



BSI Standards Publication

Security for industrial automation and control systems

Part 4-2: Technical security requirements for IACS components

National foreword

This British Standard is the UK implementation of EN IEC 62443-4-2:2019. It is identical to IEC 62443-4-2:2019.

The UK participation in its preparation was entrusted to Technical Committee GEL/65, Measurement and control.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2019
Published by BSI Standards Limited 2019

ISBN 978 0 580 93650 0

ICS 35.030; 25.040.40

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 May 2019.

Amendments/corrigenda issued since publication

Date	Text affected
------	---------------

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.

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

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.

Endorsement notice

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 -	-

This page deliberately left blank

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

15.5.3	Requirement enhancements	77
15.5.4	Security levels	78
15.6	NDR 3.2 – Protection from malicious code	78
15.6.1	Requirement	78
15.6.2	Rationale and supplemental guidance	78
15.6.3	Requirement enhancements	78
15.6.4	Security levels	78
15.7	NDR 3.10 – Support for updates	78
15.7.1	Requirement	78
15.7.2	Rationale and supplemental guidance	78
15.7.3	Requirement enhancements	78
15.7.4	Security levels	79
15.8	NDR 3.11 – Physical tamper resistance and detection	79
15.8.1	Requirement	79
15.8.2	Rationale and supplemental guidance	79
15.8.3	Requirement enhancements	79
15.8.4	Security levels	79
15.9	NDR 3.12 – Provisioning product supplier roots of trust	79
15.9.1	Requirement	79
15.9.2	Rationale and supplemental guidance	80
15.9.3	Requirement enhancements	80
15.9.4	Security levels	80
15.10	NDR 3.13 – Provisioning asset owner roots of trust	80
15.10.1	Requirement	80
15.10.2	Rationale and supplemental guidance	80
15.10.3	Requirement enhancements	81
15.10.4	Security levels	81
15.11	NDR 3.14 – Integrity of the boot process	81
15.11.1	Requirement	81
15.11.2	Rationale and supplemental guidance	81
15.11.3	Requirement enhancements	81
15.11.4	Security levels	82
15.12	NDR 5.2 – Zone boundary protection	82
15.12.1	Requirement	82
15.12.2	Rationale and supplemental guidance	82
15.12.3	Requirement enhancements	82
15.12.4	Security levels	82
15.13	NDR 5.3 – General purpose, person-to-person communication restrictions	83
15.13.1	Requirement	83
15.13.2	Rationale and supplemental guidance	83
15.13.3	Requirement enhancements	83
15.13.4	Security levels	83
Annex A	(informative) Device categories	84
A.1	General	84
A.2	Device category: embedded device	84
A.2.1	Programmable logic controller (PLC)	84
A.2.2	Intelligent electronic device (IED)	84

A.3	Device category: network device	85
A.3.1	Switch	85
A.3.2	Virtual private network (VPN) terminator	85
A.4	Device category: host device/application	85
A.4.1	Operator workstation	85
A.4.2	Data historian	86
Annex B (informative)	Mapping of CRs and REs to FR SLs 1-4	87
B.1	Overview	87
B.2	SL mapping table	87
Bibliography		93
Figure 1	– Parts of the IEC 62443 series	16
Table B.1	– Mapping of CRs and REs to FR SL levels 1-4	88

INTERNATIONAL ELECTROTECHNICAL COMMISSION

SECURITY FOR INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS –**Part 4-2: Technical security requirements for IACS components****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 62443-4-2 has been prepared by IEC technical committee 65: Industrial-process measurement, control and automation.

The text of this International Standard is based on the following documents:

FDIS	Report on voting
65/735/FDIS	65/740/RVD

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

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

A list of all parts in the IEC 62443 series, published under the general title *Security for industrial automation and control systems*, can be found on the IEC website.

Future standards in this series will carry the new general title as cited above. Titles of existing standards in this series will be updated at the time of the next edition.

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

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

INTRODUCTION

0.1 Overview

Industrial automation and control system (IACS) organizations increasingly use commercial-off-the-shelf (COTS) networked devices that are inexpensive, efficient and highly automated. Control systems are also increasingly interconnected with non-IACS networks for valid business reasons. These devices, open networking technologies and increased connectivity provide an increased opportunity for cyber-attack against control system hardware and software. That weakness may lead to health, safety and environmental (HSE), financial and/or reputational consequences in deployed control systems.

Organizations choosing to deploy business information technology (IT) cyber security solutions to address IACS security may not fully comprehend the results of their decision. While many business IT applications and security solutions can be applied to IACS, they should be applied in an appropriate way to eliminate inadvertent consequences. For this reason, the approach used to define system requirements is based on a combination of functional requirements and risk assessment, often including an awareness of operational issues as well.

IACS security countermeasures should not have the potential to cause loss of essential services and functions, including emergency procedures (IT security countermeasures, as often deployed, do have this potential). IACS security goals focus on control system availability, plant protection, plant operations (even in a degraded mode) and time-critical system response. IT security goals often do not place the same emphasis on these factors; they may be more concerned with protecting information rather than physical assets. These different goals should be clearly stated as security objectives regardless of the degree of plant integration achieved. A key step in the risk assessment, as required by IEC 62443-2-1¹ [1]², should be the identification of which services and functions are truly essential for operations (for example, in some facilities engineering support may be determined to be a non-essential service or function). In some cases, it may be acceptable for a security action to cause temporary loss of a non-essential service or function, unlike an essential service or function that should not be adversely affected.

This document provides the cyber security technical requirements for the components that make up an IACS, specifically the embedded devices, network components, host components and software applications. Annex A describes categories of devices commonly used in IACSs. This document derives its requirements from the IACS system security requirements described in IEC 62443-3-3. The intent of this document is to specify security capabilities that enable a component to mitigate threats for a given security level (SL) without the assistance of compensating countermeasures. Annex B provides a table that summarizes the SLs of each of the requirements and requirement enhancements defined in this document.

The primary goal of the IEC 62443 series is to provide a flexible framework that facilitates addressing current and future vulnerabilities in IACS and applying necessary mitigations in a systematic, defensible manner. It is important to understand that the intention of the IEC 62443 series is to build extensions to enterprise security that adapt the requirements for business IT systems and combines them with the unique requirements for strong integrity and availability needed by IACS.

¹ Many documents in the IEC 62443 series are currently under review or in development.

² Numbers in square brackets refer to the bibliography.

0.2 Purpose and intended audience

The IACS community audience for this document is intended to be asset owners, system integrators, product suppliers, and, where appropriate, compliance authorities. Compliance authorities include government agencies and regulators with the legal authority to perform audits to verify compliance with governing laws and regulations.

System integrators will use this document to assist them in procuring control system components that make up an IACS solution. The assistance will be in the form of helping system integrators specify the appropriate security capability level of the individual components they require. The primary standards for system integrators are IEC 62443-2-1 [1], IEC 62443-2-4 [3], IEC 62443-3-2 [5]³ and IEC 62443-3-3 that provide organizational and operational requirements for a security management system and guide them through the process of defining security zones for a system and the target security capability levels (SL-T) for those zones. Once the SL-T for each zone has been defined, components that provide the necessary security capabilities can be used to achieve the SL-T for each zone.

Product suppliers will use this document to understand the requirements placed on control system components for specific security capability levels (SL-C) of those components. A component may not provide a required capability itself but may be designed to integrate with a higher-level entity and thus benefit from that entity's capability – for example an embedded device may not be maintaining a user directory itself, but may integrate with a system wide authentication and authorization service and thus still meet the requirements to provide individual user authentication, authorization and management capabilities. This document will guide product suppliers as to which requirements can be allocated and which requirements should be native in the components. As defined in Practice 8 of IEC 62443-4-1, the product supplier will provide documentation on how to properly integrate the component into a system to meet a specific SL-T.

The component requirements (CRs) in this document are derived from the system requirements (SRs) in IEC 62443-3-3. The requirements in IEC 62443-3-3 are referred to as SRs, which are derived from the overall foundational requirements (FRs) defined in IEC 62443-1-1. CRs may also include a set of requirement enhancements (REs). The combination of CRs and REs is what will determine the target security level that a component is capable of.

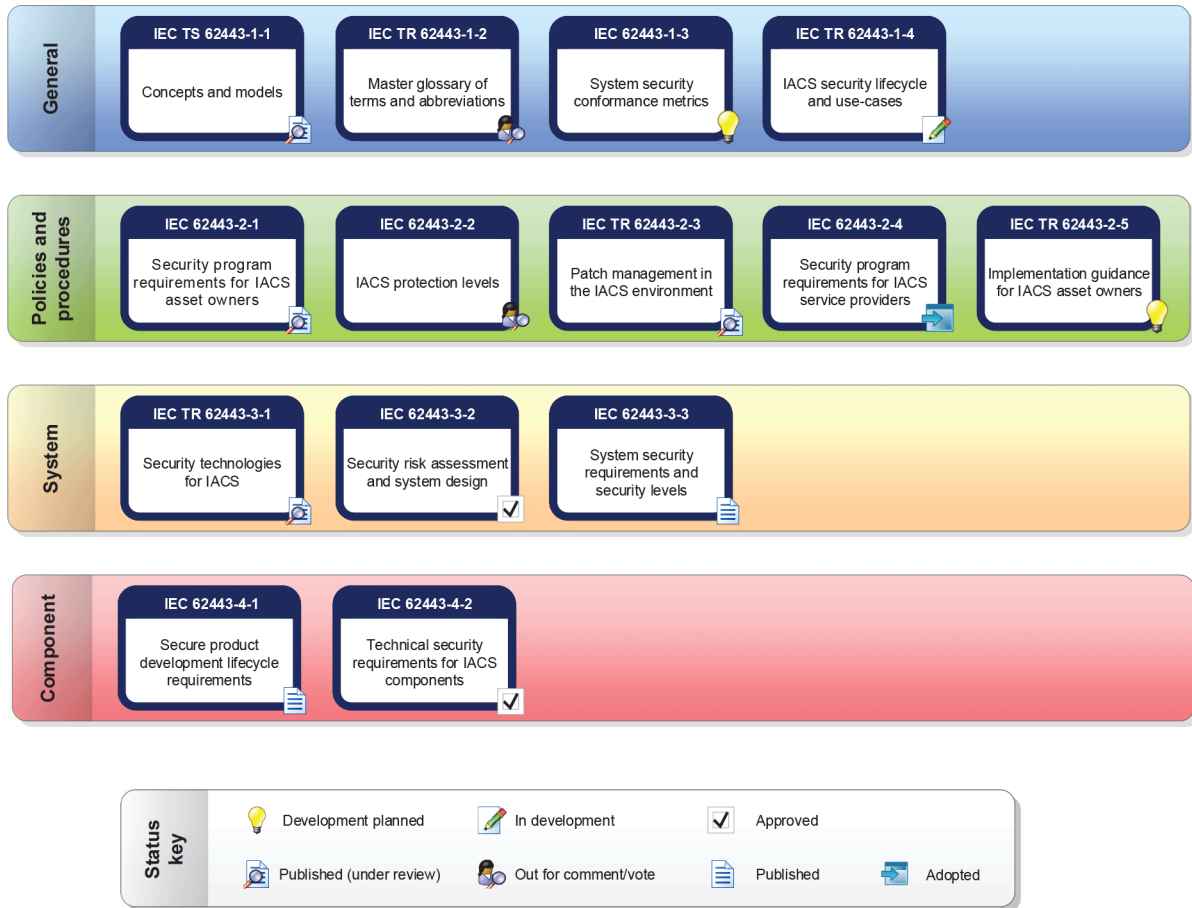
This document provides component requirements for four types of components: software application, embedded device, host device and network device. Thus, the CRs for each type of component will be designated as follows:

- Software application requirements (SAR);
- Embedded device requirements (EDR);
- Host device requirements (HDR); and
- Network device requirements (NDR).

The majority of the requirements in this document are the same for the four types of components and are thus designated simply as a CR. When there are unique component-specific requirements then the generic requirement will state that the requirements are component-specific and are located in the component-specific requirements clauses of this document.

Figure 1 shows a graphical depiction of the IEC 62443 series when this document was written.

³ Under preparation. Stage at the time of publication: IEC PRVC 62443-3-2:2018.



IEC

Figure 1 – Parts of the IEC 62443 series

SECURITY FOR INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS –

Part 4-2: Technical security requirements for IACS components

1 Scope

This part of IEC 62443 provides detailed technical control system component requirements (CRs) associated with the seven foundational requirements (FRs) described in IEC TS 62443-1-1 including defining the requirements for control system capability security levels and their components, SL-C(component).

As defined in IEC TS 62443-1-1 there are a total of seven foundational requirements (FRs):

- a) identification and authentication control (IAC),
- b) use control (UC),
- c) system integrity (SI),
- d) data confidentiality (DC),
- e) restricted data flow (RDF),
- f) timely response to events (TRE), and
- g) resource availability (RA).

These seven FRs are the foundation for defining control system security capability levels. Defining security capability levels for the control system component is the goal and objective of this document as opposed to SL-T or achieved SLs (SL-A), which are out of scope.

NOTE 1 Refer to IEC 62443-2-1 [1] for an equivalent set of non-technical, program-related, capability requirements necessary for fully achieving a SL-T(control system).

NOTE 2 The trademarks and trade names mentioned in this document are given for the convenience of users of this document. This information does not constitute an endorsement by IEC of the products named.

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 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*

3 Terms, definitions, abbreviated terms, acronyms, and conventions

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in IEC TS 62443-1-1, IEC 62443-3-3 and IEC 62443-4-1, and the following apply.

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

3.1.1

asset

physical or logical object having either a perceived or actual value to the IACS

Note 1 to entry: In this specific case, an asset is any item that should be protected as part of the IACS security management system.

Note 2 to entry: An asset is not limited to the IACS alone, but can also include the physical assets under its control

3.1.2

asset owner

individual or company responsible for one or more IACS

Note 1 to entry: Used in place of the generic term "end user" to provide differentiation.

Note 2 to entry: This includes the components that are part of the IACS.

Note 3 to entry: In the context of this document, an asset owner also includes the operator of the IACS.

3.1.3

attack

unauthorized attempt to compromise the confidentiality, integrity or availability of an IACS that derives from an intelligent threat

EXAMPLE Intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

Note 1 to entry: There are different commonly recognized classes of attack:

- An "active attack" attempts to alter system resources or affect their operation.
- A "passive attack" attempts to learn or make use of information from the system but does not affect system resources.
- An "inside attack" is an attack initiated by an entity inside the security perimeter (an "insider"), for example, an entity that is authorized to access system resources but uses them in a way not approved by those who granted the authorization.
- An "outside attack" is initiated from outside the perimeter, by an unauthorized or illegitimate user of the system (including an insider attacking from outside the security perimeter). Potential outside attackers range from amateur pranksters to organized criminals, international terrorists and hostile governments.

3.1.4

authentication

verification of the claimed identity of an entity

Note 1 to entry: Authentication is usually a prerequisite to allowing access to resources in a control system.

3.1.5

authenticator

means used to confirm the identity of an entity

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

3.1.6 authenticity

property that an entity is what it claims to be through authentication of origin and verification of integrity

Note 1 to entry: Authenticity is typically used in the context of confidence in the identity of an entity, or the validity of a transmission, a message or message originator.

3.1.7 availability

property of ensuring timely and reliable access to and use of control system information and functionality

3.1.8 communication channel

specific logical or physical communication link between assets

Note 1 to entry: A channel facilitates the establishment of a connection.

3.1.9 compensating countermeasure

countermeasure employed in lieu of or in addition to inherent security capabilities to satisfy one or more security requirements

EXAMPLE

- (component-level): locked cabinet around a controller that otherwise might be exposed to unauthorized access via its physical data interfaces;
- (control system/zone-level): physical access control (guards, gates and guns) to protect a control room to restrict access to a group of known personnel to compensate for the technical requirement for personnel to be uniquely identified by the IACS; and
- (component-level): a product supplier's programmable logic controller (PLC) cannot meet the access control capabilities from an asset owner, so the product supplier puts a firewall in front of the PLC and sells it as a system.

3.1.10 component

entity belonging to an IACS that exhibits the characteristics of one or more of a host device, network device, software application, or embedded device

3.1.11 conduit

logical grouping of communication channels, connecting two or more zones, that share common security requirements

Note 1 to entry: A conduit is allowed to traverse a zone as long as the security of the channels contained within the conduit is not impacted by the zone.

3.1.12 confidentiality

assurance that information is not disclosed to unauthorized individuals, processes, or devices

Note 1 to entry: When used in the context of an IACS, confidentiality refers to protecting IACS data and information from unauthorized access.

3.1.13 connection

association established between two or more endpoints that supports the establishment of a session

3.1.14 control system

hardware and software components of an IACS

3.1.15 countermeasure

action, device, procedure or technique that reduces a threat, a vulnerability or the consequences of an attack by minimizing the harm the attack can cause or by discovering and reporting it so that corrective action can be taken

Note 1 to entry: The term “control” is also used to describe this concept in some contexts. The term “countermeasure” has been chosen for this document to avoid confusion with the term “control” in the context of “process control” and “control system”.

3.1.16 degraded mode

mode of operation in the presence of faults that have been anticipated in the design of the control system

Note 1 to entry: Degraded modes allow the control system to continue to provide essential functions despite the deficiency of one or several system elements, for example, malfunction or outage of control equipment, disruption of communication due to failure or intentional system isolation in response to identified or suspected compromise of subsystems.

3.1.17 device

discrete physical asset that provides a set of capabilities

EXAMPLE Controllers, human-machine interfaces (HMIs), PLCs, remote terminal units (RTUs), transmitters, actuators, valves, network switches.

Note 1 to entry: A device may exhibit the characteristics of one or more of a host device, network device, software application, or embedded device.

3.1.18 embedded device

special purpose device designed to directly monitor or control an industrial process

EXAMPLE PLCs, wired or wireless field sensor devices, wired or wireless field actuator devices, safety instrumented system (SIS) controllers, distributed control system (DCS) controllers.

Note 1 to entry: Typical attributes limited storage, limited number of exposed services, programmed through an external interface, embedded operating systems (OSs) or firmware equivalent, real-time scheduler, may have an attached control panel, and may have a communications interface.

3.1.19 environment

surrounding objects, region or circumstances that may influence the behaviour of the IACS and/or may be influenced by the IACS

3.1.20 essential function

function or capability that is required to maintain health, safety, the environment (HSE) and availability for the equipment under control

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

3.1.21 event

occurrence of or change to a particular set of circumstances

Note 1 to entry: In an IACS this may be an action taken by an individual (authorized or unauthorized), a change detected within the control system (normal or abnormal) or an automated response from the control system itself (normal or abnormal).

3.1.22**firecall**

method established to provide emergency access to a secure control system

Note 1 to entry: In an emergency situation, unprivileged users can gain access to key systems to correct the problem. When a firecall is used, there is usually a review process to ensure that the access was used properly to correct a problem. These methods generally either provide a one-time use user identifier (ID) or one-time password.

3.1.23**host device**

general purpose device running an operating system (for example Microsoft Windows OS or Linux) capable of hosting one or more software applications, data stores or functions from one or more suppliers

Note 1 to entry: Typical attributes include filesystem(s), programmable services, no real time scheduler and full HMI (keyboard, mouse, etc.).

3.1.24**identifier**

pattern of symbols, unique within its security domain, that identifies, indicates or names an entity that makes an assertion or claim of identity

3.1.25**incident**

event that is not part of the expected operation of a system or service that causes, or may cause, an interruption to, or a reduction in, the quality of the service provided by the control system

3.1.26**industrial automation and control system**

collection of personnel, hardware, software and policies involved in the operation of the industrial process and that can affect or influence its safe, secure and reliable operation

3.1.27**integrity**

property of protecting the accuracy and completeness of assets

3.1.28**least privilege**

basic principle that holds that users (humans, software processes or devices) should be assigned the fewest privileges consistent with their assigned duties and functions

Note 1 to entry: Least privilege is commonly implemented as a set of roles in an IACS.

3.1.29**mobile code**

program transferred between assets that can be executed without explicit installation by the recipient

EXAMPLE JavaScript, VBScript, Java applets, ActiveX controls, Flash animations, Shockwave movies, and Microsoft Office macros.

3.1.30**mobile device**

intelligent electronic device intended for use while being transported

EXAMPLE Laptop computers, mobile robots, smart phones, hand-held programmers, tablet computers and personal digital assistants.

3.1.31

network device

device that facilitates data flow between devices, or restricts the flow of data, but may not directly interact with a control process

Note 1 to entry: Typical attributes include embedded OS or firmware, no HMI, no real-time scheduler and configured through an external interface.

3.1.32

non-repudiation

ability to prove the occurrence of a claimed event or action and its originating entities

Note 1 to entry: The purpose of non-repudiation is to resolve disputes about the occurrence or non-occurrence of the event or action and involvement of entities in the event.

3.1.33

product supplier

manufacturer of hardware and/or software product

Note 1 to entry: Used in place of the generic word “vendor” to provide differentiation.

3.1.34

remote access

access to a component by any user (human, software process or device) communicating from outside the perimeter of the zone being addressed

3.1.35

role

set of connected behaviors, privileges and obligations that may be assigned to a user or group of users (humans, software processes or devices) of an IACS

Note 1 to entry: The privileges to perform certain operations are assigned to specific roles.

3.1.36

safety instrumented system

system used to implement one or more safety-related functions

3.1.37

security level

level corresponding to the required set of countermeasures and inherent security properties of devices and systems for a zone or conduit based on assessment of risk for the zone or conduit

3.1.38

session

semi-permanent, stateful and interactive information interchange between two or more communicating components

Note 1 to entry: Typically a session has clearly defined start and end processes.

3.1.39

session ID

identifier used to indicate a specific session

3.1.40

set point

target value identified within a control system that controls one or more actions within the control system

3.1.41**software application**

one or more software programs and their dependencies that are used to interface with the process or the control system itself (for example, configuration software and historian)

Note 1 to entry: Software applications typically execute on host devices or embedded devices.

Note 2 to entry: Dependencies are any software programs that are necessary for the software application to function such as database packages, reporting tools, or any third party or open source software.

3.1.42**system integrator**

service provider that specializes in bringing together component subsystems into a whole and ensuring that those subsystems perform in accordance with project specifications

Note 1 to entry: This may also include other system supplier designations such as general automation contractor, main automation contractor, main instrument vendor, and similar.

3.1.43**threat**

set of circumstances and associated sequence of events with the potential to adversely affect operations (including mission, functions, image or reputation), assets, control systems or individuals via unauthorized access, destruction, disclosure, modification of data and/or denial of service

3.1.44**trust**

confidence that an operation, data transaction source, network or software process can be relied upon to behave as expected

Note 1 to entry: Generally, an entity can be said to 'trust' a second entity when it (the first entity) makes the assumption that the second entity will behave as the first entity expects.

Note 2 to entry: This trust may apply only for some specific function.

3.1.45**untraceability**

assurance that information cannot be used to track the time or location of a specific user

3.1.46**untrusted**

not meeting predefined requirements to be trusted

Note 1 to entry: An entity may simply be declared as untrusted.

3.1.47**update**

incremental hardware or software change in order to address security vulnerabilities, bugs, reliability or operability issues

3.1.48**upgrade**

incremental hardware or software change in order to add new features

3.1.49**zone**

collection of entities that represents partitioning of a system under consideration on the basis of their functional, logical and physical (including location) relationship

Note 1 to entry: A zone has a clear border. The security policy of a zone is typically enforced by a combination of mechanisms both at the zone edge and within the zone.

3.2 Abbreviated terms and acronyms

ACL	access control list
AES	advance encryption standard
ANSI	American National Standards Institute
API	application programming interface
ASLR	address space layout randomization
CA	certification authority
CCSC	common component security constraint
CMAC	cipher-based Message Authentication Code
COTS	commercial off the shelf
CR	component requirement
CRL	certificate revocation list
DC	data confidentiality
DCS	distributed control system
DEP	data execution prevention
DMZ	demilitarized zone
DNS	domain name service
DoS	denial of service
EDR	embedded device requirement
EICAR	European Institute for Computer Antivirus Research
EMI	electromagnetic interference
FDA	[US] Food and Drug Administration
FIPS	[US NIST] Federal Information Processing Standard
FR	foundational requirement
FTP	file transfer protocol
GCM	Galois/Counter mode
GMAC	Galois message authentication code
GUID	globally unique identifiers
HDR	host device requirement
HMI	human-machine interface
HSE	health, safety and environmental
HTTP	hypertext transfer protocol
HTTPS	HTTP secure
IAC	identification and authentication control
IACS	industrial automation and control system(s)
ID	identifier
IDS	intrusion detection system
IED	intelligent electronic device
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet protocol
IPS	intrusion prevention system
ISA	International Society of Automation
ISO	International Organization for Standardization
IT	information technology
JTAG	Joint Test Action Group

LDAP	lightweight directory access protocol
NDR	network device requirement
NIST	U.S. National Institute of Standards and Technology
NX	No Execute
OCSP	online certificate status protocol
OS	operating system
OWASP	Open Web Application Security Project
PC	personal computer
PDF	portable document format
PKI	public key infrastructure
PLC	programmable logic controller
RA	resource availability
RAM	random access memory
RDF	restricted data flow
RE	requirement enhancement
RTOS	real-time operating system
RTU	remote terminal unit
SAR	software application requirements
SFTP	secure FTP
SHA	secure hash algorithm
SI	system integrity
SIEM	security information and event management
SIF	safety instrumented function
SIS	safety instrumented system
SL	security level
SL-A	achieved security level
SL-C	capability security level
SL-T	target security level
SNMP	simple network management protocol
SP	[US NIST] Special Publication
SR	system requirement
SSH	secure socket shell
SuC	system under consideration
SQL	structured query language
TCP	transmission control protocol
TPM	trusted platform module
TRE	timely response to events
UC	use control
USB	universal serial bus
VPN	virtual private network