
**Zaščita za sisteme industrijske avtomatizacije in nadzornih sistemov - 4-2. del:
Zahteve za tehnično varnost zaščito za IACS komponente (IEC 62443-4-2:2019)**

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

Industrielle Kommunikationsnetze – IT-Sicherheit für industrielle Automatisierungssysteme – Teil 4-2: Anforderungen an Komponenten industrieller Automatisierungssysteme (IEC 62443-4-2:2019)

(standards.iteh.ai)

Sécurité des systèmes d'automatisation et de commande industrielles - Partie 4-2: Exigences de sécurité technique des composants IACS (IEC 62443-4-2:2019)

<https://standards.iteh.ai/catalog/standards/sist/81f98b69-24f5-490a-89d7-f6d7358e978e/sist-en-iec-62443-4-2-2019>

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

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

en,fr,de

iTeh STANDARD PREVIEW
(standards.iteh.ai)

SIST EN IEC 62443-4-2:2019

<https://standards.iteh.ai/catalog/standards/sist/81f98b69-24f5-490a-89d7-f6d7358e978e/sist-en-iec-62443-4-2-2019>

EUROPEAN STANDARD

EN IEC 62443-4-2

NORME EUROPÉENNE

EUROPÄISCHE NORM

April 2019

ICS 25.040.40; 35.030

English Version

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

Industrielle Kommunikationsnetze – IT-Sicherheit für
industrielle Automatisierungssysteme – Teil 4-2:
Anforderungen an Komponenten industrieller
Automatisierungssysteme
(IEC 62443-4-2:2019)

Sécurité des systèmes d'automatisation et de commande
industrielles - Partie 4-2: Exigences de sécurité technique
des composants IACS
(IEC 62443-4-2:2019)

This European Standard was approved by CENELEC on 2019-04-03. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CENELEC member.

This European Standard exists 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.

[SIST EN IEC 62443-4-2:2019](https://standards.iteh.ai/catalog/standards/sist/81f98b69-24f5-490a-89d7-)

<https://standards.iteh.ai/catalog/standards/sist/81f98b69-24f5-490a-89d7->

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



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

EN IEC 62443-4-2:2019 (E)**European foreword**

The text of document 65/735/FDIS, future edition 1 of IEC 62443-4-2, prepared by IEC/TC 65 "Industrial-process measurement, control and automation" was submitted to the IEC-CENELEC parallel vote and approved by CENELEC as EN IEC 62443-4-2:2019.

The following dates are fixed:

- latest date by which the document has to be implemented at national level by publication of an identical national standard or by endorsement (dop) 2020-01-03
- latest date by which the national standards conflicting with the document have to be withdrawn (dow) 2022-04-03

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

iTeh STANDARD PREVIEW
Endorsement notice
(standards.iteh.ai)

The text of the International Standard IEC 62443-4-2:2019 was approved by CENELEC as a European Standard without any modification.

In the official version, for Bibliography, the following notes have to be added for the standards indicated:

ISO/IEC 27002:2013 NOTE Harmonized as EN ISO/IEC 27002:2017 (not modified)
IEC 62264-1 NOTE Harmonized as EN 62264-1
IEC 62443-3-2 NOTE Harmonized as EN 62443-3-2¹

¹ Under preparation. Stage at time of publication: prEN 62443-3-2:2018.

Annex ZA (normative)

Normative references to international publications with their corresponding European publications

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.

NOTE 1 Where an International Publication has been modified by common modifications, indicated by (mod), the relevant EN/HD applies.

NOTE 2 Up-to-date information on the latest versions of the European Standards listed in this annex is available here: www.cenelec.eu.

<u>Publication</u>	<u>Year</u>	<u>Title</u>	<u>EN/HD</u>	<u>Year</u>
IEC/TS 62443-1-1	-	Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models	--	-
IEC 62443-3-3	2013	Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels	--	-
IEC 62443-4-1	-	Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements	EN IEC 62443-4-1 -	-

iTeh STANDARD PREVIEW
(standards.iteh.ai)

SIST EN IEC 62443-4-2:2019

<https://standards.iteh.ai/catalog/standards/sist/81f98b69-24f5-490a-89d7-f6d7358e978e/sist-en-iec-62443-4-2-2019>



IEC 62443-4-2

Edition 1.0 2019-02

INTERNATIONAL STANDARD

NORME INTERNATIONALE



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

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

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 25.040.40; 35.030

ISBN 978-2-8322-6597-0

**Warning! Make sure that you obtained this publication from an authorized distributor.
Attention! Veuillez vous assurer que vous avez obtenu cette publication via un distributeur agréé.**

CONTENTS

FOREWORD.....	12
INTRODUCTION.....	14
1 Scope.....	17
2 Normative references	17
3 Terms, definitions, abbreviated terms, acronyms, and conventions.....	18
3.1 Terms and definitions.....	18
3.2 Abbreviated terms and acronyms	24
3.3 Conventions.....	26
4 Common component security constraints.....	27
4.1 Overview.....	27
4.2 CCSC 1: Support of essential functions	27
4.3 CCSC 2: Compensating countermeasures	27
4.4 CCSC 3: Least privilege.....	27
4.5 CCSC 4: Software development process.....	27
5 FR 1 – Identification and authentication control	27
5.1 Purpose and SL-C(IAC) descriptions.....	27
5.2 Rationale	28
5.3 CR 1.1 – Human user identification and authentication	28
5.3.1 Requirement.....	28
5.3.2 Rationale and supplemental guidance.....	28
5.3.3 Requirement enhancements	28
5.3.4 Security levels.....	29
5.4 CR 1.2 – Software process and device identification and authentication	29
5.4.1 Requirement.....	29
5.4.2 Rationale and supplemental guidance.....	29
5.4.3 Requirement enhancements	29
5.4.4 Security levels	30
5.5 CR 1.3 – Account management.....	30
5.5.1 Requirement.....	30
5.5.2 Rationale and supplemental guidance.....	30
5.5.3 Requirement enhancements	30
5.5.4 Security levels	30
5.6 CR 1.4 – Identifier management.....	30
5.6.1 Requirement.....	30
5.6.2 Rationale and supplemental guidance.....	30
5.6.3 Requirement enhancements	31
5.6.4 Security levels	31
5.7 CR 1.5 – Authenticator management.....	31
5.7.1 Requirement.....	31
5.7.2 Rationale and supplemental guidance.....	31
5.7.3 Requirement enhancements	32
5.7.4 Security levels	32
5.8 CR 1.6 – Wireless access management	32

5.9	CR 1.7 – Strength of password-based authentication	32
5.9.1	Requirement	32
5.9.2	Rationale and supplemental guidance	32
5.9.3	Requirement enhancements	32
5.9.4	Security levels	33
5.10	CR 1.8 – Public key infrastructure certificates	33
5.10.1	Requirement	33
5.10.2	Rationale and supplemental guidance	33
5.10.3	Requirement enhancements	33
5.10.4	Security levels	33
5.11	CR 1.9 – Strength of public key-based authentication	34
5.11.1	Requirement	34
5.11.2	Rationale and supplemental guidance	34
5.11.3	Requirement enhancements	35
5.11.4	Security levels	35
5.12	CR 1.10 – Authenticator feedback	35
5.12.1	Requirement	35
5.12.2	Rationale and supplemental guidance	35
5.12.3	Requirement enhancements	35
5.12.4	Security levels	35
5.13	CR 1.11 – Unsuccessful login attempts	35
5.13.1	Requirement	35
5.13.2	Rationale and supplemental guidance	36
5.13.3	Requirement enhancements	36
5.13.4	Security levels	36
5.14	CR 1.12 – System use notification	36
5.14.1	Requirement	36
5.14.2	Rationale and supplemental guidance	36
5.14.3	Requirement enhancements	36
5.14.4	Security levels	37
5.15	CR 1.13 – Access via untrusted networks	37
5.16	CR 1.14 – Strength of symmetric key-based authentication	37
5.16.1	Requirement	37
5.16.2	Rationale and supplemental guidance	37
5.16.3	Requirement enhancements	37
5.16.4	Security levels	38
6	FR 2 – Use control	38
6.1	Purpose and SL-C(UC) descriptions	38
6.2	Rationale	38
6.3	CR 2.1 – Authorization enforcement	38
6.3.1	Requirement	38
6.3.2	Rationale and supplemental guidance	38
6.3.3	Requirement enhancements	39
6.3.4	Security levels	39
6.4	CR 2.2 – Wireless use control	40
6.4.1	Requirement	40
6.4.2	Rationale and supplemental guidance	40
6.4.3	Requirement enhancements	40
6.4.4	Security levels	40

6.5	CR 2.3 – Use control for portable and mobile devices	40
6.6	CR 2.4 – Mobile code.....	40
6.7	CR 2.5 – Session lock.....	40
6.7.1	Requirement.....	40
6.7.2	Rationale and supplemental guidance.....	41
6.7.3	Requirement enhancements	41
6.7.4	Security levels	41
6.8	CR 2.6 – Remote session termination	41
6.8.1	Requirement.....	41
6.8.2	Rationale and supplemental guidance.....	41
6.8.3	Requirement enhancements	41
6.8.4	Security levels	41
6.9	CR 2.7 – Concurrent session control.....	41
6.9.1	Requirement.....	41
6.9.2	Rationale and supplemental guidance.....	42
6.9.3	Requirement enhancements	42
6.9.4	Security levels	42
6.10	CR 2.8 – Auditable events	42
6.10.1	Requirement.....	42
6.10.2	Rationale and supplemental guidance.....	42
6.10.3	Requirement enhancements	42
6.10.4	Security levels	43
6.11	CR 2.9 – Audit storage capacity.....	43
6.11.1	Requirement.....	43
6.11.2	Rationale and supplemental guidance.....	43
6.11.3	Requirement enhancements	43
6.11.4	Security levels	43
6.12	CR 2.10 – Response to audit processing failures	43
6.12.1	Requirement.....	43
6.12.2	Rationale and supplemental guidance.....	44
6.12.3	Requirement enhancements	44
6.12.4	Security levels	44
6.13	CR 2.11 – Timestamps.....	44
6.13.1	Requirement.....	44
6.13.2	Rationale and supplemental guidance.....	44
6.13.3	Requirement enhancements	44
6.13.4	Security levels	44
6.14	CR 2.12 – Non-repudiation.....	45
6.14.1	Requirement.....	45
6.14.2	Rationale and supplemental guidance.....	45
6.14.3	Requirement enhancements	45
6.14.4	Security levels	45
6.15	CR 2.13 – Use of physical diagnostic and test interfaces	45
7	FR 3 – System integrity	45
7.1	Purpose and SL-C(SI) descriptions	45
7.2	Rationale	46

7.3	CR 3.1 – Communication integrity	46
7.3.1	Requirement	46
7.3.2	Rationale and supplemental guidance	46
7.3.3	Requirement enhancements	47
7.3.4	Security levels	47
7.4	CR 3.2 – Protection from malicious code	47
7.5	CR 3.3 – Security functionality verification	47
7.5.1	Requirement	47
7.5.2	Rationale and supplemental guidance	47
7.5.3	Requirement enhancements	47
7.5.4	Security levels	48
7.6	CR 3.4 – Software and information integrity	48
7.6.1	Requirement	48
7.6.2	Rationale and supplemental guidance	48
7.6.3	Requirement enhancements	48
7.6.4	Security levels	48
7.7	CR 3.5 – Input validation	48
7.7.1	Requirement	48
7.7.2	Rationale and supplemental guidance	49
7.7.3	Requirement enhancements	49
7.7.4	Security levels	49
7.8	CR 3.6 – Deterministic output	49
7.8.1	Requirement	49
7.8.2	Rationale and supplemental guidance	49
7.8.3	Requirement enhancements	49
7.8.4	Security levels	50
7.9	CR 3.7 – Error handling	50
7.9.1	Requirement	50
7.9.2	Rationale and supplemental guidance	50
7.9.3	Requirement enhancements	50
7.9.4	Security levels	50
7.10	CR 3.8 – Session integrity	50
7.10.1	Requirement	50
7.10.2	Rationale and supplemental guidance	51
7.10.3	Requirement enhancements	51
7.10.4	Security levels	51
7.11	CR 3.9 – Protection of audit information	51
7.11.1	Requirement	51
7.11.2	Rationale and supplemental guidance	51
7.11.3	Requirement enhancements	51
7.11.4	Security levels	51
7.12	CR 3.10 – Support for updates	52
7.13	CR 3.11 – Physical tamper resistance and detection	52
7.14	CR 3.12 – Provisioning product supplier roots of trust	52
7.15	CR 3.13 – Provisioning asset owner roots of trust	52
7.16	CR 3.14 – Integrity of the boot process	52
8	FR 4 – Data confidentiality	52
8.1	Purpose and SL-C(DC) descriptions	52
8.2	Rationale	52

8.3	CR 4.1 – Information confidentiality	52
8.3.1	Requirement	52
8.3.2	Rationale and supplemental guidance	53
8.3.3	Requirement enhancements	53
8.3.4	Security levels	53
8.4	CR 4.2 – Information persistence	53
8.4.1	Requirement	53
8.4.2	Rationale and supplemental guidance	53
8.4.3	Requirement enhancements	53
8.4.4	Security levels	54
8.5	CR 4.3 – Use of cryptography	54
8.5.1	Requirement	54
8.5.2	Rationale and supplemental guidance	54
8.5.3	Requirement enhancements	54
8.5.4	Security levels	54
9	FR 5 – Restricted data flow	55
9.1	Purpose and SL-C(RDF) descriptions	55
9.2	Rationale	55
9.3	CR 5.1 – Network segmentation	55
9.3.1	Requirement	55
9.3.2	Rationale and supplemental guidance	55
9.3.3	Requirement enhancements	56
9.3.4	Security levels	56
9.4	CR 5.2 – Zone boundary protection	56
9.5	CR 5.3 – General-purpose person-to-person communication restrictions	56
9.6	CR 5.4 – Application partitioning	56
10	FR 6 – Timely response to events	56
10.1	Purpose and SL-C(TRE) descriptions	56
10.2	Rationale	57
10.3	CR 6.1 – Audit log accessibility	57
10.3.1	Requirement	57
10.3.2	Rationale and supplemental guidance	57
10.3.3	Requirement enhancements	57
10.3.4	Security levels	57
10.4	CR 6.2 – Continuous monitoring	57
10.4.1	Requirement	57
10.4.2	Rationale and supplemental guidance	57
10.4.3	Requirement enhancements	58
10.4.4	Security levels	58
11	FR 7 – Resource availability	58
11.1	Purpose and SL-C(RA) descriptions	58
11.2	Rationale	58
11.3	CR 7.1 – Denial of service protection	59
11.3.1	Requirement	59
11.3.2	Rationale and supplemental guidance	59
11.3.3	Requirement enhancements	59
11.3.4	Security levels	59

11.4	CR 7.2 – Resource management	59
11.4.1	Requirement.....	59
11.4.2	Rationale and supplemental guidance.....	59
11.4.3	Requirement enhancements	59
11.4.4	Security levels	59
11.5	CR 7.3 – Control system backup	60
11.5.1	Requirement.....	60
11.5.2	Rationale and supplemental guidance.....	60
11.5.3	Requirement enhancements	60
11.5.4	Security levels	60
11.6	CR 7.4 – Control system recovery and reconstitution	60
11.6.1	Requirement.....	60
11.6.2	Rationale and supplemental guidance.....	60
11.6.3	Requirement enhancements	60
11.6.4	Security levels	61
11.7	CR 7.5 – Emergency power	61
11.8	CR 7.6 – Network and security configuration settings.....	61
11.8.1	Requirement.....	61
11.8.2	Rationale and supplemental guidance.....	61
11.8.3	Requirement enhancements	61
11.8.4	Security levels	61
11.9	CR 7.7 – Least functionality	61
11.9.1	Requirement.....	61
11.9.2	Rationale and supplemental guidance.....	61
11.9.3	Requirement enhancements	62
11.9.4	Security levels	62
11.10	CR 7.8 – Control system component inventory.....	62
11.10.1	Requirement.....	62
11.10.2	Rationale and supplemental guidance.....	62
11.10.3	Requirement enhancements	62
11.10.4	Security levels	62
12	Software application requirements	62
12.1	Purpose	62
12.2	SAR 2.4 – Mobile code	62
12.2.1	Requirement.....	62
12.2.2	Rationale and supplemental guidance.....	63
12.2.3	Requirement enhancements	63
12.2.4	Security levels	63
12.3	SAR 3.2 – Protection from malicious code	63
12.3.1	Requirement.....	63
12.3.2	Rationale and supplemental guidance.....	63
12.3.3	Requirement enhancements	63
12.3.4	Security levels	63
13	Embedded device requirements.....	64
13.1	Purpose	64
13.2	EDR 2.4 – Mobile code	64
13.2.1	Requirement.....	64
13.2.2	Rationale and supplemental guidance.....	64
13.2.3	Requirement enhancements	64

13.2.4	Security levels	64
13.3	EDR 2.13 – Use of physical diagnostic and test interfaces	64
13.3.1	Requirement	64
13.3.2	Rationale and supplemental guidance	65
13.3.3	Requirement enhancements	65
13.3.4	Security levels	65
13.4	EDR 3.2 – Protection from malicious code	65
13.4.1	Requirement	65
13.4.2	Rationale and supplemental guidance	65
13.4.3	Requirement enhancements	66
13.4.4	Security levels	66
13.5	EDR 3.10 – Support for updates	66
13.5.1	Requirement	66
13.5.2	Rationale and supplemental guidance	66
13.5.3	Requirement enhancements	66
13.5.4	Security levels	66
13.6	EDR 3.11 – Physical tamper resistance and detection	66
13.6.1	Requirement	66
13.6.2	Rationale and supplemental guidance	66
13.6.3	Requirement enhancements	67
13.6.4	Security levels	67
13.7	EDR 3.12 – Provisioning product supplier roots of trust	67
13.7.1	Requirement	67
13.7.2	Rationale and supplemental guidance	67
13.7.3	Requirement enhancements	67
13.7.4	Security levels	68
13.8	EDR 3.13 – Provisioning asset owner roots of trust	68
13.8.1	Requirement	68
13.8.2	Rationale and supplemental guidance	68
13.8.3	Requirement enhancements	68
13.8.4	Security levels	68
13.9	EDR 3.14 – Integrity of the boot process	69
13.9.1	Requirement	69
13.9.2	Rationale and supplemental guidance	69
13.9.3	Requirement enhancements	69
13.9.4	Security levels	69
14	Host device requirements	69
14.1	Purpose	69
14.2	HDR 2.4 – Mobile code	69
14.2.1	Requirement	69
14.2.2	Rationale and supplemental guidance	70
14.2.3	Requirement enhancements	70
14.2.4	Security levels	70
14.3	HDR 2.13 – Use of physical diagnostic and test interfaces	70
14.3.1	Requirement	70
14.3.2	Rationale and supplemental guidance	70
14.3.3	Requirement enhancements	71
14.3.4	Security levels	71
14.4	HDR 3.2 – Protection from malicious code	71

14.4.1	Requirement.....	71
14.4.2	Rationale and supplemental guidance.....	71
14.4.3	Requirement enhancements	71
14.4.4	Security levels	71
14.5	HDR 3.10 – Support for updates	71
14.5.1	Requirement.....	71
14.5.2	Rationale and supplemental guidance.....	71
14.5.3	Requirement enhancements	72
14.5.4	Security levels	72
14.6	HDR 3.11 – Physical tamper resistance and detection	72
14.6.1	Requirement.....	72
14.6.2	Rationale and supplemental guidance.....	72
14.6.3	Requirement enhancements	72
14.6.4	Security levels	72
14.7	HDR 3.12 – Provisioning product supplier roots of trust	73
14.7.1	Requirement.....	73
14.7.2	Rationale and supplemental guidance.....	73
14.7.3	Requirement enhancements	73
14.7.4	Security levels	73
14.8	HDR 3.13 – Provisioning asset owner roots of trust.....	73
14.8.1	Requirement.....	73
14.8.2	Rationale and supplemental guidance.....	73
14.8.3	Requirement enhancements	74
14.8.4	Security levels	74
14.9	HDR 3.14 – Integrity of the boot process.....	74
14.9.1	Requirement.....	74
14.9.2	Rationale and supplemental guidance.....	74
14.9.3	Requirement enhancements	74
14.9.4	Security levels	75
15	Network device requirements.....	75
15.1	Purpose	75
15.2	NDR 1.6 – Wireless access management.....	75
15.2.1	Requirement.....	75
15.2.2	Rationale and supplemental guidance.....	75
15.2.3	Requirement enhancements	75
15.2.4	Security levels	75
15.3	NDR 1.13 – Access via untrusted networks	75
15.3.1	Requirement.....	75
15.3.2	Rationale and supplemental guidance.....	76
15.3.3	Requirement enhancements	76
15.3.4	Security levels	76
15.4	NDR 2.4 – Mobile code	76
15.4.1	Requirement.....	76
15.4.2	Rationale and supplemental guidance.....	76
15.4.3	Requirement enhancements	77
15.4.4	Security levels	77
15.5	NDR 2.13 – Use of physical diagnostic and test interfaces.....	77
15.5.1	Requirement.....	77
15.5.2	Rationale and supplemental guidance.....	77