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

IECNORM.COM : Click to view the full PDF of IEC 62443-4-2:2019 CMV

Copyright International Electrotechnical Commission
Provided by IHS Markit under license with IEC
No reproduction or networking permitted without license from IHS

Sold to: ELECTROTECNICA ARTECHE HERMANOS, S.L.
Not for Resale,2019-06-26 2:27:52 UTC

THIS PUBLICATION IS COPYRIGHT PROTECTED
Copyright © 2019 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester. If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de l'IEC ou du Comité national de l'IEC du pays du demandeur. Si vous avez des questions sur le copyright de l'IEC ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de l'IEC de votre pays de résidence.

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

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.

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

CONTENTS

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

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

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

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

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

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

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

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

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

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

Figure 1 – Parts of the IEC 62443 series 16

Table B.1 – Mapping of CRs and REs to FR SL levels 1-4 88

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

SECURITY FOR INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS –

Part 4-2: Technical security requirements for IACS components

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 62443-4-2 has been prepared by IEC technical committee 65: Industrial-process measurement, control and automation.

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

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

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

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

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

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

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

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

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

INTRODUCTION

0.1 Overview

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

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

IACS security countermeasures should not have the potential to cause loss of essential services and functions, including emergency procedures (IT security countermeasures, as often deployed, do have this potential). IACS security goals focus on control system availability, plant protection, plant operations (even in a degraded mode) and time-critical system response. IT security goals often do not place the same emphasis on these factors; they may be more concerned with protecting information rather than physical assets. These different goals should be clearly stated as security objectives regardless of the degree of plant integration achieved. A key step in the risk assessment, as required by IEC 62443-2-1[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.

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.

Figure 1 – Parts of the IEC 62443 series

SECURITY FOR INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS –

Part 4-2: Technical security requirements for IACS components

1 Scope

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

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

a) identification and authentication control (IAC),

b) use control (UC),

c) system integrity (SI),

d) data confidentiality (DC),

e) restricted data flow (RDF),

f) timely response to events (TRE), and

g) resource availability (RA).

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

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

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

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC TS 62443-1-1, Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models

IEC 62443-3-3:2013, Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels

IEC 62443-4-1, Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements

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

3.1 Terms and definitions

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

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

3.1.1
asset
physical or logical object having either a perceived or actual value to the IACS

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

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

3.1.2
asset owner
individual or company responsible for one or more IACS

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

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

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

3.1.3
attack
unauthorized attempt to compromise the confidentiality, integrity or availability of an IACS that derives from an intelligent threat

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

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

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

3.1.4
authentication
verification of the claimed identity of an entity

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

3.1.5
authenticator
means used to confirm the identity of an entity

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

3.1.6
authenticity
property that an entity is what it claims to be through authentication of origin and verification of integrity

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

3.1.7
availability
property of ensuring timely and reliable access to and use of control system information and functionality

3.1.8
communication channel
specific logical or physical communication link between assets

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

3.1.9
compensating countermeasure
countermeasure employed in lieu of or in addition to inherent security capabilities to satisfy one or more security requirements

EXAMPLE

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

3.1.10
component
entity belonging to an IACS that exhibits the characteristics of one or more of a host device, network device, software application, or embedded device

3.1.11
conduit
logical grouping of communication channels, connecting two or more zones, that share common security requirements

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

3.1.12
confidentiality
assurance that information is not disclosed to unauthorized individuals, processes, or devices

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

3.1.13
connection
association established between two or more endpoints that supports the establishment of a session

3.1.14
control system
hardware and software components of an IACS

3.1.15
countermeasure
action, device, procedure or technique that reduces a threat, a vulnerability or the consequences of an attack by minimizing the harm the attack can cause or by discovering and reporting it so that corrective action can be taken

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

3.1.16
degraded mode
mode of operation in the presence of faults that have been anticipated in the design of the control system

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

3.1.17
device
discrete physical asset that provides a set of capabilities

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

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

3.1.18
embedded device
special purpose device designed to directly monitor or control an industrial process

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

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

3.1.19
environment
surrounding objects, region or circumstances that may influence the behaviour of the IACS and/or may be influenced by the IACS

3.1.20
essential function
function or capability that is required to maintain health, safety, the environment (HSE) and availability for the equipment under control

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

3.1.21
event
occurrence of or change to a particular set of circumstances

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

3.1.22
firecall
method established to provide emergency access to a secure control system

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

3.1.23
host device
general purpose device running an operating system (for example Microsoft Windows OS or Linux) capable of hosting one or more software applications, data stores or functions from one or more suppliers

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

3.1.24
identifier
pattern of symbols, unique within its security domain, that identifies, indicates or names an entity that makes an assertion or claim of identity

3.1.25
incident
event that is not part of the expected operation of a system or service that causes, or may cause, an interruption to, or a reduction in, the quality of the service provided by the control system

3.1.26
industrial automation and control system
collection of personnel, hardware, software and policies involved in the operation of the industrial process and that can affect or influence its safe, secure and reliable operation

3.1.27
integrity
property of protecting the accuracy and completeness of assets

3.1.28
least privilege
basic principle that holds that users (humans, software processes or devices) should be assigned the fewest privileges consistent with their assigned duties and functions

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

3.1.29
mobile code
program transferred between assets that can be executed without explicit installation by the recipient

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

3.1.30
mobile device
intelligent electronic device intended for use while being transported

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

3.1.31
network device
device that facilitates data flow between devices, or restricts the flow of data, but may not directly interact with a control process

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

3.1.32
non-repudiation
ability to prove the occurrence of a claimed event or action and its originating entities

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

3.1.33
product supplier
manufacturer of hardware and/or software product

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

3.1.34
remote access
access to a component by any user (human, software process or device) communicating from outside the perimeter of the zone being addressed

3.1.35
role
set of connected behaviors, privileges and obligations that may be assigned to a user or group of users (humans, software processes or devices) of an IACS

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

3.1.36
safety instrumented system
system used to implement one or more safety-related functions

3.1.37
security level
level corresponding to the required set of countermeasures and inherent security properties of devices and systems for a zone or conduit based on assessment of risk for the zone or conduit

3.1.38
session
semi-permanent, stateful and interactive information interchange between two or more communicating components

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

3.1.39
session ID
identifier used to indicate a specific session

3.1.40
set point
target value identified within a control system that controls one or more actions within the control system

3.1.41
software application
one or more software programs and their dependencies that are used to interface with the process or the control system itself (for example, configuration software and historian)

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

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

3.1.42
system integrator
service provider that specializes in bringing together component subsystems into a whole and ensuring that those subsystems perform in accordance with project specifications

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

3.1.43
threat
set of circumstances and associated sequence of events with the potential to adversely affect operations (including mission, functions, image or reputation), assets, control systems or individuals via unauthorized access, destruction, disclosure, modification of data and/or denial of service

3.1.44
trust
confidence that an operation, data transaction source, network or software process can be relied upon to behave as expected

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

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

3.1.45
untraceability
assurance that information cannot be used to track the time or location of a specific user

3.1.46
untrusted
not meeting predefined requirements to be trusted

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

3.1.47
update
incremental hardware or software change in order to address security vulnerabilities, bugs, reliability or operability issues

3.1.48
upgrade
incremental hardware or software change in order to add new features

3.1.49
zone
collection of entities that represents partitioning of a system under consideration on the basis of their functional, logical and physical (including location) relationship

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

3.2 Abbreviated terms and acronyms

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

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

3.3 Conventions

This document expands the SRs and REs defined in IEC 62443-3-3 into a series of CRs and REs for the components contained within an IACS. To maintain ease of tracing the CRs to the SRs in IEC 62443-3-3 the CR numbering will match the associated SR. This will cause some gaps and non-sequential numbering in this document. To provide clarity to the reader, rationale and supplemental guidance is provided for each baseline requirement and notes for any associated REs as is deemed necessary.

The types of components of an IACS as defined in this document are: software applications, host devices, embedded devices and network devices. The majority of the CRs and REs are applicable to all four types of components and are combined into a single component requirement (CR). Some CRs and REs are unique to a specific type of component. These component-type specific requirements have been separated into separate clauses for ease of reference. Requirements specific to software applications, embedded devices, host devices, and network devices are covered beginning with Clause 12. Where a component meets the definition of one or more of software application, host device, embedded device or network device, that component is expected to meet all of the requirements listed for each of the component types it satisfies.

Each of the seven FRs defined in IEC TS 62443-1-1 has a defined set of four security levels (SLs). These SLs are derived from the system security levels defined in IEC 62443-3-3. A component's security level is described per FR, using the notation SL-C(FR, component), with a corresponding value of 0 through 4. The control system capability level 0 for a particular FR is implicitly defined as no requirements. The baseline requirement and REs, if present, for each FR are then mapped to the component capability security level, SL-C(FR, component) 1 to 4.

For example, the purpose statement for Clause 8 is:

> Ensure the confidentiality of information on communication channels and in data repositories to prevent unauthorized disclosure.

The associated four SLs are defined as:

- SL 1 – Prevent the unauthorized disclosure of information via eavesdropping or casual exposure.
- SL 2 – Prevent the unauthorized disclosure of information to an entity actively searching for it using simple means with low resources, generic skills and low motivation.
- SL 3 – Prevent the unauthorized disclosure of information to an entity actively searching for it using sophisticated means with moderate resources, IACS specific skills and moderate motivation.
- SL 4 – Prevent the unauthorized disclosure of information to an entity actively searching for it using sophisticated means with extended resources, IACS specific skills and high motivation.

The individual CR and RE assignments are thus based on an incremental increase in overall component security for that particular FR based on knowledge and expertise from the team creating this document.

The SL-C(component), used throughout this document, signifies a capability required to meet a given SL rating for a given CR. A complete description of the SL vector concept can be found in IEC 62443-3-3.

4 Common component security constraints

4.1 Overview

When reading, specifying and implementing the component CRs detailed in Clauses 5 through 15 of this document, there are a number of common constraints that are required to be applied during the implementation of the requirements described in this document.

4.2 CCSC 1: Support of essential functions

The components of the system shall adhere to specific constraints as described in IEC 62443-3-3:2013, Clause 4.

4.3 CCSC 2: Compensating countermeasures

There will be cases where one or more requirements specified in this document cannot be met without the assistance of a compensating countermeasure that is external to the component. When this is the case the documentation for that component shall describe the appropriate countermeasures applied by the system to allow the requirement to be met when the component is integrated into a system.

4.4 CCSC 3: Least privilege

When required and appropriate, one or more system components (software applications, embedded devices, host devices and network devices) shall provide the capability for the system to enforce the concept of least privilege. Individual system components shall provide the granularity of permissions and flexibility of mapping those permissions to roles sufficient to support it. Individual accountability shall be available when required. Granularity of permissions and assignment is dependent on the type of device and the product documentation for the device should define this in the product documentation.

4.5 CCSC 4: Software development process

All of the components defined in this document shall be developed and supported following the secure product development processes described in IEC 62443-4-1.

5 FR 1 – Identification and authentication control

5.1 Purpose and SL-C(IAC) descriptions

Identify and authenticate all users (humans, software processes and devices), prior to allowing them access to the system or assets.

- SL 1 – Identify and authenticate all users (humans, software processes and devices) by mechanisms that protect against casual or coincidental access by unauthenticated entities.
- SL 2 – Identify and authenticate all users (humans, software processes and devices) by mechanisms that protect against intentional unauthenticated access by entities using simple means with low resources, generic skills and low motivation.
- SL 3 – Identify and authenticate all users (humans, software processes and devices) by mechanisms that protect against intentional unauthenticated access by entities using sophisticated means with moderate resources, IACS specific skills and moderate motivation.
- SL 4 – Identify and authenticate all users (humans, software processes and devices) by mechanisms that protect against intentional unauthenticated access by entities using sophisticated means with extended resources, IACS specific skills and high motivation.

5.2 Rationale

Identification of users is used in conjunction with authorization mechanisms to implement access control for a component. Verifying the identity of users requesting access is necessary to protect against unauthorized users from gaining access to the component. Recommendations and guidelines should include mechanisms that will operate in mixed modes. For example, some components on a communication channel require strong access control, such as strong authentication mechanisms, and others do not. By extension, access control requirements need to be extended to data at rest.

It is recommended that the number of identification and authentication mechanisms within a single zone is minimized. The use of multiple identification and authentication mechanisms makes the task of authentication and identification management more difficult to administer.

5.3 CR 1.1 – Human user identification and authentication

5.3.1 Requirement

Components shall provide the capability to identify and authenticate all human users according to IEC 62443-3-3 SR 1.1 on all interfaces capable of human user access. This capability shall enforce such identification and authentication on all interfaces that provide human user access to the component to support segregation of duties and least privilege in accordance with applicable security policies and procedures. This capability may be provided locally by the component or by integration into a system level identification and authentication system.

NOTE Applicable security policies are a local matter.

5.3.2 Rationale and supplemental guidance

All human users need to be identified and authenticated for all access to the component. Authentication of the identity of these users should be accomplished by using methods such as passwords, tokens, biometrics or physically keyed lids, and in the case of multifactor authentication, some combination thereof. The geographic location of human users can also be used as part of the authentication process. This requirement should be applied to both local and remote access to the component. This requirement comes in addition to the requirement of having such an authentication and identification at the system level.

Interfaces capable of human user access are local user interfaces such as touchscreens, push buttons, keyboards, as well as network protocols designed for human user interactions such as hypertext transfer protocol (HTTP), HTTP secure (HTTPS), file transfer protocol (FTP), secure FTP (SFTP), protocols used for device configuration tools (which are sometimes proprietary and other times use open protocols). User identification and authentication may be role-based or group-based (such as, for some component interfaces, several users may share the same identity). User identification and authentication should not hamper fast, local emergency actions.

In order to support IAC policies, as defined according to IEC 62443-2-1 [1], the component should verify the identity of all human users as a first step. In a second step, the permissions assigned to the identified human user should be enforced (see 6.3).

5.3.3 Requirement enhancements

(1) Unique identification and authentication:

Components shall provide the capability to uniquely identify and authenticate all human users.

(2) Multifactor authentication for all interfaces

Components shall provide the capability to employ multifactor authentication for all human user access to the component.

5.3.4 Security levels

The requirements for the four security levels that relate to CR 1.1 are:

- SL-C(IAC,component) 1: CR 1.1
- SL-C(IAC,component) 2: CR 1.1 (1)
- SL-C(IAC,component) 3: CR 1.1 (1) (2)
- SL-C(IAC,component) 4: CR 1.1 (1) (2)

5.4 CR 1.2 – Software process and device identification and authentication

5.4.1 Requirement

Components shall provide the capability to identify itself and authenticate to any other component (software application, embedded devices, host devices and network devices), according to IEC 62443-3-3 SR1.2.

If the component, as in the case of an application, is running in the context of a human user, in addition, the identification and authentication of the human user according to IEC 62443-3-3 SR1.1 may be part of the component identification and authentication process towards the other components.

5.4.2 Rationale and supplemental guidance

The function of identification and authentication is to map a known identity to an unknown software process or device (henceforth referred to as an entity in 5.4.2) so as to make it known before allowing any data exchange. Allowing rogue entities to send and receive control system specific data can result in detrimental behaviour of the control system.

All entities should be identified and authenticated for all access to the control system. Authentication of the identity of such entities should be accomplished by using methods such as passwords, tokens or location (physical or logical). This requirement should be applied to both local and remote access to the control system. However, in some scenarios where individual entities are used to connect to different target systems (for example, remote vendor support), it may be technically infeasible for an entity to have multiple identities. In these cases, compensating countermeasures would have to be applied.

Special attention needs to be given when identifying and authenticating portable and mobile devices. These types of devices are a known method of introducing undesired network traffic, malware and/or information exposure to control systems, including otherwise isolated networks.

Where entities function as a single group, identification and authentication may be role-based, group-based or entity-based. It is essential that local emergency actions as well as control system essential functions not be hampered by identification or authentication requirements (see Clause 4 for a more complete discussion). For example, in common protection and control schemes, a group of devices jointly execute the protection functions and communicate with multicast messages among the devices in the group. In these cases, group authentication based on shared accounts or shared symmetric keys are commonly used.

In order to support identification and authentication control policies as defined according to IEC 62443-2-1 [1], the control system verifies the identity of all entities as a first step. In a second step, the permissions assigned to the identified entity are enforced (see 6.3).

5.4.3 Requirement enhancements

(1) Unique identification and authentication

Components shall provide the capability to uniquely identify and authenticate itself to any other component.

5.4.4 Security levels

The requirements for the four security levels that relate to CR 1.2 are:

- SL-C(IAC,component) 1: Not selected
- SL-C(IAC,component) 2: CR 1.2
- SL-C(IAC,component) 3: CR 1.2 (1)
- SL-C(IAC,component) 4: CR 1.2 (1)

5.5 CR 1.3 – Account management

5.5.1 Requirement

Components shall provide the capability to support the management of all accounts directly or integrated into a system that manages accounts according to IEC 62443-3-3 SR 1.3.

5.5.2 Rationale and supplemental guidance

A component may provide this capability by integrating into a higher-level account management system. If the capability is not integrated into a higher-level account management system then the component is expected to provide the capability natively.

A common approach meeting this requirement would be a component that delegates the valuation of authentication to a directory server (for example, LDAP or Active Directory) which provides the account management capabilities required by IEC 62443-3-3 SR 1.3.

When a component integrates into a higher-level system to provide the account management capabilities there needs to be consideration for the impact to the component in the event that the higher-level system capability becomes unavailable.

5.5.3 Requirement enhancements

None

5.5.4 Security levels

The requirements for the four security levels that relate to CR 1.3 are:

- SL-C(IAC,component) 1: CR 1.3
- SL-C(IAC,component) 2: CR 1.3
- SL-C(IAC,component) 3: CR 1.3
- SL-C(IAC,component) 4: CR 1.3

5.6 CR 1.4 – Identifier management

5.6.1 Requirement

Components shall provide the capability to integrate into a system that supports the management of identifiers and/or provide the capability to support the management of identifiers directly according to IEC 62443-3-3 SR 1.4.

5.6.2 Rationale and supplemental guidance

Accounts created under CR 1.3 – Account management (5.5) require the use of one or more identifiers to distinctly identify each account. These identifiers should be unique and unambiguous as to the account with which they are associated. Some examples of identifiers in common use are account names, UNIX user IDs, Microsoft Windows account globally unique identifiers (GUID), and bound X.509 certificates. A component may provide a local

capability to associate identifiers with accounts. If the component is integrated into a system that enforces a system-wide security policy, it is highly recommended that identifiers be associated with the same account across all components in the system. In order to accomplish this, a component should be able to integrate into a system-wide identifier management capability.

5.6.3 Requirement enhancements

None

5.6.4 Security levels

The requirements for the four security levels that relate to CR 1.4 are:

- SL-C(IAC,component) 1: CR 1.4
- SL-C(IAC,component) 2: CR 1.4
- SL-C(IAC,component) 3: CR 1.4
- SL-C(IAC,component) 4: CR 1.4

5.7 CR 1.5 – Authenticator management

5.7.1 Requirement

Components shall provide the capability to:

a) support the use of initial authenticator content;

b) support the recognition of changes to default authenticators made at installation time;

c) function properly with periodic authenticator change/refresh operation; and

d) protect authenticators from unauthorized disclosure and modification when stored, used and transmitted.

5.7.2 Rationale and supplemental guidance

In addition to an identifier (see 5.6) an authenticator is required to prove identity. Control system authenticators include, but are not limited to, tokens, symmetric keys, private keys (part of a public/private key pair), biometrics, passwords, physical keys and key cards. There should be security policies in place instructing human users to take reasonable measures to safeguard authenticators, including maintaining possession of their individual authenticators, not loaning or sharing authenticators with others and reporting lost or compromised authenticators immediately.

Authenticators have a lifecycle. When an account is created automatically a new authenticator needs to be created, in order for the account owner to be able to authenticate. For example, in a password-based system, the account has a password associated with it. Definition of the initial authenticator content could be interpreted as the administrator defining the initial password that the account management system sets for all new accounts. Being able to configure these initial values makes it harder for an attacker to guess the password between account creation and first account use (which should involve the setting of a new password by the account owner). Some control systems are installed with unattended installers that create all necessary accounts with default passwords and some embedded devices are shipped with default passwords. Over time, these passwords often become general knowledge and are documented on the Internet. Being able to change the default passwords protects the system against unauthorized users using default passwords to gain access. Passwords can be obtained from storage or from transmission when used in network authentication. The complexity of this can be increased by cryptographic protections such as encryption or hashing or by handshake protocols that do not require transmission of the password at all. Still, passwords might be subject to attacks, for example, brute force guessing or breaking the cryptographic protection of passwords in transit or storage. The window of opportunity can be reduced by changing/refreshing the passwords periodically. Similar considerations apply to

authentication systems based on cryptographic keys. Enhanced protection can be achieved by using hardware mechanisms such as hardware security modules like trusted platform modules (TPMs).

The management of authenticators should be specified in applicable security policies and procedures, for example, constraints to change default authenticators, refresh periods, specification of the protection of authenticators or firecall procedures.

Besides the capabilities for authenticator management specified in this requirement, the strength of the authentication mechanism depends on the strength of the chosen authenticator (for example, password complexity or key length in public key authentication) and the policies for validating the authenticator in the authentication process (for example, how long a password is valid or which checks are performed in public key certificate validation). For the most common authentication mechanisms, password-based and public key authentication, 5.9, 5.10 and 5.11 provide further requirements.

Use of components for some operations may be restricted, requiring additional authentication (such as tokens, keys and certificates) in order to perform some functions.

5.7.3 Requirement enhancements

(1) Hardware security for authenticators

The authenticators on which the component rely shall be protected via hardware mechanisms.

EXAMPLE Password protected memory, OTP memory, hardware data integrity checks, and device security boot mechanism.

5.7.4 Security levels

The requirements for the four security levels that relate to CR 1.5 are:

- SL-C(IAC,component) 1: CR 1.5
- SL-C(IAC,component) 2: CR 1.5
- SL-C(IAC,component) 3: CR 1.5 (1)
- SL-C(IAC,component) 4: CR 1.5 (1)

5.8 CR 1.6 – Wireless access management

The wireless access management requirements are network-component-specific and can be located as requirements for network-components in Clause 15.

5.9 CR 1.7 – Strength of password-based authentication

5.9.1 Requirement

For components that utilize password-based authentication, those components shall provide or integrate into a system that provides the capability to enforce configurable password strength according to internationally recognized and proven password guidelines.

5.9.2 Rationale and supplemental guidance

The ability to enforce configurable password strength, whether it is based on minimum length, variety of characters, or duration of time (the minimum being a one-time password) is necessary to assist in increasing the overall security of user chosen passwords. Generally accepted practices and recommendations can be found in documents such as [20].

5.9.3 Requirement enhancements

(1) Password generation and lifetime restrictions for human users

Components shall provide, or integrate into a system that provides, the capability to protect against any given human user account from reusing a password for a configurable number of generations. In addition, the component shall provide the capability to enforce password minimum and maximum lifetime restrictions for human users. These capabilities shall conform to commonly accepted security industry practices. The component should provide the capability to prompt the user to change their password upon a configurable time prior to expiration.

(2) Password lifetime restrictions for all users (human, software process, or device)

Components shall provide, or integrate into a system that provides, the capability to enforce password minimum and maximum lifetime restrictions for all users.

5.9.4 Security levels

The requirements for the four security levels that relate to CR 1.7 are:

- SL-C(IAC,component) 1: CR 1.7
- SL-C(IAC,component) 2: CR 1.7
- SL-C(IAC,component) 3: CR 1.7 (1)
- SL-C(IAC,component) 4: CR 1.7 (1) (2)

5.10 CR 1.8 – Public key infrastructure certificates

5.10.1 Requirement

When public key infrastructure (PKI) is utilized, the component shall provide or integrate into a system that provides the capability to interact and operate in accordance with IEC 62443-3-3 SR1.8.

5.10.2 Rationale and supplemental guidance

The selection of an appropriate PKI should consider the organization's certificate policy which should be based on the risk associated with a breach of confidentiality of the protected information. Guidance on the policy definition can be found in commonly accepted standards and guidelines, such as the Internet Engineering Task Force (IETF) Request for Comment (RFC) 3647 [22] for X.509-based PKI. For example, the appropriate location of a certification authority (CA), whether within the control system versus on the Internet, and the list of trusted CAs should be considered in the policy and depends on the network architecture (see also IEC 62443-2-1 [1]).

5.10.3 Requirement enhancements

None

5.10.4 Security levels

The requirements for the four security levels that relate to CR 1.8 are:

- SL-C(IAC,component) 1: Not selected
- SL-C(IAC,component) 2: CR 1.8
- SL-C(IAC,component) 3: CR 1.8
- SL-C(IAC,component) 4: CR 1.8

5.11 CR 1.9 – Strength of public key-based authentication

5.11.1 Requirement

For components that utilize public-key-based authentication, those components shall provide directly or integrate into a system that provides the capability within the same IACS environment to:

a) validate certificates by checking the validity of the signature of a given certificate;

b) validate the certificate chain or, in the case of self-signed certificates, by deploying leaf certificates to all hosts that communicate with the subject to which the certificate is issued;

c) validate certificates by checking a given certificate's revocation status;

d) establish user (human, software process or device) control of the corresponding private key;

e) map the authenticated identity to a user (human, software process or device); and

f) ensure that the algorithms and keys used for the public key authentication conform to 8.5.

5.11.2 Rationale and supplemental guidance

To meet the requirements in 5.11.1 does not necessarily require a real time connection to a certificate authority. Alternative out-of-band methods may be used to meet the requirements in 5.11.1. For example, a disconnected system could install and update certifications using manual out-of-band processes.

Public/private key cryptography strongly depends on the secrecy of a given subject's private key and proper handling of the trust relationships. When verifying a trust between two entities based on public key authentication, it is essential to trace the public key certificate to a trusted entity. A common implementation error in certificate validation is to only check the validity of a certificate's signature, but not checking the trust in the signer. In a PKI setting, a signer is trusted if they are a trusted CA or have a certificate issued by a trusted CA, thus all verifiers need to trace certificates presented to them back to a trusted CA. If such a chain of trusted CAs cannot be established, the presented certificate should not be trusted.

If self-signed certificates are used instead of a PKI, the certificate subject itself signed its certificate, thus there never is a trusted third-party or CA. This should be compensated by deploying the self-signed public key certificates to all peers that need to validate them via an otherwise secured mechanism (for example, configuration of all peers in a trusted environment). Trusted certificates need to be distributed to peers through secure channels. During the validation process, a self-signed certificate should only be trusted if it is already present in the list of trusted certificates of the validating peer. The set of trusted certificates should be configured to the minimum necessary set.

In both cases, validation needs to also consider the possibility that a certificate is revoked. In a PKI setting this is typically done by maintaining certificate revocation lists (CRLs) or running an online certificate status protocol (OCSP) server. When revocation checking is not available due to control system constraints, mechanisms such as a short certificate lifetime can compensate for the lack of timely revocation information. Note that short lifetime certificates can sometimes create significant operational issues in a control system environment.

It is expected that most components will integrate into an IACS and leverage the key authentication mechanisms provided by the underlying IACS. When implementing public key authentication at the component-level of an IACS, protection of the key becomes a primary concern and objective of key storage on that component. Care should be taken in the implementation to ensure that any private keys stored within the component cannot be retrieved or tampered with (see 5.7).

NOTE Tamper resistant design methodologies and technologies are available to assist with designing a secure private key protection mechanism.

5.11.3 Requirement enhancements

(1) Hardware security for public key-based authentication

Components shall provide the capability to protect critical, long-lived private keys via hardware mechanisms.

5.11.4 Security levels

The requirements for the four security levels that relate to CR 1.9 are:

- SL-C(IAC,component) 1: Not selected
- SL-C(IAC,component) 2: CR 1.9
- SL-C(IAC,component) 3: CR 1.9 (1)
- SL-C(IAC,component) 4: CR 1.9 (1)

5.12 CR 1.10 – Authenticator feedback

5.12.1 Requirement

When a component provides an authentication capability, the component shall provide the capability to obscure feedback of authenticator information during the authentication process.

5.12.2 Rationale and supplemental guidance

Obscuring feedback protects the information from possible exploitation by unauthorized individuals, for example, displaying asterisks or other random characters when a human user types in a username and/or password obscures feedback of authentication information. Other examples include the entry of secure socket shell (SSH) token and one-time passwords. The authenticating entity should not provide any hint as to the reason for the authentication failure, such as “unknown user name.”

5.12.3 Requirement enhancements

None

5.12.4 Security levels

The requirements for the four SL levels that relate to CR 1.10 are:

- SL-C(IAC,component) 1: CR 1.10
- SL-C(IAC,component) 2: CR 1.10
- SL-C(IAC,component) 3: CR 1.10
- SL-C(IAC,component) 4: CR 1.10

5.13 CR 1.11 – Unsuccessful login attempts

5.13.1 Requirement

When a component provides an authentication capability, the component shall provide the capability to:

a) enforce a limit of a configurable number of consecutive invalid access attempts by any user (human, software process or device) during a configurable time period; and

b) deny access for a specified period of time or until unlocked by an administrator when this limit has been reached. An administrator may unlock an account prior to the expiration of the timeout period.

5.13.2 Rationale and supplemental guidance

Due to the potential for denial of service, the number of consecutive invalid access attempts may be limited. If enabled, the application or device may automatically reset to zero the number of access attempts after a predetermined time period established by the applicable security policies and procedures. Resetting the access attempts to zero will allow users (human, software process or device) to gain access if they have the correct login credentials. Automatic (without human intervention) denial of access for control system operator workstations or nodes should not be used when immediate operator responses are required in emergency situations. All lockout mechanisms should consider functional requirements for continuous operations so as to mitigate adverse denial of service operating conditions which could result in system failures or compromising the safety of the system. Allowing interactive logins to an account used for critical services could provide a potential for denial of service or other abuse.

5.13.3 Requirement enhancements

None

5.13.4 Security levels

The requirements for the four SL levels that relate to CR 1.11 are:

- SL-C(IAC,component) 1: CR 1.11
- SL-C(IAC,component) 2: CR 1.11
- SL-C(IAC,component) 3: CR 1.11
- SL-C(IAC,component) 4: CR 1.11

5.14 CR 1.12 – System use notification

5.14.1 Requirement

When a component provides local human user access/HMI, it shall provide the capability to display a system use notification message before authenticating. The system use notification message shall be configurable by authorized personnel.

5.14.2 Rationale and supplemental guidance

Privacy and security policies and procedures need to be consistent with applicable laws, directives, policies, regulations, standards and guidance. Often, the main justification for this requirement is legal prosecution of violators and proving intentional breach. This capability is thus necessary to support policy requirements, and might improve IACS security because it can be used as a deterrent. System use notification messages can be implemented in the form of warning banners displayed when individuals log in to the control system. A warning banner implemented as a posted physical notice in the control system facility does not protect against remote login issues.

Examples of elements for inclusion in the system use notification message are:

a) that the individual is accessing a system owned by the asset owner;

b) that system usage may be monitored, recorded and subject to audit;

c) that unauthorized use of the system is prohibited and subject to criminal and/or civil penalties; and

d) that use of the system indicates consent to monitoring and recording.

5.14.3 Requirement enhancements

None

5.14.4 Security levels

The requirements for the four SL levels that relate to CR 1.12 are:

- SL-C(IAC,component) 1: CR 1.12
- SL-C(IAC,component) 2: CR 1.12
- SL-C(IAC,component) 3: CR 1.12
- SL-C(IAC,component) 4: CR 1.12

5.15 CR 1.13 – Access via untrusted networks

The access via untrusted networks requirements are component-specific and can be located as requirements for each specific component type in Clauses 12 through 15.

5.16 CR 1.14 – Strength of symmetric key-based authentication

5.16.1 Requirement

For components that utilize symmetric keys, the component shall provide the capability to:

a) establish the mutual trust using the symmetric key;

b) store securely the shared secret (the authentication is valid as long as the shared secret remains secret);

c) restrict access to the shared secret; and

d) ensure that the algorithms and keys used for the symmetric key authentication conform to 8.5.

5.16.2 Rationale and supplemental guidance

Means should be defined for installing the keys into the component. This may include installing and managing the component key using out-of-band methods. This is necessary since a compromise of any symmetric keys that are stored within the component could lead to a full compromise of the system using those keys.

In practice, there are two basic ways to perform the secure authentication of a device to another: either using asymmetric cryptography (see 5.11) or by using symmetric cryptography. The choice between asymmetric and symmetric is dictated by several criteria, like key management, trust provisioning, legacy support and efficiency. Examples of symmetric key authentication schemes are Needham-Schröder or Kerberos. When symmetric key authentication is used, the party uses a secret key they have learned in the past (for example, through trust provisioning). The party proves their claimed identity by proving knowledge of the secret key (for example, by answering a challenge submitted by the other party, the examiner). The examiner has the knowledge of the same secret (also learned in the past through trust provisioning) and is able to compute the answer to the challenge performing the same cryptographic operations as the prover. The examiner can then compare the answer of the prover with its own computation. If they match, the examiner is convinced that the prover is the one they claim to be and the process can be conducted the other way around, switching roles, to achieve mutual-authentication. This mechanism is secure only if the shared secret is only known by the prover and the examiner and if the secret is diversified per prover. One instance of such a mechanism is the proper use of cipher-based message authentication code (CMAC) computations or alternatively the Galois counter mode (GCM)/Galois message authentication code (GMAC) operation modes.

5.16.3 Requirement enhancements

(1) Hardware security for symmetric key-based authentication

Components shall provide the capability to protect critical, long lived symmetric keys via hardware mechanisms.

5.16.4 Security levels

The requirements for the four SL levels that relate to CR 1.14 are:

- SL-C(IAC,control system) 1: Not selected
- SL-C(IAC,control system) 2: CR 1.14
- SL-C(IAC,control system) 3: CR 1.14 (1)
- SL-C(IAC,control system) 4: CR 1.14 (1)

6 FR 2 – Use control

6.1 Purpose and SL-C(UC) descriptions

Enforce the assigned privileges of an authenticated user (human, software process or device) to perform the requested action on the component and monitor the use of these privileges.

- SL 1 – Restrict use of the IACS according to specified privileges to protect against casual or coincidental misuse.
- SL 2 – Restrict use of the IACS according to specified privileges to protect against circumvention by entities using simple means with low resources, generic skills and low motivation.
- SL 3 – Restrict use of the IACS according to specified privileges to protect against circumvention by entities using sophisticated means with moderate resources, IACS specific skills and moderate motivation.
- SL 4 – Restrict use of the IACS according to specified privileges to protect against circumvention by entities using sophisticated means with extended resources, IACS specific skills and high motivation.

6.2 Rationale

Once the user is identified and authenticated, the component should restrict the allowed actions to the authorized use of the component. Asset owners and system integrators will have to assign, to each user (human, software process or device), group, role, etc. (see 4.5), the privileges defining the authorized use of the component. The goal of use control is to protect against unauthorized actions on the component's resources by verifying that the necessary privileges have been granted before allowing a user to perform the actions. Examples of actions are reading or writing data, downloading programs and setting configurations. Recommendations and guidelines should include mechanisms that will operate in mixed modes. For example, some component resources require strong use control protection, such as restrictive privileges, and others do not. By extension, use control requirements should be extended to data at rest. User privileges may vary based on time-of-day/date, location and means by which access is made.

6.3 CR 2.1 – Authorization enforcement

6.3.1 Requirement

Components shall provide an authorization enforcement mechanism for all identified and authenticated users based on their assigned responsibilities.

6.3.2 Rationale and supplemental guidance

Use control policies (for example, identity-based policies, role-based policies and rule-based policies) and associated read/write access enforcement mechanisms (for example, access control lists, access control matrices and cryptography) are employed to control usage between users (humans, software processes and devices) and assets (for example, devices, files, records, software processes, programs and domains).

After the control system has verified the identity of a user (human, software process or device) (see 5.3 and 5.4), it also has to verify that a requested operation is actually permitted according to the defined security policies and procedures. For example, in a role-based access control policy, the control system would check which roles are assigned to a verified user or asset and which privileges are assigned to these roles – if the requested operation is covered by the permissions, it is executed, otherwise rejected. This allows the enforcement of segregation of duties and least privileges. Usage enforcement mechanisms should not be allowed to adversely affect the operational performance of the control system.

Planned or unplanned changes to control system components can have significant effects on the overall security of the control system. Accordingly, only qualified and authorized individuals should obtain the use of control system components for purposes of initiating changes, including upgrades and modifications.

6.3.3 Requirement enhancements

(1) Authorization enforcement for all users (humans, software processes and devices)

Components shall provide an authorization enforcement mechanism for all users based on their assigned responsibilities and least privilege.

(2) Permission mapping to roles

Components shall, directly or through a compensating security mechanism, provide for an authorized role to define and modify the mapping of permissions to roles for all human users.

Roles should not be limited to fixed nested hierarchies in which a higher-level role is a super set of a lesser privileged role. For example, a system administrator should not necessarily encompass operator privileges.

NOTE 1 This RE is applicable to software processes and devices as well.

(3) Supervisor override

Components shall support a supervisor manual override for a configurable time or sequence of events.

NOTE 2 Implementation of a controlled, audited and manual override of automated mechanisms in the event of emergencies or other serious events allows a supervisor to enable an operator to quickly react to unusual conditions without closing the current session and establishing a new session as a higher privilege human user.

(4) Dual approval

Components shall support dual approval when action can result in serious impact on the industrial process.

Dual approval should be limited to actions which require a very high level of confidence that they will be performed reliably and correctly. Requiring dual approval provides emphasis to the seriousness of consequences that would result from failure of a correct action. An example of a situation in which dual approval is required would be a change to a set point of a critical industrial process. Dual approval mechanisms should not be employed when an immediate response is necessary to safeguard HSE consequences, for example, emergency shutdown of an industrial process.

6.3.4 Security levels

The requirements for the four security levels that relate to CR 2.1 are:

- SL-C(UC,component) 1: CR 2.1
- SL-C(UC,component) 2: CR 2.1 (1) (2)
- SL-C(UC,component) 3: CR 2.1 (1) (2) (3)
- SL-C(UC,component) 4: CR 2.1 (1) (2) (3) (4)

6.4 CR 2.2 – Wireless use control

6.4.1 Requirement

If a component supports usage through wireless interfaces it shall provide the capability to integrate into the system that supports usage authorization, monitoring and restrictions according to commonly accepted industry practices.

6.4.2 Rationale and supplemental guidance

Wireless use control may be implemented in different devices that make up the system. Network devices may be one of the devices that assist with use control through controls such as network admission control. For devices and applications that utilize wireless networks those devices should be able to properly utilize wireless network protection such as network admission control. Components may also implement different limitations on access based on whether the access is from wireless devices or wired devices. This does place a need that the component be able to distinguish whether the interface is through wireless or not. Some network devices provide the capability to scan for unauthorized wireless network activity in the wireless spectrum. In order to prevent a negative impact on the performance of the control system functionality, it is a good practice to deploy dedicated devices to perform checks for unauthorized network activity.

6.4.3 Requirement enhancements

None

6.4.4 Security levels

The requirements for the four SL levels that relate to CR 2.2 are:

- SL-C(UC, component) 1: CR 2.2
- SL-C(UC, component) 2: CR 2.2
- SL-C(UC, component) 3: CR 2.2
- SL-C(UC, component) 4: CR 2.2

6.5 CR 2.3 – Use control for portable and mobile devices

There is no component level requirement associated with IEC 62443-3-3 SR 2.3.

6.6 CR 2.4 – Mobile code

The use control requirements for mobile code are component-specific and can be located as requirements for each specific component type in Clauses 12 through 15.

6.7 CR 2.5 – Session lock

6.7.1 Requirement

If a component provides a human user interface, whether accessed locally or via a network, the component shall provide the capability

a) to protect against further access by initiating a session lock after a configurable time period of inactivity or by manual initiation by the user (human, software process or device); and

b) for the session lock to remain in effect until the human user who owns the session, or another authorized human user, re-establishes access using appropriate identification and authentication procedures.

6.7.2 Rationale and supplemental guidance

Session locks are used to prevent access to specified workstations or nodes. Components should activate session lock mechanisms automatically after a configurable time period. In most cases, the session locks are configured at the system level. Session locks implemented as part of this requirement may be pre-empted or limited by remote session termination, as defined in 6.8.

6.7.3 Requirement enhancements

None

6.7.4 Security levels

The requirements for the four SL levels that relate to CR 2.5 are:

- SL-C(UC, component) 1: CR 2.5
- SL-C(UC, component) 2: CR 2.5
- SL-C(UC, component) 3: CR 2.5
- SL-C(UC, component) 4: CR 2.5

6.8 CR 2.6 – Remote session termination

6.8.1 Requirement

If a component supports remote sessions, the component shall provide the capability to terminate a remote session either automatically after a configurable time period of inactivity, manually by a local authority, or manually by the user (human, software process or device) who initiated the session.

6.8.2 Rationale and supplemental guidance

A remote session is initiated whenever a component is accessed across the boundary of a zone defined by the asset owner based on their risk assessment. This requirement may be limited to sessions that are used for component monitoring and maintenance activities (not critical operations) based on the risk assessment of the control system and security policies and procedures. Some components may not allow sessions to be terminated as the session might be part of an essential function of the component.

6.8.3 Requirement enhancements

None

6.8.4 Security levels

The requirements for the four SL levels that relate to CR 2.6 are:

- SL-C(UC, component) 1: Not selected
- SL-C(UC, component) 2: CR 2.6
- SL-C(UC, component) 3: CR 2.6
- SL-C(UC, component) 4: CR 2.6

6.9 CR 2.7 – Concurrent session control

6.9.1 Requirement

Components shall provide the capability to limit the number of concurrent sessions per interface for any given user (human, software process or device).

6.9.2 Rationale and supplemental guidance

A resource starvation DoS might occur if a limit is not imposed. There is a trade-off between potentially locking out a specific user versus locking out all users and services due to a lack of resources. Product supplier and/or system integrator guidance is likely required to provide sufficient information as to how the number of concurrent sessions value should be assigned.

6.9.3 Requirement enhancements

None

6.9.4 Security levels

The requirements for the four SL levels that relate to CR 2.7 are:

- SL-C(UC, component) 1: Not selected
- SL-C(UC, component) 2: Not selected
- SL-C(UC, component) 3: CR 2.7
- SL-C(UC, component) 4: CR 2.7

6.10 CR 2.8 – Auditable events

6.10.1 Requirement

Components shall provide the capability to generate audit records relevant to security for the following categories:

a) access control;
b) request errors;
c) control system events;
d) backup and restore event;
e) configuration changes; and
f) audit log events.

Individual audit records shall include:

a) timestamp;
b) source (originating device, software process or human user account);
c) category;
d) type;
e) event ID; and
f) event result.

6.10.2 Rationale and supplemental guidance

Devices may contain either embedded firmware or run an OS. While the intent of the requirement is to cover categories of events, at least all events from the above categories that can be generated by the firmware or OS are to be included.

NOTE Security event categories are only applicable if functionality itself is provided by the component.

6.10.3 Requirement enhancements

None

6.10.4 Security levels

The requirements for the four security levels that relate to CR 2.8 are:

- SL-C(UC,component) 1: CR 2.8
- SL-C(UC,component) 2: CR 2.8
- SL-C(UC,component) 3: CR 2.8
- SL-C(UC,component) 4: CR 2.8

6.11 CR 2.9 – Audit storage capacity

6.11.1 Requirement

Components shall

a) provide the capability to allocate audit record storage capacity according to commonly recognized recommendations for log management; and

b) provide mechanisms to protect against a failure of the component when it reaches or exceeds the audit storage capacity.

6.11.2 Rationale and supplemental guidance

Components should provide sufficient audit storage capacity, and should consider retention policy, the auditing to be performed and the online audit processing requirements. Components may rely on the system into which they are integrated to provide the majority of audit storage capacity. However, the components should provide enough local storage to buffer audit data until it can be sent to the system.

Guidelines to be considered may include NIST Special Publication (SP) 800-92 [19]. The audit storage capacity should be sufficient to retain logs for a period of time required by applicable policies and regulations or business requirements.

6.11.3 Requirement enhancements

(1) Warn when audit record storage capacity threshold reached

Components shall provide the capability to issue a warning when the allocated audit record storage reaches a configurable threshold.

6.11.4 Security levels

The requirements for the four SL levels that relate to CR 2.9 are:

- SL-C(UC,component) 1: CR 2.9
- SL-C(UC,component) 2: CR 2.9
- SL-C(UC,component) 3: CR 2.9 (1)
- SL-C(UC,component) 4: CR 2.9 (1)

6.12 CR 2.10 – Response to audit processing failures

6.12.1 Requirement

Components shall

a) provide the capability to protect against the loss of essential services and functions in the event of an audit processing failure; and

b) provide the capability to support appropriate actions in response to an audit processing failure according to commonly accepted industry practices and recommendations.

6.12.2 Rationale and supplemental guidance

Audit generation typically occurs at the source of the event. Audit processing involves transmission, possible augmentation (such as, the addition of a timestamp) and persistent storage of the audit records. Audit processing failures include, for example, software or hardware errors, failures in the audit capturing mechanisms and audit storage capacity being reached or exceeded. Guidelines to be considered when designing appropriate response actions may include the NIST SP 800-92, Guide to Computer Security Log Management [19]. It should be noted that either overwriting the oldest audit records or halting audit log generation are possible responses to audit storage capacity being exceeded but imply the loss of potentially essential forensic information. Also alerting personnel could be an appropriate supporting action in response to an audit processing failure.

6.12.3 Requirement enhancements

None

6.12.4 Security levels

The requirements for the four SL levels that relate to CR 2.10 are:

- SL-C(UC,component) 1: CR 2.10
- SL-C(UC,component) 2: CR 2.10
- SL-C(UC,component) 3: CR 2.10
- SL-C(UC,component) 4: CR 2.10

6.13 CR 2.11 – Timestamps

6.13.1 Requirement

Components shall provide the capability to create timestamps (including date and time) for use in audit records.

6.13.2 Rationale and supplemental guidance

A good reference for the format of timestamps is ISO/IEC 8601:2004 [7]. Care should be taken when designing a system that periodic time-shift events, such as daylight savings time in some locations, are considered.

6.13.3 Requirement enhancements

(1) Time synchronization

Components shall provide the capability to create timestamps that are synchronized with a system wide time source.

(2) Protection of time source integrity

The time synchronization mechanism shall provide the capability to detect unauthorized alteration and cause an audit event upon alteration.

6.13.4 Security levels

The requirements for the four security levels that relate to CR 2.11 are:

- SL-C(UC,component) 1: CR 2.11
- SL-C(UC,component) 2: CR 2.11 (1)
- SL-C(UC,component) 3: CR 2.11 (1)
- SL-C(UC,component) 4: CR 2.11 (1) (2)

6.14 CR 2.12 – Non-repudiation

6.14.1 Requirement

If a component provides a human user interface, the component shall provide the capability to determine whether a given human user took a particular action.

Control elements that are not able to support such capability shall be listed in component documents.

6.14.2 Rationale and supplemental guidance

Examples of particular actions taken by a user include performing operator actions, changing control system configurations, creating information, sending a message, approving information (such as, indicating concurrence) and receiving a message. Non-repudiation protects against later false claims by a user of not having taken a specific action, by an author of not having authored a particular document, by a sender of not having transmitted a message, by a receiver of not having received a message or by a signatory of not having signed a document. Non-repudiation services can be used to determine if information originated from a user, if a user took specific actions (for example, sending an email and approving a work order) or received specific information. Non-repudiation services are obtained by employing various techniques or mechanisms (for example, user identification and authorization, digital signatures, digital message receipts and timestamps).

6.14.3 Requirement enhancements

(1) Non-repudiation for all users

Components shall provide the capability to determine whether a given user (human, software process or device) took a particular action.

6.14.4 Security levels

The requirements for the four SL levels that relate to CR 2.12 are:

- SL-C(UC,component) 1: CR 2.12
- SL-C(UC,component) 2: CR 2.12
- SL-C(UC,component) 3: CR 2.12
- SL-C(UC,component) 4: CR 2.12 (1)

6.15 CR 2.13 – Use of physical diagnostic and test interfaces

The use of physical diagnostic and test interfaces requirements are component-specific and can be located as requirements for each specific component type in Clauses 12 through 15.

7 FR 3 – System integrity

7.1 Purpose and SL-C(SI) descriptions

Ensure the integrity of the component to protect against unauthorized manipulation or modification.

- SL 1 – Protect the integrity of the IACS against casual or coincidental manipulation.
- SL 2 – Protect the integrity of the IACS against manipulation by someone using simple means with low resources, generic skills and low motivation.
- SL 3 – Protect the integrity of the IACS against manipulation by someone using sophisticated means with moderate resources, IACS specific skills and moderate motivation.
- SL 4 – Protect the integrity of the IACS against manipulation by someone using sophisticated means with extended resources, IACS specific skills and high motivation.

7.2 Rationale

Components often go through multiple testing cycles (unit testing, system testing, etc.) before they begin production to establish that the components will perform as intended before they even begin production. Once operational, asset owners are responsible for maintaining the integrity of the component. Using their risk assessment methodology, asset owners may assign different levels of integrity protection to different components, communication channels and information in their IACS. The integrity of physical assets should be maintained in both operational and non-operational states, such as during production, when in storage or during a maintenance shutdown. The integrity of logical assets should be maintained while in transit and at rest, such as being transmitted over a network or when residing in a data repository.

7.3 CR 3.1 – Communication integrity

7.3.1 Requirement

Components shall provide the capability to protect integrity of transmitted information.

7.3.2 Rationale and supplemental guidance

Many common network attacks are based on the manipulation of data in transmission, for example manipulation of network packets. Switched or routed networks provide a greater opportunity for attackers to manipulate packets as undetected access to these networks is generally easier and the switching and routing mechanisms themselves can also be manipulated in order to get more access to transmitted information. Manipulation in the context of a control system could include the change of measurement values communicated from a sensor to a receiver or the alteration of command parameters sent from a control application to an actuator.

Depending on the context (for example transmission within a local network segment versus transmission via untrusted networks) and the network type used in the transmission (for example transmission control protocol (TCP)/Internet protocol (IP) versus local serial links), feasible and appropriate mechanisms will vary. On a small network with direct links (point-to-point), physical access protection to all nodes may be sufficient on lower SLs if the endpoints' integrity is protected as well (see 7.6), while on a network distributed in areas with regular physical presence of staff or on a wide area network, physical access is likely not enforceable. If a commercial service is used to provide communication services as a commodity item rather than a fully dedicated service (for example a leased line versus a T1 link), it may be more difficult to obtain the necessary assurances regarding the implementation of needed security controls for communication integrity (for example because of legal restrictions). When it is infeasible or impractical to meet the necessary security requirements it may be appropriate to implement either appropriate compensating countermeasures or explicitly accept the additional risk.

Industrial equipment is often subject to environmental conditions that can lead to integrity issues and/or false positive incidents. The environment often contains particulates, liquids, vibration, gases, radiation, and electromagnetic interference (EMI) that can cause conditions that affect the integrity of the communication wiring and signals. The network infrastructure should be designed to minimize these physical/environmental effects on communication integrity. For example, when particulate, liquids, and/or gases are an issue, it may be necessary to use a sealed registered jack 45 (RJ-45) or M12 connector instead of a commercial-grade RJ-45 connector on the wire. The cable itself may need to use a different jacket instead to handle the particulate, liquid, and/or gas as well. In cases where vibration is an issue, M12 connectors may be necessary to prevent the spring pins on an RJ-45 connector from disconnecting during use. In cases where radiation and/or EMI are an issue, it may be necessary to use shielded twisted pair or fiber cables to prevent any effect on the communication signals. It may also be necessary to perform a wireless spectrum analysis in these areas if wireless networking is planned to verify that it is a viable solution.

7.3.3 Requirement enhancements

(1) Communication authentication

Components shall provide the capability to verify the authenticity of received information during communication.

NOTE Both integrity protection and authentication of origin can be achieved without providing confidentiality protection.

7.3.4 Security levels

The requirements for the four SL levels that relate to CR 3.1 are:

- SL-C(SI, component) 1: CR 3.1
- SL-C(SI, component) 2: CR 3.1 (1)
- SL-C(SI, component) 3: CR 3.1 (1)
- SL-C(SI, component) 4: CR 3.1 (1)

7.4 CR 3.2 – Protection from malicious code

The protection from malicious code requirements are component-specific and can be located as requirements for each specific component type in Clauses 12 through 15.

7.5 CR 3.3 – Security functionality verification

7.5.1 Requirement

Components shall provide the capability to support verification of the intended operation of security functions according to IEC 62443-3-3 SR3.3.

7.5.2 Rationale and supplemental guidance

The product supplier and/or system integrator should provide guidance on how to test the designed security controls. Asset owners need to be aware of the possible ramifications of running these verification tests during normal operations. Details of the execution of these verifications need to be specified with careful consideration of the requirements for continuous operations (for example, scheduling or prior notification).

Examples of security verification functions include:

- Verification of antivirus countermeasures by European Institute for Computer Antivirus Research (EICAR) testing of the control system file system. Antivirus software should detect the EICAR test samples and appropriate incident handling procedures should be triggered.
- Verification of the identification, authentication and use control countermeasures by attempting access with an unauthorized account (for some functionality this could be automated).
- Verification of intrusion detection systems (IDSs) as a security control by including a rule in the IDS that triggers on irregular, but known non-malicious traffic. The test could then be performed by introducing traffic that triggers this rule and the appropriate IDS monitoring and incident handling procedures.
- Confirmation that audit logging is occurring as required by security policies and procedures and has not been disabled by an internal or external entity.

7.5.3 Requirement enhancements

(1) Security functionality verification during normal operation

Components shall provide the capability to support verification of the intended operation of security functions during normal operations.

This RE needs to be carefully implemented to avoid detrimental effects. It may not be suitable for safety systems.

7.5.4 Security levels

The requirements for the four SL levels that relate to CR 3.3 are:

- SL-C(SI, component) 1: CR 3.3
- SL-C(SI, component) 2: CR 3.3
- SL-C(SI, component) 3: CR 3.3
- SL-C(SI, component) 4: CR 3.3 (1)

7.6 CR 3.4 – Software and information integrity

7.6.1 Requirement

Components shall provide the capability to perform or support integrity checks on software, configuration and other information as well as the recording and reporting of the results of these checks or be integrated into a system that can perform or support integrity checks.

7.6.2 Rationale and supplemental guidance

Integrity verification methods are employed to detect, record, report and protect against software and information tampering that may occur if other protection mechanisms (such as authorization enforcement) have been circumvented. Components should employ formal or recommended integrity mechanisms (such as cryptographic hashes). For example, such mechanisms could be used to monitor field devices for their latest configuration information to detect security breaches (including unauthorized changes).

7.6.3 Requirement enhancements

(1) Authenticity of software and information

Components shall provide the capability to perform or support authenticity checks on software, configuration and other information as well as the recording and reporting of the results of these checks or be integrated into a system that can perform or support authenticity checks.

(2) Automated notification of integrity violations

If the component is performing the integrity check, it shall be capable of automatically providing notification to a configurable entity upon discovery of an attempt to make an unauthorized change.

7.6.4 Security levels

The requirements for the four SL levels that relate to CR 3.4 are:

- SL-C(SI, component) 1: CR 3.4
- SL-C(SI, component) 2: CR 3.4 (1)
- SL-C(SI, component) 3: CR 3.4 (1) (2)
- SL-C(SI, component) 4: CR 3.4 (1) (2)

7.7 CR 3.5 – Input validation

7.7.1 Requirement

Components shall validate the syntax, length and content of any input data that is used as an industrial process control input or input via external interfaces that directly impacts the action of the component.

7.7.2 Rationale and supplemental guidance

Rules for checking the valid syntax of input data such as set points should be in place to verify that this information has not been tampered with and conforms to the specification. Inputs passed to interpreters should be pre-screened to prevent the content from being unintentionally interpreted as commands. Note that this is a security CR, thus it does not address human error, for example supplying a legitimate integer number which is outside the expected range.

Generally accepted industry practices for input data validation include out-of-range values for a defined field type, invalid characters in data fields, missing or incomplete data and buffer overflow. Additional examples where invalid inputs lead to system security issues include SQL injection attacks, cross-site scripting or malformed packets (as commonly generated by protocol fuzzers). Guidelines to be considered should include well-known guidelines such as the Open Web Application Security Project (OWASP) Code Review Guide [21].

7.7.3 Requirement enhancements

None

7.7.4 Security levels

The requirements for the four SL levels that relate to CR 3.5 are:

- SL-C(SI, component) 1: CR 3.5
- SL-C(SI, component) 2: CR 3.5
- SL-C(SI, component) 3: CR 3.5
- SL-C(SI, component) 4: CR 3.5

7.8 CR 3.6 – Deterministic output

7.8.1 Requirement

Components that physically or logically connect to an automation process shall provide the capability to set outputs to a predetermined state if normal operation as defined by the component supplier cannot be maintained.

7.8.2 Rationale and supplemental guidance

The deterministic behaviour of control system outputs as a result of threat actions against the control system devices and software is an important characteristic to ensure the integrity of normal operations. Ideally, the device continues to operate normally while under attack, but if the control system cannot maintain normal operation, then the control system outputs need to fail to a predetermined state. The appropriate predetermined state of control system outputs is device dependent and could be one of the following user configurable options:

- Unpowered – the outputs fail to the unpowered state;
- Hold – the outputs fail to the last-known good value; or
- Fixed – the outputs fail to a fixed value that is determined by the asset owner or an application; or
- Dynamic – the outputs fail to one of the above options based on the current state.

7.8.3 Requirement enhancements

None

7.8.4 Security levels

The requirements for the four SL levels that relate to CR 3.6 are:

- SL-C(SI, component) 1: CR 3.6
- SL-C(SI, component) 2: CR 3.6
- SL-C(SI, component) 3: CR 3.6
- SL-C(SI, component) 4: CR 3.6

7.9 CR 3.7 – Error handling

7.9.1 Requirement

Components shall identify and handle error conditions in a manner that does not provide information that could be exploited by adversaries to attack the IACS.

7.9.2 Rationale and supplemental guidance

The product supplier and/or system integrator should carefully consider the structure and content of error messages. Error messages generated by the component should provide timely and useful information without revealing potentially harmful information that could be used by adversaries to exploit the IACS. Disclosure of this information should be justified by the necessity for timely resolution of error conditions. Guidelines to be considered could include well-known guidelines such as the OWASP Code Review Guide.

A good example of an error message that could help adversaries attack an IACS would be to provide details of why authentication with the system failed. For example, stating invalid user or invalid password in the feedback would help an adversary attack the IACS and thus should not be provided.

7.9.3 Requirement enhancements

None

7.9.4 Security levels

The requirements for the four SL levels that relate to CR 3.7 are:

- SL-C(SI, component) 1: CR 3.7
- SL-C(SI, component) 2: CR 3.7
- SL-C(SI, component) 3: CR 3.7
- SL-C(SI, component) 4: CR 3.7

7.10 CR 3.8 – Session integrity

7.10.1 Requirement

Components shall provide mechanisms to protect the integrity of communications sessions including:

a) the capability to invalidate session identifiers upon user logout or other session termination (including browser sessions);

b) the capability to generate a unique session identifier for each session and recognize only session identifiers that are system-generated; and

c) the capability to generate unique session identifiers with commonly accepted sources of randomness.

7.10.2 Rationale and supplemental guidance

This control focuses on communications protection at the session, versus packet, level. The intent of this control is to establish grounds for confidence at each end of a communications session in the ongoing identity of the other party and in the validity of the information being transmitted. For example, this control addresses man-in-the-middle attacks including session hijacking, insertion of false information into a session or replay attacks. Use of session integrity mechanisms can have a significant overhead and therefore their use should be considered in light of requirements for real-time communications.

Session hijacking and other man-in-the-middle attacks or injections of false information often take advantage of easy-to-guess session IDs (keys or other shared secrets) or use of session IDs that were not properly invalidated after session termination. Therefore the validity of a session authenticator should be tightly connected to the lifetime of a session. Employing randomness in the generation of unique session IDs helps to protect against brute-force attacks to determine future session IDs.

7.10.3 Requirement enhancements

None

7.10.4 Security levels

The requirements for the four SL levels that relate to CR 3.8 are:

- SL-C(SI, component) 1: Not selected
- SL-C(SI, component) 2: CR 3.8
- SL-C(SI, component) 3: CR 3.8
- SL-C(SI, component) 4: CR 3.8

7.11 CR 3.9 – Protection of audit information

7.11.1 Requirement

Components shall protect audit information, audit logs, and audit tools (if present) from unauthorized access, modification and deletion.

7.11.2 Rationale and supplemental guidance

Audit information includes all information (for example, audit records, audit settings and audit reports) needed to successfully audit control system activity. The audit information is important for error correction, security breach recovery, investigations and related efforts. Mechanisms for enhanced protection against modification and deletion include the storage of audit information to hardware-enforced write-once media.

7.11.3 Requirement enhancements

(1) Audit records on write-once media

Components shall provide the capability to store audit records on hardware-enforced write-once media.

7.11.4 Security levels

The requirements for the four SL levels that relate to CR 3.9 are:

- SL-C(SI, component) 1: Not selected
- SL-C(SI, component) 2: CR 3.9
- SL-C(SI, component) 3: CR 3.9
- SL-C(SI, component) 4: CR 3.9 (1)

7.12 CR 3.10 – Support for updates

The support for updates requirements are component-specific and can be located as requirements for each specific device type in Clauses 12 through 15.

7.13 CR 3.11 – Physical tamper resistance and detection

The physical tamper resistance and detection requirements are component-specific and can be located as requirements for each specific device type in Clauses 12 through 15.

7.14 CR 3.12 – Provisioning product supplier roots of trust

The provisioning product supplier roots of trust requirements are component-specific and can be located as requirements for each specific device type in Clauses 12 through 15.

7.15 CR 3.13 – Provisioning asset owner roots of trust

The provisioning asset owner roots of trust requirements are component-specific and can be located as requirements for each specific device type in Clauses 12 through 15.

7.16 CR 3.14 – Integrity of the boot process

The integrity of the boot process requirements are component-specific and can be located as requirements for each specific device type in Clauses 12 through 15.

8 FR 4 – Data confidentiality

8.1 Purpose and SL-C(DC) descriptions

Ensure the confidentiality of information on communication channels and in data stored in repositories to protect against unauthorized disclosure.

- SL 1 – Prevent the unauthorized disclosure of information via eavesdropping or casual exposure.
- SL 2 – Prevent the unauthorized disclosure of information to an entity actively searching for it using simple means with low resources, generic skills and low motivation.
- SL 3 – Prevent the unauthorized disclosure of information to an entity actively searching for it using sophisticated means with moderate resources, IACS specific skills and moderate motivation.
- SL 4 – Prevent the unauthorized disclosure of information to an entity actively searching for it using sophisticated means with extended resources, IACS specific skills and high motivation.

8.2 Rationale

Some component-generated information, whether at rest or in transit, is of a confidential or sensitive nature. This implies that some communication channels and datastores require protection against eavesdropping and unauthorized access.

8.3 CR 4.1 – Information confidentiality

8.3.1 Requirement

Components shall

a) provide the capability to protect the confidentiality of information at rest for which explicit read authorization is supported; and

b) support the protection of the confidentiality of information in transit as defined in IEC 62443-3-3 SR 4.1.

8.3.2 Rationale and supplemental guidance

The decision whether a given information should be protected or not depends on the context and cannot be made at product design. However, the fact that an organization limits access to information by configuring explicit read authorizations in the control system is an indicator that this information should be protected by the organization. Thus, all information for which the component supports the capability to assign explicit read authorizations should be considered potentially sensitive and thus the component should also provide the capability to protect its confidentiality.

Confidentiality of information in transit requires system level capabilities which the component should be able to support.

For confidentiality protection, 8.5 provides further requirements.

8.3.3 Requirement enhancements

None

8.3.4 Security levels

The requirements for the four SL levels that relate to CR 4.1 are:

- SL-C(DC, component) 1: CR 4.1
- SL-C(DC, component) 2: CR 4.1
- SL-C(DC, component) 3: CR 4.1
- SL-C(DC, component) 4: CR 4.1

8.4 CR 4.2 – Information persistence

8.4.1 Requirement

Components shall provide the capability to erase all information, for which explicit read authorization is supported, from components to be released from active service and/or decommissioned.

8.4.2 Rationale and supplemental guidance

Removal of a control system component from active service should not provide the opportunity for unintentional release of information for which explicit read authorization is supported. An example of such information can include authentication information and network configuration information stored in non-volatile storage or other cryptographic information that would facilitate unauthorized or malicious activity.

Information produced by the actions of a user or role (or the actions of a software process acting on behalf of a user or role) should not be disclosed to a different user or role in an uncontrolled fashion. Control of control system information or data persistence prevents information stored on a shared resource from being unintentionally disclosed after that resource has been released back to the control system.

8.4.3 Requirement enhancements

(1) Erase of shared memory resources

Components shall provide the capability to protect against unauthorized and unintended information transfer via volatile shared memory resources.

Volatile memory resources are those that generally do not retain information after being released to memory management. However, there are attacks against random access memory (RAM) which might extract key material or other confidential data before it is actually over-written. Therefore, when volatile shared memory is released back to the control system for use by a different user, all unique data and connections to unique data need to be purged from the resource so it is not visible or accessible to the new user.

(2) Erase verification

Components shall provide the capability to verify that the erasure of information occurred.

8.4.4 Security levels

The requirements for the four SL levels that relate to CR 4.2 are:

- SL-C(DC, component) 1: Not selected
- SL-C(DC, component) 2: CR 4.2
- SL-C(DC, component) 3: CR 4.2 (1) (2)
- SL-C(DC, component) 4: CR 4.2 (1) (2)

8.5 CR 4.3 – Use of cryptography

8.5.1 Requirement

If cryptography is required, the component shall use cryptographic security mechanisms according to internationally recognized and proven security practices and recommendations.

8.5.2 Rationale and supplemental guidance

The selection of cryptographic protection should be based on a threat and risk analysis which covers the value of the information being protected, the consequences of the confidentiality and integrity of the information being breached, the time period during which the information is confidential and control system operating constraints. This can involve either information at rest, in transit, or both. Note that backups are an example of information at rest, and should be considered as part of a data confidentiality and integrity assessment process. The control system product supplier should document the practices and procedures relating to cryptographic key establishment and management. The control system should utilize established and tested encryption and hash algorithms, such as the advanced encryption standard (AES) and the secure hash algorithm (SHA) series, and key sizes based on an assigned standard. Key generation needs to be performed using an effective random number generator. The security policies and procedures for key management need to address periodic key changes, key destruction, key distribution and encryption key backup in accordance with defined standards. Generally accepted practices and recommendations can be found in documents such as NIST SP 800-57, Recommendation for Key Management – Part 1: General [18]. Implementation requirements can be found for example in FIPS 140-2, Security Requirements for Cryptographic Modules [17] or ISO/IEC 19790 [9].

This CR, along with 5.10, CR 1.8 – Public key infrastructure certificates, may be applicable when meeting many other requirements defined within this document.

8.5.3 Requirement enhancements

None

8.5.4 Security levels

The requirements for the four security levels that relate to CR 4.3 are:

- SL-C(DC,component) 1: CR 4.3
- SL-C(DC,component) 2: CR 4.3

- SL-C(DC,component) 3: CR 4.3
- SL-C(DC,component) 4: CR 4.3

9 FR 5 – Restricted data flow

9.1 Purpose and SL-C(RDF) descriptions

Segment the control system via zones and conduits to limit the unnecessary flow of data.

- SL 1 – Prevent the casual or coincidental circumvention of zone and conduit segmentation.
- SL 2 – Prevent the intended circumvention of zone and conduit segmentation by entities using simple means with low resources, generic skills and low motivation.
- SL 3 – Prevent the intended circumvention of zone and conduit segmentation by entities using sophisticated means with moderate resources, IACS specific skills and moderate motivation.
- SL 4 – Prevent the intended circumvention of zone and conduit segmentation by entities using sophisticated means with extended resources, IACS specific skills and high motivation.

9.2 Rationale

Using their risk assessment methodology defined in IEC 62443-3-2 [5], asset owners should determine necessary information flow restrictions and thus, by extension, determine the configuration of the conduits used to deliver this information. Derived recommendations and guidelines should include mechanisms that range from disconnecting control system networks from business or public networks to using unidirectional gateways, single stateful firewalls or DMZ configurations to manage the flow of information.

9.3 CR 5.1 – Network segmentation

9.3.1 Requirement

Components shall support a segmented network to support zones and conduits, as needed, to support the broader network architecture based on logical segmentation and criticality.

9.3.2 Rationale and supplemental guidance

Network segmentation is used by organizations for a variety of purposes, including cyber security. The main reasons for segmenting networks are to reduce the exposure, or ingress, of network traffic into a control system and reduce the spread, or egress, of network traffic from a control system. This improves overall system response and reliability as well as provides a measure of cyber security protection. It also allows different network segments within the control system, including critical control systems and safety-related systems, to be segmented from other systems for an additional level of protection.

Access from the control system to the World Wide Web should be clearly justified based on control system operational requirements.

Network segmentation and the level of protection it provides will vary greatly depending on the overall network architecture used by an asset owner in their facility and even system integrators within their control systems. Logically segmenting networks based on their functionality provides some measure of protection, but may still lead to single-points-of-failure if a network device is compromised. Physically segmenting networks provides another level of protection by removing that single-point-of-failure case, but will lead to a more complex and more costly network design. These trade-offs will need to be evaluated during the network design process (see IEC 62443-2-1 [1]).

In response to an incident, it may be necessary to break the connections between different network segments. In that event, the services necessary to support essential operations should be maintained in such a way that the devices can continue to operate properly and/or shutdown in an orderly manner. This may require that some servers may need to be duplicated on the control system network to support normal network features, for example dynamic host configuration protocol (DHCP), domain name service (DNS) or local CAs. It may also mean that some critical control systems and safety-related systems be designed from the beginning to be completely isolated from other networks.

9.3.3 Requirement enhancements

None

9.3.4 Security levels

The requirements for the four SL levels that relate to CR 5.1 are:

- SL-C(RDF, component) 1: CR 5.1
- SL-C(RDF, component) 2: CR 5.1
- SL-C(RDF, component) 3: CR 5.1
- SL-C(RDF, component) 4: CR 5.1

9.4 CR 5.2 – Zone boundary protection

The zone boundary protection requirements are network-component-specific and can be located as requirements for network devices in Clause 15.

9.5 CR 5.3 – General-purpose person-to-person communication restrictions

The general-purpose person-to-person communication restriction requirements are network-component-specific and can be located as requirements for network devices in Clause 15.

9.6 CR 5.4 – Application partitioning

There is no component level requirement associated with IEC 62443-3-3 SR 5.4.

10 FR 6 – Timely response to events

10.1 Purpose and SL-C(TRE) descriptions

Respond to security violations by notifying the proper authorities, reporting needed evidence of the violation and taking timely corrective action when incidents are discovered.

- SL 1 – Monitor the operation of the components of the IACS, and respond to incidents when discovered, by collecting and providing the forensic evidence when queried.
- SL 2 – Monitor the operation of the components of the IACS, and respond to incidents when discovered, by actively collecting and periodically reporting forensic evidence.
- SL 3 – Monitor the operation of the components of the IACS, and respond to incidents when discovered, by actively collecting and pushing forensic evidence to the proper authorities.
- SL 4 – Monitor the operation of the components of the IACS, and respond to incidents when discovered, by actively collecting and pushing forensic evidence to the proper authorities in near real-time.

10.2 Rationale

Although a system may begin operation in a secure state, it is important to be able to monitor the system to ensure that it remains in that secure state. If an event impacts the security of a system, timely notification of the event may be critical to mitigating the associated risk. Asset owners should establish security policies and procedures and proper lines of communication and control needed to respond to security violations. Derived recommendations and guidelines should include mechanisms that collect, report, preserve and automatically correlate the forensic evidence to ensure timely corrective action. The use of monitoring tools and techniques should not adversely affect the operational performance of the control system.

10.3 CR 6.1 – Audit log accessibility

10.3.1 Requirement

Components shall provide the capability for authorized humans and/or tools to access audit logs on a read-only basis.

10.3.2 Rationale and supplemental guidance

The applications and devices may generate audit records about events occurring in that application or device (see 6.10). Access to these audit logs is necessary to support filtering audit logs, identifying and removing information that is redundant, reviewing and reporting activity during after-the-fact investigations of security incidents. In general, audit reduction and report generation should be performed on a separate information system. Manual access to the audit records (such as, screen views or printouts) is sufficient for meeting the base requirement, but is insufficient for higher SLs. Programmatic access is commonly used to provide the audit log information to analysis mechanisms such as security information and event management (SIEM).

10.3.3 Requirement enhancements

(1) Programmatic access to audit logs

Components shall provide programmatic access to audit records by either using an application programming interface (API) or sending the audit records to a centralized system.

10.3.4 Security levels

The requirements for the four SL levels that relate to CR 6.1 are:

- SL-C(TRE, component) 1: CR 6.1
- SL-C(TRE, component) 2: CR 6.1
- SL-C(TRE, component) 3: CR 6.1 (1)
- SL-C(TRE, component) 4: CR 6.1 (1)

10.4 CR 6.2 – Continuous monitoring

10.4.1 Requirement

Components shall provide the capability to be continuously monitored using commonly accepted security industry practices and recommendations to detect, characterize and report security breaches in a timely manner.

10.4.2 Rationale and supplemental guidance

Control system monitoring capability can be achieved through a variety of tools and techniques (for example, IDS, intrusion prevention system (IPS), protection from malicious code mechanisms and network monitoring mechanisms). As attacks become more

sophisticated, these monitoring tools and techniques will need to become more sophisticated as well, including for example behaviour-based IDS/IPS.

Monitoring devices should be strategically deployed within the control system (for example, at selected perimeter locations and near server farms supporting critical applications) to collect essential information. Monitoring mechanisms may also be deployed at ad hoc locations within the control system to track specific transactions.

Monitoring should include appropriate reporting mechanisms to allow for a timely response to events. To keep the reporting focused and the amount of reported information to a level that can be processed by the recipients, mechanisms such as SIEM are commonly applied to correlate individual events into aggregate reports that establish a larger context in which the raw events occurred.

10.4.3 Requirement enhancements

None

10.4.4 Security levels

The requirements for the four SL levels that relate to CR 6.2 are:

- SL-C(TRE, component) 1: Not selected
- SL-C(TRE, component) 2: CR 6.2
- SL-C(TRE, component) 3: CR 6.2
- SL-C(TRE, component) 4: CR 6.2

11 FR 7 – Resource availability

11.1 Purpose and SL-C(RA) descriptions

Ensure the availability of components against the degradation or denial of essential services.

- SL 1 – Ensure that the component operates reliably under normal production conditions and prevents denial-of-service situations caused by the casual or coincidental actions of an entity.
- SL 2 – Ensure that the component operates reliably under normal and abnormal production conditions and prevents denial-of-service situations by entities using simple means with low resources, generic skills and low motivation.
- SL 3 – Ensure that the component operates reliably under normal, abnormal, and extreme production conditions and prevents denial-of-service situations by entities using sophisticated means with moderate resources, IACS specific skills and moderate motivation.
- SL 4 – Ensure that the component operates reliably under normal, abnormal, and extreme production conditions and prevents denial-of-service situations by entities using sophisticated means with extended resources, IACS specific skills and high motivation.

11.2 Rationale

The aim of this series of CRs is to ensure that the component is resilient against various types of DoS events. This includes the partial or total unavailability of component functionality at various levels. In particular, security incidents in the component should not affect essential functions or other safety-related functions.

11.3 CR 7.1 – Denial of service protection

11.3.1 Requirement

Components shall provide the capability to maintain essential functions when operating in a degraded mode as the result of a DoS event.

11.3.2 Rationale and supplemental guidance

Components may be subjected to different forms of DoS situations. When these occur, the component should be designed in such a manner that it maintains essential functions necessary for continued safe operations while in a degraded mode.

11.3.3 Requirement enhancements

(1) Manage communication load from component

Components shall provide the capability to mitigate the effects of information and/or message flooding types of DoS events.

11.3.4 Security levels

The requirements for the four SL levels that relate to CR 7.1 are:

- SL-C(RA, component) 1: CR 7.1
- SL-C(RA, component) 2: CR 7.1 (1)
- SL-C(RA, component) 3: CR 7.1 (1)
- SL-C(RA, component) 4: CR 7.1 (1)

11.4 CR 7.2 – Resource management

11.4.1 Requirement

Components shall provide the capability to limit the use of resources by security functions to protect against resource exhaustion.

11.4.2 Rationale and supplemental guidance

Resource management (for example, network segmentation or priority schemes) prevents a lower-priority software process from delaying or interfering with the control system servicing any higher-priority software process. For example, initiating network scans, patching and/or antivirus checks on an operating system can cause severe disruption to normal operations. Traffic rate limiting schemes should be considered as a mitigation technique.

11.4.3 Requirement enhancements

None

11.4.4 Security levels

The requirements for the four SL levels that relate to CR 7.2 are:

- SL-C(RA, component) 1: CR 7.2
- SL-C(RA, component) 2: CR 7.2
- SL-C(RA, component) 3: CR 7.2
- SL-C(RA, component) 4: CR 7.2

11.5 CR 7.3 – Control system backup

11.5.1 Requirement

Components shall provide the capability to participate in system level backup operations in order to safeguard the component state (user- and system-level information). The backup process shall not affect the normal component operations.

11.5.2 Rationale and supplemental guidance

The availability of up-to-date backups is essential for recovery from a control system failure and/or misconfiguration. Automating this function ensures that all required files are captured, reducing operator overhead.

When designing to support a backup capability, consideration should be given to information that will be stored in backups. Some of this information may contain cryptographic keys and other information that is protected through security controls while part of the system. Once the information is placed into a backup it most likely will not have the same controls in place to protect it. Thus, the component backup ability needs to include the mechanisms to support the necessary protection of the information that is contained in the backup. This may include encryption of the backup, encryption of the sensitive data as part of the backup procedure or not including the sensitive information as part of the backup. If the backup is encrypted it is important not to include the cryptographic keys as part of the backup but to backup the cryptographic keys as part of a separate more secure backup procedure.

11.5.3 Requirement enhancements

(1) Backup integrity verification

Components shall provide the capability to validate the integrity of backed up information prior to the initiation of a restore of that information.

11.5.4 Security levels

The requirements for the four SL levels that relate to CR 7.3 are:

- SL-C(RA, component) 1: CR 7.3
- SL-C(RA, component) 2: CR 7.3 (1)
- SL-C(RA, component) 3: CR 7.3 (1)
- SL-C(RA, component) 4: CR 7.3 (1)

11.6 CR 7.4 – Control system recovery and reconstitution

11.6.1 Requirement

Components shall provide the capability to be recovered and reconstituted to a known secure state after a disruption or failure.

11.6.2 Rationale and supplemental guidance

Component recovery and reconstitution to a known secure state means that all system parameters (either default or configurable) are set to secure values, security-critical patches are reinstalled, security-related configuration settings are reestablished, system documentation and operating procedures are available, components are reinstalled and configured with established settings, information from the most recent, known secure backups is loaded and the system is fully tested and functional.

11.6.3 Requirement enhancements

None

11.6.4 Security levels

The requirements for the four SL levels that relate to CR 7.4 are:

- SL-C(RA, component) 1: CR 7.4
- SL-C(RA, component) 2: CR 7.4
- SL-C(RA, component) 3: CR 7.4
- SL-C(RA, component) 4: CR 7.4

11.7 CR 7.5 – Emergency power

There is no component level requirement associated with IEC 62443-3-3 SR 7.5.

11.8 CR 7.6 – Network and security configuration settings

11.8.1 Requirement

Components shall provide the capability to be configured according to recommended network and security configurations as described in guidelines provided by the control system supplier. The component shall provide an interface to the currently deployed network and security configuration settings.

11.8.2 Rationale and supplemental guidance

These configuration settings are the adjustable parameters of the control system components. By default, the component should be configured to the recommended settings. In order for a component to detect and correct any deviations from the approved and/or recommended configuration settings, the component needs to support monitoring and control of changes to the configuration settings in accordance with security policies and procedures.

11.8.3 Requirement enhancements

(1) Machine-readable reporting of current security settings

Components shall provide the capability to generate a report listing the currently deployed security settings in a machine-readable format.

11.8.4 Security levels

The requirements for the four SL levels that relate to CR 7.6 are:

- SL-C(RA, component) 1: CR 7.6
- SL-C(RA, component) 2: CR 7.6
- SL-C(RA, component) 3: CR 7.6 (1)
- SL-C(RA, component) 4: CR 7.6 (1)

11.9 CR 7.7 – Least functionality

11.9.1 Requirement

Components shall provide the capability to specifically restrict the use of unnecessary functions, ports, protocols and/or services.

11.9.2 Rationale and supplemental guidance

Components are capable of providing a wide variety of functions and services. Some of the functions and services provided may not be necessary to support IACS functionality. Therefore, by default, functions beyond a baseline configuration should be disabled. Additionally, it is sometimes convenient to provide multiple services from a single component

of a control system, but doing so increases the risk compared to limiting the services provided by any one component.

11.9.3 Requirement enhancements

None

11.9.4 Security levels

The requirements for the four SL levels that relate to CR 7.7 are:

- SL-C(RA, component) 1: CR 7.7
- SL-C(RA, component) 2: CR 7.7
- SL-C(RA, component) 3: CR 7.7
- SL-C(RA, component) 4: CR 7.7

11.10 CR 7.8 – Control system component inventory

11.10.1 Requirement

Components shall provide the capability to support a control system component inventory according to IEC 62443-3-3 SR 7.8.

11.10.2 Rationale and supplemental guidance

Components may bring their own set of components into the overall control system. When this is the case then those components need to provide a mechanism to augment the overall component inventory which is compatible with IEC 62443-2-4 [3] SP.06.02.

11.10.3 Requirement enhancements

None

11.10.4 Security levels

The requirements for the four SL levels that relate to CR 7.8 are:

- SL-C(RA, component) 1: Not selected
- SL-C(RA, component) 2: CR 7.8
- SL-C(RA, component) 3: CR 7.8
- SL-C(RA, component) 4: CR 7.8

12 Software application requirements

12.1 Purpose

The purpose of this set of requirements is to document requirements that are specific to software applications.

12.2 SAR 2.4 – Mobile code

12.2.1 Requirement

In the event that a software application utilizes mobile code technologies, that application shall provide the capability to enforce a security policy for the usage of mobile code technologies. The security policy shall allow, at a minimum, the following actions for each mobile code technology used on the software application:

a) Control execution of mobile code;

b) Control which users (human, software process, or device) are allowed to transfer mobile code to/from the application;

c) Control the execution of mobile code based on the results of an integrity check prior to the code being executed.

12.2.2 Rationale and supplemental guidance

Mobile code technologies include, but are not limited to, Java, JavaScript, ActiveX, portable document format (PDF), Postscript, Shockwave movies, Flash animations and VBScript. Usage restrictions apply to both the selection and use of mobile code installed on servers and mobile code downloaded and executed on individual workstations. Control procedures should prevent the development, acquisition or introduction of unacceptable mobile code within the control system in which the component resides. For example, mobile code exchanges may be disallowed directly within the control system, but may be allowed in a controlled adjacent environment maintained by IACS personnel.

12.2.3 Requirement enhancements

(1) Mobile code authenticity check

The application shall provide the capability to enforce a security policy that allows the device to control execution of mobile code based on the results of an authenticity check prior to the code being executed.

12.2.4 Security levels

The requirements for the four SL levels that relate to SAR 2.4 are:

- SL-C(UC, component) 1: SAR 2.4
- SL-C(UC, component) 2: SAR 2.4 (1)
- SL-C(UC, component) 3: SAR 2.4 (1)
- SL-C(UC, component) 4: SAR 2.4 (1)

12.3 SAR 3.2 – Protection from malicious code

12.3.1 Requirement

The application product supplier shall qualify and document which protection from malicious code mechanisms are compatible with the application and note any special configuration requirements.

12.3.2 Rationale and supplemental guidance

Protection from malicious code (for example, viruses, worms, Trojan horses and spyware) may be provided by the control system application or by an external service or application. Control system applications need to be compatible with mechanisms designed to protect them from malicious code. This requirement does not imply that the product supplier is to qualify and document all malicious code protection mechanisms which are compatible with the application but implies that the product supplier is to qualify and document at least one mechanism.

12.3.3 Requirement enhancements

None

12.3.4 Security levels

The requirements for the four SL levels that relate to SAR 3.2 are:

- SL-C(SI, component) 1: SAR 3.2

- SL-C(SI, component) 2: SAR 3.2
- SL-C(SI, component) 3: SAR 3.2
- SL-C(SI, component) 4: SAR 3.2

13 Embedded device requirements

13.1 Purpose

The purpose of this set of requirements is to document requirements that are specific to embedded devices.

13.2 EDR 2.4 – Mobile code

13.2.1 Requirement

In the event that an embedded device utilizes mobile code technologies, the embedded device shall provide the capability to enforce a security policy for the usage of mobile code technologies. The security policy shall allow, at a minimum, the following actions for each mobile code technology used on the embedded device:

a) Control execution of mobile code;

b) Control which users (human, software process, or device) are allowed to upload mobile code to the device;

c) Control the execution of mobile code based on the results of an integrity check prior to the code being executed.

13.2.2 Rationale and supplemental guidance

Mobile code technologies include, but are not limited to, Java, JavaScript, ActiveX, PDF, Postscript, Shockwave movies, Flash animations and VBScript. Usage restrictions apply to both the selection and use of mobile code installed on servers and mobile code downloaded and executed on individual workstations. Control procedures should prevent the development, acquisition or introduction of unacceptable mobile code within the control system in which the component resides. For example, mobile code exchanges may be disallowed directly within the control system, but may be allowed in a controlled adjacent environment maintained by IACS personnel.

13.2.3 Requirement enhancements

(1) Mobile code authenticity check

The embedded device shall provide the capability to enforce a security policy that allows the device to control execution of mobile code based on the results of an authenticity check prior to the code being executed.

13.2.4 Security levels

The requirements for the four SL levels that relate to EDR 2.4 are:

- SL-C(UC, component) 1: EDR 2.4
- SL-C(UC, component) 2: EDR 2.4 (1)
- SL-C(UC, component) 3: EDR 2.4 (1)
- SL-C(UC, component) 4: EDR 2.4 (1)

13.3 EDR 2.13 – Use of physical diagnostic and test interfaces

13.3.1 Requirement

Embedded devices shall protect against unauthorized use of the physical factory diagnostic and test interface(s) (e.g. JTAG debugging).

13.3.2 Rationale and supplemental guidance

Factory diagnostic and test interface(s) are created at various locations within the embedded device to assist the embedded device's developers and factory personnel as they test the functional implementation, and when errors are discovered to subsequently remove them from the embedded device. However, these same interfaces should be carefully protected from access by unauthorized entities to protect the essential functionality provided by the embedded device to the IACS.

If a diagnostic and test interface does not provide an ability to control the embedded device or to access non-public information, then it will not need an authentication mechanism. This shall be determined via a threat and risk assessment. An example of this would be JTAG debugging, in which JTAG is used to take control of the processor and execute arbitrary commands, versus a JTAG boundary scan where JTAG is used to simply read information (which may be publicly available information).

There may be cases where the factory diagnostic and test interface(s) use network communications with the device. When this is the case those interfaces are to be subjected to all of the requirements of this document.

13.3.3 Requirement enhancements

(1) Active monitoring

Embedded devices shall provide active monitoring of the device's diagnostic and test interface(s) and generate an audit log entry when attempts to access these interface(s) are detected.

13.3.4 Security levels

The requirements for the four SL levels that relate to EDR 2.13 are:

- SL-C(SI, component) 1: Not selected
- SL-C(SI, component) 2: EDR 2.13
- SL-C(SI, component) 3: EDR 2.13 (1)
- SL-C(SI, component) 4: EDR 2.13 (1)

13.4 EDR 3.2 – Protection from malicious code

13.4.1 Requirement

The embedded device shall provide the capability to protect from installation and execution of unauthorized software.

13.4.2 Rationale and supplemental guidance

Unauthorized software may contain malicious code and thus be harmful to the component. If an embedded device is able to utilize a compensating control, it need not directly support protection from malicious code. It is assumed that the IACS will be responsible for providing the required safeguards. However, for scenarios such as having a local universal serial bus (USB) host access, the need for protection from malicious code should be determined by a risk assessment.

Detection mechanisms should be able to detect integrity violations of application binaries and data files. Techniques may include, but are not limited to, binary integrity and attributes monitoring, hashing and signature techniques.

Prevention techniques may include, but are not limited to, removable media control, sandbox techniques and specific computing platforms mechanisms such as restricted firmware update capabilities, No Execute (NX) bit, data execution prevention (DEP), address space layout

randomization (ASLR), stack corruption detection and mandatory access controls. See 10.4 for an associated requirement involving control system monitoring tools and techniques.

13.4.3 Requirement enhancements

None

13.4.4 Security levels

The requirements for the four SL levels that relate to EDR 3.2 are:

- SL-C(SI, component) 1: EDR 3.2
- SL-C(SI, component) 2: EDR 3.2
- SL-C(SI, component) 3: EDR 3.2
- SL-C(SI, component) 4: EDR 3.2

13.5 EDR 3.10 – Support for updates

13.5.1 Requirement

The embedded device shall support the ability to be updated and upgraded.

13.5.2 Rationale and supplemental guidance

Embedded devices over their installed lifetime may have the need for installation of updates and upgrades. There will be cases where embedded devices are supporting or executing essential functions as well. When this is the case the embedded device needs to have mechanisms in place to support patching and updating without impacting the essential functions of high availability systems (see 4.2). One example for providing this capability would be to support redundancy within the embedded device.

13.5.3 Requirement enhancements

(1) Update authenticity and integrity

The embedded device shall validate the authenticity and integrity of any software update or upgrade prior to installation.

13.5.4 Security levels

The requirements for the four SL levels that relate to EDR 3.10 are:

- SL-C(SI, component) 1: EDR 3.10
- SL-C(SI, component) 2: EDR 3.10 (1)
- SL-C(SI, component) 3: EDR 3.10 (1)
- SL-C(SI, component) 4: EDR 3.10 (1)

13.6 EDR 3.11 – Physical tamper resistance and detection

13.6.1 Requirement

The embedded device shall provide tamper resistance and detection mechanisms to protect against unauthorized physical access into the device.

13.6.2 Rationale and supplemental guidance

The purpose of tamper resistance mechanisms is to prevent an attempt by an attacker to execute an unauthorized physical action against an IACS device. Secondary to prevention, detection and response are essential should a tampering event occur.

Tamper resistance mechanisms are most effectively used in combinations to prevent access to any critical components. Tamper resistance consists of using specialized materials to make tampering of a device or module difficult. This can include such features as hardened enclosures, locks, encapsulation, or security screws. Putting in place tight airflow paths will increase the difficulty of probing the product internals.

The purpose of tamper evidence is to ensure that visible or electronic evidence remains when a tampering event occurs. Many simple evidence techniques are comprised of seals and tapes to make it obvious that there has been physical tampering. More sophisticated techniques include switches.

13.6.3 Requirement enhancements

(1) Notification of a tampering attempt

The embedded device shall be capable of automatically providing notification to a configurable set of recipients upon discovery of an attempt to make an unauthorized physical access. All notifications of tampering shall be logged as part of the overall audit logging function.

13.6.4 Security levels

The requirements for the four SL levels that relate to EDR 3.11 are:

- SL-C(SI, component) 1: Not selected
- SL-C(SI, component) 2: EDR 3.11
- SL-C(SI, component) 3: EDR 3.11 (1)
- SL-C(SI, component) 4: EDR 3.11 (1)

13.7 EDR 3.12 – Provisioning product supplier roots of trust

13.7.1 Requirement

Embedded devices shall provide the capability to provision and protect the confidentiality, integrity, and authenticity of product supplier keys and data to be used as one or more “roots of trust” at the time of manufacture of the device.

13.7.2 Rationale and supplemental guidance

In order for a component to be able to validate the authenticity and integrity of the hardware, software, and data provided by the product supplier, it should possess a trusted source of data to perform the validation process. This trusted source of data is referred to as the “root of trust” for the system. This trusted source of data may be a set of cryptographic hashes of “known good” software, or it may be the public portion of an asymmetric cryptographic key pair to be used in the validation of cryptographic signatures. This trusted data is often used to validate critical software, firmware, and data prior to booting the firmware or operating system of a component, in order to validate that the component will boot into a “known good” state in which all security mechanisms are known to be operational and uncompromised. “Root of trust” data is often protected via hardware mechanisms, preventing any modification of the data during normal operations of the component. Modification of product supplier root of trust data is typically limited to the product supplier’s provisioning process, where the product supplier has a trusted process to perform the provisioning of the data. Instead, information to be validated against the root of trust is submitted to the validation process through a hardware or software API which performs the validation and returns the results without exposing the protected data.

13.7.3 Requirement enhancements

None

13.7.4 Security levels

The requirements for the four SL levels that relate to EDR 3.12 are:

- SL-C(SI, component) 1: Not selected
- SL-C(SI, component) 2: EDR 3.12
- SL-C(SI, component) 3: EDR 3.12
- SL-C(SI, component) 4: EDR 3.12

13.8 EDR 3.13 – Provisioning asset owner roots of trust

13.8.1 Requirement

Embedded devices shall

a) provide the capability to provision and protect the confidentiality, integrity, and authenticity of asset owner keys and data to be used as “roots of trust”; and

b) support the capability to provision without reliance on components that may be outside of the device’s security zone.

13.8.2 Rationale and supplemental guidance

Product suppliers have established mechanisms to ensure that the software and firmware on their components is authentic, and the integrity of that software and firmware has not been compromised. This allows the product supplier to provide the asset owner with a “known good” state from which to operate. However, many product suppliers also provide mechanisms for asset owners to extend the functionality of their devices through the use of mobile code, user programs, or other such means. In order to protect the security of the component, it is important that these extensions to the component’s functionality also be validated to ensure that they are authorized, and that the asset owner has approved of their origins.

In order to perform these validations, the component should contain data that provides a way to differentiate between valid and invalid origins. The list of valid and invalid origins will differ from asset owner to asset owner, and it is unlikely that a product supplier will have a complete list of every possible valid origin at time of manufacture. Therefore, it is important that the product supplier provide a way for the asset owner to securely provision their own “roots of trust” which provide the ability to distinguish between origins allowed by the asset owner’s security policy, and those that are not. The authenticity and integrity of these “roots of trust” should be protected so that malicious actors cannot add additional roots of trust that grant them the ability to operate on the component.

A root of trust can also be used as a basis communications security, such as communications integrity required by CR 3.1 – Communication integrity (7.3) or communications confidentiality required by CR 4.1 – Information confidentiality (8.3).

Requirements such as EDR 2.4 – Mobile code (13.2) require the component to complete authenticity checks on mobile code prior to the execution of mobile code. The roots of trust provided by this requirement provide the data necessary to validate the origin and integrity of mobile code, allowing the component to independently determine if the code is allowed to execute.

13.8.3 Requirement enhancements

None

13.8.4 Security levels

The requirements for the four SL levels that relate to EDR 3.13 are:

- SL-C(SI, component) 1: Not selected
- SL-C(SI, component) 2: EDR 3.13
- SL-C(SI, component) 3: EDR 3.13
- SL-C(SI, component) 4: EDR 3.13

13.9 EDR 3.14 – Integrity of the boot process

13.9.1 Requirement

Embedded devices shall verify the integrity of the firmware, software, and configuration data needed for the component's boot and runtime processes prior to use.

13.9.2 Rationale and supplemental guidance

In order to make assurances to an asset owner that a component's security functionality has not been compromised, it is necessary to ensure that the component's software and firmware has not been tampered with, and that the software and firmware is valid to execute on the component. Therefore, the component should perform checks to validate the integrity of the component's firmware and/or software prior to use during the boot process, to ensure that the component does not boot into an insecure or invalid operating state that could damage the component or provide a path for a malicious actor to gain access to additional components, assets, or data.

13.9.3 Requirement enhancements

(1) Authenticity of the boot process

Embedded devices shall use the component's product supplier roots of trust to verify the authenticity of the firmware, software, and configuration data needed for the component's boot process prior to it being used in the boot process.

13.9.4 Security levels

The requirements for the four SL levels that relate to EDR 3.14 are:

- SL-C(SI, component) 1: EDR 3.14
- SL-C(SI, component) 2: EDR 3.14 (1)
- SL-C(SI, component) 3: EDR 3.14 (1)
- SL-C(SI, component) 4: EDR 3.14 (1)

14 Host device requirements

14.1 Purpose

The purpose of this set of requirements is to document requirements that are specific to host devices.

14.2 HDR 2.4 – Mobile code

14.2.1 Requirement

In the event that a host device utilizes mobile code technologies, that host device shall provide the capability to enforce a security policy for the usage of mobile code technologies. The security policy shall allow, at a minimum, the following actions for each mobile code technology used on the host device:

a) control execution of mobile code;

b) control which users (human, software process, or device) are allowed to upload mobile code to the host device; and

c) control the code execution based upon integrity checks on the mobile code and prior to the code being executed.

14.2.2 Rationale and supplemental guidance

Mobile code technologies include, but are not limited to, Java, JavaScript, ActiveX, PDF, Postscript, Shockwave movies, Flash animations and VBScript. Usage restrictions apply to both the selection and use of mobile code installed on servers and mobile code downloaded and executed on individual workstations. Control procedures should prevent the development, acquisition or introduction of unacceptable mobile code within the control system in which the host device resides. For example, mobile code exchanges may be disallowed directly with the control system, but may be allowed in a controlled adjacent environment maintained by IACS personnel.

Mobile code could be secured by adding integrity, authenticity, and authorization checks to the code itself (application layer), or for “just-in-time” code execution through transmitting the mobile code via a secure communications tunnel which provides these attributes, or any mechanism equivalent to these options.

14.2.3 Requirement enhancements

(1) Mobile code authenticity check

The host device shall provide the capability to enforce a security policy that allows the device to control execution of mobile code based on the results of an authenticity check prior to the code being executed.

14.2.4 Security levels

The requirements for the four SL levels that relate to HDR 2.4 are:

- SL-C(UC, component) 1: HDR 2.4
- SL-C(UC, component) 2: HDR 2.4(1)
- SL-C(UC, component) 3: HDR 2.4 (1)
- SL-C(UC, component) 4: HDR 2.4 (1)

14.3 HDR 2.13 – Use of physical diagnostic and test interfaces

14.3.1 Requirement

Host devices shall protect against unauthorized use of the physical factory diagnostic and test interface(s) (e.g. JTAG debugging).

14.3.2 Rationale and supplemental guidance

Factory diagnostic and test interface(s) are created at various locations within the host device to assist the component’s developers and factory personnel as they test the functional implementation, and when errors are discovered to subsequently remove them from the component. However, these same interfaces should be carefully protected from access by unauthorized entities to protect the essential functionality provided by the component to the IACS.

There may be cases where the factory diagnostic and test interface(s) use network communications with the device. When this is the case those interfaces are to be subjected to all of the requirements of this document.

If a diagnostic and test interface does not provide an ability to control the host device or to access non-public information, then it will not need an authentication mechanism. This shall be determined via a threat and risk assessment. An example of this would be JTAG debugging, in which JTAG is used to take control of the processor and execute arbitrary

commands, versus a JTAG boundary scan where JTAG is used to simply read information (which may be publicly available information).

14.3.3 Requirement enhancements

(1) Active monitoring

Host devices shall provide active monitoring of the device's diagnostic and test interface(s) and generate an audit log entry when attempts to access these interface(s) are detected.

14.3.4 Security levels

The requirements for the four SL levels that relate to HDR 2.13 are:

- SL-C(SI, component) 1: Not selected
- SL-C(SI, component) 2: HDR 2.13
- SL-C(SI, component) 3: HDR 2.13 (1)
- SL-C(SI, component) 4: HDR 2.13 (1)

14.4 HDR 3.2 – Protection from malicious code

14.4.1 Requirement

There shall be mechanisms on host devices that are qualified by the IACS product supplier to provide protection from malicious code. The IACS product supplier shall document any special configuration requirements related to protection from malicious code.

14.4.2 Rationale and supplemental guidance

Host devices need to support the use of malicious code protection (against, for example, viruses, worms, Trojan horses and spyware). The product supplier should qualify and document the configuration of protection from malicious code mechanisms so that the primary mission of the control system is maintained.

14.4.3 Requirement enhancements

(1) Report version of code protection

The host device shall automatically report the software and file versions of protection from malicious code in use (as part of overall logging function).

14.4.4 Security levels

The requirements for the four SL levels that relate to HDR 3.2 are:

- SL-C(SI, component) 1: HDR 3.2
- SL-C(SI, component) 2: HDR 3.2 (1)
- SL-C(SI, component) 3: HDR 3.2 (1)
- SL-C(SI, component) 4: HDR 3.2 (1)

14.5 HDR 3.10 – Support for updates

14.5.1 Requirement

Host devices shall support the ability to be updated and upgraded.

14.5.2 Rationale and supplemental guidance

Host devices over their installed lifetime may have the need for installation of updates and upgrades. There will be cases where host devices are supporting or executing essential

functions as well. When this is the case the host device should have mechanisms in place to support patching and updating without impacting the essential functions of high availability systems (see 4.2). One example for providing this capability would be to support redundancy within the host device.

14.5.3 Requirement enhancements

(1) Update authenticity and integrity

Host devices shall validate the authenticity and integrity of any software update or upgrade prior to installation.

14.5.4 Security levels

The requirements for the four SL levels that relate to HDR 3.10 are:

- SL-C(SI, component) 1: HDR 3.10
- SL-C(SI, component) 2: HDR 3.10 (1)
- SL-C(SI, component) 3: HDR 3.10 (1)
- SL-C(SI, component) 4: HDR 3.10 (1)

14.6 HDR 3.11 – Physical tamper resistance and detection

14.6.1 Requirement

Host devices shall provide the capability to support tamper resistance and detection mechanisms to protect against unauthorized physical access into the device.

14.6.2 Rationale and supplemental guidance

The purpose of tamper resistance mechanisms is to prevent an attempt by an attacker to execute an unauthorized physical action against an IACS device. Secondary to prevention, detection and response are essential should a tampering event occur.

Tamper resistance mechanisms are most effectively used in combinations to prevent access to any critical components. Tamper resistance consists of using specialized materials to make tampering of a device or module difficult. This can include such features as hardened enclosures, locks, encapsulation, or security screws. Putting in place tight airflow paths will increase the difficulty of probing the product internals.

The purpose of tamper evidence is to ensure that visible or electronic evidence remains when a tampering event occurs. Many simple evidence techniques are comprised of seals and tapes to make it obvious that there has been physical tampering. More sophisticated techniques include switches.

14.6.3 Requirement enhancements

(1) Notification of a tampering attempt

Host devices shall be capable of automatically providing notification to a configurable set of recipients upon discovery of an attempt to make an unauthorized physical access. All notifications of tampering shall be logged as part of the overall audit logging function.

14.6.4 Security levels

The requirements for the four SL levels that relate to HDR 3.11 are:

- SL-C(SI, component) 1: Not selected
- SL-C(SI, component) 2: HDR 3.11
- SL-C(SI, component) 3: HDR 3.11 (1)
- SL-C(SI, component) 4: HDR 3.11 (1)

14.7 HDR 3.12 – Provisioning product supplier roots of trust

14.7.1 Requirement

Host devices shall provide the capability to provision and protect the confidentiality, integrity, and authenticity of product supplier keys and data to be used as one or more “roots of trust” at the time of manufacture of the device.

14.7.2 Rationale and supplemental guidance

In order for a component to be able to validate the authenticity and integrity of the hardware, software, and data provided by the product supplier, it should possess a trusted source of data to perform the validation process. This trusted source of data is referred to as the “root of trust” for the system. This trusted source of data may be a set of cryptographic hashes of “known good” software, or it may be the public portion of an asymmetric cryptographic key pair to be used in the validation of cryptographic signatures. This trusted data is often used to validate critical software, firmware, and data prior to booting the firmware or operating system of a component, in order to validate that the component will boot into a “known good” state in which all security mechanisms are known to be operational and uncompromised. “Root of trust” data can be protected by software or hardware implemented mechanisms to prevent any modification of the data during normal operations of the component. Modification of product supplier root of trust data is typically limited to the product supplier’s provisioning process, where the product supplier has a trusted process to perform the provisioning of the data. Instead, information to be validated against the root of trust is submitted to the validation process through a hardware or software API which performs the validation and returns the results without exposing the protected data.

14.7.3 Requirement enhancements

None

14.7.4 Security levels

The requirements for the four SL levels that relate to HDR 3.12 are:

- SL-C(SI, component) 1: Not selected
- SL-C(SI, component) 2: HDR 3.12
- SL-C(SI, component) 3: HDR 3.12
- SL-C(SI, component) 4: HDR 3.12

14.8 HDR 3.13 – Provisioning asset owner roots of trust

14.8.1 Requirement

Host devices shall

a) provide the capability to provision and protect the confidentiality, integrity, and authenticity of asset owner keys and data to be used as “roots of trust”; and

b) support the capability to provision without reliance on components that may be outside of the device’s security zone.

14.8.2 Rationale and supplemental guidance

Product suppliers have established mechanisms to ensure that the software and firmware on their components is authentic, and the integrity of that software and firmware has not been compromised. This allows the product supplier to provide the asset owner with a “known good” state from which to operate. However, many product suppliers also provide mechanisms for asset owners to extend the functionality of their devices through the use of mobile code, user programs, or other such means. In order to protect the security of the component, it is important that these extensions to the component’s functionality also be

validated to ensure that they are authorized, and that the asset owner has approved of their origins.

In order to perform these validations, the component should contain data that provides a way to differentiate between valid and invalid origins. The list of valid and invalid origins will differ from asset owner to asset owner, and it is unlikely that a product supplier will have a complete list of every possible valid origin at time of manufacture. Therefore, it is important that the product supplier provide a way for the asset owner to securely provision their own “roots of trust” which provide the ability to distinguish between origins allowed by the asset owner’s security policy, and those that are not. The authenticity and integrity of these “roots of trust” should be protected so that malicious actors cannot add additional roots of trust that grant them the ability to operate on the component.

Requirements such as HDR 2.4 – Mobile code (14.2) require the component to complete authenticity checks on mobile code prior to the execution of mobile code. The roots of trust provided by this requirement provide the data necessary to validate the origin and integrity of mobile code, allowing the component to independently determine if the code is allowed to execute.

A root of trust can also be used as a basis communications security, such as communications integrity required by CR 3.1 – Communication integrity (7.3) or communications confidentiality required by CR 4.1 – Information confidentiality (8.3).

14.8.3 Requirement enhancements

None

14.8.4 Security levels

The requirements for the four SL levels that relate to HDR 3.13 are:

- SL-C(SI, component) 1: Not selected
- SL-C(SI, component) 2: HDR 3.13
- SL-C(SI, component) 3: HDR 3.13
- SL-C(SI, component) 4: HDR 3.13

14.9 HDR 3.14 – Integrity of the boot process

14.9.1 Requirement

Host devices shall verify the integrity of the firmware, software, and configuration data needed for the component’s boot process prior to it being used in the boot process.

14.9.2 Rationale and supplemental guidance

In order to make assurances to an asset owner that a component’s security functionality has not been compromised, it is necessary to ensure that the component’s software and firmware has not been tampered with, and that the software and firmware is valid to execute on the component. Therefore, the component should perform checks to validate the integrity and authenticity of the component’s firmware and/or software prior to the boot process, to ensure that the component does not boot into an insecure or invalid operating state that could damage the component or provide a path for a malicious actor to gain access to additional components, assets, or data.

14.9.3 Requirement enhancements

(1) Authenticity of the boot process

Host devices shall use the component's product supplier roots of trust to verify the authenticity of the firmware, software, and configuration data needed for the component's boot process prior to it being used in the boot process.

14.9.4 Security levels

The requirements for the four SL levels that relate to HDR 3.14 are:

- SL-C(SI, component) 1: HDR 3.14
- SL-C(SI, component) 2: HDR 3.14 (1)
- SL-C(SI, component) 3: HDR 3.14 (1)
- SL-C(SI, component) 4: HDR 3.14 (1)

15 Network device requirements

15.1 Purpose

The purpose of this set of requirements is to document requirements that are specific to network devices.

15.2 NDR 1.6 – Wireless access management

15.2.1 Requirement

A network device supporting wireless access management shall provide the capability to identify and authenticate all users (humans, software processes or devices) engaged in wireless communication.

15.2.2 Rationale and supplemental guidance

Any wireless technology can, and in most cases should, be considered as just another communication protocol option. Thus, it should be subject to the same IACS security requirements as any other communication type utilized by the IACS. However, from a security point of view, there is at least one significant difference between wired and wireless communications. Physical security countermeasures are typically less effective when using wireless.

15.2.3 Requirement enhancements

(1) Unique identification and authentication

The network device shall provide the capability to uniquely identify and authenticate all users (humans, software processes or devices) engaged in wireless communication.

15.2.4 Security levels

The requirements for the four SL levels that relate to NDR 1.6 are:

- SL-C(UC, component) 1: NDR 1.6
- SL-C(UC, component) 2: NDR 1.6 (1)
- SL-C(UC, component) 3: NDR 1.6 (1)
- SL-C(UC, component) 4: NDR 1.6 (1)

15.3 NDR 1.13 – Access via untrusted networks

15.3.1 Requirement

The network device supporting device access into a network shall provide the capability to monitor and control all methods of access to the network device via untrusted networks.

15.3.2 Rationale and supplemental guidance

The network device should protect against unauthorized connections or subversion of authorized connections.

Examples of access to the network device via untrusted networks typically include remote access methods (such as, dial-up, broadband and wireless) as well as connections from a company's office (non-control system) network. The network device may provide ACL (access control list) functionality to restrict access by:

Layer 2 forwarding devices such as Ethernet switches:

a) MAC address

b) VLAN

Layer 3 forwarding devices such as routers, gateways and firewalls:

a) IP address

b) port and protocol

c) virtual private networks

15.3.3 Requirement enhancements

(1) Explicit access request approval

The network device shall provide the capability to deny access requests via untrusted networks unless explicitly approved by an assigned role.

15.3.4 Security levels

The requirements for the four SL levels that relate to NDR 1.13 are:

- SL-C(UC, component) 1: NDR 1.13
- SL-C(UC, component) 2: NDR 1.13
- SL-C(UC, component) 3: NDR 1.13 (1)
- SL-C(UC, component) 4: NDR 1.13 (1)

15.4 NDR 2.4 – Mobile code

15.4.1 Requirement

In the event that a network device utilizes mobile code technologies, the network device shall provide the capability to enforce a security policy for the usage of mobile code technologies. The security policy shall allow, at a minimum, the following actions for each mobile code technology used on the network device:

a) control execution of mobile code;

b) control which users (human, software process, or device) are allowed to transfer mobile code to/from the network device; and

c) control the code execution based upon integrity checks on mobile code and prior to the code being executed

15.4.2 Rationale and supplemental guidance

Mobile code technologies include, but are not limited to, Java, JavaScript, ActiveX, PDF, Postscript, Shockwave movies, Flash animations and VBScript. Usage restrictions apply to both the selection and use of mobile code installed on servers and mobile code downloaded and executed on individual workstations. Control procedures should prevent the development, acquisition or introduction of unacceptable mobile code within the control system in which the component resides. For example, mobile code exchanges may be disallowed directly within

the control system, but may be allowed in a controlled adjacent environment maintained by IACS personnel.

Mobile code could be secured by adding integrity, authenticity, and authorization checks to the code itself (application layer), or for “just-in-time” code execution through transmitting the mobile code via a secure communications tunnel which provides these attributes, or any mechanism equivalent to these options.

15.4.3 Requirement enhancements

(1) Mobile code authenticity check

The network device shall provide the capability to enforce a security policy that allows the device to control execution of mobile code based on the results of an authenticity check prior to the code being executed.

15.4.4 Security levels

The requirements for the four SL levels that relate to NDR 2.4 are:

- SL-C(UC, component) 1: NDR 2.4
- SL-C(UC, component) 2: NDR 2.4 (1)
- SL-C(UC, component) 3: NDR 2.4 (1)
- SL-C(UC, component) 4: NDR 2.4 (1)

15.5 NDR 2.13 – Use of physical diagnostic and test interfaces

15.5.1 Requirement

Network devices shall protect against unauthorized use of the physical factory diagnostic and test interface(s) (e.g. JTAG debugging).

15.5.2 Rationale and supplemental guidance

Factory diagnostic and test interface(s) are created at various locations within the component to assist the component’s developers and factory personnel as they test the functional implementation, and when errors are discovered to subsequently remove them from the component. However, these same interfaces should be carefully protected from access by unauthorized entities to protect the essential functionality provided by the component to the IACS.

There may be cases where the factory diagnostic and test interface(s) use network communications with the device. When this is the case those interfaces are to be subjected to all of the requirements of this document.

Note that if a diagnostic and test interface does not provide the ability to control the product, or to access non-public information, then it will not need an authentication mechanism. This should be determined via a threat assessment. An example of this would be JTAG debugging, in which JTAG is used to take control of the processor and execute arbitrary commands, versus a JTAG boundary scan where JTAG is used to simply read information (which may be publicly available information).

15.5.3 Requirement enhancements

(1) Active monitoring

Network devices shall provide active monitoring of the device’s diagnostic and test interface(s) and generate an audit log entry when attempts to access these interface(s) are detected.

15.5.4 Security levels

The requirements for the four SL levels that relate to NDR 2.13 are:

- SL-C(SI, component) 1: Not selected
- SL-C(SI, component) 2: NDR 2.13
- SL-C(SI, component) 3: NDR 2.13 (1)
- SL-C(SI, component) 4: NDR 2.13 (1)

15.6 NDR 3.2 – Protection from malicious code

15.6.1 Requirement

The network device shall provide for protection from malicious code.

15.6.2 Rationale and supplemental guidance

If a network device is able to utilize a compensating control, it need not directly support protection from malicious code. One such possible compensating control would be the use of network packet filtering devices to identify and remove malicious code while in transit. It is assumed that the IACS will be responsible for providing the required safeguards. However, for scenarios such as having a local USB host access, the need for protection from malicious code should be evaluated.

15.6.3 Requirement enhancements

None

15.6.4 Security levels

The requirements for the four SL levels that relate to NDR 3.2 are:

- SL-C(SI, component) 1: NDR 3.2
- SL-C(SI, component) 2: NDR 3.2
- SL-C(SI, component) 3: NDR 3.2
- SL-C(SI, component) 4: NDR 3.2

15.7 NDR 3.10 – Support for updates

15.7.1 Requirement

Network devices shall support the ability to be updated and upgraded.

15.7.2 Rationale and supplemental guidance

Network devices over their installed lifetime may require installation of updates and upgrades. There will be cases where network devices are supporting or executing essential functions as well. When this is the case the network device should have mechanisms in place to support patching and updating without impacting the essential functions of high availability systems (see 4.2). One example for providing this capability would be to support redundancy within the network device.

15.7.3 Requirement enhancements

(1) Update authenticity and integrity

Network devices shall validate the authenticity and integrity of any software update or upgrade prior to installation.

15.7.4 Security levels

The requirements for the four SL levels that relate to NDR 3.10 are:

- SL-C(SI, component) 1: NDR 3.10
- SL-C(SI, component) 2: NDR 3.10 (1)
- SL-C(SI, component) 3: NDR 3.10 (1)
- SL-C(SI, component) 4: NDR 3.10 (1)

15.8 NDR 3.11 – Physical tamper resistance and detection

15.8.1 Requirement

Network devices shall provide tamper resistance and detection mechanisms to protect against unauthorized physical access into the device.

15.8.2 Rationale and supplemental guidance

The purpose of tamper resistance mechanisms is to prevent an attempt by an attacker to execute an unauthorized physical action against an IACS device. Secondary to prevention, detection and response are essential should a tampering event occur.

Tamper resistance mechanisms are most effectively used in combinations to prevent access to any critical components. Tamper resistance consists of using specialized materials to make tampering of a device or module difficult. This can include such features as hardened enclosures, locks, encapsulation, or security screws. Putting in place tight airflow paths will increase the difficulty of probing the product internals.

The purpose of tamper evidence is to ensure that visible or electronic evidence remains when a tampering event occurs. Many simple evidence techniques are comprised of seals and tapes to make it obvious that there has been physical tampering. More sophisticated techniques include switches.

15.8.3 Requirement enhancements

(1) Notification of a tampering attempt

Network devices shall be capable of automatically providing notification to a configurable set of recipients upon discovery of an attempt to make an unauthorized physical access. All notifications of tampering shall be logged as part of the overall audit logging function.

15.8.4 Security levels

The requirements for the four SL levels that relate to NDR 3.11 are:

- SL-C(SI, component) 1: Not selected
- SL-C(SI, component) 2: NDR 3.11
- SL-C(SI, component) 3: NDR 3.11 (1)
- SL-C(SI, component) 4: NDR 3.11 (1)

15.9 NDR 3.12 – Provisioning product supplier roots of trust

15.9.1 Requirement

Network devices shall provide the capability to provision and protect the confidentiality, integrity, and authenticity of product supplier keys and data to be used as one or more “roots of trust” at the time of manufacture of the device.

15.9.2 Rationale and supplemental guidance

In order for a component to be able to validate the authenticity and integrity of the hardware, software, and data provided by the product supplier, it should possess a trusted source of data to perform the validation process. This trusted source of data is referred to as the “root of trust” for the system. This trusted source of data may be a set of cryptographic hashes of “known good” software, or it may be the public portion of an asymmetric cryptographic key pair to be used in the validation of cryptographic signatures. This trusted data is often used to validate critical software, firmware, and data prior to booting the firmware or operating system of a component, in order to validate that the component will boot into a “known good” state in which all security mechanisms are known to be operational and uncompromised. “Root of trust” data is often protected by software or hardware implemented mechanisms to prevent any modification of the data during normal operations of the component. Modification of product supplier root of trust data is typically limited to the product supplier’s provisioning process, where the product supplier has a trusted process to perform the provisioning of the data. Instead, information to be validated against the root of trust is submitted to the validation process through a hardware or software API which performs the validation and returns the results without exposing the protected data.

15.9.3 Requirement enhancements

None

15.9.4 Security levels

The requirements for the four SL levels that relate to NDR 3.12 are:

- SL-C(SI, component) 1: Not selected
- SL-C(SI, component) 2: NDR 3.12
- SL-C(SI, component) 3: NDR 3.12
- SL-C(SI, component) 4: NDR 3.12

15.10 NDR 3.13 – Provisioning asset owner roots of trust

15.10.1 Requirement

Network devices shall

a) provide the capability to provision and protect the confidentiality, integrity, and authenticity of asset owner keys and data to be used as “roots of trust”; and

b) support the capability to provision without reliance on components that may be outside of the device’s security zone.

15.10.2 Rationale and supplemental guidance

Product suppliers have established mechanisms to ensure that the software and firmware on their components is authentic, and the integrity of that software and firmware has not been compromised. This allows the product supplier to provide the asset owner with a “known good” state from which to operate. However, many product suppliers also provide mechanisms for asset owners to extend the functionality of their devices through the use of mobile code, user programs, or other such means. In order to protect the security of the component, it is important that these extensions to the component’s functionality also be validated to ensure that they are authorized, and that the asset owner has approved of their origins.

In order to perform these validations, the component should contain data that provides a way to differentiate between valid and invalid origins. The list of valid and invalid origins will differ from asset owner to asset owner, and it is unlikely that a product supplier will have a complete list of every possible valid origin at time of manufacture. Therefore, it is important that the product supplier provide a way for the asset owner to securely provision their own “roots of

trust" which provide the ability to distinguish between origins allowed by the asset owner's security policy, and those that are not. The authenticity and integrity of these "roots of trust" should be protected so that malicious actors cannot add additional roots of trust that grant them the ability to operate on the component.

Requirements such as NDR 2.4 – Mobile code (15.4) require the component to complete authenticity checks on mobile code prior to the execution of mobile code. The roots of trust provided by this requirement provide the data necessary to validate the origin and integrity of mobile code, allowing the component to independently determine if the code is allowed to execute.

A root of trust is used to provide communications security, such as communications integrity required by CR 3.1 – Communication integrity (7.3) or communications confidentiality required by CR 4.1 – Information confidentiality (8.3).

15.10.3 Requirement enhancements

None

15.10.4 Security levels

The requirements for the four SL levels that relate to NDR 3.13 are:

- SL-C(SI, component) 1: Not selected
- SL-C(SI, component) 2: NDR 3.13
- SL-C(SI, component) 3: NDR 3.13
- SL-C(SI, component) 4: NDR 3.13

15.11 NDR 3.14 – Integrity of the boot process

15.11.1 Requirement

Network devices shall verify the integrity of the firmware, software, and configuration data needed for the component's boot process prior to it being used in the boot process.

15.11.2 Rationale and supplemental guidance

In order to make assurances to an asset owner that a component's security functionality has not been compromised, it is necessary to ensure that the component's software and firmware has not been tampered with, and that the software and firmware is valid to execute on the component. Therefore, the component should perform checks to validate the integrity and authenticity of the component's firmware and/or software prior to the boot process, to ensure that the component does not boot into an insecure or invalid operating state that could damage the component or provide a path for a malicious actor to gain access to additional components, assets, or data.

15.11.3 Requirement enhancements

(1) Authenticity of the boot process

Network devices shall use the component's product supplier roots of trust to verity the authenticity of the firmware, software, and configuration data needed for the component's boot process prior to it being used in the boot process.

15.11.4 Security levels

The requirements for the four SL levels that relate to NDR 3.14 are:

- SL-C(SI, component) 1: NDR 3.14
- SL-C(SI, component) 2: NDR 3.14 (1)
- SL-C(SI, component) 3: NDR 3.14 (1)
- SL-C(SI, component) 4: NDR 3.14 (1)

15.12 NDR 5.2 – Zone boundary protection

15.12.1 Requirement

A network device at a zone boundary shall provide the capability to monitor and control communications at zone boundaries to enforce the compartmentalization defined in the risk-based zones and conduits model.

15.12.2 Rationale and supplemental guidance

Any connections to outside of each security zone should occur through managed interfaces consisting of appropriate boundary protection devices (for example, proxies, gateways, routers, firewalls, unidirectional gateways, guards and encrypted tunnels) arranged in an effective architecture (for example, firewalls protecting application gateways residing in a DMZ). Control system boundary protections at any designated alternate processing sites should provide the same levels of protection as that of the primary site.

15.12.3 Requirement enhancements

(1) Deny all, permit by exception

The network component shall provide the capability to deny network traffic by default and allow network traffic by exception (also termed deny all, permit by exception).

(2) Island mode

The network component shall provide the capability to protect against any communication through the control system boundary (also termed island mode).

NOTE 1 Examples of when this capability can be used include where a security violation and/or breach has been detected within the control system, or an attack is occurring at the enterprise level.

(3) Fail close

The network component shall provide the capability to protect against any communication through the control system boundary when there is an operational failure of the boundary protection mechanisms (also termed fail close).

NOTE 2 Examples of when this capability can be used include scenarios where a hardware failure or power failure causes boundary protection devices to function in a degraded mode or fail entirely.

15.12.4 Security levels

The requirements for the four SL levels that relate to NDR 5.2 are:

- SL-C(SI, component) 1: NDR 5.2
- SL-C(SI, component) 2: NDR 5.2 (1)
- SL-C(SI, component) 3: NDR 5.2 (1) (2) (3)
- SL-C(SI, component) 4: NDR 5.2 (1) (2) (3)

15.13 NDR 5.3 – General purpose, person-to-person communication restrictions

15.13.1 Requirement

A network device at a zone boundary shall provide the capability to protect against general purpose, person-to-person messages from being received from users or systems external to the control system.

15.13.2 Rationale and supplemental guidance

General purpose, person-to-person communications systems include but are not limited to: email systems, forms of social media (Twitter, Facebook, picture galleries, etc.) or any message systems that permit the transmission of any type of executable file. These systems are usually utilized for private purposes that are not related to control system operations, and therefore the risks imposed by these systems normally outweigh any perceived benefit.

These types of general purpose communications systems are commonly used as attack vectors to introduce malware to the control system, pass information for which read authorization exists to locations external to the control system and introduce excessive network loading that can be used to create security problems or launch attacks on the control system.

Network devices could realize such restrictions, for example, by blocking specific communications based on port numbers and source and/or target address as well as more in depth checks by application layer firewalls.

15.13.3 Requirement enhancements

None

15.13.4 Security levels

The requirements for the four SL levels that relate to NDR 5.3 are:

- SL-C(SI, component) 1: NDR 5.3
- SL-C(SI, component) 2: NDR 5.3
- SL-C(SI, component) 3: NDR 5.3
- SL-C(SI, component) 4: NDR 5.3

Annex A
(informative)

Device categories

A.1 General

The devices described in these categories are intended as representative samples for each category, and not an exhaustive list.

A.2 Device category: embedded device

A.2.1 Programmable logic controller (PLC)

The term "programmable logic controller" is expanded from IEC 60050-351:2013, 351-47-22 [11] and is commonly used in the process and discrete manufacturing industries. A PLC is a device that typically resides on the lower levels of the automation system (such as level 1 and 2 of the Purdue Enterprise Reference Architecture in ANSI/ISA-95.00.01 [15]). PLCs commonly use ruggedized hardware to allow for operation in industrial environments and are commonly based on commercial real-time operating systems (RTOS). Increasingly smart sensors and actuators are also receiving forms of process control capability. PLCs and smart sensor/actuators are programmed to execute control logic based on inputs from the process (obtained from instrumentation like traditional temperature sensors, pressure sensors, vibration sensors). The control logic's output is used to control the industrial process (through actuators such as valves, pumps). The programming is usually done using engineering software commonly run on host devices (for example, laptops or PC workstations). A common programming language for control logic is IEC 61131-3, [13]. In larger systems, PLCs often also communicate the process conditions as obtained from sensors to higher-level servers and/or operator workstations and receive instructions from higher-level control functions or operator workstations, which are translated into or forwarded as commands to actuators. For the communication to higher-level functions such as control servers or operator workstations, modern PLCs use Ethernet and transmission control protocol (TCP)/Internet protocol (IP)-based protocols, while for the communication to the instrumentation, industry standard fieldbuses are commonly used (some of which are also available on Ethernet carriers, but usually do not use the TCP/IP stack). Special PLCs are used for executing safety functions which ensure that the process under control remains within the bounds of safe operation at all times. PLCs, especially executing safety functions, should meet hard real-time and high integrity and availability requirements.

A.2.2 Intelligent electronic device (IED)

The term "intelligent electronic device" is expanded from IEC TR 61850-1:2013 [14]. An intelligent electronic device (IED) is conceptually very similar to a PLC, but the term is more commonly used in power systems (specifically substation automation). An IED receives measurements from the power equipment (for example, transformers, switches and circuit breakers) and executes control logic or protection functions. Similar to PLCs, IEDs are commonly programmed and parameterized using engineering software commonly run on host devices (for example laptops and PC workstations). A modern standard way of describing the configuration of IEDs and their functions is defined in IEC TR 61850-1. The output of the logic executed by IEDs is transmitted to actuators (switches, circuit breakers, etc.). As opposed to PLCs, IEDs commonly also have a HMI which allows a human user standing in front of the IED to use the IED's functionality (often a subset necessary to support essential functions). Also, substations, and therefore the IEDs used therein, have to be able to operate in complete isolation (such as without any communication to higher-level systems outside the substation or even without any communication to other IEDs or station-level workstations or servers). Modern IEDs usually use Ethernet and TCP/IP-based protocols to communicate to higher-level components, while communication to other IEDs may be done using Ethernet-based protocols (in some cases TCP/IP-based, often directly on Ethernet) or fieldbuses (some of

which are available also on Ethernet carriers, but do not use the TCP/IP stack). Similar to PLCs, IEDs should meet hard real-time and high integrity and availability requirements.

A.3 Device category: network device

A.3.1 Switch

The term "switch" is expanded from IEC 60050-732:2010, 732-01-22 [12]. A switch is a device in computer networks that links multiple network segments or network nodes together. A switch is typically located at layer 2 (data link layer) of the OSI model (see ISO/IEC 7498-1 [6]). Modern switches, especially those designed for use in larger networks, typically provide interfaces for configuration management and network management. These interfaces may support the configuration of the switch (for example web-based via HTTP/HTTPS, file-based via FTP/SFTP, command-line-based via SSH or via simple network management protocol (SNMP)) as well as log and event management (for example via syslog).

A.3.2 Virtual private network (VPN) terminator

The term "virtual private network" is expanded from IEC 60050-732:2010, 732-01-10 [12]. Virtual private networks are logical networks that allow for the extension of private networks across distances that are bridged by public networks. The use of the public network to cover the distance is transparent/invisible to the VPN users. VPNs are established by creating a logical tunnel at the border of the two segments of the private network. The tunnel is established by VPN terminators, which are devices located at the network border. The data packets from one segment are encapsulated (commonly also encrypted) at the VPN terminator at then sent through a public network to the peer VPN terminator. There, the encapsulation is removed (usually involving decryption) and the original packet is recovered and forwarded into the local network segment. VPNs are also often used to allow roaming users secure access to resources on their home network. In this scenario, a client software on the roaming device acts as a local VPN terminator, encapsulating (and usually encrypting) all data packets and forwarding them to the VPN terminator on the home network border. Establishment of the tunnel between VPN terminators should be authenticated, which, in the scenario of roaming users, typically is a user-based authentication. Hence, VPN terminators may be used to collect data about roaming users, which may allow tracing their location and other privacy related data.

A.4 Device category: host device/application

A.4.1 Operator workstation

Operator workstations are used in control systems to display process information to human users or operators and to allow them to interact with the control system (for example initiate operational actions on the process, such as opening a valve, closing a switch, modifying process set points). Depending on the respective operational requirements, operator workstations are often required to be continuously available (at least a minimum set of workstations out of all installed ones) to allow for an uninterrupted view of the process conditions and the opportunity to interact with the process immediately, if necessary. In order to obtain the data to be displayed and to send the commands issued by the human user, operator workstations typically communicate with control servers and connectivity servers in the control systems, sometimes they also directly communicate with PLCs. This communication is commonly using Ethernet and TCP/IP-based protocols. Operator workstations typically do not have to meet hard-real time requirements, but have high integrity and (at least as a set of operator workstations) high availability requirements. They are typically built from COTS PC hardware and run COTS client operating systems.

A.4.2 Data historian

Data historians are used in control systems to collect and maintain long-term process history data. This data is commonly collected from control servers or directly from PLCs using protocols based on Ethernet and TCP/IP. The data may be used in a variety of analyses, for example, for process optimization or performance reporting but may also be used in reporting to regulatory entities such as emission reporting or documentation of the product's production process integrity (for example, as required by the US Food and Drug Administration (FDA) regulations for pharmaceutical products). They are typically built from COTS PC/server hardware and run COTS client/server operating systems. Data is commonly stored using COTS database products. Communication to data access clients and data sources is commonly using TCP/IP-based protocols. Depending on the criticality of the process history from a business perspective, data historians have moderate availability and integrity requirements and typically no hard real-time requirements.

Annex B
(informative)

Mapping of CRs and REs to FR SLs 1-4

B.1 Overview

Annex B is intended to provide overall guidance to the reader as to how SL levels 0 to 4 are differentiated on an FR-by-FR basis via the defined CRs and their associated REs.

B.2 SL mapping table

Table B.1 indicates which component level requirements apply to which FRs for a given component security level capability SL – SL-C(xx, component). For a given FR, the required component level requirements to meet a given SL-C are denoted by a check mark.

As an example, a component that achieves SL-1 in FR 7 satisfies the base requirements of CRs 7.1 through 7.7. Note that satisfying CR 7.8 is not necessary to meet SL-1 because it is not selected until SL-2 and higher security levels. Meeting SL-1 in this way is also denoted SL-C(RA, component) = 1, to indicate that the component has a capability security level of 1 in resource availability, or FR 7.

A component that meets SL-2 in FR 7, or SL-C(RA, component) = 2 satisfies all requirements from SL-1, and additionally satisfy CR 7.1 RE(1), CR 7.3 RE(1), and the base requirement for CR 7.8.

Similarly, a component that meets SL-3 in FR 7, or SL-C (RA, component) = 3 satisfies all requirements from SL-2, and additionally satisfy CR 7.6 RE(1).

A component that meets SL-4 in FR7, or SL-C(RA, component) = 4 satisfies all requirements from SL-3. There are no base requirements or requirement enhancements in FR 7 that are unique to SL-4, and thus all components which meet SL-3 also inherently meet SL-4.

Refer to IEC 62443 -3-3:2013, Annex A for how a full SL vector that includes all foundational requirements would be denoted.

For clarification the acronyms used in the table are shown at the end of the table.

Table B.1 – Mapping of CRs and REs to FR SL levels 1-4

SRs and REs	SL 1	SL 2	SL 3	SL 4
FR 1 – Identification and authentication control (IAC)				
CR 1.1 – Human user identification and authentication	☐	☐	☐	☐
RE (1) Unique identification and authentication:		☐	☐	☐
RE (2) Multifactor authentication for all interfaces			☐	☐
CR 1.2 – Software process and device identification and authentication		☐	☐	☐
RE (1) Unique identification and authentication			☐	☐
CR 1.3 – Account management	☐	☐	☐	☐
CR 1.4 – Identifier management	☐	☐	☐	☐
CR 1.5 – Authenticator management	☐	☐	☐	☐
RE (1) Hardware security for authenticators			☐	☐
NDR 1.6 – Wireless access management	☐	☐	☐	☐
RE (1) Unique identification and authentication		☐	☐	☐
CR 1.7 – Strength of password-based authentication	☐	☐	☐	☐
RE (1) Password generation and lifetime restrictions for human users			☐	☐
RE (2) Password lifetime restrictions for all users (human, software process, or device)				☐
CR 1.8 – Public key infrastructure certificates		☐	☐	☐
CR 1.9 – Strength of public key-based authentication		☐	☐	☐
RE (1) Hardware security for public key-based authentication			☐	☐
CR 1.10 – Authenticator feedback	☐	☐	☐	☐
CR 1.11 – Unsuccessful login attempts	☐	☐	☐	☐
CR 1.12 – System use notification	☐	☐	☐	☐
NDR 1.13 – Access via untrusted networks	☐	☐	☐	☐
RE (1) Explicit access request approval			☐	☐
CR 1.14 – Strength of symmetric key-based authentication		☐	☐	☐
RE (1) Hardware security for symmetric key-based authentication			☐	☐

SRs and REs	SL 1	SL 2	SL 3	SL 4
FR 2 – Use control (UC)				
CR 2.1 – Authorization enforcement	□	□	□	□
RE (1) Authorization enforcement for all users (humans, software processes and devices)		□	□	□
RE (2) Permission mapping to roles		□	□	□
RE (3) Supervisor override			□	□
RE (4) Dual approval				□
CR 2.2 – Wireless use control	□	□	□	□
CR 2.3 – Use control for portable and mobile devices				
SAR 2.4 – Mobile code	□	□	□	□
RE (1) Mobile code authenticity check		□	□	□
EDR 2.4 – Mobile code	□	□	□	□
RE (1) Mobile code authenticity check		□	□	□
HDR 2.4 – Mobile code	□	□	□	□
RE (1) Mobile code authenticity check		□	□	□
NDR 2.4 – Mobile code	□	□	□	□
RE (1) Mobile code authenticity check		□	□	□
CR 2.5 – Session lock	□	□	□	□
CR 2.6 – Remote session termination		□	□	□
CR 2.7 – Concurrent session control			□	□
CR 2.8 – Auditable events	□	□	□	□
CR 2.9 – Audit storage capacity	□	□	□	□
RE (1) Warn when audit record storage capacity threshold reached			□	□
CR 2.10 – Response to audit processing failures	□	□	□	□
CR 2.11 – Timestamps	□	□	□	□
RE (1) Time synchronization		□	□	□
RE (2) Protection of time source integrity				□
CR 2.12 – Non-repudiation	□	□	□	□
RE (1) Non-repudiation for all users				□

SRs and REs	SL 1	SL 2	SL 3	SL 4
EDR 2.13 – Use of physical diagnostic and test interfaces		☐	☐	☐
RE (1) Active monitoring			☐	☐
HDR 2.13 – Use of physical diagnostic and test interfaces		☐	☐	☐
RE (1) Active monitoring			☐	☐
NDR 2.13 – Use of physical diagnostic and test interfaces		☐	☐	☐
RE (1) Active monitoring			☐	☐
FR 3 – System integrity (SI)				
CR 3.1 – Communication integrity	☐	☐	☐	☐
RE (1) Communication authentication		☐	☐	☐
SAR 3.2 – Protection from malicious code	☐	☐	☐	☐
EDR 3.2 – Protection from malicious code	☐	☐	☐	☐
HDR 3.2 – Protection from malicious code	☐	☐	☐	☐
RE (1) Report version of code protection		☐	☐	☐
NDR 3.2 – Protection from malicious code	☐	☐	☐	☐
CR 3.3 – Security functionality verification	☐	☐	☐	☐
RE (1) Security functionality verification during normal operation				☐
CR 3.4 – Software and information integrity	☐	☐	☐	☐
RE (1) Authenticity of software and information		☐	☐	☐
RE (2) Automated notification of integrity violations			☐	☐
CR 3.5 – Input validation	☐	☐	☐	☐
CR 3.6 – Deterministic output	☐	☐	☐	☐
CR 3.7 – Error handling	☐	☐	☐	☐
CR 3.8 – Session integrity		☐	☐	☐
CR 3.9 – Protection of audit information		☐	☐	☐
RE (1) Audit records on write-once media				☐
EDR 3.10 – Support for updates	☐	☐	☐	☐
RE (1) Update authenticity and integrity		☐	☐	☐
HDR 3.10 – Support for updates	☐	☐	☐	☐

SRs and REs	SL 1	SL 2	SL 3	SL 4
RE (1) Update authenticity and integrity		□	□	□
NDR 3.10 – Support for updates	□	□	□	□
RE (1) Update authenticity and integrity		□	□	□
EDR 3.11 – Physical tamper resistance and detection		□	□	□
RE (1) Notification of a tampering attempt			□	□
HDR 3.11 – Physical tamper resistance and detection		□	□	□
RE (1) Notification of a tampering attempt			□	□
NDR 3.11 – Physical tamper resistance and detection		□	□	□
RE (1) Notification of a tampering attempt			□	□
EDR 3.12 – Provisioning product supplier roots of trust		□	□	□
HDR 3.12 – Provisioning product supplier roots of trust		□	□	□
NDR 3.12 – Provisioning product supplier roots of trust		□	□	□
EDR 3.13 – Provisioning asset owner roots of trust		□	□	□
HDR 3.13 – Provisioning asset owner roots of trust		□	□	□
NDR 3.13 – Provisioning asset owner roots of trust		□	□	□
EDR 3.14 – Integrity of the boot process	□	□	□	□
RE (1) Authenticity of the boot process		□	□	□
HDR 3.14 – Integrity of the boot process	□	□	□	□
RE (1) Authenticity of the boot process		□	□	□
NDR 3.14 – Integrity of the boot process	□	□	□	□
RE (1) Authenticity of the boot process		□	□	□
FR 4 – Data confidentiality (DC)				
CR 4.1 – Information confidentiality	□	□	□	□
CR 4.2 – Information persistence		□	□	□
RE (1) Erase of shared memory resources			□	□
RE (2) Erase verification			□	□
CR 4.3 – Use of cryptography	□	□	□	□

SRs and REs	SL 1	SL 2	SL 3	SL 4
FR 5 – Restricted data flow (RDF)				
CR 5.1 – Network segmentation	□	□	□	□
NDR 5.2 – Zone boundary protection	□	□	□	□
RE (1) Deny all, permit by exception		□	□	□
RE (2) Island mode			□	□
RE (3) Fail close			□	□
NDR 5.3 – General purpose, person-to-person communication restrictions	□	□	□	□
FR 6 – Timely response to events (TRE)				
CR 6.1 – Audit log accessibility	□	□	□	□
RE (1) Programmatic access to audit logs			□	□
CR 6.2 – Continuous monitoring		□	□	□
FR 7 – Resource availability (RA)				
CR 7.1 – Denial of service protection	□	□	□	□
RE(1) Manage communication load from component		□	□	□
CR 7.2 – Resource management	□	□	□	□
CR 7.3 – Control system backup	□	□	□	□
RE (1) Backup integrity verification		□	□	□
CR 7.4 – Control system recovery and reconstitution	□	□	□	□
CR 7.5 – Emergency power				
CR 7.6 – Network and security configuration settings	□	□	□	□
RE (1) Machine-readable reporting of current security settings			□	□
CR 7.7 – Least functionality	□	□	□	□
CR 7.8 – Control system component inventory		□	□	□

Key

CR: Component requirement which is common to all types of components

SAR: Software application requirement

EDR: Embedded device requirement

HDR: Host device requirement

NDR: Network device requirement

Bibliography

NOTE 1 This bibliography includes references to sources used in the creation of this document as well as references to sources that can aid the reader in developing a greater understanding of cyber security as a whole and developing a management system. Not all references in this bibliography are referred to throughout the text of this document. The references have been broken down into different categories depending on the type of source they are.

References to other parts, both existing and anticipated, of the IEC 62443 series:

NOTE 2 Some of these references are published documents, under development, or anticipated. They are all listed here for completeness of the currently authorized parts of the IEC 62443 series.

[1] IEC 62443-2-1, Industrial communication networks – Network and system security – Part 2-1: Establishing an industrial automation and control system security program

[2] IEC TR 62443-2-3, Security for industrial automation and control systems – Part 2-3: Patch management in the IACS environment

[3] IEC 62443-2-4, Security for industrial automation and control systems – Part 2-4: Security program requirements for IACS service providers

[4] IEC TR 62443-3-1, Industrial communication networks – Network and system security – Part 3-1: Security technologies for industrial automation and control systems

[5] IEC 62443-3-2[4], Security for industrial automation and control systems – Part 3-2: Security risk assessment and system design

Other standards references:

[6] ISO/IEC 7498-1:1994, Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model

[7] ISO/IEC 8601:2004, Data elements and interchange formats – Information interchange – Representation of dates and times

[8] ISO/IEC 15408-1:2009, Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model

[9] ISO/IEC 19790, Information technology – Security techniques – Security requirements for cryptographic modules

[10] ISO/IEC 27002:2013, Information technology – Security techniques – Code of practice for information security management

[11] IEC 60050-351, International Electrotechnical Vocabulary – Part 351: Control technology (available at http://www.electropedia.org)

[12] IEC 60050-732, International Electrotechnical Vocabulary – Part 732: Computer network technology (available at http://www.electropedia.org)

[13] IEC 61131-3, Programmable controllers – Part 3: Programming languages

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

[14] IEC TR 61850-1:2013, Communication networks and systems for power utility automation – Part 1: Introduction and overview

[15] ANSI/ISA-95.00.01-2010 (IEC 62264-1 Mod), Enterprise-Control System Integration – Part 1: Models and Terminology

[16] ISO/IEC 11889-1:2015, Information technology – Trusted Platform Module Library – Part1: Architecture

Other documents and published resources:

[17] FIPS 140-2, Security Requirements for Cryptographic Modules

[18] NIST SP 800-57, Recommendation for Key Management – Part 1: General

[19] NIST SP 800-92, Guide to Computer Security Log Management

[20] NIST SP800-63-2, Electronic Authentication Guideline

Websites:

[21] OWASP Code Review Guide, available at https://www.owasp.org/index.php/Code_Review_Guide

[22] RFC 3647 – Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework https://www.ietf.org/rfc/rfc3647.txt

_____

SOMMAIRE

AVANT-PROPOS 106
INTRODUCTION 108
1 Domaine d'application 111
2 Références normatives 111
3 Termes, définitions, termes abrégés, acronymes et conventions 112
3.1 Termes et définitions 112
3.2 Termes abrégés et acronymes 118
3.3 Conventions 120
4 Contraintes communes en matière de sécurité du composant 121
4.1 Vue d'ensemble 121
4.2 Support des fonctions essentielles CCSC 1 121
4.3 Contre-mesures compensatoires CCSC 2 121
4.4 Droit d'accès minimal CCSC 3 121
4.5 Processus de développement logiciel CCSC 4 122
5 FR 1 – Contrôle d'identification et d'authentification 122
5.1 Objet et descriptions du SL-C(IAC) 122
5.2 Justification 122
5.3 CR 1.1 – Identification et authentification d'un utilisateur humain 122
5.3.1 Exigences 122
5.3.2 Justification et recommandations complémentaires 123
5.3.3 Amélioration d'exigences 123
5.3.4 Niveaux de sécurité 123
5.4 CR 1.2 – Identification et authentification du processus logiciel et de l'appareil 123
5.4.1 Exigences 123
5.4.2 Justification et recommandations complémentaires 124
5.4.3 Amélioration d'exigences 124
5.4.4 Niveaux de sécurité 124
5.5 CR 1.3 – Gestion de compte 124
5.5.1 Exigences 124
5.5.2 Justification et recommandations complémentaires 125
5.5.3 Amélioration d'exigences 125
5.5.4 Niveaux de sécurité 125
5.6 CR 1.4 – Gestion d'identificateur 125
5.6.1 Exigences 125
5.6.2 Justification et recommandations complémentaires 125
5.6.3 Amélioration d'exigences 125
5.6.4 Niveaux de sécurité 125
5.7 CR 1.5 – Gestion d'authentifiant 126
5.7.1 Exigences 126
5.7.2 Justification et recommandations complémentaires 126
5.7.3 Amélioration d'exigences 127
5.7.4 Niveaux de sécurité 127
5.8 CR 1.6 – Gestion des accès sans fil 127
5.9 CR 1.7 – Force de l'authentification basée sur mot de passe 127
5.9.1 Exigences 127
5.9.2 Justification et recommandations complémentaires 127

5.9.3 Amélioration d'exigences 127
5.9.4 Niveaux de sécurité 128
5.10 CR 1.8 – Certificats d'infrastructure à clés publiques 128
5.10.1 Exigences 128
5.10.2 Justification et recommandations complémentaires 128
5.10.3 Amélioration d'exigences 128
5.10.4 Niveaux de sécurité 128
5.11 CR 1.9 – Force de l'authentification basée sur clé publique 128
5.11.1 Exigences 128
5.11.2 Justification et recommandations complémentaires 129
5.11.3 Amélioration d'exigences 130
5.11.4 Niveaux de sécurité 130
5.12 CR 1.10 – Retour de l'authentifiant 130
5.12.1 Exigences 130
5.12.2 Justification et recommandations complémentaires 130
5.12.3 Amélioration d'exigences 130
5.12.4 Niveaux de sécurité 130
5.13 CR 1.11 – Tentatives infructueuses de connexion 130
5.13.1 Exigences 130
5.13.2 Justification et recommandations complémentaires 131
5.13.3 Amélioration d'exigences 131
5.13.4 Niveaux de sécurité 131
5.14 CR 1.12 – Notification d'utilisation du système 131
5.14.1 Exigences 131
5.14.2 Justification et recommandations complémentaires 131
5.14.3 Amélioration d'exigences 132
5.14.4 Niveaux de sécurité 132
5.15 CR 1.13 – Accès par l'intermédiaire de réseaux non sécurisés 132
5.16 CR 1.14 – Force de l'authentification basée sur clé symétrique 132
5.16.1 Exigences 132
5.16.2 Justification et recommandations complémentaires 132
5.16.3 Amélioration d'exigences 133
5.16.4 Niveaux de sécurité 133
6 FR 2 – Contrôle d'utilisation 133
6.1 Objet et descriptions du SL-C(UC) 133
6.2 Justification 133
6.3 CR 2.1 – Mise en œuvre d'autorisation 134
6.3.1 Exigences 134
6.3.2 Justification et recommandations complémentaires 134
6.3.3 Amélioration d'exigences 134
6.3.4 Niveaux de sécurité 135
6.4 CR 2.2 – Contrôle d'utilisation sans fil 135
6.4.1 Exigences 135
6.4.2 Justification et recommandations complémentaires 135
6.4.3 Amélioration d'exigences 135
6.4.4 Niveaux de sécurité 135
6.5 CR 2.3 – Contrôle d'utilisation pour les appareils portables et mobiles 136
6.6 CR 2.4 – Code mobile 136

6.7 CR 2.5 – Verrouillage de session 136
6.7.1 Exigences 136
6.7.2 Justification et recommandations complémentaires 136
6.7.3 Amélioration d'exigences 136
6.7.4 Niveaux de sécurité 136
6.8 CR 2.6 – Fermeture de la session à distance 136
6.8.1 Exigences 136
6.8.2 Justification et recommandations complémentaires 136
6.8.3 Amélioration d'exigences 137
6.8.4 Niveaux de sécurité 137
6.9 CR 2.7 – Contrôle de sessions simultanées 137
6.9.1 Exigences 137
6.9.2 Justification et recommandations complémentaires 137
6.9.3 Amélioration d'exigences 137
6.9.4 Niveaux de sécurité 137
6.10 CR 2.8 – Événements auditables 137
6.10.1 Exigences 137
6.10.2 Justification et recommandations complémentaires 138
6.10.3 Amélioration d'exigences 138
6.10.4 Niveaux de sécurité 138
6.11 CR 2.9 – Capacité de stockage des données d'audit 138
6.11.1 Exigences 138
6.11.2 Justification et recommandations complémentaires 138
6.11.3 Amélioration d'exigences 139
6.11.4 Niveaux de sécurité 139
6.12 CR 2.10 – Réponse aux défaillances de traitement des audits 139
6.12.1 Exigences 139
6.12.2 Justification et recommandations complémentaires 139
6.12.3 Amélioration d'exigences 139
6.12.4 Niveaux de sécurité 139
6.13 CR 2.11 – Horodatages 140
6.13.1 Exigences 140
6.13.2 Justification et recommandations complémentaires 140
6.13.3 Amélioration d'exigences 140
6.13.4 Niveaux de sécurité 140
6.14 CR 2.12 – Non-répudiation 140
6.14.1 Exigences 140
6.14.2 Justification et recommandations complémentaires 140
6.14.3 Amélioration d'exigences 141
6.14.4 Niveaux de sécurité 141
6.15 CR 2.13 – Utilisation d'interfaces physiques de diagnostic et d'essai 141
7 FR 3 – Intégrité du système 141
7.1 Objet et descriptions du SL-C(SI) 141
7.2 Justification 141
7.3 CR 3.1 – Intégrité de la communication 141
7.3.1 Exigences 141
7.3.2 Justification et recommandations complémentaires 142
7.3.3 Amélioration d'exigences 142
7.3.4 Niveaux de sécurité 142

7.4 CR 3.2 – Protection contre les programmes malveillants 143
7.5 CR 3.3 – Vérification de la fonctionnalité de sécurité 143
7.5.1 Exigences 143
7.5.2 Justification et recommandations complémentaires 143
7.5.3 Amélioration d'exigences 143
7.5.4 Niveaux de sécurité 143
7.6 CR 3.4 – Intégrité des logiciels et des informations 144
7.6.1 Exigences 144
7.6.2 Justification et recommandations complémentaires 144
7.6.3 Amélioration d'exigences 144
7.6.4 Niveaux de sécurité 144
7.7 CR 3.5 – Validation d'entrée 144
7.7.1 Exigences 144
7.7.2 Justification et recommandations complémentaires 144
7.7.3 Amélioration d'exigences 145
7.7.4 Niveaux de sécurité 145
7.8 CR 3.6 – Sortie déterministe 145
7.8.1 Exigences 145
7.8.2 Justification et recommandations complémentaires 145
7.8.3 Amélioration d'exigences 145
7.8.4 Niveaux de sécurité 146
7.9 CR 3.7 – Traitement des erreurs 146
7.9.1 Exigences 146
7.9.2 Justification et recommandations complémentaires 146
7.9.3 Amélioration d'exigences 146
7.9.4 Niveaux de sécurité 146
7.10 CR 3.8 – Intégrité de la session 146
7.10.1 Exigences 146
7.10.2 Justification et recommandations complémentaires 147
7.10.3 Amélioration d'exigences 147
7.10.4 Niveaux de sécurité 147
7.11 CR 3.9 – Protection des informations d'audit 147
7.11.1 Exigences 147
7.11.2 Justification et recommandations complémentaires 147
7.11.3 Amélioration d'exigences 147
7.11.4 Niveaux de sécurité 147
7.12 CR 3.10 – Support pour les mises à jour 148
7.13 CR 3.11 – Résistance aux violations physiques et détection 148
7.14 CR 3.12 – Fourniture des racines de confiance du fournisseur de produit 148
7.15 CR 3.13 – Fourniture des racines de confiance du propriétaire d'actif 148
7.16 CR 3.14 – Intégrité du processus d'amorçage 148
8 FR 4 – Confidentialité des données 148
8.1 Objet et descriptions du SL-C(DC) 148
8.2 Justification 148
8.3 CR 4.1 – Confidentialité des informations 149
8.3.1 Exigences 149
8.3.2 Justification et recommandations complémentaires 149
8.3.3 Amélioration d'exigences 149
8.3.4 Niveaux de sécurité 149

8.4 CR 4.2 – Persistance des informations 149
8.4.1 Exigences 149
8.4.2 Justification et recommandations complémentaires 149
8.4.3 Amélioration d'exigences 150
8.4.4 Niveaux de sécurité 150
8.5 CR 4.3 – Utilisation de la cryptographie 150
8.5.1 Exigences 150
8.5.2 Justification et recommandations complémentaires 150
8.5.3 Amélioration d'exigences 151
8.5.4 Niveaux de sécurité 151
9 FR 5 – Transfert de données limité 151
9.1 Objet et descriptions du SL-C(RDF) 151
9.2 Justification 151
9.3 CR 5.1 – Segmentation du réseau 152
9.3.1 Exigences 152
9.3.2 Justification et recommandations complémentaires 152
9.3.3 Amélioration d'exigences 152
9.3.4 Niveaux de sécurité 152
9.4 CR 5.2 – Protection des limites de zone 153
9.5 CR 5.3 – Restrictions des communications entre des personnes d'ordre général 153
9.6 CR 5.4 – Partitionnement des applications 153
10 FR 6 – Réponse appropriée aux événements 153
10.1 Objet et descriptions du SL-C(TRE) 153
10.2 Justification 153
10.3 CR 6.1 – Accessibilité au journal d'audit 153
10.3.1 Exigences 153
10.3.2 Justification et recommandations complémentaires 154
10.3.3 Amélioration d'exigences 154
10.3.4 Niveaux de sécurité 154
10.4 CR 6.2 – Surveillance continue 154
10.4.1 Exigences 154
10.4.2 Justification et recommandations complémentaires 154
10.4.3 Amélioration d'exigences 155
10.4.4 Niveaux de sécurité 155
11 FR 7 – Disponibilité des ressources 155
11.1 Objet et descriptions du SL-C(RA) 155
11.2 Justification 155
11.3 CR 7.1 – Protection contre le refus de service 155
11.3.1 Exigences 155
11.3.2 Justification et recommandations complémentaires 155
11.3.3 Amélioration d'exigences 156
11.3.4 Niveaux de sécurité 156
11.4 CR 7.2 – Gestion des ressources 156
11.4.1 Exigences 156
11.4.2 Justification et recommandations complémentaires 156
11.4.3 Amélioration d'exigences 156
11.4.4 Niveaux de sécurité 156

11.5 CR 7.3 – Sauvegarde du système de commande 156
11.5.1 Exigences 156
11.5.2 Justification et recommandations complémentaires 156
11.5.3 Amélioration d'exigences 157
11.5.4 Niveaux de sécurité 157
11.6 CR 7.4 – Récupération et reconstitution du système de commande 157
11.6.1 Exigences 157
11.6.2 Justification et recommandations complémentaires 157
11.6.3 Amélioration d'exigences 157
11.6.4 Niveaux de sécurité 157
11.7 CR 7.5 – Alimentation de secours 158
11.8 CR 7.6 – Paramètres de configuration du réseau et de la sécurité 158
11.8.1 Exigences 158
11.8.2 Justification et recommandations complémentaires 158
11.8.3 Amélioration d'exigences 158
11.8.4 Niveaux de sécurité 158
11.9 CR 7.7 – Fonctionnalité minimale 158
11.9.1 Exigences 158
11.9.2 Justification et recommandations complémentaires 158
11.9.3 Amélioration d'exigences 158
11.9.4 Niveaux de sécurité 159
11.10 CR 7.8 – Inventaire des composants du système de commande 159
11.10.1 Exigences 159
11.10.2 Justification et recommandations complémentaires 159
11.10.3 Amélioration d'exigences 159
11.10.4 Niveaux de sécurité 159
12 Exigences relatives aux applications logicielles 159
12.1 Objet 159
12.2 SAR 2.4 – Code mobile 159
12.2.1 Exigences 159
12.2.2 Justification et recommandations complémentaires 160
12.2.3 Amélioration d'exigences 160
12.2.4 Niveaux de sécurité 160
12.3 SAR 3.2 – Protection contre les programmes malveillants 160
12.3.1 Exigences 160
12.3.2 Justification et recommandations complémentaires 160
12.3.3 Amélioration d'exigences 160
12.3.4 Niveaux de sécurité 160
13 Exigences relatives aux appareils intégrés 161
13.1 Objet 161
13.2 EDR 2.4 – Code mobile 161
13.2.1 Exigences 161
13.2.2 Justification et recommandations complémentaires 161
13.2.3 Amélioration d'exigences 161
13.2.4 Niveaux de sécurité 161
13.3 EDR 2.13 – Utilisation d'interfaces physiques de diagnostic et d'essai 161
13.3.1 Exigences 161
13.3.2 Justification et recommandations complémentaires 162
13.3.3 Amélioration d'exigences 162

13.3.4 Niveaux de sécurité 162
13.4 EDR 3.2 – Protection contre les programmes malveillants 162
13.4.1 Exigences 162
13.4.2 Justification et recommandations complémentaires 162
13.4.3 Amélioration d'exigences 163
13.4.4 Niveaux de sécurité 163
13.5 EDR 3.10 – Support pour les mises à jour 163
13.5.1 Exigences 163
13.5.2 Justification et recommandations complémentaires 163
13.5.3 Amélioration d'exigences 163
13.5.4 Niveaux de sécurité 163
13.6 EDR 3.11 – Résistance aux violations physiques et détection 163
13.6.1 Exigences 163
13.6.2 Justification et recommandations complémentaires 164
13.6.3 Amélioration d'exigences 164
13.6.4 Niveaux de sécurité 164
13.7 EDR 3.12 – Fourniture des racines de confiance du fournisseur de produit 164
13.7.1 Exigences 164
13.7.2 Justification et recommandations complémentaires 164
13.7.3 Amélioration d'exigences 165
13.7.4 Niveaux de sécurité 165
13.8 EDR 3.13 – Fourniture des racines de confiance du propriétaire d'actif 165
13.8.1 Exigences 165
13.8.2 Justification et recommandations complémentaires 165
13.8.3 Amélioration d'exigences 166
13.8.4 Niveaux de sécurité 166
13.9 EDR 3.14 – Intégrité du processus d'amorçage 166
13.9.1 Exigences 166
13.9.2 Justification et recommandations complémentaires 166
13.9.3 Amélioration d'exigences 166
13.9.4 Niveaux de sécurité 166
14 Exigences relatives aux appareils hôtes 167
14.1 Objet 167
14.2 HDR 2.4 – Code mobile 167
14.2.1 Exigences 167
14.2.2 Justification et recommandations complémentaires 167
14.2.3 Amélioration d'exigences 167
14.2.4 Niveaux de sécurité 167
14.3 HDR 2.13 – Utilisation d'interfaces physiques de diagnostic et d'essai 168
14.3.1 Exigences 168
14.3.2 Justification et recommandations complémentaires 168
14.3.3 Amélioration d'exigences 168
14.3.4 Niveaux de sécurité 168
14.4 HDR 3.2 – Protection contre les programmes malveillants 168
14.4.1 Exigences 168
14.4.2 Justification et recommandations complémentaires 168
14.4.3 Amélioration d'exigences 169
14.4.4 Niveaux de sécurité 169

14.5 HDR 3.10 – Support pour les mises à jour 169
14.5.1 Exigences 169
14.5.2 Justification et recommandations complémentaires 169
14.5.3 Amélioration d'exigences 169
14.5.4 Niveaux de sécurité 169
14.6 HDR 3.11 – Résistance aux violations physiques et détection 169
14.6.1 Exigences 169
14.6.2 Justification et recommandations complémentaires 169
14.6.3 Amélioration d'exigences 170
14.6.4 Niveaux de sécurité 170
14.7 HDR 3.12 – Fourniture des racines de confiance du fournisseur de produit 170
14.7.1 Exigences 170
14.7.2 Justification et recommandations complémentaires 170
14.7.3 Amélioration d'exigences 171
14.7.4 Niveaux de sécurité 171
14.8 HDR 3.13 – Fourniture des racines de confiance du propriétaire d'actif 171
14.8.1 Exigences 171
14.8.2 Justification et recommandations complémentaires 171
14.8.3 Amélioration d'exigences 172
14.8.4 Niveaux de sécurité 172
14.9 HDR 3.14 – Intégrité du processus d'amorçage 172
14.9.1 Exigences 172
14.9.2 Justification et recommandations complémentaires 172
14.9.3 Amélioration d'exigences 172
14.9.4 Niveaux de sécurité 172
15 Exigences relatives aux appareils de réseaux 172
15.1 Objet 172
15.2 NDR 1.6 – Gestion des accès sans fil 173
15.2.1 Exigences 173
15.2.2 Justification et recommandations complémentaires 173
15.2.3 Amélioration d'exigences 173
15.2.4 Niveaux de sécurité 173
15.3 NDR 1.13 – Accès par l'intermédiaire de réseaux non sécurisés 173
15.3.1 Exigences 173
15.3.2 Justification et recommandations complémentaires 173
15.3.3 Amélioration d'exigences 174
15.3.4 Niveaux de sécurité 174
15.4 NDR 2.4 – Code mobile 174
15.4.1 Exigences 174
15.4.2 Justification et recommandations complémentaires 174
15.4.3 Amélioration d'exigences 174
15.4.4 Niveaux de sécurité 175
15.5 NDR 2.13 – Utilisation d'interfaces physiques de diagnostic et d'essai 175
15.5.1 Exigences 175
15.5.2 Justification et recommandations complémentaires 175
15.5.3 Amélioration d'exigences 175
15.5.4 Niveaux de sécurité 175

15.6 NDR 3.2 – Protection contre les programmes malveillants 175
15.6.1 Exigences 175
15.6.2 Justification et recommandations complémentaires 176
15.6.3 Amélioration d'exigences 176
15.6.4 Niveaux de sécurité 176
15.7 NDR 3.10 – Support pour les mises à jour 176
15.7.1 Exigences 176
15.7.2 Justification et recommandations complémentaires 176
15.7.3 Amélioration d'exigences 176
15.7.4 Niveaux de sécurité 176
15.8 NDR 3.11 – Résistance aux violations physiques et détection 177
15.8.1 Exigences 177
15.8.2 Justification et recommandations complémentaires 177
15.8.3 Amélioration d'exigences 177
15.8.4 Niveaux de sécurité 177
15.9 NDR 3.12 – Fourniture des racines de confiance du fournisseur de produit 177
15.9.1 Exigences 177
15.9.2 Justification et recommandations complémentaires 177
15.9.3 Amélioration d'exigences 178
15.9.4 Niveaux de sécurité 178
15.10 NDR 3.13 – Fourniture des racines de confiance du propriétaire d'actif 178
15.10.1 Exigences 178
15.10.2 Justification et recommandations complémentaires 178
15.10.3 Amélioration d'exigences 179
15.10.4 Niveaux de sécurité 179
15.11 NDR 3.14 – Intégrité du processus d'amorçage 179
15.11.1 Exigences 179
15.11.2 Justification et recommandations complémentaires 179
15.11.3 Amélioration d'exigences 179
15.11.4 Niveaux de sécurité 179
15.12 NDR 5.2 – Protection des limites de zone 180
15.12.1 Exigences 180
15.12.2 Justification et recommandations complémentaires 180
15.12.3 Amélioration d'exigences 180
15.12.4 Niveaux de sécurité 180
15.13 NDR 5.3 – Restrictions des communications entre des personnes d'ordre général 181
15.13.1 Exigences 181
15.13.2 Justification et recommandations complémentaires 181
15.13.3 Amélioration d'exigences 181
15.13.4 Niveaux de sécurité 181
Annexe A (informative) Catégories d'appareils 182
A.1 Généralités 182
A.2 Catégorie d'appareil: appareil intégré 182
A.2.1 Automate programmable (PLC) 182
A.2.2 Appareil électronique intelligent (IED) 182
A.3 Catégorie d'appareil: appareil de réseau 183
A.3.1 Commutateur 183
A.3.2 Terminateur RPV (réseau privé virtuel) 183

A.4 Catégorie d'appareil: appareil/application hôte 183
A.4.1 Poste de travail de l'opérateur 183
A.4.2 Historique des données 184
Annexe B (informative) Mapping des CR et des RE avec les FR des SL 1 à 4 185
B.1 Vue d'ensemble 185
B.2 Tableau de mapping des niveaux de sécurité 185
Bibliographie 191

Figure 1 – Parties de la série IEC 62443 110

Tableau B.1 – Mapping des CR et des RE avec les niveaux FR SL 1-4 186

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
65/735/FDIS	65/740/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.

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.

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.

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 62443-2-4, 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
- Exigences relatives aux appareils de réseaux (NDR);

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

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

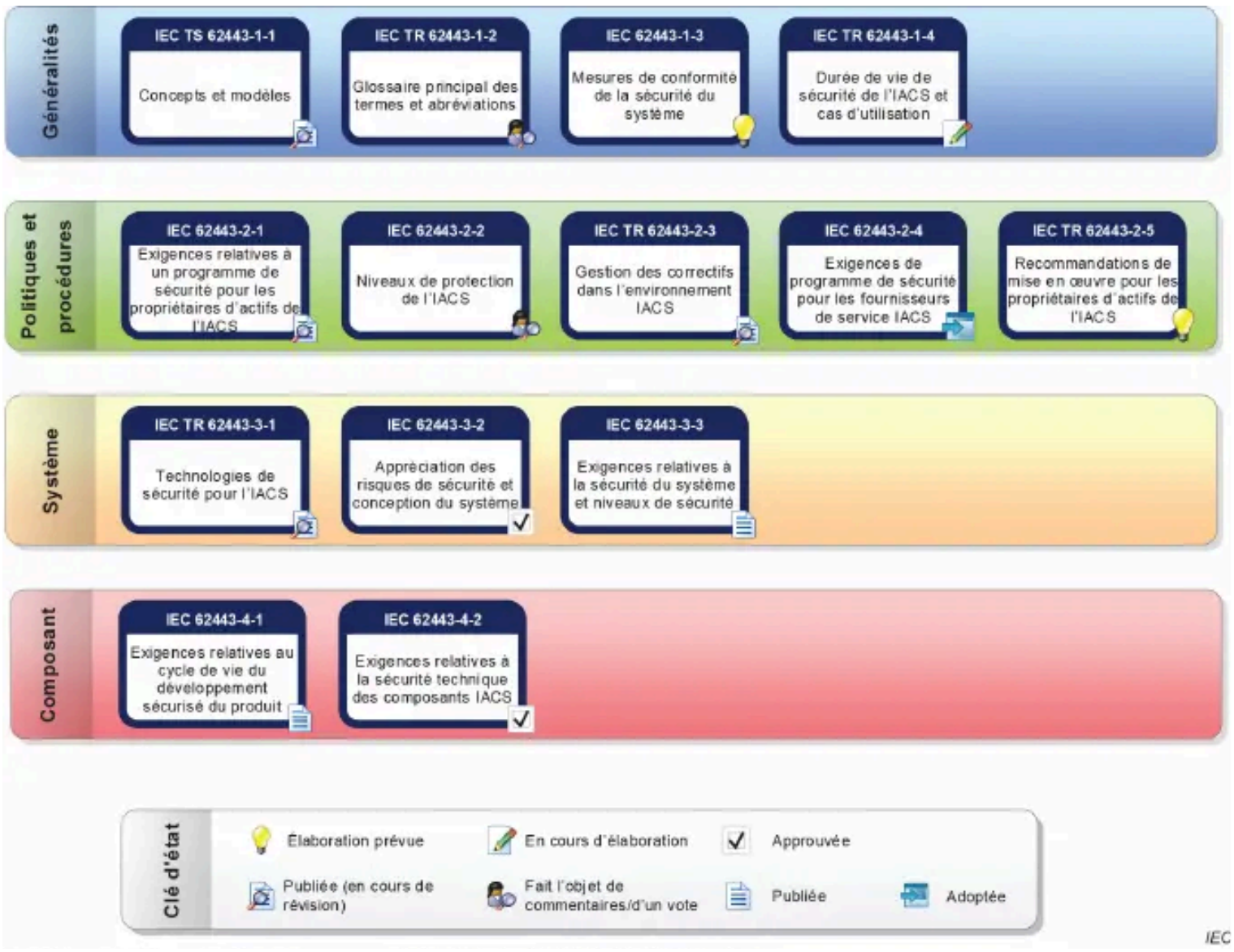

Figure 1 – Parties de la série IEC 62443

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)

3 Termes, définitions, termes abrégés, acronymes et conventions

3.1 Termes et définitions

Pour les besoins du présent document, les termes et définitions de l'IEC TS 62443-1-1, l'IEC 62443-3-3 et l'IEC 62443-4-1, ainsi que les suivants, s'appliquent.

NOTE La plupart des termes et définitions ci-dessous reposent sur des sources ISO (Organisation internationale de normalisation), IEC (Commission Électrotechnique Internationale) et U.S. National Institute of Standards and Technology (NIST), auxquelles des modifications ont parfois été apportées afin d'améliorer la pertinence des exigences en matière de sécurité de l'IACS.

3.1.1
actif
objet physique ou logique ayant une valeur perçue ou réelle pour l'IACS

Note 1 à l'article: Dans ce cas précis, un actif est un élément qu'il convient de protéger dans le cadre du système de gestion de la sécurité IACS.

Note 2 à l'article: Un actif ne se limite pas à l'IACS seul, mais il peut également inclure les actifs physiques qu'il contrôle.

3.1.2
propriétaire d'actif
personne ou société responsable d'un ou de plusieurs IACS

Note 1 à l'article: Utilisé à la place du terme générique «utilisateur final» pour les différencier.

Note 2 à l'article: Inclut les composants faisant partie intégrante de l'IACS.

Note 3 à l'article: Dans le contexte du présent document, un propriétaire d'actif inclut également l'opérateur de l'IACS.

3.1.3
attaque
tentative non autorisée visant à compromettre la confidentialité, l'intégrité ou la disponibilité d'un IACS de la part d'une menace délibérée

EXEMPLE Acte réfléchi qui est une tentative délibérée (compte tenu en particulier de la méthode ou de la technique utilisée) de contourner les services de sécurité et d'enfreindre la politique de sécurité du système.

Note 1 à l'article: Différentes classes d'attaque sont reconnues:

– Une «attaque active» est une tentative de modification des ressources du système ou de leur fonctionnement.
– Une «attaque passive» est une tentative de prise de connaissance ou d'utilisation des informations d'un système, sans affecter ses ressources.
– Une «attaque interne» est une attaque lancée par une entité à l'intérieur du périmètre de sécurité (un «intrus»). Il s'agit, par exemple, d'une entité autorisée à accéder aux ressources du système, mais qui les utilise sans l'approbation des personnes qui ont autorisé l'accès.
– Une «attaque externe» est une attaque lancée depuis l'extérieur du périmètre par un utilisateur non autorisé ou illégitime du système (y compris un intrus qui lance une attaque depuis l'extérieur du périmètre de sécurité). Les pirates extérieurs potentiels vont du farceur amateur aux organisations criminelles, aux terroristes internationaux et aux gouvernements hostiles.

3.1.4
authentification
vérification de l'identité revendiquée d'une entité

Note 1 à l'article: En règle générale, l'authentification est une condition préalable à l'accès aux ressources d'un système de commande.

3.1.5
authentifiant
moyen utilisé pour confirmer l'identité d'une entité

EXEMPLE Un mot de passe ou un jeton peut faire office d'authentifiant.

3.1.6
authenticité
propriété selon laquelle une entité est bien ce qu'elle revendique être au moyen d'une authentification de son origine et de la vérification de son intégrité

Note 1 à l'article: En règle générale, l'authenticité est utilisée pour établir la confiance en l'identité d'une entité ou en la validité d'une transmission, d'un message ou de l'expéditeur d'un message.

3.1.7
disponibilité
propriété assurant un accès opportun et fiable aux informations et fonctionnalités du système de commande et leur utilisation

3.1.8
canal de communication
liaison spécifique de communication logique ou physique entre les actifs

Note 1 à l'article: Un canal facilite l'établissement d'une connexion.

3.1.9
contre-mesure compensatoire
contre-mesure utilisée en lieu et place ou en complément des capacités de sécurité inhérentes pour satisfaire à une ou plusieurs exigences de sécurité

EXEMPLE

– (niveau du composant): enceinte verrouillée autour d'un contrôleur qui pourrait, dans d'autres circonstances, être exposée à un accès non autorisé par ses interfaces physiques de données;
– (niveau du système de commande/de la zone): commande d'accès physique (protections, portes et pistolets) pour protéger une salle de commande et limiter l'accès à un groupe de personnes connues, venant en complément des exigences techniques relatives aux personnes que l'IACS identifie de manière unique; et
– (niveau du composant): l'automate programmable (PLC) d'un fournisseur de produit ne pouvant pas satisfaire aux capacités de contrôle d'accès d'un propriétaire d'actif, le fournisseur place un pare-feu devant le PLC et le vend comme un système.

3.1.10
composant
entité appartenant à un IACS qui présente les caractéristiques d'un ou plusieurs appareils hôtes, appareils de réseaux, applications logicielles ou appareils intégrés

3.1.11
conduit
groupement logique de canaux de communication, connectant au moins deux zones, et partageant des exigences communes de sécurité

Note 1 à l'article: La traversée d'une zone par un conduit est admise tant que cette zone n'a pas d'impact sur la sécurité des canaux que le conduit contient.

3.1.12
confidentialité
assurance que les informations ne sont pas divulguées à des individus, processus ou appareils non autorisés

Note 1 à l'article: Utilisée dans le contexte d'un IACS, la confidentialité fait référence à la protection des données et informations de l'IACS depuis un accès non autorisé.

3.1.13
connexion
association établie entre au moins deux points d'extrémité et prenant en charge l'établissement d'une session

3.1.14
système de commande
composants matériels ou logiciels d'un IACS

3.1.15
contre-mesure
action, appareil, procédure ou technique qui réduit une menace, une vulnérabilité ou les conséquences d'une attaque en réduisant le plus possible les préjudices dont l'attaque peut être à l'origine ou en la détectant et la signalant de manière à pouvoir lancer une action corrective

Note 1 à l'article: Dans certains cas, le terme «commande» est également utilisé pour décrire ce concept. Le terme «contre-mesure» a été choisi dans le présent document pour éviter la confusion avec le terme «commande» dans le contexte de la «commande de processus» et du «système de commande».

3.1.16
mode dégradé
mode de fonctionnement en présence de défauts qui ont été anticipés dans la conception du système de commande

Note 1 à l'article: Les modes dégradés permettent au système de commande de continuer à assurer les fonctions essentielles malgré la déficience d'un ou de plusieurs de ses éléments de système (dysfonctionnement ou coupure de l'équipement de commande, interruption de la communication par suite d'une défaillance ou isolation volontaire du système en réponse à une atteinte identifiée ou suspectée des sous-systèmes, par exemple).

3.1.17
appareil
actif physique discret qui fournit un ensemble de capacités

EXEMPLE Contrôleurs, interfaces homme/machine (IHM), automates programmables, terminaux à distance (RTU), émetteurs-récepteurs, actionneurs, soupapes, interrupteurs de réseau.

Note 1 à l'article: Un appareil peut présenter les caractéristiques d'un ou plusieurs appareils hôtes, appareils de réseaux, applications logicielles ou appareils intégrés.

3.1.18
appareil intégré
appareil spécial conçu pour surveiller ou commander directement un processus industriel

EXEMPLE Automates programmables, appareils capteurs de terrain câblés ou sans fil, appareils actionneurs de terrain câblés ou sans fil, contrôleurs de système instrumenté de sécurité (SIS) et contrôleurs de système à commande distribuée (DCS).

Note 1 à l'article: Le stockage limité d'attributs classiques, le nombre limité de services exposés, programmés au moyen d'une interface externe, les systèmes d'exploitation (OS) intégrés ou micrologiciels équivalents et les programmeurs en temps réel peuvent disposer d'un panneau de commande et d'une interface de communication.

3.1.19
environnement
objets, région ou circonstances environnant(e)s qui peuvent avoir un impact sur le comportement de l'IACS et/ou peuvent être influencés par l'IACS

3.1.20
fonction essentielle
fonction ou capacité exigée pour maintenir la santé, la sécurité, l'environnement (HSE) et la disponibilité de l'équipement commandé

Note 1 à l'article: Les fonctions essentielles incluent, entre autres, la fonction instrumentée de sécurité (SIF), la fonction de commande et l'aptitude de l'opérateur à visualiser et manipuler l'équipement commandé. La perte des fonctions essentielles est souvent appelée perte de protection, perte de commande et perte de visualisation, respectivement. Dans certains secteurs industriels, des fonctions supplémentaires peuvent être considérées comme étant essentielles (l'historique, par exemple).

3.1.21
événement
occurrence ou changement d'un ensemble particulier de circonstances

Note 1 à l'article: Dans un IACS, il peut s'agir d'une action réalisée par un individu (autorisé ou non), d'un changement détecté au sein du système de commande (normal ou anormal) ou d'une réponse automatique du système de commande lui-même (normale ou anormale).

3.1.22
firecall (accès temporaire d'urgence)
méthode permettant d'assurer un accès d'urgence à un système de commande sécurisé

Note 1 à l'article: Dans une situation d'urgence, les utilisateurs sans privilège peuvent obtenir l'accès à des systèmes à clés pour corriger le problème. Si un firecall est utilisé, un processus de révision permet en général d'assurer que l'accès a été correctement utilisé pour corriger un problème. En règle générale, ces méthodes fournissent un identificateur utilisateur (ID) ou un mot de passe à usage unique.

3.1.23
appareil hôte
appareil d'usage courant fonctionnant sur un système d'exploitation (Microsoft Windows ou Linux, par exemple) capable d'héberger au moins une application logicielle, un magasin de données ou une fonction provenant d'un ou de plusieurs fournisseurs

Note 1 à l'article: Les attributs classiques sont des systèmes de fichiers, des services programmables, pas de programmeur en temps réel et une IHM complète (clavier, souris, etc.).

3.1.24
identificateur
ensemble de symboles, unique dans son domaine de sécurité, qui permet d'identifier, d'indiquer ou de nommer une entité qui affirme ou revendique une identité

3.1.25
incident
événement qui ne fait pas partie du fonctionnement prévu d'un système ou d'un service et qui provoque (ou peut provoquer) une interruption ou une réduction de la qualité du service fourni par le système de commande

3.1.26
système d'automatisation et de commande industrielles
ensemble des personnes, matériels, logiciels et politiques impliqués dans le processus industriel et qui peuvent affecter ou influencer la sûreté, la sécurité et la fiabilité de son fonctionnement

3.1.27
intégrité
propriété assurant une protection de l’exactitude et de l’exhaustivité des actifs

3.1.28
droit d'accès minimal
principe de base selon lequel il convient d'attribuer aux utilisateurs (êtres humains, processus logiciels ou appareils) les moindres privilèges en fonction de leurs responsabilités et fonctions

Note 1 à l'article: Le droit d'accès minimal est souvent mis en œuvre dans le cadre d'un ensemble de rôles dans un IACS.

3.1.29
code mobile
programme transféré entre des actifs qui peut être exécuté sans installation explicite par le destinataire

EXEMPLE JavaScript, VBScript, applets Java, contrôles ActiveX, animations Flash, films Shockwave et macros Microsoft Office.

3.1.30
appareil mobile
appareil électronique intelligent destiné à être transporté

EXEMPLE Ordinateurs portables, robots mobiles, smartphones, programmateurs portatifs, tablettes et assistants numériques personnels.

3.1.31
appareil de réseau
appareil qui facilite ou limite le transfert de données entre les appareils, mais qui peut ne pas interagir directement avec un processus de commande

Note 1 à l'article: Les attributs classiques sont un système d'exploitation ou micrologiciel intégré, pas d'IHM, pas de programmeur en temps réel et une configuration par l'intermédiaire d'une interface externe.

3.1.32
non-répudiation
aptitude à démontrer l'occurrence d'un événement ou d'une action revendiqué(e) et ses entités d'origine

Note 1 à l'article: La non-répudiation a pour objet de résoudre les litiges quant à la survenue ou pas de l'événement ou de l'action et à l'implication des entités dans l'événement.

3.1.33
fournisseur de produit
fabricant du matériel et/ou du produit logiciel

Note 1 à l'article: Utilisé à la place du terme générique «fournisseur» pour faire la distinction.

3.1.34
accès distant
accès à un composant par un utilisateur (être humain, processus logiciel ou appareil) qui communique depuis l'extérieur du périmètre de la zone concernée

3.1.35
rôle
ensemble de comportements, de droits d'accès et d'obligations pouvant être attribués à un utilisateur ou groupe d'utilisateurs (êtres humains, processus logiciels ou appareils) d'un IACS

Note 1 à l'article: Les droits d'accès permettant d'exécuter certaines opérations sont attribués à des rôles spécifiques.

3.1.36
système instrumenté de sécurité
système permettant de mettre en œuvre une ou plusieurs fonctions liées à la sécurité

3.1.37
niveau de sécurité
niveau correspondant à l’ensemble exigé de contre-mesures et de propriétés inhérentes de sécurité des appareils et systèmes pour une zone ou un conduit selon l’appréciation du risque pour la zone ou le conduit

3.1.38
session
échange d'informations semi-permanent, dynamique et interactif entre au moins deux composants qui communiquent

Note 1 à l'article: En règle générale, les processus de début et de fin d'une session sont clairement définis.

3.1.39
ID de session
identificateur utilisé pour indiquer une session spécifique

3.1.40
point de consigne
valeur cible identifiée au sein d'un système de commande et qui contrôle une ou plusieurs actions à l'intérieur de ce système

3.1.41
application logicielle
un ou plusieurs programmes logiciels et leurs dépendances, utilisés pour assurer l'interface avec le processus ou le système de commande lui-même (logiciel de configuration et historien, par exemple)

Note 1 à l'article: Les applications logicielles s'exécutent en général sur des appareils hôtes ou des appareils intégrés.

Note 2 à l'article: Les dépendances sont des programmes logiciels dont a besoin l'application logicielle pour fonctionner (modules de base de données, outils de génération de rapports ou logiciel tiers ou libre, par exemple).

3.1.42
intégrateur système
fournisseur de services dont la spécialité consiste à regrouper les sous-systèmes de composants et à assurer qu'ils fonctionnent conformément aux spécifications du projet

Note 1 à l'article: Il peut également s'agir de sous-traitant général d'automatisation, de sous-traitant principal d'automatisation, de fournisseur principal d'instruments et analogues.

3.1.43
menace
ensemble de circonstances et séquence associée d’événements susceptibles d'avoir un impact négatif sur les opérations (y compris la mission, les fonctions, l'image ou la réputation), les actifs, les systèmes de commande ou les personnes par un accès non autorisé, la destruction, la révélation, la modification des données et/ou le refus de service

3.1.44
confiance
conviction selon laquelle le comportement d’une opération, d’une source de transaction de données, d’un réseau ou d’un processus logiciel peut être fiable comme prévu

Note 1 à l'article: En règle générale, une entité peut «faire confiance» à une autre entité lorsqu'elle (la première entité) part de l'hypothèse selon laquelle la deuxième entité se comportera comme elle le prévoit.

Note 2 à l'article: Cette confiance peut s'appliquer uniquement pour certaines fonctions particulières.

3.1.45
non traçabilité
assurance que les informations ne peuvent pas être utilisées pour suivre la durée ou l'emplacement d'un utilisateur spécifique

3.1.46
non sécurisé
qui ne satisfait pas aux exigences de confiance prédéfinies

Note 1 à l'article: Une entité peut simplement être déclarée comme étant non sécurisée.

3.1.47
mise à jour
modification incrémentielle du matériel ou du logiciel visant à résoudre les vulnérabilités de sécurité, les bugs ou les problèmes de fiabilité ou d'aptitude au fonctionnement

3.1.48
mise à niveau
modification incrémentielle du matériel ou du logiciel visant à ajouter de nouvelles fonctions

3.1.49
zone
ensemble d'entités qui représente le partitionnement d'un système à l'étude sur la base de leurs relations fonctionnelles, logiques et physiques (y compris l'emplacement)

Note 1 à l'article: Une zone présente une frontière claire. La politique de sécurité d'une zone est en général renforcée par une combinaison de mécanismes tant aux abords de la zone qu'à l'intérieur de celle-ci.

3.2 Termes abrégés et acronymes

ACL	access control list (liste de contrôle d'accès)
AES	advance encryption standard (norme de chiffrement avancé)
ANSI	American National Standards Institute (institut national de normalisation américain)
API	application programming interface (interface de programmation d'application)
ASLR	address space layout randomization (mise en espace d'adressage aléatoire)
AC	autorité de certification
CCSC	common component security constraint (contrainte commune en matière de sécurité du composant)
CMAC	cipher-based message authentication code (code d'authentification de message par chiffrement)
COTS	commercial off the shelf (produit commercial sur étagère)
CR	component requirement (exigence relative au composant)
CRL	certificate revocation list (liste de révocation de certificat)
DC	data confidentiality (confidentialité des données)
DCS	distributed control system (système à commande distribuée)
DEP	data execution prevention (prévention d'exécution des données)
DMZ	demilitarized zone (zone démilitarisée)
DNS	domain name service (service de noms de domaine)
DoS	denial of service (refus de service)
EDR	embedded device requirement (exigence relative aux appareils intégrés)
EICAR	European Institute for Computer Antivirus Research (institut européen de recherche en virologie informatique)
IEM	interférences électromagnétiques
FDA	[US] Food and Drug Administration
FIPS	[US NIST] Federal Information Processing Standard
FR	foundational requirement (exigence fondamentale)
FTP	file transfer protocol (protocole de transfert de fichiers)
GCM	Galois/Counter mode (mode Galois/Counter)
GMAC	Galois message authentication code (code d'authentification de message Galois)
GUID	globally unique identifiers (identificateurs globaux uniques)
HDR	host device requirement (exigence relative aux appareils hôtes)
IHM	interface homme/machine
HSE	health, safety and environmental (santé, sécurité et environnement)
HTTP	hypertext transfer protocol (protocole de transfert hypertexte)
HTTPS	HTTP sécurisé

IAC	identification and authentication control (contrôle d'identification et d'authentification)
IACS	industrial automation and control system(s) (système(s) d'automatisation et de commande industrielles)
ID	identificateur
IDS	intrusion detection system (système de détection des intrusions)
IED	intelligent electronic device (appareil électronique intelligent)
IEC	International Electrotechnical Commission (Commission Electrotechnique Internationale)
IEEE	Institute of Electrical and Electronics Engineers (institut des ingénieurs électriciens et électroniciens)
IP	Internet protocol (protocole Internet)
IPS	intrusion prevention system (système de prévention des intrusions)
ISA	International Society of Automation
ISO	International Organization for Standardization (organisation internationale de normalisation)
IT	information technology (technologie de l'information)
JTAG	Joint Test Action Group
LDAP	lightweight directory access protocol (protocole d'accès au répertoire allégé)
NDR	network device requirement (exigence relative aux appareils de réseaux)
NIST	U.S. National Institute of Standards and Technology
NX	No Execute (pas d'exécution)
OCSP	online certificate status protocol (protocole d'état de vérification en ligne de certificat)
OS	operating system (système d'exploitation)
OWASP	Open Web Application Security Project (projet de sécurité ouvert d'application Web)
PC	personal computer (ordinateur personnel)
PDF	portable document format
PKI	public key infrastructure (infrastructure à clés publiques)
PLC	programmable logic controller (automate programmable)
RA	resource availability (disponibilité des ressources)
RAM	random access memory (mémoire à accès aléatoire)
RDF	restricted data flow (transfert de données limité)
RE	requirement enhancement (amélioration d'exigences)
RTOS	real-time operating system (système d'exploitation en temps réel)
RTU	remote terminal unit (terminal à distance)
SAR	software application requirements (exigences relatives aux applications logicielles)
SFTP	secure FTP (FTP sécurisé)
SHA	secure hash algorithm (algorithme de compression sécurisé)
SI	system integrity (intégrité du système)
SIEM	security information and event management (gestion des informations sur la sécurité et des événements)
SIF	safety instrumented function (fonction instrumentée de sécurité)
SIS	safety instrumented system (système instrumenté de sécurité)

SL	security level (niveau de sécurité)
SL-A	achieved security level (niveau de sécurité atteint)
SL-C	capability security level (niveau de sécurité de capacité)
SL-T	target security level (niveau de sécurité cible)
SNMP	simple network management protocol (protocole de gestion de réseau simple)
SP	[US NIST] Special Publication (publication spéciale)
SR	system requirement (exigence relative au système)
SSH	secure socket shell
SuC	system under consideration (système à l'étude)
SQL	structured query language (langage de requête structurée)
TCP	transmission control protocol (protocole de contrôle de transmission)
TPM	trusted platform module (module de plateforme digne de confiance)
TRE	timely response to events (réponse appropriée aux événements)
UC	use control (contrôle d'utilisation)
USB	universal serial bus (bus série universel)
RPV	réseau privé virtuel

3.3 Conventions

Le présent document développe les SR et les RE définies dans l'IEC 62443-3-3 en une série de CR et de RE destinées aux composants d'un même IACS. Pour faciliter le suivi des CR par rapport aux SR de l'IEC 62443-3-3, la numérotation des unes correspond à celle des autres. Cela a pour conséquence des écarts et une numérotation non séquentielle dans le présent document. Pour faciliter la lecture et dans toute la mesure du possible, chacune des exigences de base et des notes est justifiée et fait l'objet de recommandations complémentaires pour toutes les RE correspondantes.

Les types de composants d'un IACS tels que définis dans le présent document sont les applications logicielles, les appareils hôtes, les appareils intégrés et les appareils de réseaux. La plupart des exigences relatives au composant (CR) et des améliorations d'exigences (RE) sont applicables aux quatre types de composants et sont combinées en une seule exigence relative au composant (CR). Certaines CR et RE sont uniques à un type particulier de composant. Ces exigences spécifiques à un type de composant ont été traitées dans des articles séparés par souci de commodité. Les exigences spécifiques aux applications logicielles, aux appareils intégrés, aux appareils hôtes et aux appareils de réseaux sont couvertes à partir de l'Article 12. Lorsqu'un composant satisfait à la définition d'une ou plusieurs applications logicielles ou d'un ou plusieurs appareils hôtes, appareils intégrés ou appareils de réseaux, ce composant est réputé satisfaire à toutes les exigences indiquées pour chaque type de composant auquel il correspond.

Chacune des sept exigences fondamentales (FR) de l'IEC TS 62443-1-1 comprend un ensemble défini de quatre niveaux de sécurité (SL). Ces SL sont déduits des niveaux de sécurité du système définis dans l'IEC 62443-3-3. Un niveau de sécurité du composant est décrit par FR à l'aide de la notation SL-C(FR, composant), accompagnée d'une valeur correspondante comprise entre 0 et 4. Le niveau de sécurité 0 du système de commande pour une FR particulière est défini de manière implicite comme ne faisant l'objet d'aucune exigence. Les exigences de base et les RE, le cas échéant, sont ensuite mises en correspondance avec le niveau de sécurité de capacité du composant, SL-C(FR, composant) 1 à 4.

Par exemple, l'Article 8 énonce l'objet de la manière suivante:

Vérifier la confidentialité des informations présentes sur les canaux de communication et dans les référentiels de données afin d'éviter toute divulgation non autorisée.

Les quatre SL correspondants sont définis comme suit:

- SL 1 – Empêcher la divulgation non autorisée des informations par écoute informatique ou exposition occasionnelle.
- SL 2 – Empêcher la divulgation non autorisée des informations à une entité qui les recherche activement, en utilisant des moyens simples avec peu de ressources, des compétences génériques et peu de motivation.
- SL 3 – Empêcher la divulgation non autorisée des informations à une entité qui les recherche activement, en utilisant des moyens sophistiqués avec des ressources modérées, des compétences spécifiques à l'IACS et une motivation modérée.
- SL 4 – Empêcher la divulgation non autorisée des informations à une entité qui les recherche activement, en utilisant des moyens sophistiqués avec des ressources étendues, des compétences spécifiques à l'IACS et une motivation élevée.

Les attributions de CR et de RE individuelles reposent donc sur une augmentation progressive de la sécurité générale du composant pour cette FR particulière, en fonction des connaissances et de l'expertise de l'équipe qui crée le présent document.

Le SL-C(composant), utilisé tout au long du présent document, signifie que la satisfaction à un classement SL donné pour une CR donnée est exigée de la part d'une capacité. Une description complète du concept de vecteur SL peut être consultée dans l'IEC 62443-3-3.

4 Contraintes communes en matière de sécurité du composant

4.1 Vue d'ensemble

La lecture, la spécification et la mise en œuvre des CR décrites dans les Articles 5 à 15 du présent document prouvent qu'il existe un certain nombre de contraintes communes dont l'application est exigée au cours de la mise en œuvre des exigences décrites dans le présent document.

4.2 Support des fonctions essentielles CCSC 1

Les composants du système doivent respecter les contraintes spécifiques décrites à l'Article 4 de l'IEC 62443-3-3:2013.

4.3 Contre-mesures compensatoires CCSC 2

Dans certains cas, une ou plusieurs exigences spécifiées dans le présent document ne peuvent pas être satisfaites sans l'aide d'une contre-mesure compensatoire externe au composant. Si c'est le cas, la documentation de ce composant doit décrire les contre-mesures appropriées que le système applique pour pouvoir satisfaire à l'exigence lors de l'intégration du composant dans un système.

4.4 Droit d'accès minimal CCSC 3

Si cela est exigé et approprié, un ou plusieurs composants du système (applications logicielles, appareils intégrés, appareils hôtes et appareils de réseaux) doivent permettre au système d'imposer le concept de droit d'accès minimal. Les composants individuels du système doivent assurer la granularité des droits d'accès et la souplesse du mapping de ces droits d'accès aux rôles suffisante pour sa prise en charge. L'imputabilité individuelle doit être disponible, si exigée. La granularité des droits d'accès et de l'attribution dépend du type d'appareil, et il convient que la documentation du produit correspondant à l'appareil le définisse.

4.5 Processus de développement logiciel CCSC 4

Tous les composants définis dans le présent document doivent être développés et pris en charge selon les processus de développement sécurisé du produit décrits dans l'IEC 62443-4-1.

5 FR 1 – Contrôle d'identification et d'authentification

5.1 Objet et descriptions du SL-C(IAC)

Identifier et authentifier tous les utilisateurs (êtres humains, processus logiciels et appareils) avant de leur permettre d'accéder au système ou aux actifs.

- SL 1 – Identifier et authentifier tous les utilisateurs (êtres humains, processus logiciels et appareils) par des mécanismes de protection contre les accès fortuits ou occasionnels par des entités non authentifiées.
- SL 2 – Identifier et authentifier tous les utilisateurs (êtres humains, processus logiciels et appareils) par des mécanismes de protection contre les accès non authentifiés volontaires par des entités utilisant des moyens simples avec peu de ressources, des compétences génériques et peu de motivation.
- SL 3 – Identifier et authentifier tous les utilisateurs (êtres humains, processus logiciels et appareils) par des mécanismes de protection contre les accès non authentifiés volontaires par des entités utilisant des moyens sophistiqués avec des ressources modérées, des compétences spécifiques à l'IACS et une motivation modérée.
- SL 4 – Identifier et authentifier tous les utilisateurs (êtres humains, processus logiciels et appareils) par des mécanismes de protection contre les accès non authentifiés volontaires par des entités utilisant des moyens sophistiqués avec des ressources étendues, des compétences spécifiques à l'IACS et une motivation élevée.

5.2 Justification

Une identification des utilisateurs est utilisée conjointement avec des mécanismes d’autorisation afin de mettre en œuvre le contrôle d’accès d’un composant. La vérification de l’identité des utilisateurs qui demandent un accès est nécessaire pour assurer une protection contre l’accès au composant par des utilisateurs non autorisés. Il convient que les recommandations et lignes directrices contiennent les mécanismes qui fonctionneront en mode mixte. Par exemple, certains composants sur un canal de communication, contrairement à d’autres, exigent un important contrôle d'accès (de stricts mécanismes d'authentification, par exemple). Par extension, les exigences en matière de contrôle d'accès doivent être étendues aux données au repos.

Il est recommandé de réduire le plus possible le nombre de mécanismes d'identification et d'authentification dans une seule zone. L'utilisation de plusieurs de ces mécanismes complique l'administration des tâches de gestion de l'authentification et de l'identification.

5.3 CR 1.1 – Identification et authentification d'un utilisateur humain

5.3.1 Exigences

Les composants doivent offrir la possibilité d'identifier et d'authentifier tous les utilisateurs humains conformément à l'IEC 62443-3-3 SR 1.1 sur toutes les interfaces auxquelles ils sont en mesure d’accéder. Cette capacité doit mettre en place ce type d'identification et d'authentification sur toutes les interfaces qui permettent à un utilisateur humain d'accéder au composant pour assurer la répartition des tâches et des droits d'accès minimaux conformément aux politiques et procédures de sécurité applicables. Cette capacité peut être assurée de manière locale par le composant ou par intégration dans un système d’identification et d’authentification au niveau du système.

NOTE Les politiques de sécurité applicables sont un enjeu local.

5.3.2 Justification et recommandations complémentaires

Il est nécessaire d'identifier et d'authentifier tous les utilisateurs humains qui accèdent au composant. Il convient d'authentifier l'identité de ces utilisateurs par des mots de passe, des jetons, des éléments biométriques ou des couvercles verrouillés physiquement et, en cas d'authentification à plusieurs facteurs, par l'une de leurs combinaisons. L'emplacement géographique des utilisateurs humains peut également être utilisé dans le cadre du processus d'authentification. Il convient d'appliquer cette exigence tant à l'accès local qu'à l'accès distant au composant. Cette exigence vient en complément de l'exigence de présenter ce type de mécanisme d'authentification et d'identification au niveau du système.

Les interfaces permettant d'assurer l'accès des utilisateurs humains sont, par exemple, les écrans tactiles, les boutons-poussoirs, les claviers, et des protocoles de réseau conçus pour des interactions humaines, comme le protocole de transfert hypertexte (HTTP), HTTP sécurisé (HTTPS), le protocole de transfert de fichiers (FTP), FTP sécurisé (SFTP), les protocoles utilisés pour les outils de configuration des appareils (qui sont parfois propriétaires et d'autres fois utilisent des protocoles ouverts). L'identification et l'authentification de l'utilisateur peuvent reposer sur les rôles ou sur les groupes (comme pour certaines interfaces de composant, plusieurs utilisateurs peuvent partager la même identité). Il convient que l'identification et l'authentification de l'utilisateur ne gênent pas les actions d'urgence rapides locales.

Pour prendre en charge les politiques IAC telles que définies selon l'IEC 62443-3-3 [13], il convient que le composant vérifie en tout premier lieu l'identité de tous les utilisateurs humains. En second lieu, il convient de renforcer les droits d'accès attribués à l'utilisateur humain identifié (voir 5.3).

5.3.3 Amélioration d'exigences

(1) Identification et authentification uniques:

Les composants doivent offrir la possibilité d'identifier et d'authentifier de manière unique tous les utilisateurs humains.

(2) Authentification à plusieurs facteurs pour toutes les interfaces

Les composants doivent offrir la possibilité d'utiliser l'authentification à plusieurs facteurs pour tous les utilisateurs humains qui accèdent au composant.

5.3.4 Niveaux de sécurité

Les exigences pour les quatre niveaux de sécurité liés à CR 1.1 sont les suivantes:

- SL-C(IAC,composant) 1: CR 1.1
- SL-C(IAC,composant) 2: CR 1.1 (1)
- SL-C(IAC,composant) 3: CR 1.1 (1) (2)
- SL-C(IAC,composant) 4: CR 1.1 (1) (2)

5.4 CR 1.2 – Identification et authentification du processus logiciel et de l’appareil

5.4.1 Exigences

Les composants doivent offrir la possibilité de s'identifier et de s'authentifier auprès d’un autre composant (application logicielle, appareils intégrés, appareils hôtes et appareils de réseaux), conformément à l'IEC 62443-3-3 SR1.2.

De plus, si le composant fonctionne dans le contexte d'une utilisation par l'homme, comme c’est le cas lors d’une application, l'identification et l'authentification de ce dernier selon l'IEC 62443-3-3 SR1.1 peuvent faire partie du processus d'identification et d'authentification du composant auprès d'autres composants.

5.4.2 Justification et recommandations complémentaires

La fonction d'identification et d'authentification consiste à mettre en correspondance une identité connue et un processus logiciel ou appareil inconnu (appelé «entité» en 5.4.1) de manière à le faire connaître pour échanger des données. Permettre à des entités malveillantes d'envoyer et de recevoir des données spécifiques au système de commande peut donner lieu à un comportement préjudiciable du système de commande.

Il convient d'identifier et d'authentifier toutes les entités qui accèdent au système de commande. Il convient d'authentifier l'identité de ces entités par des méthodes comme les mots de passe, les jetons ou selon l'emplacement (physique ou logique). Il convient d'appliquer cette exigence tant à l'accès local qu'à l'accès distant au système de commande. Toutefois, dans certains scénarii dans lesquels des entités individuelles sont utilisées pour se connecter à différents systèmes cibles (le support à distance d'un fournisseur, par exemple), il peut être impossible d'un point de vue technique d'avoir plusieurs identités. Dans ces cas, des contre-mesures compensatoires devraient être appliquées.

Une attention particulière doit être portée lors de l'identification et de l'authentification des appareils portables et mobiles. Ces types d'appareils sont un vecteur connu d'introduction d'un trafic de réseau indésirable, d'exposition aux logiciels malveillants et/ou d'exposition des informations relatives au système de commande, y compris sur les réseaux isolés.

Lorsque les entités fonctionnent comme un seul groupe, l'identification et l'authentification peuvent reposer sur le rôle, le groupe ou l'entité. Il est fondamental que les actions locales d'urgence et les fonctions essentielles du système de commande ne soient pas gênées par les exigences d'identification ou d'authentification (voir l'Article 4 pour une présentation plus exhaustive). Par exemple, dans des schémas courants de protection et de commande, un groupe d'appareils exécute conjointement les fonctions de protection et communique avec les messages multidiffusion entre les appareils du groupe. Dans ces cas, l'authentification de groupe reposant sur des comptes partagés ou des clés symétriques partagées est souvent utilisée.

Pour prendre en charge les politiques de contrôle d'identification et d'authentification telles que définies selon l'IEC 62443-2-1 [11], le système de commande vérifie en tout premier lieu l'identité de toutes les entités. En second lieu, les droits d'accès attribués à l'entité identifiée sont renforcés (voir 6.3).

5.4.3 Amélioration d'exigences

(1) Identification et authentification uniques

Les composants doivent offrir la possibilité de s'identifier et s'authentifier de manière unique auprès des autres composants.

5.4.4 Niveaux de sécurité

Les exigences pour les quatre niveaux de sécurité liés à CR 1.2 sont les suivantes:

- SL-C(IAC,composant) 1: Non choisi
- SL-C(IAC,composant) 2: CR 1.2
- SL-C(IAC,composant) 3: CR 1.2 (1)
- SL-C(IAC,composant) 4: CR 1.2 (1)

5.5 CR 1.3 – Gestion de compte

5.5.1 Exigences

Les composants doivent offrir la possibilité de prendre en charge la gestion directe de tous les comptes ou l'intégrer dans un système qui gère tous les comptes selon l'IEC 62443-3-3 SR 1.3.

5.5.2 Justification et recommandations complémentaires

Un composant peut offrir cette possibilité en s'intégrant dans un système de gestion de compte de niveau supérieur. Si la possibilité n’est pas intégrée dans un système de gestion de compte de niveau supérieur, le composant est présumé offrir nativement la possibilité.

Une approche courante satisfaisant à cette exigence serait un composant qui délègue la validité de l'authentification à un serveur d'annuaire (LDAP ou Active Directory, par exemple) qui fournit les capacités de gestion de compte exigées par l'IEC 62443-3-3 SR 1.3.

Si un composant s'intègre dans un système de niveau supérieur pour fournir les capacités de gestion de compte, il est nécessaire de prendre en considération l'impact sur le composant en cas d'indisponibilité de la capacité du système de niveau supérieur.

5.5.3 Amélioration d'exigences

Aucune

5.5.4 Niveaux de sécurité

Les exigences pour les quatre niveaux de sécurité liés à CR 1.3 sont les suivantes:

- SL-C(IAC,composant) 1: CR 1.3
- SL-C(IAC,composant) 2: CR 1.3
- SL-C(IAC,composant) 3: CR 1.3
- SL-C(IAC,composant) 4: CR 1.3

5.6 CR 1.4 – Gestion d’identificateur

5.6.1 Exigences

Les composants doivent offrir la possibilité de s'intégrer dans un système qui prend en charge la gestion des identificateurs et/ou de prendre en charge la gestion directe des identificateurs selon l'IEC 62443-3-3 SR 1.4.

5.6.2 Justification et recommandations complémentaires

Les comptes créés selon CR 1.3 – Gestion de compte (5.5) exigent l’utilisation d’un ou plusieurs identificateurs pour identifier chaque compte distinctement. Il convient que ces identificateurs soient uniques et sans ambiguïté concernant le compte auquel ils sont associés. Les noms de comptes, identificateurs utilisateurs UNIX, identificateurs globaux uniques (GUID) de comptes Microsoft Windows, et certificats liés X.509 sont des exemples d’identificateurs d’usage commun. Un composant peut offrir la possibilité locale d’associer les identificateurs à des comptes. Si le composant est intégré dans un système qui applique une politique de sécurité à l’échelle du système, il est fortement recommandé d’associer les identificateurs au même compte pour tous les composants du système. Pour ce faire, il convient qu’un composant soit en mesure de s’intégrer dans une capacité de gestion d’identificateur à l’échelle du système.

5.6.3 Amélioration d'exigences

Aucune

5.6.4 Niveaux de sécurité

Les exigences pour les quatre niveaux de sécurité liés à CR 1.4 sont les suivantes:

- SL-C(IAC,composant) 1: CR 1.4
- SL-C(IAC,composant) 2: CR 1.4
- SL-C(IAC,composant) 3: CR 1.4
- SL-C(IAC,composant) 4: CR 1.4

5.7 CR 1.5 – Gestion d'authentifiant

5.7.1 Exigences

Les composants doivent offrir la possibilité de:

a) prendre en charge l'utilisation du contenu initial de l'authentifiant;

b) prendre en charge la reconnaissance des modifications apportées aux authentifiants par défaut au moment de l'installation;

c) fonctionner correctement avec des opérations périodiques de modification/actualisation des authentifiants; et

d) protéger les authentifiants contre toute divulgation et modification non autorisées lors du stockage, de l'utilisation et de la transmission.

5.7.2 Justification et recommandations complémentaires

Outre l'identificateur (voir 5.6), un authentifiant est exigé pour prouver l'identité. Les authentifiants de système de commande incluent, entre autres, les jetons, les clés symétriques, les clés privées (partie d'une paire de clés publique/privée), les éléments biométriques, les mots de passe, les clés physiques et les cartes-clés. Il convient de mettre en place des politiques de sécurité afin que les utilisateurs humains prennent des mesures raisonnables pour protéger les authentifiants, y compris de conserver la possession de leurs authentifiants individuels, de ne pas les prêter ni les partager avec d'autres personnes et de signaler immédiatement la perte ou la compromission des authentifiants.

Les authentifiants ont une durée de vie. Lors de la création d'un compte, il est nécessaire de créer automatiquement un authentifiant pour que le titulaire du compte soit en mesure de procéder à l'authentification. Par exemple, dans un système à mot de passe, le compte est associé à un mot de passe. Une des interprétations possibles de la définition du contenu initial de l'authentifiant est la définition par l'administrateur du mot de passe initial défini par le système de gestion de compte pour tous les nouveaux comptes. La capacité de configurer ces valeurs initiales rend plus difficile pour un attaquant de deviner le mot de passe entre la création du compte et sa première utilisation (pour cela, il convient que le titulaire du compte définisse un nouveau mot de passe). Certains systèmes de commande sont installés avec des programmes d'installation sans surveillance qui créent tous les comptes nécessaires avec des mots de passe par défaut, certains appareils intégrés étant quant à eux livrés avec des mots de passe par défaut. Avec le temps, ces mots de passe deviennent connus et sont disponibles sur Internet. Être en mesure de modifier les mots de passe par défaut permet de protéger le système contre les utilisateurs non autorisés qui utilisent les mots de passe par défaut pour y accéder. Les mots de passe peuvent être obtenus depuis le stockage ou la transmission lorsqu'ils sont utilisés dans le cadre d'une authentification réseau. La complexité peut être augmentée par des protections cryptographiques (chiffrement ou hachage, par exemple) ou par des protocoles d'établissement de liaison qui n'exigent aucune transmission du mot de passe. Pour autant, les mots de passe peuvent faire l'objet d'attaques (une attaque en force pour deviner ou briser la protection cryptographique des mots de passe en transit ou stockés, par exemple). Les occasions peuvent être limitées en modifiant/actualisant régulièrement les mots de passe. Des considérations analogues s'appliquent aux systèmes d'authentification basés sur les clés cryptographiques. La protection peut être améliorée à l'aide de mécanismes matériels tels que les modules de sécurité matérielle (les modules de plateforme digne de confiance (TPM), par exemple).

Il convient de spécifier la gestion des authentifiants dans les politiques et procédures applicables de sécurité (contraintes de modifier les authentifiants par défaut, période d'actualisation, spécification de la protection des authentifiants ou procédures firecall, par exemple).

Outre les capacités de gestion des authentifiants spécifiées dans cette exigence, la force du mécanisme d'authentification dépend de l'authentifiant choisi (la complexité du mot de passe ou la longueur de clé dans le cas d'une authentification par clé publique, par exemple) et des politiques de validation des authentifiants dans le processus d'authentification (la mesure

dans laquelle un mot de passe est valide ou les vérifications réalisées dans le cadre d'une validation de certificat à clé publique, par exemple). Pour les mécanismes d'authentification les plus courants (authentification basée sur mot de passe et sur clé publique), les paragraphes 5.9, 5.10 et 5.11 spécifient d'autres exigences.

L'utilisation de composants pour certaines opérations peut être limitée et exiger une authentification supplémentaire (des jetons, des clés et des certificats, par exemple) pour exécuter certaines fonctions.

5.7.3 Amélioration d'exigences

(1) Sécurité matérielle des authentifiants

Les authentifiants sur lesquels s'appuie le composant doivent être protégés par des mécanismes matériels.

EXEMPLE Mémoire protégée par mot de passe, mémoire OTP, contrôles d'intégrité matériels des données et mécanisme d'amorçage de la sécurité des appareils.

5.7.4 Niveaux de sécurité

Les exigences pour les quatre niveaux de sécurité liés à CR 1.5 sont les suivantes:

- SL-C(IAC,composant) 1: CR 1.5
- SL-C(IAC,composant) 2: CR 1.5
- SL-C(IAC,composant) 3: CR 1.5 (1)
- SL-C(IAC,composant) 4: CR 1.5 (1)

5.8 CR 1.6 – Gestion des accès sans fil

Les exigences relatives à la gestion des accès sans fil sont spécifiques aux composants de réseau et peuvent être considérées comme des exigences pour les composants de réseau de l'Article 15.

5.9 CR 1.7 – Force de l'authentification basée sur mot de passe

5.9.1 Exigences

Les composants qui utilisent l'authentification basée sur mot de passe doivent fournir un système, ou s'y intégrer, qui offre la possibilité de renforcer le mot de passe configurable conformément aux lignes directrices reconnues et éprouvées au niveau international concernant les mots de passe.

5.9.2 Justification et recommandations complémentaires

L'aptitude à renforcer le mot de passe configurable, qu'il s'agisse de sa longueur minimale, de la variété de ses caractères ou de sa durée (le minimum étant un mot de passe à usage unique) est indispensable à l'accroissement de la sécurité globale des mots de passe choisis par l'utilisateur. En règle générale, les pratiques acceptées et les recommandations peuvent être consultées dans des documents tels que [20].

5.9.3 Amélioration d'exigences

(1) Restrictions en matière de génération et de durée de vie des mots de passe pour les utilisateurs humains

Les composants doivent fournir un système, ou s'y intégrer, qui offre la possibilité de protéger un compte d'utilisateur humain donné contre les réutilisations d'un mot de passe pour un nombre configurable de générations. De plus, le composant doit offrir la possibilité de renforcer les restrictions en matière de durée de vie maximale et minimale des mots de passe pour les utilisateurs humains. Ces capacités doivent être conformes aux pratiques du secteur de la sécurité acceptées d'un commun accord.

Il convient que le composant offre la possibilité d'inviter l'utilisateur à modifier son mot de passe à un moment configurable avant son expiration.

(2) Restrictions en matière de durée de vie des mots de passe pour tous les utilisateurs (êtres humains, processus logiciels ou appareils)

Les composants doivent fournir un système, ou s'y intégrer, offrant la possibilité de renforcer les restrictions en matière de durée de vie minimale et maximale des mots de passe pour tous les utilisateurs.

5.9.4 Niveaux de sécurité

Les exigences pour les quatre niveaux de sécurité liés à CR 1.7 sont les suivantes:

- SL-C(IAC,composant) 1: CR 1.7
- SL-C(IAC,composant) 2: CR 1.7
- SL-C(IAC,composant) 3: CR 1.7 (1)
- SL-C(IAC,composant) 4: CR 1.7 (1) (2)

5.10 CR 1.8 – Certificats d'infrastructure à clés publiques

5.10.1 Exigences

Si une infrastructure à clés publiques (PKI) est utilisée, le composant doit fournir un système, ou s'y intégrer, offrant la possibilité d'interagir et de fonctionner conformément à l'IEC 62443-3-3 SR1.8.

5.10.2 Justification et recommandations complémentaires

Il convient que le choix d'une infrastructure à clés publiques tienne compte de la politique de l'organisation en matière de certificats, dont il convient qu'elle repose sur le risque lié à une violation de la confidentialité des informations protégées. Des recommandations relatives à la définition de la politique peuvent être consultées dans les normes et lignes directrices acceptées d'un commun accord (Request for Comment (RFC) 3647 [24] de l'Internet Engineering Task Force (IETF) relative au PKI basée sur le certificat X.509, par exemple). Par exemple, dans le cadre de la politique mise en place qui dépend de l'architecture réseau, il convient de tenir compte de l'emplacement approprié d'une autorité de certification (AC), à l'intérieur du système de commande ou sur Internet, et de la liste des AC dignes de confiance (voir également l'IEC 62443-2-1 [1]).

5.10.3 Amélioration d'exigences

Aucune

5.10.4 Niveaux de sécurité

Les exigences pour les quatre niveaux de sécurité liés à CR 1.8 sont les suivantes:

- SL-C(IAC,composant) 1: Non choisi
- SL-C(IAC,composant) 2: CR 1.8
- SL-C(IAC,composant) 3: CR 1.8
- SL-C(IAC,composant) 4: CR 1.8

5.11 CR 1.9 – Force de l'authentification basée sur clé publique

5.11.1 Exigences

Les composants qui utilisent l'authentification basée sur clé publique doivent fournir directement un système, ou s'y intégrer, qui offre les possibilités suivantes dans le même environnement IACS:

validation des certificats par contrôle de la validité de la signature d'un certificat donné;

validation de la chaîne de certificats ou, dans le cas de certificats autosignés, par déploiement des certificats feuilles à tous les hôtes qui communiquent avec le détenteur auquel le certificat est délivré;

c) validation des certificats par contrôle du statut de révocation d'un certificat donné;

d) établissement du contrôle d'utilisateur (être humain, processus logiciel ou appareil) de la clé privée correspondante;

e) mise en correspondance de l'identité authentifiée avec un utilisateur (être humain, processus logiciel ou appareil); et

f) garantie que les algorithmes et les clés utilisés pour l'authentification par clé publique sont conformes à 8.5.

5.11.2 Justification et recommandations complémentaires

La satisfaction aux exigences de 5.11.1 n'exige pas nécessairement une connexion en temps réel à une autorité de certification. D'autres méthodes hors bande peuvent être utilisées pour satisfaire aux exigences de 5.11.1. Par exemple, un système déconnecté pourrait installer et mettre à jour des certifications à l'aide de processus manuels hors bande.

La cryptographie à clé publique/privée dépend beaucoup du secret d'une clé privée d'un détenteur donné et de la bonne gestion des relations de confiance. Lors de la vérification de la relation de confiance entre deux entités sur la base de l'authentification par clé publique, il est essentiel d'assurer le suivi du certificat de clé publique vers une entité digne de confiance. Une erreur de mise en œuvre habituelle dans la validation du certificat consiste à ne contrôler que la validité de la signature du certificat, mais pas la confiance du signataire. Dans une infrastructure à clés publiques, un signataire est digne de confiance si son autorité de certification l'est également ou si son certificat est délivré par une AC digne de confiance, tous les vérificateurs nécessitant donc de tracer les certificats qui leur sont présentés jusqu'à une AC digne de confiance. Si ce type de chaîne ne peut pas être établi, il convient de ne pas faire confiance au certificat présenté.

Si des certificats autosignés sont utilisés à la place d'une infrastructure à clés publiques, le détenteur du certificat signe lui-même son certificat, et il n'y a donc jamais de tiers ou d'AC digne de confiance. Il convient alors de déployer des certificats de clé publique autosignés vers tous les homologues qui ont besoin de les faire valider par un autre mécanisme sécurisé (configuration de tous les homologues dans un environnement digne de confiance, par exemple). Les certificats dignes de confiance nécessitent d'être distribués à des homologues par l'intermédiaire de canaux sécurisés. Lors du processus de validation, il convient qu'un certificat autosigné soit uniquement digne de confiance s'il est déjà présent dans la liste des certificats dignes de confiance de l'homologue de validation. Il convient de configurer l'ensemble des certificats dignes de confiance au nombre minimal nécessaire.

Dans les deux cas, la validation nécessite également de tenir compte de la possibilité de révocation d'un certificat. Dans une infrastructure à clés publiques, il s'agit souvent de gérer des listes de révocation de certificat (CRL) ou d'utiliser un serveur OCSP (protocole d'état de vérification en ligne de certificat). Si le contrôle de révocation n'est pas disponible en raison de contraintes sur le système de commande, des mécanismes peuvent compenser le manque d'informations pertinentes sur la révocation (une durée de vie courte du certificat, par exemple). Il est à noter que les certificats dont la durée de vie est courte peuvent parfois être à l'origine de problèmes opérationnels importants dans un environnement de système de commande.

La plupart des composants sont présumés s'intégrer dans un IACS et exploiter les mécanismes d'authentification à clés fournis par l'IACS sous-jacent. Lors de la mise en œuvre d'une authentification par clé publique au niveau du composant d'un IACS, la protection de la clé devient une préoccupation et un objectif essentiels du stockage de clé sur ce composant. Lors de la mise en œuvre, il convient de veiller à assurer que les clés privées stockées dans le composant ne peuvent pas être récupérées ou manipulées frauduleusement (voir 5.7).

NOTE Des méthodologies et technologies de conception inviolable sont disponibles pour aider à concevoir un mécanisme de protection sécurisé à clé privée.

5.11.3 Amélioration d'exigences

(1) Sécurité matérielle pour l'authentification basée sur clé publique

Les composants doivent offrir la possibilité de protéger les clés privées cruciales à long terme au moyen des mécanismes matériels.

5.11.4 Niveaux de sécurité

Les exigences pour les quatre niveaux de sécurité liés à CR 1.9 sont les suivantes:

- SL-C(IAC,composant) 1: Non choisi
- SL-C(IAC,composant) 2: CR 1.9
- SL-C(IAC,composant) 3: CR 1.9 (1)
- SL-C(IAC,composant) 4: CR 1.9 (1)

5.12 CR 1.10 – Retour de l'authentifiant

5.12.1 Exigences

Si un composant offre une capacité d'authentification, il doit permettre de masquer le retour d'informations de l'authentifiant lors du processus correspondant.

5.12.2 Justification et recommandations complémentaires

Masquer le retour d'informations permet d'éviter qu'elles ne soient éventuellement exploitées par des individus non autorisés (un astérisque ou d'autres caractères aléatoires, par exemple, permettent de masquer le retour des informations d'authentification lorsqu'un utilisateur humain saisit un nom d'utilisateur et/ou un mot de passe). Les jetons SSH et les mots de passe à usage unique sont d'autres exemples de masquage. Il convient que l'entité d'authentification ne donne pas d'indication quant à la raison de l'échec de l'authentification («nom d'utilisateur inconnu», par exemple).

5.12.3 Amélioration d'exigences

Aucune

5.12.4 Niveaux de sécurité

Les exigences pour les quatre niveaux de sécurité SL liés à CR 1.10 sont les suivantes:

- SL-C(IAC,composant) 1: CR 1.10
- SL-C(IAC,composant) 2: CR 1.10
- SL-C(IAC,composant) 3: CR 1.10
- SL-C(IAC,composant) 4: CR 1.10

5.13 CR 1.11 – Tentatives infructueuses de connexion

5.13.1 Exigences

Si un composant fournit une capacité d'authentification, il doit offrir la possibilité:

a) d’appliquer une limite quant au nombre configurable de tentatives d'accès non valides successives par un utilisateur (être humain, processus logiciel ou appareil) pendant une période de temps configurable; et

b) de refuser l'accès pendant une période de temps spécifiée ou jusqu'au déverrouillage par un administrateur lorsque cette limite a été atteinte. Un administrateur peut déverrouiller un compte avant l'expiration de la période de temporisation.

5.13.2 Justification et recommandations complémentaires

Compte tenu des éventuels refus de service, le nombre de tentatives d'accès non valides consécutives peut être limité. Si c'est le cas, l'application ou l'appareil peut automatiquement remettre à zéro le nombre de tentatives d'accès à l'issue d'une période de temps prédéterminée établie par les politiques et procédures de sécurité applicables. La remise à zéro des tentatives d'accès autorise l'accès aux utilisateurs (êtres humains, processus logiciel ou appareil) disposant des informations d'identification de connexion correctes. Il convient de ne pas utiliser le refus automatique d'accès (sans intervention de l'homme) pour les postes de travail ou les nœuds de l'opérateur du système de commande lorsque des réponses immédiates de la part de l'opérateur sont exigées dans des situations d'urgence. Il convient que tous les mécanismes de verrouillage tiennent compte des exigences fonctionnelles en matière de fonctionnement continu, de manière à limiter les conditions de fonctionnement de refus de service préjudiciables qui pourraient donner lieu à des défaillances du système ou compromettre la sécurité du système. Le fait d'autoriser les connexions interactives à un compte utilisé pour les services cruciaux peut générer un éventuel refus de service ou d'autres abus.

5.13.3 Amélioration d'exigences

Aucune

5.13.4 Niveaux de sécurité

Les exigences pour les quatre niveaux de sécurité SL liés à CR 1.11 sont les suivantes:

- SL-C(IAC,composant) 1: CR 1.11
- SL-C(IAC,composant) 2: CR 1.11
- SL-C(IAC,composant) 3: CR 1.11
- SL-C(IAC,composant) 4: CR 1.11

5.14 CR 1.12 – Notification d'utilisation du système

5.14.1 Exigences

Si un composant fournit un accès utilisateur humain local/une IHM, il doit offrir la possibilité d'afficher un message de notification d'utilisation du système avant de procéder à l'authentification. Le message de notification d'utilisation du système doit être configurable par des personnes autorisées.

5.14.2 Justification et recommandations complémentaires

Il est nécessaire que les politiques et procédures de protection de la vie privée et de sécurité soient cohérentes avec les lois, directives, politiques, règlements, normes et recommandations applicables. Souvent, la principale justification de cette exigence est la poursuite pénale des contrevenants et la démonstration d'une violation intentionnelle. Cette capacité est donc nécessaire à la prise en charge des exigences en matière de politique et peut améliorer la sécurité de l'IACS, car elle peut être utilisée comme un élément de dissuasion. Les messages de notification d'utilisation du système peuvent être mis en œuvre sous la forme de bannières d'avertissement lorsque des personnes se connectent au système de commande. Une bannière d'avertissement mise en œuvre sous la forme d'une notice physique postée dans le système de commande ne protège pas contre les problèmes de connexion à distance.

Des exemples d'éléments à inclure dans le message de notification d'utilisation du système sont présentés ci-dessous:

l'individu accède à un système appartenant au propriétaire d'actif;

l'utilisation du système peut être surveillée, enregistrée et faire l'objet d'un audit;

l'utilisation non autorisée du système est interdite et fait l'objet de sanctions pénales et/ou civiles; et

l'utilisation du système implique d'accepter la surveillance et l'enregistrement.

5.14.3 Amélioration d'exigences

Aucune

5.14.4 Niveaux de sécurité

Les exigences pour les quatre niveaux de sécurité SL liés à CR 1.12 sont les suivantes:

- SL-C(IAC,composant) 1: CR 1.12
- SL-C(IAC,composant) 2: CR 1.12
- SL-C(IAC,composant) 3: CR 1.12
- SL-C(IAC,composant) 4: CR 1.12

5.15 CR 1.13 – Accès par l'intermédiaire de réseaux non sécurisés

Les exigences relatives à l'accès par l'intermédiaire de réseaux non sécurisés sont spécifiques au composant et peuvent être considérées comme des exigences pour chaque type de composant spécifique de l'Article 12 à l'Article 15.

5.16 CR 1.14 – Force de l'authentification basée sur clé symétrique

5.16.1 Exigences

Les composants qui utilisent des clés symétriques doivent offrir la possibilité:

a) d'établir la confiance mutuelle à l'aide de la clé symétrique;

b) de stocker en toute sécurité le secret partagé (l'authentification est valide tant que le secret partagé reste un secret);

c) de limiter l'accès au secret partagé; et

d) d'assurer que les algorithmes et les clés utilisés pour l'authentification par clé symétrique sont conformes à 5.11 ou 8.5.

5.16.2 Justification et recommandations complémentaires

Il convient de définir les moyens permettant d'installer les clés dans le composant. Il peut s'agir d'installer et de gérer la clé de composant par des méthodes hors bande. Cela est nécessaire étant donné qu'une compromission de clés symétriques stockées dans le composant pourrait donner lieu à la compromission totale du système à l'aide de ces clés.

Dans la pratique, il existe deux moyens fondamentaux de sécurisation de l'authentification d'un appareil auprès d'un autre: la cryptographie asymétrique (voir 5.11) ou la cryptographie symétrique. Le choix entre ces deux méthodes est dicté par plusieurs critères, comme la gestion de clés, la confiance, le support existant et l'efficacité. Needham-Schröder ou Kerberos sont des exemples de schémas d'authentification par clé symétrique. Si l'authentification par clé symétrique est utilisée, la partie utilise une clé secrète dont elle a pris connaissance par le passé (par la confiance, par exemple). La partie prouve son identité revendiquée en démontrant qu'elle connaît la clé secrète (en répondant à un défi soumis par l'autre partie, l'interrogateur, par exemple). L'interrogateur connaît ce secret (également appris par le passé par la confiance) et est en mesure de calculer la réponse au défi en réalisant les mêmes opérations cryptographiques que le démonstrateur. L'interrogateur peut alors comparer la réponse du démonstrateur à son propre calcul. Si elles correspondent, l'interrogateur est sûr que le démonstrateur est bien celui qu'il dit être, et le processus peut continuer dans l'autre sens, en inversant les rôles, afin d'assurer une authentification mutuelle. Ce mécanisme n'est sûr que si le secret partagé est uniquement connu du démonstrateur et de l'interrogateur et si le secret est diversifié par le démonstrateur. Un autre exemple de ce

type de mécanisme est l'utilisation de modes de fonctionnement par code d'authentification de message par chiffrement (CMAC) ou, en variante, par mode Galois/Counter (GCM)/code d'authentification de message Galois (GMAC).

5.16.3 Amélioration d'exigences

(1) Sécurité matérielle pour l'authentification basée sur clé symétrique

Les composants doivent offrir la possibilité de protéger les clés symétriques cruciales à long terme au moyen des mécanismes matériels.

5.16.4 Niveaux de sécurité

Les exigences pour les quatre niveaux de sécurité liés à CR 1.14 sont les suivantes:

- SL-C(IAC,système de commande) 1: Non choisi
- SL-C(IAC,système de commande) 2: CR 1.14
- SL-C(IAC,système de commande) 3: CR 1.14 (1)
- SL-C(IAC,système de commande) 4: CR 1.14 (1)

6 FR 2 – Contrôle d'utilisation

6.1 Objet et descriptions du SL-C(UC)

Renforcer les droits d'accès attribués d'un utilisateur authentifié (être humain, processus logiciel ou appareil) pour exécuter les actions demandées sur le composant et surveiller l'utilisation de ces droits d'accès.

- SL 1 – Limiter l'utilisation de l'IACS en fonction des droits d'accès spécifiés afin d'assurer la protection contre les mauvaises utilisations fortuites ou occasionnelles.
- SL 2 – Limiter l'utilisation de l'IACS en fonction des droits d'accès spécifiés afin d'assurer la protection contre les contournements par des entités utilisant des moyens simples avec peu de ressources, des compétences génériques et peu de motivation.
- SL 3 – Limiter l'utilisation de l'IACS en fonction des droits d'accès spécifiés afin d'assurer la protection contre les contournements par des entités utilisant des moyens sophistiqués avec des ressources modérées, des compétences spécifiques à l'IACS et une motivation modérée.
- SL 4 – Limiter l'utilisation de l'IACS en fonction des droits d'accès spécifiés afin d'assurer la protection contre les contournements par des entités utilisant des moyens sophistiqués avec des ressources étendues, des compétences spécifiques à l'IACS et une motivation élevée.

6.2 Justification

Une fois l'utilisateur identifié et authentifié, il convient que le composant limite les actions admises à l'utilisation autorisée du composant. Les propriétaires d'actif et les intégrateurs systèmes doivent attribuer à chaque utilisateur (être humain, processus logiciel ou appareil), groupe, rôle, etc. (voir 4.5), les droits d'accès définissant l'utilisation autorisée du composant. Le contrôle d'utilisation a pour objet d'assurer la protection contre les actions non autorisées sur les ressources du composant en vérifiant que les droits d'accès nécessaires ont été accordés avant de permettre à l'utilisateur d'exécuter des actions. Les actions sont, par exemple, la lecture ou l'écriture de données, le téléchargement de programmes et la définition des configurations. Il convient que les recommandations et lignes directrices contiennent les mécanismes qui fonctionneront en mode mixte. Par exemple, certaines ressources de composant exigent une forte protection par contrôle d'utilisation (des droits d'accès restrictifs, par exemple), alors que d'autres pas. Par extension, il convient d'étendre les exigences en matière de contrôle d'utilisation aux données au repos. Les droits d'accès utilisateur peuvent varier en fonction de l'heure/de la date, de l'emplacement et des moyens d'accès.

6.3 CR 2.1 – Mise en œuvre d'autorisation

6.3.1 Exigences

Les composants doivent offrir un mécanisme de mise en œuvre d'autorisation pour tous les utilisateurs identifiés et authentifiés en fonction des responsabilités attribuées.

6.3.2 Justification et recommandations complémentaires

Des politiques de contrôle d'utilisation (par exemple, des politiques basées sur l'identité, les rôles et les réglementations) et les mécanismes associés de mise en œuvre de l'accès en lecture/écriture (par exemple, listes de contrôle d'accès, matrices de contrôle d'accès et cryptographie) sont employées pour contrôler l'utilisation entre les utilisateurs (êtres humains, processus logiciels et appareils) et les actifs (par exemple, appareils, fichiers, enregistrements, processus logiciels, programmes et domaines).

Dès lors que le système de commande a vérifié l'identité d'un utilisateur (être humain, processus logiciel ou appareil) (voir 5.3 et 5.4), il doit également vérifier qu'une opération demandée est vraiment admise conformément aux politiques et procédures de sécurité définies. Par exemple, dans une politique de contrôle d'accès basée sur les rôles, le système de commande vérifie les rôles attribués à un utilisateur ou actif vérifié et les droits d'accès attribués à ces rôles. Si l'opération demandée est couverte par ces droits d'accès, elle est exécutée. Dans le cas contraire, elle est rejetée. Ceci permet la mise en œuvre d'une séparation des devoirs et des droits d'accès minimaux. Il convient de veiller à ce que les mécanismes de mise en œuvre des politiques d'utilisation ne compromettent pas les performances opérationnelles du système de commande.

Les modifications prévues ou non prévues apportées aux composants du système de commande peuvent avoir des effets significatifs sur la sécurité globale du système de commande. En conséquence, il convient que seuls des individus qualifiés et autorisés soient en mesure d'utiliser les composants du système de commande afin d'apporter des modifications, y compris des mises à niveau et des modifications.

6.3.3 Amélioration d'exigences

(1) Mise en œuvre d'autorisation pour tous les utilisateurs (êtres humains, processus logiciels et appareils)

Les composants doivent offrir un mécanisme de mise en œuvre d'autorisation pour tous les utilisateurs en fonction des responsabilités et droits d'accès minimaux attribués.

(2) Mapping des droits d'accès aux rôles

Les composants doivent, directement ou par un mécanisme de sécurité compensatoire, prévoir un rôle autorisé pour définir et modifier le mapping des droits d'accès aux rôles pour tous les utilisateurs humains.

Il convient de ne pas limiter les rôles à des hiérarchies imbriquées fixes, dans lesquelles un rôle de niveau supérieur est un surensemble d'un rôle disposant de droits d'accès moindres. Par exemple, il convient qu'un administrateur système n'englobe pas nécessairement les droits d'accès de l'opérateur.

NOTE 1 Cette RE est également applicable aux processus logiciels et aux appareils.

(3) Permission du superviseur

Les composants doivent prendre en charge la permission manuelle du superviseur pour une durée ou séquence d'événements configurable.

NOTE 2 En ayant recours à la mise en œuvre d'une permission contrôlée, auditée et manuelle d'annulation des mécanismes automatisés en cas d'urgence ou d'événement grave, le superviseur permet à un opérateur de réagir rapidement à des conditions inhabituelles sans fermer la session en cours et établir une nouvelle session en tant qu'utilisateur humain présentant des droits d'accès plus élevés.

(4) Double approbation

Les composants doivent prendre en charge la double approbation lorsqu'une action peut avoir un impact sérieux sur le processus industriel.

Il convient de limiter la double approbation aux actions qui exigent un niveau de confiance très élevé pour être exécutées correctement et en toute fiabilité. Le fait d'exiger une double approbation permet de mettre l'accent sur la gravité des conséquences de l'échec d'une action correcte. Un exemple de situation dans laquelle une double approbation est exigée serait le changement de point de consigne d'un processus industriel crucial. Il convient de ne pas utiliser les mécanismes de double approbation si une réponse immédiate est nécessaire pour protéger la santé, la sécurité et l'environnement (HSE), comme l'arrêt d'urgence d'un processus industriel, par exemple.

6.3.4 Niveaux de sécurité

Les exigences pour les quatre niveaux de sécurité liés à CR 2.1 sont les suivantes:

- SL-C(UC,composant) 1: CR 2.1
- SL-C(UC,composant) 2: CR 2.1 (1) (2)
- SL-C(UC,composant) 3: CR 2.1 (1) (2) (3)
- SL-C(UC,composant) 4: CR 2.1 (1) (2) (3) (4)

6.4 CR 2.2 – Contrôle d'utilisation sans fil

6.4.1 Exigences

Si un composant prend en charge l'utilisation par l'intermédiaire d'interfaces sans fil, il doit offrir la possibilité de s’intégrer dans le système qui prend en charge l’autorisation, la surveillance et les restrictions relatives à l'utilisation conformément aux pratiques industrielles acceptées d'un commun accord.

6.4.2 Justification et recommandations complémentaires

Le contrôle d'utilisation sans fil peut être mis en œuvre dans différents appareils qui composent le système. Les appareils de réseaux peuvent être des appareils qui aident au contrôle d'utilisation par l'intermédiaire, par exemple, du contrôle d'admission au réseau. Pour les appareils et applications qui utilisent les réseaux sans fil, il convient que ces appareils soient en mesure d'utiliser correctement la protection de réseau sans fil (contrôle d'admission au réseau, par exemple). Les composants peuvent également mettre en œuvre différentes limitations d'accès selon que l'accès a lieu depuis des appareils sans fil ou des appareils câblés. Il est alors nécessaire que le composant soit en mesure de déterminer si l'interface est câblée ou pas. Certains appareils de réseaux offrent la possibilité d'analyser l'activité des réseaux sans fil non autorisés dans le spectre sans fil. Pour éviter un impact négatif sur les performances de la fonctionnalité du système de commande, il est judicieux de déployer des appareils dédiés au contrôle des activités non autorisées du réseau.

6.4.3 Amélioration d'exigences

Aucune

6.4.4 Niveaux de sécurité

Les exigences pour les quatre niveaux de sécurité SL liés à CR 2.2 sont les suivantes:

- SL-C(UC, composant) 1: CR 2.2
- SL-C(UC, composant) 2: CR 2.2
- SL-C(UC, composant) 3: CR 2.2
- SL-C(UC, composant) 4: CR 2.2

6.5 CR 2.3 – Contrôle d'utilisation pour les appareils portables et mobiles

Aucune exigence de niveau de composant n'est associée à l'IEC 62443-3 CR 2.3.

6.6 CR 2.4 – Code mobile

Les exigences relatives au contrôle d'utilisation pour le code mobile sont spécifiques au composant et peuvent être considérées comme des exigences pour chaque type de composant spécifique de l'Article 12 à l'Article 15.

6.7 CR 2.5 – Verrouillage de session

6.7.1 Exigences

Si un composant fournit une interface d'utilisateur humain, qu'elle soit accessible en local ou par l'intermédiaire d'un réseau, le composant doit offrir la possibilité

a) de la protéger contre l'accès par un verrouillage de session après une période de temps configurable d'inactivité ou dans le cadre d'une procédure manuelle par l'utilisateur (être humain, processus logiciel ou appareil); et

b) de maintenir le verrouillage de session tant que l'utilisateur humain qui détient la session ou qu'un autre utilisateur humain autorisé n'a pas rétabli l'accès à l'aide des procédures appropriées d'identification et d'authentification.

6.7.2 Justification et recommandations complémentaires

Les verrouillages de session sont utilisés pour empêcher l'accès aux postes de travail ou nœuds spécifiés. Il convient que les composants activent automatiquement les mécanismes de verrouillage de session après une période de temps configurable. Dans la plupart des cas, les verrouillages de session sont configurés au niveau du système. Les verrouillages de session mis en œuvre dans le cadre de cette exigence peuvent être préemptés ou limités par une fermeture de session à distance, tel que défini au 6.8.

6.7.3 Amélioration d'exigences

Aucune

6.7.4 Niveaux de sécurité

Les exigences pour les quatre niveaux de sécurité SL liés à CR 2.5 sont les suivantes:

- SL-C(UC, composant) 1: CR 2.5
- SL-C(UC, composant) 2: CR 2.5
- SL-C(UC, composant) 3: CR 2.5
- SL-C(UC, composant) 4: CR 2.5

6.8 CR 2.6 – Fermeture de la session à distance

6.8.1 Exigences

Si un composant prend en charge les sessions à distance, il doit offrir la possibilité de les fermer de façon automatique après une période d'inactivité configurable, de façon manuelle par une autorité locale ou de façon manuelle par l'utilisateur (être humain, processus logiciel ou appareil) qui a lancé la session.

6.8.2 Justification et recommandations complémentaires

Une session à distance est lancée à chaque accès à un composant dans la limite d'une zone définie par le propriétaire d'actif en fonction de son appréciation du risque. Cette exigence peut être limitée aux sessions utilisées pour la surveillance du composant et pour les activités

de maintenance (pas les opérations cruciales) en fonction de l'appréciation du risque du système de commande et des politiques et procédures de sécurité. Certains composants peuvent ne pas permettre de fermer des sessions si elles font partie intégrante d'une fonction essentielle du composant.

6.8.3 Amélioration d'exigences

Aucune

6.8.4 Niveaux de sécurité

Les exigences pour les quatre niveaux de sécurité SL liés à CR 2.6 sont les suivantes:

- SL-C(UC, composant) 1: Non choisi
- SL-C(UC, composant) 2: CR 2.6
- SL-C(UC, composant) 3: CR 2.6
- SL-C(UC, composant) 4: CR 2.6

6.9 CR 2.7 – Contrôle de sessions simultanées

6.9.1 Exigences

Les composants doivent offrir la possibilité de limiter le nombre de sessions simultanées par interface pour un utilisateur donné (être humain, processus logiciel ou appareil).

6.9.2 Justification et recommandations complémentaires

Un refus de service par insuffisance de ressources peut se produire si une limite n'est pas imposée. Il existe un compromis entre l'éventuel verrouillage d'un utilisateur spécifique et le verrouillage de tous les utilisateurs et services par suite d’un manque de ressources. Les recommandations du fournisseur de produit et/ou de l'intégrateur système sont susceptibles d'être exigées pour fournir les informations suffisantes quant au nombre de sessions simultanées qu'il convient d'attribuer.

6.9.3 Amélioration d'exigences

Aucune

6.9.4 Niveaux de sécurité

Les exigences pour les quatre niveaux de sécurité SL liés à CR 2.7 sont les suivantes:

- SL-C(UC, composant) 1: Non choisi
- SL-C(UC, composant) 2: Non choisi
- SL-C(UC, composant) 3: CR 2.7
- SL-C(UC, composant) 4: CR 2.7

6.10 CR 2.8 – Événements auditables

6.10.1 Exigences

Les composants doivent offrir la possibilité de générer des enregistrements d'audit pertinents pour la sécurité des catégories suivantes:

contrôle d'accès;

erreurs de demande;

événements du système de commande;

événement de sauvegarde et de restauration;

modifications de configuration; et

événements de journalisation.

Les enregistrements d'audit individuels doivent inclure:

a) l'horodatage;
b) la source (appareil d'origine, processus logiciel ou compte d'utilisateur humain);
c) la catégorie;
d) le type;
e) l'ID d'événement; et
f) le résultat d'événement.

6.10.2 Justification et recommandations complémentaires

Les appareils peuvent contenir un micrologiciel intégré ou exécuter un système d'exploitation. L'exigence ayant pour objet de couvrir les catégories d'événements, au moins tous les événements issus des catégories ci-dessus qui peuvent être générés par le micrologiciel ou le système d'exploitation doivent être inclus.

NOTE Les catégories d'événements liés à la sécurité sont uniquement applicables si la fonctionnalité elle-même est fournie par le composant.

6.10.3 Amélioration d'exigences

Aucune

6.10.4 Niveaux de sécurité

Les exigences pour les quatre niveaux de sécurité liés à CR 2.8 sont les suivantes:

- SL-C(UC,composant) 1: CR 2.8
- SL-C(UC,composant) 2: CR 2.8
- SL-C(UC,composant) 3: CR 2.8
- SL-C(UC,composant) 4: CR 2.8

6.11 CR 2.9 – Capacité de stockage des données d'audit

6.11.1 Exigences

Les composants doivent

a) offrir la possibilité d'allouer une capacité de stockage des enregistrements d'audit conformément aux recommandations communément reconnues en matière de gestion des journaux; et
b) prévoir des mécanismes visant à assurer une protection contre la défaillance du composant lorsque celui-ci atteint ou dépasse la capacité de stockage des données d'audit.

6.11.2 Justification et recommandations complémentaires

Il convient que les composants offrent une capacité de stockage des données d'audit suffisante et tiennent compte de la politique de rétention, de l'audit à réaliser et des exigences de traitement en ligne des audits. Les composants peuvent s'appuyer sur le système dans lequel ils sont intégrés pour fournir la majorité de la capacité de stockage des données d'audit. Toutefois, il convient que les composants offrent un stockage local suffisant pour mettre les données d'audit en mémoire tampon jusqu'à ce qu'elles puissent être envoyées au système.

Les lignes directrices à prendre en compte peuvent inclure le document NIST Special Publication (SP) 800-92 [19]. Il convient que la capacité de stockage des données d'audit soit suffisante pour conserver les journaux pendant la durée exigée par les politiques et règlements applicables ou par les exigences professionnelles.

6.11.3 Amélioration d'exigences

(1) Avertir lorsque le seuil de capacité de stockage des données d'audit est atteint

Les composants doivent offrir la possibilité d'émettre une mise en garde lorsque la capacité de stockage attribuée des enregistrements d'audit atteint un seuil configurable.

6.11.4 Niveaux de sécurité

Les exigences pour les quatre niveaux de sécurité SL liés à CR 2.9 sont les suivantes:

- SL-C(UC,composant) 1: CR 2.9
- SL-C(UC,composant) 2: CR 2.9
- SL-C(UC,composant) 3: CR 2.9 (1)
- SL-C(UC,composant) 4: CR 2.9 (1)

6.12 CR 2.10 – Réponse aux défaillances de traitement des audits

6.12.1 Exigences

Les composants doivent

a) offrir la possibilité d'assurer une protection contre la perte des services et fonctions essentiels en cas de défaillance de traitement des audits; et

b) offrir la possibilité de prendre en charge les actions appropriées en réponse à une défaillance de traitement des audits selon les pratiques et recommandations acceptées d'un commun accord par le secteur industriel.

6.12.2 Justification et recommandations complémentaires

La génération d'un audit a souvent lieu à la source de l'événement. Le traitement des audits implique la transmission, la possible augmentation (ajout d'un horodatage, par exemple) et le stockage permanent des enregistrements d'audit. Les défaillances de traitement des audits incluent, par exemple, les erreurs logicielles ou matérielles, les défaillances dans les mécanismes de capture des données d'audit et la capacité de stockage des données d'audit atteinte ou dépassée. Les lignes directrices à prendre en compte lors de la conception des actions appropriées peuvent inclure le NIST SP 800-92, Guide to Computer Security Log Management [19]. Il convient de noter qu'en réponse à un éventuel dépassement de la capacité de stockage des données d'audit, les enregistrements d'audit les plus anciens peuvent être écrasés ou la génération des journaux d'audit interrompue, cela impliquant toutefois la perte d'éventuelles informations essentielles. De même, il peut être approprié d'alerter le personnel en réponse à une défaillance de traitement des audits.

6.12.3 Amélioration d'exigences

Aucune

6.12.4 Niveaux de sécurité

Les exigences pour les quatre niveaux de sécurité SL liés à CR 2.10 sont les suivantes:

- SL-C(UC,composant) 1: CR 2.10
- SL-C(UC,composant) 2: CR 2.10
- SL-C(UC,composant) 3: CR 2.10
- SL-C(UC,composant) 4: CR 2.10

6.13 CR 2.11 – Horodatages

6.13.1 Exigences

Les composants doivent offrir la possibilité de créer des horodatages (incluant la date et l'heure) à utiliser dans les enregistrements d'audit.

6.13.2 Justification et recommandations complémentaires

Une bonne référence pour le format des horodatages est celle de l'ISO/IEC 8601:2004 [17].
Lors de la conception d'un système, il convient de veiller à prendre en considération les événements périodiques de décalage temporel tels que l'heure d'été dans certaines régions.

6.13.3 Amélioration d'exigences

(1) Synchronisation temporelle

Les composants doivent offrir la possibilité de créer des horodatages synchronisés avec l'horloge du système.

(2) Protection de l'intégrité de l'horloge

Le mécanisme de synchronisation temporelle doit offrir la possibilité de détecter toute altération non autorisée et de générer un événement d'audit relatif à l'altération.

6.13.4 Niveaux de sécurité

Les exigences pour les quatre niveaux de sécurité liés à CR 2.11 sont les suivantes:

- SL-C(UC,composant) 1: CR 2.11
- SL-C(UC,composant) 2: CR 2.11 (1)
- SL-C(UC,composant) 3: CR 2.11 (1)
- SL-C(UC,composant) 4: CR 2.11 (1) (2)

6.14 CR 2.12 – Non-répudiation

6.14.1 Exigences

Si un composant fournit une interface d'utilisateur humain, il doit offrir la possibilité de déterminer si un utilisateur humain donné a réalisé une action particulière.

Les éléments de contrôle qui ne sont pas en mesure de prendre en charge ce type de capacité doivent figurer dans les documents du composant.

6.14.2 Justification et recommandations complémentaires

L'exécution des actions de l'opérateur, la modification des configurations du système de commande, la création d'informations, l'envoi d'un message, l'approbation d'informations (l'indication de concurrence, par exemple) et la réception d'un message sont des exemples d'actions particulières réalisées par un utilisateur. La non-répudiation protège contre les fausses déclarations ultérieures formulées par un utilisateur qui déclare ne pas avoir réalisé une action spécifique, par un auteur qui déclare ne pas être l'auteur d'un document particulier, par un émetteur qui déclare ne pas avoir transmis de message, par un destinataire qui déclare ne pas avoir reçu de message ou par un signataire qui déclare ne pas avoir signé de document. Les services de non-répudiation peuvent être utilisés pour déterminer si les informations proviennent d'un utilisateur, si un utilisateur a réalisé des actions spécifiques (envoi d'un message électronique et approbation d'un ordre de travail, par exemple) ou s'il a reçu des informations particulières. Les services de non-répudiation sont obtenus en utilisant différentes techniques ou différents mécanismes (identification et authentification de l'utilisateur, signatures numériques, réceptions et horodatages de message numérique, par exemple).

6.14.3 Amélioration d'exigences

(1) Non-répudiation pour tous les utilisateurs

Les composants doivent offrir la possibilité de déterminer si un utilisateur donné (être humain, processus logiciel ou appareil) a réalisé une action particulière.

6.14.4 Niveaux de sécurité

Les exigences pour les quatre niveaux de sécurité SL liés à CR 2.12 sont les suivantes:

- SL-C(UC,composant) 1: CR 2.12
- SL-C(UC,composant) 2: CR 2.12
- SL-C(UC,composant) 3: CR 2.12
- SL-C(UC,composant) 4: CR 2.12 (1)

6.15 CR 2.13 – Utilisation d'interfaces physiques de diagnostic et d'essai

Les exigences relatives à l'utilisation d'interfaces physiques de diagnostic et d'essai sont spécifiques au composant et peuvent être considérées comme des exigences pour chaque type de composant spécifique de l'Article 12 à l'Article 15.

7 FR 3 – Intégrité du système

7.1 Objet et descriptions du SL-C(SI)

Assurer l'intégrité du composant pour assurer une protection contre toute manipulation ou modification non autorisée.

- SL 1 – Protéger l'intégrité de l'IACS face aux manipulations fortuites ou occasionnelles.
- SL 2 – Protéger l'intégrité de l'IACS contre toute manipulation par des personnes utilisant des moyens simples avec peu de ressources, des compétences génériques et peu de motivation.
- SL 3 – Protéger l'intégrité de l'IACS contre toute manipulation par des personnes utilisant des moyens sophistiqués avec des ressources modérées, des compétences spécifiques à l'IACS et une motivation modérée.
- SL 4 – Protéger l'intégrité de l'IACS contre toute manipulation par des personnes utilisant des moyens sophistiqués avec des ressources étendues, des compétences spécifiques à l'IACS et une motivation élevée.

7.2 Justification

Les composants font souvent l'objet de plusieurs cycles d'essai (essai de l'unité, essai du système, etc.) afin d'établir qu'ils fonctionnent comme prévu avant même d'être produits. Une fois le composant opérationnel, les propriétaires d'actif sont chargés d'assurer son intégrité. En s'appuyant sur leur méthodologie d'appréciation du risque, les propriétaires d'actif peuvent attribuer différents niveaux de protection de l'intégrité à différents composants, canaux de communication et informations dans leur IACS. Il convient d'assurer l'intégrité des actifs physiques tant à l'état de fonctionnement qu'à l'état non opérationnel (pendant la production, le stockage ou un arrêt pour maintenance, par exemple). Il convient d'assurer l'intégrité des actifs logiques en transit et au repos (lors de la transmission sur un réseau ou lorsqu'ils se trouvent dans un référentiel de données, par exemple).

7.3 CR 3.1 – Intégrité de la communication

7.3.1 Exigences

Les composants doivent offrir la possibilité de protéger l'intégrité des informations transmises.

7.3.2 Justification et recommandations complémentaires

La plupart des attaques de réseau courantes reposent sur la manipulation des données en cours de transmission (la manipulation des paquets réseau, par exemple). Les réseaux commutés ou routés offrent une plus grande opportunité aux attaquants de manipuler les paquets, l'accès non détecté à ces réseaux étant en général plus facile et les mécanismes de commutation et de routage eux-mêmes pouvant également être manipulés afin d'obtenir un meilleur accès aux informations transmises. Dans le contexte d'un système de commande, la manipulation peut inclure la modification des valeurs de mesure communiquées par un capteur à un récepteur ou l'altération des paramètres de commande envoyés d'une application de commande à un actionneur.

En fonction du contexte (transmission au sein d'un segment de réseau local par rapport à la transmission par l'intermédiaire de réseaux non sécurisés, par exemple) et du type de réseau utilisé dans la transmission (TCP/IP par rapport aux liaisons série locales, par exemple), les mécanismes plausibles et appropriés varient. Sur un petit réseau comportant des liens directs (point à point), la protection physique des accès à tous les nœuds peut être suffisante à des niveaux de sécurité inférieurs si l'intégrité des points d'extrémité est également protégée (voir 7.6), alors que sur un réseau réparti dans des zones dans lesquelles le personnel est souvent physiquement présent ou sur un réseau étendu, l'accès physique est susceptible de ne pas être réalisable. Si un service commercial est utilisé pour assurer des services de communication comme un élément d'article plutôt qu'un service totalement dédié (une ligne louée plutôt qu'une liaison T1, par exemple), il peut s'avérer plus difficile d'obtenir les assurances nécessaires concernant la mise en œuvre des contrôles de sécurité pour l'intégrité des communications (en raison des restrictions juridiques, par exemple). S'il s'avère impossible ou peu pratique de satisfaire aux exigences de sécurité nécessaires, il peut être judicieux de mettre en œuvre des contre-mesures compensatoires appropriées ou d'accepter le risque supplémentaire de manière explicite.

Les équipements industriels sont souvent soumis aux conditions environnementales, ce qui peut poser des problèmes d'intégrité et/ou provoquer des faux positifs. La plupart du temps, l'environnement contient des particules, des liquides, des vibrations, des gaz, des rayonnements et des interférences électromagnétiques (IEM) qui peuvent générer des conditions ayant un impact sur l'intégrité des câbles et signaux de communication. Il convient que l'infrastructure de réseau soit conçue de manière à réduire le plus possible ces effets physiques/environnementaux sur l'intégrité de la communication. Par exemple, en présence de particules, de liquides et/ou de gaz, il peut s'avérer nécessaire d'équiper le câble d'un connecteur RJ-45 (Registered Jack 45) ou M12 étanche à la place d'un connecteur RJ-45 de qualité commerciale. Le câble lui-même peut être équipé d'une gaine différente pour se protéger également des particules, des liquides et/ou des gaz. En présence de vibrations, des connecteurs M12 peuvent être nécessaires pour éviter que les goupilles creuses d'un connecteur RJ-45 ne se déconnectent pendant l'utilisation. En présence de rayonnements et/ou d'interférences électromagnétiques, il peut s'avérer nécessaire d'utiliser des câbles torsadés ou à fibre optique blindés pour protéger les signaux de communication. Il peut également être nécessaire de procéder à une analyse du spectre sans fil dans ces zones si une mise en réseau sans fil est prévue pour vérifier qu'il s'agit d'une solution viable.

7.3.3 Amélioration d'exigences

(1) Authentification de la communication

Les composants doivent offrir la possibilité de vérifier l’authenticité des informations reçues pendant la communication.

NOTE La protection de l’intégrité et l’authentification de l’origine peuvent être effectuées sans protection de la confidentialité.

7.3.4 Niveaux de sécurité

Les exigences pour les quatre niveaux de sécurité SL liés à CR 3.1 sont les suivantes:

- SL-C(SI, composant) 1: CR 3.1

- SL-C(SI, composant) 2: CR 3.1 (1)
- SL-C(SI, composant) 3: CR 3.1 (1)
- SL-C(SI, composant) 4: CR 3.1 (1)

7.4 CR 3.2 – Protection contre les programmes malveillants

Les exigences relatives à la protection contre les programmes malveillants sont spécifiques au composant et peuvent être considérées comme des exigences pour chaque type de composant spécifique de l'Article 12 à l'Article 15.

7.5 CR 3.3 – Vérification de la fonctionnalité de sécurité

7.5.1 Exigences

Les composants doivent offrir la possibilité de prendre en charge la vérification du fonctionnement prévu des fonctions de sécurité selon l' IEC 62443-3-3 SR3.3.

7.5.2 Justification et recommandations complémentaires

Il convient que le fournisseur du produit et/ou l'intégrateur système donnent les recommandations relatives aux essais des contrôles de sécurité prévus. Il est indispensable que les propriétaires d'actif soient bien conscients des éventuelles répercussions liées à l'exécution de ces essais de vérification pendant le fonctionnement normal. Il est nécessaire de spécifier les détails de l'exécution de ces vérifications en portant une attention particulière aux exigences en matière de fonctionnement continu (planification ou notification préalable, par exemple).

Exemples de fonctions de vérification de la sécurité:

- Vérification des contre-mesures antivirus par des essais du système de fichiers du système de commande réalisés par l'European Institute for Computer Antivirus Research (EICAR). Il convient que le logiciel antivirus détecte les échantillons d’essai de l’EICAR et que des procédures appropriées de traitement des incidents soient déclenchées.
- Vérification des contre-mesures de contrôle de l'identification, de l'authentification et de l'utilisation en procédant à une tentative d'accès avec un compte non autorisé (cette procédure peut être automatisée pour certaines fonctionnalités).
- Vérification des systèmes de détection d'intrusion (IDS) comme contrôle de sécurité, en intégrant une règle dans l'IDS qui se déclenche en cas de trafic anormal, mais réputé non malveillant. L'essai peut alors être réalisé en introduisant un trafic qui déclenche cette règle et les procédures appropriées de surveillance IDS et de traitement des incidents.
- Confirmation que la journalisation d'audit est assurée comme cela est exigé dans le cadre des politiques et procédures de sécurité, et qu'elle n'a pas été désactivée par une entité interne ou externe.

7.5.3 Amélioration d'exigences

(1) Vérification de la fonctionnalité de sécurité pendant le fonctionnement normal

Les composants doivent offrir la possibilité de prendre en charge la vérification du fonctionnement prévu des fonctions de sécurité pendant les opérations normales.

Il est nécessaire de soigneusement mettre en œuvre cette RE pour éviter les effets néfastes. Elle peut ne pas être pertinente pour les systèmes de sécurité.

7.5.4 Niveaux de sécurité

Les exigences pour les quatre niveaux de sécurité SL liés à CR 3.3 sont les suivantes:

- SL-C(SI, composant) 1: CR 3.3

- SL-C(SI, composant) 2: CR 3.3
- SL-C(SI, composant) 3: CR 3.3
- SL-C(SI, composant) 4: CR 3.3 (1)

7.6 CR 3.4 – Intégrité des logiciels et des informations

7.6.1 Exigences

Les composants doivent offrir la possibilité de réaliser ou de prendre en charge les contrôles d'intégrité des logiciels, de la configuration et des autres informations, et d'enregistrer et consigner les résultats de ces contrôles ou d'être intégrés dans un système qui peut se charger de ces contrôles.

7.6.2 Justification et recommandations complémentaires

Les méthodes de vérification de l'intégrité permettent de détecter, d'enregistrer, de consigner et d'assurer la protection contre la manipulation frauduleuse des logiciels ou des informations, ce qui peut se produire si les autres mécanismes de protection (la mise en œuvre d'autorisation, par exemple) ont été contournés. Il convient que les composants utilisent des mécanismes d'intégrité formels ou recommandés (les empreintes numériques, par exemple). Par exemple, ces mécanismes pourraient être utilisés pour surveiller les dernières informations de configuration des appareils de terrain afin de détecter les brèches de sécurité (y compris les changements non autorisés).

7.6.3 Amélioration d'exigences

(1) Authenticité des logiciels et des informations

Les composants doivent offrir la possibilité de réaliser ou de prendre en charge les contrôles d'authenticité des logiciels, de la configuration et des autres informations, et d'enregistrer et consigner les résultats de ces contrôles ou d'être intégrés dans un système qui peut se charger de ces contrôles.

(2) Notification automatisée des violations d'intégrité

Si le composant procède à un contrôle d'intégrité, il doit être en mesure d'informer automatiquement une entité configurable de la détection d'une tentative de modification non autorisée.

7.6.4 Niveaux de sécurité

Les exigences pour les quatre niveaux de sécurité SL liés à CR 3.4 sont les suivantes:

- SL-C(SI, composant) 1: CR 3.4
- SL-C(SI, composant) 2: CR 3.4 (1)
- SL-C(SI, composant) 3: CR 3.4 (1) (2)
- SL-C(SI, composant) 4: CR 3.4 (1) (2)

7.7 CR 3.5 – Validation d'entrée

7.7.1 Exigences

Les composants doivent valider la syntaxe, la longueur et le contenu des données d’entrée utilisées pour le contrôle de processus industriel ou d'une entrée par l'intermédiaire d'interfaces externes ayant un impact direct sur l'action du composant.

7.7.2 Justification et recommandations complémentaires

Il convient de mettre en place des règles de contrôle de la validité de la syntaxe de ces données d'entrée (des points d'extrémité, par exemple) pour vérifier que ces informations n'ont pas été manipulées de manière frauduleuse et qu'elles sont conformes à la spécification. Il convient que les entrées transmises à des interpréteurs soient préalablement examinées

afin d'éviter que le contenu ne soit par mégarde interprété comme des commandes. Il est à noter qu'il s'agit d'une CR de sécurité et qu'à ce titre, elle ne concerne pas les erreurs humaines (fourniture d'un nombre entier légitime hors de la plage prévue, par exemple).

En règle générale, les pratiques acceptées dans l'industrie en matière de validation des données d'entrée incluent les valeurs aberrantes pour un type de champ défini, les caractères non valides dans les champs de données, les données manquantes ou incomplètes et le débordement de la mémoire tampon. Les attaques par injection SQL, les attaques de type "cross-site scripting" (injection de code indirecte), les paquets mal formés (souvent issus de de générateurs de protocole) sont d'autres exemples dans lesquels des entrées non valides compromettent la sécurité du système. Il convient que les lignes directrices à prendre en considération incluent, par exemple, l'Open Web Application Security Project (OWASP) Code Review Guide [21].

7.7.3 Amélioration d'exigences

Aucune

7.7.4 Niveaux de sécurité

Les exigences pour les quatre niveaux de sécurité SL liés à CR 3.5 sont les suivantes:

- SL-C(SI, composant) 1: CR 3.5
- SL-C(SI, composant) 2: CR 3.5
- SL-C(SI, composant) 3: CR 3.5
- SL-C(SI, composant) 4: CR 3.5

7.8 CR 3.6 – Sortie déterministe

7.8.1 Exigences

Les composants qui se connectent de manière physique ou logique à un processus d’automatisation doivent offrir la possibilité de définir des sorties à un état prédéterminé si le fonctionnement normal tel que défini par le fournisseur de composants ne peut pas être maintenu.

7.8.2 Justification et recommandations complémentaires

Le comportement déterministe des sorties du système de commande par suite d’actions malveillantes contre les appareils et logiciels du système de commande est une caractéristique importante permettant d'assurer l'intégrité des opérations normales. Dans l'idéal, l’appareil continue de fonctionner normalement malgré l'attaque, mais si le système de commande ne peut pas maintenir le fonctionnement normal, ses sorties nécessitent de passer à un état prédéterminé. L'état prédéterminé approprié des sorties du système de commande dépend de l’appareil et peut être l'une des options suivantes, configurables par l'utilisateur:

- Hors tension – les sorties passent à l'état hors tension;
- Maintien – les sorties passent à la dernière valeur correcte connue; ou
- Fixe – les sorties passent à une valeur fixe déterminée par le propriétaire d'actif ou une application; ou
- Dynamique – les sorties passent à l'une des options ci-dessus en fonction de l'état en cours.

7.8.3 Amélioration d'exigences

Aucune

7.8.4 Niveaux de sécurité

Les exigences pour les quatre niveaux de sécurité SL liés à CR 3.6 sont les suivantes:

- SL-C(SI, composant) 1: CR 3.6
- SL-C(SI, composant) 2: CR 3.6
- SL-C(SI, composant) 3: CR 3.6
- SL-C(SI, composant) 4: CR 3.6

7.9 CR 3.7 – Traitement des erreurs

7.9.1 Exigences

Les composants doivent identifier et traiter les conditions d'erreur de telle sorte que les adversaires ne puissent exploiter aucune information pour attaquer l'IACS.

7.9.2 Justification et recommandations complémentaires

Il convient que le fournisseur de produit et/ou l'intégrateur système examinent attentivement la structure et le contenu des messages d'erreur. Il convient que les messages d'erreur générés par le composant donnent des informations pertinentes et utiles sans révéler d'informations potentiellement préjudiciables qui pourraient être utilisées par des adversaires pour exploiter l'IACS. Il convient que la divulgation de ces informations soit justifiée par la nécessité de résolution opportune des conditions d'erreur. Les lignes directrices à prendre en considération peuvent inclure des lignes directrices bien connues (OWASP Code Review Guide, par exemple).

Un bon exemple de message d'erreur qui pourrait aider les adversaires à attaquer l'IACS consisterait à divulguer les raisons pour lesquelles l'authentification auprès du système n'a pas abouti. Par exemple, le fait d'indiquer un utilisateur ou mot de passe non valide dans le message de retour aiderait un adversaire à attaquer l'IACS. Il convient donc de ne pas le faire.

7.9.3 Amélioration d'exigences

Aucune

7.9.4 Niveaux de sécurité

Les exigences pour les quatre niveaux de sécurité SL liés à CR 3.7 sont les suivantes:

- SL-C(SI, composant) 1: CR 3.7
- SL-C(SI, composant) 2: CR 3.7
- SL-C(SI, composant) 3: CR 3.7
- SL-C(SI, composant) 4: CR 3.7

7.10 CR 3.8 – Intégrité de la session

7.10.1 Exigences

Les composants doivent fournir les mécanismes de protection de l'intégrité des sessions de communication, y compris:

a) la possibilité d'invalider les identificateurs de session après la déconnexion de l'utilisateur ou toute autre fermeture de session (y compris les sessions de navigation);
b) la possibilité de générer un identificateur unique pour chaque session et de reconnaître uniquement les identificateurs de session générés par le système; et
c) la possibilité de générer des identificateurs de session uniques avec des sources de randomisation communément acceptées.

7.10.2 Justification et recommandations complémentaires

Ce contrôle porte sur la protection des communications au niveau de la session, par opposition à la protection au niveau du paquet. Ce contrôle vise à poser les bases d'une confiance, à chaque extrémité d'une session de communication, en l'identité de l'autre partie et en la validité des informations transmises. Par exemple, ce contrôle porte sur les attaques de l'intercepteur, y compris le détournement de session, l'insertion de fausses informations dans une session ou les attaques par rejeu. L'utilisation des mécanismes d'intégrité de session peut impliquer d'importantes surcharges d'informations. Il convient donc de la prendre en considération à la lumière des exigences en matière de communication en temps réel.

Le détournement de session et autres attaques de l'intercepteur ou insertions de fausses informations profitent souvent d'ID de session (clés ou secrets partagés) faciles à deviner ou de l'utilisation d'ID qui n'ont pas été correctement invalidés après la fermeture de session. Par conséquent, il convient que la validité d'un authentifiant de session soit étroitement liée à la durée de vie de la session. L'utilisation de la randomisation pour générer des ID de session uniques facilite la protection contre les attaques en force pour déterminer les ID de session ultérieurs.

7.10.3 Amélioration d'exigences

Aucune

7.10.4 Niveaux de sécurité

Les exigences pour les quatre niveaux de sécurité SL liés à CR 3.8 sont les suivantes:

- SL-C(SI, composant) 1: Non choisi
- SL-C(SI, composant) 2: CR 3.8
- SL-C(SI, composant) 3: CR 3.8
- SL-C(SI, composant) 4: CR 3.8

7.11 CR 3.9 – Protection des informations d'audit

7.11.1 Exigences

Les composants doivent protéger les informations d'audit, les journaux d’audit et les outils d'audit (le cas échéant) contre les accès, modifications et suppressions non autorisés.

7.11.2 Justification et recommandations complémentaires

Les informations d'audit incluent toutes les informations (enregistrements, vérifications et rapports d'audit, par exemple) nécessaires à la réussite des activités de contrôle d'audit. Les informations d'audit sont essentielles à la correction des erreurs, à la reprise après une brèche de sécurité, aux enquêtes et efforts associés. Les mécanismes de protection améliorée contre les modifications et les suppressions incluent le stockage des informations d'audit sur un support inscriptible mis en place par le matériel.

7.11.3 Amélioration d'exigences

(1) Enregistrements d'audit sur support inscriptible

Les composants doivent offrir la possibilité de stocker les enregistrements d'audit sur un support inscriptible mis en place par le matériel.

7.11.4 Niveaux de sécurité

Les exigences pour les quatre niveaux de sécurité SL liés à CR 3.9 sont les suivantes:

- SL-C(SI, composant) 1: Non choisi
- SL-C(SI, composant) 2: CR 3.9

- SL-C(SI, composant) 3: CR 3.9
- SL-C(SI, composant) 4: CR 3.9 (1)

7.12 CR 3.10 – Support pour les mises à jour

Les exigences relatives au support pour les mises à jour sont spécifiques au composant et peuvent être considérées comme des exigences pour chaque type de composant spécifique de l'Article12 à l'Article15.

7.13 CR 3.11 – Résistance aux violations physiques et détection

Les exigences relatives à la résistance aux violations physiques et à leur détection sont spécifiques au composant et peuvent être considérées comme des exigences pour chaque type d’appareils spécifique de l'Article12 à l'Article15.

7.14 CR 3.12 – Fourniture des racines de confiance du fournisseur de produit

Les exigences relatives à la fourniture des racines de confiance du fournisseur de produit sont spécifiques au composant et peuvent être considérées comme des exigences pour chaque type de composant spécifique de l'Article12 à l'Article15.

7.15 CR 3.13 – Fourniture des racines de confiance du propriétaire d'actif

Les exigences relatives à la fourniture des racines de confiance du propriétaire d'actif sont spécifiques au composant et peuvent être considérées comme des exigences pour chaque type d’appareils spécifique de l'Article12 à l'Article15.

7.16 CR 3.14 – Intégrité du processus d'amorçage

Les exigences relatives à l'intégrité du processus d'amorçage sont spécifiques au composant et peuvent être considérées comme des exigences pour chaque type d’appareils spécifique de l'Article12 à l'Article15.

8 FR 4 – Confidentialité des données

8.1 Objet et descriptions du SL-C(DC)

Vérifier la confidentialité des informations présentes sur les canaux de communication et dans les données stockées dans des référentiels afin d’assurer une protection contre toute divulgation non autorisée.

- SL 1 – Empêcher la divulgation non autorisée des informations par écoute informatique ou exposition occasionnelle.
- SL 2 – Empêcher la divulgation non autorisée des informations à une entité qui les recherche activement, en utilisant des moyens simples avec peu de ressources, des compétences génériques et peu de motivation.
- SL 3 – Empêcher la divulgation non autorisée des informations à une entité qui les recherche activement, en utilisant des moyens sophistiqués avec des ressources modérées, des compétences spécifiques à l'IACS et une motivation modérée.
- SL 4 – Empêcher la divulgation non autorisée des informations à une entité qui les recherche activement, en utilisant des moyens sophistiqués avec des ressources étendues, des compétences spécifiques à l'IACS et une motivation élevée.

8.2 Justification

Certaines informations générées par le composant, qu'elles soient au repos ou en transit, sont de nature confidentielle ou sensible. Cela implique que certains canaux de

communication et magasins de données exigent d'être protégés contre les écoutes informatiques et les accès non autorisés.

8.3 CR 4.1 – Confidentialité des informations

8.3.1 Exigences

Les composants doivent

a) offrir la possibilité de protéger la confidentialité des informations au repos pour lesquelles une autorisation explicite de lecture est prise en charge; et

b) prendre en charge la protection de la confidentialité des informations en transit conformément à l'IEC 62443-3-3 SR 4.1.

8.3.2 Justification et recommandations complémentaires

Il convient que la décision de protéger ou pas des informations dépende du contexte. Elle ne peut pas être prise au moment de la conception du produit. Toutefois, le fait qu'une organisation limite l'accès aux informations en configurant les autorisations explicites de lecture dans le système de commande indique qu'il convient qu'elle les protège. Ainsi, il convient de considérer comme étant potentiellement sensibles toutes les informations pour lesquelles le composant offre la possibilité d'attribuer des autorisations explicites de lecture. Il convient donc qu'il offre également la possibilité de protéger leur confidentialité.

La confidentialité des informations en transit exige des capacités au niveau du système qu'il convient que le composant soit en mesure de prendre en charge.

Pour la protection de la confidentialité, 8.5 donne des exigences supplémentaires.

8.3.3 Amélioration d'exigences

Aucune

8.3.4 Niveaux de sécurité

Les exigences pour les quatre niveaux de sécurité SL liés à CR 4.1 sont les suivantes:

- SL-C(DC, composant) 1: CR 4.1
- SL-C(DC, composant) 2: CR 4.1
- SL-C(DC, composant) 3: CR 4.1
- SL-C(DC, composant) 4: CR 4.1

8.4 CR 4.2 – Persistance des informations

8.4.1 Exigences

Les composants doivent offrir la possibilité d'effacer des composants libérés du service actif et/ou mis hors service toutes les informations faisant l'objet d'une autorisation explicite de lecture.

8.4.2 Justification et recommandations complémentaires

Il convient que le retrait du service actif d'un composant du système de commande n'offre pas la possibilité de diffusion involontaire d'informations faisant l'objet d'une autorisation explicite de lecture. Il peut s'agir, par exemple, d'informations d’authentification et de configuration de réseau stockées dans une mémoire non volatile ou d'autres informations cryptographiques susceptibles de faciliter les activités non autorisées ou malveillantes.

Il convient de ne pas divulguer sans contrôle à un autre utilisateur ou un autre rôle les informations créées par les actions d'un utilisateur ou d'un rôle (ou celles d'un processus logiciel agissant au nom de l'un d'eux). Le contrôle des informations du système de commande ou la persistance des données évite que les informations stockées sur une ressource partagée ne soient involontairement diffusées après que ladite ressource a été restituée au système de commande.

8.4.3 Amélioration d'exigences

(1) Effacer les ressources de la mémoire partagée

Les composants doivent offrir la possibilité d’assurer une protection contre le transfert non autorisé et imprévu des informations par l'intermédiaire de ressources de mémoire partagée volatile.

Les ressources de mémoire volatile sont des ressources qui ne conservent en général pas les informations après la gestion de mémoire. Toutefois, certaines attaques perpétrées contre la mémoire RAM peuvent permettre d'extraire des informations essentielles ou d'autres données confidentielles avant qu'elles ne soient réellement écrasées. Par conséquent, si la mémoire partagée volatile est rendue au système de commande afin d'être utilisée par un autre utilisateur, il est nécessaire de purger de la ressource toutes les données uniques et leurs connexions, de sorte qu'elles ne soient plus visibles ni accessibles par un nouvel utilisateur.

(2) Vérification de l'effacement

Les composants doivent offrir la possibilité de vérifier que les informations ont été effacées.

8.4.4 Niveaux de sécurité

Les exigences pour les quatre niveaux de sécurité SL liés à CR 4.2 sont les suivantes:

- SL-C(DC, composant) 1: Non choisi
- SL-C(DC, composant) 2: CR 4.2
- SL-C(DC, composant) 3: CR 4.2 (1) (2)
- SL-C(DC, composant) 4: CR 4.2 (1) (2)

8.5 CR 4.3 – Utilisation de la cryptographie

8.5.1 Exigences

Si la cryptographie est exigée, le composant doit utiliser les mécanismes cryptographiques de sécurité conformément aux pratiques et recommandations reconnues et éprouvées au niveau international.

8.5.2 Justification et recommandations complémentaires

Il convient de choisir la protection cryptographique en fonction d’une analyse des menaces et des risques couvrant la valeur des informations protégées, des conséquences de la confidentialité et de l’intégrité des informations auxquelles il a été porté atteinte, de la durée de confidentialité des informations et des contraintes de fonctionnement du système de commande. Cela peut concerner les informations au repos et/ou en transit. Il est à noter que les sauvegardes sont un exemple d'informations au repos et qu'il convient de les prendre en considération dans le cadre du processus d'évaluation de la confidentialité et de l’intégrité des données. Il convient que le fournisseur de produit du système de commande justifie les pratiques et procédures relatives à la mise en place et à la gestion des clés cryptographiques. Il convient que le système de commande utilise les algorithmes de chiffrement et de hachage mis en place et soumis à l’essai, comme la norme de chiffrement avancé (AES) et l'algorithme de compression sécurisé (SHA), ainsi que les tailles de clé reposant sur une norme attribuée. Il est nécessaire de générer des clés à l'aide d'un générateur de nombres aléatoires efficace. Il est nécessaire que les politiques et procédures de sécurité pour la gestion de clé portent sur les modifications régulières de clé, la destruction de clé, la distribution de clé et la

sauvegarde de clé de chiffrement conformément aux normes définies. En règle générale, les pratiques acceptées et les recommandations peuvent être consultées dans des documents tels que NIST SP 800-57, Recommendation for Key Management – Part 1: General [18]. Les exigences de mise en œuvre peuvent être consultées, par exemple dans FIPS 140-2, Security Requirements for Cryptographic Modules [17] ou dans l'ISO/IEC 19790 [9].

Cette CR, ainsi que 5.10, CR 1.8 – Certificats d'infrastructure à clés publiques, peuvent être applicables pour satisfaire aux autres exigences définies dans les limites du présent document.

8.5.3 Amélioration d'exigences

Aucune

8.5.4 Niveaux de sécurité

Les exigences pour les quatre niveaux de sécurité liés à CR 4.3 sont les suivantes:

- SL-C(DC,composant) 1: CR 4.3
- SL-C(DC,composant) 2: CR 4.3
- SL-C(DC,composant) 3: CR 4.3
- SL-C(DC,composant) 4: CR 4.3

9 FR 5 – Transfert de données limité

9.1 Objet et descriptions du SL-C(RDF)

Segmenter le système de commande au moyen des zones et des conduits pour limiter le transfert inutile de données.

- SL 1 – Empêcher le contournement fortuit ou occasionnel d'une segmentation en zones et conduits.
- SL 2 – Empêcher le contournement délibéré d'une segmentation en zones et conduits par des entités utilisant des moyens simples avec peu de ressources, des compétences génériques et peu de motivation.
- SL 3 – Empêcher le contournement délibéré d'une segmentation en zones et conduits par des entités utilisant des moyens sophistiqués avec des ressources modérées, des compétences spécifiques à l'IACS et une motivation modérée.
- SL 4 – Empêcher le contournement délibéré d'une segmentation en zones et conduits par des entités utilisant des moyens sophistiqués avec des ressources étendues, des compétences spécifiques à l'IACS et une motivation élevée.

9.2 Justification

Grâce à leur méthodologie d'appréciation du risque définie dans l'IEC 62443-3-2 [5], il convient que les propriétaires d'actif déterminent les restrictions en matière de transfert d'informations et, par conséquent, déterminent par extension la configuration des conduits utilisés pour délivrer ces informations. Il convient que les recommandations et lignes directrices déduites incluent des mécanismes allant de la déconnexion des réseaux de système de commande des réseaux professionnels ou publics, à l'utilisation de passerelles unidirectionnelles, de pare-feu dynamiques uniques ou de configurations de zones démilitarisées pour gérer le transfert d'informations.

9.3 CR 5.1 – Segmentation du réseau

9.3.1 Exigences

Les composants doivent prendre en charge un réseau segmenté pour la prise en charge de zones et de conduits, en fonction des besoins, afin de prendre en charge une architecture réseau plus vaste reposant sur la segmentation logique et la criticité.

9.3.2 Justification et recommandations complémentaires

La segmentation du réseau est utilisée par les organismes pour une multitude de raisons, y compris la cybersécurité. La segmentation de réseaux vise principalement à réduire l'exposition, ou l'infiltration, du trafic des réseaux dans un système de commande et à réduire la propagation, ou l'évacuation, du trafic des réseaux depuis un système de commande. Cette segmentation améliore la réponse et la fiabilité globales du système tout en fournissant une mesure de protection de cybersécurité. Elle permet également d'obtenir différents segments de réseaux au sein du système de commande, y compris les systèmes essentiels de commande et les systèmes liés à la sécurité, depuis d'autres systèmes pour obtenir un niveau supplémentaire de protection.

Il convient de justifier clairement l'accès à la toile (World Wide Web) à partir du système de commande selon les exigences opérationnelles du système de commande.

La segmentation du réseau et le niveau de protection qu'elle fournit varient fortement en fonction de l'architecture globale du réseau utilisée par un propriétaire d'actif dans ses locaux ou même par les intégrateurs systèmes au sein de leurs systèmes de commande. Les réseaux segmentés de manière logique selon leur fonctionnalité fournissent une mesure de protection, mais ils peuvent engendrer des points de défaillance uniques si un appareil de réseau est compromis. La segmentation physique de réseaux fournit un autre niveau de protection en retirant la situation de points de défaillance uniques, mais elle donne lieu à une conception de réseau plus complexe et plus onéreuse. Ces compromis nécessitent une évaluation au cours du processus de conception du réseau (voir l'IEC 62443-3-2-1 [13]).

En réponse à un incident, il peut être nécessaire de rompre les connexions entre les différents segments de réseaux. Dans ce cas, il convient de maintenir les services nécessaires à la prise en charge d'opérations essentielles de sorte que les appareils puissent continuer à fonctionner correctement et/ou s'arrêter de manière ordonnée. Ceci peut exiger la nécessité de reproduire certains serveurs sur le réseau du système de commande afin de prendre en charge les fonctionnalités normales du réseau, comme le protocole DHCP, le service de noms de domaine (DNS) ou les AC locales, par exemple. Ceci peut également signifier que certains systèmes essentiels de commande et systèmes liés à la sécurité sont initialement conçus pour être complètement isolés des autres réseaux.

9.3.3 Amélioration d'exigences

Aucune

9.3.4 Niveaux de sécurité

Les exigences pour les quatre niveaux de sécurité SL liés à CR 5.1 sont les suivantes:

- SL-C(RDF, composant) 1: CR 5.1
- SL-C(RDF, composant) 2: CR 5.1
- SL-C(RDF, composant) 3: CR 5.1
- SL-C(RDF, composant) 4: CR 5.1

9.4 CR 5.2 – Protection des limites de zone

Les exigences relatives à la protection des limites de zone sont spécifiques au composant de réseau et peuvent être considérées comme des exigences pour les appareils de réseaux de l'Article 15.

9.5 CR 5.3 – Restrictions des communications entre des personnes d'ordre général

Les exigences relatives aux restrictions des communications entre des personnes d'ordre général sont spécifiques au composant de réseau et peuvent être considérées comme des exigences pour les appareils de réseaux de l'Article 15.

9.6 CR 5.4 – Partitionnement des applications

Aucune exigence de niveau de composant n'est associée à l'IEC 62443-3 SR 5.4.

10 FR 6 – Réponse appropriée aux événements

10.1 Objet et descriptions du SL-C(TRE)

Répondre à des violations de sécurité en informant les autorités compétentes, en apportant les preuves nécessaires de la violation et en procédant aux actions correctives correspondantes lorsque des incidents sont détectés.

- SL 1 – Surveiller le fonctionnement des composants de l'IACS et répondre aux incidents détectés en rassemblant et en apportant les preuves demandées.
- SL 2 – Surveiller le fonctionnement des composants de l'IACS et répondre aux incidents détectés en rassemblant activement et en apportant régulièrement des preuves.
- SL 3 – Surveiller le fonctionnement des composants de l'IACS et répondre aux incidents détectés en rassemblant activement les preuves et en les transmettant aux autorités compétentes.
- SL 4 – Surveiller le fonctionnement des composants de l'IACS et répondre aux incidents détectés en rassemblant activement les preuves et en les transmettant pratiquement en temps réel aux autorités compétentes.

10.2 Justification

Bien qu'un système puisse commencer à fonctionner dans un état sûr, il est important d'être en mesure de surveiller le système pour assurer qu'il reste dans cet état sûr. Si un événement affecte la sécurité d'un système, une notification appropriée de l'événement peut être cruciale pour l'atténuation du risque associé. Il convient que les propriétaires d'actif établissent les politiques et procédures de sécurité, ainsi que les voies de communication et de contrôle nécessaires pour répondre à des violations de sécurité. Il convient que les recommandations et lignes directrices déduites incluent des mécanismes permettant de rassembler, consigner, préserver et corréler automatiquement les preuves afin de procéder aux actions correctives correspondantes. Il convient que l'utilisation d'outils et de techniques de surveillance n'ait pas d'impact négatif sur les performances opérationnelles du système de commande.

10.3 CR 6.1 – Accessibilité au journal d'audit

10.3.1 Exigences

Les composants doivent offrir la possibilité aux personnes et/ou outils autorisés d'accéder en lecture seule aux journaux d'audit.

10.3.2 Justification et recommandations complémentaires

Les applications et appareils peuvent générer des enregistrements d'audit relatifs aux événements dont elles/ils font l'objet (voir 6.10). L'accès à ces journaux d'audit est nécessaire à la prise en charge du filtrage de ces journaux, à l'identification et la suppression des informations redondantes, à la révision et au rapport d'activité pendant les enquêtes après-coup des incidents de sécurité. En règle générale, il convient de procéder à un audit et à la génération d'un rapport sur un système d'information séparé. L'accès manuel aux enregistrements d'audit (affichages-écrans ou impressions, par exemple) suffit à satisfaire aux exigences de base, mais ne suffit à atteindre des niveaux de sécurité plus élevés. L'accès programmatique est souvent utilisé pour soumettre les informations du journal d'audit à des mécanismes d'analyse comme la gestion des informations sur la sécurité et des événements (SIEM).

10.3.3 Amélioration d'exigences

(1) Accès programmatique aux journaux d'audit

Les composants doivent assurer un accès programmatique aux enregistrements d'audit à l'aide d'une interface de programmation d'application (API) ou en envoyant les enregistrements d'audit à un système centralisé.

10.3.4 Niveaux de sécurité

Les exigences pour les quatre niveaux de sécurité SL liés à CR 6.1 sont les suivantes:

- SL-C(TRE, composant) 1: CR 6.1
- SL-C(TRE, composant) 2: CR 6.1
- SL-C(TRE, composant) 3: CR 6.1 (1)
- SL-C(TRE, composant) 4: CR 6.1 (1)

10.4 CR 6.2 – Surveillance continue

10.4.1 Exigences

Les composants doivent offrir la possibilité d'être surveillés en permanence dans le cadre de pratiques et de recommandations en matière de sécurité communément acceptées, afin de détecter, caractériser et signaler les brèches de sécurité de façon opportune.

10.4.2 Justification et recommandations complémentaires

La capacité de surveillance du système de commande peut être obtenue au moyen d’un ensemble d'outils et de techniques (IDS, système de prévention des intrusions (IPS), mécanismes de protection contre les programmes malveillants et mécanismes de surveillance du réseau, par exemple). Les attaques étant de plus en plus sophistiquées, il est nécessaire que ces outils et techniques de surveillance le deviennent également, et qu'ils intègrent un IDS/IPS basé sur le comportement, par exemple.

Il convient de déployer de manière stratégique les appareils de surveillance au sein du système de commande (à des emplacements précis et à proximité de grappes de serveurs prenant en charge les applications cruciales, par exemple) afin de rassembler des informations essentielles. Les mécanismes de surveillance peuvent également être déployés à des emplacements ad hoc au sein du système de commande afin d'assurer le suivi de transactions particulières.

Il convient que la surveillance comprenne des mécanismes de génération de rapport appropriés permettant de répondre de manière appropriée aux événements. Pour faciliter la génération de rapport et maintenir la quantité d'informations à un niveau pouvant être traité par les destinataires, des mécanismes comme SIEM sont souvent appliqués pour corréler des événements individuels dans des rapports globaux qui élargissent le contexte dans lequel sont survenus les événements bruts.

10.4.3 Amélioration d'exigences

Aucune

10.4.4 Niveaux de sécurité

Les exigences pour les quatre niveaux de sécurité SL liés à CR 6.2 sont les suivantes:

- SL-C(TRE, composant) 1: Non choisi
- SL-C(TRE, composant) 2: CR 6.2
- SL-C(TRE, composant) 3: CR 6.2
- SL-C(TRE, composant) 4: CR 6.2

11 FR 7 – Disponibilité des ressources

11.1 Objet et descriptions du SL-C(RA)

Assurer la disponibilité des composants face à une dégradation ou à un refus de services essentiels.

- SL 1 – Assurer que le composant fonctionne en toute fiabilité dans les conditions normales de production, et éviter les situations de refus de service par suite d'actions fortuites ou occasionnelles d'une entité.
- SL 2 – Assurer que le composant fonctionne en toute fiabilité dans les conditions normales et anormales de production, et éviter les situations de refus de service par des entités utilisant des moyens simples avec peu de ressources, des compétences génériques et peu de motivation.
- SL 3 – Assurer que le composant fonctionne en toute fiabilité dans les conditions normales, anormales et extrêmes de production, et éviter les situations de refus de service par des entités utilisant des moyens sophistiqués avec des ressources modérées, des compétences spécifiques à l'IACS et une motivation modérée.
- SL 4 – Assurer que le composant fonctionne en toute fiabilité dans les conditions normales, anormales et extrêmes de production, et éviter les situations de refus de service par des entités utilisant des moyens sophistiqués avec des ressources étendues, des compétences spécifiques à l'IACS et une motivation élevée.

11.2 Justification

Cette série de CR a pour objet d'assurer la résilience du composant face aux différents types d'événements de refus de service (DoS). Cela inclut l'indisponibilité partielle ou totale de la fonctionnalité du composant à différents niveaux. En particulier, il convient que les incidents de sécurité n'aient pas d'impact sur des fonctions essentielles ou sur d'autres fonctions liées à la sécurité.

11.3 CR 7.1 – Protection contre le refus de service

11.3.1 Exigences

Les composants doivent offrir la possibilité de maintenir les fonctions essentielles lorsqu'ils fonctionnent en mode dégradé par suite d'un événement DoS.

11.3.2 Justification et recommandations complémentaires

Les composants peuvent faire l'objet de différentes formes de situations DoS. Si ces situations se produisent, il convient que le composant soit conçu de manière à maintenir les fonctions essentielles nécessaires au fonctionnement sûr tout en étant en mode dégradé.

11.3.3 Amélioration d'exigences

(1) Gérer la charge de communication provenant du composant

Les composants doivent offrir la possibilité d'atténuer les effets des flots d'informations et/ou de messages des événements DoS.

11.3.4 Niveaux de sécurité

Les exigences pour les quatre niveaux de sécurité SL liés à CR 7.1 sont les suivantes:

- SL-C(RA, composant) 1: CR 7.1
- SL-C(RA, composant) 2: CR 7.1 (1)
- SL-C(RA, composant) 3: CR 7.1 (1)
- SL-C(RA, composant) 4: CR 7.1 (1)

11.4 CR 7.2 – Gestion des ressources

11.4.1 Exigences

Les composants doivent offrir la possibilité de limiter l'utilisation des ressources par des fonctions de sécurité visant à assurer une protection contre l'épuisement des ressources.

11.4.2 Justification et recommandations complémentaires

La gestion des ressources (segmentation de réseau ou schémas de priorité, par exemple) empêche un processus logiciel de priorité inférieure de retarder ou de gêner le système de commande utilisé pour un processus logiciel de priorité plus élevée. Par exemple, le fait de procéder à des analyses du réseau, d'appliquer des correctifs et/ou de procéder à un contrôle antivirus sur un système d'exploitation peut perturber gravement le fonctionnement normal. Il convient de considérer les schémas de limitation du débit comme une technique d'atténuation.

11.4.3 Amélioration d'exigences

Aucune

11.4.4 Niveaux de sécurité

Les exigences pour les quatre niveaux de sécurité SL liés à CR 7.2 sont les suivantes:

- SL-C(RA, composant) 1: CR 7.2
- SL-C(RA, composant) 2: CR 7.2
- SL-C(RA, composant) 3: CR 7.2
- SL-C(RA, composant) 4: CR 7.2

11.5 CR 7.3 – Sauvegarde du système de commande

11.5.1 Exigences

Les composants doivent offrir la possibilité de participer aux opérations de sauvegarde au niveau du système afin de protéger l'état du composant (informations au niveau de l'utilisateur et du système). Le processus de sauvegarde ne doit pas avoir d'impact sur le fonctionnement normal du composant.

11.5.2 Justification et recommandations complémentaires

La disponibilité de sauvegardes à jour est essentielle pour la récupération en cas de défaillance et/ou de mauvaise configuration du système de commande. Le fait d'automatiser cette fonction permet d'assurer que tous les fichiers exigés sont capturés, ce qui réduit la charge de travail de l'opérateur.

Lors de la conception de la prise en charge d'une capacité de sauvegarde, il convient de tenir compte des informations qui seront stockées dans les sauvegardes. Certaines de ces informations peuvent contenir des clés cryptographiques et d'autres informations protégées par des contrôles de sécurité tout en faisant partie intégrante du système. Une fois les informations placées dans une sauvegarde, les contrôles qui les protègent sont susceptibles de ne plus être les mêmes. Par conséquent, la fonction de sauvegarde de composant nécessite d'inclure des mécanismes de prise en charge de la protection nécessaire des informations contenues dans la sauvegarde. Il peut s'agir du chiffrement de la sauvegarde, du chiffrement des données sensibles de la procédure de sauvegarde ou de ne pas inclure les informations sensibles dans la sauvegarde. Si la sauvegarde est chiffrée, il est important de ne pas inclure les clés cryptographiques dans la sauvegarde, mais de les sauvegarder dans le cadre d'une procédure plus sécurisée.

11.5.3 Amélioration d'exigences

(1) Vérification de l'intégrité de la sauvegarde

Les composants doivent offrir la possibilité de valider l'intégrité des informations sauvegardées avant de restaurer ces informations.

11.5.4 Niveaux de sécurité

Les exigences pour les quatre niveaux de sécurité SL liés à CR 7.3 sont les suivantes:

- SL-C(RA, composant) 1: CR 7.3
- SL-C(RA, composant) 2: CR 7.3 (1)
- SL-C(RA, composant) 3: CR 7.3 (1)
- SL-C(RA, composant) 4: CR 7.3 (1)

11.6 CR 7.4 – Récupération et reconstitution du système de commande

11.6.1 Exigences

Les composants doivent offrir la possibilité d'être récupérés et reconstitués à un état sûr connu après une perturbation ou une défaillance.

11.6.2 Justification et recommandations complémentaires

La récupération et la reconstitution du composant à un état sûr connu signifient que des valeurs sécurisées sont attribuées à tous les paramètres du système (par défaut ou configurables), que des correctifs essentiels pour la sécurité sont réinstallés, que les paramètres de configuration liés à la sécurité sont rétablis, que les procédures de documentation et de fonctionnement du système sont disponibles, que les composants sont réinstallés et configurés avec des paramètres établis, que les informations provenant des dernières sauvegardes de sécurité connues sont chargées et que le système a été intégralement soumis à l'essai et qu'il fonctionne.

11.6.3 Amélioration d'exigences

Aucune

11.6.4 Niveaux de sécurité

Les exigences pour les quatre niveaux de sécurité SL liés à CR 7.4 sont les suivantes:

- SL-C(RA, composant) 1: CR 7.4
- SL-C(RA, composant) 2: CR 7.4
- SL-C(RA, composant) 3: CR 7.4
- SL-C(RA, composant) 4: CR 7.4

11.7 CR 7.5 – Alimentation de secours

Aucune exigence de niveau de composant n'est associée à l'IEC 62443-3 CR 7.5.

11.8 CR 7.6 – Paramètres de configuration du réseau et de la sécurité

11.8.1 Exigences

Les composants doivent offrir la possibilité d'être configurés selon les configurations recommandées en matière de réseau et de sécurité, décrites dans les lignes directrices données par le fournisseur du système de commande. Le composant doit fournir une interface avec les paramètres de configuration déployés en matière de réseau et de sécurité.

11.8.2 Justification et recommandations complémentaires

Ces paramètres de configuration sont les paramètres ajustables des composants du système de commande. Par défaut, il convient de configurer le composant avec les paramètres recommandés. Pour qu'un composant détecte et corrige tous les écarts par rapport aux paramètres de configuration approuvés et/ou recommandés, il est nécessaire qu'il assure la surveillance et le contrôle des modifications apportées aux paramètres de configuration selon les politiques et procédures de sécurité.

11.8.3 Amélioration d'exigences

(1) Génération d'un rapport lisible par une machine des paramètres de sécurité en cours

Les composants doivent offrir la possibilité de générer un rapport, dans un format lisible par une machine, dans lequel figurent les paramètres de sécurité déployés.

11.8.4 Niveaux de sécurité

Les exigences pour les quatre niveaux de sécurité SL liés à CR 7.6 sont les suivantes:

- SL-C(RA, composant) 1: CR 7.6
- SL-C(RA, composant) 2: CR 7.6
- SL-C(RA, composant) 3: CR 7.6 (1)
- SL-C(RA, composant) 4: CR 7.6 (1)

11.9 CR 7.7 – Fonctionnalité minimale

11.9.1 Exigences

Les composants doivent offrir la possibilité de limiter de manière spécifique l'utilisation de fonctions, d'accès, de protocoles et/ou de services inutiles.

11.9.2 Justification et recommandations complémentaires

Les composants sont en mesure de fournir un large éventail de fonctions et de services. Certaines de ces fonctions et certains de ces services fournis peuvent ne pas être nécessaires à la prise en charge de la fonctionnalité IACS. Par conséquent, il convient de désactiver par défaut les fonctions allant au-delà de la configuration de base. De plus, il s'avère parfois pratique de fournir plusieurs services à partir d'un seul composant d'un système de commande, mais cela augmente le risque comparé à la limitation des services fournis par l'un des composants.

11.9.3 Amélioration d'exigences

Aucune

11.9.4 Niveaux de sécurité

Les exigences pour les quatre niveaux de sécurité SL liés à CR 7.7 sont les suivantes:

- SL-C(RA, composant) 1: CR 7.7
- SL-C(RA, composant) 2: CR 7.7
- SL-C(RA, composant) 3: CR 7.7
- SL-C(RA, composant) 4: CR 7.7

11.10 CR 7.8 – Inventaire des composants du système de commande

11.10.1 Exigences

Les composants doivent offrir la possibilité d'assurer l'inventaire des composants du système de commande selon l'IEC 62443-3-3 SR 7.8.

11.10.2 Justification et recommandations complémentaires

Les composants peuvent introduire leur propre ensemble de composants dans le système global de commande. Si c'est le cas, il est nécessaire que ces composants offrent un mécanisme permettant d'augmenter l'inventaire global de composants compatible avec l'IEC 62443-2-4 [3] SP.06.02.

11.10.3 Amélioration d'exigences

Aucune

11.10.4 Niveaux de sécurité

Les exigences pour les quatre niveaux de sécurité SL liés à CR 7.8 sont les suivantes:

- SL-C(RA, composant) 1: Non choisi
- SL-C(RA, composant) 2: CR 7.8
- SL-C(RA, composant) 3: CR 7.8
- SL-C(RA, composant) 4: CR 7.8

12 Exigences relatives aux applications logicielles

12.1 Objet

Cet ensemble d'exigences a pour objet de documenter les exigences spécifiques à des applications logicielles.

12.2 SAR 2.4 – Code mobile

12.2.1 Exigences

Si une application logicielle utilise des technologies de code mobile, elle doit offrir la possibilité de mettre en place une politique de sécurité permettant de les utiliser. La politique de sécurité doit au moins permettre de réaliser les actions suivantes pour chaque technologie de code mobile utilisée sur l'application logicielle:

a) Exécution de contrôle du code mobile;

b) Contrôler les utilisateurs (êtres humains, processus logiciels ou appareils) autorisés à transférer le code mobile vers/depuis l'application; et

c) Contrôler l’exécution du code mobile d’après les résultats d’un contrôle d’intégrité avant d'exécuter le code.

12.2.2 Justification et recommandations complémentaires

Les technologies de code mobile incluent, entre autres, Java, JavaScript, ActiveX, Portable Document Format (PDF), Postscript, les films Shockwave, les animations Flash et VBScript. L'utilisation de restrictions s'applique au choix et à l'utilisation du code mobile installé sur les serveurs et au code mobile téléchargé et exécuté sur des postes individuels. Il convient que les procédures de contrôle empêchent le développement, l'acquisition ou l'introduction de code mobile inacceptable au sein du système de commande dans lequel réside le composant. Par exemple, les échanges de code mobile peuvent être désactivés directement dans le système de commande, mais peuvent être admis dans un environnement adjacent contrôlé géré par le personnel IACS.

12.2.3 Amélioration d'exigences

(1) Contrôle d’authenticité du code mobile

L'application doit offrir la possibilité d’appliquer une politique de sécurité permettant à l’appareil de contrôler l’exécution du code mobile d’après les résultats d’un contrôle d’authenticité avant d’exécuter le code.

12.2.4 Niveaux de sécurité

Les exigences pour les quatre niveaux de sécurité SL liés à SAR 2.4 sont les suivantes:

- SL-C(UC, composant) 1: SAR 2.4
- SL-C(UC, composant) 2: SAR 2.4 (1)
- SL-C(UC, composant) 3: SAR 2.4 (1)
- SL-C(UC, composant) 4: SAR 2.4 (1)

12.3 SAR 3.2 – Protection contre les programmes malveillants

12.3.1 Exigences

Le fournisseur du produit d'application doit indiquer et préciser quelles sont les protections contre les programmes malveillants compatibles avec l'application, et indiquer toutes les exigences particulières en matière de configuration.

12.3.2 Justification et recommandations complémentaires

La protection contre les programmes malveillants (virus, vers informatiques, chevaux de Troie et logiciels espions, par exemple) peut être assurée par l’application du système de commande ou par un service ou une application externe. Il est nécessaire que les applications du système de commande soient compatibles avec les mécanismes visant à les protéger contre les programmes malveillants. Cette exigence n’impose pas au fournisseur de produits de qualifier et documenter tous les mécanismes de protection contre les programmes malveillants qui sont compatibles avec l’application, mais elle implique que le fournisseur de produits qualifie et documente au moins un mécanisme.

12.3.3 Amélioration d'exigences

Aucune

12.3.4 Niveaux de sécurité

Les exigences pour les quatre niveaux de sécurité SL liés à SAR 3.2 sont les suivantes:

- SL-C(SI, composant) 1: SAR 3.2
- SL-C(SI, composant) 2: SAR 3.2
- SL-C(SI, composant) 3: SAR 3.2
- SL-C(SI, composant) 4: SAR 3.2

13 Exigences relatives aux appareils intégrés

13.1 Objet

Cet ensemble d'exigences a pour objet de documenter les exigences spécifiques aux appareils intégrés.

13.2 EDR 2.4 – Code mobile

13.2.1 Exigences

Si un appareil intégré utilise des technologies de code mobile, il doit offrir la possibilité de mettre en place une politique de sécurité permettant de les utiliser. La politique de sécurité doit au moins permettre de réaliser les actions suivantes pour chaque technologie de code mobile utilisée sur l'appareil intégré:

a) Exécution de contrôle du code mobile;

b) Contrôler les utilisateurs (êtres humains, processus logiciels ou appareils) autorisés à charger le code mobile sur l'appareil; et

c) Contrôler l'exécution du code mobile d'après les résultats d'un contrôle d'intégrité avant d'exécuter le code.

13.2.2 Justification et recommandations complémentaires

Les technologies de code mobile incluent, entre autres, Java, JavaScript, ActiveX, Portable Document Format (PDF), Postscript, les films Shockwave, les animations Flash et VBScript. L'utilisation de restrictions s'applique au choix et à l'utilisation du code mobile installé sur les serveurs et au code mobile téléchargé et exécuté sur des postes individuels. Il convient que les procédures de contrôle empêchent le développement, l'acquisition ou l'introduction de code mobile inacceptable au sein du système de commande dans lequel réside le composant. Par exemple, les échanges de code mobile peuvent être désactivés directement dans le système de commande, mais peuvent être admis dans un environnement adjacent contrôlé géré par le personnel IACS.

13.2.3 Amélioration d'exigences

(1) Contrôle d'authenticité du code mobile

L'appareil intégré doit offrir la possibilité d'appliquer une politique de sécurité permettant à l'appareil de contrôler l'exécution du code mobile d'après les résultats d'un contrôle d'authenticité avant d'exécuter le code.

13.2.4 Niveaux de sécurité

Les exigences pour les quatre niveaux de sécurité SL liés à EDR 2.4 sont les suivantes:

- SL-C(UC, composant) 1: EDR 2.4
- SL-C(UC, composant) 2: EDR 2.4 (1)
- SL-C(UC, composant) 3: EDR 2.4 (1)
- SL-C(UC, composant) 4: EDR 2.4 (1)

13.3 EDR 2.13 – Utilisation d'interfaces physiques de diagnostic et d'essai

13.3.1 Exigences

Les appareils intégrés doivent assurer une protection contre l'utilisation non autorisée des interfaces physiques de diagnostic et d'essai en usine (débogage JTAG, par exemple).

13.3.2 Justification et recommandations complémentaires

Les interfaces de diagnostic et d'essai en usine sont créées à différents endroits dans l'appareil intégré. Elles visent à aider les développeurs d'appareil intégré et le personnel à soumettre la mise en œuvre à l'essai, et si des erreurs sont détectées, à les éliminer de l'appareil intégré. Toutefois, il convient de protéger soigneusement ces mêmes interfaces contre tout accès par des entités non autorisées afin de protéger les fonctionnalités essentielles fournies par l'appareil intégré à l'IACS.

Si une interface de diagnostic et d'essai n'offre pas la possibilité de contrôler l'appareil intégré ou d'accéder aux informations non publiques, elle ne nécessite pas de mécanisme d'authentification. Ceci doit être déterminé par une appréciation des menaces et des risques, telle que le débogage JTAG, qui utilise JTAG pour contrôler le processeur et exécuter les commandes arbitraires, par rapport au registre à décalage périphérique JTAG, qui utilise JTAG pour lire simplement les informations (qui peuvent être des informations accessibles au public).

Dans certains cas, les interfaces de diagnostic et d'essai en usine peuvent utiliser les communications réseau avec l'appareil. Si c'est le cas, ces interfaces doivent satisfaire à toutes les exigences du présent document.

13.3.3 Amélioration d'exigences

(1) Surveillance active

Les appareils intégrés doivent assurer la surveillance active des interfaces de diagnostic et d'essai de l'appareil et générer une entrée de journal d'audit si une tentative d'accès à ces interfaces a été détectée.

13.3.4 Niveaux de sécurité

Les exigences pour les quatre niveaux de sécurité SL liés à EDR 2.13 sont les suivantes:

- SL-C(SI, composant) 1: Non choisi
- SL-C(SI, composant) 2: EDR 2.13
- SL-C(SI, composant) 3: EDR 2.13 (1)
- SL-C(SI, composant) 4: EDR 2.13 (1)

13.4 EDR 3.2 – Protection contre les programmes malveillants

13.4.1 Exigences

L'appareil intégré doit offrir la possibilité de se protéger contre l'installation et l'exécution de logiciels non autorisés.

13.4.2 Justification et recommandations complémentaires

Les logiciels non autorisés peuvent contenir des programmes malveillants et ainsi nuire au composant. Si un appareil intégré est en mesure d'utiliser un contrôle compensatoire, il ne nécessite pas directement d'assurer la protection contre les programmes malveillants. L'IACS est présumé être chargé de fournir les protections exigées. Toutefois, dans certains cas (en présence d'un accès hôte USB, par exemple), il convient de déterminer la nécessité d'une protection contre les programmes malveillants par une appréciation du risque.

Il convient que les mécanismes de détection soient en mesure de détecter les violations d'intégrité des fichiers binaires et des fichiers de données de l'application. Les techniques peuvent inclure, entre autres, la surveillance de l'intégrité binaire et des attributs, le hachage et les techniques de signature.

Les techniques de prévention peuvent inclure, entre autres, le contrôle de support amovible, les techniques de bac à sable et les mécanismes de plateformes de calcul spécifiques comme les capacités de mise à jour restreintes de micrologiciel, NX-Bit (No Execute), la prévention de l'exécution des données (DEP), la distribution aléatoire de l'espace d'adressage (ASLR), la détection de la corruption de pile et les contrôles d'accès obligatoires. Voir pour une exigence associée concernant des outils et techniques de surveillance du système de commande.

13.4.3 Amélioration d'exigences

Aucune

13.4.4 Niveaux de sécurité

Les exigences pour les quatre niveaux de sécurité SL liés à EDR 3.2 sont les suivantes:

- SL-C(SI, composant) 1: EDR 3.2
- SL-C(SI, composant) 2: EDR 3.2
- SL-C(SI, composant) 3: EDR 3.2
- SL-C(SI, composant) 4: EDR 3.2

13.5 EDR 3.10 – Support pour les mises à jour

13.5.1 Exigences

L’appareil intégré doit offrir la possibilité d'être mis à jour et mis à niveau.

13.5.2 Justification et recommandations complémentaires

Pendant toute leur durée de vie, les appareils intégrés peuvent avoir besoin de mises à jour et de mises à niveau. Dans certains cas, les appareils intégrés prennent en charge ou exécutent également des fonctions essentielles. Si c'est le cas, il est nécessaire que l’appareil intégré comporte des mécanismes d'application de correctifs et de mises à jour n'ayant aucun impact sur les fonctions essentielles des systèmes à haute disponibilité (voir 4.2). Il s'agit, par exemple, d'assurer la redondance au sein de l’appareil intégré.

13.5.3 Amélioration d'exigences

(1) Mettre à jour l'authenticité et l'intégrité

L’appareil intégré doit valider l'authenticité et l'intégrité d'une mise à jour ou d’une mise à niveau d’un logiciel avant de l'installer.

13.5.4 Niveaux de sécurité

Les exigences pour les quatre niveaux de sécurité SL liés à EDR 3.10 sont les suivantes:

- SL-C(SI, composant) 1: EDR 3.10
- SL-C(SI, composant) 2: EDR 3.10 (1)
- SL-C(SI, composant) 3: EDR 3.10 (1)
- SL-C(SI, composant) 4: EDR 3.10 (1)

13.6 EDR 3.11 – Résistance aux violations physiques et détection

13.6.1 Exigences

L’appareil intégré doit fournir des mécanismes de résistance et de détection des violations pour assurer une protection contre les accès physiques non autorisés dans l’appareil.

13.6.2 Justification et recommandations complémentaires

Les mécanismes de résistance aux violations ont pour objet d'empêcher un attaquant d'exécuter une action physique non autorisée contre un appareil IACS. Outre la prévention, la détection et la réponse sont essentielles en cas de manipulation frauduleuse.

Les mécanismes de résistance aux violations sont plus efficaces lorsqu'ils sont combinés pour empêcher l'accès à l'un des composants cruciaux. La résistance aux violations consiste à utiliser des matériaux spécialisés pour rendre difficile la manipulation frauduleuse d'un appareil ou d'un module. Il peut s'agir de boîtiers renforcés, de verrous, d'encapsulation ou de vis de sécurité. Des trajectoires de circulation d'air tendues rendent plus difficile l'accès aux éléments internes du produit.

Le témoin d'intégrité a pour objet d'apporter la preuve visible ou électronique d'une manipulation frauduleuse. De nombreuses techniques consistent à utiliser des scellés pour mettre en évidence toute tentative de violation physique. Les commutateurs sont des techniques plus sophistiquées.

13.6.3 Amélioration d'exigences

(1) Notification d'une tentative de violation

L’appareil intégré doit être en mesure d'informer automatiquement un ensemble configurable de destinataires d'une tentative d'accès physique non autorisée. Toutes les notifications de violation doivent être consignées dans le cadre de la fonction de journalisation globale d'audit.

13.6.4 Niveaux de sécurité

Les exigences pour les quatre niveaux de sécurité liés à EDR 3.11 sont les suivantes:

- SL-C(SI, composant) 1: Non choisi
- SL-C(SI, composant) 2: EDR 3.11
- SL-C(SI, composant) 3: EDR 3.11 (1)
- SL-C(SI, composant) 4: EDR 3.11 (1)

13.7 EDR 3.12 – Fourniture des racines de confiance du fournisseur de produit

13.7.1 Exigences

Les appareils intégrés doivent offrir la possibilité d'assurer et de protéger la confidentialité, l'intégrité et l'authenticité des clés et des données du fournisseur de produit à utiliser comme une ou plusieurs «racines de confiance» au moment de la fabrication de l’appareil.

13.7.2 Justification et recommandations complémentaires

Pour qu'un composant soit en mesure de valider l'authenticité et l'intégrité du matériel, du logiciel et des données fournies par le fournisseur de produit, il convient qu’il comporte une source de données digne de confiance pour exécuter le processus de validation. Cette source de données digne de confiance est appelée «racine de confiance» pour le système. Cette source de données digne de confiance peut être un ensemble d'empreintes numériques de logiciels «corrects connus» ou peut être la partie publique d'une paire de clés cryptographiques asymétriques à utiliser dans la validation des signatures cryptographiques. Ces données dignes de confiance sont souvent utilisées pour valider les logiciels, micrologiciels indispensables et données cruciales avant l'amorçage du micrologiciel ou du système d'exploitation d'un composant, afin de valider le fait que le composant s'amorce à un état «correct connu» dans lequel tous les mécanismes de sécurité sont réputés être opérationnels et parfaitement sûrs. Les données «racines de confiance» sont souvent protégées par des mécanismes matériels, ce qui empêche de les modifier pendant le fonctionnement normal du composant. La modification des données «racines de confiance» du fournisseur de produit se limite en général au processus de provisionnement du

fournisseur de produit, ce dernier disposant d'un processus digne de confiance permettant de mettre les données à disposition. Les informations à valider par rapport à la racine de confiance sont plutôt soumises au processus de validation par l'intermédiaire d'une API matérielle ou logicielle qui procède à la validation et renvoie les résultats sans exposer les données protégées.

13.7.3 Amélioration d'exigences

Aucune

13.7.4 Niveaux de sécurité

Les exigences pour les quatre niveaux de sécurité SL liés à EDR 3.12 sont les suivantes:

- SL-C(SI, composant) 1: Non choisi
- SL-C(SI, composant) 2: EDR 3.12
- SL-C(SI, composant) 3: EDR 3.12
- SL-C(SI, composant) 4: EDR 3.12

13.8 EDR 3.13 – Fourniture des racines de confiance du propriétaire d'actif

13.8.1 Exigences

Les appareils intégrés doivent

a) offrir la possibilité d'assurer et de protéger la confidentialité, l'intégrité et l'authenticité des clés et des données du propriétaire d'actif à utiliser comme «racines de confiance»; et
b) assurer la mise à disposition sans recourir aux composants qui peuvent se trouver hors de la zone de sécurité de l’appareil.

13.8.2 Justification et recommandations complémentaires

Les fournisseurs de produits ont mis en place des mécanismes visant à assurer l'authenticité des logiciels et micrologiciels présents sur leur composant et à vérifier que leur intégrité n’a pas été compromise. Cela permet au fournisseur de produit d'assurer au propriétaire d'actif un état «correct connu» à partir duquel opérer. Toutefois, de nombreux fournisseurs de produits proposent également des mécanismes permettant aux propriétaires d'actif d'étendre les fonctionnalités de leurs appareils par l'utilisation d'un code mobile, de programmes utilisateur ou d'autres moyens de même type. Pour protéger la sécurité du composant, il est également important de valider ces extensions de fonctionnalités de manière à assurer qu'elles sont autorisées et que le propriétaire d'actif a approuvé leur origine.

Pour procéder à ces validations, il convient que le composant contienne des données offrant un moyen de différencier les origines valides de celles qui ne le sont pas. La liste des origines valides et non valides diffère d'un propriétaire d'actif à l'autre, et il est peu probable qu'un fournisseur de produit dispose de la liste exhaustive de toutes les origines valides possibles au moment de la fabrication. Par conséquent, il est important que le fournisseur de produit propose au propriétaire d'actif un moyen de mettre à disposition ses propres «racines de confiance» en toute sécurité, offrant la possibilité de différencier les origines admises par la politique de sécurité du propriétaire d'actif de celles qui ne le sont pas. Il convient de protéger l'authenticité et l'intégrité de ces «racines de confiance» de sorte que des personnes malveillantes ne puissent pas ajouter d'autres racines de confiance leur donnant la possibilité de faire fonctionner le composant.

Une racine de confiance peut également être utilisée comme base pour la sécurité des communications, telle que l’intégrité de la communication exigée par CR 3.1 – Intégrité de la communication (7.3) ou la confidentialité des communications exigée par CR 4.1 – Confidentialité des informations (8.3).

(13.2) Des exigences comme celles de EDR 2.4 – Code mobile exigent que le composant contrôle l'authenticité du code mobile avant de l'exécuter. Les racines de confiance faisant l'objet de cette exigence fournissent les données nécessaires à la validation de l'origine et de l'intégrité du code mobile, permettant au composant de déterminer en toute indépendance si l'exécution du code est admise.

13.8.3 Amélioration d'exigences

Aucune

13.8.4 Niveaux de sécurité

Les exigences pour les quatre niveaux de sécurité SL liés à EDR 3.13 sont les suivantes:

- SL-C(SI, composant) 1: Non choisi
- SL-C(SI, composant) 2: EDR 3.13
- SL-C(SI, composant) 3: EDR 3.13
- SL-C(SI, composant) 4: EDR 3.13

13.9 EDR 3.14 – Intégrité du processus d'amorçage

13.9.1 Exigences

Les appareils intégrés doivent vérifier l'intégrité des micrologiciels, des logiciels et des données de configuration nécessaires aux processus d'amorçage et d'exécution du composant avant de les utiliser.

13.9.2 Justification et recommandations complémentaires

Pour donner l'assurance à un propriétaire d'actif que les fonctions de sécurité d'un composant n'ont pas été compromises, il est nécessaire d'assurer que les logiciels et micrologiciels du composant n'ont pas été manipulés de manière frauduleuse et qu'ils sont valides pour fonctionner sur le composant. Par conséquent, il convient que le composant procède aux contrôles pour vérifier l'intégrité de ses micrologiciels et/ou logiciels avant de les utiliser pendant le processus d'amorçage, afin d'assurer qu'il ne s'amorce pas dans un état de fonctionnement non sécurisé ou non valide qui pourrait l'endommager ou permettre à une personne malveillante d'accéder à d'autres composants, actifs ou données.

13.9.3 Amélioration d'exigences

(1) Authenticité du processus d'amorçage

Les appareils intégrés doivent utiliser les racines de confiance du fournisseur de produit du composant pour vérifier l'authenticité des micrologiciels, des logiciels et des données de configuration nécessaires au processus d'amorçage du composant avant de les utiliser dans ce processus.

13.9.4 Niveaux de sécurité

Les exigences pour les quatre niveaux de sécurité SL liés à EDR 3.14 sont les suivantes:

- SL-C(SI, composant) 1: EDR 3.14
- SL-C(SI, composant) 2: EDR 3.14 (1)
- SL-C(SI, composant) 3: EDR 3.14 (1)
- SL-C(SI, composant) 4: EDR 3.14 (1)

14 Exigences relatives aux appareils hôtes

14.1 Objet

Cet ensemble d'exigences a pour objet de documenter les exigences spécifiques aux appareils hôtes.

14.2 HDR 2.4 – Code mobile

14.2.1 Exigences

Si un appareil hôte utilise des technologies de code mobile, il doit offrir la possibilité de mettre en place une politique de sécurité permettant de les utiliser. La politique de sécurité doit au moins permettre de réaliser les actions suivantes pour chaque technologie de code mobile utilisée sur l'appareil hôte:

a) exécution de contrôle du code mobile;

b) contrôler les utilisateurs (êtres humains, processus logiciels ou appareils) autorisés à télécharger le code mobile vers l'appareil hôte; et

c) contrôler l'exécution du code mobile d'après les contrôles d'intégrité avant d'exécuter le code.

14.2.2 Justification et recommandations complémentaires

Les technologies de code mobile incluent, entre autres, Java, JavaScript, ActiveX, Portable Document Format (PDF), Postscript, les films Shockwave, les animations Flash et VBScript. L'utilisation de restrictions s'applique au choix et à l'utilisation du code mobile installé sur les serveurs et au code mobile téléchargé et exécuté sur des postes individuels. Il convient que les procédures de contrôle empêchent le développement, l'acquisition ou l'introduction de code mobile inacceptable au sein du système de commande dans lequel réside l'appareil hôte. Par exemple, les échanges de code mobile peuvent être désactivés directement avec le système de commande, mais peuvent être admis dans un environnement adjacent contrôlé géré par le personnel IACS.

Le code mobile peut être sécurisé en y ajoutant des contrôles d'intégrité, d'authenticité et d'autorisation (couche d'application). L'exécution du code «juste-à-temps» peut être sécurisée en transmettant le code mobile par un tunnel sûr de communication qui fournit ces attributs. Tout mécanisme équivalant à ces options peut également être utilisé.

14.2.3 Amélioration d'exigences

(1) Contrôle d'authenticité du code mobile

L'appareil hôte doit offrir la possibilité d'appliquer une politique de sécurité permettant à l'appareil de contrôler l'exécution du code mobile d'après les résultats d'un contrôle d'authenticité avant d'exécuter le code.

14.2.4 Niveaux de sécurité

Les exigences pour les quatre niveaux de sécurité SL liés à HDR 2.4 sont les suivantes:

- SL-C(UC, composant) 1: HDR 2.4
- SL-C(UC, composant) 2: HDR 2.4 (1)
- SL-C(UC, composant) 3: HDR 2.4 (1)
- SL-C(UC, composant) 4: HDR 2.4 (1)

14.3 HDR 2.13 – Utilisation d'interfaces physiques de diagnostic et d'essai

14.3.1 Exigences

Les appareils hôtes doivent assurer une protection contre l'utilisation non autorisée des interfaces physiques de diagnostic et d'essai en usine (débogage JTAG, par exemple).

14.3.2 Justification et recommandations complémentaires

Les interfaces de diagnostic et d'essai en usine sont créées à différents endroits dans l'appareil hôte. Elles visent à aider les développeurs de composant et le personnel à soumettre la mise en œuvre à l'essai, et si des erreurs sont détectées, à les éliminer du composant. Toutefois, il convient de protéger soigneusement ces mêmes interfaces contre tout accès par des entités non autorisées afin de protéger les fonctionnalités essentielles fournies par le composant à l'IACS.

Dans certains cas, les interfaces de diagnostic et d'essai en usine peuvent utiliser les communications réseau avec l'appareil. Si c'est le cas, ces interfaces doivent satisfaire à toutes les exigences du présent document.

Si une interface de diagnostic et d'essai n'offre pas la possibilité de contrôler l'appareil hôte ou d'accéder aux informations non publiques, elle ne nécessite pas de mécanisme d'authentification. Ceci doit être déterminé par une appréciation des menaces et des risques, telle que le débogage JTAG, qui utilise JTAG pour contrôler le processeur et exécuter les commandes arbitraires, par rapport au registre à décalage périphérique JTAG, qui utilise JTAG pour lire simplement les informations (qui peuvent être des informations accessibles au public).

14.3.3 Amélioration d'exigences

(1) Surveillance active

Les appareils hôtes doivent assurer la surveillance active des interfaces de diagnostic et d'essai de l'appareil et générer une entrée de journal d'audit si une tentative d'accès à ces interfaces a été détectée.

14.3.4 Niveaux de sécurité

Les exigences pour les quatre niveaux de sécurité SL liés à HDR 2.13 sont les suivantes:

- SL-C(SI, composant) 1: Non choisi
- SL-C(SI, composant) 2: HDR 2.13
- SL-C(SI, composant) 3: HDR 2.13 (1)
- SL-C(SI, composant) 4: HDR 2.13 (1)

14.4 HDR 3.2 – Protection contre les programmes malveillants

14.4.1 Exigences

Les appareils hôtes doivent comporter des mécanismes homologués par le fournisseur de produit IACS assurant la protection contre les programmes malveillants. Le fournisseur de produit IACS doit documenter toutes les exigences de configuration particulières relatives à la protection contre les programmes malveillants.

14.4.2 Justification et recommandations complémentaires

Il est nécessaire que les appareils hôtes assurent la protection contre les programmes malveillants (virus, vers informatiques, chevaux de Troie et logiciels espions, par exemple). Il convient que le fournisseur de produit choisisse et documente la configuration de la protection contre les mécanismes de programme malveillant de manière à maintenir la mission principale du système de commande.

14.4.3 Amélioration d'exigences

(1) Consigner la version de la protection contre le programme

L'appareil hôte doit consigner automatiquement les versions des logiciels et fichiers utilisés à des fins de protection contre les programmes malveillants (dans le cadre de la fonction de journalisation globale).

14.4.4 Niveaux de sécurité

Les exigences pour les quatre niveaux de sécurité SL liés à HDR 3.2 sont les suivantes:

- SL-C(SI, composant) 1: HDR 3.2
- SL-C(SI, composant) 2: HDR 3.2 (1)
- SL-C(SI, composant) 3: HDR 3.2 (1)
- SL-C(SI, composant) 4: HDR 3.2 (1)

14.5 HDR 3.10 – Support pour les mises à jour

14.5.1 Exigences

Les appareils hôtes doivent offrir la possibilité d'être mis à jour et mis à niveau.

14.5.2 Justification et recommandations complémentaires

Pendant toute leur durée de vie, les appareils hôtes peuvent avoir besoin de mises à jour et de mises à niveau. Dans certains cas, les appareils hôtes prennent en charge ou exécutent également des fonctions essentielles. Si c'est le cas, il convient que l'appareil hôte comporte des mécanismes d'application de correctifs et de mise à jour n'ayant aucun impact sur les fonctions essentielles des systèmes à haute disponibilité (voir 4.2). Il s'agit, par exemple, d'assurer la redondance au sein de l'appareil hôte.

14.5.3 Amélioration d'exigences

(1) Mettre à jour l'authenticité et l'intégrité

L'appareil hôte doit valider l'authenticité et l'intégrité d'une mise à jour ou d'une mise à niveau d'un logiciel avant de l'installer.

14.5.4 Niveaux de sécurité

Les exigences pour les quatre niveaux de sécurité SL liés à HDR 3.10 sont les suivantes:

- SL-C(SI, composant) 1: HDR 3.10
- SL-C(SI, composant) 2: HDR 3.10 (1)
- SL-C(SI, composant) 3: HDR 3.10 (1)
- SL-C(SI, composant) 4: HDR 3.10 (1)

14.6 HDR 3.11 – Résistance aux violations physiques et détection

14.6.1 Exigences

Les appareils hôtes doivent offrir la possibilité de prendre en charge des mécanismes de résistance et de détection des violations pour assurer une protection contre les accès physiques non autorisés dans l'appareil.

14.6.2 Justification et recommandations complémentaires

Les mécanismes de résistance aux violations ont pour objet d'empêcher un attaquant d'exécuter une action physique non autorisée contre un appareil IACS. Outre la prévention, la détection et la réponse sont essentielles en cas de manipulation frauduleuse.

Les mécanismes de résistance aux violations sont plus efficaces lorsqu'ils sont combinés pour empêcher l'accès à l'un des composants cruciaux. La résistance aux violations consiste à utiliser des matériaux spécialisés pour rendre difficile la manipulation frauduleuse d'un appareil ou d'un module. Il peut s'agir de boîtiers renforcés, de verrous, d'encapsulation ou de vis de sécurité. Des trajectoires de circulation d'air tendues rendent plus difficile l'accès aux éléments internes du produit.

Le témoin d'intégrité a pour objet d'apporter la preuve visible ou électronique d'une manipulation frauduleuse. De nombreuses techniques consistent à utiliser des scellés pour mettre en évidence toute tentative de violation physique. Les commutateurs sont des techniques plus sophistiquées.

14.6.3 Amélioration d'exigences

(1) Notification d'une tentative de violation

Les appareils hôtes doivent être en mesure d'informer automatiquement un ensemble configurable de destinataires d'une tentative d'accès physique non autorisée. Toutes les notifications de violation doivent être consignées dans le cadre de la fonction de journalisation globale d'audit.

14.6.4 Niveaux de sécurité

Les exigences pour les quatre niveaux de sécurité SL liés à HDR 3.11 sont les suivantes:

- SL-C(SI, composant) 1: Non choisi
- SL-C(SI, composant) 2: HDR 3.11
- SL-C(SI, composant) 3: HDR 3.11 (1)
- SL-C(SI, composant) 4: HDR 3.11 (1)

14.7 HDR 3.12 – Fourniture des racines de confiance du fournisseur de produit

14.7.1 Exigences

Les appareils hôtes doivent offrir la possibilité d'assurer et de protéger la confidentialité, l'intégrité et l'authenticité des clés et des données du fournisseur de produit à utiliser comme une ou plusieurs «racines de confiance» au moment de la fabrication de l’appareil.

14.7.2 Justification et recommandations complémentaires

Pour qu'un composant soit en mesure de valider l'authenticité et l'intégrité du matériel, du logiciel et des données fournies par le fournisseur de produit, il convient qu’il comporte une source de données digne de confiance pour exécuter le processus de validation. Cette source de données digne de confiance est appelée «racine de confiance» pour le système. Cette source de données digne de confiance peut être un ensemble d'empreintes numériques de logiciels «corrects connus» ou peut être la partie publique d'une paire de clés cryptographiques asymétriques à utiliser dans la validation des signatures cryptographiques. Ces données dignes de confiance sont souvent utilisées pour valider les logiciels, micrologiciels indispensables et données cruciales avant l'amorçage du micrologiciel ou du système d'exploitation d'un composant, afin de valider le fait que le composant s'amorcera à un état «correct connu» dans lequel tous les mécanismes de sécurité sont réputés être opérationnels et parfaitement sûrs. Les données «racines de confiance» peuvent être protégées par des mécanismes logiciels ou matériels, ce qui empêche de les modifier pendant le fonctionnement normal du composant. La modification des données «racines de confiance» du fournisseur de produit se limite en général au processus de provisionnement du fournisseur de produit, ce dernier disposant d'un processus digne de confiance permettant de mettre les données à disposition. Les informations à valider par rapport à la racine de confiance sont plutôt soumises au processus de validation par l'intermédiaire d'une API matérielle ou logicielle qui procède à la validation et renvoie les résultats sans exposer les données protégées.

14.7.3 Amélioration d'exigences

Aucune

14.7.4 Niveaux de sécurité

Les exigences pour les quatre niveaux de sécurité SL liés à HDR 3.12 sont les suivantes:

- SL-C(SI, composant) 1: Non choisi
- SL-C(SI, composant) 2: HDR 3.12
- SL-C(SI, composant) 3: HDR 3.12
- SL-C(SI, composant) 4: HDR 3.12

14.8 HDR 3.13 – Fourniture des racines de confiance du propriétaire d'actif

14.8.1 Exigences

Les appareils hôtes doivent

a) offrir la possibilité d'assurer et de protéger la confidentialité, l'intégrité et l'authenticité des clés et des données du propriétaire d'actif à utiliser comme «racines de confiance»; et

b) assurer la mise à disposition sans recourir aux composants qui peuvent se trouver hors de la zone de sécurité de l’appareil.

14.8.2 Justification et recommandations complémentaires

Les fournisseurs de produits ont mis en place des mécanismes visant à assurer l'authenticité des logiciels et micrologiciels présents sur leur composant et à vérifier que leur intégrité n'a pas été compromise. Cela permet au fournisseur de produit d'assurer au propriétaire d'actif un état «correct connu» à partir duquel opérer. Toutefois, de nombreux fournisseurs de produits proposent également des mécanismes permettant aux propriétaires d'actif d'étendre les fonctionnalités de leurs appareils par l'utilisation d'un code mobile, de programmes utilisateur ou d'autres moyens de même type. Pour protéger la sécurité du composant, il est également important de valider ces extensions de fonctionnalités de manière à assurer qu'elles sont autorisées et que le propriétaire d'actif a approuvé leur origine.

Pour procéder à ces validations, il convient que le composant contienne des données offrant un moyen de différencier les origines valides de celles qui ne le sont pas. La liste des origines valides et non valides diffère d'un propriétaire d'actif à l'autre, et il est peu probable qu'un fournisseur de produit dispose de la liste exhaustive de toutes les origines valides possibles au moment de la fabrication. Par conséquent, il est important que le fournisseur de produit propose au propriétaire d'actif un moyen de mettre à disposition ses propres «racines de confiance» en toute sécurité, offrant la possibilité de différencier les origines admises par la politique de sécurité du propriétaire d'actif de celles qui ne le sont pas. Il convient de protéger l'authenticité et l'intégrité de ces «racines de confiance» de sorte que des personnes malveillantes ne puissent pas ajouter d'autres racines de confiance leur donnant la possibilité de faire fonctionner le composant.

Des exigences comme celles de HDR 2.4 – Code mobile (11.2) exigent que le composant contrôle l'authenticité du code mobile avant de l'exécuter. Les racines de confiance faisant l'objet de cette exigence fournissent les données nécessaires à la validation de l'origine et de l'intégrité du code mobile, permettant au composant de déterminer en toute indépendance si l’exécution du code est admise.

Une racine de confiance peut également être utilisée comme base pour la sécurité des communications, telle que l’intégrité de la communication exigée par CR 3.1 – Intégrité de la communication (7.3) ou la confidentialité des communications exigée par CR 4.1 – Confidentialité des informations (8.3).

14.8.3 Amélioration d'exigences

Aucune

14.8.4 Niveaux de sécurité

Les exigences pour les quatre niveaux de sécurité SL liés à HDR 3.13 sont les suivantes:

- SL-C(SI, composant) 1: Non choisi
- SL-C(SI, composant) 2: HDR 3.13
- SL-C(SI, composant) 3: HDR 3.13
- SL-C(SI, composant) 4: HDR 3.13

14.9 HDR 3.14 – Intégrité du processus d'amorçage

14.9.1 Exigences

Les appareils hôtes doivent vérifier l'intégrité des micrologiciels, des logiciels et des données de configuration nécessaires au processus d'amorçage du composant avant de les utiliser dans ce processus.

14.9.2 Justification et recommandations complémentaires

Pour donner l'assurance à un propriétaire d'actif que les fonctions de sécurité d'un composant n'ont pas été compromises, il est nécessaire d'assurer que les logiciels et micrologiciels du composant n'ont pas été manipulés de manière frauduleuse et qu'ils sont valides pour fonctionner sur le composant. Par conséquent, il convient que le composant procède aux contrôles pour vérifier l'intégrité et l'authenticité de ses micrologiciels et/ou logiciels avant le processus d'amorçage, afin d'assurer qu'il ne s'amorce pas dans un état de fonctionnement non sécurisé ou non valide qui pourrait l'endommager ou permettre à une personne malveillante d'accéder à d'autres composants, actifs ou données.

14.9.3 Amélioration d'exigences

(1) Authenticité du processus d'amorçage

Les appareils hôtes doivent utiliser les racines de confiance du fournisseur de produit du composant pour vérifier l’authenticité des micrologiciels, des logiciels et des données de configuration nécessaires au processus d'amorçage du composant avant de les utiliser dans ce processus.

14.9.4 Niveaux de sécurité

Les exigences pour les quatre niveaux de sécurité SL liés à HDR 3.14 sont les suivantes:

- SL-C(SI, composant) 1: HDR 3.14
- SL-C(SI, composant) 2: HDR 3.14 (1)
- SL-C(SI, composant) 3: HDR 3.14 (1)
- SL-C(SI, composant) 4: HDR 3.14 (1)

15 Exigences relatives aux appareils de réseaux

15.1 Objet

Cet ensemble d'exigences a pour objet de documenter les exigences spécifiques aux appareils de réseaux.

15.2 NDR 1.6 – Gestion des accès sans fil

15.2.1 Exigences

Un appareil de réseau qui prend en charge la gestion des accès sans fil doit offrir la possibilité d'identifier et d'authentifier tous les utilisateurs (êtres humains, processus logiciels ou appareils) qui participent à la communication sans fil.

15.2.2 Justification et recommandations complémentaires

Une technologie sans fil peut, et il convient qu'elle le soit dans la plupart des cas, être considérée comme une autre option de protocole de communication. Ainsi, il convient qu'elle fasse l'objet des mêmes exigences de sécurité IACS que les autres types de communication utilisés par l'IACS. Toutefois, du point de vue de la sécurité, il existe au moins une différence de taille entre les communications câblées et les communications sans fil. Les contre-mesures physiques de sécurité sont en général moins efficaces avec les communications sans fil.

15.2.3 Amélioration d'exigences

(1) Identification et authentification uniques

L'appareil de réseau doit offrir la possibilité d'identifier et d'authentifier de manière unique tous les utilisateurs (êtres humains, processus logiciels ou appareils) qui participent à la communication sans fil.

15.2.4 Niveaux de sécurité

Les exigences pour les quatre niveaux de sécurité SL liés à NDR 1.6 sont les suivantes:

- SL-C(UC, composant) 1: NDR 1.6
- SL-C(UC, composant) 2: NDR 1.6 (1)
- SL-C(UC, composant) 3: NDR 1.6 (1)
- SL-C(UC, composant) 4: NDR 1.6 (1)

15.3 NDR 1.13 – Accès par l'intermédiaire de réseaux non sécurisés

15.3.1 Exigences

L'appareil de réseau qui prend en charge l'accès de l’appareil dans un réseau doit offrir la possibilité de surveiller et de contrôler tous les modes d'accès à l'appareil de réseau par l’intermédiaire de réseaux non sécurisés.

15.3.2 Justification et recommandations complémentaires

Il convient de protéger l’appareil de réseau contre les connexions non autorisées ou la subversion de connexions autorisées.

Les méthodes d'accès distant par des réseaux non sécurisés (par ligne commutée, à large bande et sans fil, par exemple) et les connexions à partir d'un réseau d'entreprise (système non contrôlé) sont des exemples d'accès à l'appareil de réseau par l'intermédiaire de réseaux non sécurisés. L’appareil de réseau peut offrir une fonctionnalité de liste de contrôle d’accès (ACL) pour limiter l’accès par:

Appareils d'acheminement de la couche 2 tels que les commutateurs Ethernet:

- adresse MAC
- VLAN

Appareils d'acheminement de la couche 3 tels que les routeurs, les passerelles et les pare-feu:

a) adresse IP
b) port et protocole
c) réseaux privés virtuels

15.3.3 Amélioration d'exigences

(1) Approbation de demande d'accès explicite

L'appareil de réseau doit offrir la possibilité de refuser les demandes d'accès par l'intermédiaire de réseaux non sécurisés, sauf si elles sont explicitement approuvées par un rôle assigné.

15.3.4 Niveaux de sécurité

Les exigences pour les quatre niveaux de sécurité liés à NDR 1.13 sont les suivantes:

- SL-C(UC, composant) 1: NDR 1.13
- SL-C(UC, composant) 2: NDR 1.13
- SL-C(UC, composant) 3: NDR 1.13 (1)
- SL-C(UC, composant) 4: NDR 1.13 (1)

15.4 NDR 2.4 – Code mobile

15.4.1 Exigences

Si un appareil de réseau utilise des technologies de code mobile, il doit offrir la possibilité de mettre en place une politique de sécurité permettant de les utiliser. La politique de sécurité doit au moins permettre de réaliser les actions suivantes pour chaque technologie de code mobile utilisée sur l'appareil de réseau:

a) exécution de contrôle du code mobile;
b) contrôler les utilisateurs (êtres humains, processus logiciels ou appareils) autorisés à transférer le code mobile vers/depuis l'appareil de réseau; et
c) contrôler l’exécution du code mobile d’après les contrôles d’intégrité avant d'exécuter le code.

15.4.2 Justification et recommandations complémentaires

Les technologies de code mobile incluent, entre autres, Java, JavaScript, ActiveX, Portable Document Format (PDF), Postscript, les films Shockwave, les animations Flash et VBScript. L'utilisation de restrictions s'applique au choix et à l'utilisation du code mobile installé sur les serveurs et au code mobile téléchargé et exécuté sur des postes individuels. Il convient que les procédures de contrôle empêchent le développement, l'acquisition ou l'introduction de code mobile inacceptable au sein du système de commande dans lequel réside le composant. Par exemple, les échanges de code mobile peuvent être désactivés directement dans le système de commande, mais peuvent être admis dans un environnement adjacent contrôlé géré par le personnel IACS.

Le code mobile peut être sécurisé en y ajoutant des contrôles d’intégrité, d’authenticité et d’autorisation (couche d’application). L’exécution du code «juste-à-temps» peut être sécurisée en transmettant le code mobile par un tunnel sûr de communication qui fournit ces attributs. Tout mécanisme équivalant à ces options peut également être utilisé.

15.4.3 Amélioration d'exigences

(1) Contrôle d’authenticité du code mobile

L’appareil de réseau doit offrir la possibilité d’appliquer une politique de sécurité permettant à l’appareil de contrôler l’exécution du code mobile d’après les résultats d’un contrôle d’authenticité avant d’exécuter le code.

15.4.4 Niveaux de sécurité

Les exigences pour les quatre niveaux de sécurité SL liés à NDR 2.4 sont les suivantes:

- SL-C(UC, composant) 1: NDR 2.4
- SL-C(UC, composant) 2: NDR 2.4 (1)
- SL-C(UC, composant) 3: NDR 2.4 (1)
- SL-C(UC, composant) 4: NDR 2.4 (1)

15.5 NDR 2.13 – Utilisation d'interfaces physiques de diagnostic et d'essai

15.5.1 Exigences

Les appareils de réseaux doivent assurer une protection contre l'utilisation non autorisée des interfaces physiques de diagnostic et d'essai en usine (débogage JTAG, par exemple).

15.5.2 Justification et recommandations complémentaires

Les interfaces de diagnostic et d'essai en usine sont créées à différents endroits dans le composant. Elles visent à aider les développeurs de composant et le personnel à soumettre la mise en œuvre à l'essai, et si des erreurs sont détectées, à les éliminer du composant. Toutefois, il convient de protéger soigneusement ces mêmes interfaces contre tout accès par des entités non autorisées afin de protéger les fonctionnalités essentielles fournies par le composant à l'IACS.

Dans certains cas, les interfaces de diagnostic et d'essai en usine peuvent utiliser les communications réseau avec l'appareil. Si c'est le cas, ces interfaces doivent satisfaire à toutes les exigences du présent document.

Il est à noter que si une interface de diagnostic et d'essai n'offre pas la possibilité de contrôler le produit ou d'accéder aux informations non publiques, elle ne nécessite pas de mécanisme d'authentification. Il convient de déterminer cela par une appréciation des menaces, telle que le débogage JTAG, qui utilise JTAG pour contrôler le processeur et exécuter les commandes arbitraires, par rapport au registre à décalage périphérique JTAG, qui utilise JTAG pour lire simplement les informations (qui peuvent être des informations accessibles au public).

15.5.3 Amélioration d'exigences

(1) Surveillance active

Les appareils de réseaux doivent assurer la surveillance active des interfaces de diagnostic et d'essai de l'appareil et générer une entrée de journal d'audit si une tentative d'accès à ces interfaces a été détectée.

15.5.4 Niveaux de sécurité

Les exigences pour les quatre niveaux de sécurité SL liés à NDR 2.13 sont les suivantes:

- SL-C(SI, composant) 1: Non choisi
- SL-C(SI, composant) 2: NDR 2.13
- SL-C(SI, composant) 3: NDR 2.13 (1)
- SL-C(SI, composant) 4: NDR 2.13 (1)

15.6 NDR 3.2 – Protection contre les programmes malveillants

15.6.1 Exigences

L'appareil de réseau doit assurer la protection contre les programmes malveillants.

15.6.2 Justification et recommandations complémentaires

Si un appareil de réseau est en mesure d'utiliser un contrôle compensatoire, il ne nécessite pas directement d'assurer la protection contre les programmes malveillants. Un type de contrôle compensatoire consisterait à utiliser des appareils de filtrage de paquet réseau pour identifier et éliminer les programmes malveillants pendant le transit. L'IACS est présumé être chargé de fournir les protections exigées. Toutefois, dans certains cas (en présence d'un accès hôte USB local, par exemple), il convient d'évaluer la nécessité d'une protection contre les programmes malveillants.

15.6.3 Amélioration d'exigences

Aucune

15.6.4 Niveaux de sécurité

Les exigences pour les quatre niveaux de sécurité SL liés à NDR 3.2 sont les suivantes:

- SL-C(SI, composant) 1: NDR 3.2
- SL-C(SI, composant) 2: NDR 3.2
- SL-C(SI, composant) 3: NDR 3.2
- SL-C(SI, composant) 4: NDR 3.2

15.7 NDR 3.10 – Support pour les mises à jour

15.7.1 Exigences

Les appareils de réseaux doivent offrir la possibilité d'être mis à jour et mis à niveau.

15.7.2 Justification et recommandations complémentaires

Pendant toute leur durée de vie, les appareils de réseaux peuvent exiger des mises à jour et des mises à niveau. Dans certains cas, les appareils de réseaux prennent en charge ou exécutent également des fonctions essentielles. Si c'est le cas, il convient que l'appareil de réseau comporte des mécanismes d'application de correctifs et de mise à jour n'ayant aucun impact sur les fonctions essentielles des systèmes à haute disponibilité (4.2). Il s'agit, par exemple, d'assurer la redondance au sein de l'appareil de réseau.

15.7.3 Amélioration d'exigences

(1) Mettre à jour l'authenticité et l'intégrité

Les appareils de réseaux doivent valider l'authenticité et l'intégrité d'une mise à jour ou d'une mise à niveau d'un logiciel avant de l'installer.

15.7.4 Niveaux de sécurité

Les exigences pour les quatre niveaux de sécurité SL liés à NDR 3.10 sont les suivantes:

- SL-C(SI, composant) 1: NDR 3.10
- SL-C(SI, composant) 2: NDR 3.10 (1)
- SL-C(SI, composant) 3: NDR 3.10 (1)
- SL-C(SI, composant) 4: NDR 3.10 (1)

15.8 NDR 3.11 – Résistance aux violations physiques et détection

15.8.1 Exigences

Les appareils de réseaux doivent fournir des mécanismes de résistance et de détection des violations pour assurer une protection contre les accès physiques non autorisés dans l’appareil.

15.8.2 Justification et recommandations complémentaires

Les mécanismes de résistance aux violations ont pour objet d'empêcher un attaquant d'exécuter une action physique non autorisée contre un appareil IACS. Outre la prévention, la détection et la réponse sont essentielles en cas de manipulation frauduleuse.

Les mécanismes de résistance aux violations sont plus efficaces lorsqu'ils sont combinés pour empêcher l'accès à l'un des composants cruciaux. La résistance aux violations consiste à utiliser des matériaux spécialisés pour rendre difficile la manipulation frauduleuse d'un appareil ou d'un module. Il peut s'agir de boîtiers renforcés, de verrous, d'encapsulation ou de vis de sécurité. Des trajectoires de circulation d'air tendues rendent plus difficile l'accès aux éléments internes du produit.

Le témoin d'intégrité a pour objet d'apporter la preuve visible ou électronique d'une manipulation frauduleuse. De nombreuses techniques consistent à utiliser des scellés pour mettre en évidence toute tentative de violation physique. Les commutateurs sont des techniques plus sophistiquées.

15.8.3 Amélioration d'exigences

(1) Notification d'une tentative de violation

Les appareils de réseaux doivent être en mesure d'informer automatiquement un ensemble configurable de destinataires d'une tentative d'accès physique non autorisée. Toutes les notifications de violation doivent être consignées dans le cadre de la fonction de journalisation globale d'audit.

15.8.4 Niveaux de sécurité

Les exigences pour les quatre niveaux de sécurité SL liés à NDR 3.11 sont les suivantes:

- SL-C(SI, composant) 1: Non choisi
- SL-C(SI, composant) 2: NDR 3.11
- SL-C(SI, composant) 3: NDR 3.11 (1)
- SL-C(SI, composant) 4: NDR 3.11 (1)

15.9 NDR 3.12 – Fourniture des racines de confiance du fournisseur de produit

15.9.1 Exigences

Les appareils de réseaux doivent offrir la possibilité d'assurer et de protéger la confidentialité, l'intégrité et l'authenticité des clés et des données du fournisseur de produit à utiliser comme une ou plusieurs «racines de confiance» au moment de la fabrication de l’appareil.

15.9.2 Justification et recommandations complémentaires

Pour qu'un composant soit en mesure de valider l'authenticité et l'intégrité du matériel, du logiciel et des données fournies par le fournisseur de produit, il convient qu’il dispose d'une source de données digne de confiance pour exécuter le processus de validation. Cette source de données digne de confiance est appelée «racine de confiance» pour le système. Cette source de données digne de confiance peut être un ensemble d'empreintes numériques de logiciels «corrects connus» ou peut être la partie publique d'une paire de clés cryptographiques asymétriques à utiliser dans la validation des signatures cryptographiques.

Ces données dignes de confiance sont souvent utilisées pour valider les logiciels, micrologiciels indispensables et données cruciales avant l'amorçage du micrologiciel ou du système d'exploitation d'un composant, afin de valider le fait que le composant s'amorcera à un état «correct connu» dans lequel tous les mécanismes de sécurité sont réputés être opérationnels et parfaitement sûrs. Les données «racines de confiance» sont souvent protégées par des mécanismes logiciels ou matériels, ce qui empêche de les modifier pendant le fonctionnement normal du composant. La modification des données «racines de confiance» du fournisseur de produit se limite en général au processus de provisionnement du fournisseur de produit, ce dernier disposant d'un processus digne de confiance permettant de mettre les données à disposition. Les informations à valider par rapport à la racine de confiance sont plutôt soumises au processus de validation par l'intermédiaire d'une API matérielle ou logicielle qui procède à la validation et renvoie les résultats sans exposer les données protégées.

15.9.3 Amélioration d'exigences

Aucune

15.9.4 Niveaux de sécurité

Les exigences pour les quatre niveaux de sécurité SL liés à NDR 3.12 sont les suivantes:

- SL-C(SI, composant) 1: Non choisi
- SL-C(SI, composant) 2: NDR 3.12
- SL-C(SI, composant) 3: NDR 3.12
- SL-C(SI, composant) 4: NDR 3.12

15.10 NDR 3.13 – Fourniture des racines de confiance du propriétaire d'actif

15.10.1 Exigences

Les appareils de réseaux doivent

a) offrir la possibilité d'assurer et de protéger la confidentialité, l'intégrité et l'authenticité des clés et des données du propriétaire d'actif à utiliser comme «racines de confiance»; et

b) assurer la mise à disposition sans recourir aux composants qui peuvent se trouver hors de la zone de sécurité de l’appareil.

15.10.2 Justification et recommandations complémentaires

Les fournisseurs de produits ont mis en place des mécanismes visant à assurer l'authenticité des logiciels et micrologiciels présents sur leur composant et à vérifier que leur intégrité n’a pas été compromise. Cela permet au fournisseur de produit d'assurer au propriétaire d'actif un état «correct connu» à partir duquel opérer. Toutefois, de nombreux fournisseurs de produits proposent également des mécanismes permettant aux propriétaires d'actif d'étendre les fonctionnalités de leurs appareils par l'utilisation d'un code mobile, de programmes utilisateur ou d'autres moyens de même type. Pour protéger la sécurité du composant, il est également important de valider ces extensions de fonctionnalités de manière à assurer qu'elles sont autorisées et que le propriétaire d'actif a approuvé leur origine.

Pour procéder à ces validations, il convient que le composant contienne des données offrant un moyen de différencier les origines valides de celles qui ne le sont pas. La liste des origines valides et non valides diffère d'un propriétaire d'actif à l'autre, et il est peu probable qu'un fournisseur de produit dispose de la liste exhaustive de toutes les origines valides possibles au moment de la fabrication. Par conséquent, il est important que le fournisseur de produit propose au propriétaire d'actif un moyen de mettre à disposition ses propres «racines de confiance» en toute sécurité, offrant la possibilité de différencier les origines admises par la politique de sécurité du propriétaire d'actif de celles qui ne le sont pas. Il convient de protéger l'authenticité et l'intégrité de ces «racines de confiance» de sorte que des personnes

malveillantes ne puissent pas ajouter d'autres racines de confiance leur donnant la possibilité de faire fonctionner le composant.

Des exigences comme celles de NDR 2.4 – Code mobile (1) exigent que le composant contrôle l'authenticité du code mobile avant de l'exécuter. Les racines de confiance faisant l'objet de cette exigence fournissent les données nécessaires à la validation de l'origine et de l'intégrité du code mobile, permettant au composant de déterminer en toute indépendance si l'exécution du code est admise.

Une racine de confiance peut également être utilisée comme base pour la sécurité des communications (7.3), telle que l'intégrité de la communication exigée par CR 3.1 – Intégrité de la communication ou la confidentialité des communications exigée par CR 4.1 – Confidentialité des informations (8.3).

15.10.3 Amélioration d'exigences

Aucune

15.10.4 Niveaux de sécurité

Les exigences pour les quatre niveaux de sécurité SL liés à NDR 3.13 sont les suivantes:

- SL-C(SI, composant) 1: Non choisi
- SL-C(SI, composant) 2: NDR 3.13
- SL-C(SI, composant) 3: NDR 3.13
- SL-C(SI, composant) 4: NDR 3.13

15.11 NDR 3.14 – Intégrité du processus d'amorçage

15.11.1 Exigences

Les appareils de réseaux doivent vérifier l'intégrité des micrologiciels, des logiciels et des données de configuration nécessaires au processus d'amorçage du composant avant de les utiliser dans ce processus.

15.11.2 Justification et recommandations complémentaires

Pour donner l'assurance à un propriétaire d'actif que les fonctions de sécurité d'un composant n'ont pas été compromises, il est nécessaire d'assurer que les logiciels et micrologiciels du composant n'ont pas été manipulés de manière frauduleuse et qu'ils sont valides pour fonctionner sur le composant. Par conséquent, il convient que le composant procède aux contrôles pour vérifier l'intégrité et l'authenticité de ses micrologiciels et/ou logiciels avant le processus d'amorçage, afin d'assurer qu'il ne s'amorce pas dans un état de fonctionnement non sécurisé ou non valide qui pourrait l'endommager ou permettre à une personne malveillante d'accéder à d'autres composants, actifs ou données.

15.11.3 Amélioration d'exigences

(1) Authenticité du processus d'amorçage

Les appareils de réseaux doivent utiliser les racines de confiance du fournisseur de produit du composant pour vérifier l'authenticité des micrologiciels, des logiciels et des données de configuration nécessaires au processus d'amorçage du composant avant de les utiliser dans ce processus.

15.11.4 Niveaux de sécurité

Les exigences pour les quatre niveaux de sécurité SL liés à NDR 3.14 sont les suivantes:

- SL-C(SI, composant) 1: NDR 3.14

- SL-C(SI, composant) 2: NDR 3.14 (1)
- SL-C(SI, composant) 3: NDR 3.14 (1)
- SL-C(SI, composant) 4: NDR 3.14 (1)

15.12 NDR 5.2 – Protection des limites de zone

15.12.1 Exigences

Un appareil de réseau à une limite de zone doit offrir la possibilité de surveiller et contrôler les communications au niveau des limites de zone pour mettre en place le cloisonnement défini dans le modèle de zones et de conduits basé sur le risque.

15.12.2 Justification et recommandations complémentaires

Il convient que toutes les connexions vers l'extérieur de chaque zone de sécurité aient lieu par l'intermédiaire d'interfaces gérées composées d’appareils de protection des limites appropriés (proxies, passerelles, routeurs, pare-feu, passerelles unidirectionnelles, protections et tunnels chiffrés, par exemple) disposés dans une architecture efficace (les pare-feu protégeant les passerelles d'application résidant dans une zone démilitarisée, par exemple). Il convient que les protections des limites du système de commande au niveau d'autres sites de traitement désignés offrent les mêmes niveaux de protection que ceux du site principal.

15.12.3 Amélioration d'exigences

(1) Refuser tout, autoriser par exception

Le composant de réseau doit offrir la possibilité de refuser le trafic du réseau par défaut et d'autoriser le trafic du réseau par exception (également appelé «refuser tout, autoriser par exception»).

(2) Mode insulaire

Le composant de réseau doit offrir la possibilité d’assurer une protection contre toute communication par la limite du système de commande (également appelée «mode insulaire»).

NOTE 1 Cette capacité peut être utilisée, par exemple, si une violation et/ou une brèche de sécurité a été détectée à l'intérieur du système de commande ou en cas d'attaque au niveau de l'entreprise.

(3) Fermeture en cas d'échec

Le composant de réseau doit offrir la possibilité d'empêcher d’assurer une protection contre toute communication par la limite du système de commande en cas de défaillance opérationnelle des mécanismes de protection des limites (également appelée «fermeture en cas d'échec»).

NOTE 2 Cette capacité peut être utilisée, par exemple, si une défaillance matérielle ou une défaillance de réseau provoque le fonctionnement en mode dégradé ou la totale défaillance des appareils de protection des limites.

15.12.4 Niveaux de sécurité

Les exigences pour les quatre niveaux de sécurité liés à NDR 5.2 sont les suivantes:

- SL-C(SI, composant) 1: NDR 5.2
- SL-C(SI, composant) 2: NDR 5.2 (1)
- SL-C(SI, composant) 3: NDR 5.2 (1) (2) (3)
- SL-C(SI, composant) 4: NDR 5.2 (1) (2) (3)

15.13 NDR 5.3 – Restrictions des communications entre des personnes d'ordre général

15.13.1 Exigences

Un appareil de réseau au niveau d'une limite de zone doit offrir la possibilité d’assurer une protection contre la réception de messages entre des personnes d'ordre général de la part d'utilisateurs ou de systèmes extérieurs au système de commande.

15.13.2 Justification et recommandations complémentaires

Les systèmes de communication entre des personnes d'ordre général incluent, entre autres, les systèmes de messagerie électronique, les formulaires sur les médias sociaux (Twitter, Facebook, galeries de photos, etc.) ou les systèmes de messagerie permettant d'envoyer tout type de fichier exécutable. En général, ces systèmes sont utilisés dans le cadre privé, sans lien avec les opérations du système de commande, les risques que représentent ces systèmes l'emportant donc en principe sur tous les avantages perçus.

Ces types de systèmes de communication d'ordre général sont souvent les vecteurs d'attaque visant à introduire des logiciels malveillants dans le système de commande, à extraire du système de commande des informations faisant l'objet d'autorisations de lecture et à introduire une charge de réseau excessive pour pouvoir créer des problèmes de sécurité ou attaquer le système de commande.

Les appareils de réseaux peuvent mettre en place ces restrictions, par exemple, en bloquant des communications spécifiques en fonction des numéros de port et de l'adresse source et/ou cible, et par des contrôles plus approfondis réalisés par les pare-feu de couche d'application.

15.13.3 Amélioration d'exigences

Aucune

15.13.4 Niveaux de sécurité

Les exigences pour les quatre niveaux de sécurité SL liés à NDR 5.3 sont les suivantes:

- SL-C(SI, composant) 1: NDR 5.3
- SL-C(SI, composant) 2: NDR 5.3
- SL-C(SI, composant) 3: NDR 5.3
- SL-C(SI, composant) 4: NDR 5.3

Annexe A
(informative)

Catégories d’appareils

A.1 Généralités

Les appareils décrits dans les catégories qui suivent sont donnés à titre d’échantillons représentatifs pour chaque catégorie et ne constituent pas une liste exhaustive.

A.2 Catégorie d’appareil: appareil intégré

A.2.1 Automate programmable (PLC)

Le terme «automate programmable» est étendu de l'IEC 60050-351:2013, 351-47-22 [14] est souvent utilisé dans les industries de transformation et les industries de travail en discontinu. Un PLC est un appareil qui réside en général aux niveaux inférieurs du système d'automatisation (le niveau 1 et le niveau 2 de l'architecture de référence PERA (Purdue Enterprise Reference Architecture) de l'ANSI/ISA-95.00.01 [15], par exemple). En règle générale, les PLC utilisent un matériel renforcé adapté au fonctionnement dans des environnements industriels et reposent souvent sur des systèmes d'exploitation en temps réel (RTOS) commerciaux. Les capteurs et actionneurs de plus en plus intelligents reçoivent également des formes de possibilités de commandes de processus. Les PLC et les capteurs/actionneurs intelligents sont programmés pour exécuter une logique de commande basée sur des entrées issues du processus (obtenues à partir d'instruments comme des capteurs types de température, de pression, de vibrations, etc.). La sortie de la logique de commande est utilisée pour commander le processus industriel (par l'intermédiaire d'actionneurs comme des soupapes, des pompes, etc.). La programmation est en général assurée par des logiciels d'ingénierie installés sur les appareils hôtes (ordinateurs portables ou PC, par exemple). L'IEC 61131-3 [13] présente un langage de programmation courant pour la logique de commande. Dans les systèmes plus importants, les PLC communiquent également souvent aux serveurs de niveau supérieur et/ou aux postes de travail de l'opérateur les conditions de processus obtenues auprès des capteurs, et reçoivent des instructions de la part des fonctions de commande de niveau supérieur ou des postes de travail de l'opérateur, qui sont traduites ou transférées aux actionneurs sous forme de commandes. Pour la communication avec les fonctions de niveau supérieur (serveurs de commande ou postes de travail de l'opérateur, par exemple), les PLC modernes utilisent les protocoles Ethernet et TCP/IP, alors que pour la communication avec les instruments, des bus de terrain conformes aux normes industrielles sont utilisés (dont certains sont également disponibles sur les porteuses Ethernet, mais n'utilisent en général pas la pile TCP/IP). Des PLC particuliers sont utilisés pour exécuter les fonctions de sécurité afin d’assurer que le processus commandé reste en permanence dans les limites d'un fonctionnement sécurisé. Il convient que les PLC, et plus particulièrement l’exécution des fonctions de sécurité, satisfassent aux exigences de temps réel dur et d'intégrité et disponibilité élevées.

A.2.2 Appareil électronique intelligent (IED)

Le terme «appareil électronique intelligent» est étendu de l'IEC TR 61850-1:2013, 3.1 [12] d'un point de vue conceptuel, un appareil électronique intelligent (IED) est très similaire à un PLC, mais le terme est plus souvent utilisé dans les systèmes d'alimentation (particulièrement en automatisation de poste). L’IED reçoit des mesurages depuis l’équipement d’alimentation (un transformateur, un commutateur ou un disjoncteur, par exemple) et exécute la logique de commande ou les fonctions de protection. Comme les PLC, les IED sont souvent programmés et paramétrés à l'aide de logiciels d'ingénierie installés sur les appareils hôtes (ordinateurs portables ou PC, par exemple). Un moyen normalisé moderne de décrire la configuration des IED et leurs fonctions est présenté dans l'IEC TR 61850-1. Le résultat de la logique exécutée par les IED est transmis aux actionneurs (commutateurs, disjoncteurs, etc.). À l'inverse des PLC, les IED comportent souvent également une IHM permettant à un utilisateur humain, face

à un IED, d'utiliser ses fonctionnalités (souvent un sous-ensemble nécessaire à la prise en charge des fonctions essentielles). De même, les postes, et donc les IED qu'ils utilisent, doivent être en mesure de fonctionner en isolement complet (sans communication avec les systèmes de niveau supérieur à l'extérieur du poste, voire sans communication avec d'autres IED, postes ou serveurs au niveau du poste). Les IED modernes utilisent en général les protocoles Ethernet et TCP/IP pour communiquer avec les composants de niveau supérieur, alors que la communication avec d'autres IED peut être assurée à l'aide de protocoles Ethernet (dans certains cas TCP/IP, souvent directement sur Ethernet) ou de bus de terrain (dont certains sont également disponibles sur des porteuses Ethernet, mais n'utilisent pas la pile TCP/IP). À l'instar des PLC, il convient que les IED satisfassent aux exigences de temps réel dur et d'intégrité et disponibilité élevées.

A.3 Catégorie d’appareil: appareil de réseau

A.3.1 Commutateur

Le terme «commutateur» est étendu de l'IEC 60050-732:2010, 732-01-12 [12] Un commutateur est un appareil dans les réseaux d'ordinateurs qui relie plusieurs segments de réseau ou nœuds de réseau. Un commutateur se trouve en général au niveau de la couche 2 (couche de liaison de données) du modèle OSI (voir l'ISO/IEC 7498-1 [8]). Les commutateurs modernes, et plus particulièrement ceux conçus pour être utilisés dans des réseaux plus larges, fournissent en général des interfaces pour la gestion de configuration et la gestion de réseau. Ces interfaces peuvent prendre en charge la configuration du commutateur (Web par HTTP/HTTPS, fichier par FTP/SFTP, ligne de commande par SSH ou par le protocole de gestion de réseau simple (SNMP), par exemple) et la gestion des journaux et des événements (par syslog, par exemple).

A.3.2 Terminateur RPV (réseau privé virtuel)

Le terme «réseau privé virtuel» est étendu de l'IEC 60050-732:2010, 732-01-10 [11] Les réseaux privés virtuels sont des réseaux logiques qui permettent d'étendre les réseaux privés sur des distances couvertes par les réseaux publics. L'utilisation du réseau public pour couvrir la distance est transparente/invisible pour les utilisateurs du RPV. Les RPV sont établis en créant un tunnel logique à la limite des deux segments du réseau privé. Le tunnel est établi par les terminateurs RPV, qui sont des appareils placés à la limite du réseau. Les paquets de données provenant d'un segment sont encapsulés (et souvent chiffrés) au niveau du terminateur RPV, puis envoyés par l'intermédiaire d'un réseau public au terminateur RPV homologue. Ici, l'encapsulation est retirée (ce qui implique en général un déchiffrement) et le paquet d'origine est récupéré et transféré dans le segment de réseau local. Les RPV sont également souvent utilisés pour permettre aux utilisateurs itinérants d'accéder en toute sécurité aux ressources de leur réseau domestique. Dans ce scénario, un logiciel client sur l’appareil itinérant fait office de terminateur RPV local, qui encapsule (et souvent déchiffre) tous les paquets de données et les transmet au terminateur RPV à la limite du réseau domestique. Il convient que l'établissement du tunnel entre les terminateurs RPV soit authentifié ce qui, dans le cas des utilisateurs itinérants, est souvent une authentification basée sur l'utilisateur. Ainsi, les terminateurs RPV peuvent être utilisés pour collecter des données relatives aux utilisateurs itinérants, ce qui peut permettre de suivre leur situation et d'autres données privées.

A.4 Catégorie d’appareil: appareil/application hôte

A.4.1 Poste de travail de l'opérateur

Les postes de travail de l'opérateur sont utilisés pour afficher les informations de processus aux utilisateurs humains ou aux opérateurs et leur permettre d'interagir avec le système de commande (lancer des actions opérationnelles sur le processus, comme l'ouverture d'une soupape, la fermeture d'un commutateur, la modification des points de consigne du processus, par exemple). En fonction des exigences opérationnelles respectives, il est souvent exigé que les postes de travail de l'opérateur soient disponibles en permanence (au moins un nombre

minimal de postes de travail sur tous ceux qui sont installés) pour avoir une vision intégrale des conditions du processus et l'opportunité d'interagir immédiatement avec le processus, si nécessaire. Pour obtenir les données à afficher et envoyer les commandes émises par l'utilisateur humain, les postes de travail de l'opérateur communiquent en général avec les serveurs de commande et les serveurs de connectivité dans les systèmes de commande, et communiquent parfois directement avec les PLC. Cette communication utilise souvent les protocoles Ethernet et TCP/IP. En règle générale, les postes de travail de l'opérateur ne doivent pas satisfaire aux exigences de temps réel dur, mais doivent satisfaire aux exigences d'intégrité et (au moins comme un ensemble de postes de travail de l'opérateur) de disponibilité élevées. Ils sont en général construits à partir d'un matériel PC COTS et fonctionnent sur des systèmes d'exploitation clients COTS.

A.4.2 Historique des données

Les historiques de données sont utilisés dans les systèmes de commande pour collecter et maintenir les données d'historique du processus à long terme. Ces données sont souvent collectées auprès des serveurs de commande ou directement auprès des PLC à l'aide de protocoles Ethernet et TCP/IP. Les données peuvent être utilisées dans une variété d'analyses, par exemple, pour optimiser le processus ou générer des rapports de performances, mais elles peuvent également être utilisées pour générer des rapports auprès d'entités de réglementation, comme ceux relatifs à l'intégrité du processus de production du produit (comme l'exigent les règlements de l'US Food and Drug Administration (FDA) relatifs aux produits pharmaceutiques, par exemple). Ils sont en général construits à partir d'un matériel PC/serveur COTS et fonctionnent sur des systèmes d'exploitation serveur/client COTS. Les données sont souvent stockées à l'aide de produits de base de données COTS. La communication avec les clients d'accès aux données et les sources de données est souvent assurée à l'aide des protocoles TCP/IP. Selon la criticité de l'historique de processus d'un point de vue professionnel, les historiques de données font l'objet d'exigences modérées en matière de disponibilité et d'intégrité et d'aucune exigence de temps réel dur.

Annexe B
(informative)

Mapping des CR et des RE avec les FR des SL 1 à 4

B.1 Vue d'ensemble

L'Annexe Bvise à fournir au lecteur les recommandations générales quant à la manière de différencier les niveaux de sécurité 0 à 4, FR par FR et en fonction des CR définies et de leurs RE associées.

B.2 Tableau de mapping des niveaux de sécurité

Le Tableau B.1indique les exigences de niveau de composant qui s'appliquent aux FR pour une capacité de niveau de sécurité du composant SL – SL-C(xx, composant) donnée. Pour une FR donnée, les exigences en matière de niveau de composant exigé satisfaisant à un SL-C donné sont indiquées par une coche.

À titre d'exemple, un composant qui atteint un SL-1 pour une FR 7 satisfait aux exigences de base des CR 7.1 à 7.7. À noter que la satisfaction à CR 7.8 n'est pas nécessaire pour satisfaire au SL-1, car cette CR n'est choisie que lorsque SL-2 est atteint au minimum. La satisfaction à SL-1 de cette manière est également notée SL-C(RA, composant) = 1 pour indiquer que le composant a un niveau de sécurité de capacité de 1 pour la RA ou une FR 7.

Un composant qui satisfait à SL-2 pour une FR 7, ou SL-C(RA, composant) = 2, satisfait à toutes les exigences à partir de SL-1 ainsi qu'à la RE(1) de la CR 7.1, la RE(1) de la CR 7.3 et l'exigence de base pour CR 7.8.

De même, un composant qui satisfait à SL-3 pour une FR 7, ou SL-C(RA, composant) = 3, satisfait à toutes les exigences à partir de SL-2 ainsi qu'à la RE(1) de la CR 7.6.

Un composant qui satisfait à SL-4 pour une FR 7, ou SL-C(RA, composant) = 4, satisfait à toutes les exigences à partir de SL-3. Pour FR 7, aucune exigence de base ou amélioration d'exigences ne s'applique uniquement à SL-4. Par conséquent, tous les composants qui satisfont à SL-3 satisfont également à SL-4 de manière intrinsèque.

Voir l'Annexe A de l'IEC 62443-3:2013 pour obtenir des informations sur la manière dont est représenté le vecteur SL complet comprenant toutes les FR.

Pour obtenir des clarifications, les acronymes utilisés dans le tableau sont présentés à la fin du tableau.

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

SR et RE	SL 1	SL 2	SL 3	SL 4
FR 1 – Contrôle d'identification et d'authentification (IAC)				
CR 1.1 – Identification et authentification d'un utilisateur humain	□	□	□	□
RE (1) Identification et authentification uniques:		□	□	□
RE (2) Authentification à plusieurs facteurs pour toutes les interfaces				□
CR 1.2 – Identification et authentification du processus logiciel et de l'appareil		□	□	□
RE (1) Identification et authentification uniques			□	□
CR 1.3 – Gestion de compte	□	□	□	□
CR 1.4 – Gestion d'identificateur	□	□	□	□
CR 1.5 – Gestion d'authentifiant	□	□	□	□
RE (1) Sécurité matérielle des authentifiants			□	□
NDR 1.6 – Gestion des accès sans fil	□	□	□	□
RE (1) Identification et authentification uniques		□	□	□
CR 1.7 – Force de l'authentification basée sur mot de passe	□	□	□	□
RE (1) Restrictions en matière de génération et de durée de vie des mots de passe pour les utilisateurs humains			□	□
RE (2) Restrictions en matière de durée de vie des mots de passe pour tous les utilisateurs (êtres humains, processus logiciels ou appareils)				□
CR 1.8 – Certificats d'infrastructure à clés publiques		□	□	□
CR 1.9 – Force de l'authentification basée sur clé publique		□	□	□
RE (1) Sécurité matérielle pour l'authentification basée sur clé publique			□	□
CR 1.10 – Retour de l'authentifiant	□	□	□	□
CR 1.11 – Tentatives infructueuses de connexion	□	□	□	□
CR 1.12 – Notification d'utilisation du système	□	□	□	□
NDR 1.13 – Accès par l'intermédiaire de réseaux non sécurisés	□	□	□	□
RE (1) Approbation de demande d'accès explicite			□	□
CR 1.14 – Force de l'authentification basée sur clé symétrique		□	□	□
RE (1) Sécurité matérielle pour l'authentification basée sur clé symétrique			□	□

SR et RE	SL 1	SL 2	SL 3	SL 4
FR 2 – Contrôle d'utilisation (UC)				
CR 2.1 – Mise en œuvre d'autorisation	☐	☐	☐	☐
RE (1) Mise en œuvre d'autorisation pour tous les utilisateurs (êtres humains, processus logiciels et appareils)		☐	☐	☐
RE (2) Mapping des droits d'accès aux rôles		☐	☐	☐
RE (3) Permission du superviseur			☐	☐
RE (4) Double approbation				☐
CR 2.2 – Contrôle d'utilisation sans fil	☐	☐	☐	☐
CR 2.3 – Contrôle d'utilisation pour les appareils portables et mobiles				
SAR 2.4 – Code mobile	☐	☐	☐	☐
RE (1) Contrôle d'authenticité du code mobile		☐	☐	☐
EDR 2.4 – Code mobile	☐	☐	☐	☐
RE (1) Contrôle d'authenticité du code mobile		☐	☐	☐
HDR 2.4 – Code mobile	☐	☐	☐	☐
RE (1) Contrôle d'authenticité du code mobile		☐	☐	☐
NDR 2.4 – Code mobile	☐	☐	☐	☐
RE (1) Contrôle d'authenticité du code mobile		☐	☐	☐
CR 2.5 – Verrouillage de session	☐	☐	☐	☐
CR 2.6 – Fermeture de la session à distance		☐	☐	☐
CR 2.7 – Contrôle de sessions simultanées			☐	☐
CR 2.8 – Événements auditables	☐	☐	☐	☐
CR 2.9 – Capacité de stockage des données d'audit	☐	☐	☐	☐
RE (1) Avertir lorsque le seuil de capacité de stockage des données d'audit est atteint			☐	☐
CR 2.10 – Réponse aux défaillances de traitement des audits	☐	☐	☐	☐
CR 2.11 – Horodatages	☐	☐	☐	☐
RE (1) Synchronisation temporelle		☐	☐	☐
RE (2) Protection de l'intégrité de l'horloge				☐
CR 2.12 – Non-répudiation	☐	☐	☐	☐
RE (1) Non-répudiation pour tous les utilisateurs				☐

SR et RE	SL 1	SL 2	SL 3	SL 4
EDR 2.13 – Utilisation d'interfaces physiques de diagnostic et d'essai		□	□	□
RE (1) Surveillance active			□	□
HDR 2.13 – Utilisation d'interfaces physiques de diagnostic et d'essai		□	□	□
RE (1) Surveillance active			□	□
NDR 2.13 – Utilisation d'interfaces physiques de diagnostic et d'essai		□	□	□
RE (1) Surveillance active			□	□
FR 3 – Intégrité du système (SI)				
CR 3.1 – Intégrité de la communication	□	□	□	□
RE (1) Authentification de la communication		□	□	□
SAR 3.2 – Protection contre les programmes malveillants	□	□	□	□
EDR 3.2 – Protection contre les programmes malveillants	□	□	□	□
HDR 3.2 – Protection contre les programmes malveillants	□	□	□	□
RE (1) Consigner la version de la protection contre le programme		□	□	□
NDR 3.2 – Protection contre les programmes malveillants	□	□	□	□
CR 3.3 – Vérification de la fonctionnalité de sécurité	□	□	□	□
RE (1) Vérification de la fonctionnalité de sécurité pendant le fonctionnement normal				□
CR 3.4 – Intégrité des logiciels et des informations	□	□	□	□
RE (1) Authenticité des logiciels et des informations		□	□	□
RE (2) Notification automatisée des violations d'intégrité			□	□
CR 3.5 – Validation d'entrée	□	□	□	□
CR 3.6 – Sortie déterministe	□	□	□	□
CR 3.7 – Traitement des erreurs	□	□	□	□
CR 3.8 – Intégrité de la session		□	□	□
CR 3.9 – Protection des informations d'audit		□	□	□
RE (1) Enregistrements d'audit sur support inscriptible				□
EDR 3.10 – Support pour les mises à jour	□	□	□	□
RE (1) Mettre à jour l'authenticité et l'intégrité			□	□
HDR 3.10 – Support pour les mises à jour	□	□	□	□

SR et RE	SL 1	SL 2	SL 3	SL 4
RE (1) Mettre à jour l'authenticité et l'intégrité		□	□	□
NDR 3.10 – Support pour les mises à jour	□	□	□	□
RE (1) Mettre à jour l'authenticité et l'intégrité		□	□	□
EDR 3.11 – Résistance aux violations physiques et détection		□	□	□
RE (1) Notification d'une tentative de violation			□	□
HDR 3.11 – Résistance aux violations physiques et détection		□	□	□
RE (1) Notification d'une tentative de violation			□	□
NDR 3.11 – Résistance aux violations physiques et détection		□	□	□
RE (1) Notification d'une tentative de violation			□	□
EDR 3.12 – Fourniture des racines de confiance du fournisseur de produit		□	□	□
HDR 3.12 – Fourniture des racines de confiance du fournisseur de produit		□	□	□
NDR 3.12 – Fourniture des racines de confiance du fournisseur de produit		□	□	□
EDR 3.13 – Fourniture des racines de confiance du propriétaire d'actif		□	□	□
HDR 3.13 – Fourniture des racines de confiance du propriétaire d'actif		□	□	□
NDR 3.13 – Fourniture des racines de confiance du propriétaire d'actif		□	□	□
EDR 3.14 – Intégrité du processus d'amorçage	□	□	□	□
RE (1) Authenticité du processus d'amorçage		□	□	□
HDR 3.14 – Intégrité du processus d'amorçage	□	□	□	□
RE (1) Authenticité du processus d'amorçage		□	□	□
NDR 3.14 – Intégrité du processus d'amorçage	□	□	□	□
RE (1) Authenticité du processus d'amorçage		□	□	□
FR 4 – Confidentialité des données (DC)				
CR 4.1 – Confidentialité des informations	□	□	□	□
CR 4.2 – Persistance des informations		□	□	□
RE (1) Effacer les ressources de la mémoire partagée			□	□
RE (2) Vérification de l'effacement			□	□
CR 4.3 – Utilisation de la cryptographie	□	□	□	□

SR et RE	SL 1	SL 2	SL 3	SL 4
FR 5 – Transfert de données limité (RDF)				
CR 5.1 – Segmentation du réseau	□	□	□	□
NDR 5.2 – Protection des limites de zone	□	□	□	□
RE (1) Refuser tout, autoriser par exception		□	□	□
RE (2) Mode insulaire			□	□
RE (3) Fermeture en cas d'échec			□	□
NDR 5.3 – Restrictions des communications entre des personnes d'ordre général	□	□	□	□
FR 6 – Réponse appropriée aux événements (TRE)				
CR 6.1 – Accessibilité au journal d'audit	□	□	□	□
RE (1) Accès programmatique aux journaux d'audit			□	□
CR 6.2 – Surveillance continue		□	□	□
FR 7 – Disponibilité des ressources (RA)				
CR 7.1 – Protection contre le refus de service	□	□	□	□
RE (1) Gérer la charge de communication provenant du composant		□	□	□
CR 7.2 – Gestion des ressources	□	□	□	□
CR 7.3 – Sauvegarde du système de commande	□	□	□	□
RE (1) Vérification de l'intégrité de la sauvegarde		□	□	□
CR 7.4 – Récupération et reconstitution du système de commande	□	□	□	□
CR 7.5 – Alimentation de secours				
CR 7.6 – Paramètres de configuration du réseau et de la sécurité	□	□	□	□
RE (1) Génération d'un rapport lisible par une machine des paramètres de sécurité en cours			□	□
CR 7.7 – Fonctionnalité minimale	□	□	□	□
CR 7.8 – Inventaire des composants du système de commande		□	□	□

Légende

CR: Exigence de composant commune à tous les types de composants

SAR: Exigences relatives aux applications logicielles

EDR: Exigence relative aux appareils intégrés

HDR: Exigence relative aux appareils hôtes

NDR Exigence relative aux appareils de réseaux

Bibliographie

NOTE 1 Cette bibliographie inclut des références aux sources utilisées lors de la création du présent document, ainsi que des références à des sources qui peuvent aider le lecteur à mieux comprendre la cybersécurité dans son ensemble et à développer un système de gestion. Toutes les références de cette bibliographie ne sont pas mentionnées tout au long du présent document. Les références ont été réparties en catégories différentes en fonction du type de leur source.

Références à d'autres parties, tant existantes qu'attendues, de la série IEC 62443:

NOTE 2 Certaines de ces références sont des documents publiés, en cours d'élaboration ou anticipés. Elles sont toutes énumérées dans cette bibliographie par souci d'exhaustivité des parties actuellement autorisées de la série IEC 62443.

[1] IEC 62443-2-1, Réseaux industriels de communication – Sécurité dans les réseaux et les systèmes – Partie 2-1: Établissement d'un programme de sécurité pour les systèmes d'automatisation et de commande industrielles

[2] IEC TR 62443-2-3, Security for industrial automation and control systems – Part 2-3: Patch management in the IACS environment (disponible en anglais seulement)

[3] IEC 62443-2-4, Sécurité des automatismes industriels et des systèmes de commande – Partie 2-4: Exigences de programme de sécurité pour les fournisseurs de service IACS

[4] IEC TR 62443-3-1, Industrial communication networks – Network and system security – Part 3-1: Security technologies for industrial automation and control systems (disponible en anglais seulement)

[5] IEC 62443-3-2[4], Security for industrial automation and control systems – Part 3-2: Security risk assessment and system design (disponible en anglais seulement)

Autres références:

[6] ISO/IEC 7498-1:1994, Technologies de l'information – Modèle de référence de base pour l'interconnexion de systèmes ouverts (OSI): Le modèle de base

[7] ISO/IEC 8601:2004, Data elements and interchange formats – Information interchange – Representation of dates and times (disponible en anglais seulement)

[8] ISO/IEC 15408-1:2009, Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model (disponible en anglais seulement)

[9] ISO/IEC 19790, Information technology – Security techniques – Security requirements for cryptographic modules (disponible en anglais seulement)

[10] ISO/IEC 27002:2013, Technologies de l'information – Techniques de sécurité – Code de bonne pratique pour le management de la sécurité de l'information

[11] IEC 60050-351, Vocabulaire Électrotechnique International – Partie 351: Technologie de commande et de régulation (disponible à l'adresse http://www.electropedia.org)

[12] IEC 60050-732, Vocabulaire Électrotechnique International – Partie 732: Techniques des réseaux d'ordinateurs (disponible à l'adresse http://www.electropedia.org)

---

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

[13] IEC 61131-3, Automates programmables – Partie 3: Langages de programmation

[14] IEC TR 61850-1:2013, Réseaux et systèmes de communication pour l'automatisation des systèmes électriques – Partie 1: Introduction et présentation

[15] ANSI/ISA-95.00.01-2010 (IEC 62264-1 Mod), Enterprise-Control System Integration – Part 1: Models and Terminology

[16] ISO/IEC 11889-1:2015, Information technology – Trusted Platform Module Library – Part 1: Architecture (disponible en anglais seulement)

Autres documents et ressources publiées:

[17] FIPS 140-2, Security Requirements for Cryptographic Modules

[18] NIST SP 800-57, Recommendation for Key Management – Part 1: General

[19] NIST SP 800-92, Guide to Computer Security Log Management

[20] NIST SP 800-63-2, Electronic Authentication Guideline

Sites Web:

[21] OWASP Code Review Guide, disponible à l'adresse https://www.owasp.org/index.php/Code_Review_Guide

[22] RFC 3647 – Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework https://www.ietf.org/rfc/rfc3647.txt

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

3, rue de Varembé
PO Box 131
CH-1211 Geneva 20
Switzerland

Tel: + 41 22 919 02 11
Fax: + 41 22 919 03 00
info@iec.ch
www.iec.ch