
Zaščita industrijske avtomatizacije in nadzornih sistemov - 4-1. del: Zahteve za varnost izdelka v obdobju razvoja izdelka

Security for industrial automation and control systems - Part 4-1: Secure product development lifecycle requirements

IT-Sicherheit für industrielle Automatisierungssysteme - Teil 4-1: Anforderungen an den Lebenszyklus für eine sichere Produktentwicklung

Sécurité des automatismes industriels et des systèmes de commande - Partie 4-1 : Exigences applicables au cycle de vie de développement sécurisé des produits

Ta slovenski standard je istoveten z: EN IEC 62443-4-1:2018/prAA:2026

ICS:

13.020.60	Življenjski cikli izdelkov	Product life-cycles
25.040.01	Sistemi za avtomatizacijo v industriji na splošno	Industrial automation systems in general
35.030	Informacijska varnost	IT Security

SIST EN IEC 62443-4-1:2018/oprAA:2026 en,fr,de

Sample Document

get full document from standards.iteh.ai

EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM

DRAFT
EN IEC 62443-4-1:2018

prAA

March 2026

ICS 35.030; 25.040.40

English Version

Security for industrial automation and control systems - Part 4-1: Secure product development lifecycle requirements

Sécurité des automatismes industriels et des systèmes de commande - Partie 4-1 : Exigences applicables au cycle de vie de développement sécurisé des produits

IT-Sicherheit für industrielle Automatisierungssysteme - Teil 4-1: Anforderungen an den Lebenszyklus für eine sichere Produktentwicklung

This draft amendment prAA, if approved, will modify the European Standard EN IEC 62443-4-1:2018; 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 CEN-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: 81487

Ref. No. EN IEC 62443-4-1:2018/prAA:2026 E

1	Contents	
2	European foreword	5
3	Introduction	6
4	1 Modification to the Introduction	6
5	2 Modification to Clause 1, “Scope”	6
6	3 Modification to Clause 2, “Normative references”	6
7	4 Modification to Clause 3, “Terms, definitions, abbreviated terms, acronyms and conventions”	6
8	4.1 Modification to Subclause 3.1, “Terms and definitions”	6
9	4.2 Modification to Subclause 3.2, “Abbreviated terms and acronyms”	13
10	4.3 Modification to Subclause 3.3, “Conventions”	14
11	5 Modification to Clause 4, “General principles”	14
12	5.1 Modification to Subclause 4.1, “Concepts”	14
13	5.2 Modification to Subclause 4.2, “Maturity model”	15
14	6 Modification to Clause 5, “Practice 1 – Security Management”	16
15	6.1 Modification to all Subclauses	16
16	6.2 Modification to Subclause 5.2, “SM-1: Development process”	17
17	6.3 Modification to Subclause 5.4, “SM-2: Identification of responsibilities”	17
18	6.4 Modification to Subclause 5.5, “SM-3: Identification of applicability”	17
19	6.5 Modification to Subclause 5.6, “SM-4: Security expertise”	18
20	6.6 Modification to Subclause 5.7, “SM-5: Process scoping”	18
21	6.7 Modification to Subclause 5.8, “SM-6: File integrity”	18
22	6.8 Modification to Subclause 5.9, “SM-7: Development environment security”	18
23	6.9 Modification to Subclause 5.10, “SM-8: Control for private keys”	19
24	6.10 Modification to Subclause 5.11, “SM-9: Security requirements for externally provided components”	
25	19	
26	6.11 Deletion of Subclause 5.12, “SM-10: Custom developed components from third-party suppliers” ...	20
27	6.12 Addition of Subclause 5.11, “SM-10: Policy on vulnerability handling”	20
28	6.13 Modification of Subclause 5.13, “SM-11: Assessing and addressing security-related issues”	21
29	6.14 Modification of Subclause 5.14, “SM-12: Process verification”	21
30	6.15 Modification of Subclause 5.15, “SM-13: Continuous improvement”	22
31	6.16 Modification of Subclause 5.15, “SM-11: Assessing and addressing security-related issues”	23
32	6.17 Modification of Subclause 5.16, “SM-15: Process verification”	24
33	6.18 Modification of Subclause 5.17, “SM-16: Regular product security reviews “	24
34	6.19 Modification of Subclause 5.18, “SM-17: Continuous improvement”	25
35	7 Addition of Clause 6, “Practice 2 – Security risk management”	26
36	8 Modification to Clause 6, “Practice 2 – Specification of security requirements”	32

37	9	Modification to Clause 7, “Practice 3 – Secure by design”	34
38	9.1	Modification to the clause number and title	34
39	9.2	Modification to Subclause 7.1, “Purpose”	34
40	9.3	Modification to Subclause 7.2, “SD-1: Secure design principles “	34
41	9.4	Modification to Subclause 7.3, “SD-2: Defense in depth design”	36
42	9.5	Modification to Subclause 7.4, “SD-3: Security design review”	37
43	9.6	Modification to Subclause 7.5, “SD-4: Secure design best practices”	37
44	9.7	Addition of Subclause 8.6, “SD-5: Secure by default”	38
45	10	Modification to Clause 8, “Practice 4 – Secure implementation”	40
46	10.1	Modification to the Clause number	40
47	10.2	Modification to Subclause 8.1, “Purpose”	40
48	10.3	Modification to Subclause 8.2, “Applicability”	40
49	10.4	Modification to Subclause 8.3, “SI-1: Security implementation review”	40
50	10.5	Modification to Subclause 8.4, “SI-2: Secure coding standards”	41
51	11	Modification to Clause 9, “Practice 5 – Security verification and validation testing”	41
52	12	Modification to Clause 10, “Practice 6 – Management of security-related issues”	46
53	12.1	Modification to Subclause 10.1, “Purpose”	47
54	12.2	Modification to Subclause 10.2, “DM-1: Receiving notifications of security-related issues”	47
55	12.3	Modification to Subclause 10.3, “DM-2: Reviewing security-related issues”	47
56	12.4	Modification to Subclause 10.4, “DM-3: Assessing security-related issues”	47
57	12.5	Modification to Subclause 10.5, “DM-4: Addressing security-related issues”	48
58	12.6	Modification to Subclause 10.6, “DM-5: Disclosing security-related issues”	49
59	12.7	Modification to Subclause 10.7, “DM-6: Periodic review of security defect management practice”	50
60	13	Modification to Clause 11, “Practice 7 – Security update management”	50
61	13.1	Modification to Subclause 11.2 “SUM-1: Security update qualification”	50
62	13.2	Modification to Subclause 11.3, “SUM-2: Security update documentation”	51
63	13.3	Modification to Subclause 11.4 “SUM-3: Dependent component or operating system security update documentation”	51
64	13.4	Modification to Subclause 11.5, “SUM-4: Security update delivery”	52
65	13.5	Modification to Subclause 11.6, “SUM-5: Timely delivery of security patches”	52
66	13.6	Modification to Subclause 11 after 11.6	53
67	14	Modification to Clause 12, “Practice 8 – Security guidelines”	54
68	14.1	Modification to Subclause 12.2, “SG-1: Product defense in depth”	55
69	14.2	Modification to Subclause 12.3, “SG-2: Product defense in depth”	55
70	14.3	Modification to Subclause 12.4, “SG-3: Security handling guidelines”	56
71	14.4	Modification to Subclause 12.5, “ SG-4: Secure disposal guidelines”	57
72	14.5	Modification to Subclause 12.6, “SG-5: Secure operation guidelines”	57
73	14.6	Modification to Subclause 12.7, “SG-6: Account management guidelines”	58

EN IEC 62443-4-1:2018/prAA:2026 (E)

75	14.7	Modification to Subclause 12.8, "SG-7: Documentation review"	58
76	15	Deletion of Annex A, "Possible metrics"	58
77	16	Modification to Annex B, "Table of requirements "	59
78		Annex A (informative) Table of requirements.....	60
79	17	Addition of Annex B, "Product security context category"	62
80		Annex B (normative) Product security context category	63
81	18	Addition of Annex C, "Applicability of product security requirements and security risk	
82		management workflow"	64
83		Annex C (normative) Applicability of product security requirements and security risk management	
84		workflow	65
85	19	Addition of Annex D, "Identification and documentation of applicable product security test	
86		modules"	70
87		Annex D (normative) Applicability of product security requirements and security risk management	
88		workflow	71
89	20	Addition of Annex E, "Statement of Applicability – Documentation Template"	72
90		Annex E (informative) Statement of applicability - Documentation template	73
91	21	Addition of Annex F, "Mapping prEN 40000-1-2"	74
92		Annex F (informative) Mapping of EN 40000-1-2.....	75
93	22	Addition of Annex G, "Mapping prEN 40000-1-3"	76
94		Annex G (informative) Mapping EN 40000-1-3.....	77
95	23	Modification to the "Bibliography"	79

get full document from standards.iteh.ai

96 European foreword

97 This document (EN IEC 62443-4-1:2018/prAA:2026) has been prepared by Technical Committee
98 CLC/TC 65X "Industrial-process measurement, control and automation".

99 This document is currently submitted to the Enquiry.

100 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)

101 This document will modify EN IEC 62443-4-1:2018 (PR = 81847).

102 EN IEC 62443-4-1:2018/prAA:2026 includes the following significant technical modifications with respect to
103 EN IEC 62443-4-1:2018:

104 — update of existing requirements and introduction of new requirements;

105 — update by introducing an applicability assessment process;

106 — additon of new practice Risk management.

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

EN IEC 62443-4-1:2018/prAA:2026 (E)**110 Introduction**

111 The purpose of this amendment is to identify and modify the requirements and associated clauses to align
 112 with the EU Cyber Resilience Act essential cybersecurity requirements, so that the amendment
 113 (EN IEC 62443-4-1:2018/prAA:2026), once made available by CENELEC, can be used as a normative
 114 reference by EN IEC 62443-4-2:2019/prAA:2026.

115 1 Modification to the Introduction

116 *Replace the content of the Introduction with the following:*

117 “This document is part of a series of standards that addresses the issue of security for automation and control
 118 systems (ACS). This document describes product development lifecycle requirements related to cyber
 119 security for products intended for use in the automation and control systems environment and provides
 120 guidance on how to meet the requirements described for each element.

121 This document is the part of the EN IEC 62443 series that contains security requirements for developers of
 122 any automation and control products where security is a concern.”

123 2 Modification to Clause 1, “Scope”

124 *Replace the content with the following:*

125 “This part of EN IEC 62443 specifies process requirements for the secure development of products used in
 126 automation and control systems. It defines a secure development lifecycle (SDL) for the purpose of
 127 developing and maintaining secure products. This secure development lifecycle includes security risk
 128 management, security requirements definition, secure design, secure implementation (including coding
 129 guidelines), verification and validation, defect management, security update management and product end-of-
 130 life. These requirements can be applied to new or existing processes for developing, maintaining and retiring
 131 hardware, software or firmware for new or existing products. These requirements apply to the developer and
 132 maintainer of the product, but not to the integrator or product user. A summary list of the requirements in this
 133 document can be found in Annex B.”

134 3 Modification to Clause 2, “Normative references”

135 *Replace the reference with the following:*

136 IEC 62443-2-4:2015,¹ *Security for industrial automation and control systems – Part 2-4: Security program*
 137 *requirements for IACS service providers*

**138 4 Modification to Clause 3, “Terms, definitions, abbreviated terms, acronyms and
139 conventions”****140 4.1 Modification to Subclause 3.1, “Terms and definitions”**

141 *Replace the 1st paragraph with the following:*

142 “For the purposes of this document, the terms and definitions given in IEC/TR 62443-1-2 [1] and the following
 143 apply.”

144 *Replace term entry 3.1.3 with the following:*

¹ As impacted by IEC 62443-2-4:2015/AMD1:2017.

- 145 **3.1.3**
 146 **access control**
 147 <process>
 148 process by which use of system resources is regulated according to a security policy and is permitted by only
 149 authorized product users according to that policy
- 150 Note 1 to entry: Access control includes identification and authentication requirements specified in other parts of the
 151 EN IEC 62443 series.
- 152 *Replace term entry 3.1.4 with the following:*
- 153 **3.1.4**
 154 **administrator**
 155 product user who has been authorized to manage security policies/capabilities for a product or system
- 156 *Replace Note 1 to entry in 3.1.5 with the following:*
- 157 Note 1 to entry: In this specific case, an asset is an object that is part of an ACS.
- 158 *Delete term entry 3.1.6 “asset owner”.*
- 159 *Replace the clause number for term entry “attack surface” to 3.1.6 from 3.1.7.*
- 160 *Replace the clause number of term entry “audit log” to 3.1.7 from 3.1.8.*
- 161 *Replace the clause number of term entry “authentication” to 3.1.8 from 3.1.9 and replace the notes to entry*
 162 *with the following:*
- 163 Note 1 to entry: Not all credentials used to authenticate an identity are created equally. The trustworthiness of the
 164 credential is determined by the configured authentication mechanism. Hardware or software-based mechanisms can force
 165 product users to prove their identity before accessing data on a device. A typical example is proving the identity of a user
 166 usually through an identity provider.
- 167 Note 2 to entry: Authentication includes verifying human product users as well as non-human product users such as
 168 devices or processes.
- 169 *Add the following term entry 3.1.9:*
- 170 **3.1.9**
 171 **authenticated security test**
 172 test which allows the tester to directly access products using remote administrative protocols such as secure
 173 shell (SSH) or remote desktop protocol (RDP) and to authenticate to the products using provided credentials
- 174 Note 1 to entry: Authenticated security tests provide a more thorough view and more detailed insights of the tested
 175 product compared to unauthenticated security tests. They can therefore identify additional vulnerabilities at the product
 176 which had not been detected by unauthorized security tests.
- 177 *Replace term entry 3.1.10 “automation solution” with the following:*
- 178 **3.1.10**
 179 **automation and control system**
 180 **ACS**
 181 collection of integrated components that provide functions for monitoring, controlling and managing the
 182 operation of equipment under control
- 183 *Add the following term entry 3.1.11*
- 184 **3.1.11**
 185 **automation and control system component**
 186 **ACS component**
 187 component developed and supported according to the secure development processes described in
 188 EN IEC 62443-4-1 and implementing the applicable technical requirements of EN IEC 62443-4-2
- 189 *Add the following term entry 3.1.12:*

EN IEC 62443-4-1:2018/prAA:2026 (E)**3.1.12****automation and control solution**

collection of people processes and automation and control systems with the purpose of monitoring, controlling and managing the operation of equipment under control

Note 1 to entry: An automation and control solution includes the instantiation of one or more automation and control systems.

Note 2 to entry: Automation and control solution is used as a proper noun in this part of the EN IEC 62443 series.

Note 3 to entry: The difference between the automation and control system and the automation and control solution is that the automation and control system is incorporated into the automation and control solution design (for example, a specific number of workstations, controllers and devices in a specific configuration), which is then implemented. The resulting configuration is referred to as the automation and control solution.

Note 4 to entry: The automation and control solution can be comprised of components from multiple suppliers including the product supplier of the automation and control system.

Replace the clause number of term entry “banned function” to 3.1.13 from 3.1.11.

Replace term entry 3.1.14 “best practices” with the following

3.1.14**best practices**

guidelines for securely designing, developing, verifying and validating, maintaining or retiring products that the supplier has determined are commonly recommended by both the security and industrial automation communities

EXAMPLE least privilege, economy of mechanism and least common mechanism

Replace term entry 3.1.13 “component” with the following:

3.1.15**component**

one of the parts that make up a product or system. A component may be hardware or software and may be subdivided into other components

Replace term entry 3.1.14 “configuration management” with the following:

3.1.16**configuration management**

discipline of identifying the components of an evolving system for the purposes of controlling changes to those components and maintaining continuity and traceability throughout the secure product development lifecycle

Add the following term entry 3.1.17:

3.1.17**cryptographic mechanism**

element of software or hardware that provides a cryptographic service, such as confidentiality, integrity, source authentication, and access control

Note 1 to entry: The cryptographic mechanism can be, for example, a set of cryptographic algorithms or a protocol utilizing cryptography.

Delete term entry 3.1.18 “externally provided component”.

Replace the clause number of term entry “defense in depth” to 3.1.18 from 3.1.15.

Replace the clause number of term entry “dependent component” to 3.1.19 from 3.1.16 and replace the example with the following:

EXAMPLE Java run time environment or a driver

Delete term entry 3.1.20 “industrial automation and control system”.

234 *Replace term entry 3.1.17 “deprecated function” with the following:*

235 **3.1.20**

236 **deprecated function**

237 software method that is supported but whose use is no longer recommended

238 *Add the following term entry 3.1.21:*

239 **3.1.21**

240 **equipment under control**

241 equipment, machinery, apparatus, or plant used for manufacturing, process, transportation, medical, or other
242 activities

243 [SOURCE: IEC 61508-4:2010]

244 *Add the following term entry 3.1.22:*

245 **3.1.22**

246 **essential function**

247 function or capability that is required to maintain health, safety, the environment and availability for the
248 equipment under control

249 Note 1 to entry: Essential functions include, but are not limited to, the safety instrumented function (SIF), the control
250 function and the ability of the operator to view and manipulate the equipment under control. The loss of essential functions
251 is commonly termed loss of protection, loss of control and loss of view respectively. In some industries additional functions
252 such as history may be considered essential.

253 *Replace the clause number of term entry “fuzz testing” to 3.1.23 from 3.1.19.*

254 *Add the following term entry 3.1.24:*

255 **3.1.24**

256 **information category**

257 logical grouping of information that shares a common purpose and set of security requirements

258 *Add the following term entry 3.1.25:*

259 **3.1.25**

260 **intended use**

261 use for which a product is designed by the product supplier, describing the explicit and implicit assumptions
262 about the product’s properties and capabilities

263 Note 1 to entry: The intended use does not describe specific product features, e.g. security update capability,
264 authentication mechanism.

265 EXAMPLE The intended use of a network switch is to switch network traffic in an enterprise environment used by skilled
266 persons.

267 *Replace term entry 3.1.22 “product” with the following:*

268 **3.1.26**

269 **product**

270 system, subsystem or component that is manufactured, developed or refined

271 Note 1 to entry: in the context of EN IEC 62443-3-3 [4] a product is an automation and control system (ACS)

272 Note 2 to entry: in the context of EN IEC 62443-4-2 [5] a product is an ACS component

273 *Replace term entry 3.1.23 “configuration management” with the following:*

274 **3.1.27**

275 **product security context**

276 security provided to the product by the environment (product user deployment) in which the product is
277 intended to be used

EN IEC 62443-4-1:2018/prAA:2026 (E)

278 Note 1 to entry: The security provided to the product by its intended environment can effectively restrict the threats that are
279 applicable to the product.

280 Note 2 to entry: The product security context is derived from the intended use.

281 *Add the following term entry 3.1.28:*

3.1.28**product security context category**

284 structural categorization describing the product security context through different factors to support
285 comparable assumptions about the product's security context

286 *Add the following term entry 3.1.29:*

3.1.29**product security incident**

289 security compromise that has a measurable impact on the product user, or an attempted compromise that, if
290 successful, would have resulted in a measurable impact on the product user

291 *Replace the clause number of term entry "product supplier" to 3.1.30 from 3.1.24.*

292 *Replace term entry 3.1.25 "product users" with the following:*

3.1.31**product user**

295 user of the hardware and/or software product including administrator, integrator and maintenance personnel,
296 and vendor of other components or products that reuse or contain this product

297 *Replace the clause number of term entry "record" to 3.1.32 from 3.1.26.*

298 *Replace the clause number of term entry "regression" to 3.1.33 from 3.1.27.*

299 *Add the following term entry 3.1.34:*

3.1.34**review**

302 activity undertaken to determine the suitability, adequacy and effectiveness of the subject matter to achieve
303 established objectives

304 [SOURCE: ISO 31073:2022, 3.3.41]

305 *Replace the clause number of term entry "root cause" to 3.1.35 from 3.1.28.*

306 *Add the following term entry 3.1.36:*

3.1.36**secure by default**

309 state of the product being securely configured upon installation or deployment according to its intended use
310 and product security context

311 *Replace the clause number of term entry "security defect" to 3.1.37 from 3.1.29.*

312 *Replace term entry 3.1.30 "security advisor" with the following:*

3.1.38**security advisor**

315 organizational role to guide team in the process of the SDL (Security Development Lifecycle)

316 Note 1 to entry: Security advisor may be part of the project team or may be consultant to the team to provide guidance
317 and assistance where required.

318 *Replace the clause number of term entry "security-related issue" to 3.1.39 from 3.1.32 and add the following
319 example:*

320 EXAMPLE A product vulnerability is a type of security-related issue.

321 *Add the following term entry 3.1.40:*

- 322 **3.1.40**
 323 **security support period**
 324 period during which a product supplier ensures that security support processes are active and security issues
 325 in the product are handled
- 326 Note 1 to entry: The length and obligations of security support can be pre-determined by regulatory or contractual terms.
- 327 *Add the following term entry 3.1.41:*
- 328 **3.1.41**
 329 **security test grade**
 330 **STG**
 331 defined set of security test modules.
- 332 Note 1 to entry: Security test grades are STG-1, STG-2, STG-3, and STG-4.
- 333 *Add the following term entry 3.1.42:*
- 334 **3.1.42**
 335 **security test module**
 336 **STM**
 337 specification of a security testing activity, describing the aim of the security test, the testing methodology and
 338 acceptance criteria.
- 339 *Replace term entry 3.1.21 “patch management” with the following:*
- 340 **3.1.43**
 341 **security update management**
 342 area of systems management that involves acquiring, testing and installing software security updates (code
 343 changes) to a product
- 344 Note 1 to entry: See IEC/TR 62443-2-3 [2] for additional information.
- 345 Note 2 to entry: Security update management also applies to the process of keeping included 3rd party libraries current
 346 before releasing a product.
- 347 *Replace term entry 3.1.33 “security-related issue” with the following:*
- 348 **3.1.44**
 349 **security verification and validation testing**
 350 testing performed to assess the overall security of a component or product when used in its intended product
 351 security context and to determine if a component or product satisfies the product security requirements and
 352 satisfies its designed security purpose
- 353 Note 1 to entry: Security verification testing supplements security validation testing with additional testing focused on the
 354 product security context and defence in depth strategy
- 355 *Add the following term entry 3.1.45:*
- 356 **3.1.45**
 357 **software bill of materials (SBOM)**
 358 information in a structured format that allows the exchange of information for a software package, which might
 359 usefully include name, version, origin, license, copyright and known vulnerabilities in a manner useful to third
 360 parties
- 361 [SOURCE: ISO/IEC 18974:2023(en), 3.12, modified — a reference to SPDX as possible format was removed]
- 362 *Add the following term entry 3.1.46:*
- 363 **3.1.46**
 364 **supporting measure**
 365 functions and procedures external to the product to support the implementation of the product security
 366 requirements
- 367 Note 1 to entry: Functions are e.g. provided by the underlying software or hardware.

EN IEC 62443-4-1:2018/prAA:2026 (E)

368 Note 2 to entry: Procedures have e.g. the aim to ensure physical protection.

369 *Add the following term entry 3.1.47:*

3.1.47**system**

372 interacting, interrelated, or interdependent elements forming a complex whole

373 *Replace the clause number of term entry “system integrator” to 3.1.48 from 3.1.34.*

374 *Add the following term entry 3.1.49:*

3.1.49**test**

377 activity in which a system or component is executed under specified conditions, the results are observed or
378 recorded, and an evaluation is made of some aspect of the system or component

379 Note 1 to entry: A test is carried out to measure or classify a characteristic or a property of an item by applying to the item
380 a set of environmental and operating conditions and/or requirements.

381 [SOURCE: ISO/IEC/IEEE 29119-2:2021, 3.21]

382 *Add the following term entry 3.1.50:*

3.1.50**third-party component**

385 component included in a product that is developed and maintained by a third-party supplier.

386 Note 1 to entry: This includes components which are specifically developed by a third-party supplier for the product
387 supplier.

388 *Replace term entry 3.1.35 “third-party supplier” with the following:*

3.1.51**third-party supplier**

391 organization independent of the product supplier organization

392 Note 1 to entry: A third-party supplier can also mean a different legal entity of the corporation the product supplier
393 organization belongs to.

394 *Replace the clause number of term entry “threat” to 3.1.52 from 3.1.36.*

395 *Replace the clause number of term entry “threat modelling” to 3.1.53 from 3.1.37.*

396 *Add the following term entry 3.1.54:*

3.1.54**threat scenario**

399 description of how a threat, exploiting one or more vulnerabilities could trigger an incident leading to adverse
400 impact

401 *Replace the clause number of term entry “trust boundary” to 3.1.55 from 3.1.38.*

402 *Add the following term entry 3.1.56:*

3.1.56**unauthenticated security test**

405 unauthenticated security tests are security tests performed without any authentication at the tested products.

406 *Replace term entry 3.1.39 “unit testing” with the following:.*

3.1.57**unit testing**

409 verification that an individual unit of computer software or hardware performs as intended

410 Note 1 to entry: Automated verification, or testing, is generally performed by computer test software.

411 Note 2 to entry: What constitutes a unit of source code is a design decision. A unit is often designed as the smallest
 412 testable part of an application. It may include one or more computer program modules and may also include associated
 413 control data, usage procedures and operating procedures. In procedural programming, a unit could be an entire module
 414 but is more commonly an individual function or procedure. In object-oriented programming, a unit is often an entire
 415 interface, such as a class, but could be an individual method.

416 *Replace the clause number of term entry “user” to 3.1.58 from 3.1.40.*

417 *Replace the clause number of term entry “zone” to 3.1.59 from 3.1.41.*

418 **4.2 Modification to Subclause 3.2, “Abbreviated terms and acronyms”**

419 *Replace the list of abbreviated terms and acronyms with the following:*

ACL	Access control list
ACS	Automation control system
CMMI	Capability maturity model integration
CMMI-DEV	Capability maturity model integration for development
CMU	Carnegie Mellon University
COTS	Commercial off the shelf
CVSS	Common vulnerability scoring system
DAST	Dynamic application security testing
DM	Defect management
FDIS	Final Draft International Standard
HTTP	Hypertext transfer protocol
IEC	International Electrotechnical Commission
ISA	International Society of Automation
ISO	International Organization for Standardization
MIN	Minimum
OWASP	Open Web Application Security Project
QA	Quality assurance
SAST	Static Application Security Testing
SL-C	Capability Security Level
SD	Secure Design
SDL	Security development lifecycle
SDLA	Secure Development Lifecycle Assessment
SEI	Software Engineering Institute
SG	Security guidelines
SI	Secure implementation
SL	Security level
SL-C	Capability security level
SM	Security management
SR	Security requirements
STG	Security test grade