
**Zaščita za sisteme industrijske avtomatizacije in nadzornih sistemov - 4-2. del:
Zahteve za tehnično varnost zaščito za komponente ACS**

Security for industrial automation and control systems - Part 4-2: Technical security requirements for ACS components

Industrielle Kommunikationsnetze - IT-Sicherheit für industrielle Automatisierungssysteme - Teil 4-2: Technische Sicherheitsanforderungen an Komponenten industrieller Automatisierungssysteme (IACS)

Sécurité des systèmes d'automatisation et de commande industrielles - Partie 4-2: Exigences de sécurité technique des composants IACS

Ta slovenski standard je istoveten z: EN IEC 62443-4-2:2019/prAA:2026

ICS:

25.040.01	Sistemi za avtomatizacijo v industriji na splošno	Industrial automation systems in general
35.030	Informacijska varnost	IT Security

SIST EN IEC 62443-4-2:2019/oprAA:2026 en,fr,de

Sample Document

get full document from standards.iteh.ai

EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM

DRAFT
EN IEC 62443-4-2:2019

prAA

March 2026

ICS 25.040.40; 35.030

English Version

Security for industrial automation and control systems - Part 4-2: Technical security requirements for ACS components

Sécurité des systèmes d'automatisation et de commande
industrielles - Partie 4-2: Exigences de sécurité technique
des composants IACS

Industrielle Kommunikationsnetze - IT-Sicherheit für
industrielle Automatisierungssysteme - Teil 4-2: Technische
Sicherheitsanforderungen an Komponenten industrieller
Automatisierungssysteme (IACS)

This draft amendment prAA, if approved, will modify the European Standard EN IEC 62443-4-2:2019; it is submitted to CENELEC members for enquiry.

Deadline for CENELEC: 2026-06-05.

It has been drawn up by CLC/TC 65X.

If this draft becomes an amendment, CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this amendment the status of a national standard without any alteration.

This draft amendment was established by CENELEC in three official versions (English, French, German).

A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the GEN-CENELEC Management Centre has the same status as the official versions.

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

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

Warning : This document is not a European Standard. It is distributed for review and comments. It is subject to change without notice and shall not be referred to as a European Standard.



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

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

© 2026 CENELEC All rights of exploitation in any form and by any means reserved worldwide for CENELEC Members.

Project: 79973

Ref. No. EN IEC 62443-4-2:2019/prAA:2026 E

Contents

	Page
1 European foreword	6
2 Introduction	7
3 1 Modification to the title	7
4 2 Modification to the Introduction	7
5 2.1 Modification to Subclause 0.1, "Overview"	7
6 2.2 Modification to Subclause 0.2, "Purpose and intended audience"	7
7 3 Modification to Clause 1, "Scope"	7
8 4 Modification to Clause 2, "Normative references"	8
9 5 Modification to Clause 3, "Terms, definitions, abbreviated terms, acronyms, and conventions"	8
10 5.1 Modification to Subclause 3.1, "Terms and definitions"	8
11 5.2 Modification to Subclause 3.2, "Abbreviated terms and acronyms"	14
12 5.3 Modification to Subclause 3.3, "Conventions"	17
13 6 Modification to Clause 4, "Common component security constraints"	18
14 6.1 Modification to Subclause 4.1, "Overview"	18
15 6.2 Modification to Subclause 4.2, "CCSC 1 Support of essential functions"	18
16 6.3 Modification to Subclause 4.3, "CCSC 2 Compensating countermeasures"	18
17 6.4 Deletion of Subclause 4.4, "CCSC 3 Least privilege"	18
18 6.5 Modification to Subclause 4.5, "CCS4 Software development process"	18
19 6.6 Addition of subclause 4.5, "Security evaluation"	18
20 7 Modification to Clause 5, "FR 1 – Identification and authentication control"	18
21 7.1 Modification to Subclause 5.1, "Purpose and SL-C(IAC) descriptions"	18
22 7.2 Modification to Subclause 5.3, "CR 1.1 Human user identification and authentication"	19
23 7.3 Modification to Subclause 5.4, "CR 1.2 Software process and device identification and authentication"	21
24	
25 7.4 Modification to Subclause 5.5, "CR 1.3 Account management"	24
26 7.5 Modification to Subclause 5.6, "CR 1.4 Identifier management"	24
27 7.6 Modification to Subclause 5.7, "CR 1.5 Authenticator management"	25
28 7.7 Modification to Subclause 5.8, "CR 1.6 Wireless access management"	28
29 7.8 Modification to Subclause 5.9, "CR 1.7 Strength of password-based authentication"	29
30 7.9 Modification to Subclause 5.10, "CR 1.8 – Public key infrastructure certificates"	31
31 7.10 Modification to Subclause 5.11, "CR 1.9 –Strength of certificate-bases authentication"	32
32 7.11 Modification to Subclause 5.12, "CR 1.10 – Authenticator feedback"	34
33 7.12 Modification to Subclause 5.13, "CR 1.11 – Unsuccessful login attempts"	35
34 7.13 Modification to Subclause 5.14, "CR 1.12 – System use notification"	36

35	7.14	Modification to Subclause 5.15, "CR 1.13 – Access via untrusted networks"	37
36	7.15	Modification to Subclause 5.16, "CR 1.14 – Strength of symmetric key-based authentication"	39
37	8	Modification to Clause 6, "FR 2 – Use control"	39
38	8.1	Modification to Subclause 6.1, "Purpose and SL-C(UC) descriptions"	39
39	8.2	Modification to Subclause 6.2, "Rationale"	40
40	8.3	Modification to Subclause 6.3, "CR 2.1 – Authorization enforcement"	40
41	8.4	Modification to Subclause 6.4, "CR 2.2 – Wireless use control"	44
42	8.5	Modification to Subclause 6.5, "CR 2.3 – Use control for portable and mobile devices"	45
43	8.6	Modification to Subclause 6.6, "CR 2.4 – Mobile code"	45
44	8.7	Modification to Subclause 6.7, "CR 2.5 – Session lock"	47
45	8.8	Modification to Subclause 6.8, "CR 2.6 – Remote session termination"	48
46	8.9	Modification to Subclause 6.9, "CR 2.7 – Concurrent session control"	49
47	8.10	Modification to Subclause 6.10, "CR 2.8 – Auditable events"	50
48	8.11	Modification to Subclause 6.11, "CR 2.9 – Audit storage capacity"	53
49	8.12	Modification to Subclause 6.12, "CR 2.10 – Response to audit processing failures"	54
50	8.13	Modification to Subclause 6.13, "CR 2.11 – Timestamps"	55
51	8.14	Modification to Subclause 6.14, "CR 2.12 – Non-repudiation"	58
52	8.15	Modification to Subclause 6.15, "CR 2.13 – Use of physical diagnostic and test interfaces"	59
53	9	Modification to Clause 7, "FR 3 – System integrity"	61
54	9.1	Modification to Subclause 7.1, Purpose and SL-C(SI) descriptions	61
55	9.2	Modification to Subclause 7.3, CR 3.1 – Communication integrity	61
56	9.3	Modification to Subclause 7.4, "CR 3.2 – Protection from malicious code"	63
57	9.4	Modification to Subclause 7.5, "CR 3.3 – Security functionality verification"	65
58	9.5	Modification to Subclause 7.6, "CR 3.4 – Software and information integrity"	65
59	9.6	Modification to Subclause 7.7, "CR 3.5 – Input validation"	68
60	9.7	Modification to Subclause 7.8, "CR 3.6 – Deterministic output"	69
61	9.8	Modification to Subclause 7.9, CR 3.7 – Error handling	71
62	9.9	Modification to Subclause 7.10, "CR 3.8 – Session integrity"	72
63	9.10	Modification to Subclause 7.11, "CR 3.9 – Protection of audit information"	73
64	9.11	Modification to Subclause 7.12, "CR 3.10 – Support for updates"	75
65	9.12	Modification to Subclause 7.13, "CR 3.11 – Physical tamper resistance and detection"	77
66	9.13	Modification to Subclause 7.14, "CR 3.12 – Provisioning product supplier roots of trust"	79
67	9.14	Modification to Subclause 7.15, "CR 3.13 – Provisioning asset owner roots of trust"	80
68	9.15	Modification to Subclause 7.16, "CR 3.14 – Integrity of the boot process"	82
69	10	Modification to Clause 8, "FR 4 – Data confidentiality"	84
70	10.1	Modification to Subclause 8.1, "Purpose and SL-C(SI) descriptions"	84
71	10.2	Modification to Subclause 8.3, "CR 4.1 – Information confidentiality"	84
72	10.3	Modification to Subclause 8.4, "CR 4.2 – Information persistence"	86

EN IEC 62443-4-2:2019/prAA:2026 (E)

73	10.4	Modification to Subclause 8.5, “CR 4.3 – Use of cryptography”	88
74	11	Modification to Clause 9, “FR 5 – Restricted data flow”	89
75	11.1	Modification to Subclause 9.1, “Purpose and SL-C(SI) descriptions”	89
76	11.2	Modification to Subclause 9.3, “CR 5.1 – Network segmentation”	90
77	11.3	Modification to Subclause 9.4, “CR 5.2 – Zone boundary protection”	91
78	11.4	Modification to Subclause 9.5, “CR 5.3 – General-purpose person-to-person communication	94
79	restrictions”		
80	11.5	Modification to Subclause 9.6, “CR 5.4 – Application partitioning”	94
81	12	Modification to Clause 10, “FR 6 – Timely response to events”	94
82	12.1	Modification to Subclause 10.1, “Purpose and SL-C(SI) descriptions”	94
83	12.2	Modification to Subclause 10.3, “CR 6.1 – Audit log accessibility”	95
84	12.3	Modification to Subclause 10.4, “CR 6.2 – Continuous monitoring”	96
85	13	Modification to Clause 11, “FR 7 – Resource availability”	98
86	13.1	Modification to Subclause 11.1, “Purpose and SL-C(SI) descriptions”	98
87	13.2	Modification to Subclause 11.2, “Rationale”	98
88	13.3	Modification to Subclause 11.3, “CR 7.1 – Denial of service protection”	98
89	13.4	Modification to Subclause 11.4, “CR 7.2 – Resource management”	100
90	13.5	Modification to Subclause 11.5, “CR 7.3 – Control system backup”	101
91	13.6	Modification to Subclause 11.6, “CR 7.4 – Control system recovery and reconstitution”	102
92	13.7	Modification to Subclause 11.5, “CR 7.5 – Emergency power”	103
93	13.8	Modification to Subclause 11.8, “CR 7.6 – Network and security configuration settings”	104
94	13.9	Modification to Subclause 11.10, “CR 7.7 – Least functionality”	105
95	13.10	Modification to Subclause 11.10, “CR 7.8 – Control system component inventory”	106
96	13.11	Addition of Subclause 11.11, “CR 7.9 – Component Reset”	107
97	14	Deletion of Clause 12, “Software application requirements”	108
98	15	Deletion of Clause 13, “Embedded device requirements”	108
99	16	Deletion of Clause 14, “Host device requirements”	108
100	17	Deletion of Clause 15, “Network device requirements”	108
101	18	Modification to Annex A, “Device categories”	108
102	Annex A (informative) Mapping of CRs and REs to SL-Cs		109
103	19	Modification to Annex B, “Mapping of CRs and REs to FR SLs 1-4”	112
104	Annex B (normative) Security evaluation methodology		113
105	20	Addition of Annex C “Security evaluation methodology”	146
106	Annex C (informative) ACS component specification		147
107	21	Addition of Annex D, “Mapping of EN IEC 62443-4-1 requirement artefacts to the evaluation	148
108	activities”		
109	Annex D (informative) Mapping of EN IEC 62443-4-1 requirement artefacts to the evaluation activities		149
110			
111	22	Addition of Annex E, “Overview evaluation activities”	152

112	Annex E (informative) Overview evaluation activities	153
113	23 Addition of Annex F, “Mapping of the evaluation activities to CLC IEC/TS 62443-6-2:2025”	155
114	Annex F (informative) Mapping of the evaluation activities to CLC IEC/TS 62443-6-2:2025	156
115	24 Addition of Annex G, “Security test grades and security test modules”	157
116	Annex G (informative) Security test grades and security test modules	158
117	25 Addition of Annex H, “Threats mapping to EU CRA essential cybersecurity requirements”	183
118	Annex H (informative) Threats mapping to EU CRA essential cybersecurity requirements	184
119	26 Addition of Annex ZZ, “Relationship between this European standard and the essential	
120	cybersecurity requirements of Regulation (EU) 2024/2847 aimed to be covered”	189
121	Annex ZZ (informative) Relationship between this European standard and the essential cybersecurity	
122	requirements of Regulation (EU) 2024/2847 aimed to be covered	190
123	27 Modifications to the “Bibliography”	192

Sample Document

get full document from standards.iteh.ai

EN IEC 62443-4-2:2019/prAA:2026 (E)124 **European foreword**

125 This document (EN IEC 62443-4-2:2019/prAA:2026) has been prepared by CLC/TC 65X "Industrial-process
126 measurement, control and automation".

127 This document is currently submitted to the Enquiry.

128 The following dates are proposed:

- latest date by which the existence of this (doa) dav + 6 months
document has to be announced at national level
- latest date by which this document has to be (dop) dav + 12 months
implemented at national level by publication of
an identical national standard or by
endorsement
- latest date by which the national standards (dow) dav + 36 months
conflicting with this document have to be (to be confirmed or
withdrawn modified when voting)

129 This document will amend EN IEC 62443-4-2:2019.

130 EN IEC 62443-4-2:2019/prAA:2026 includes the following significant technical modifications with respect to
131 EN IEC 62443-4-2:2019:

- 132 — update of existing requirements and introduction of new requirements;
- 133 — update by introducing a full evaluation methodology;
- 134 — updates of requirements to include requirement-specific applicability criteria, acceptance criteria and
135 evaluation artefacts.

136 This document has been prepared under a standardization request addressed to CENELEC by the European
137 Commission. The Standing Committee of the EFTA States subsequently approves these requests for its
138 Member States.

139 For the relationship with EU Legislation, see informative Annex ZZ, which is an integral part of this document.

140 Introduction

141 The purpose of this amendment is to identify and modify the requirements and associated clauses to align with
 142 the EU Cyber Resilience Act essential cybersecurity requirements, so that the amendment
 143 (EN IEC 62443-4-2:2019/prAA:2025), once made available by CENELEC, can be offered for citation under the
 144 Cyber Resilience Act.

145 1 Modification to the title

146 *Replace the title with the following:*

147 “Security for industrial automation and control systems - Part 4-2: Technical security requirements for ACS
 148 components”

149 2 Modification to the Introduction

150 2.1 Modification to Subclause 0.1, “Overview”

151 *Replace the whole content of “0.1 Overview” with the following:*

152 “This document defines cybersecurity technical requirements for components used in operational technology
 153 (OT) environments. OT is the technology for detecting, managing or causing change through the monitoring or
 154 control of physical entities – for example sensors, actuators, programmable logic controllers (PLCs), industrial
 155 communication devices, supervisory control systems and related software applications.

156 These requirements can support interested parties (e.g. during conformity assessment activities) to achieve
 157 comparability of assessment results. Annex B introduces a security evaluation methodology that integrates
 158 lifecycle-based practices with component-level assurance criteria.”

159 2.2 Modification to Subclause 0.2, “Purpose and intended audience”

160 *Replace the whole content of “0.2 Purpose and intended audience” with the following:*

161 “This document is intended for product suppliers, but also other interested parties involved in the development,
 162 integration, testing, and assessment of automation and control system components. Relevant stakeholders
 163 include, but are not limited to, security engineers, software and hardware developers, system architects, product
 164 managers, test engineers, compliance and regulatory personnel, security incident response personnel, and
 165 documentation personnel.

166 This document helps product suppliers to understand the security requirements placed on ACS components.
 167 An ACS component might not provide a required capability itself but might be designed to integrate with a
 168 higher-level entity and thus benefit from that entity’s capability – for example a device might not be maintaining
 169 a user directory itself but might integrate with a system wide authentication and authorization service and thus
 170 still meet the requirements to provide individual user authentication, authorization and management capabilities.
 171 This document will guide product suppliers as to which requirements can be allocated and which requirements
 172 should be native in the components.”

173 3 Modification to Clause 1, “Scope”

174 *Replace the whole content of “Scope” with the following:*

175 “This document provides detailed technical control system component requirements (CRs) associated with the
 176 seven foundational requirements (FRs) including defining the requirements for automation control systems
 177 capability security levels and their components, SL-C(component).

178 The seven foundational requirements (FRs) are:

- 179 a) identification and authentication control (IAC),
- 180 b) use control (UC),

EN IEC 62443-4-2:2019/prAA:2026 (E)

- 181 c) system integrity (SI),
 182 d) data confidentiality (DC),
 183 e) restricted data flow (RDF),
 184 f) timely response to events (TRE), and
 185 g) resource availability (RA).

186 These seven foundational requirements provide a basis for the technical security requirements in this document.
 187 The first of these, FR-1, addresses the capabilities necessary to reliably identify and authenticate all users
 188 (humans, software processes, and devices) attempting to access the component. FR-2 addresses the
 189 capabilities necessary to enforce the assigned privileges of an authenticated user (human, software process,
 190 and device) to perform actions on a component and monitor use of these privileges. FR-3 addresses the
 191 capabilities necessary for the integrity of the component to protect against unauthorized manipulation or
 192 modification. FR-4 addresses the capabilities necessary for the confidentiality of information on communication
 193 data flows and in data stored at rest and processed by the component to prevent unauthorized disclosure. FR-
 194 5 addresses the capabilities necessary to support segmentation of networks and data flows and limit
 195 unnecessary and unwanted flow of data. FR-6 addresses the capabilities necessary to respond to security
 196 violations by notifying the proper authority, reporting needed evidence of a violation and taking timely corrective
 197 action when incidents are discovered. FR-7 addresses the capabilities necessary to protect the availability of
 198 components against the degradation or denial of essential functions and services.

199 Within each FR, the technical security requirements are grouped into security levels as a basis for selection of
 200 security measures as part of a risk-based approach.”

201 **4 Modification to Clause 2, “Normative references”**

202 *Replace the second normative reference with the following:*

203 EN IEC 62443-3-3:2019, *Industrial communication networks - Network and system security - Part 3-3: System*
 204 *security requirements and security levels*

205 *Replace the third normative reference with the following:*

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

208 **5 Modification to Clause 3, “Terms, definitions, abbreviated terms, acronyms, and** 209 **conventions”**

210 **5.1 Modification to Subclause 3.1, “Terms and definitions”**

211 *Replace the content of subclause 3.1 with the following:*

212 “

213 For the purposes of this document, the terms and definitions given in EN IEC 62443-3-3:2019 and
 214 EN IEC 62443-4-1:2018, and the following apply.

215 NOTE Many of the following terms and definitions are originally based on relevant International Organization for
 216 Standardization (ISO), International Electrotechnical Commission (IEC) and US. National Institute of Standards and
 217 Technology (NIST) sources, sometimes with minor modifications to enhance suitability for ACS security requirements.”

¹ As impacted by EN IEC 62443-4-1:2018/prAA:2026.

218 *Add the following term entry 3.1.1:*

219 **3.1.1**

220 **ACS component specification**

221 list of artefacts resulting from the application of an EN IEC 62443-4-1 secure development lifecycle to an ACS
222 component

223 *Add the following term entry 3.1.2:*

224 **3.1.2**

225 **artefact**

226 result of executing a secure development lifecycle or documented evidence according to the process
227 requirements of EN IEC 62443-4-1

228 EXAMPLE documented threat models, definitions and descriptions of security requirements, or test case specifications
229 and results

230 Note 1 to entry: Artefact is used with the same meaning as evidence but implies that the processes of EN IEC 62443-4-1
231 were applied to the product.

232 [SOURCE: CLC IEC/TS 62443-6-2:2025]

233 *Replace the clause number of term entry “asset” to 3.1.3 from 3.1.1 and replace “IACS” with “ACS”.*

234 *Replace clause number of term entry “asset owner” to 3.1.4 from 3.1.2 and replace “IACS” with “ACS”.*

235 *Replace the clause number of term entry “attack” to 3.1.5 from 3.1.3 and replace “IACS” with “ACS”.*

236 *Add the following term entry 3.1.6:*

237 **3.1.6**

238 **authenticated security test**

239 security test allowing a tester direct access to products or components using remote administrative protocols
240 and to authenticate to the products or components using provided credentials

241 EXAMPLE Secure shell (SSH) or remote desktop protocol (RDP) are examples of remote administrative protocols

242 Note 1 to entry: Authenticated security tests provide a more thorough view and more detailed insights of the tested product
243 compared to unauthenticated security tests. They can therefore identify additional vulnerabilities at the product which had
244 not been detected by unauthorized security tests.

245 *Replace the clause number of term entry “authentication” to 3.1.7 from 3.1.4.*

246 *Replace the clause number of term entry “authenticator” to 3.1.8 from 3.1.5.*

247 *Replace the clause number of term entry “authenticator” to 3.1.9 from 3.1.6.*

248 *Add the following term entry 3.1.10:*

249 **3.1.10**

250 **automation and control system**

251 collection of integrated components that provide functions for monitoring, controlling and managing the
252 operation of equipment under control

253 *Add the following term entry 3.1.11:*

254 **3.1.11**

255 **automation and control system component**

256 component developed and supported according to the secure development processes described in
257 EN IEC 62443-4-1 and implementing the applicable technical requirements of EN IEC 62443-4-2

258 *Replace the clause number of term entry “availability” to 3.1.12 from 3.1.7.*

259 *Add the following term entry 3.1.13:*

EN IEC 62443-4-2:2019/prAA:2026 (E)

- 260 **3.1.13**
 261 **check**
 262 generate a verdict by a simple comparison
 263 [SOURCE: ISO/IEC 18045:2022, 3.1]
 264 *Replace the clause number of term entry “communication channel” to 3.1.14 from 3.1.8.*
 265 *Replace the clause number of term entry “compensating countermeasure” to 3.1.15 from 3.1.9 and replace*
 266 *“IACS” with “ACS”.*
 267 *Replace the clause number of term entry “component” to 3.1.16 from 3.1.10.*
 268 *Replace the clause number of term entry “conduit” to 3.1.17 from 3.1.11.*
 269 *Replace the clause number of term entry “confidentiality” to 3.1.18 from 3.1.2 and replace “IACS” with “ACS”.*
 270 *Replace the clause number of term entry “conduit” to 3.1.19 from 3.1.13.*
 271 *Replace the clause number of term entry “control system” to 3.1.20 from 3.1.14 and replace “IACS” with “ACS”.*
 272 *Replace the clause number of term entry “compensating countermeasure” to 3.1.21 from 3.1.15.*
 273 *Replace the clause number of term entry “degraded mode” to 3.1.22 from 3.1.16.*
 274 *Replace the clause number of term entry “device” to 3.1.23 from 3.1.17.*
 275 *Replace the clause number of term entry “embedded device” to 3.1.24 from 3.1.18.*
 276 *Replace the clause number of term entry “environment” to 3.1.25 from 3.1.19 and replace “IACS” with “ACS”.*
 277 *Add the following term entry 3.1.26:*
 278 **3.1.26**
 279 **equipment under control**
 280 equipment, machinery, apparatus, or plant used for manufacturing, process, transportation, medical, or other
 281 activities
 282 [SOURCE: IEC 61508-4:2010]
 283 *Replace the clause number of term entry “essential function” to 3.1.27 from 3.1.20.*
 284 *Add the following term entry 3.1.28:*
 285 **3.1.28**
 286 **evaluation**
 287 systematic determination of the extent to which the target of evaluation meets its specified requirements by
 288 either a check (3.1.13) or examine (3.1.33)
 289 Note 1 to entry: In the EN IEC 62443 series evaluation is used during conformity assessment.
 290 [SOURCE: CLC IEC/TS 62443-6-2:2025]
 291 *Add the following term entry 3.1.29:*
 292 **3.1.29**
 293 **evaluation activity**
 294 determination if the target of evaluation meets the referenced requirements of the standard
 295 [SOURCE: CLC IEC/TS 62443-6-2:2025]
 296 *Add the following term entry 3.1.30:*
 297 **3.1.30**
 298 **evaluation criteria**
 299 criteria used to determine whether the target of evaluation fulfils the evaluated requirement in a suitable manner
 300 [SOURCE: CLC IEC/TS 62443-6-2:2025]
 301 *Add the following term entry 3.1.31:*

- 302 **3.1.31**
 303 **evaluator**
 304 individual or organization that performs the evaluation
 305 [SOURCE: ISO 25040:2011, 4.25]
 306 *Replace the clause number of term entry “event” to 3.1.32 from 3.1.21 and replace “IACS” with “ACS”.*
 307 *Add the following term entry 3.1.33:*
- 308 **3.1.33**
 309 **examine**
 310 generate a verdict by analysis using evaluator expertise
 311 [SOURCE: ISO/IEC 18045:2022, 3.9]
 312 *Add the following term entry 3.1.34:*
- 313 **3.1.34**
 314 **external interface**
 315 physical or logical interface of a component that can be accessed from outside the component
 316 EXAMPLE Machine, network, user interfaces, and API are types of external interfaces.
- 317 *Replace the clause number of term entry “firecall” to 3.1.35 from 3.1.22.*
 318 *Replace the clause number of term entry “host device” to 3.1.36 from 3.1.23.*
 319 *Replace the clause number of term entry “identifier” to 3.1.37 from 3.1.24.*
 320 *Replace the clause number of term entry “incident” to 3.1.38 from 3.1.25.*
 321 *Delete the term entry 3.1.26 “industrial automation and control system” and replace the clause number of term*
 322 *entry “integrity” to 3.1.39 from 3.1.27.*
- 323 *Add the following term entry 3.1.40:*
- 324 **3.1.40**
 325 **intended use**
 326 use for which a product is designed by the product supplier, describing the explicit and implicit assumptions
 327 about the product’s properties and capabilities
- 328 EXAMPLE The intended use of a network switch is to switch network traffic in an enterprise environment used by
 329 skilled persons. The intended use does not describe specific product features, e.g. security update capability, authentication
 330 mechanism.
- 331 Note 1 to entry: The product security context is derived from the intended use
- 332 *Replace the clause number of term entry “least privilege” to 3.1.41 from 3.1.28 and replace “IACS” with “ACS”.*
 333 *Replace term entry 3.1.29 “mobile code” with the following.*
- 334 **3.1.42**
 335 **mobile code**
 336 code or script loaded, transferred or entered from a source external to the component that can be executed
 337 without explicit installation by the recipient
- 338 EXAMPLE JavaScript, VBScript, Serialized Java objects, Shell scripts and other scripting languages.
- 339 *Replace the clause number of term entry “mobile device” to 3.1.43 from 3.1.30.*
 340 *Replace the clause number of term entry “network device” to 3.1.44 from 3.1.31.*
 341 *Replace the clause number of term entry “non-repudiation” to 3.1.45 from 3.1.32.*
 342 *Add the following term entry 3.1.46:*

EN IEC 62443-4-2:2019/prAA:2026 (E)

343 **3.1.46**
 344 **operational technology**
 345 technology for detecting, facilitating, managing or causing change, through automation, monitoring or control,
 346 to a physical entity or environment

347 [SOURCE: IEC/TS 62443-1-1:2009]

348 *Add the following term entry 3.1.47:*

349 **3.1.47**
 350 **product**
 351 system, subsystem or component that is manufactured, developed or refined

352 Note 1 to entry: In the context of EN IEC 62443-3-3:2019 a product is an automation and control system (ACS).

353 Note 2 to entry: In the context of this document a product is an ACS component.

354 *Add the following term entry 3.1.48:*

355 **3.1.48**
 356 **product security context**
 357 security provided to the product by the environment (product user deployment) in which the product is intended
 358 to be used

359 *Replace the clause number of term entry “product supplier” to 3.1.49 from 3.1.33.*

360 *Replace the clause number of term entry “remote access” to 3.1.50 from 3.1.34.*

361 *Replace the clause number of term entry “role” to 3.1.51 from 3.1.35 and replace “IACS” with “ACS”.*

362 *Replace the clause number of term entry “safety instrumented system” to 3.1.52 from 3.1.36.*

363 *Replace term entry 3.1.37 “security level” with the following:*

364 **3.1.53**
 365 **security level**
 366 set of security measures that supports a degree of risk reduction

367 *Add the following term entry 3.1.54:*

368 **3.1.54**
 369 **security test grade**
 370 defined set of security test modules

371 *Add the following term entry 3.1.55:*

372 **3.1.55**
 373 **security test module**
 374 specification of a security testing activity, describing the aim of the security test, the testing methodology and
 375 acceptance criteria

376 *Add the following term entry 3.1.56:*

377 **3.1.56**
 378 **security verification and validation testing**
 379 testing performed to assess the overall security of a component, product or system when used in its intended
 380 product security context and to determine if a component, product or system satisfies the product security
 381 requirements and satisfies its designed security purpose

382 Note 1 to entry: Examples for security testing according to IEC 62443-4-1 are threat mitigation testing, vulnerability testing
 383 and penetration testing.

384 Note 2 to entry: Security verification and validation testing is the term used in EN IEC 62443-4-1.

385 [SOURCE: EN IEC 62443-4-1:2018, 3.1.44, modified — the notes have been added]

386 *Add the following term entry 3.1.57:*

- 387 **3.1.57**
 388 **sensitive information**
 389 information and related data that needs to be protected under law or for which unavailability, disclosure,
 390 modification or loss impacts security
- 391 *Replace the clause number of term entry "session" to 3.1.58 from 3.1.38.*
 392 *Replace the clause number of term entry "session ID" to 3.1.59 from 3.1.39.*
 393 *Replace the clause number of term entry "setpoint" to 3.1.60 from 3.1.40.*
 394 *Add the following term entry 3.1.61:*
- 395 **3.1.61**
 396 **single purpose component**
 397 dedicated device that is exclusively allocated to a single entity and single application
 398 EXAMPLE Sensor, actuator, unmanaged network switch
- 399 *Replace the clause number of term entry "software application" to 3.1.62 from 3.1.41.*
 400 *Add the following term entry 3.1.63:*
- 401 **3.1.63**
 402 **supporting measure**
 403 functions (e.g. provided by the underlying software or hardware) and procedures (e.g. to ensure physical
 404 protection) provided by the product security context to support the implementation of the component
 405 requirement
- 406 *Add the following term entry 3.1.64:*
- 407 **3.1.64**
 408 **system**
 409 interacting, interrelated, or interdependent elements forming a complex whole
- 410 *Replace the clause number of term entry "system integrator" to 3.1.65 from 3.1.42.*
 411 *Add the following term entry 3.1.66:*
- 412 **3.1.66**
 413 **target of evaluation**
 414 subject of a security evaluation
- 415 Note 1 to entry: the subject of a security evaluation is a product, i.e. either an automation and control system (ACS) or an
 416 ACS component.
- 417 *Replace the clause number of term entry "threat" to 3.1.67 from 3.1.43.*
 418 *Add the following term entry 3.1.68:*
- 419 **3.1.68**
 420 **time-related information**
 421 information or related data representing an absolute or relative time or that can be used to derive an absolute
 422 or relative time
- 423 Note 1 to entry: Time-related information might be the period of time, in seconds, since power up of the component, or
 424 simply the sequence of occurred events
- 425 *Replace the clause number of term entry "trust" to 3.1.69 from 3.1.44.*
 426 *Add the following term entry 3.1.70:*
- 427 **3.1.70**
 428 **unauthenticated security test**
 429 security test performed without any authentication at the tested product or component
- 430 *Replace the clause number of term entry "untraceability" to 3.1.71 from 3.1.45.*