



DPC: 24 / 30484649 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: 10 January 2024

Origin: International

Latest date for receipt of comments: 28 February 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 28 February 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

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.	



121/156/CD

COMMITTEE DRAFT (CD)

PROJECT NUMBER:

IEC 63208 ED1

DATE OF CIRCULATION:

2024-01-05

CLOSING DATE FOR COMMENTS:

2024-03-29

SUPERSEDES DOCUMENTS:

121/155/RR

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:

TC121 Officers support circulation of CD1 for project IEC 63208 ED1

Secretary Note: NC experts are kindly requested to refer their comments to line number.

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.

49	7.3.2.6	CR 1.7 – Strength of password-based authentication	37
50	7.3.2.7	CR 1.8 – Public key infrastructure certificates	38
51	7.3.2.8	CR 1.9 – Strength of public key-based authentication	38
52	7.3.2.9	CR 1.10 – Authenticator feedback	38
53	7.3.2.10	CR 1.11 – Unsuccessful login attempts	38
54	7.3.2.11	CR 1.14 – Strength of symmetric key-based authentication	39
55	7.3.3	FR 2 – Use control	39
56	7.3.3.1	Purpose	39
57	7.3.3.2	Rationale	39
58	7.3.3.3	CR 2.1 – Authorization enforcement	39
59	7.3.3.4	CR 2.2 – Wireless use control	39
60	7.3.3.5	EDR 2.4 – Mobile code	40
61	7.3.3.6	SAR 2.4 – Mobile code	40
62	7.3.3.7	CR 2.5 – Session lock	41
63	7.3.3.8	CR 2.6 – Remote session termination	41
64	7.3.3.9	CR 2.7 – Concurrent session control	41
65	7.3.3.10	CR 2.8 – Auditable events	41
66	7.3.3.11	CR 2.9 – Audit storage capacity	42
67	7.3.3.12	CR 2.10 – Response to audit processing failures	42
68	7.3.3.13	CR 2.11 Timestamp	42
69	7.3.3.14	CR 2.12 – Non-repudiation	43
70	7.3.3.15	EDR 2.13 – Use of physical diagnostic and test interfaces	43
71	7.3.4	FR 3 – System integrity	43
72	7.3.4.1	Purpose	43
73	7.3.4.2	Rationale	43
74	7.3.4.3	CR 3.1 – Communication integrity	43
75	7.3.4.4	EDR 3.2 – Protection from malicious code	44
76	7.3.4.5	SAR 3.2 – Protection from malicious code	45
77	7.3.4.6	CR 3.3 – Security functionality verification	45
78	7.3.4.7	CR 3.4 – Software and information integrity	45
79	7.3.4.8	CR 3.5 – Input validation	46
80	7.3.4.9	CR 3.6 – Deterministic output	46
81	7.3.4.10	CR 3.7 – Error handling	47
82	7.3.4.11	CR 3.8 – Session Integrity	47
83	7.3.4.12	CR 3.9 – Protection of audit information	47
84	7.3.4.13	EDR 3.10 – Support for Updates	47
85	7.3.4.14	EDR 3.11 – Physical tamper resistance and detection	48
86	7.3.4.15	EDR 3.12 – Provisioning product supplier roots of trust	48
87	7.3.4.16	EDR 3.13 – Provisioning asset owner roots of trust	48
88	7.3.4.17	EDR 3.14 – Integrity of the boot process	49
89	7.3.5	FR 4 – Data confidentiality	49
90	7.3.5.1	Purpose	49
91	7.3.5.2	Rationale	49
92	7.3.5.3	CR 4.3 – Use of cryptography	49
93	7.3.6	FR 5 – Restricted data flow	49
94	7.3.7	FR 6 – Timely response to events	50
95	7.3.7.1	Purpose	50
96	7.3.7.2	Rationale	50
97	7.3.7.3	CR 6.1 – Audit log accessibility	50
98	7.3.8	FR 7 – Resource availability	50

99	7.3.8.1	Purpose.....	50
100	7.3.8.2	Rationale.....	50
101	7.3.8.3	CR 7.1 – Denial of service protection	50
102	7.3.8.4	CR 7.2 – Resource management.....	51
103	7.3.8.5	CR 7.3 – Control system backup	51
104	7.3.8.6	CR 7.4 – Control system recovery and reconstitution	52
105	7.3.8.7	CR 7.6 – Network and security configuration settings	52
106	7.3.8.8	CR 7.7 – Least functionality	52
107	7.3.8.9	CR 7.8 – Control system inventory	53
108	8	Instructions for installation, operation and maintenance	53
109	8.1	User instruction requirement.....	53
110	8.2	User instruction rational	54
111	8.3	User instruction enhancement	54
112	8.4	User instruction implementation.....	54
113	9	Conformance verification and testing.....	54
114	9.1	General.....	54
115	9.2	Life cycle management.....	54
116	9.3	Physical access	54
117	9.3.1	Verification of physical access and environment	54
118	9.3.2	Physical access and environment enhancement	55
119	9.4	FR 1 – Identification and authentication control.....	55
120	9.4.1	CR 1.1 – Human user identification and authentication	55
121	9.4.1.1	Requirement verification	55
122	9.4.1.2	Requirement enhancement verification	55
123	9.4.2	CR 1.2 – Software and equipment identification and authentication	55
124	9.4.2.1	Requirement verification	55
125	9.4.2.2	Requirement enhancement verification	56
126	9.4.3	CR 1.5 – Authenticator management	56
127	9.4.3.1	Requirement verification	56
128	9.4.4	CR 1.7 – Strength of password-based authentication	56
129	9.4.4.1	Requirement verification	56
130	9.4.5	CR 1.8 – Public key infrastructure certificates	56
131	9.4.5.1	Requirement verification	56
132	9.4.6	CR 1.9 – Strength of public key-based authentication	57
133	9.4.6.1	Requirement verification	57
134	9.4.7	CR 1.10 – Authenticator feedback	57
135	9.4.7.1	Requirement verification	57
136	9.4.8	CR 1.11 – Unsuccessful login attempts.....	57
137	9.4.8.1	Requirement verification	57
138	9.4.9	CR 1.14 – Strength of symmetric key-based authentication	57
139	9.4.9.1	Requirement verification	57
140	9.5	FR 2 – Use control	58
141	9.5.1	CR 2.1 – Authorization enforcement	58
142	9.5.1.1	Requirement verification	58
143	9.5.1.2	Requirement enhancement verification	58
144	9.5.2	CR 2.2 – Wireless use control	58
145	9.5.2.1	Requirement verification	58
146	9.5.3	EDR 2.4 – Mobile code.....	58
147	9.5.3.1	Requirement verification	58
148	9.5.3.2	Requirement enhancement verification.....	59

149	9.5.4	SAR 2.4 – Mobile code.....	59
150	9.5.4.1	Requirement verification	59
151	9.5.4.2	Requirement enhancement verification	59
152	9.5.5	CR 2.5 – Session lock	59
153	9.5.5.1	Requirement verification	59
154	9.5.6	CR 2.6 – Remote session termination	59
155	9.5.6.1	Requirement verification	59
156	9.5.7	CR 2.7 – Concurrent session control	60
157	9.5.7.1	Requirement verification	60
158	9.5.8	CR 2.8 – Auditable events	60
159	9.5.8.1	Requirement verification	60
160	9.5.9	CR 2.9 – Audit storage capacity	60
161	9.5.9.1	Requirement verification	60
162	9.5.10	CR 2.10 – Response to audit processing failures	60
163	9.5.10.1	Requirement verification	60
164	9.5.11	CR 2.11 – Timestamps	61
165	9.5.11.1	Requirement verification	61
166	9.5.11.2	Requirement enhancement verification	61
167	9.5.12	CR 2.12 – Non-repudiation	61
168	9.5.12.1	Requirement verification	61
169	9.5.13	EDR 2.13 – Use of physical diagnostic and test interfaces	61
170	9.5.13.1	Requirement verification	61
171	9.6	FR 3 – System integrity	61
172	9.6.1	CR 3.1 – Communication integrity	61
173	9.6.1.1	Requirement verification	61
174	9.6.1.2	Requirement enhancement verification	62
175	9.6.2	EDR 3.2 – Protection from malicious code	62
176	9.6.2.1	Requirement verification	62
177	9.6.3	SAR 3.2 – Protection from malicious code	62
178	9.6.3.1	Requirement verification	62
179	9.6.4	CR 3.3 – Security functionality verification	62
180	9.6.4.1	Requirement verification	62
181	9.6.4.2	Requirement enhancement verification	63
182	9.6.5	CR 3.4 – Software and information integrity	63
183	9.6.5.1	Requirement verification	63
184	9.6.5.2	Requirement enhancement verification	63
185	9.6.6	CR 3.5 – Input validation	63
186	9.6.6.1	Requirement verification	63
187	9.6.7	CR 3.6 – Deterministic output	63
188	9.6.7.1	Requirement verification	63
189	9.6.8	CR 3.7 – Error handling.....	64
190	9.6.8.1	Requirement verification	64
191	9.6.9	CR 3.8 – Session Integrity.....	64
192	9.6.9.1	Requirement verification	64
193	9.6.10	CR 3.9 – Protection of audit information	64
194	9.6.10.1	Requirement verification	64
195	9.6.11	EDR 3.10 – Support for updates	64
196	9.6.11.1	Requirement verification	64
197	9.6.11.2	Requirement enhancement verification	65
198	9.6.12	EDR 3.11 – Physical tamper resistance and detection.....	65

199		9.6.12.1 Requirement verification	65
200	9.6.13	EDR 3.12 – Provisioning product supplier roots of trust	65
201		9.6.13.1 Requirement verification	65
202	9.6.14	EDR 3.13 – Provisioning asset owner roots of trust	65
203		9.6.14.1 Requirement verification	65
204	9.6.15	EDR 3.14 – Integrity of the boot process	66
205		9.6.15.1 Requirement verification	66
206		9.6.15.2 Requirement enhancement verification	66
207	9.7	FR 4 – Data confidentiality	66
208	9.7.1	CR 4.3 – Use of cryptography	66
209		9.7.1.1 Requirement verification	66
210	9.8	FR 6 – Timely response to events	66
211	9.8.1	CR 6.1 – Audit log accessibility	66
212		9.8.1.1 Requirement verification	66
213		9.8.1.2 Requirement enhancement verification	67
214	9.9	FR 7 – Resource availability	67
215	9.9.1	CR 7.1 – Denial of service protection	67
216		9.9.1.1 Requirement verification	67
217		9.9.1.2 Requirement enhancement verification	67
218	9.9.2	CR 7.2 – Resource management	67
219		9.9.2.1 Requirement verification	67
220	9.9.3	CR 7.3 – Control system backup	67
221		9.9.3.1 Requirement verification	67
222		9.9.3.2 Requirement enhancement verification	68
223	9.9.4	CR 7.4 – Control system recovery and reconstitution	68
224		9.9.4.1 Requirement verification	68
225	9.9.5	CR 7.6 – Network and security configuration settings	68
226		9.9.5.1 Requirement verification	68
227	9.9.6	CR 7.7 – Least functionality	68
228		9.9.6.1 Requirement verification	68
229	9.9.7	CR 7.8 – Control system inventory	68
230		9.9.7.1 Requirement verification	68
231	Annex A (informative)	Cybersecurity and electrical system architecture	70
232	A.1	General	70
233	A.2	Typical architecture involving switchgear and controlgear and their assembly	70
234	A.2.1	Building	70
235	A.2.2	Manufacturing	71
236	Annex B (informative)	Use case studies	73
237	B.1	General	73
238	B.2	Use case 1 – Protection against Denial of Service (DoS) attack	74
239	B.3	Use case 2 – Protection against unauthorized modification of sensing device	75
240	B.4	Use case 3 – Protection against unauthorized modification of wireless	
241		equipment	76
242	B.5	Use case 4 – Protection against threat actor remotely taking control of a	
243		“Managing” intelligent assembly	77
244	Annex C (Informative)	Development methods of cybersecurity aspects	79
245	Annex D (informative)	Instructions to be provided to the user of the equipment and for	
246		integration into an assembly	80
247	D.1	General	80
248	D.2	Risk assessment and security planning	80
249	D.2.1	Risk assessment	80

250	D.2.2	Security plan.....	80
251	D.3	Recommendations for design and installation of the system integrating	
252		switchgear and controlgear and their assemblies	81
253	D.3.1	General access control.....	81
254	D.3.2	Recommendations for local access	81
255	D.3.3	Recommendations for remote access	82
256	D.3.4	Recommendations for firmware upgrades	82
257	D.3.5	Recommendations for the end of life.....	83
258	D.4	Instructions for an assembly	83
259	Annex E (normative)	Security protection profile of soft-starter, motor starter and	
260		semiconductor controller	84
261	E.1	Introduction.....	84
262	E.1.1	Protection profile reference	84
263	E.1.2	Target of evaluation overview.....	84
264	E.1.3	General mission objectives.....	84
265	E.1.4	Features	85
266	E.1.5	Product usage.....	85
267	E.1.6	Users.....	85
268	E.2	Assumptions	86
269	E.3	Conformance claims and conformance statement.....	86
270	E.4	Security problem definition	86
271	E.4.1	Critical assets of the environment.....	86
272	E.4.2	ToE critical assets.....	87
273	E.4.3	Threat Model	87
274		E.4.3.1 Attackers	87
275		E.4.3.2 Threats.....	87
276	E.5	Security objectives	88
277	E.6	Security requirements	88
278	E.6.1	Security functional requirements.....	88
279	E.6.2	Security assurance requirements.....	88
280	Annex F (normative)	Security protection profiles of circuit-breaker	90
281	F.1	Introduction.....	90
282	F.1.1	Protection profile reference	90
283	F.1.2	Target of evaluation overview.....	90
284	F.1.3	General mission objectives.....	90
285	F.1.4	Features	91
286	F.1.5	Product usage.....	91
287	F.1.6	Users.....	91
288	F.2	Assumptions	91
289	F.3	Conformance claims and conformance statement.....	92
290	F.4	Security problem definition	92
291	F.4.1	Critical assets of the environment.....	92
292	F.4.2	ToE critical assets.....	92
293	F.4.3	Threat Model	93
294		F.4.3.1 Attackers	93
295		F.4.3.2 Threats.....	93
296	F.5	Security objectives	94
297	F.6	Security requirements	94
298	F.6.1	Security functional requirements.....	94
299	F.6.2	Security assurance requirements.....	94
300	Annex G (normative)	Protection profile of transfer switch equipment	95

301	G.1	Introduction	95
302	G.1.1	Protection profile reference	95
303	G.1.2	Target of evaluation overview	95
304	G.1.2.1	Overview	95
305	G.1.3	General mission objectives	96
306	G.1.4	Features	96
307	G.1.5	Product usage	96
308	G.1.6	Users	96
309	G.2	Assumptions	96
310	G.3	Conformance claims and conformance statement	96
311	G.4	Security problem definition	97
312	G.4.1	Critical assets of the environment	97
313	G.4.2	ToE critical assets	97
314	G.4.3	Threat Model	98
315	G.4.3.1	Attackers	98
316	G.4.3.2	Threats	98
317	G.5	Security objectives	98
318	G.6	Security requirements	98
319	G.6.1	Security functional requirements	98
320	G.6.2	Security assurance requirements	99
321	Annex H (normative) Protection profile for wireless controlgear with its communication interface		100
322			
323	H.1	Introduction	100
324	H.1.1	Protection profile reference	100
325	H.1.2	Target of evaluation overview	100
326	H.1.3	General mission objectives	101
327	H.1.4	Features	101
328	H.1.5	Product usage	101
329	H.1.6	Users	101
330	H.2	Assumptions	101
331	H.3	Conformance claims and conformance statement	102
332	H.4	Security problem definition	102
333	H.4.1	Critical assets of the environment	102
334	H.4.2	ToE critical assets	102
335	H.4.3	Threat Model	103
336	H.4.3.1	Attackers	103
337	H.4.3.2	Threats	103
338	H.5	Security objectives	104
339	H.6	Security requirements	104
340	H.6.1	Security functional requirements	104
341	H.6.2	Security assurance requirements	104
342	Annex I (informative) Equipment requirements by level of exposure		105
343	Annex J (informative) Bridging references to cybersecurity management systems		106
344	Bibliography		112
345			
346	Figure 1 – Standard landscape		12
347	Figure 2 – Example of physical interfaces of an embedded device in an equipment which can be subject to an attack		23
348			
349	Figure 3 – Example of relation between security and safety		24
350	Figure 4 – Control system architecture with switchgear and controlgear		28

351	Figure 5 – Control system connectivity level C3	29
352	Figure 6 – Control system connectivity level C4	30
353	Figure 7 – Control system connectivity level C5	30
354	Figure 8 – Structure of a security protection profile	32
355	Figure°9 – Example of security instruction symbol	54
356	Figure°A.1 – Building electrical architecture	71
357	Figure°A.2 – Industrial plants	72
358	Figure E.1 – Machinery control architecture	84
359	Figure F.1 – Circuit-breaker in its environment	90
360	Figure G.1 – Electrical distribution architecture	95
361	Figure H.1 – Machinery control architecture	100
362		
363	Table 1 – Potential attack levels	22
364	Table 2 – Typical threats	22
365	Table 3 – Impact evaluation	25
366	Table 4 – Roles related to security responsibilities	26
367	Table 5 – Level of exposure of an equipment	31
368	Table 6 – Equipment security level	31
369	Table°7 – Physical access related requirement references	33
370	Table°8 – Physical access enhancement related requirement references	33
371	Table B.1 – List of actors	73
372	Table B.2 – Base line requirement	73
373	Table B.3 – Security problems of use cases	74
374	Table E.1 – Security requirements for the critical assets of the environment	87
375	Table E.2 – Security requirements for the critical assets	87
376	Table E.3 – Security functional requirements	88
377	Table F.1 – Security requirements for the critical assets of the environment	92
378	Table F.2 – Security requirements for the critical assets	93
379	Table F.3 – Security functional requirements	94
380	Table G.1 – Security requirements for the critical assets of the environment	97
381	Table G.2 – Security requirements for the critical assets	97
382	Table G.3 – Security functional requirements	99
383	Table H.1 – Security requirements for the critical assets of the environment	102
384	Table H.2 – Security requirements for the critical assets	103
385	Table H.3 – Security functional requirements	104
386	Table I.1 – Equipment requirements by level of exposure	105
387	Table J.1 – Useful security standards	106
388	Table J.2 – Contribution of switchgear and controlgear and their assemblies to ISO	
389	and IEC horizontal security framework	107
390	Table J.3 – Mapping to other security framework	110
391	Table J.4 – Requirements for IACS not relevant for switchgear and controlgear and	
392	their assemblies	110
393	Table J.5 – Requirements for IoT device not relevant for switchgear and controlgear	
394	and their assemblies	111
395		

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
------------	-----------

448

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

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

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

- 455 • reconfirmed,
- 456 • withdrawn,
- 457 • replaced by a revised edition, or
- 458 • amended.

459

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

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

463

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.

464

465

466

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 protection 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 functionality of equipment, in all operating modes, as a consequence of the implementation of security countermeasures.

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

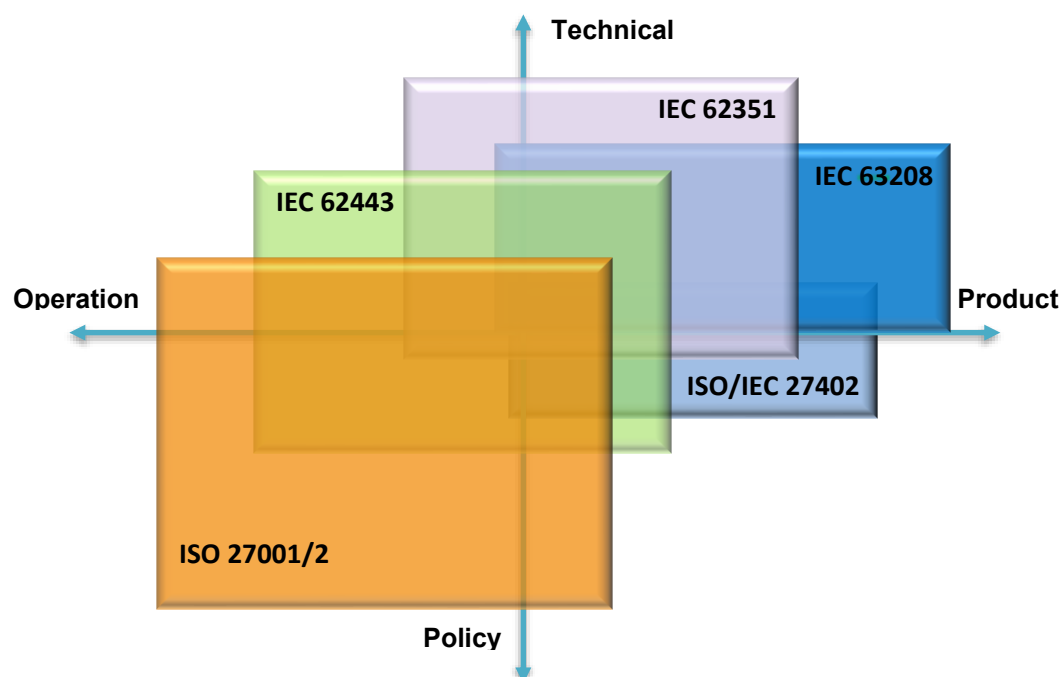


Figure 1 – Standard landscape

Figure 1 positions the 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 functionalities. 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 technics 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.

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 and during the whole lifecycle of the equipment. 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;
- 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 H).

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 safety related 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 J)

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
- data confidentiality other than for critical security parameters.

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

2 Normative references

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

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

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

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

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

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

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

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

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

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

3 Terms, definitions and abbreviated terms

3.1 Terms and definitions

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

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

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

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.

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

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

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

603 **3.1.2**

604 **attack**

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

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

608 **3.1.3**

609 **attack surface**

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

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

613 **3.1.4**

614 **attack vector**

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

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

618 **3.1.5**

619 **authentication**

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

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

622 **3.1.6**

623 **authenticator**

624 means used to confirm the identity of an entity

625 EXAMPLE A password or token may be used as an authenticator

626 **3.1.7**

627 **authenticity**

628 property that an entity is what it claims to be

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

630 **3.1.8**

631 **authorization**

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

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

635 **3.1.9**

636 **ordinary person**

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

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

639 **3.1.10**

640 **authorized person**

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

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

643 **3.1.11**

644 **availability**

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

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

647 **3.1.12**

648 **confidentiality**

649 property that information is not made available or disclosed to unauthorized individuals, entities
650 or processes

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

652 **3.1.13**

653 **countermeasure**

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

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

658 **3.1.14**

659 **critical security parameter**

660 **CSP**

661 security related information whose disclosure or modification can compromise the security of a
662 cryptographic module

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

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

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

667 **3.1.15**

668 **cybersecurity**

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

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

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

678 **3.1.16**

679 **data integrity**

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

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

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

3.1.17**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]

3.1.18**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.]

3.1.19**denial of service**

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

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

3.1.20**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]

3.1.21**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]

3.1.22**security related main function****essential 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 by the manufacturer

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 protection 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.

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

3.1.23**complementary function**

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

3.1.24**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]

3.1.25**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]

3.1.26**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]

3.1.27**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.]

3.1.28**protection profile**

PP

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

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

3.1.29**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.

3.1.30**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]

3.1.31**safety related function**

function of the equipment whose failure can result in an immediate increase of risk

Note 1 to entry: Typical immediate increase of risk can be the:

- 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.

3.1.32**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.

3.1.33**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

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.

817	IDS	intrusion detection system
818	IPS	intrusion prevention system
819	IP	internet protocol
820	IT	information technology
821	IoT	Internet of things
822	MLP	multiprotocol label switching
823	NFC	near field communication
824	OT	operational technology
825	PLC	programmable logic controller
826	P2P	peer to peer connection
827	RBAC	role-based access control
828	RS485	recommended standard 485 (according to TIA 485-A)
829	SCADA	supervisory control and data acquisition
830	SD card	secure digital card
831	SSL	secure socket layer
832	ULP	universal logic plug
833	USB	universal serial bus
834	VPN	virtual private network

835 **4 General**

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

840 **5 Security objectives**

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

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

846 The availability and the integrity of the safety related functions of the equipment listed in 7.3.1.1
847 shall be identified as precondition to the security objectives by referring to each product
848 standard and the safety risk assessment performed by the manufacturer of the equipment.

849 **6 Security lifecycle management**

850 **6.1 General**

851 The protections against security attacks are determined based on the results of a security risk
852 assessment in order to identify the potential threats and vulnerabilities, and to define the
853 countermeasures in a document called security requirements specification. As described in IEC
854 62443-4-1 and ISO/IEC 27001, it covers each phase of the life cycle of the equipment and the
855 relevant stakeholders, and it takes into account its physical access and the limits of its
856 environmental conditions (see Figure 2 as an example).

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

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 technics 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		

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

Table 2 – Typical threats

BSI ^a Top 10 threats	Use case		Level of attack
	Number	Name	
Infiltration of malware via removable media and external hardware			
Malware infection 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
Control components connected to the internet	UC4 (B.5)	Use case 4 – Protection against threat actor remotely taking control of a "Managing" intelligent assembly	Substantial
Intrusion via remote access	UC3 (B.4)	Use case 3 – Protection against unauthorized modification of wireless equipment	Substantial
Technical malfunctions and force majeure			
Compromising of smartphones in the production environment			
^a German Federal Office for Information Security			

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.

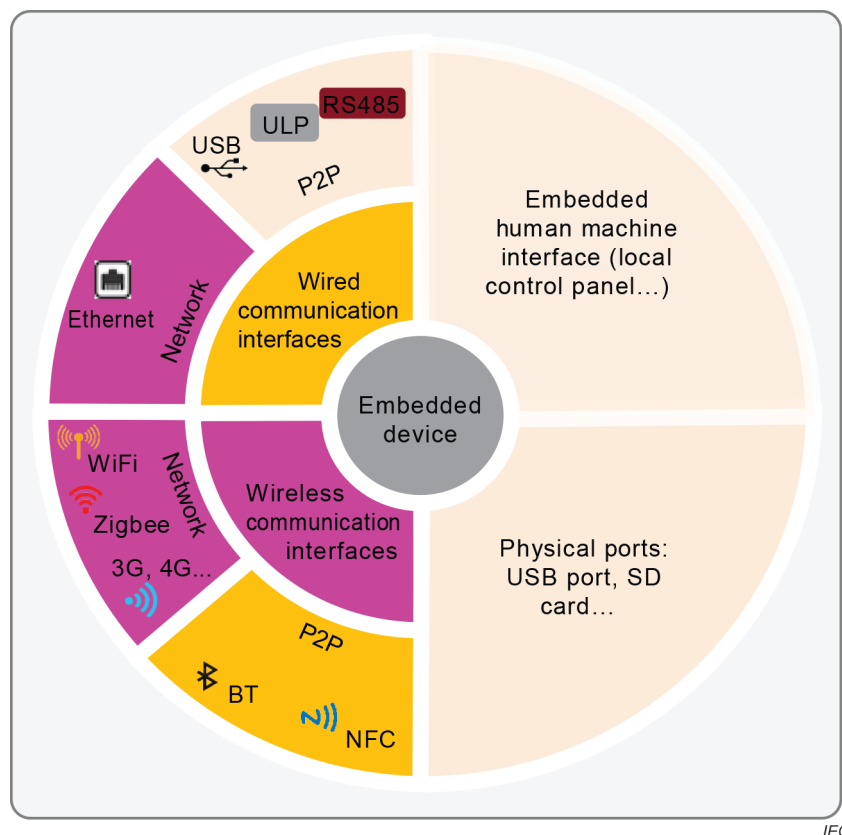


Figure 2 – Example of physical interfaces of an embedded device in an equipment which can be subject to an attack

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 G;
- 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;

- 891 – user accessible physical ports;
- 892 – potential attack vectors including attacks on the hardware if applicable;
- 893 – potential threats according to Table 2, their likelihood, and their severity and consequences as defined in 6.2.3.;
- 894
- 895 – relation to safety as given in 6.2.2;
- 896 – mitigations and/or dispositions for each threat;
- 897 – security-related issues identified;
- 898 – 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.
- 899

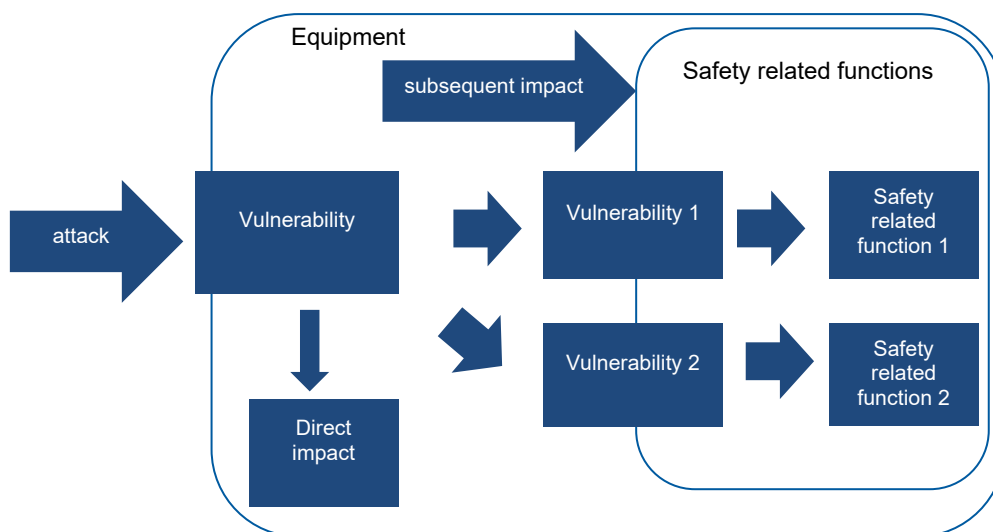
900 NOTE This list is derived from IEC 62443-4-1:2018.

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

904 6.2.2 Relationship between safety and security

905 The safety risk assessment of the equipment shall include the possible interaction between the
 906 safety related functions and the security functions. In case of interaction, further actions shall
 907 be taken to ensure there is no impact on the safety related functions.

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



915

916 **Figure 3 – Example of relation between security and safety**

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

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

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	Temporarily 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 equipment manufacturer. 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.

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 by the manufacturer of the equipment. 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 manufacturer ^b	Define products, systems or services security objectives, intended use & instructions	Original manufacturer	Component supplier	Product supplier
Contractor/integrator	Apply manufacturer system design & service instructions	Electrical contractor and large panel builder	Integrator (OEM)	Integration service provider
Maintenance and repair	Apply manufacturer's commissioning & update instructions	Electrical installer and small panel builder	Maintenance (OEM or MRO or end-user)	Maintenance service provider
End-user	Apply manufacturer's operating instructions	Facility manager	Operator	Asset owner
^a Not covered by this document (for mapping only).				
^b Includes manufacturer 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;

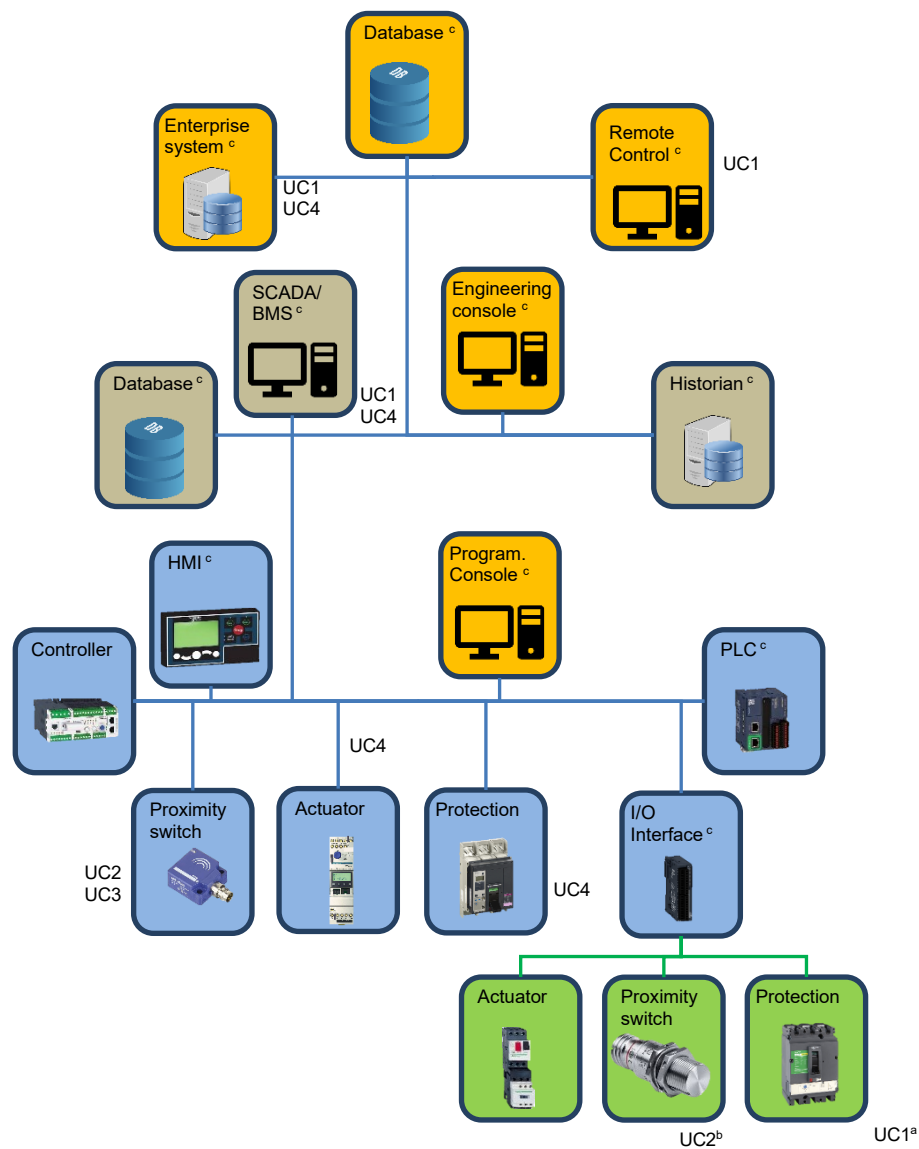
EXAMPLE: A protection equipment associated with an edge communication interface providing monitoring information accessible by a SCADA is CF2.

- 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.

1010 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

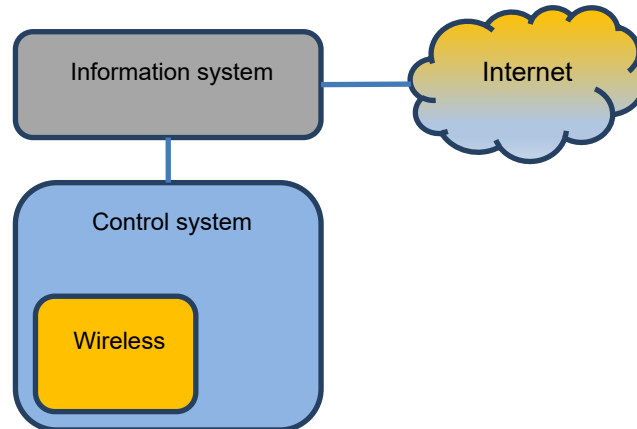
1011 **Figure 4 – Control system architecture with switchgear and controlgear**

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 network is completely closed.
- C2: connected to the information system of the enterprise 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.

C3: connectivity C2 using wireless communication as depicted in



- Figure 5. The wireless access gives more vulnerabilities to attacks.

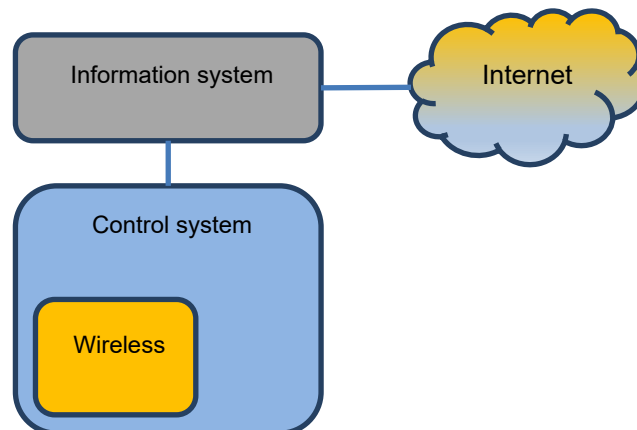


Figure 5 – Control system connectivity level C3

- C4: distributed control system permitting operations from outside as depicted in Figure 6. 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).

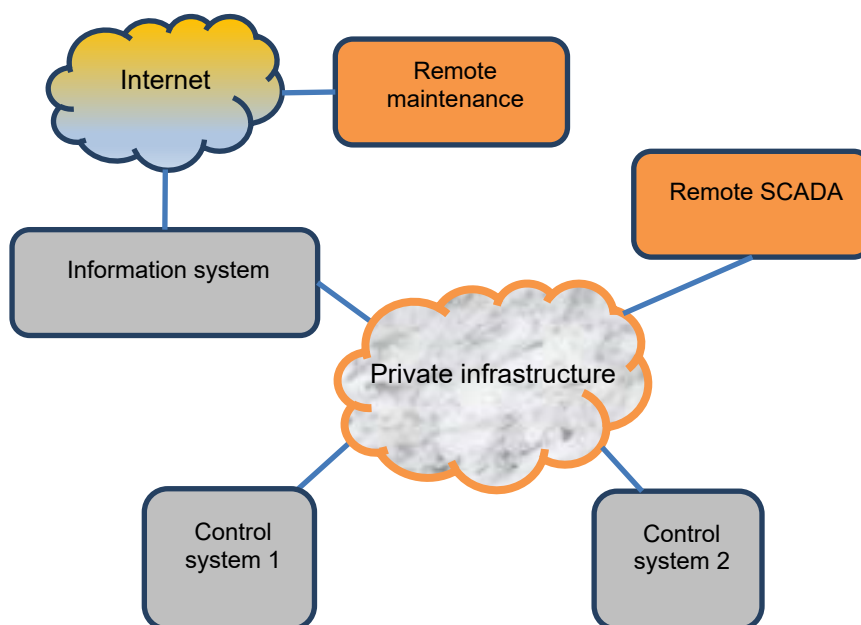


Figure 6 – Control system connectivity level C4

- C5: distributed control system with public infrastructure (Internet) as depicted in Figure 7. 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.

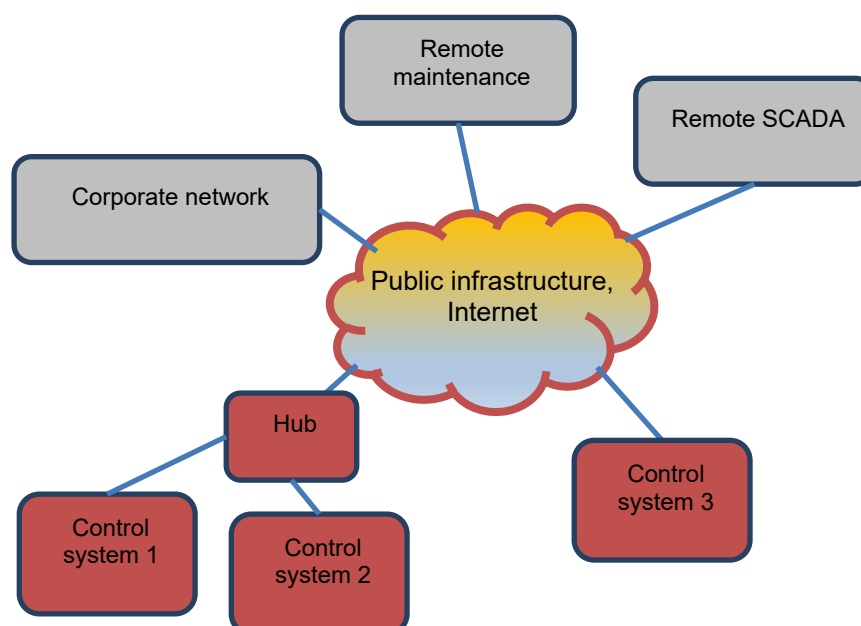


Figure 7 – Control system connectivity level C5

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.

1041 NOTE This classification is derived from ANSSI Classification method and key measures.

1042 6.7.4 Exposure levels of equipment

1043 The exposure of equipment included in the control system is a combination of its levels of
1044 communication functionality and connectivity. Table 5 gives a level of exposure from E1 (least
1045 exposed) to E5 (most exposed). This indicates the amount of risk that can be introduced into
1046 the control system. A higher risk will require a more extensive risk assessment.

1047 **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						

1048 NOTE This classification is derived from ANSSI Classification method and key measures.

1049 The levels of functionality and connectivity do not vary independently. Therefore, some cells
1050 may not correspond to any real system. Other factors can influence the levels, including the
1051 number of devices involved, and the heterogeneity of the devices used. Those factors should
1052 be considered in the risk assessment.

1053 Non-communicating devices illustrated in green in Figure 4 are not considered in the levels of
1054 exposure; but shall be covered in the whole risk assessment when they include embedded
1055 software.

1056 The level of exposure is used for evaluating the severity of the exposure of the equipment to
1057 attacks in order to select the appropriate countermeasure. See Annex B.

1058 6.7.5 Equipment security levels

1059 The technical function of the building or of the machinery in which the equipment is included
1060 should have a target security level defined by the system integrator, the machine builder, or the
1061 facility manager of a building. The equipment used as a part or as the complete technical
1062 function shall provide the capability to meet the target level. The equipment security level does
1063 not include any additional compensating countermeasure.

1064 NOTE: IEC TS 62443-1-1 defines the target, achieved and capability security levels and IEC 62443-2-1 provides
1065 additional information.

1066 The equipment security level in Table 6 can be determined by combining the level of impact
1067 and the level of exposure resulting in the level of potential attack defined in Table 1.

1068 **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					

1069

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 8 is following Annex B of ISO/IEC 15408-1:2022.

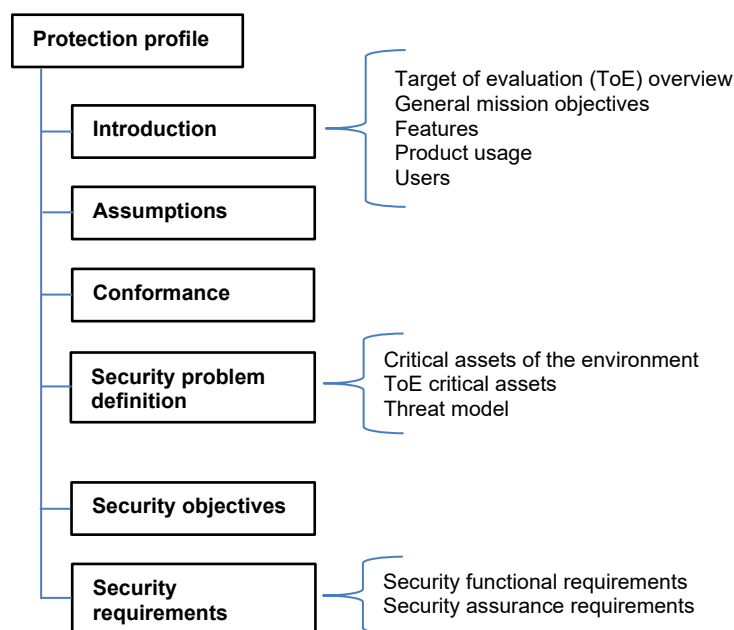


Figure 8 – Structure of a security protection profile

Security protection profiles for switchgear and controlgear are given in Annex E to Annex H 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 manufacturer 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 H.

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.

1096 PA-2 – Appropriate user instructions shall be given for addressing the following requirements:

1097 - Installation rules: According to IEC 60364-7-729, restricted access areas with
1098 switchgear and controlgear assemblies shall not provide access to unauthorized
1099 persons. In addition, door(s) provided for closed restricted access areas shall allow easy
1100 evacuation to the outside by opening without the use of a key, tool or any other device
1101 not part of the opening mechanism.

1102 - Electrical circuits and equipment for critical operations power systems shall be
1103 accessible to qualified personnel only.

1104 7.2.2 Physical access and environment rational

1105 Physical security measures are generally defined at the building facility level for managing its
1106 access and to reduce the risk of accidental or deliberate damage or loss of the building assets
1107 and intellectual property. These measures are often associated with other risks such as safety,
1108 environmental, regulatory, etc. The main operations of an equipment are defined by their
1109 relevant product standard. They are generally readily accessible to an authorised person, i.e.
1110 without additional access logging operation on the equipment.

1111 Providing physical security for the electrical room of a building or the control panel of a machine
1112 is essential to reduce the potential of many threats. These locations often contain essential
1113 electrical power control of the building and safety related control system of machinery. It is
1114 essential that access to these areas be limited to authorized users only.

1115 Table°7 provides references from the relevant security standards corresponding to the
1116 requirements of subclause 7.2.1.

1117 **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

1118 Table°8 provides references to possible security enhancements from the relevant security
1119 standards corresponding to the recommendations of subclause 7.2.3.

1120 **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 J.2

1121

1122 7.2.3 PA-e – Physical access and environment enhancement

1123 According to A.11 of ISO/IEC 27001:2013, several requirements are derived to premises where
1124 low voltage switchgear and controlgear assemblies are installed. Appropriate user instructions
1125 should be given for addressing the following requirements in a) and b).).

1126 a) PA-e1 – For secured areas in order to prevent unauthorized physical access, damage and
1127 interference to the security related main functions of the equipment:

1128 1) PA-e1.1 – Physical security perimeters should be defined and used to protect areas that
1129 contain equipment supporting security related main functions.

1130 2) PA-e1.2 – Physical entry controls: access control should be defined and implemented to
1131 authorized persons for entering premises where the equipment is accessible such as
1132 electrical restricted access areas.