invited to submit, with their comments, notification of any relevant "In Some Countries" clauses to be included should this proposal proceed. Recipients are reminded that the CDV stage is the final stage for submitting ISC clauses. (See [AC/22/2007](#) or [NEW GUIDANCE DOC](#)).

TITLE: <b>Switchgear and controlgear and their assemblies for low voltage – Security aspects</b>
---

PROPOSED STABILITY DATE: 2028
-------------------------------

NOTE FROM TC/SC OFFICERS:
---------------------------

Copyright © 2024 International Electrotechnical Commission, IEC. All rights reserved. It is permitted to download this electronic file, to make a copy and to print out the content for the sole purpose of preparing National Committee positions. You may not copy or "mirror" the file or printed version of the document, or any part of it, for any other purpose without permission in writing from IEC.

## CONTENTS

FOREWORD .....	11
INTRODUCTION .....	13
1 Scope .....	15
2 Normative references .....	16
3 Terms, definitions and abbreviated terms .....	16
3.1 Terms and definitions .....	16
3.2 Abbreviated terms .....	22
4 General .....	23
5 Security objectives .....	23
6 Security lifecycle management .....	24
6.1 General .....	24
6.2 Security risk assessment .....	26
6.2.1 General .....	26
6.2.2 Relationship between safety and security .....	27
6.2.3 Impact assessment .....	28
6.2.4 Security risk assessment result .....	28
6.3 Response to security risk .....	28
6.4 Security requirement specification .....	29
6.5 Roles and responsibilities .....	29
6.6 Important data .....	29
6.7 Control system architecture .....	30
6.7.1 Control system .....	30
6.7.2 Levels of communication functionalities .....	30
6.7.3 Levels of connectivity .....	32
6.7.4 Exposure levels of equipment .....	34
6.7.5 Equipment security levels .....	35
6.7.6 Security protection profile .....	35
7 Security requirements .....	36
7.1 General .....	36
7.2 Physical access and environment .....	36
7.2.1 PA – Physical access and environment requirement .....	36
7.2.2 Physical access and environment rationale .....	37
7.2.3 PA-e – Physical access and environment enhancement .....	37
7.2.4 Physical access and environment typical implementation .....	38
7.3 Equipment requirement .....	39
7.3.1 General .....	39
7.3.1.1 Main functions .....	39
7.3.1.2 Compensating countermeasure .....	39
7.3.1.3 Security requirements for the equipment .....	39
7.3.2 FR 1 – Identification and authentication control .....	40
7.3.2.1 Purpose .....	40
7.3.2.2 Rationale .....	40
7.3.2.3 CR 1.1 – Human user identification and authentication .....	40
7.3.2.4 CR 1.2 – Software and equipment identification and authentication .....	41
7.3.2.5 CR 1.5 – Authenticator management .....	41

	7.3.2.6	CR 1.7 – Strength of password-based authentication .....	41
	7.3.2.7	CR 1.8 – Public key infrastructure certificates .....	42
	7.3.2.8	CR 1.9 – Strength of public key-based authentication .....	42
	7.3.2.9	CR 1.10 – Authenticator feedback .....	42
	7.3.2.10	CR 1.11 – Unsuccessful login attempts .....	43
	7.3.2.11	CR 1.14 – Strength of symmetric key-based authentication .....	43
7.3.3	FR 2 – Use control .....		43
	7.3.3.1	Purpose .....	43
	7.3.3.2	Rationale .....	43
	7.3.3.3	CR 2.1 – Authorisation enforcement .....	43
	7.3.3.4	CR 2.2 – Wireless use control .....	44
	7.3.3.5	EDR 2.4 – Mobile code .....	44
	7.3.3.6	CR 2.5 – Session lock .....	45
	7.3.3.7	CR 2.6 – Remote session termination .....	45
	7.3.3.8	CR 2.7 – Concurrent session control .....	46
	7.3.3.9	CR 2.8 – Auditable events .....	46
	7.3.3.10	CR 2.9 – Audit storage capacity .....	46
	7.3.3.11	CR 2.10 – Response to audit processing failures .....	47
	7.3.3.12	CR 2.11 Timestamp .....	47
	7.3.3.13	CR 2.12 – Non-repudiation .....	48
	7.3.3.14	EDR 2.13 – Use of physical diagnostic and test interfaces .....	48
7.3.4	FR 3 – System integrity .....		48
	7.3.4.1	Purpose .....	48
	7.3.4.2	Rationale .....	48
	7.3.4.3	CR 3.1 – Communication integrity .....	49
	7.3.4.4	EDR 3.2 – Protection from malicious code .....	49
	7.3.4.5	CR 3.3 – Security functionality verification .....	50
	7.3.4.6	CR 3.4 – Software and information integrity .....	50
	7.3.4.7	CR 3.5 – Input validation .....	51
	7.3.4.8	CR 3.6 – Deterministic output .....	51
	7.3.4.9	CR 3.7 – Error handling .....	52
	7.3.4.10	CR 3.8 – Session Integrity .....	52
	7.3.4.11	CR 3.9 – Protection of audit information .....	52
	7.3.4.12	EDR 3.10 – Support for Updates .....	53
	7.3.4.13	EDR 3.11 – Physical tamper resistance and detection .....	53
	7.3.4.14	EDR 3.12 – Provisioning product supplier roots of trust .....	53
	7.3.4.15	EDR 3.13 – Provisioning asset owner roots of trust .....	54
	7.3.4.16	EDR 3.14 – Integrity of the boot process .....	54
7.3.5	FR 4 – Data confidentiality .....		55
	7.3.5.1	Purpose .....	55
	7.3.5.2	Rationale .....	55
	7.3.5.3	CR 4.1 – Information confidentiality .....	55
	7.3.5.4	CR 4.3 – Use of cryptography .....	55
7.3.6	FR 5 – Restricted data flow .....		55
7.3.7	FR 6 – Timely response to events .....		56
	7.3.7.1	Purpose .....	56
	7.3.7.2	Rationale .....	56
	7.3.7.3	CR 6.1 – Audit log accessibility .....	56
7.3.8	FR 7 – Resource availability .....		56

7.3.8.1	Purpose .....	56
7.3.8.2	Rationale .....	56
7.3.8.3	CR 7.1 – Denial of service protection .....	56
7.3.8.4	CR 7.2 – Resource management.....	57
7.3.8.5	CR 7.3 – Control system backup .....	58
7.3.8.6	CR 7.4 – Control system recovery and reconstitution .....	58
7.3.8.7	CR 7.6 – Network and security configuration settings.....	58
7.3.8.8	CR 7.7 – Least functionality .....	59
7.3.8.9	CR 7.8 – Control system inventory .....	60
8	Instructions for installation, operation and maintenance.....	60
8.1	User instruction requirement .....	60
8.2	User instruction enhancement.....	60
8.3	User instruction implementation .....	61
9	Conformance verification and testing .....	61
9.1	General.....	61
9.2	Design documentation .....	61
9.3	Physical access .....	61
9.3.1	Verification of physical access and environment .....	61
9.3.2	Physical access and environment enhancement .....	61
9.4	FR 1 – Identification and authentication control.....	62
9.4.1	CR 1.1 – Human user identification and authentication .....	62
	9.4.1.1 Requirement verification .....	62
	9.4.1.2 Requirement CR 1.1 e.1 verification .....	62
9.4.2	CR 1.2 – Software and equipment identification and authentication .....	62
	9.4.2.1 Requirement verification .....	62
	9.4.2.2 Requirement CR 1.2 e.1 verification.....	62
9.4.3	CR 1.5 – Authenticator management .....	63
	9.4.3.1 Requirement verification .....	63
9.4.4	CR 1.7 – Strength of password-based authentication.....	63
	9.4.4.1 Requirement verification .....	63
9.4.5	CR 1.8 – Public key infrastructure certificates.....	63
	9.4.5.1 Requirement verification .....	63
9.4.6	CR 1.9 – Strength of public key-based authentication .....	63
	9.4.6.1 Requirement verification .....	63
9.4.7	CR 1.10 – Authenticator feedback .....	64
	9.4.7.1 Requirement verification .....	64
9.4.8	CR 1.11 – Unsuccessful login attempts.....	64
	9.4.8.1 Requirement verification .....	64
9.4.9	CR 1.14 – Strength of symmetric key-based authentication .....	64
	9.4.9.1 Requirement verification .....	64
9.5	FR 2 – Use control.....	65
9.5.1	CR 2.1 – Authorisation enforcement .....	65
	9.5.1.1 Requirement verification .....	65
	9.5.1.2 Requirement CR 2.1 e.1 verification.....	65
9.5.2	CR 2.2 – Wireless use control.....	65
	9.5.2.1 Requirement verification .....	65
9.5.3	EDR 2.4 – Mobile code .....	65
	9.5.3.1 Requirement verification .....	65
	9.5.3.2 Requirement EDR 2.4 e.1 verification .....	66

9.5.4	CR 2.5 – Session lock .....	66
	9.5.4.1 Requirement verification .....	66
9.5.5	CR 2.6 – Remote session termination .....	66
	9.5.5.1 Requirement verification .....	66
9.5.6	CR 2.7 – Concurrent session control .....	66
	9.5.6.1 Requirement verification .....	66
9.5.7	CR 2.8 – Auditable events .....	66
	9.5.7.1 Requirement verification .....	66
9.5.8	CR 2.9 – Audit storage capacity .....	67
	9.5.8.1 Requirement verification .....	67
	9.5.8.2 Requirement CR 2.9 e.1 verification .....	67
9.5.9	CR 2.10 – Response to audit processing failures .....	67
	9.5.9.1 Requirement verification .....	67
9.5.10	CR 2.11 – Timestamps .....	67
	9.5.10.1 Requirement verification .....	67
	9.5.10.2 Requirement CR 2.11 e.1 verification .....	68
9.5.11	CR 2.12 – Non-repudiation .....	68
	9.5.11.1 Requirement verification .....	68
9.5.12	EDR 2.13 – Use of physical diagnostic and test interfaces .....	68
	9.5.12.1 Requirement verification .....	68
9.6	FR 3 – System integrity .....	68
9.6.1	CR 3.1 – Communication integrity .....	68
	9.6.1.1 Requirement verification .....	68
	9.6.1.2 Requirement CR 3.1 e.1 verification .....	68
9.6.2	EDR 3.2 – Protection from malicious code .....	69
	9.6.2.1 Requirement verification .....	69
9.6.3	CR 3.3 – Security functionality verification .....	69
	9.6.3.1 Requirement verification .....	69
9.6.4	CR 3.4 – Software and information integrity .....	69
	9.6.4.1 Requirement verification .....	69
	9.6.4.2 Requirement CR 3.4 e.1 verification .....	69
9.6.5	CR 3.5 – Input validation .....	70
	9.6.5.1 Requirement verification .....	70
9.6.6	CR 3.6 – Deterministic output .....	70
	9.6.6.1 Requirement verification .....	70
9.6.7	CR 3.7 – Error handling .....	70
	9.6.7.1 Requirement verification .....	70
9.6.8	CR 3.8 – Session Integrity .....	70
	9.6.8.1 Requirement verification .....	70
9.6.9	CR 3.9 – Protection of audit information .....	71
	9.6.9.1 Requirement verification .....	71
9.6.10	EDR 3.10 – Support for updates .....	71
	9.6.10.1 Requirement verification .....	71
	9.6.10.2 Requirement CR 3.10 e.1 verification .....	71
9.6.11	EDR 3.11 – Physical tamper resistance and detection .....	71
	9.6.11.1 Requirement verification .....	71
9.6.12	EDR 3.12 – Provisioning product supplier roots of trust .....	72
	9.6.12.1 Requirement verification .....	72
9.6.13	EDR 3.13 – Provisioning asset owner roots of trust .....	72

9.6.13.1	Requirement verification .....	72
9.6.14	EDR 3.14 – Integrity of the boot process.....	72
9.6.14.1	Requirement verification .....	72
9.6.14.2	Requirement CR 3.14 e.1 verification.....	72
9.7	FR 4 – Data confidentiality .....	73
9.7.1	CR 4.1 – Information confidentiality .....	73
9.7.1.1	Requirement verification .....	73
9.7.2	CR 4.3 – Use of cryptography.....	73
9.7.2.1	Requirement verification .....	73
9.8	FR 6 – Timely response to events.....	73
9.8.1	CR 6.1 – Audit log accessibility.....	73
9.8.1.1	Requirement verification .....	73
9.9	FR 7 – Resource availability .....	73
9.9.1	CR 7.1 – Denial of service protection.....	73
9.9.1.1	Requirement verification .....	73
9.9.2	CR 7.2 – Resource management .....	74
9.9.2.1	Requirement verification .....	74
9.9.3	CR 7.3 – Control system backup.....	74
9.9.3.1	Requirement verification .....	74
9.9.3.2	Requirement CR 7.3 e.1 verification.....	74
9.9.4	CR 7.4 – Control system recovery and reconstitution.....	74
9.9.4.1	Requirement verification .....	74
9.9.5	CR 7.6 – Network and security configuration settings .....	74
9.9.5.1	Requirement verification .....	74
9.9.6	CR 7.7 – Least functionality.....	75
9.9.6.1	Requirement verification .....	75
9.9.7	CR 7.8 – Control system inventory.....	75
9.9.7.1	Requirement verification .....	75
Annex A (informative)	Cybersecurity and electrical system architecture .....	76
A.1	General.....	76
A.2	Typical architecture involving switchgear, controlgear and their assembly.....	76
A.2.1	Building .....	76
A.2.2	Manufacturing.....	77
Annex B (informative)	Use case studies .....	79
B.1	General.....	79
B.2	Use case 1 – Protection against Denial of Service (DoS) attack.....	80
B.3	Use case 2 – Protection against unauthorised modification of sensing device .....	81
B.4	Use case 3 – Protection against unauthorised modification of wireless equipment.....	82
B.5	Use case 4 – Protection against threat actor remotely taking control of a “Managing” intelligent assembly.....	82
Annex C (Informative)	Development methods of cybersecurity measures.....	84
Annex D (informative)	Instructions to be provided to the user of the equipment and for integration into an assembly .....	85
D.1	General.....	85
D.2	Risk assessment and security planning.....	85
D.2.1	Risk assessment .....	85
D.2.2	Security plan .....	85



D.3	Recommendations for design and installation of the system integrating switchgear, controlgear and their assemblies .....	86
D.3.1	General access control .....	86
D.3.2	Recommendations for local access .....	86
D.3.3	Recommendations for remote access .....	87
D.3.4	Recommendations for firmware upgrades .....	87
D.3.5	Recommendations for the end of life .....	88
D.4	Instructions for an assembly .....	88
Annex E (normative)	Security protection profile of soft-starter and semiconductor controller .....	89
E.1	Introduction .....	89
E.1.1	Security protection profile reference .....	89
E.1.2	Target of evaluation overview .....	89
E.1.3	General mission objectives .....	90
E.1.4	Features .....	90
E.1.5	Product usage .....	90
E.1.6	Users .....	90
E.2	Assumptions .....	91
E.3	Conformance claims and conformance statement .....	91
E.4	Security problem definition .....	91
E.4.1	Critical assets of the environment .....	91
E.4.2	ToE critical assets .....	92
E.4.3	Threat Model .....	92
E.4.3.1	Attackers .....	92
E.4.3.2	Threats .....	92
E.5	Security objectives .....	93
E.6	Security requirements .....	93
E.6.1	Security functional requirements .....	93
E.6.2	Security assurance requirements .....	93
Annex F (normative)	Security protection profile of network connected motor starter .....	94
F.1	Introduction .....	94
F.1.1	Security protection profile reference .....	94
F.1.2	Target of evaluation overview .....	94
F.1.3	General mission objectives .....	94
F.1.4	Features .....	95
F.1.5	Product usage .....	95
F.1.6	Users .....	95
F.2	Assumptions .....	95
F.3	Conformance claims and conformance statement .....	96
F.4	Security problem definition .....	96
F.4.1	Critical assets of the environment .....	96
F.4.2	ToE critical assets .....	96
F.4.3	Threat Model .....	97
F.4.3.1	Attackers .....	97
F.4.3.2	Threats .....	97
F.5	Security objectives .....	97
F.6	Security requirements .....	98
F.6.1	Security functional requirements .....	98
F.6.2	Security assurance requirements .....	98

Annex G (normative) Security protection profile of circuit-breaker .....	99
G.1 Introduction .....	99
G.1.1 Security protection profile reference .....	99
G.1.2 Target of evaluation overview .....	99
G.1.3 General mission objectives .....	99
G.1.4 Features .....	100
G.1.5 Product usage .....	100
G.1.6 Users .....	100
G.2 Assumptions .....	100
G.3 Conformance claims and conformance statement .....	101
G.4 Security problem definition .....	101
G.4.1 Critical assets of the environment .....	101
G.4.2 ToE critical assets .....	102
G.4.3 Threat Model .....	102
G.4.3.1 Attackers .....	102
G.4.3.2 Threats .....	102
G.5 Security objectives .....	103
G.6 Security requirements .....	103
G.6.1 Security functional requirements .....	103
G.6.2 Security assurance requirements .....	103
Annex H (normative) Security protection profile of transfer switch equipment .....	104
H.1 Introduction .....	104
H.1.1 Security protection profile reference .....	104
H.1.2 Target of evaluation overview .....	104
H.1.2.1 Overview .....	104
H.1.3 General mission objectives .....	105
H.1.4 Features .....	105
H.1.5 Product usage .....	105
H.1.6 Users .....	105
H.2 Assumptions .....	106
H.3 Conformance claims and conformance statement .....	106
H.4 Security problem definition .....	106
H.4.1 Critical assets of the environment .....	106
H.4.2 ToE critical assets .....	107
H.4.3 Threat Model .....	107
H.4.3.1 Attackers .....	107
H.4.3.2 Threats .....	107
H.5 Security objectives .....	108
H.6 Security requirements .....	108
H.6.1 Security functional requirements .....	108
H.6.2 Security assurance requirements .....	108
Annex I (normative) Security protection profile for wireless controlgear with its communication interface .....	110
I.1 Introduction .....	110
I.1.1 Security protection profile reference .....	110
I.1.2 Target of evaluation overview .....	110
I.1.3 General mission objectives .....	111
I.1.4 Features .....	111
I.1.5 Product usage .....	111

1.1.6	Users.....	111
1.2	Assumptions .....	111
1.3	Conformance claims and conformance statement .....	112
1.4	Security problem definition.....	112
1.4.1	Critical assets of the environment.....	112
1.4.2	ToE critical assets .....	112
1.4.3	Threat Model .....	113
1.4.3.1	Attackers.....	113
1.4.3.2	Threats .....	113
1.5	Security objectives.....	113
1.6	Security requirements .....	114
1.6.1	Security functional requirements.....	114
1.6.2	Security assurance requirements.....	114
Annex J (informative)	Equipment requirements by level of exposure .....	115
Annex K (informative)	Bridging references to cybersecurity management systems .....	117
Annex L (informative)	Mapping of provisions to the essential cybersecurity requirements of the European Cyber Resilient Act Annexes .....	123
Bibliography.....		126
Figure 1 – Standard landscape .....		13
Figure 2 – Example of physical interfaces of an embedded device in an equipment which can be subject to an attack .....		26
Figure 3 – Example of relation between security and safety .....		27
Figure 4 – Control system architecture with switchgear and controlgear.....		31
Figure 5 – Control system connectivity level C1 .....		32
Figure 6 – Control system connectivity level C2 .....		32
Figure 7 – Control system connectivity level C3 .....		33
Figure 8 – Control system connectivity level C4 .....		33
Figure 9 – Control system connectivity level C5 .....		34
Figure 10 – Structure of a security protection profile .....		36
Figure 11 – Example of security instruction symbol.....		61
Figure A.1 – Building electrical architecture .....		77
Figure A.2 – Industrial plants .....		78
Figure E.1 – Machinery control architecture .....		89
Figure F.1 – Machinery control architecture .....		94
Figure G.1 – Circuit-breaker in its environment .....		99
Figure H.1 – Functional units of the transfer switch equipment.....		104
Figure I.1 – Machinery control architecture .....		110
Table 1 – Potential attack levels .....		24
Table 2 – Typical threats.....		25
Table 3 – Impact evaluation .....		28
Table 4 – Roles related to security responsibilities.....		29
Table 5 – Level of exposure of an equipment.....		34
Table 6 – Equipment security level .....		35

Table 7 – Physical access related requirement references .....	37
Table 8 – Physical access enhancement related requirement references .....	37
Table B.1 – List of actors .....	79
Table B.2 – Base line requirement .....	79
Table B.3 – Security problems of use cases .....	79
Table E.1 – Security requirements for the critical assets of the environment .....	91
Table E.2 – Security requirements for the critical assets .....	92
Table E.3 – Security functional requirements .....	93
Table F.1 – Security requirements for the critical assets of the environment .....	96
Table F.2 – Security requirements for the critical assets .....	97
Table F.3 – Security functional requirements .....	98
Table G.1 – Security requirements for the critical assets of the environment .....	101
Table G.2 – Security requirements for the critical assets .....	102
Table G.3 – Security functional requirements .....	103
Table H.1 – Security requirements for the critical assets of the environment .....	107
Table H.2 – Security requirements for the critical assets .....	107
Table H.3 – Security functional requirements .....	108
Table I.1 – Security requirements for the critical assets of the environment .....	112
Table I.2 – Security requirements for the critical assets .....	113
Table I.3 – Security functional requirements .....	114
Table J.1 – Equipment requirements by level of exposure .....	115
Table K.1 – Useful security standards .....	117
Table K.2 – Contribution of switchgear, controlgear and their assemblies to ISO and IEC horizontal security framework .....	118
Table K.3 – Mapping to other security framework .....	121
Table K.4 – Requirements for IACS not relevant for switchgear, controlgear and their assemblies .....	121
Table K.5 – Requirements for IoT device not relevant for switchgear, controlgear and their assemblies .....	122
Table L.1 – Mapping to the essential cybersecurity requirements of the CRA Annexe I .....	123

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

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

This edition cancels and replaces the 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:

FDIS	Report on voting
121/XXX/FDIS	121/XXX/RVD

Full information on the voting for the approval of this International Standard can be found in the report on voting indicated in the above table.

This document has been drafted in accordance with the ISO/IEC Directives, Part 2.

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

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

The National Committees are requested to note that for this document the stability date is ....

THIS TEXT IS INCLUDED FOR THE INFORMATION OF THE NATIONAL COMMITTEES AND WILL BE DELETED AT THE PUBLICATION STAGE.

**IMPORTANT** – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.