IEC 62443-4-2

Edition 1.0 2019-02

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

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

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
info@iec.ch
www.iec.ch

About the IEC
The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications
The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigendum or an amendment might have been published.

IEC publications search - webstore.iec.ch/advsearchform
The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee,…). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished
Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and once a month by email.

IEC Customer Service Centre - webstore.iec.ch/csc
If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: sales@iec.ch.

Electropedia - www.electropedia.org
The world's leading online dictionary on electrotechnology, containing more than 22 000 terminological entries in English and French, with equivalent terms in 16 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary
67 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

A propos de l'IEC
La Commission Electrotechnique Internationale (IEC) est la première organisation mondiale qui élabore et publie des Normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

A propos des publications IEC
Le contenu technique des publications IEC est constamment revu. Veuillez vous assurer que vous possédez l’édition la plus récente, un corrigendum ou amendement peut avoir été publié.

Recherche de publications IEC - webstore.iec.ch/advsearchform
La recherche avancée permet de trouver des publications IEC en utilisant différents critères (numéro de référence, texte, comité d’études,…). Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

IEC Just Published - webstore.iec.ch/justpublished
Restez informé sur les nouvelles publications IEC. Just Published détaille les nouvelles publications parues. Disponible en ligne et une fois par mois par email.

Service Clients - webstore.iec.ch/csc
Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: sales@iec.ch.

Electropedia - www.electropedia.org
Le premier dictionnaire d'électrotechnologie en ligne au monde, avec plus de 22 000 articles terminologiques en anglais et en français, ainsi que les termes équivalents dans 16 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

Glossaire IEC - std.iec.ch/glossary
67 000 entrées terminologiques électrotechniques, en anglais et en français, extraites des articles Termes et Définitions des publications IEC parues depuis 2002. Plus certaines entrées antérieures extraites des publications des CE 37, 77, 86 et CISPR de l'IEC.

IEC 62443-4-2

Edition 1.0 2019-02

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

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

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.