This is a preview - click here to buy the full publication

IEC 62443-4-2

Edition 1.0 2019-01

PRE-RELEASE VERSION (FDIS)

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

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.

® Registered trademark of the International Electrotechnical Commission
Marque déposée de la Commission Electrotechnique Internationale

This is a preview - click here to buy the full publication

65/735/FDIS

FINAL DRAFT INTERNATIONAL STANDARD (FDIS)

PROJECT NUMBER: **IEC 62443-4-2 ED1**	
DATE OF CIRCULATION: **2018-12-21**	CLOSING DATE FOR VOTING: **2019-02-01**
SUPERSEDES DOCUMENTS: **65/663/CDV,65/691/RVC**	

IEC TC 65 : INDUSTRIAL-PROCESS MEASUREMENT, CONTROL AND AUTOMATION	
SECRETARIAT: France	SECRETARY: Mr Rudy BELLIARDI
OF INTEREST TO THE FOLLOWING COMMITTEES: TC 44,SC 45A,TC 57,SC 62A	HORIZONTAL STANDARD: ☐
FUNCTIONS CONCERNED: ☐ EMC ☐ ENVIRONMENT ☐ QUALITY ASSURANCE ☐ SAFETY	
☒ SUBMITTED FOR CENELEC PARALLEL VOTING **Attention IEC-CENELEC parallel voting** The attention of IEC National Committees, members of CENELEC, is drawn to the fact that this Final Draft International Standard (FDIS) is submitted for parallel voting. The CENELEC members are invited to vote through the CENELEC online voting system.	☐ NOT SUBMITTED FOR CENELEC PARALLEL VOTING

This document is a draft distributed for approval. It may not be referred to as an International Standard until published as such.

In addition to their evaluation as being acceptable for industrial, technological, commercial and user purposes, Final Draft International Standards may on occasion have to be considered in the light of their potential to become standards to which reference may be made in national regulations.

Recipients of this document are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

TITLE:

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

PROPOSED STABILITY DATE: 2021

NOTE FROM TC/SC OFFICERS:

Copyright © 2018 International Electrotechnical Commission, IEC. All rights reserved. It is permitted to download this electronic file, to make a copy and to print out the content for the sole purpose of preparing National Committee positions. You may not copy or "mirror" the file or printed version of the document, or any part of it, for any other purpose without permission in writing from IEC.

This is a preview - click here to buy the full publication

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

This is a preview - click here to buy the full publication

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

This is a preview - click here to buy the full publication

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

This is a preview - click here to buy the full publication

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 49
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 50
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 51
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

This is a preview - click here to buy the full publication

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 56
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 58
11.3.1 Requirement 58
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 59
11.5.1 Requirement 59

This is a preview - click here to buy the full publication

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....60
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....61
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

This is a preview - click here to buy the full publication

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

This is a preview - click here to buy the full publication

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

This is a preview - click here to buy the full publication

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 81
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 82
15.13.1 Requirement 82
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

This is a preview - click here to buy the full publication

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

This is a preview - click here to buy the full publication

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/XX/FDIS	65/XX/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.

This is a preview - click here to buy the full publication

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.

This is a preview - click here to buy the full publication

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 62443-2-1[1] [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.

This is a preview - click here to buy the full publication

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).

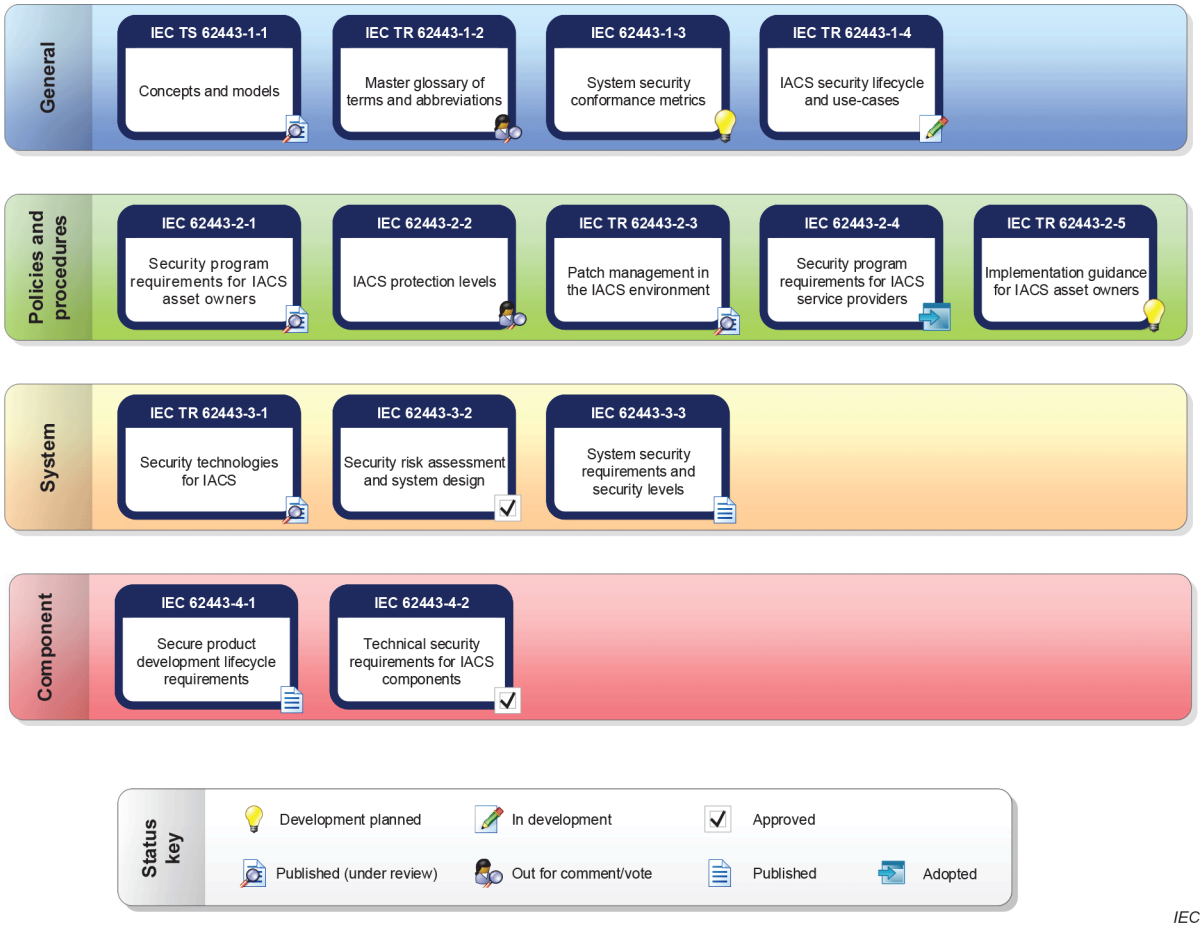
The majority of the requirements in this document are the same for the four types of components and are thus designated simply as a CR. When there are unique component-specific requirements then the generic requirement will state that the requirements are component-specific and are located in the component-specific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

This is a preview - click here to buy the full publication



IEC

Figure 1 – Parts of the IEC 62443 series

This is a preview - click here to buy the full publication

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*

This is a preview - click here to buy the full publication

SOMMAIRE

AVANT-PROPOS 12
INTRODUCTION 14
1 Domaine d'application 17
2 Références normatives 17
3 Termes, définitions, termes abrégés, acronymes et conventions 18
3.1 Termes et définitions 18
3.2 Termes abrégés et acronymes 24
3.3 Conventions 26
4 Contraintes communes en matière de sécurité du composant 27
4.1 Vue d'ensemble 27
4.2 Support des fonctions essentielles CCSC 1 27
4.3 Contre-mesures compensatoires CCSC 2 27
4.4 Droit d'accès minimal CCSC 3 27
4.5 Processus de développement logiciel CCSC 4 28
5 FR 1 – Contrôle d'identification et d'authentification 28
5.1 Objet et descriptions du SL-C(IAC) 28
5.2 Justification 28
5.3 CR 1.1 – Identification et authentification d'un utilisateur humain 28
5.3.1 Exigences 28
5.3.2 Justification et recommandations complémentaires 29
5.3.3 Amélioration d'exigences 29
5.3.4 Niveaux de sécurité 29
5.4 CR 1.2 – Identification et authentification du processus logiciel et de l'appareil 29
5.4.1 Exigences 29
5.4.2 Justification et recommandations complémentaires 30
5.4.3 Amélioration d'exigences 30
5.4.4 Niveaux de sécurité 30
5.5 CR 1.3 – Gestion de compte 30
5.5.1 Exigences 30
5.5.2 Justification et recommandations complémentaires 31
5.5.3 Amélioration d'exigences 31
5.5.4 Niveaux de sécurité 31
5.6 CR 1.4 – Gestion d'identificateur 31
5.6.1 Exigences 31
5.6.2 Justification et recommandations complémentaires 31
5.6.3 Amélioration d'exigences 31
5.6.4 Niveaux de sécurité 31
5.7 CR 1.5 – Gestion d'authentifiant 32
5.7.1 Exigences 32
5.7.2 Justification et recommandations complémentaires 32
5.7.3 Amélioration d'exigences 33
5.7.4 Niveaux de sécurité 33
5.8 CR 1.6 – Gestion des accès sans fil 33
5.9 CR 1.7 – Force de l'authentification basée sur mot de passe 33
5.9.1 Exigences 33

This is a preview - click here to buy the full publication

5.9.2 Justification et recommandations complémentaires 33
5.9.3 Amélioration d'exigences 33
5.9.4 Niveaux de sécurité 34
5.10 CR 1.8 – Certificats d'infrastructure à clés publiques 34
5.10.1 Exigences 34
5.10.2 Justification et recommandations complémentaires 34
5.10.3 Amélioration d'exigences 34
5.10.4 Niveaux de sécurité 34
5.11 CR 1.9 – Force de l'authentification basée sur clé publique 35
5.11.1 Exigences 35
5.11.2 Justification et recommandations complémentaires 35
5.11.3 Amélioration d'exigences 36
5.11.4 Niveaux de sécurité 36
5.12 CR 1.10 – Retour de l'authentifiant 36
5.12.1 Exigences 36
5.12.2 Justification et recommandations complémentaires 36
5.12.3 Amélioration d'exigences 36
5.12.4 Niveaux de sécurité 36
5.13 CR 1.11 – Tentatives infructueuses de connexion 36
5.13.1 Exigences 36
5.13.2 Justification et recommandations complémentaires 37
5.13.3 Amélioration d'exigences 37
5.13.4 Niveaux de sécurité 37
5.14 CR 1.12 – Notification d'utilisation du système 37
5.14.1 Exigences 37
5.14.2 Justification et recommandations complémentaires 37
5.14.3 Amélioration d'exigences 38
5.14.4 Niveaux de sécurité 38
5.15 CR 1.13 – Accès par l'intermédiaire de réseaux non sécurisés 38
5.16 CR 1.14 – Force de l'authentification basée sur clé symétrique 38
5.16.1 Exigences 38
5.16.2 Justification et recommandations complémentaires 38
5.16.3 Amélioration d'exigences 39
5.16.4 Niveaux de sécurité 39
6 FR 2 – Contrôle d'utilisation 39
6.1 Objet et descriptions du SL-C(UC) 39
6.2 Justification 39
6.3 CR 2.1 – Mise en œuvre d'autorisation 40
6.3.1 Exigences 40
6.3.2 Justification et recommandations complémentaires 40
6.3.3 Amélioration d'exigences 40
6.3.4 Niveaux de sécurité 41
6.4 CR 2.2 – Contrôle d'utilisation sans fil 41
6.4.1 Exigences 41
6.4.2 Justification et recommandations complémentaires 41
6.4.3 Amélioration d'exigences 41
6.4.4 Niveaux de sécurité 41
6.5 CR 2.3 – Contrôle d'utilisation pour les appareils portables et mobiles 42
6.6 CR 2.4 – Code mobile 42

This is a preview - click here to buy the full publication

6.7 CR 2.5 – Verrouillage de session 42
6.7.1 Exigences 42
6.7.2 Justification et recommandations complémentaires 42
6.7.3 Amélioration d'exigences 42
6.7.4 Niveaux de sécurité 42
6.8 CR 2.6 – Fermeture de la session à distance 42
6.8.1 Exigences 42
6.8.2 Justification et recommandations complémentaires 43
6.8.3 Amélioration d'exigences 43
6.8.4 Niveaux de sécurité 43
6.9 CR 2.7 – Contrôle de sessions simultanées 43
6.9.1 Exigences 43
6.9.2 Justification et recommandations complémentaires 43
6.9.3 Amélioration d'exigences 43
6.9.4 Niveaux de sécurité 43
6.10 CR 2.8 – Événements auditables 43
6.10.1 Exigences 43
6.10.2 Justification et recommandations complémentaires 44
6.10.3 Amélioration d'exigences 44
6.10.4 Niveaux de sécurité 44
6.11 CR 2.9 – Capacité de stockage des données d'audit 44
6.11.1 Exigences 44
6.11.2 Justification et recommandations complémentaires 44
6.11.3 Amélioration d'exigences 45
6.11.4 Niveaux de sécurité 45
6.12 CR 2.10 – Réponse aux défaillances de traitement des audits 45
6.12.1 Exigences 45
6.12.2 Justification et recommandations complémentaires 45
6.12.3 Amélioration d'exigences 45
6.12.4 Niveaux de sécurité 45
6.13 CR 2.11 – Horodatages 46
6.13.1 Exigences 46
6.13.2 Justification et recommandations complémentaires 46
6.13.3 Amélioration d'exigences 46
6.13.4 Niveaux de sécurité 46
6.14 CR 2.12 – Non-répudiation 46
6.14.1 Exigences 46
6.14.2 Justification et recommandations complémentaires 46
6.14.3 Amélioration d'exigences 47
6.14.4 Niveaux de sécurité 47
6.15 CR 2.13 – Utilisation d'interfaces physiques de diagnostic et d'essai 47
7 FR 3 – Intégrité du système 47
7.1 Objet et descriptions du SL-C(SI) 47
7.2 Justification 47
7.3 CR 3.1 – Intégrité de la communication 48
7.3.1 Exigences 48
7.3.2 Justification et recommandations complémentaires 48
7.3.3 Amélioration d'exigences 48
7.3.4 Niveaux de sécurité 49

This is a preview - click here to buy the full publication

7.4 CR 3.2 – Protection contre les programmes malveillants 49
7.5 CR 3.3 – Vérification de la fonctionnalité de sécurité 49
7.5.1 Exigences 49
7.5.2 Justification et recommandations complémentaires 49
7.5.3 Amélioration d'exigences 49
7.5.4 Niveaux de sécurité 50
7.6 CR 3.4 – Intégrité des logiciels et des informations 50
7.6.1 Exigences 50
7.6.2 Justification et recommandations complémentaires 50
7.6.3 Amélioration d'exigences 50
7.6.4 Niveaux de sécurité 50
7.7 CR 3.5 – Validation d'entrée 50
7.7.1 Exigences 50
7.7.2 Justification et recommandations complémentaires 51
7.7.3 Amélioration d'exigences 51
7.7.4 Niveaux de sécurité 51
7.8 CR 3.6 – Sortie déterministe 51
7.8.1 Exigences 51
7.8.2 Justification et recommandations complémentaires 51
7.8.3 Amélioration d'exigences 52
7.8.4 Niveaux de sécurité 52
7.9 CR 3.7 – Traitement des erreurs 52
7.9.1 Exigences 52
7.9.2 Justification et recommandations complémentaires 52
7.9.3 Amélioration d'exigences 52
7.9.4 Niveaux de sécurité 52
7.10 CR 3.8 – Intégrité de la session 52
7.10.1 Exigences 52
7.10.2 Justification et recommandations complémentaires 53
7.10.3 Amélioration d'exigences 53
7.10.4 Niveaux de sécurité 53
7.11 CR 3.9 – Protection des informations d'audit 53
7.11.1 Exigences 53
7.11.2 Justification et recommandations complémentaires 53
7.11.3 Amélioration d'exigences 53
7.11.4 Niveaux de sécurité 54
7.12 CR 3.10 – Support pour les mises à jour 54
7.13 CR 3.11 – Résistance aux violations physiques et détection 54
7.14 CR 3.12 – Fourniture des racines de confiance du fournisseur de produit 54
7.15 CR 3.13 – Fourniture des racines de confiance du propriétaire d'actif 54
7.16 CR 3.14 – Intégrité du processus d'amorçage 54
8 FR 4 – Confidentialité des données 54
8.1 Objet et descriptions du SL-C(DC) 54
8.2 Justification 55
8.3 CR 4.1 – Confidentialité des informations 55
8.3.1 Exigences 55
8.3.2 Justification et recommandations complémentaires 55
8.3.3 Amélioration d'exigences 55
8.3.4 Niveaux de sécurité 55

This is a preview - click here to buy the full publication

8.4 CR 4.2 – Persistance des informations 55
8.4.1 Exigences 55
8.4.2 Justification et recommandations complémentaires 56
8.4.3 Amélioration d'exigences 56
8.4.4 Niveaux de sécurité 56
8.5 CR 4.3 – Utilisation de la cryptographie 56
8.5.1 Exigences 56
8.5.2 Justification et recommandations complémentaires 56
8.5.3 Amélioration d'exigences 57
8.5.4 Niveaux de sécurité 57
9 FR 5 – Transfert de données limité 57
9.1 Objet et descriptions du SL-C(RDF) 57
9.2 Justification 57
9.3 CR 5.1 – Segmentation du réseau 58
9.3.1 Exigences 58
9.3.2 Justification et recommandations complémentaires 58
9.3.3 Amélioration d'exigences 58
9.3.4 Niveaux de sécurité 58
9.4 CR 5.2 – Protection des limites de zone 59
9.5 CR 5.3 – Restrictions des communications entre des personnes d'ordre général 59
9.6 CR 5.4 – Partitionnement des applications 59
10 FR 6 – Réponse appropriée aux événements 59
10.1 Objet et descriptions du SL-C(TRE) 59
10.2 Justification 59
10.3 CR 6.1 – Accessibilité au journal d'audit 59
10.3.1 Exigences 59
10.3.2 Justification et recommandations complémentaires 60
10.3.3 Amélioration d'exigences 60
10.3.4 Niveaux de sécurité 60
10.4 CR 6.2 – Surveillance continue 60
10.4.1 Exigences 60
10.4.2 Justification et recommandations complémentaires 60
10.4.3 Amélioration d'exigences 61
10.4.4 Niveaux de sécurité 61
11 FR 7 – Disponibilité des ressources 61
11.1 Objet et descriptions du SL-C(RA) 61
11.2 Justification 61
11.3 CR 7.1 – Protection contre le refus de service 61
11.3.1 Exigences 61
11.3.2 Justification et recommandations complémentaires 61
11.3.3 Amélioration d'exigences 62
11.3.4 Niveaux de sécurité 62
11.4 CR 7.2 – Gestion des ressources 62
11.4.1 Exigences 62
11.4.2 Justification et recommandations complémentaires 62
11.4.3 Amélioration d'exigences 62
11.4.4 Niveaux de sécurité 62
11.5 CR 7.3 – Sauvegarde du système de commande 62

This is a preview - click here to buy the full publication

11.5.1 Exigences 62
11.5.2 Justification et recommandations complémentaires 62
11.5.3 Amélioration d'exigences 63
11.5.4 Niveaux de sécurité 63
11.6 CR 7.4 – Récupération et reconstitution du système de commande 63
11.6.1 Exigences 63
11.6.2 Justification et recommandations complémentaires 63
11.6.3 Amélioration d'exigences 63
11.6.4 Niveaux de sécurité 63
11.7 CR 7.5 – Alimentation de secours 64
11.8 CR 7.6 – Paramètres de configuration du réseau et de la sécurité 64
11.8.1 Exigences 64
11.8.2 Justification et recommandations complémentaires 64
11.8.3 Amélioration d'exigences 64
11.8.4 Niveaux de sécurité 64
11.9 CR 7.7 – Fonctionnalité minimale 64
11.9.1 Exigences 64
11.9.2 Justification et recommandations complémentaires 64
11.9.3 Amélioration d'exigences 64
11.9.4 Niveaux de sécurité 65
11.10 CR 7.8 – Inventaire des composants du système de commande 65
11.10.1 Exigences 65
11.10.2 Justification et recommandations complémentaires 65
11.10.3 Amélioration d'exigences 65
11.10.4 Niveaux de sécurité 65
12 Exigences relatives aux applications logicielles 65
12.1 Objet 65
12.2 SAR 2.4 – Code mobile 65
12.2.1 Exigences 65
12.2.2 Justification et recommandations complémentaires 66
12.2.3 Amélioration d'exigences 66
12.2.4 Niveaux de sécurité 66
12.3 SAR 3.2 – Protection contre les programmes malveillants 66
12.3.1 Exigences 66
12.3.2 Justification et recommandations complémentaires 66
12.3.3 Amélioration d'exigences 66
12.3.4 Niveaux de sécurité 66
13 Exigences relatives aux appareils intégrés 67
13.1 Objet 67
13.2 EDR 2.4 – Code mobile 67
13.2.1 Exigences 67
13.2.2 Justification et recommandations complémentaires 67
13.2.3 Amélioration d'exigences 67
13.2.4 Niveaux de sécurité 67
13.3 EDR 2.13 – Utilisation d'interfaces physiques de diagnostic et d'essai 67
13.3.1 Exigences 67
13.3.2 Justification et recommandations complémentaires 68
13.3.3 Amélioration d'exigences 68
13.3.4 Niveaux de sécurité 68

This is a preview - click here to buy the full publication

13.4 EDR 3.2 – Protection contre les programmes malveillants 68
13.4.1 Exigences 68
13.4.2 Justification et recommandations complémentaires 68
13.4.3 Amélioration d'exigences 69
13.4.4 Niveaux de sécurité 69
13.5 EDR 3.10 – Support pour les mises à jour 69
13.5.1 Exigences 69
13.5.2 Justification et recommandations complémentaires 69
13.5.3 Amélioration d'exigences 69
13.5.4 Niveaux de sécurité 69
13.6 EDR 3.11 – Résistance aux violations physiques et détection 69
13.6.1 Exigences 69
13.6.2 Justification et recommandations complémentaires 70
13.6.3 Amélioration d'exigences 70
13.6.4 Niveaux de sécurité 70
13.7 EDR 3.12 – Fourniture des racines de confiance du fournisseur de produit 70
13.7.1 Exigences 70
13.7.2 Justification et recommandations complémentaires 70
13.7.3 Amélioration d'exigences 71
13.7.4 Niveaux de sécurité 71
13.8 EDR 3.13 – Fourniture des racines de confiance du propriétaire d'actif 71
13.8.1 Exigences 71
13.8.2 Justification et recommandations complémentaires 71
13.8.3 Amélioration d'exigences 72
13.8.4 Niveaux de sécurité 72
13.9 EDR 3.14 – Intégrité du processus d'amorçage 72
13.9.1 Exigences 72
13.9.2 Justification et recommandations complémentaires 72
13.9.3 Amélioration d'exigences 72
13.9.4 Niveaux de sécurité 72
14 Exigences relatives aux appareils hôtes 73
14.1 Objet 73
14.2 HDR 2.4 – Code mobile 73
14.2.1 Exigences 73
14.2.2 Justification et recommandations complémentaires 73
14.2.3 Amélioration d'exigences 73
14.2.4 Niveaux de sécurité 73
14.3 HDR 2.13 – Utilisation d'interfaces physiques de diagnostic et d'essai 74
14.3.1 Exigences 74
14.3.2 Justification et recommandations complémentaires 74
14.3.3 Amélioration d'exigences 74
14.3.4 Niveaux de sécurité 74
14.4 HDR 3.2 – Protection contre les programmes malveillants 74
14.4.1 Exigences 74
14.4.2 Justification et recommandations complémentaires 74
14.4.3 Amélioration d'exigences 75
14.4.4 Niveaux de sécurité 75
14.5 HDR 3.10 – Support pour les mises à jour 75
14.5.1 Exigences 75

This is a preview - click here to buy the full publication

14.5.2 Justification et recommandations complémentaires 75
14.5.3 Amélioration d'exigences 75
14.5.4 Niveaux de sécurité 75
14.6 HDR 3.11 – Résistance aux violations physiques et détection 75
14.6.1 Exigences 75
14.6.2 Justification et recommandations complémentaires 75
14.6.3 Amélioration d'exigences 76
14.6.4 Niveaux de sécurité 76
14.7 HDR 3.12 – Fourniture des racines de confiance du fournisseur de produit 76
14.7.1 Exigences 76
14.7.2 Justification et recommandations complémentaires 76
14.7.3 Amélioration d'exigences 77
14.7.4 Niveaux de sécurité 77
14.8 HDR 3.13 – Fourniture des racines de confiance du propriétaire d'actif 77
14.8.1 Exigences 77
14.8.2 Justification et recommandations complémentaires 77
14.8.3 Amélioration d'exigences 78
14.8.4 Niveaux de sécurité 78
14.9 HDR 3.14 – Intégrité du processus d'amorçage 78
14.9.1 Exigences 78
14.9.2 Justification et recommandations complémentaires 78
14.9.3 Amélioration d'exigences 78
14.9.4 Niveaux de sécurité 78
15 Exigences relatives aux appareils de réseaux 78
15.1 Objet 78
15.2 NDR 1.6 – Gestion des accès sans fil 79
15.2.1 Exigences 79
15.2.2 Justification et recommandations complémentaires 79
15.2.3 Amélioration d'exigences 79
15.2.4 Niveaux de sécurité 79
15.3 NDR 1.13 – Accès par l'intermédiaire de réseaux non sécurisés 79
15.3.1 Exigences 79
15.3.2 Justification et recommandations complémentaires 79
15.3.3 Amélioration d'exigences 80
15.3.4 Niveaux de sécurité 80
15.4 NDR 2.4 – Code mobile 80
15.4.1 Exigences 80
15.4.2 Justification et recommandations complémentaires 80
15.4.3 Amélioration d'exigences 80
15.4.4 Niveaux de sécurité 81
15.5 NDR 2.13 – Utilisation d'interfaces physiques de diagnostic et d'essai 81
15.5.1 Exigences 81
15.5.2 Justification et recommandations complémentaires 81
15.5.3 Amélioration d'exigences 81
15.5.4 Niveaux de sécurité 81
15.6 NDR 3.2 – Protection contre les programmes malveillants 81
15.6.1 Exigences 81
15.6.2 Justification et recommandations complémentaires 82
15.6.3 Amélioration d'exigences 82

This is a preview - click here to buy the full publication

15.6.4 Niveaux de sécurité 82
15.7 NDR 3.10 – Support pour les mises à jour 82
15.7.1 Exigences 82
15.7.2 Justification et recommandations complémentaires 82
15.7.3 Amélioration d'exigences 82
15.7.4 Niveaux de sécurité 82
15.8 NDR 3.11 – Résistance aux violations physiques et détection 83
15.8.1 Exigences 83
15.8.2 Justification et recommandations complémentaires 83
15.8.3 Amélioration d'exigences 83
15.8.4 Niveaux de sécurité 83
15.9 NDR 3.12 – Fourniture des racines de confiance du fournisseur de produit 83
15.9.1 Exigences 83
15.9.2 Justification et recommandations complémentaires 83
15.9.3 Amélioration d'exigences 84
15.9.4 Niveaux de sécurité 84
15.10 NDR 3.13 – Fourniture des racines de confiance du propriétaire d'actif 84
15.10.1 Exigences 84
15.10.2 Justification et recommandations complémentaires 84
15.10.3 Amélioration d'exigences 85
15.10.4 Niveaux de sécurité 85
15.11 NDR 3.14 – Intégrité du processus d'amorçage 85
15.11.1 Exigences 85
15.11.2 Justification et recommandations complémentaires 85
15.11.3 Amélioration d'exigences 85
15.11.4 Niveaux de sécurité 85
15.12 NDR 5.2 – Protection des limites de zone 86
15.12.1 Exigences 86
15.12.2 Justification et recommandations complémentaires 86
15.12.3 Amélioration d'exigences 86
15.12.4 Niveaux de sécurité 86
15.13 NDR 5.3 – Restrictions des communications entre des personnes d'ordre général 87
15.13.1 Exigences 87
15.13.2 Justification et recommandations complémentaires 87
15.13.3 Amélioration d'exigences 87
15.13.4 Niveaux de sécurité 87
Annexe A (informative) Catégories d'appareils 88
A.1 Généralités 88
A.2 Catégorie d'appareil: appareil intégré 88
A.2.1 Automate programmable (PLC) 88
A.2.2 Appareil électronique intelligent (IED) 88
A.3 Catégorie d'appareil: appareil de réseau 89
A.3.1 Commutateur 89
A.3.2 Terminateur RPV (réseau privé virtuel) 89
A.4 Catégorie d'appareil: appareil/application hôte 89
A.4.1 Poste de travail de l'opérateur 89
A.4.2 Historique des données 90
Annexe B (informative) Mapping des CR et des RE avec les FR des SL 1 à 4 91

This is a preview - click here to buy the full publication

B.1 Vue d'ensemble 91
B.2 Tableau de mapping des niveaux de sécurité 91
Bibliographie 97

Figure 1 – Parties de la série IEC 62443 16

Tableau B.1 – Mapping des CR et des RE avec les niveaux FR SL 1-4 92

This is a preview - click here to buy the full publication

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

SÉCURITÉ DES SYSTÈMES D'AUTOMATISATION ET DE COMMANDE INDUSTRIELLES –

Partie 4-2: Exigences de sécurité technique des composants IACS

AVANT-PROPOS

1) La Commission Electrotechnique Internationale (IEC) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de l'IEC). L'IEC a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. À cet effet, l'IEC – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de l'IEC"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'IEC, participent également aux travaux. L'IEC collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
2) Les décisions ou accords officiels de l'IEC concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de l'IEC intéressés sont représentés dans chaque comité d'études.
3) Les Publications de l'IEC se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de l'IEC. Tous les efforts raisonnables sont entrepris afin que l'IEC s'assure de l'exactitude du contenu technique de ses publications; l'IEC ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de l'IEC s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de l'IEC dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de l'IEC et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) L'IEC elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de l'IEC. L'IEC n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
7) Aucune responsabilité ne doit être imputée à l'IEC, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de l'IEC, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de l'IEC ou de toute autre Publication de l'IEC, ou au crédit qui lui est accordé.
8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de l'IEC peuvent faire l'objet de droits de brevet. L'IEC ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets et de ne pas avoir signalé leur existence.

La Norme internationale IEC 62443-4-2 a été établie par le comité d'études 65 de l'IEC: Mesure, commande et automation dans les processus industriels.

Le texte de cette Norme internationale est issu des documents suivants:

FDIS	Rapport de vote
65/XX/FDIS	65/XX/RVD

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à l'approbation de cette Norme internationale.

Ce document a été rédigé selon les Directives ISO/IEC, Partie 2.

This is a preview - click here to buy the full publication

Une liste de toutes les parties de la série IEC 62443, publiées sous le titre général *Sécurité des systèmes d'automatisation et de commande industrielles*, peut être consultée sur le site web de l'IEC.

Les futures normes de cette série porteront dorénavant le nouveau titre général cité ci-dessus. Le titre des normes existant déjà dans cette série sera mis à jour lors de la prochaine édition.

Le comité a décidé que le contenu de ce document ne sera pas modifié avant la date de stabilité indiquée sur le site web de l'IEC sous "http://webstore.iec.ch" dans les données relatives au document recherché. À cette date, le document sera

- reconduit,
- supprimé,
- remplacé par une édition révisée, ou
- amendé.

IMPORTANT – Le logo *"colour inside"* qui se trouve sur la page de couverture de cette publication indique qu'elle contient des couleurs qui sont considérées comme utiles à une bonne compréhension de son contenu. Les utilisateurs devraient, par conséquent, imprimer cette publication en utilisant une imprimante couleur.

This is a preview - click here to buy the full publication

INTRODUCTION

0.1 Vue d'ensemble

L'industrie des systèmes d'automatisation et de commande industrielles (IACS) utilise de plus en plus les appareils en réseau sur étagère (COTS), peu onéreux, rentables et hautement automatisés. En outre, les systèmes de commande et les réseaux non IACS sont de plus en plus interconnectés, et ce, pour des raisons commerciales tangibles. Ces appareils, technologies de réseau ouvert et connectivités accrues sont exposés dans une plus large mesure aux cyberattaques contre les matériels et les logiciels de système de commande. Cette faiblesse peut avoir des conséquences sur la santé, la sécurité et l'environnement (HSE), des conséquences financières et/ou des conséquences sur la réputation des systèmes de commande déployés.

Les organisations qui choisissent de déployer des solutions en matière de cybersécurité des technologies de l'information (IT) d'entreprise pour assurer la sécurité du système d'automatisation et de commande industrielles (IACS) peuvent ne pas totalement appréhender les effets de leur décision. Même si de nombreuses applications IT d'entreprise et solutions de sécurité peuvent être appliquées à l'IACS, il convient de le faire de manière appropriée afin d'éliminer toutes les conséquences indésirables. C'est la raison pour laquelle la méthode de définition des exigences du système est fondée sur une combinaison d'exigences fonctionnelles et d'appréciation du risque, ce qui implique souvent d'être également sensible aux enjeux opérationnels.

Il convient que les contre-mesures mises en place en matière de sécurité IACS ne soient pas susceptibles de provoquer des pertes de services et de fonctions essentiels, y compris les procédures d'urgence (les contre-mesures de sécurité IT, souvent déployées, présentent ce risque). La sécurité IACS a pour principaux objectifs la disponibilité du système de commande, la protection de l'usine, le fonctionnement de l'usine (même en mode dégradé) et la réponse du système prioritaire. Souvent, la sécurité informatique ne met pas ces facteurs sur le même plan. La plupart du temps, il peut s'agir de protéger les informations plutôt que les actifs physiques. Il convient de définir clairement ces différents objectifs comme relevant de la sécurité, quel que soit le degré d'intégration atteint. Il convient qu'une étape fondamentale de l'appréciation du risque, telle qu'exigée par l'IEC 62443-2-1[1] [1][2], consiste à identifier les services et fonctions réellement essentiels pour le fonctionnement (dans certaines installations, le support technique peut être déterminé comme étant un service ou une fonction non essentiel(le), par exemple). Dans certains cas, il peut être acceptable, dans le cadre d'une action de sécurité, de provoquer la perte temporaire d'un service ou d'une fonction non essentiel(le), à l'inverse d'un service ou d'une fonction essentiel(le) qu'il convient de ne pas affecter.

Le présent document fournit les exigences techniques en matière de cybersécurité des composants d'un IACS, en particulier des appareils intégrés, des composants de réseau, des composants hôtes et des applications logicielles. L'Annexe A décrit des catégories d'appareils couramment utilisés dans les IACS. Les exigences du présent document sont déduites des exigences de sécurité des systèmes IACS décrites dans l'IEC 62443-3-3. Le présent document a pour objet de spécifier les capacités de sécurité permettant à un composant d'atténuer les menaces pesant sur un système présentant un niveau de sécurité (SL) donné sans l'aide de contre-mesures compensatoires. Un tableau récapitulant les SL de chacune des exigences et améliorations d'exigences définies dans le présent document est donné à l'Annexe B.

---

1 De nombreux documents de la série IEC 62443 sont en cours de révision ou d'élaboration.

2 Les chiffres entre crochets se réfèrent à la bibliographie.

This is a preview - click here to buy the full publication

L'objectif principal de la série IEC 62443 est de fournir un cadre souple permettant de résoudre aisément les vulnérabilités actuelles et futures des IACS, et de mettre en œuvre les mesures d'atténuation nécessaires de manière systématique et justifiable. Il est important de bien comprendre que la série IEC 62443 vise à étendre la sécurité d'entreprise afin d'adapter les exigences des systèmes IT d'entreprise et les combine aux exigences uniques de fortes intégrité et disponibilité dont ont besoin les IACS.

0.2 Objet et public visé

Dans la communauté IACS, le présent document s'adresse aux propriétaires d'actifs, aux intégrateurs systèmes, aux fournisseurs de produits et, le cas échéant, aux autorités compétentes. Les autorités compétentes sont les organismes gouvernementaux et les organismes de réglementation ayant autorité légale de procéder à des audits pour vérifier la conformité aux lois et règlements en vigueur.

Les intégrateurs systèmes se fondent sur le présent document pour procurer les composants de système de commande qui constituent la solution IACS. En effet, le présent document leur permet de spécifier le niveau de capacité de sécurité approprié des composants individuels qu'ils exigent. Les principales normes destinées aux intégrateurs systèmes sont l'IEC 62443-2-1 [1], l'IEC 62443-2-4 [3], l'IEC 62443-3-2 [5] [3] et l'IEC 62443-3-3. Ces normes indiquent les exigences organisationnelles et opérationnelles pour les systèmes de gestion de la sécurité et les orientent tout au long du processus de définition des zones de sécurité et des niveaux de capacité de sécurité (SL-T) à atteindre pour ces zones. Lorsque le SL-T de chaque zone a été défini, les composants présentant les capacités nécessaires de sécurité peuvent être utilisés pour atteindre le SL-T pour chaque zone.

Les fournisseurs de produits utilisent le présent document pour bien comprendre les exigences dont font l'objet les composants du système de commande pour leur niveau de capacité de sécurité (SL-C) spécifique. Un composant peut ne pas fournir une capacité exigée lui-même, mais peut être conçu pour être intégré à une entité de niveau supérieur et, par conséquent, bénéficier de ses capacités (par exemple, un appareil intégré peut ne pas maintenir lui-même un répertoire utilisateur, mais peut être intégré à un service d'authentification et d'autorisation au niveau du système, et donc toujours satisfaire aux exigences en matière de capacités d'authentification, d'autorisation et de gestion d'utilisateurs individuels). Le présent document aide les fournisseurs de produits à connaître les exigences pouvant être attribuées et les exigences convenues comme natives dans les composants. Comme cela a été défini dans la Pratique 8 de l'IEC 62443-4-1, le fournisseur de produit met à disposition la documentation relative à l'intégration correcte du composant dans un système afin de satisfaire à un SL-T spécifique.

Dans le présent document, les exigences relatives au composant (CR) sont déduites des exigences relatives au système (SR) indiquées dans l'IEC 62443-3-3. Les exigences de l'IEC 62443-3-3, appelées SR, sont déduites des exigences fondamentales (FR) générales définies dans l'IEC 62443-1-1. Les exigences relatives au composant (CR) peuvent également inclure un ensemble d'améliorations d'exigences (RE). La combinaison des CR et des RE détermine le niveau de sécurité cible qu'un composant est capable d'atteindre.

Le présent document donne les exigences pour quatre types de composants: application logicielle, appareil intégré, appareil hôte et appareil de réseau. Ainsi, les exigences pour chaque type de composant se présentent comme suit:

- Exigences relatives aux applications logicielles (SAR);
- Exigences relatives aux appareils intégrés (EDR);
- Exigences relatives aux appareils hôtes (HDR); et

[3] En cours d'élaboration. Stade au moment de la publication IEC PRVC 62443-3-2:2018.

This is a preview - click here to buy the full publication

- Exigences relatives aux appareils de réseaux (NDR);

La majorité des exigences du présent document sont les mêmes pour les quatre types de composants et sont donc de simples exigences relatives au composant. En présence d'exigences spécifiques à un seul composant, l'exigence générique les signale comme telles et précise qu'elles se trouvent dans les articles du présent document relatifs aux exigences spécifiques au composant.

La Figure 1 est une représentation graphique de la série IEC 62443 lors de la rédaction du présent document.

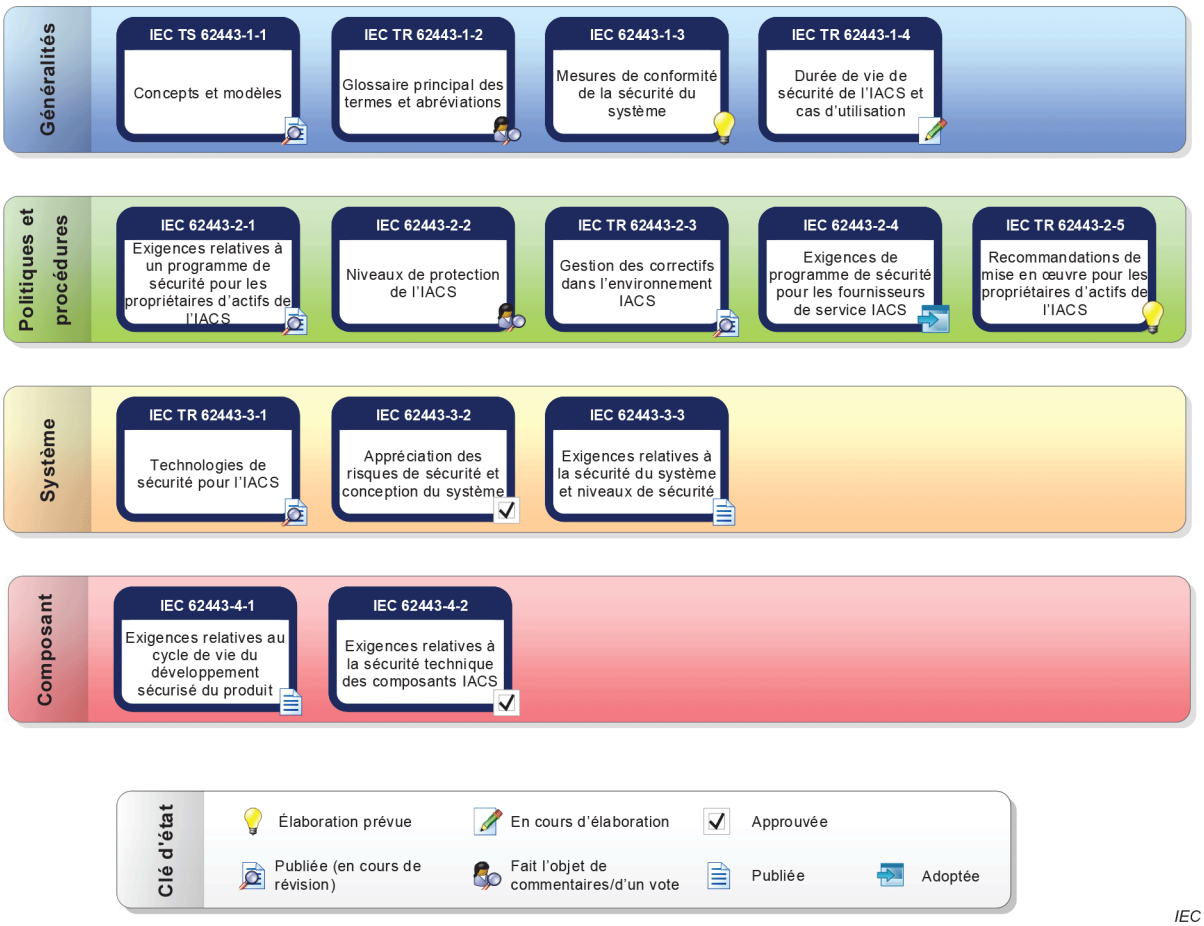


Figure 1 – Parties de la série IEC 62443

This is a preview - click here to buy the full publication

SÉCURITÉ DES SYSTÈMES D'AUTOMATISATION ET DE COMMANDE INDUSTRIELLES –

Partie 4-2: Exigences de sécurité technique des composants IACS

1 Domaine d'application

La présente partie de l'IEC 62443 indique les exigences relatives au composant (CR) d'un système de commande technique ainsi que les sept exigences fondamentales (FR) décrites dans l'IEC TS 62443-1-1, y compris la définition des exigences relatives aux niveaux de sécurité de capacité des systèmes de commande et à leurs composants, SL-C(composant).

Comme l'indique l'IEC TS 62443-1-1, il existe en tout sept exigences fondamentales (FR):

a) contrôle d'identification et d'authentification (IAC),
b) contrôle d'utilisation (UC),
c) intégrité du système (SI),
d) confidentialité des données (DC),
e) transfert de données limité (RDF),
f) réponse appropriée aux événements (TRE), et
g) disponibilité des ressources (RA).

Ces sept exigences fondamentales sont à la base de la définition des niveaux de capacité de sécurité des systèmes de commande. Le présent document a pour objet de définir les niveaux de capacité de sécurité du composant du système de commande, par opposition au SL-T ou aux niveaux de sécurité atteints (SL-A), qui n'entrent pas dans le domaine d'application.

NOTE 1 Voir l'IEC 62443-2-1 [1] pour obtenir un ensemble équivalent d'exigences de capacité non techniques liées aux programmes, nécessaires pour atteindre un niveau SL-T(système de commande).

NOTE 2 Les appellations et marques mentionnées dans le présent document sont données à l'intention des utilisateurs du présent document. Cette information ne signifie nullement que l'IEC approuve ou recommande l'emploi exclusif des produits ainsi désignés.

2 Références normatives

Les documents suivants cités dans le texte constituent, pour tout ou partie de leur contenu, des exigences du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

IEC TS 62443-1-1, *Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models* (disponible en anglais seulement)

IEC 62443-3-3:2013, *Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels* (disponible en anglais seulement)

IEC 62443-4-1, *Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements* (disponible en anglais seulement)