



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.**

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

IECNORM.COM : Click to view the full PDF of IEC 62443 4-2 ed 1.0:2019

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.

IECNORM.COM : Click to view the full PDF of IEC 62443-4-2:2019 1.0:2019

INTRODUCTION

0.1 Overview

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

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

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

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

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

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

² Numbers in square brackets refer to the bibliography.

0.2 Purpose and intended audience

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

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

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

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

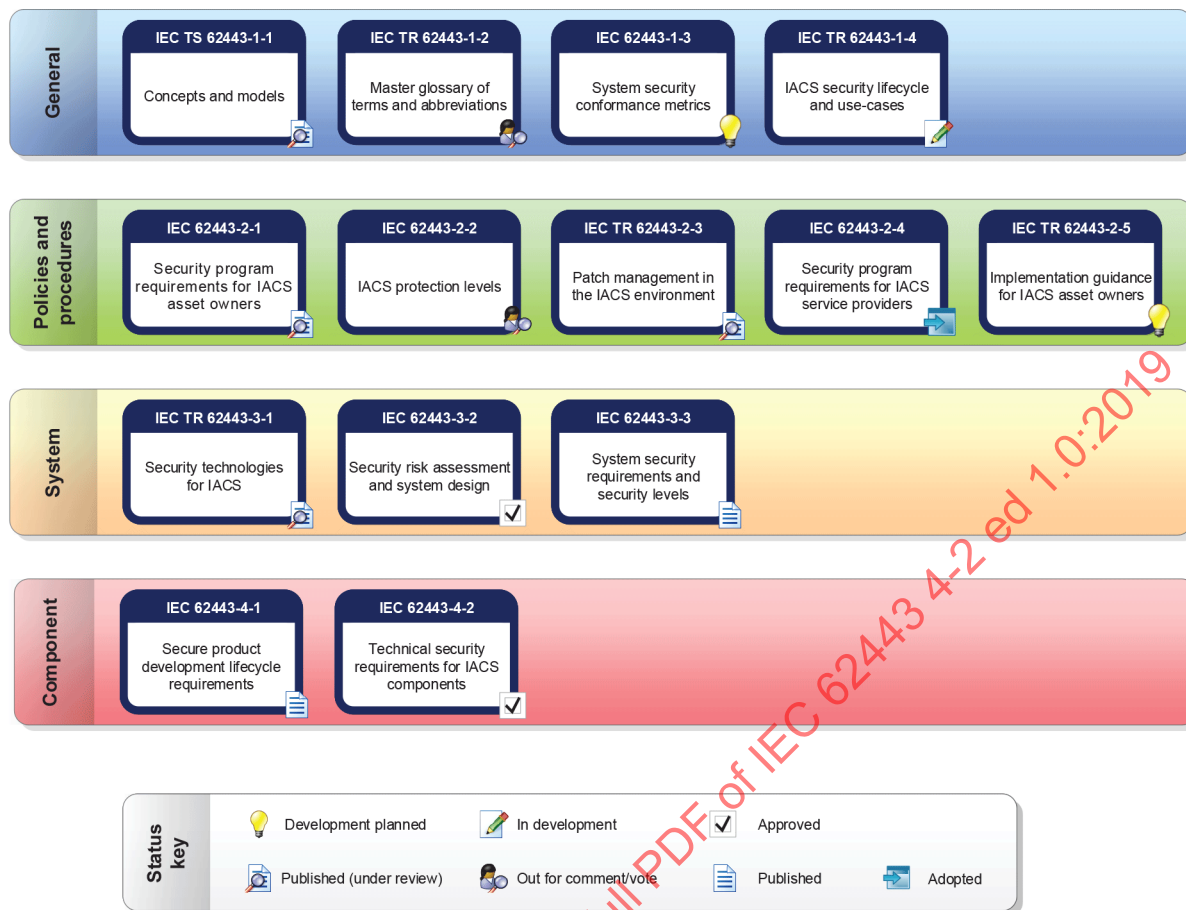
This document provides component requirements for four types of components: software application, embedded device, host device and network device. Thus, the CRs for each type of component will be designated as follows:

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

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

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

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



IEC

Figure 1 – Parts of the IEC 62443 series

SECURITY FOR INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS –

Part 4-2: Technical security requirements for IACS components

1 Scope

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

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

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

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

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

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

2 Normative references

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

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

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

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

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 auditable	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	Termineur RPV (réseau privé virtuel).....	183