IEC 62443-3-3

Edition 1.0 2013-08

INTERNATIONAL STANDARD

Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels

IEC 62443-3-3:2013(E)

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

Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00
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 corrigenda or an amendment might have been published.

Useful links:

IEC publications search - www.iec.ch/searchpub

The advanced search enables you 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It also gives information on projects, replaced and withdrawn publications.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 on-line and also once a month by email.

Electropedia - www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing more than 30 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary (IEV) on-line.

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: csc@iec.ch.

IEC®

IEC 62443-3-3

Edition 1.0 2013-08

INTERNATIONAL STANDARD

colour inside

Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

PRICE CODE XC

ICS 25.040.40; 35.110

ISBN 978-2-8322-1036-9

Warning! Make sure that you obtained this publication from an authorized distributor.

CONTENTS

FOREWORD 9
0 Introduction 11
0.1 Overview 11
0.2 Purpose and intended audience 12
0.3 Usage within other parts of the IEC 62443 series 12
1 Scope 14
2 Normative references 14
3 Terms, definitions, abbreviated terms, acronyms, and conventions 14
3.1 Terms and definitions 14
3.2 Abbreviated terms and acronyms 20
3.3 Conventions 22
4 Common control system security constraints 22
4.1 Overview 22
4.2 Support of essential functions 23
4.3 Compensating countermeasures 23
4.4 Least privilege 24
5 FR 1 – Identification and authentication control 24
5.1 Purpose and SL-C(IAC) descriptions 24
5.2 Rationale 24
5.3 SR 1.1 – Human user identification and authentication 24
5.3.1 Requirement 24
5.3.2 Rationale and supplemental guidance 24
5.3.3 Requirement enhancements 25
5.3.4 Security levels 25
5.4 SR 1.2 – Software process and device identification and authentication 26
5.4.1 Requirement 26
5.4.2 Rationale and supplemental guidance 26
5.4.3 Requirement enhancements 26
5.4.4 Security levels 27
5.5 SR 1.3 – Account management 27
5.5.1 Requirement 27
5.5.2 Rationale and supplemental guidance 27
5.5.3 Requirement enhancements 27
5.5.4 Security levels 27
5.6 SR 1.4 – Identifier management 28
5.6.1 Requirement 28
5.6.2 Rationale and supplemental guidance 28
5.6.3 Requirement enhancements 28
5.6.4 Security levels 28
5.7 SR 1.5 – Authenticator management 28
5.7.1 Requirement 28
5.7.2 Rationale and supplemental guidance 28
5.7.3 Requirement enhancements 29
5.7.4 Security levels 29
5.8 SR 1.6 – Wireless access management 30
5.8.1 Requirement 30

5.8.2 Rationale and supplemental guidance 30
5.8.3 Requirement enhancements 30
5.8.4 Security levels 30
5.9 SR 1.7 – Strength of password-based authentication 30
5.9.1 Requirement 30
5.9.2 Rationale and supplemental guidance 30
5.9.3 Requirement enhancements 31
5.9.4 Security levels 31
5.10 SR 1.8 – Public key infrastructure (PKI) certificates 31
5.10.1 Requirement 31
5.10.2 Rationale and supplemental guidance 31
5.10.3 Requirement enhancements 32
5.10.4 Security levels 32
5.11 SR 1.9 – Strength of public key authentication 32
5.11.1 Requirement 32
5.11.2 Rationale and supplemental guidance 32
5.11.3 Requirement enhancements 33
5.11.4 Security levels 33
5.12 SR 1.10 – Authenticator feedback 33
5.12.1 Requirement 33
5.12.2 Rationale and supplemental guidance 33
5.12.3 Requirement enhancements 33
5.12.4 Security levels 33
5.13 SR 1.11 – Unsuccessful login attempts 34
5.13.1 Requirement 34
5.13.2 Rationale and supplemental guidance 34
5.13.3 Requirement enhancements 34
5.13.4 Security levels 34
5.14 SR 1.12 – System use notification 34
5.14.1 Requirement 34
5.14.2 Rationale and supplemental guidance 34
5.14.3 Requirement enhancements 35
5.14.4 Security levels 35
5.15 SR 1.13 – Access via untrusted networks 35
5.15.1 Requirement 35
5.15.2 Rationale and supplemental guidance 35
5.15.3 Requirement enhancements 35
5.15.4 Security levels 35
6 FR 2 – Use control 36
6.1 Purpose and SL-C(UC) descriptions 36
6.2 Rationale 36
6.3 SR 2.1 – Authorization enforcement 36
6.3.1 Requirement 36
6.3.2 Rationale and supplemental guidance 36
6.3.3 Requirement enhancements 37
6.3.4 Security levels 37
6.4 SR 2.2 – Wireless use control 37
6.4.1 Requirement 37
6.4.2 Rationale and supplemental guidance 38

6.4.3 Requirement enhancements 38
6.4.4 Security levels 38
6.5 SR 2.3 – Use control for portable and mobile devices 38
6.5.1 Requirement 38
6.5.2 Rationale and supplemental guidance 38
6.5.3 Requirement enhancements 39
6.5.4 Security levels 39
6.6 SR 2.4 – Mobile code 39
6.6.1 Requirement 39
6.6.2 Rationale and supplemental guidance 39
6.6.3 Requirement enhancements 39
6.6.4 Security levels 39
6.7 SR 2.5 – Session lock 40
6.7.1 Requirement 40
6.7.2 Rationale and supplemental guidance 40
6.7.3 Requirement enhancements 40
6.7.4 Security levels 40
6.8 SR 2.6 – Remote session termination 40
6.8.1 Requirement 40
6.8.2 Rationale and supplemental guidance 40
6.8.3 Requirement enhancements 40
6.8.4 Security levels 41
6.9 SR 2.7 – Concurrent session control 41
6.9.1 Requirement 41
6.9.2 Rationale and supplemental guidance 41
6.9.3 Requirement enhancements 41
6.9.4 Security levels 41
6.10 SR 2.8 – Auditable events 41
6.10.1 Requirement 41
6.10.2 Rationale and supplemental guidance 41
6.10.3 Requirement enhancements 42
6.10.4 Security levels 42
6.11 SR 2.9 – Audit storage capacity 42
6.11.1 Requirement 42
6.11.2 Rationale and supplemental guidance 42
6.11.3 Requirement enhancements 42
6.11.4 Security levels 43
6.12 SR 2.10 – Response to audit processing failures 43
6.12.1 Requirement 43
6.12.2 Rationale and supplemental guidance 43
6.12.3 Requirement enhancements 43
6.12.4 Security levels 43
6.13 SR 2.11 – Timestamps 43
6.13.1 Requirement 43
6.13.2 Rationale and supplemental guidance 43
6.13.3 Requirement enhancements 44
6.13.4 Security levels 44
6.14 SR 2.12 – Non-repudiation 44
6.14.1 Requirement 44

6.14.2 Rationale and supplemental guidance 44
6.14.3 Requirement enhancements 44
6.14.4 Security levels 44
7 FR 3 – System integrity 45
7.1 Purpose and SL-C(SI) descriptions 45
7.2 Rationale 45
7.3 SR 3.1 – Communication integrity 45
7.3.1 Requirement 45
7.3.2 Rationale and supplemental guidance 45
7.3.3 Requirement enhancements 46
7.3.4 Security levels 46
7.4 SR 3.2 – Malicious code protection 46
7.4.1 Requirement 46
7.4.2 Rationale and supplemental guidance 46
7.4.3 Requirement enhancements 47
7.4.4 Security levels 47
7.5 SR 3.3 – Security functionality verification 47
7.5.1 Requirement 47
7.5.2 Rationale and supplemental guidance 47
7.5.3 Requirement enhancements 48
7.5.4 Security levels 48
7.6 SR 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 49
7.6.4 Security levels 49
7.7 SR 3.5 – Input validation 49
7.7.1 Requirement 49
7.7.2 Rationale and supplemental guidance 49
7.7.3 Requirement enhancements 49
7.7.4 Security levels 49
7.8 SR 3.6 – Deterministic output 50
7.8.1 Requirement 50
7.8.2 Rationale and supplemental guidance 50
7.8.3 Requirement enhancements 50
7.8.4 Security levels 50
7.9 SR 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 51
7.10 SR 3.8 – Session integrity 51
7.10.1 Requirement 51
7.10.2 Rationale and supplemental guidance 51
7.10.3 Requirement enhancements 51
7.10.4 Security levels 51
7.11 SR 3.9 – Protection of audit information 52
7.11.1 Requirement 52
7.11.2 Rationale and supplemental guidance 52

7.11.3 Requirement enhancements 52
7.11.4 Security levels 52
8 FR 4 – Data confidentiality 52
8.1 Purpose and SL-C(DC) descriptions 52
8.2 Rationale 52
8.3 SR 4.1 – Information confidentiality 53
8.3.1 Requirement 53
8.3.2 Rationale and supplemental guidance 53
8.3.3 Requirement enhancements 53
8.3.4 Security levels 53
8.4 SR 4.2 – Information persistence 54
8.4.1 Requirement 54
8.4.2 Rationale and supplemental guidance 54
8.4.3 Requirement enhancements 54
8.4.4 Security levels 54
8.5 SR 4.3 – Use of cryptography 54
8.5.1 Requirement 54
8.5.2 Rationale and supplemental guidance 55
8.5.3 Requirement enhancements 55
8.5.4 Security levels 55
9 FR 5 – Restricted data flow 55
9.1 Purpose and SL-C(RDF) descriptions 55
9.2 Rationale 55
9.3 SR 5.1 – Network segmentation 56
9.3.1 Requirement 56
9.3.2 Rationale and supplemental guidance 56
9.3.3 Requirement enhancements 56
9.3.4 Security levels 57
9.4 SR 5.2 – Zone boundary protection 57
9.4.1 Requirement 57
9.4.2 Rationale and supplemental guidance 57
9.4.3 Requirement enhancements 57
9.4.4 Security levels 58
9.5 SR 5.3 – General purpose person-to-person communication restrictions 58
9.5.1 Requirement 58
9.5.2 Rationale and supplemental guidance 58
9.5.3 Requirement enhancements 58
9.5.4 Security levels 59
9.6 SR 5.4 – Application partitioning 59
9.6.1 Requirement 59
9.6.2 Rationale and supplemental guidance 59
9.6.3 Requirement enhancements 59
9.6.4 Security levels 59
10 FR 6 – Timely response to events 59
10.1 Purpose and SL-C(TRE) descriptions 59
10.2 Rationale 60
10.3 SR 6.1 – Audit log accessibility 60
10.3.1 Requirement 60
10.3.2 Rationale and supplemental guidance 60

10.3.3 Requirement enhancements 60
10.3.4 Security levels 60
10.4 SR 6.2 – Continuous monitoring 60
10.4.1 Requirement 60
10.4.2 Rationale and supplemental guidance 60
10.4.3 Requirement enhancements 61
10.4.4 Security levels 61
11 FR 7 – Resource availability 61
11.1 Purpose and SL-C(RA) descriptions 61
11.2 Rationale 61
11.3 SR 7.1 – Denial of service protection 62
11.3.1 Requirement 62
11.3.2 Rationale and supplemental guidance 62
11.3.3 Requirement enhancements 62
11.3.4 Security levels 62
11.4 SR 7.2 – Resource management 62
11.4.1 Requirement 62
11.4.2 Rationale and supplemental guidance 62
11.4.3 Requirement enhancements 62
11.4.4 Security levels 63
11.5 SR 7.3 – Control system backup 63
11.5.1 Requirement 63
11.5.2 Rationale and supplemental guidance 63
11.5.3 Requirement enhancements 63
11.5.4 Security levels 63
11.6 SR 7.4 – Control system recovery and reconstitution 63
11.6.1 Requirement 63
11.6.2 Rationale and supplemental guidance 63
11.6.3 Requirement enhancements 64
11.6.4 Security levels 64
11.7 SR 7.5 – Emergency power 64
11.7.1 Requirement 64
11.7.2 Rationale and supplemental guidance 64
11.7.3 Requirement enhancements 64
11.7.4 Security levels 64
11.8 SR 7.6 – Network and security configuration settings 64
11.8.1 Requirement 64
11.8.2 Rationale and supplemental guidance 64
11.8.3 Requirement enhancements 65
11.8.4 Security levels 65
11.9 SR 7.7 – Least functionality 65
11.9.1 Requirement 65
11.9.2 Rationale and supplemental guidance 65
11.9.3 Requirement enhancements 65
11.9.4 Security levels 65
11.10 SR 7.8 – Control system component inventory 66
11.10.1 Requirement 66
11.10.2 Rationale and supplemental guidance 66
11.10.3 Requirement enhancements 66

11.10.4 Security levels 66
Annex A (informative) Discussion of the SL vector 67
Annex B (informative) Mapping of SRs and REs to FR SL levels 1-4 75
Bibliography...79

Figure 1 – Structure of the IEC 62443 series 13
Figure A.1 – High-level process-industry example showing zones and conduits 69
Figure A.2 – High-level manufacturing example showing zones and conduits........................70
Figure A.3 – Schematic of correlation of the use of different SL types 71

Table B.1 – Mapping of SRs and REs to FR SL levels 1-4 *(1 of 4)* 75

INTERNATIONAL ELECTROTECHNICAL COMMISSION

____

INDUSTRIAL COMMUNICATION NETWORKS – NETWORK AND SYSTEM SECURITY –

Part 3-3: System security requirements and security levels

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 62443-3-3 has been prepared by IEC technical committee 65: Industrial-process measurement, control and automation.

The text of this standard is based on the following documents:

FDIS	Report on voting
65/531/FDIS	65/540/RVD

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

This publication 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 *Industrial communication networks – Network and system security*, can be found on the IEC website.

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

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

A bilingual version of this publication may be issued at a later date.

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.