



DPC: 24 / 30492860 DC

BSI Group Headquarters

389 Chiswick High Road London W4 4AL

Tel: +44 (0)20 8996 9000

Fax: +44 (0)20 8996 7400

www.bsigroup.com

Date: 09 May 2024

Origin: International

Latest date for receipt of comments: 29 May 2024

Project No. 2023/02999

Responsible committee: PEL/121 Switchgear and Controlgear and their assemblies for low voltage

Interested committees:

Title: BS EN IEC 63208 Switchgear and controlgear and their assemblies for low voltage - Security aspects

Please notify the secretary if you are aware of any keywords that might assist in classifying or identifying the standard or if the content of this standard

- i) has any issues related to 3rd party IPR, patent or copyright
- ii) affects other national standard(s)
- iii) requires additional national guidance or information

**WARNING: THIS IS A DRAFT AND MUST NOT BE REGARDED OR USED AS A BRITISH STANDARD.
THIS DRAFT IS NOT CURRENT BEYOND 31 May 2024**This draft is issued to allow comments from interested parties; all comments will be given consideration prior to publication. No acknowledgement will normally be sent. **See overleaf for information on the submission of comments.**

No copying is allowed, in any form, without prior written permission from BSI except as permitted under the Copyright, Designs and Patent Act 1988 or for circulation within a nominating organization for briefing purposes. Electronic circulation is limited to dissemination by e-mail within such an organization by committee members.

Further copies of this draft may be purchased from BSI Shop <http://shop.bsigroup.com> or from BSI Customer Services, Tel: +44(0) 20 8996 9001 or email cservices@bsigroup.com. British, International and foreign standards are also available from BSI Customer Services.Information on the co-operating organizations represented on the committees referenced above may be obtained from <http://standardsdevelopment.bsigroup.com>

Responsible Committee Secretary: **Mr Simon Bounds (BSI)**Direct tel: **0208 996 7281**E-mail: simon.bounds@bsigroup.com

Full document details: 24/30492860 DC

Introduction

This draft standard is based on national and international discussions. Your comments on this draft are invited and will assist in the preparation of the consequent standard.

For international standards, comments will be reviewed by the relevant UK national committee before sending the consensus UK vote and comments to the international committee, which will then decide appropriate action. If the international standard is approved, it is usual for the text to be published as a British Standard.

For national standards, comments will be reviewed by the relevant UK national committee and the resulting standards published as a British Standard.

UK Vote

Please indicate whether you consider the UK should submit a negative (with supporting technical reasons) or positive vote on this draft. Please indicate if you are aware of any reason why this draft standard should not be published as a British Standard.

Submission of Comments

- **Annotated drafts are not acceptable and will be rejected.**
- All comments should be submitted online at <https://standardsdevelopment.bsigroup.com/>. You will need to register in order to comment.

Template for comments and secretariat observations

Date: xx/xx/20xx	Document: ISO/DIS xxxx
------------------	------------------------

1	2	(3)	4	5	(6)	7
MB	Clause No./ Subclause No./Annex (e.g. 3.1)	Paragraph/Figure/ Table/Note	Type of comment	Commend (justification for change) by the MB	Proposed change by the MB	Secretariat observations on each comment submitted
	3.1	Definition 1	ed	Definition is ambiguous and needs clarifying.	Amend to read '...so that the mains connector to which no connection...'	
	6.4	Paragraph 2	te	The use of the UV photometer as an alternative cannot be supported as serious problems have been encountered in its use in the UK.	Delete reference to UV photometer.	



PROJECT NUMBER: IEC 63208 ED1	
DATE OF CIRCULATION: 2024-05-03	CLOSING DATE FOR COMMENTS: 2024-06-28
SUPERSEDES DOCUMENTS: 121/156/CD, 121/163A/CC	

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	PROPOSED HORIZONTAL STANDARD: ☐ Other TC/SCs are requested to indicate their interest, if any, in this CD to the secretary.
FUNCTIONS CONCERNED: ☐ EMC ☐ ENVIRONMENT ☐ QUALITY ASSURANCE ☐ SAFETY	

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 local regulations or technical reasons that may exist and should be considered should this proposal proceed, recognizing that failure to address such requirements could result in the need for new or existing "In Some Countries" clauses. (See [AC/22/2007](#) or [NEW GUIDANCE DOC](#)).

TITLE:

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

NOTE FROM TC/SC OFFICERS:

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	23
6.1 General	23
6.2 Security risk assessment	25
6.2.1 General	25
6.2.2 Relationship between safety and security	26
6.2.3 Impact assessment	27
6.2.4 Security risk assessment result	27
6.3 Response to security risk	28
6.4 Security requirement specification	28
6.5 Roles and responsibilities	28
6.6 Important data	28
6.7 Control system architecture	29
6.7.1 Control system	29
6.7.2 Levels of communication functionalities	29
6.7.3 Levels of connectivity	31
6.7.4 Exposure levels of equipment	33
6.7.5 Equipment security levels	34
6.7.6 Security protection profile	34
7 Security requirements	35
7.1 General	35
7.2 Physical access and environment	35
7.2.1 PA – Physical access and environment requirement	35
7.2.2 Physical access and environment rational	36
7.2.3 PA-e – Physical access and environment enhancement	36
7.2.4 Physical access and environment typical implementation	37
7.3 Equipment requirement	37
7.3.1 General	37
7.3.1.1 Main functions	37
7.3.1.2 Compensating countermeasure	38
7.3.1.3 Security requirements for the equipment	38
7.3.2 FR 1 – Identification and authentication control	39
7.3.2.1 Purpose	39
7.3.2.2 Rationale	39
7.3.2.3 CR 1.1 – Human user identification and authentication	39
7.3.2.4 CR 1.2 – Software and equipment identification and authentication	40

	7.3.2.5	CR 1.5 – Authenticator management.....	40
	7.3.2.6	CR 1.7 – Strength of password-based authentication	40
	7.3.2.7	CR 1.8 – Public key infrastructure certificates	41
	7.3.2.8	CR 1.9 – Strength of public key-based authentication	41
	7.3.2.9	CR 1.10 – Authenticator feedback	41
	7.3.2.10	CR 1.11 – Unsuccessful login attempts	42
	7.3.2.11	CR 1.14 – Strength of symmetric key-based authentication	42
7.3.3	FR 2 – Use control.....		42
	7.3.3.1	Purpose	42
	7.3.3.2	Rationale	42
	7.3.3.3	CR 2.1 – Authorization enforcement.....	42
	7.3.3.4	CR 2.2 – Wireless use control	43
	7.3.3.5	EDR 2.4 – Mobile code	43
	7.3.3.6	CR 2.5 – Session lock.....	44
	7.3.3.7	CR 2.6 – Remote session termination	44
	7.3.3.8	CR 2.7 – Concurrent session control	45
	7.3.3.9	CR 2.8 – Auditable events.....	45
	7.3.3.10	CR 2.9 – Audit storage capacity	46
	7.3.3.11	CR 2.10 – Response to audit processing failures	46
	7.3.3.12	CR 2.11 Timestamp	46
	7.3.3.13	CR 2.12 – Non-repudiation.....	47
	7.3.3.14	EDR 2.13 – Use of physical diagnostic and test interfaces	47
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	48
	7.3.4.4	EDR 3.2 – Protection from malicious code	49
	7.3.4.5	CR 3.3 – Security functionality verification	49
	7.3.4.6	CR 3.4 – Software and information integrity	49
	7.3.4.7	CR 3.5 – Input validation.....	50
	7.3.4.8	CR 3.6 – Deterministic output	51
	7.3.4.9	CR 3.7 – Error handling	51
	7.3.4.10	CR 3.8 – Session Integrity	51
	7.3.4.11	CR 3.9 – Protection of audit information.....	52
	7.3.4.12	EDR 3.10 – Support for Updates	52
	7.3.4.13	EDR 3.11 – Physical tamper resistance and detection.....	52
	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.....	53
	7.3.4.16	EDR 3.14 – Integrity of the boot process	53
7.3.5	FR 4 – Data confidentiality.....		54
	7.3.5.1	Purpose	54
	7.3.5.2	Rationale	54
	7.3.5.3	CR 4.1 – Information confidentiality.....	54
	7.3.5.4	CR 4.3 – Use of cryptography	54
7.3.6	FR 5 – Restricted data flow.....		55
7.3.7	FR 6 – Timely response to events.....		55
	7.3.7.1	Purpose	55
	7.3.7.2	Rationale	55

7.3.7.3	CR 6.1 – Audit log accessibility	55
7.3.8	FR 7 – Resource availability	55
7.3.8.1	Purpose	55
7.3.8.2	Rationale	55
7.3.8.3	CR 7.1 – Denial of service protection	56
7.3.8.4	CR 7.2 – Resource management.....	56
7.3.8.5	CR 7.3 – Control system backup	57
7.3.8.6	CR 7.4 – Control system recovery and reconstitution	57
7.3.8.7	CR 7.6 – Network and security configuration settings.....	58
7.3.8.8	CR 7.7 – Least functionality	58
7.3.8.9	CR 7.8 – Control system inventory	59
8	Instructions for installation, operation and maintenance.....	59
8.1	User instruction requirement	59
8.2	User instruction enhancement.....	60
8.3	User instruction implementation	60
9	Conformance verification and testing	60
9.1	General.....	60
9.2	Life cycle management	60
9.3	Physical access	60
9.3.1	Verification of physical access and environment	60
9.3.2	Physical access and environment enhancement	61
9.4	FR 1 – Identification and authentication control.....	61
9.4.1	CR 1.1 – Human user identification and authentication	61
9.4.1.1	Requirement verification	61
9.4.1.2	Requirement CR 1.1 e.1 verification	61
9.4.2	CR 1.2 – Software and equipment identification and authentication	61
9.4.2.1	Requirement verification	61
9.4.2.2	Requirement CR 1.2 e.1 verification	62
9.4.3	CR 1.5 – Authenticator management	62
9.4.3.1	Requirement verification	62
9.4.4	CR 1.7 – Strength of password-based authentication.....	62
9.4.4.1	Requirement verification	62
9.4.5	CR 1.8 – Public key infrastructure certificates.....	62
9.4.5.1	Requirement verification	62
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	63
9.4.7.1	Requirement verification	63
9.4.8	CR 1.11 – Unsuccessful login attempts.....	63
9.4.8.1	Requirement verification	63
9.4.9	CR 1.14 – Strength of symmetric key-based authentication	63
9.4.9.1	Requirement verification	63
9.5	FR 2 – Use control.....	64
9.5.1	CR 2.1 – Authorization enforcement	64
9.5.1.1	Requirement verification	64
9.5.1.2	Requirement CR 2.1 e.1 verification	64
9.5.2	CR 2.2 – Wireless use control.....	64
9.5.2.1	Requirement verification	64

9.5.3	EDR 2.4 – Mobile code	64
	9.5.3.1 Requirement verification	64
	9.5.3.2 Requirement EDR 2.4 e.1 verification	65
9.5.4	CR 2.5 – Session lock	65
	9.5.4.1 Requirement verification	65
9.5.5	CR 2.6 – Remote session termination	65
	9.5.5.1 Requirement verification	65
9.5.6	CR 2.7 – Concurrent session control	65
	9.5.6.1 Requirement verification	65
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	66
	9.5.8.1 Requirement verification	66
	9.5.8.2 Requirement CR 2.9 e.1 verification	66
9.5.9	CR 2.10 – Response to audit processing failures	66
	9.5.9.1 Requirement verification	66
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	67
9.5.11	CR 2.12 – Non-repudiation	67
	9.5.11.1 Requirement verification	67
9.5.12	EDR 2.13 – Use of physical diagnostic and test interfaces	67
	9.5.12.1 Requirement verification	67
9.6	FR 3 – System integrity	67
9.6.1	CR 3.1 – Communication integrity	67
	9.6.1.1 Requirement verification	67
	9.6.1.2 Requirement CR 3.1 e.1 verification	68
9.6.2	EDR 3.2 – Protection from malicious code	68
	9.6.2.1 Requirement verification	68
9.6.3	CR 3.3 – Security functionality verification	68
	9.6.3.1 Requirement verification	68
9.6.4	CR 3.4 – Software and information integrity	68
	9.6.4.1 Requirement verification	68
	9.6.4.2 Requirement CR 3.4 e.1 verification	69
9.6.5	CR 3.5 – Input validation	69
	9.6.5.1 Requirement verification	69
9.6.6	CR 3.6 – Deterministic output	69
	9.6.6.1 Requirement verification	69
9.6.7	CR 3.7 – Error handling	69
	9.6.7.1 Requirement verification	69
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	70
	9.6.9.1 Requirement verification	70
9.6.10	EDR 3.10 – Support for updates	70
	9.6.10.1 Requirement verification	70
	9.6.10.2 Requirement CR 3.10 e.1 verification	70
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	71
9.6.12.1	Requirement verification	71
9.6.13	EDR 3.13 – Provisioning asset owner roots of trust	71
9.6.13.1	Requirement verification	71
9.6.14	EDR 3.14 – Integrity of the boot process.....	71
9.6.14.1	Requirement verification	71
9.6.14.2	Requirement CR 3.14 e.1 verification	72
9.7	FR 4 – Data confidentiality	72
9.7.1	CR 4.1 – Information confidentiality	72
9.7.1.1	Requirement verification	72
9.7.2	CR 4.3 – Use of cryptography	72
9.7.2.1	Requirement verification	72
9.8	FR 6 – Timely response to events	72
9.8.1	CR 6.1 – Audit log accessibility.....	72
9.8.1.1	Requirement verification	72
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	73
9.9.2.1	Requirement verification	73
9.9.3	CR 7.3 – Control system backup.....	73
9.9.3.1	Requirement verification	73
9.9.3.2	Requirement CR 7.3 e.1 verification	73
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	74
9.9.6.1	Requirement verification	74
9.9.7	CR 7.8 – Control system inventory.....	74
9.9.7.1	Requirement verification	74
Annex A	(informative) Cybersecurity and electrical system architecture	75
A.1	General.....	75
A.2	Typical architecture involving switchgear and controlgear and their assembly.....	75
A.2.1	Building	75
A.2.2	Manufacturing.....	76
Annex B	(informative) Use case studies	78
B.1	General.....	78
B.2	Use case 1 – Protection against Denial of Service (DoS) attack	79
B.3	Use case 2 – Protection against unauthorized modification of sensing device	80
B.4	Use case 3 – Protection against unauthorized modification of wireless equipment.....	81
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 aspects	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 and 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	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.....	94
Annex F (normative)	Security protection profile of network connected motor starter.....	95
F.1	Introduction.....	95
F.1.1	Protection profile reference.....	95
F.1.2	Target of evaluation overview	95
F.1.3	General mission objectives	95
F.1.4	Features	96
F.1.5	Product usage	96
F.1.6	Users.....	96
F.2	Assumptions	97
F.3	Conformance claims and conformance statement	97
F.4	Security problem definition.....	97
F.4.1	Critical assets of the environment.....	97
F.4.2	ToE critical assets	98
F.4.3	Threat Model	98
F.4.3.1	Attackers.....	98

F.4.3.2	Threats	98
F.5	Security objectives	99
F.6	Security requirements	99
F.6.1	Security functional requirements	99
F.6.2	Security assurance requirements	100
Annex G (normative)	Security protection profiles of circuit-breaker	101
G.1	Introduction	101
G.1.1	Protection profile reference	101
G.1.2	Target of evaluation overview	101
G.1.3	General mission objectives	101
G.1.4	Features	102
G.1.5	Product usage	102
G.1.6	Users	102
G.2	Assumptions	102
G.3	Conformance claims and conformance statement	103
G.4	Security problem definition	103
G.4.1	Critical assets of the environment	103
G.4.2	ToE critical assets	104
G.4.3	Threat Model	104
G.4.3.1	Attackers	104
G.4.3.2	Threats	104
G.5	Security objectives	105
G.6	Security requirements	105
G.6.1	Security functional requirements	105
G.6.2	Security assurance requirements	106
Annex H (normative)	Protection profile of transfer switch equipment	107
H.1	Introduction	107
H.1.1	Protection profile reference	107
H.1.2	Target of evaluation overview	107
H.1.2.1	Overview	107
H.1.3	General mission objectives	108
H.1.4	Features	108
H.1.5	Product usage	108
H.1.6	Users	108
H.2	Assumptions	109
H.3	Conformance claims and conformance statement	109
H.4	Security problem definition	109
H.4.1	Critical assets of the environment	109
H.4.2	ToE critical assets	110
H.4.3	Threat Model	110
H.4.3.1	Attackers	110
H.4.3.2	Threats	110
H.5	Security objectives	111
H.6	Security requirements	111
H.6.1	Security functional requirements	111
H.6.2	Security assurance requirements	112
Annex I (normative)	Protection profile for wireless controlgear with its communication interface	113

I.1	Introduction.....	113
I.1.1	Protection profile reference.....	113
I.1.2	Target of evaluation overview	113
I.1.3	General mission objectives	114
I.1.4	Features	114
I.1.5	Product usage	114
I.1.6	Users.....	114
I.2	Assumptions	114
I.3	Conformance claims and conformance statement	115
I.4	Security problem definition.....	115
I.4.1	Critical assets of the environment.....	115
I.4.2	ToE critical assets	116
I.4.3	Threat Model	116
	I.4.3.1 Attackers.....	116
	I.4.3.2 Threats	116
I.5	Security objectives.....	117
I.6	Security requirements	117
I.6.1	Security functional requirements.....	117
I.6.2	Security assurance requirements.....	118
Annex J (informative)	Equipment requirements by level of exposure	119
Annex K (informative)	Bridging references to cybersecurity management systems	121
Annex L (informative)	Mapping of provisions to the essential cybersecurity requirements of the European Cyber Resilient Act Annexes	127
Bibliography.....		130
Figure 1 – Standard landscape		14
Figure 2 – Example of physical interfaces of an embedded device in an equipment which can be subject to an attack		25
Figure 3 – Example of relation between security and safety		26
Figure 4 – Control system architecture with switchgear and controlgear.....		30
Figure 5 – Control system connectivity level C1		31
Figure 6 – Control system connectivity level C2		31
Figure 7 – Control system connectivity level C3		32
Figure 8 – Control system connectivity level C4		32
Figure 9 – Control system connectivity level C5		33
Figure 10 – Structure of a security protection profile		35
Figure°11 – Example of security instruction symbol		60
Figure°A.1 – Building electrical architecture.....		76
Figure°A.2 – Industrial plants.....		77
Figure E.1 – Machinery control architecture		89
Figure F.1 – Machinery control architecture		95
Figure G.1 – Circuit-breaker in its environment		101
Figure H.1 – Functional units of the transfer switch equipment.....		107
Figure I.1 – Machinery control architecture		113

Table 1 – Potential attack levels	24
Table 2 – Typical threats.....	24
Table 3 – Impact evaluation	27
Table 4 – Roles related to security responsibilities.....	28
Table 5 – Level of exposure of an equipment.....	33
Table 6 – Equipment security level	34
Table°7 – Physical access related requirement references	36
Table°8 – Physical access enhancement related requirement references.....	36
Table B.1 – List of actors	78
Table B.2 – Base line requirement	78
Table B.3 – Security problems of use cases.....	78
Table E.1 – Security requirements for the critical assets of the environment	92
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	98
Table F.2 – Security requirements for the critical assets	98
Table F.3 – Security functional requirements	99
Table G.1 – Security requirements for the critical assets of the environment.....	103
Table G.2 – Security requirements for the critical assets.....	104
Table G.3 – Security functional requirements.....	105
Table H.1 – Security requirements for the critical assets of the environment.....	110
Table H.2 – Security requirements for the critical assets.....	110
Table H.3 – Security functional requirements	111
Table I.1 – Security requirements for the critical assets of the environment	115
Table I.2 – Security requirements for the critical assets	116
Table I.3 – Security functional requirements	117
Table J.1 – Equipment requirements by level of exposure.....	119
Table K.1 – Useful security standards.....	121
Table K.2 – Contribution of switchgear and controlgear and their assemblies to ISO and IEC horizontal security framework	122
Table K.3 – Mapping to other security framework.....	125
Table K.4 – Requirements for IACS not relevant for switchgear and controlgear and their assemblies.....	125
Table K.5 – Requirements for IoT device not relevant for switchgear and controlgear and their assemblies	126
Table L.1 – Mapping to the essential cybersecurity requirements of the CRA Annexe I	127

INTERNATIONAL ELECTROTECHNICAL COMMISSION

**LOW-VOLTAGE SWITCHGEAR AND CONTROLGEAR AND THEIR
ASSEMBLIES –
SECURITY ASPECTS**

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
XX/XX/FDIS	XX/XX/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.

INTRODUCTION

The growing use of data communication capabilities by switchgear and 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 actual power supply values, monitoring data, data logging and remote upgrade.

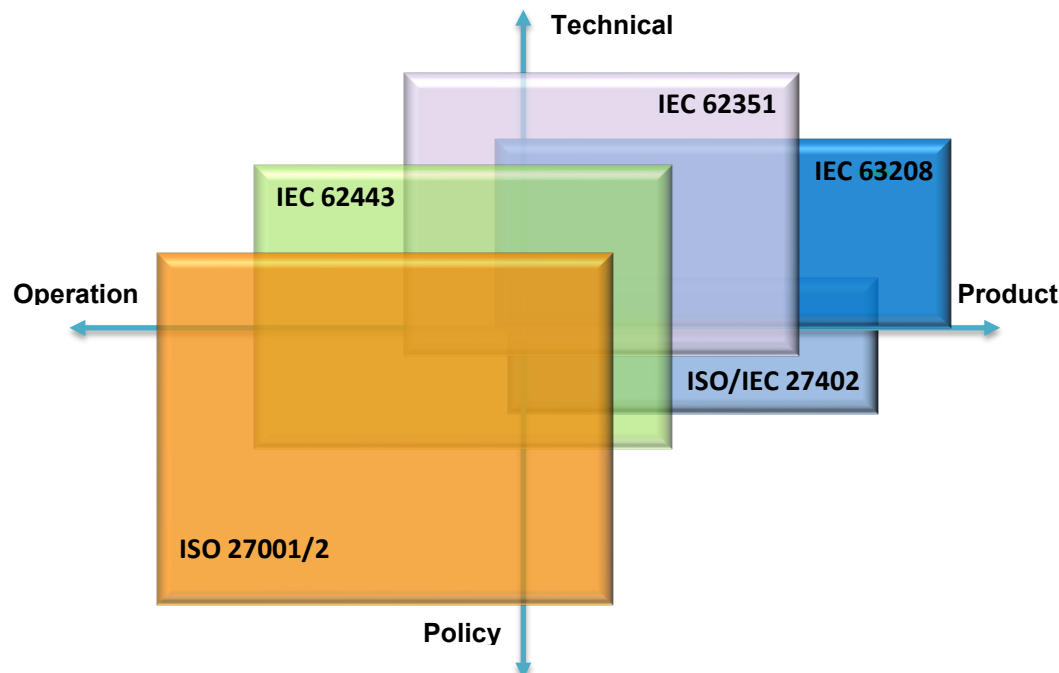
For these typical applications of electrical distribution and machinery, minimum cybersecurity requirements are needed for maintaining an acceptable level of safety integrity of the main functions for equipment, with or without data communication capability. These requirements are intended to limit the 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.

27



28

Figure 1 – Standard landscape

Figure 1 positions the standard landscape of the standards considered in this document with respects 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 and controlgear 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 requirement 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.

55

LOW-VOLTAGE SWITCHGEAR AND CONTROLGEAR AND THEIR ASSEMBLIES – SECURITY ASPECTS

1 Scope

This document applies to the security related main functions of switchgear and controlgear and their assemblies, called equipment, in the context of operational technology. It is applicable to equipment with wired or wireless data communication means and their physical accessibility, within their limits of environmental conditions.

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 level for the equipment;
- countermeasures for the physical access and the environment derived from ISO/IEC 27001:2013;
- 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 of the switching device or the control device, which can lead to hazardous situations;
- unavailability of the protective functions (overcurrent, earth leakage, 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 requirement 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

98 – data confidentiality other than for critical security parameters.

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

100 **2 Normative references**

101 The following documents are referred to in the text in such a way that some or all of their content
102 constitutes requirements of this document. For dated references, only the edition cited applies.
103 For undated references, the latest edition of the referenced document (including any
104 amendments) applies.

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

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

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

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

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

114 IEC TS 62443-6-2:2024¹, *Security evaluation methodology for IEC 62443 - Part 4-2: Technical*
115 *security requirements for IACS components*

116 ISO/IEC 27001:2013, *Information technology – Security techniques – Information security*
117 *management systems – Requirements*

118 ISO/IEC 27005, *Information security, cybersecurity and privacy protection — Guidance on*
119 *managing information security risks*

120 ISO/IEC 27402:2023², *Cybersecurity – IoT security and privacy – Device baseline requirements*

121 **3 Terms, definitions and abbreviated terms**

122 **3.1 Terms and definitions**

123 For the purposes of this document, the following terms and definitions given in
124 IEC 60947-1:2020 and the following apply.

125 ISO and IEC maintain terminological databases for use in standardization at the following
126 addresses:

- 127 • IEC Electropedia: available at <http://www.electropedia.org/>
- 128 • ISO Online browsing platform: available at <http://www.iso.org/obp>

¹ Currently under development at the stage IEC CD TS 62443-6-2

² Currently under development at the stage ISO/IEC FDIS 27402:2023

3.1.1**audit log****event storing****telemetry**

logs collecting the evidence of selected user activities, exceptions, and information security events

Note 1 to entry: These logs are kept for an agreed period of time to assist in future investigations.

Note 2 to entry: Audit logs can be used to comply with legal requirements.

[SOURCE: ISO/IEC 24775-2:2014, 3.1.7 modified with additional synonymous names]

3.1.2**attack**

attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset

[SOURCE: ISO/IEC 27000:2018, 3.2]

3.1.3**attack surface**

set of attack points that an attacker can use in order to trigger an attack

[SOURCE: ISO/TS 12812-2:2017, 3.4, modified – "enter or capture data in an information system" replaced by "trigger an attack".]

3.1.4**attack vector**

path or means by which an attacker can gain access to a device in order to generate an attack

[SOURCE: ISO/IEC 27032:2012, 4.10, modified – "computer or network server" replaced by "device" and "deliver a malicious outcome" by "generate an attack".]

3.1.5**authentication**

security measure designed to establish the validity of a transmission, message, or originator

[SOURCE: IEC TS 62443-1-1:2009, 3.2.13, modified – Last part of the definition deleted.]

3.1.6**authenticator**

means used to confirm the identity of an entity

EXAMPLE A password or token may be used as an authenticator

3.1.7**authenticity**

property that an entity is what it claims to be

[SOURCE: ISO/IEC 27000:2018, 3.6]

3.1.8**authorization**

right or permission that is granted to a system entity or an individual to access a system resource

169 [SOURCE: IEC TS 62443-1-1:2009, 3.2.14, modified – Addition of "or an individual".]

170 **3.1.9**

171 **ordinary person**

172 person who is neither a skilled person nor an instructed person

173 [SOURCE: IEC 60050-826:2004, 826-18-03]

174 **3.1.10**

175 **authorized person**

176 skilled or instructed person who is empowered to execute defined work

177 [SOURCE: IEC 61439-1:2020, 3.7.17]

178 **3.1.11**

179 **availability**

180 property of being accessible and usable upon demand by an authorized entity

181 [SOURCE: ISO/IEC 27000:2018, 3.7]

182 **3.1.12**

183 **building management system**

184 **BMS**

185 computer-based system installed in buildings that controls and monitors the building's
186 mechanical and electrical equipment such as heating, cooling, ventilating, lighting, power,
187 disaster prevention, and security systems

188 [SOURCE: ISO 18566-1:2017, 3.6]

189 **3.1.13**

190 **confidentiality**

191 property that information is not made available or disclosed to unauthorized individuals, entities
192 or processes

193 [SOURCE: ISO/IEC 24767-1:2008, 2.1.2]

194 **3.1.14**

195 **countermeasure**

196 action, device, procedure, or technique that reduces a threat, a vulnerability, or an attack by
197 eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting
198 it so that corrective action can be taken

199 [SOURCE: IEC TS 62443-1-1:2009, 3.2.33, modified – Note deleted.]

200 **3.1.15**

201 **critical security parameter**

202 **CSP**

203 security related information whose disclosure or modification can compromise the security of a
204 cryptographic module

205 EXAMPLE: Secret and private cryptographic keys, authentication data such as passwords, PINs, certificates or other
206 trust anchors.

207 Note 1 to entry: A CSP can be plaintext or encrypted.

208 [SOURCE: ISO/IEC 19790:2012, definition 3.18]

3.1.16**cybersecurity**

preservation of confidentiality, integrity and availability of information in the cyberspace

Note 1 to entry: The objective is to reduce the risk of causing personal injury or endangering public health, losing public or consumer confidence, disclosing sensitive assets, failing to protect business assets or failing to comply with regulations. These concepts are applied to any system in the production process and include both stand-alone and networked components. Communications between systems may be either through internal messaging or by any human or machine interfaces that authenticate, operate, control, or exchange data with any of these control systems. Cybersecurity includes the concepts of identification, authentication, accountability, authorization, availability, and privacy.

[SOURCE: ISO/IEC 27032:2012, 4.20, modified – Notes replaced with the Note to entry.]

3.1.17**data integrity**

property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner

Note 1 to entry: This term deals with constancy of and confidence in data values, not with the information that the values represent or the trustworthiness of the source of the values.

[SOURCE: IEC TS 62443-1-1:2009, 3.2.38]

3.1.18**defence in depth**

provision of multiple security protections, especially in layers, with the intent to delay if not prevent an attack

Note 1 to entry: Defence in depth implies layers of security and detection, even on single systems, and provides the following features:

- attackers are faced with breaking through or bypassing each layer without being detected;
- a flaw in one layer can be mitigated by capabilities in other layers;
- a system security becomes a set of layers within the overall network security.

[SOURCE: IEC TS 62443-1-1:2009, 3.2.40]

3.1.19**system integrity**

property that a system performs its intended function in an unimpaired manner, free from deliberate or accidental unauthorized manipulation

[SOURCE: ISO/TR 11633-2:2009, 2.14, modified – "of the system" deleted.]

3.1.20**denial of service**

prevention of authorized access to resources or the delaying of time-critical operations

[SOURCE: ISO 7498-2:1989, 3.3.25]

3.1.21**hazardous situation**

circumstance in which people, property or the environment is/are exposed to one or more hazards

[SOURCE: ISO/IEC Guide 51:2014, 3.4]

3.1.22**security audit**

independent review and examination of a system's records and activities to determine the adequacy of system controls, ensure compliance with established security policy and procedures, detect breaches in security services, and recommend any changes that are indicated for countermeasures

[SOURCE: IEC TS 62443-1-1:2009, 3.2.101]

3.1.23**security related main function****essential function****main function**

<of switchgear and controlgear and their assemblies>

function of switchgear or controlgear or their assemblies whose failure can result in its unwanted operation which can lead to hazardous situations, in the loss or the corruption of its protective function, or in the loss or the corruption of an extended functionality defined in the product documentation

Note 1 to entry: When an additional function such as energy monitoring of a circuit-breaker can be subject to attack leading to the corruption of the security related main function, such as the short-circuit protection, this additional function is considered as a security related main function.

Note 2 to entry: Main functions include, but are not limited to, the electrical protective function, the control function and the ability of the operator to view and manipulate the equipment. The loss of main functions is commonly termed loss of protection, loss of control and loss of view respectively.

EXAMPLE

- unintended operation of the switching device or the control device, which can lead to hazardous situations;
- unavailability of the protective functions (overcurrent, earth leakage, etc.).

[SOURCE: IEC 62443-3-3:2013, derived from 3.1.22]

3.1.24**complementary function**

<of switchgear and controlgear and their assemblies> function of switchgear or controlgear or their assemblies not identified as security related main function

3.1.25**threat**

potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm

[SOURCE: IEC TS 62443-1-1:2009, 3.2.125]

3.1.26**security policy**

set of rules that specify or regulate how a system or organization provides security services to protect its assets

[SOURCE: IEC TS 62443-1-1:2009, 3.2.112]

3.1.27**security vulnerability**

weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat

[SOURCE: ISO/IEC TR 24772:2013, 3.1.5.3]

3.1.28**security risk assessment**

process that systematically identifies potential vulnerabilities to valuable system resources and threats to those resources, quantifies loss exposures and consequences based on probability of occurrence, and (optionally) recommends how to allocate resources to countermeasures to minimize the exposure

[SOURCE: IEC TS 62443-1-1:2009, 3.2.88, modified – "total exposure" replaced by "the exposure" and notes deleted.]

3.1.29**protection profile**

PP

implementation-independent statement of security needs for a target of evaluation type

[SOURCE: ISO/IEC 15408-1:2009, 3.1.52]

3.1.30**mobile software program****mobile code**

software program or parts of programs transferred from remote system through communication link that can be executed automatically

EXAMPLE JavaScript, Java applets or ActiveX controls often downloaded from the internet into HTML web pages to be executed locally.

3.1.31**operational technology**

OT

hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices and systems, processes and events in the organization

[SOURCE: ISO/IEC TR 23188:2020, 3.2.7]

3.1.32**safety**

freedom from risk which is not tolerable

[SOURCE: ISO/IEC Guide 51: 2014, 3.14]

3.1.33**security**

condition that results from the establishment and maintenance of protective measures that ensure a state of inviolability from hostile acts or influences

[SOURCE: IEC TS 62351-2:2008, 2.2.173]

3.1.34**supervisory control and data acquisition system****SCADA system**

type of loosely coupled distributed monitoring and control system commonly associated with electric power transmission and distribution systems, oil and gas pipelines, and water and sewage systems

3.1.35**smart manufacturing**

domain of integrated products, processes and resources (cyber, physical, human) to create and deliver products and services, which also collaborates with other domains within an enterprise's value chains and continuously improves its performance aspects

Note 1 to entry: Performance aspects include agility, efficiency, safety, security, sustainability or any other performance indicators identified by the enterprise.

Note 2 to entry: In addition to manufacturing, other enterprise domains can include engineering, logistics, marketing, procurement, sales or any other domains identified by the enterprise.

3.1.36**user interface**

component of an interactive system (software or hardware) that provides the information and controls necessary for the user to accomplish specific tasks with the interactive system

Note 1 to entry: Dip switch, control switch, operating means or manual setting are not considered as user interface.

[SOURCE: ISO 1503:2008, 3.17]

3.2 Abbreviated terms

APN	access point name
AR	additional recommendation(s)
BMS	building management systems
BT	Bluetooth® ³
CCTV	closed circuit television
CF	communication functionalities
CVSS	common vulnerability scoring system
CR	component requirement
CRL	certificate revocation list
DNP	distributed network protocol
DMZ	demilitarized zone
DoS	denial of service
DDoS	distributed denial of service
EMC	electromagnetic compatibility
ERP	enterprise resource planning
FR	foundational requirement
HMI	human machine interface
HVAC	heating, ventilation, and air conditioning
ICS	industrial control system
IDS	intrusion detection system
IPS	intrusion prevention system
IP	internet protocol
IT	information technology

³ Bluetooth® trademark is an example of a suitable communication protocol available commercially. This information is given for the convenience of users of this document and does not constitute an endorsement by IEC of this communication protocol.

376	IoT	Internet of things
377	MLP	multiprotocol label switching
378	NFC	near field communication
379	OT	operational technology
380	PLC	programmable logic controller
381	P2P	peer to peer connection
382	RBAC	role-based access control
383	RS485	recommended standard 485 (according to TIA 485-A)
384	SCADA	supervisory control and data acquisition
385	SD card	secure digital card
386	SSL	secure socket layer
387	ULP	universal logic plug
388	USB	universal serial bus
389	VPN	virtual private network

390 **4 General**

391 The integrity or the availability of the main functions of switchgear and controlgear and their
392 assemblies can depend on physical security and cybersecurity aspects. The existing
393 procedures for physically accessing equipment shall be considered as part of the security
394 countermeasures together with the cybersecurity countermeasures.

395 **5 Security objectives**

396 In the context of electrical distribution with switchgear and machine control with controlgear
397 (see Annex A), the overall security objectives are to ensure they operate as designed and
398 configured and specially to avoid unintended operation and to protect their security related main
399 functions.

400 The main security aspects to be considered are: data integrity, authenticity and availability.

401 The availability and the integrity of the main functions of the equipment listed in 7.3.1.1 shall
402 be identified as precondition to the security objectives by referring to each product standard
403 and the safety risk assessment performed by the designer of the equipment.

404 **6 Security lifecycle management**

405 **6.1 General**

406 The protections against security attacks are determined based on the results of a security risk
407 assessment in order to identify the potential threats and vulnerabilities, and to define the
408 countermeasures in a document called security requirements specification. As described in IEC
409 62443-4-1 and ISO/IEC 27001, it covers each phase of the life cycle of the equipment and the
410 relevant stakeholders, and it takes into account its physical access and the limits of its
411 environmental conditions (see Figure 2 as an example).

412 To determine the necessary security assurance measures and their parameters, it is necessary
413 to define the expected threat actor, characterized with a specific strength, also called potential
414 attack levels. The levels given in Table 1 are assumed in this document.

415

Table 1 – Potential attack levels

Level	Potential attack	Method of evaluation
Basic	Known basic risks of cyber incidents and cyberattacks	Review of the technical documentation ^a
Substantial	Known cybersecurity risks, and the risk of incidents and cyberattacks carried out by actors with limited skills and resources	Review of the absence of publicly known vulnerabilities and testing of the correctly implemented necessary security functionalities ^b
High	Complex cyberattacks using state-of-the-art techniques carried out by actors with significant skills and resources	Review of the absence of publicly known vulnerabilities, testing of the correctly implemented necessary security functionalities and assessment of their resistance to skilled attackers (threat actor), using penetration testing ^c
^a Correspond to SL 1 of Annex A of IEC 62443-3-2:2020 ^b Correspond to SL 2 of Annex A of IEC 62443-3-2:2020 ^c Correspond to SL 3 of Annex A of IEC 62443-3-2:2020		

416

417 Typical threats and their associated countermeasures are given in the use cases described in
418 Annex B, as listed below in Table 2. Specific threats related to particular security protection
419 profiles are given in Annex E to Annex H.

420

Table 2 – Typical threats

BSI ^a Top 10 threats	Use case		Level of attack
	Number	Name	
Infiltration of malware via removable media and mobile systems			
Infection with malware via internet and intranet			
Human error and sabotage	UC2 (B.3)	Use case 2 – Protection against unauthorized modification of sensing device	basic
Compromising of extranet and cloud components			
Social engineering and phishing			
(D)Dos attacks	UC1 (B.2)	Use case 1 – Protection against Denial of Service (DoS) attack	Substantial
Internet connected control components	UC4 (B.5)	Use case 4 – Protection against threat actor remotely taking control of a “Managing” intelligent assembly	Substantial
Intrusion via remote maintenance access	UC3 (B.4)	Use case 3 – Protection against unauthorized modification of wireless equipment	Substantial
Technical failure and force majeure			
Soft- and hardware vulnerabilities in the supply chain			
^a German Federal Office for Information Security, BSI-CS 005 ED1.50:2022-05-03			

421

The risk associated with corrupting certain security related main functions in some industries can be so severe that efforts associated with risk mitigation may outweigh the benefit of utilizing programmable digital products and highly integrated systems. In such cases, a risk analysis detailing the benefits and drawbacks of utilizing such products and systems is recommended.

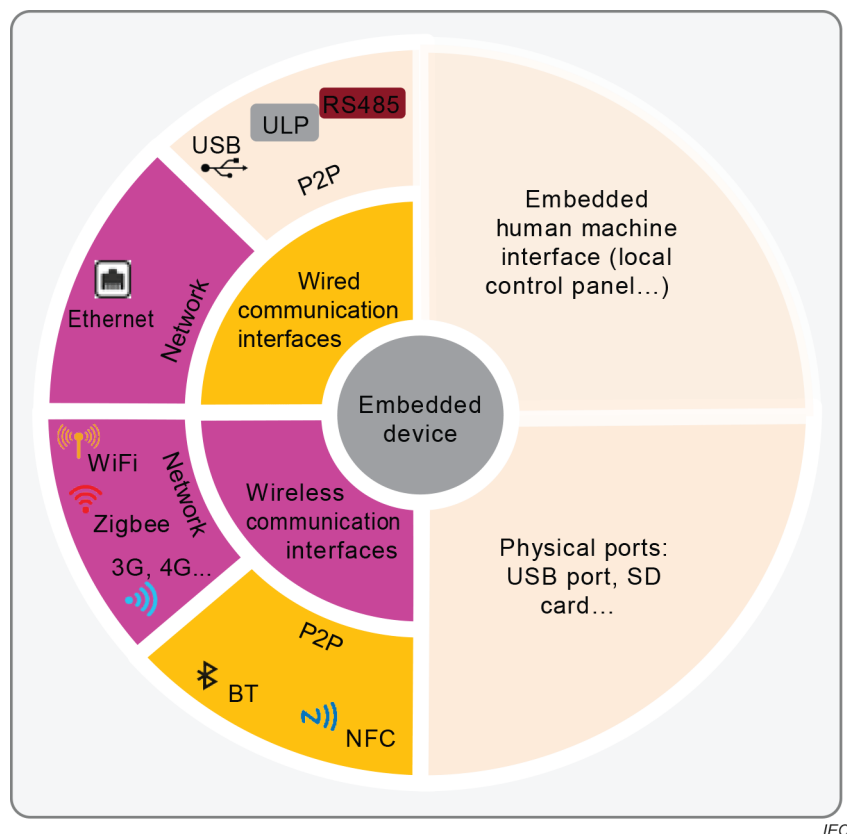


Figure 2 – Example of physical interfaces of an embedded device in an equipment which can be subject to an attack

6.2 Security risk assessment

6.2.1 General

In general, a security risk assessment includes an equipment/system in its environment on which threats and known vulnerabilities are taken into account. After being performed, this assessment will allow defining relevant countermeasures to fulfil the overall security objectives.

All relevant threats and known equipment/system vulnerabilities possibly affecting the main functions of the equipment shall be considered and documented as part of the security risk assessment.

The following aspects shall be considered in the risk assessment in combination with the potential attack level of Table 1:

- defined context using the relevant protection profile such as defined in Annex E to Annex H;
- correct flow of categorized information throughout the intended system architecture defined in 6.7;
- trust boundaries;
- main functions;
- data stores;

- intended interaction with other equipment;
- communication protocols implemented in the equipment;
- user accessible physical ports;
- potential attack vectors including attacks on the hardware if applicable;
- potential threats according to Table 2, their likelihood, and their severity and consequences as defined in 6.2.3.;
- relation to safety as given in 6.2.2;
- mitigations and/or dispositions for each threat;
- security-related issues identified;
- external dependencies in the form of drivers or third-party applications (code that is not developed by the supplier) that are linked into the application.

NOTE This list is derived from IEC 62443-4-1:2018.

A vulnerability assessment shall be carried out to identify vulnerabilities, to which identified threats are exploitable, of the equipment within its intended use and the potential influence related to its security related main functions.

NOTE The vulnerability assessment of external dependencies can be facilitated by searching the vulnerabilities registered in CPE database (Common Platform Enumeration).

6.2.2 Relationship between safety and security

The safety risk assessment of the equipment shall include the possible interaction between the main functions of the equipment listed in 7.3.1.1 and the security protection functions. In case of interaction, further actions shall be taken to ensure there is no impact on the main functions.

Figure 3 shows an example of an attack using a vulnerability of an interface of the equipment leading to a direct impact on complementary functionalities (e.g., loss of service) and a subsequent impact to main functions of the equipment. This subsequent impact can be triggered because of specific vulnerabilities on the main functions. In this example, the implementation of the countermeasures should be established at the appropriate level (equipment or individual main function) taking into consideration possible impact of the security countermeasures on the main functions.

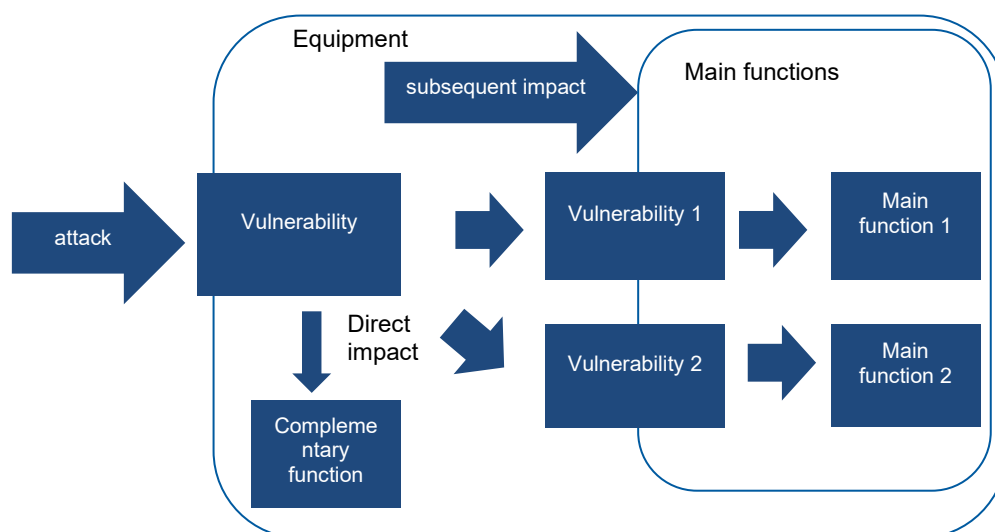


Figure 3 – Example of relation between security and safety

For the common application of functional safety according to IEC 61508 series and cybersecurity according to IEC 62443 series, see IEC TS 63069⁴.

6.2.3 Impact assessment

The assessment of the potential impacts of an attack shall be performed following a standardised method according to

- ISO/IEC 27005 for general purpose applications or
- IEC 62443-3-2 for industrial control systems.

The impacts should be evaluated according to the levels defined in Table 3 in the context of the intended system including impacts on the end user.

NOTE Regional standards such as NIST SP 800-30 can also be used.

Table 3 – Impact evaluation

Level	Safety ^a	Operation	Reputation
Critical	Death or irreversible injuries	Durably inoperable	Durable loss of trust
Moderate	Significant injuries	Temporary failover	Unsatisfied customer
Minor	Benign injuries	No main function affected	Small incident
^a Safety risks are covered by the requirements of the relevant product standard completed by the safety risk assessment performed by the designer of the equipment. Safety risk assessment shall be taking in consideration in the security risk assessment without change.			

Note: The levels are adapted from Table E.1 b) of ISO/IEC 27005:2011 and the most relevant impacts from E.2.1 of the ISO/IEC 27005:2011. For example, legal, financial or contractual impacts are more relevant for asset owner of buildings or production systems than switchgear, controlgear and assembly suppliers.

6.2.4 Security risk assessment result

The risk assessment shall result in the description of:

- the intended system covered by a security risk assessment (e.g. mobile control panel, optional communication interface);
- the architecture(s) into which the equipment is intended for according to 6.7;
- the various phases such as design, implementation, commissioning, operation, and maintenance of the equipment and the intended system;
- the identified vulnerabilities that could be exploited by threats and result in security risks (including intentional attacks on the hardware, embedded software and parameterization software, as well as unintended events resulting from human error);
- the potential consequences resulting from the security risks, by considering the possibility under which condition these can occur;
- for each phase, the requirements for additional countermeasures;
- the information on the countermeasures taken to reduce or remove the threats.

⁴ Currently under development at the stage IEC CD TS 63069.

6.3 Response to security risk

Responses to security risks include the following:

- mitigate intolerable security risks by:
 - a) designing the security risk out (avoid); or
 - b) limiting the security risk; or
 - c) transferring or sharing the security risk (by implementing compensating countermeasure in another entity);
- accept the security risk if tolerable.

6.4 Security requirement specification

Based on the results of the security risk assessment including the vulnerabilities of the equipment, a security requirements specification shall be generated with at least the following:

- the description of the security related main function of the equipment;
- vulnerabilities that can have an impact on this function and assumed threats, if applicable;
- consequences on the security related main function;
- description of proposed security countermeasure(s) based on the security requirements given in Clause 6.7.5.

6.5 Roles and responsibilities

Switchgear and controlgear of electrical installation and machinery are managed slightly differently but generally, the different actors apply the instructions given product documentation. The responsibilities related to cybersecurity illustrated in Table 4 confirm this principle.

Table 4 – Roles related to security responsibilities

Roles	Security responsibilities	Example of mapping to system roles		
		Electrical installation	Electrical supply, sensor, control of machinery	Automation control system (IEC 62443-1-1) a
Equipment designer ^b	Define products, systems or services security objectives, intended use & instructions	Original manufacturer	Component supplier	Product supplier
Contractor/integrator	Apply system design & service instructions of the product documentation	Electrical contractor and large panel builder	Integrator (OEM)	Integration service provider
Maintenance and repair	Apply commissioning & update instructions of the product documentation	Electrical installer and small panel builder	Maintenance (OEM or MRO or end-user)	Maintenance service provider
End-user	Apply operating instructions of the product documentation	Facility manager	Operator	Asset owner
a Not covered by this document (for mapping only).				
b Includes the designer of component, combination of components and assemblies.				

NOTE In building electrical installation, the asset owner of the installation or equipment is not operating, maintaining, and upgrading it. These responsibilities are managed generally by the end user following the terms of a facility contract.

6.6 Important data

Special care should be taken to protect the important data. The important data for the integrity and the availability of the main functions of the equipment are the following:

- operating data related to hazardous operation (electrical interlocking, motor starting, reclosing, etc);
- equipment configuration data, including:
 - circuit-breaker overcurrent protection settings (equipment ratings, number of poles, etc);
 - proximity switch settings (sensing range, normally open or normally close output position, etc).

Other data related to the security related main functions of the equipment may also be identified.

6.7 Control system architecture

6.7.1 Control system

Typically, low voltage switchgear and controlgear are installed within assemblies. When needed, communication interfaces are implemented (e.g. gateway) to give remote access for monitoring and control. This can be called a control system.

The attack surface of an attack to a control system is largely a function of its architecture. To assess the architecture-related risks, its level of functionality and its external connectivity should be evaluated.

6.7.2 Levels of communication functionalities

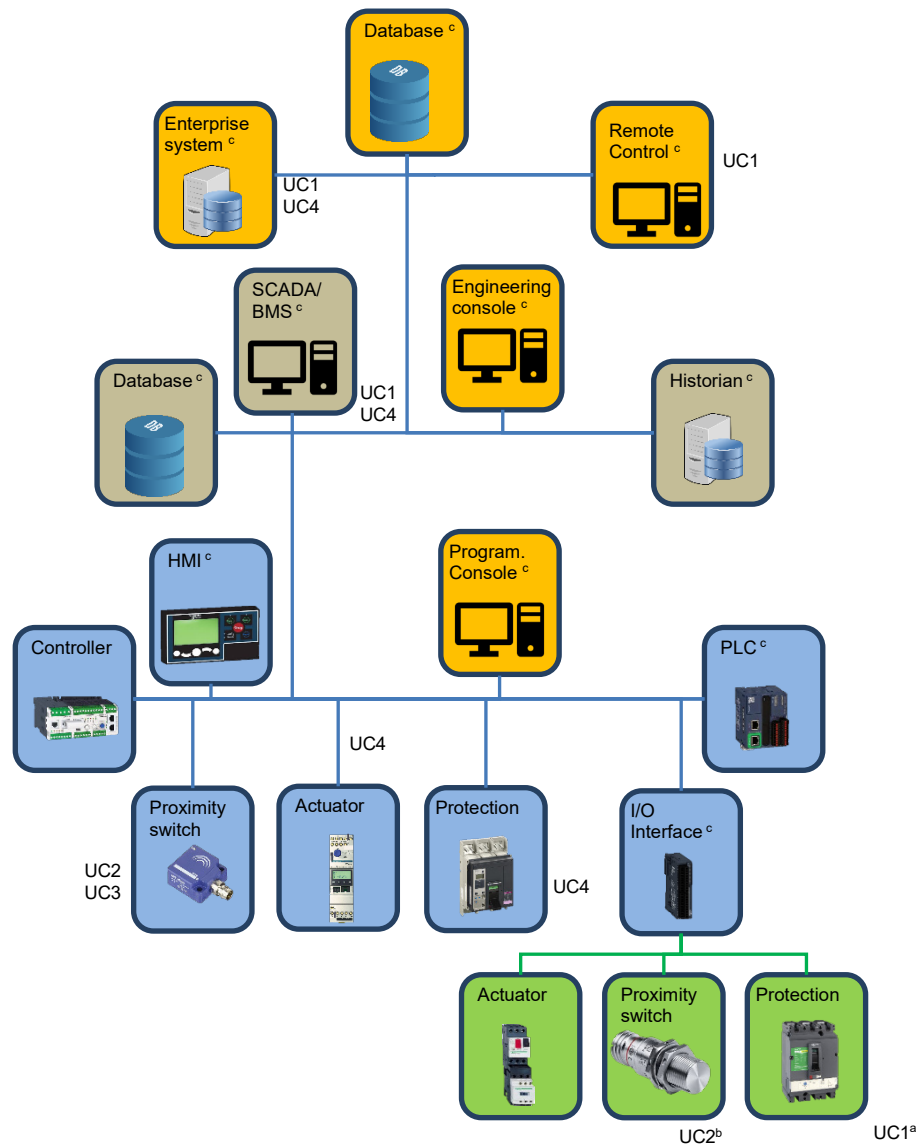
The level of communication functionalities (CF) or the range of communication capabilities of the control system can be classified into three levels:

- CF1: minimal systems including switchgear & controlgear devices, programmable logics, HMIs and actuators excluding software programming consoles. Point to point communication links may be considered as "CF1-" with limited functionality such as serial communication line and limited zone such as within a machine or within switchgear and controlgear assembly;
- CF2: complex systems with supervisory control and data acquisition (SCADA) or building management systems (BMS), including databases but excluding programming consoles and engineering workstations;
EXAMPLE: A protection equipment associated with an edge communication interface providing monitoring information accessible by a SCADA is CF2.
- CF3: very complex system with permanently-connected programming consoles or engineering workstations and other enterprise systems with distant remote control automation systems.

Distributed control systems with or without process engineering console are considered as CF3.

NOTE Special attention is on programming consoles and engineering stations, which provide significant additional tools to an attacker (threat actor). Their permanent presence in the control system is sufficient to justify a maximum level. This classification is derived from ANSSI Classification method and key measures, the French Network and Security Agency.

566 Figure 4 illustrate these levels of functionality in a control system architecture.



Key

UC use case number from Annex B

^a local console communication port access

^b local HMI access

^c equipment outside the scope of this document

— communication links (wired or wireless)

— control wires

■ non-communicating devices

■ CF1

■ CF2

■ CF3

567

Figure 4 – Control system architecture with switchgear and controlgear

6.7.3 Levels of connectivity

The connectivity (Cx) of a control system can be classified by the following categories:

- C1: isolated. The whole control system in Figure 5 network is completely closed.

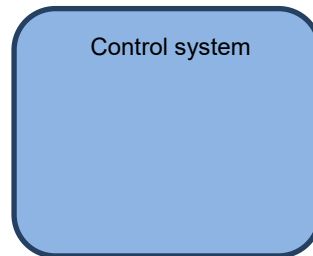


Figure 5 – Control system connectivity level C1

- C2: The control system is connected to the information system of the enterprise as illustrated in Figure 6 but without permitting operations from outside this information system. The information system can be connected to a public network such as the Internet or even distributed across multiple sites.

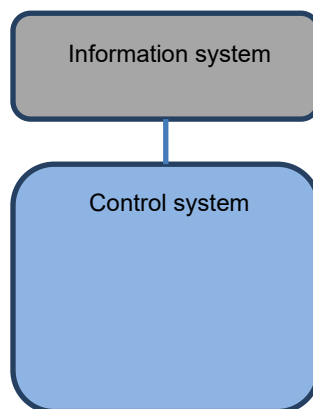


Figure 6 – Control system connectivity level C2

- C3: connectivity C2 using wireless communication as depicted in Figure 7. The wireless access gives more vulnerabilities to attacks.

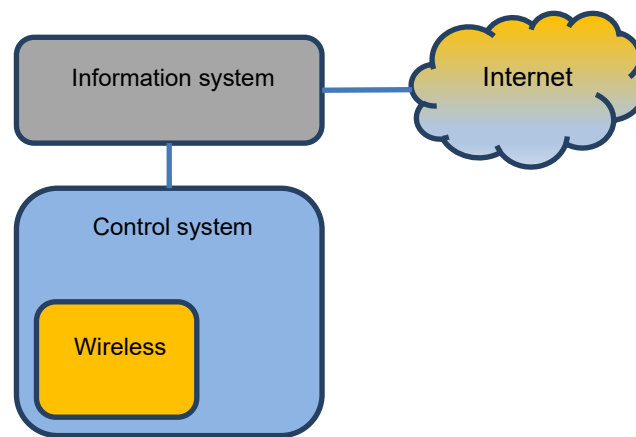


Figure 7 – Control system connectivity level C3

- C4: distributed control system permitting operations from outside as depicted in Figure 8. Different sites communicate with each other via a private infrastructure. This may be completely private or leased from a telecommunications operator. This category also includes control systems that permit operations from outside the site or from a management network (e.g. remote maintenance, remote management).

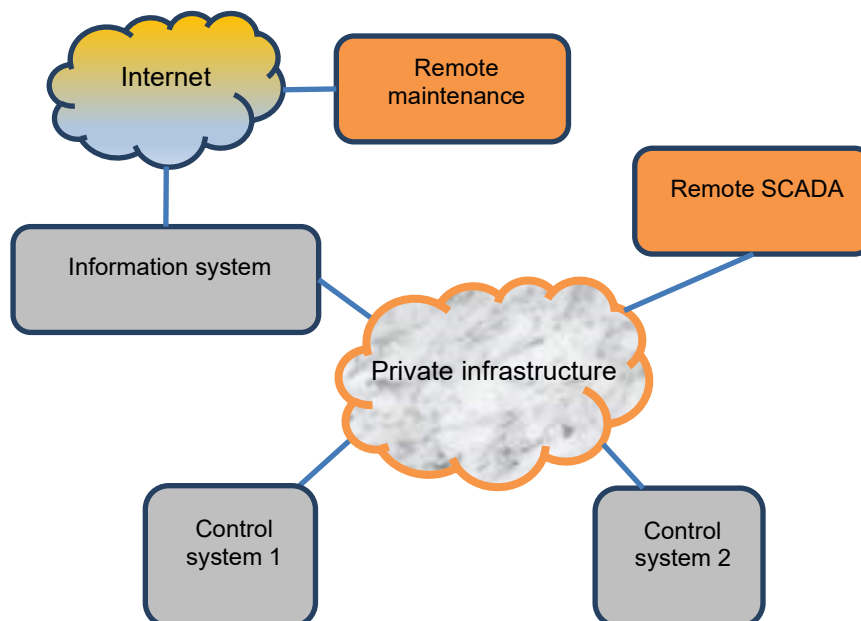


Figure 8 – Control system connectivity level C4

- C5: distributed control system with public infrastructure (Internet) as depicted in Figure 9. An attacker (threat actor) can easily reach various access points of the control system. Therefore, additional countermeasures are required. Moreover, no resources are dedicated to the control system, which can become a "collateral victim" of abnormally high network utilization.

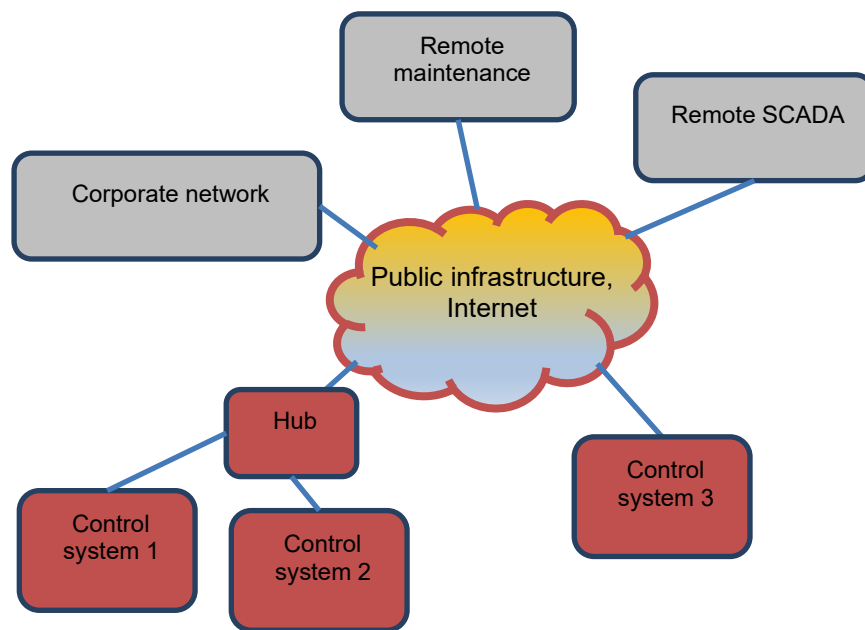


Figure 9 – Control system connectivity level C5

Infrastructure such as private access point name (APN) or virtual private network (VPN) of type multiprotocol label switching (MLP) falls into this category.

In this category, new potential vulnerabilities related to the presence of an infrastructure are very difficult – or even impossible – to monitor and control in their entirety, in particular from the perspective of physical access. All vulnerabilities related to remote maintenance are also present.

NOTE This classification is derived from ANSSI Classification method and key measures.

6.7.4 Exposure levels of equipment

The exposure of equipment included in the control system is a combination of its levels of communication functionality and connectivity. Table 5 gives a level of exposure from E1 (least exposed) to E5 (most exposed). This indicates the amount of risk that can be introduced into the control system. A higher risk will require a more extensive risk assessment.

Table 5 – Level of exposure of an equipment

Functionality/Connectivity	C1	C2	C3	C4	C5
CF3	E3	E3	E4	E4	E5
CF2	E2	E2	E3	E4	E5
CF1	E1	E2	E3	E4	E5
E1 least exposed E5 most exposed					

NOTE This classification is derived from ANSSI Classification method and key measures.

The levels of functionality and connectivity do not vary independently. Therefore, some cells may not correspond to any real system. Other factors can influence the levels, including the number of devices involved, and the heterogeneity of the devices used. Those factors should be considered in the risk assessment.

Non-communicating devices illustrated in green in Figure 4 are not considered in the levels of exposure; but shall be covered in the whole risk assessment when they include embedded software.

The level of exposure is used for evaluating the severity of the exposure of the equipment to attacks in order to select the appropriate countermeasure. See Annex B.

6.7.5 Equipment security levels

The technical function of the building or of the machinery in which the equipment is included should have a target security level defined by the system integrator, the machine builder, or the facility manager of a building. The equipment used as a part or as the complete technical function shall provide the capability to meet the target level. The equipment security level does not include any additional compensating countermeasure.

NOTE: IEC TS 62443-1-1 defines the target, achieved and capability security levels and IEC 62443-2-1 provides additional information.

The equipment security level in Table 6 can be determined by combining the level of impact and the level of exposure resulting in the level of potential attack defined in Table 1.

Table 6 – Equipment security level

Impact ^a	Exposure ^b				
	E1	E2	E3	E4	E5
Critical	Basic	Substantial	Substantial	High	High
Moderate	Basic	Basic	Substantial	Substantial	High
minor	Basic	Basic	Basic	Substantial	Substantial
a See Table 3					
b See Table 5					

6.7.6 Security protection profile

A security protection profile provides a generic set of assurance security requirements applicable to an equipment category while considering the context of the operational environment and the risk factors.

It is a step towards an effective way of dealing with security risk analysis and security targets. It helps to scale security controls and security-related process activities in accordance to the identified risks, i.e. to spend most effort where the highest risks are.

Ultimately, it defines a harmonised conformity assessment methodology for the evaluating of the security of an equipment.

The structure of the security profile given in Figure 10 is following Annex B of ISO/IEC 15408-1:2022.

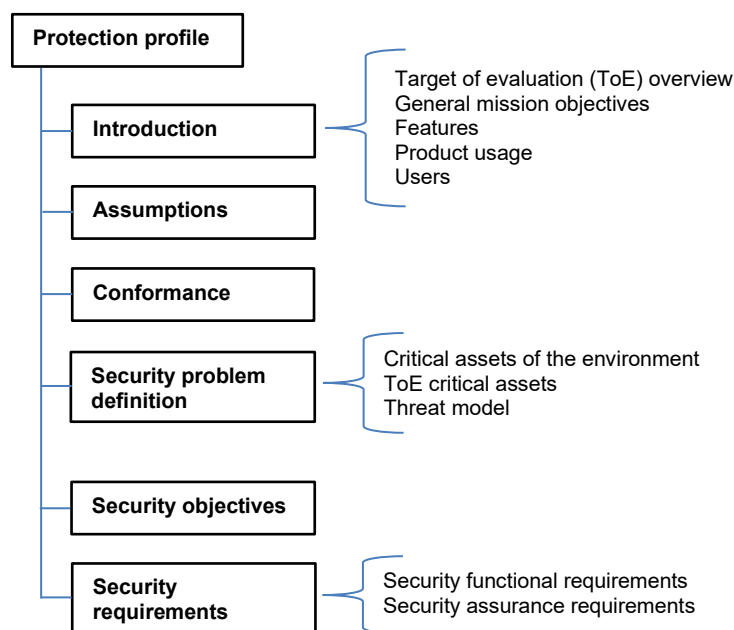


Figure 10 – Structure of a security protection profile

Security protection profiles for switchgear and controlgear are given in Annex E to Annex I and can be given in annex to the product standard.

7 Security requirements

7.1 General

The following requirements are based on the typical use cases of Annex B.

Following the approach of Clause 6, the designer of the equipment shall implement the relevant security countermeasures given in the following subclauses. Cybersecurity protection profiles specifying generic security evaluation criteria for several equipment categories are provided in Annex E to Annex I.

7.2 Physical access and environment

7.2.1 PA – Physical access and environment requirement

PA-1 – Operating, functional setting and resetting means of the main functions shall be easily accessible. Specific accessibility requirements are defined by the relevant product standard.

PA-2 – Appropriate user instructions shall be given for addressing the following requirements:

- Installation rules: According to IEC 60364-7-729, restricted access areas with switchgear and controlgear assemblies shall not provide access to unauthorized persons.
- Electrical circuits and equipment for critical operations power systems shall be accessible to qualified personnel only.

The verification of this requirement shall be performed according to 9.3.1.

7.2.2 Physical access and environment rational

Physical security measures are generally defined at the building facility level for managing its access and to reduce the risk of accidental or deliberate damage or loss of the building assets and intellectual property. These measures are often associated with other risks such as safety, environmental, regulatory, etc. The main operations of an equipment are defined by their relevant product standard. They are generally readily accessible to an authorised person, i.e. without additional access logging operation on the equipment.

Providing physical security for the electrical room of a building or the control panel of a machine is essential to reduce the potential of many threats. These locations often contain essential electrical power control of the building and safety related control system of machinery. It is essential that access to these areas be limited to authorized users only.

Table°7 provides references from the relevant security standards corresponding to the requirements of subclause 7.2.1.

Table°7 – Physical access related requirement references

Requirement ID	Source	Source requirement reference
PA-1	IEC 62443-4-2:2019	CCSC 1 – Support of essential functions

Table°8 provides references to possible security enhancements from the relevant security standards corresponding to the recommendations of subclause 7.2.3.

Table°8 – Physical access enhancement related requirement references

Requirement ID	Source	Source requirement reference
PA-e1.1PA-e1.2 PA-e1.4, PA-e2.1, PA-e2.2 and PA-e2.3	ISO/IEC 27001:2013	A.11 – Physical and environmental security (adapted) See Table K.2

7.2.3 PA-e – Physical access and environment enhancement

According to A.11 of ISO/IEC 27001:2013, several requirements are derived to premises where low voltage switchgear and controlgear assemblies are installed. Appropriate user instructions should be given for addressing the following requirements in a) and b).).

a) PA-e1 – For secured areas in order to prevent unauthorized physical access, damage and interference to the security related main functions of the equipment:

- 1) PA-e1.1 – Physical security perimeters should be defined and used to protect areas that contain equipment supporting security related main functions.
- 2) PA-e1.2 – Physical entry controls: access control should be defined and implemented to authorized persons for entering premises where the equipment is accessible such as electrical restricted access areas.
- 3) PA-e1.3 – Detective and reactive physical security monitoring: security means should be deployed to monitor premises security. For example, CCTV should be used to view and record access to sensitive areas within an organization's premises, guards should be deployed to detect intruder access to an organization's premises, or burglar alarms and other devices should be used to detect the presence of intruders within an organization's premises.
- 4) PA-e1.4 – Protecting against external and environmental attacks: physical protection against natural disasters, physical attack or accidents should be considered, and if appropriate should be designed and implemented.

b) PA-e2 – For equipment in order to prevent loss, damage, theft or corruption of equipment and interruption to the organization's operations:

1) PA-e2.1 – Equipment siting and protection: facilities should be secured to avoid unauthorized access. Controls should be adopted to minimize the risk of potential physical and environmental threats, for example theft, fire, explosives, smoke, water (or water supply failure), dust, vibration, chemical effects, higher EMC disturbance levels than the generic levels given for the relevant EMC environment and vandalism.

2) PA-e2.2 – Cabling security: power and telecommunications cabling carrying data or supporting information services should be protected from interception, interference or damage.

PA-e2.3 – Equipment maintenance: equipment should be correctly maintained to ensure its continued availability and integrity. For example, firmware should be updated according to the product documentation.

The verification of this requirement shall be performed according to 9.3.2.

7.2.4 Physical access and environment typical implementation

Typical measures for managing the physical access to the equipment are locked doors of technical rooms and individual distribution and control switchboards, sealed panels, alarm systems and video monitoring.

Accessibility to assemblies for operating and servicing conditions by ordinary persons and authorized persons are defined in 8.4.6 of IEC 61439-1:2020.

NOTE In North America, requirement for physical security of critical operations power systems are given in Clause 708.5 of NFPA 730, Guide for Premises Security.

Accessibility related to safety of machinery are defined by IEC 60204-1:2016, especially in clauses:

- 5.3.4 for the operating means of the supply disconnecting device,
- 5.4 for the devices for removal of power for prevention of unexpected start-up,
- 5.5 for devices for isolating electrical equipment,
- 5.6 for protection against unauthorized, inadvertent and/or mistaken connection.
- 9.2.3.5 for operating modes
- 9.2.4.5 for portable cableless operator control stations,
- 9.4.1 for the control functions in the event of failure
- 10 for operator interface and machine-mounted control devices
- 11 for location, mounting, and enclosures of controlgear

Additional requirements for equipment suitable for isolation are given in 8.1.7 of IEC 60947-1:2020.

7.3 Equipment requirement

7.3.1 General

7.3.1.1 Main functions

Security countermeasures shall not prevent, delay or in general affect the local setting, operation and alarming of the main functions of the equipment. Following 4.2 of IEC 62443-3, the essential functions in this document are the following functions, but not limited to:

- Overcurrent protections (short-circuit and overload) of the controlled circuit or load;

- Residual current protection of the electrical installation;
- Disconnecter (providing isolation) of an electric circuit including its padlocking;
- Making and breaking capability of the controlled circuit or load either by a manual operating means or by a remotely operated switching device;
- Ensuring continuity of energy supply by transferring a load between sources;
- Controlled acceleration and deceleration of a motor load or ramp up and ramp down of a non-motor load and inrush limit function;
- Operating a switching function when exceeding a rated operating temperature value converted from the PTC thermistor incorporated in rotating electrical machines and to reset the switching function below the reset temperature;
- Detecting internal arc-fault current protecting assemblies by processing light-effects;
- Quenching an internal arc-fault current, to limit the voltage drop in low-impedance state and be able to be reset;
- Switching a signal when mechanically actuated;
- Switching a signal or modulate the voltage or the current when detecting an object at specified distance in front of the electronic sensing element of the equipment;
- Emitting a light or sound signal when powered.

Installation rules given by IEC 60364 series and safety of machinery given by IEC 60204-1 require easy access to local operating means such as pushbutton, handle, etc. Local setting of the protection level (rotary wheel, dip switch, etc.) can be required to be adjusted quickly such as the overload protection in case of a tight current setting for protecting a critical load.

NOTE 1 When a security mechanism is used for managing the access to a safety function, only this security mechanism is covered by this document.

7.3.1.2 Compensating countermeasure

The principle of compensating countermeasure is defined by IEC TS 62443-1-1 and used by IEC 62443-3-3 for control systems. It is extended in this document to all equipment (overcurrent protections, actuators, sensors, assemblies, etc.).

The final implementation of the security protection embedded in the equipment as a compensating countermeasure shall be described in the target of evaluation as defined in Annex E to Annex I.

7.3.1.3 Security requirements for the equipment

The generic security requirements applicable to an equipment are classified following the seven foundational requirements (FRs) defined by IEC TS 62443-1-1 and are using the codification of IEC 62443-4-2 component requirement (CR x.x). Each requirement (CR x.x) includes subclauses for a base requirement and a possible requirement enhancement for reinforced security control.

NOTE IEC 62443 differentiate the security requirements for the control system (SRs) and for its components (CRs) as a combination of software applications running on host devices (workstation), embedded devices (programmable logic controller) and network devices (switch, router, firewall). Technically, the CRs requirements are referring to the SRs using the same numbering and are very similar.

The equipment shall either follow:

- the generic list of requirements of 7.3.2 to 7.3.8 as far as applicable or
- a security protection profile defined in Annex E to Annex I.

7.3.2 FR 1 – Identification and authentication control**7.3.2.1 Purpose**

Subclause 5.1 SL 1 and SL 2 of IEC 62443-4-2:2019 applies.

7.3.2.2 Rationale

Subclause 5.2 of IEC 62443-4-2:2019 applies to the equipment without the second paragraph which is not feasible with switchgear and controlgear generally not supporting centralised identification and authentication mechanism.

Examples to preventing unauthorized access and modification are:

- human user identification and authentication;
- authentication for networks;
- wireless access management;
- strength of password-based authentication;
- password generation and lifetime restrictions for human users.

7.3.2.3 CR 1.1 – Human user identification and authentication**7.3.2.3.1 Applicability**

This requirement is applicable when

- the equipment is intended to be connected to a network with an exposure greater than E1 or
- the equipment provides human user interface with the capability of modification of the security related parameters of the equipment.

The local user interface to the main functions as given in 7.3.1.1 does not require access control.

The requirement of 7.3.2.3.4 is applicable when the equipment is intended to be connected to a network with an exposure greater than E3.

7.3.2.3.2 Requirement

The requirement CR 1.1 given in 5.3.1 of IEC 62443-4-2:2019 applies when applicable as specified in 7.3.2.3.1.

The verification of this requirement shall be performed according to 9.4.1.1.

7.3.2.3.3 Requirement rational

See 5.3.2 of IEC 62443-4-2:2019 and the following addition.

Role based access control (RBAC) techniques should be used to implement authentication and authorization mechanisms. Authentication of users could be achieved for example using passwords, smartcards, biometric data, etc.

7.3.2.3.4 CR 1.1 e.1 – Unique identification and authentication

The requirement CR 1.1 RE (1) given in 5.3.3 of IEC 62443-4-2:2019 applies to the equipment when applicable as specified in 7.3.2.3.1.