IEC 62443-3-3

Edition 1.0 2013-08

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

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

Réseaux industriels de communication – Sécurité dans les réseaux et les systèmes – Partie 3-3: Exigences de sécurité des systèmes et niveaux de sécurité

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

ICS 25.040.40; 35.110

ISBN 978-2-8322-6422-5

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

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

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

6.14.1 Requirement 44
6.14.2 Rationale and supplemental guidance 44
6.14.3 Requirement enhancements 44
6.14.4 Security levels 44
7 FR 3 – System integrity 45
7.1 Purpose and SL-C(SI) descriptions 45
7.2 Rationale 45
7.3 SR 3.1 – Communication integrity 45
7.3.1 Requirement 45
7.3.2 Rationale and supplemental guidance 45
7.3.3 Requirement enhancements 46
7.3.4 Security levels 46
7.4 SR 3.2 – Malicious code protection 46
7.4.1 Requirement 46
7.4.2 Rationale and supplemental guidance 46
7.4.3 Requirement enhancements 47
7.4.4 Security levels 47
7.5 SR 3.3 – Security functionality verification 47
7.5.1 Requirement 47
7.5.2 Rationale and supplemental guidance 47
7.5.3 Requirement enhancements 48
7.5.4 Security levels 48
7.6 SR 3.4 – Software and information integrity 48
7.6.1 Requirement 48
7.6.2 Rationale and supplemental guidance 48
7.6.3 Requirement enhancements 49
7.6.4 Security levels 49
7.7 SR 3.5 – Input validation 49
7.7.1 Requirement 49
7.7.2 Rationale and supplemental guidance 49
7.7.3 Requirement enhancements 49
7.7.4 Security levels 49
7.8 SR 3.6 – Deterministic output 50
7.8.1 Requirement 50
7.8.2 Rationale and supplemental guidance 50
7.8.3 Requirement enhancements 50
7.8.4 Security levels 50
7.9 SR 3.7 – Error handling 50
7.9.1 Requirement 50
7.9.2 Rationale and supplemental guidance 50
7.9.3 Requirement enhancements 50
7.9.4 Security levels 51
7.10 SR 3.8 – Session integrity 51
7.10.1 Requirement 51
7.10.2 Rationale and supplemental guidance 51
7.10.3 Requirement enhancements 51
7.10.4 Security levels 51
7.11 SR 3.9 – Protection of audit information 52
7.11.1 Requirement 52

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

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

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

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

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

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

INDUSTRIAL COMMUNICATION NETWORKS – NETWORK AND SYSTEM SECURITY –

Part 3-3: System security requirements and security levels

FOREWORD

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

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

This bilingual version (2019-01) corresponds to the monolingual English version, published in 2013-08.

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

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

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

The French version of this standard has not been voted upon.

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

A list of all parts in the IEC 62443 series, published under the general title *Industrial communication networks – Network and system security*, can be found on the IEC website.

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

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

The contents of the corrigendum of April 2014 have been included in this copy.

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.

0 Introduction

0.1 Overview

NOTE 1 This standard is part of series of standards that addresses the issue of security for industrial automation and control systems (IACS). It has been developed by working group 4, task group 2 of the IEC99 committee in cooperation with IEC TC65/WG10. This document prescribes the security requirements for control systems related to the seven foundational requirements defined in IEC 62443-1-1 and assigns system security levels (SLs) to the system under consideration (SuC).

NOTE 2 The format of this standard follows the ISO/IEC requirements discussed in ISO/IEC Directives, Part 2 [11].[1] These directives specify the format of the standard as well as the use of terms like “shall”, “should”, and “may”. The requirements specified in normative clauses use the conventions discussed in Appendix H of the ISO/IEC Directives.

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

IACS security measures should not have the potential to cause loss of essential services and functions, including emergency procedures. (IT security measures, 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 need to be clearly stated as security objectives regardless of the degree of plant integration achieved. A key step in risk assessment, as required by IEC 62443-2-1[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 standard assumes that a security program has been established and is being operated in accordance with IEC 62443-2-1. Furthermore, it is assumed that patch management is implemented consistently with the recommendations detailed in IEC/TR 62443-2-3 [5] utilizing the appropriate control system requirements and requirement enhancements as described in this standard. In addition, IEC 62443-3-2 [8] describes how a project defines risk-based security levels (SLs) which then are used to select products with the appropriate technical security capabilities as detailed in this standard. Key input to this standard included ISO/IEC 27002 [15] and NIST SP800-53, rev 3 [24] (see Clause 2 and the Bibliography for a more complete listing of source material).

---

1 Numbers in square brackets refer to the Bibliography.

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

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 availability needed by IACS.

0.2 Purpose and intended audience

The IACS community audience for this standard is intended to be asset owners, system integrators, product suppliers, service providers 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, product suppliers and service providers will use this standard to evaluate whether their products and services can provide the functional security capability to meet the asset owner's target security level (SL-T) requirements. As with the assignment of SL-Ts, the applicability of individual control system requirements (SRs) and requirement enhancements (REs) needs to be based on an asset owner's security policies, procedures and risk assessment in the context of their specific site. Note that some SRs contain specific conditions for permissible exceptions, such as where meeting the SR will violate fundamental operational requirements of a control system (which may trigger the need for compensating countermeasures).

When designing a control system to meet the set of SRs associated with specific SL-Ts, it is not necessary that every component of the proposed control system support every system requirement to the level mandated in this standard. Compensating countermeasures can be employed to provide the needed functionality to other subsystems, such that the overall SL-T requirements are met at the control system level. Inclusion of compensating countermeasures during the design phase should be accompanied by comprehensive documentation so that the resulting achieved control system SL, SL-A(control system), fully reflects the intended security capabilities inherent in the design. Similarly, during certification testing and/or post-installation audits, compensating countermeasures can be utilized and documented in order to meet the overall control system SL.

There is insufficient detail in this standard to design and build an integrated security architecture. That requires additional system-level analysis and development of derived requirements that are the subject of other standards in the IEC 62443 series (see 0). Note that providing specifications detailed enough to build a security architecture are not the goal of this standard. The goal is to define a common, minimum set of requirements to reach progressively more stringent security levels. The actual design of an architecture that meets these requirements is the job of system integrators and product suppliers. In this task, they retain the freedom to make individual choices, thus supporting competition and innovation. Thus this standard strictly adheres to specifying functional requirements, and does not address how these functional requirements should be met.

0.3 Usage within other parts of the IEC 62443 series

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

IEC 62443-3-2 uses the SRs and REs as a checklist. After the system under consideration (SuC) has been described in terms of zones and conduits, and individual target SLs have been assigned to these zones and conduits, the SRs and REs in this standard, as well as their mapping to capability SLs (SL-Cs), are used to compile a list of requirements which the control system design needs to meet. A given control system design can then be checked for completeness, thereby providing the SL-As.

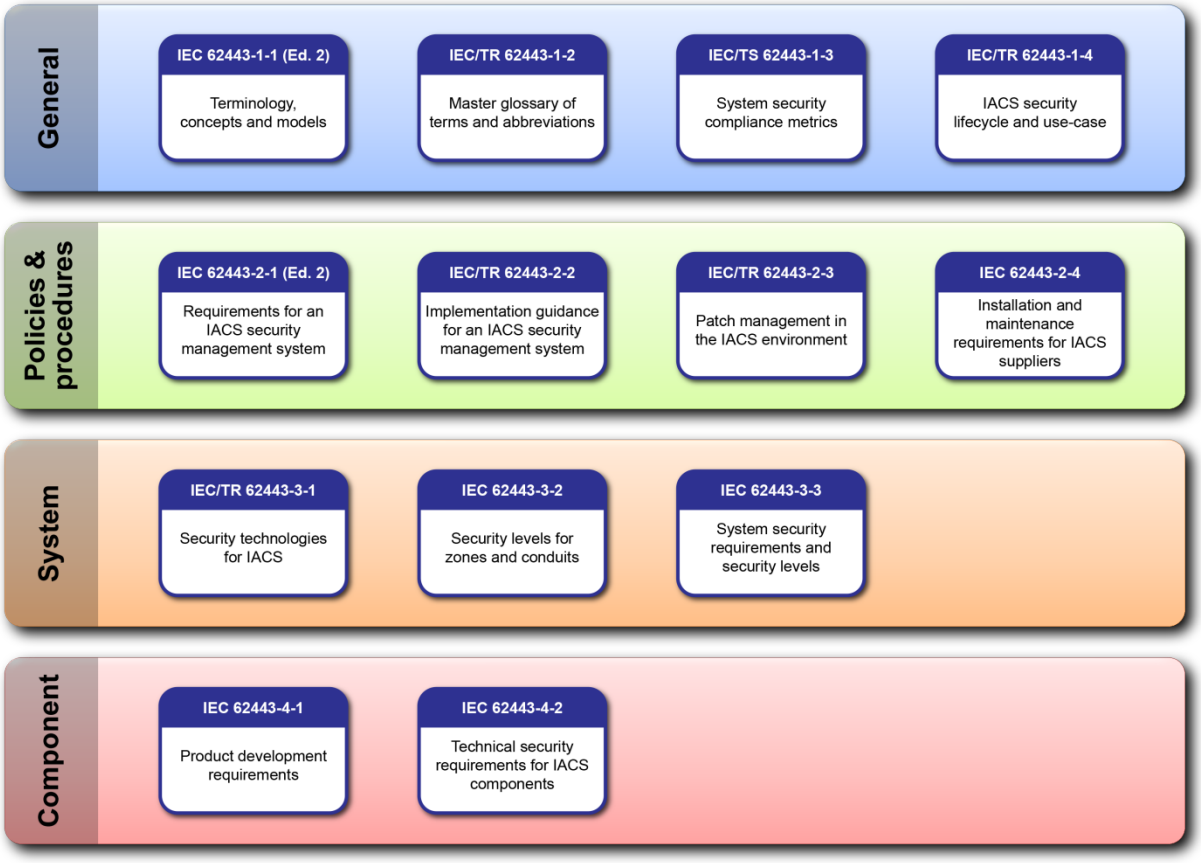


Figure 1 – Structure of the IEC 62443 series

IEC/TS 62443-1-3 [2] uses the foundational requirements (FRs), SRs, REs and the mapping to SL-Cs as a checklist to test for completeness of the specification of quantitative metrics. The quantitative security compliance metrics are context specific. Together with IEC 62443-3-2, the asset owner's SL-T assignments are translated into quantitative metrics that can be used to support system analysis and design trade-off studies, to develop a security architecture.

IEC 62443-4-1 [9] addresses the overall requirements during the development of products. As such, IEC 62443-4-1 is product supplier centric. Product security requirements are derived from the list of baseline requirements and REs specified in this standard. Normative quality specifications in IEC 62443-4-1 will be used when developing these product capabilities.

IEC 62443-4-2 [10] contains sets of derived requirements that provide a detailed mapping of the SRs specified in this standard to subsystems and components of the SuC. At the time this standard was written, the component categories addressed in IEC 62443-4-2 were: embedded devices, host devices, network devices and applications. As such, IEC 62443-4-2 is vendor (product supplier and service provider) centric. Product security requirements are first derived from the list of baseline requirements and REs specified in this standard. Security requirements and metrics from IEC 62443-3-2 and IEC/TS 62443-1-3 are used to refine these normative derived requirements.

INDUSTRIAL COMMUNICATION NETWORKS – NETWORK AND SYSTEM SECURITY –

Part 3-3: System security requirements and security levels

1 Scope

This part of the IEC 62443 series provides detailed technical control system requirements (SRs) associated with the seven foundational requirements (FRs) described in IEC 62443-1-1 including defining the requirements for control system capability security levels, SL-C(control system). These requirements would be used by various members of the industrial automation and control system (IACS) community along with the defined zones and conduits for the system under consideration (SuC) while developing the appropriate control system target SL, SL-T(control system), for a specific asset.

As defined in IEC 62443-1-1 there are a total of seven 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 requirements are the foundation for control system capability SLs, SL-C (control system). Defining security capability at the control system level is the goal and objective of this standard as opposed to target SLs, SL-T, or achieved SLs, SL-A, which are out of scope.

See IEC 62443-2-1 for an equivalent set of non-technical, program-related, capability SRs necessary for fully achieving a control system target SL.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 62443-1-1:2009, *Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models*

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

SOMMAIRE

AVANT-PROPOS 89
0 Introduction 91
0.1 Vue d'ensemble 91
0.2 Objectif et public visé 92
0.3 Utilisation dans d'autres parties de la série IEC 62443 93
1 Domaine d'application 95
2 Références normatives 95
3 Termes, définitions, termes abrégés, acronymes et conventions 96
3.1 Termes et définitions 96
3.2 Termes abrégés et acronymes 101
3.3 Conventions 103
4 Contraintes communes de sécurité du système de commande 104
4.1 Présentation 104
4.2 Prise en charge des fonctions essentielles 104
4.3 Contre-mesures compensatoires 105
4.4 Moindre privilège 106
5 FR 1– Commande d'identification et d'authentification 106
5.1 Objectif et descriptions du SL-C(IAC) 106
5.2 Justification 106
5.3 SR 1.1 – Identification et authentification d'utilisateur humain 106
5.3.1 Exigence 106
5.3.2 Justification et recommandations supplémentaires 106
5.3.3 Améliorations d'exigences 107
5.3.4 Niveaux de sécurité 107
5.4 SR 1.2 – Identification et authentification du processus logiciel et de l'appareil 108
5.4.1 Exigence 108
5.4.2 Justification et recommandations supplémentaires 108
5.4.3 Améliorations d'exigences 109
5.4.4 Niveaux de sécurité 109
5.5 SR 1.3 – Gestion des comptes 109
5.5.1 Exigence 109
5.5.2 Justification et recommandations supplémentaires 109
5.5.3 Améliorations d'exigences 109
5.5.4 Niveaux de sécurité 109
5.6 SR 1.4 – Gestion des identificateurs 110
5.6.1 Exigence 110
5.6.2 Justification et recommandations supplémentaires 110
5.6.3 Améliorations d'exigences 110
5.6.4 Niveaux de sécurité 110
5.7 SR 1.5 – Gestion des authentifiants 110
5.7.1 Exigence 110
5.7.2 Justification et recommandations supplémentaires 111
5.7.3 Améliorations d'exigences 112
5.7.4 Niveaux de sécurité 112
5.8 SR 1.6 – Gestion des accès sans fil 112
5.8.1 Exigence 112

5.8.2 Justification et recommandations supplémentaires 112
5.8.3 Améliorations d'exigences 112
5.8.4 Niveaux de sécurité 112
5.9 SR 1.7 – Force de l'authentification basée sur le mot de passe 113
5.9.1 Exigence 113
5.9.2 Justification et recommandations supplémentaires 113
5.9.3 Améliorations d'exigences 113
5.9.4 Niveaux de sécurité 114
5.10 SR 1.8 – Certificats d'infrastructure à clés publiques (ICP) 114
5.10.1 Exigence 114
5.10.2 Justification et recommandations supplémentaires 114
5.10.3 Améliorations d'exigences 114
5.10.4 Niveaux de sécurité 114
5.11 SR 1.9 – Force de l'authentification de clé publique 114
5.11.1 Exigence 114
5.11.2 Justification et recommandations supplémentaires 115
5.11.3 Améliorations d'exigences 115
5.11.4 Niveaux de sécurité 115
5.12 SR 1.10 – Rétroaction de l'authentifiant 116
5.12.1 Exigence 116
5.12.2 Justification et recommandations supplémentaires 116
5.12.3 Améliorations d'exigences 116
5.12.4 Niveaux de sécurité 116
5.13 SR 1.11 – Tentatives d'authentification infructueuses 116
5.13.1 Exigence 116
5.13.2 Justification et recommandations supplémentaires 116
5.13.3 Améliorations d'exigences 117
5.13.4 Niveaux de sécurité 117
5.14 SR 1.12 – Notification d'utilisation du système 117
5.14.1 Exigence 117
5.14.2 Justification et recommandations supplémentaires 117
5.14.3 Améliorations d'exigences 117
5.14.4 Niveaux de sécurité 117
5.15 SR 1.13 – Accès par des réseaux non sécurisés 118
5.15.1 Exigence 118
5.15.2 Justification et recommandations supplémentaires 118
5.15.3 Améliorations d'exigences 118
5.15.4 Niveaux de sécurité 118
6 FR 2 – Commande d'utilisation 118
6.1 Objectif et descriptions du SL-C(UC) 118
6.2 Justification 119
6.3 SR 2.1 – Application de l'autorisation 119
6.3.1 Exigence 119
6.3.2 Justification et recommandations supplémentaires 119
6.3.3 Améliorations d'exigences 120
6.3.4 Niveaux de sécurité 120
6.4 SR 2.2 –Contrôle d'utilisation sans fil 120
6.4.1 Exigence 120
6.4.2 Justification et recommandations supplémentaires 121

6.4.3 Améliorations d'exigences 121
6.4.4 Niveaux de sécurité 121
6.5 SR 2.3 – Contrôle d'utilisation des appareils mobiles et portables 121
6.5.1 Exigence 121
6.5.2 Justification et recommandations supplémentaires 121
6.5.3 Améliorations d'exigences 122
6.5.4 Niveaux de sécurité 122
6.6 SR 2.4 – Code mobile 122
6.6.1 Exigence 122
6.6.2 Justification et recommandations supplémentaires 122
6.6.3 Améliorations d'exigences 122
6.6.4 Niveaux de sécurité 123
6.7 SR 2.5 – Verrouillage de session 123
6.7.1 Exigence 123
6.7.2 Justification et recommandations supplémentaires 123
6.7.3 Améliorations d'exigences 123
6.7.4 Niveaux de sécurité 123
6.8 SR 2.6 – Terminaison de session distante 123
6.8.1 Exigence 123
6.8.2 Justification et recommandations supplémentaires 124
6.8.3 Améliorations d'exigences 124
6.8.4 Niveaux de sécurité 124
6.9 SR 2.7 – Commande de sessions concomitantes 124
6.9.1 Exigence 124
6.9.2 Justification et recommandations supplémentaires 124
6.9.3 Améliorations d'exigences 124
6.9.4 Niveaux de sécurité 124
6.10 SR 2.8 – Événements auditables 125
6.10.1 Exigence 125
6.10.2 Justification et recommandations supplémentaires 125
6.10.3 Améliorations d'exigences 125
6.10.4 Niveaux de sécurité 125
6.11 SR 2.9 – Capacité de stockage de l'audit 126
6.11.1 Exigence 126
6.11.2 Justification et recommandations supplémentaires 126
6.11.3 Améliorations d'exigences 126
6.11.4 Niveaux de sécurité 126
6.12 SR 2.10 – Réponse aux échecs de traitement d'audit 126
6.12.1 Exigence 126
6.12.2 Justification et recommandations supplémentaires 126
6.12.3 Améliorations d'exigences 127
6.12.4 Niveaux de sécurité 127
6.13 SR 2.11– Horodatages 127
6.13.1 Exigence 127
6.13.2 Justification et recommandations supplémentaires 127
6.13.3 Améliorations d'exigences 127
6.13.4 Niveaux de sécurité 127
6.14 SR 2.12 – Non-répudiation 128
6.14.1 Exigence 128

6.14.2 Justification et recommandations supplémentaires 128
6.14.3 Améliorations d'exigences 128
6.14.4 Niveaux de sécurité 128
7 FR 3 – Intégrité du système 128
7.1 Objectif et descriptions du SL-C(SI) 128
7.2 Justification 129
7.3 SR 3.1 – Intégrité de la communication 129
7.3.1 Exigence 129
7.3.2 Justification et recommandations supplémentaires 129
7.3.3 Améliorations d'exigences 130
7.3.4 Niveaux de sécurité 130
7.4 SR 3.2 – Protection contre les programmes malveillants 130
7.4.1 Exigence 130
7.4.2 Justification et recommandations supplémentaires 130
7.4.3 Améliorations d'exigences 131
7.4.4 Niveaux de sécurité 131
7.5 SR 3.3 – Vérification des fonctionnalités de sécurité 131
7.5.1 Exigence 131
7.5.2 Justification et recommandations supplémentaires 131
7.5.3 Améliorations d'exigences 132
7.5.4 Niveaux de sécurité 132
7.6 SR 3.4 – Intégrité du logiciel et des informations 132
7.6.1 Exigence 132
7.6.2 Justification et recommandations supplémentaires 132
7.6.3 Améliorations d'exigences 133
7.6.4 Niveaux de sécurité 133
7.7 SR 3.5 – Validation en entrée 133
7.7.1 Exigence 133
7.7.2 Justification et recommandations supplémentaires 133
7.7.3 Améliorations d'exigences 133
7.7.4 Niveaux de sécurité 134
7.8 SR 3.6 – Sortie déterministe 134
7.8.1 Exigence 134
7.8.2 Justification et recommandations supplémentaires 134
7.8.3 Améliorations d'exigences 134
7.8.4 Niveaux de sécurité 134
7.9 SR 3.7 – Traitement des erreurs 134
7.9.1 Exigence 134
7.9.2 Justification et recommandations supplémentaires 134
7.9.3 Améliorations d'exigences 135
7.9.4 Niveaux de sécurité 135
7.10 SR 3.8 – Intégrité de la session 135
7.10.1 Exigence 135
7.10.2 Justification et recommandations supplémentaires 135
7.10.3 Améliorations d'exigences 135
7.10.4 Niveaux de sécurité 136
7.11 SR 3.9 – Protection des informations d’audit 136
7.11.1 Exigence 136
7.11.2 Justification et recommandations supplémentaires 136

7.11.3 Améliorations d'exigences 136
7.11.4 Niveaux de sécurité 136
8 FR 4 – Confidentialité des données 136
8.1 Objectif et descriptions du SL-C(DC) 136
8.2 Justification 137
8.3 SR 4.1 – Confidentialité des informations 137
8.3.1 Exigence 137
8.3.2 Justification et recommandations supplémentaires 137
8.3.3 Améliorations d'exigences 138
8.3.4 Niveaux de sécurité 138
8.4 SR 4.2 – Persistance des informations 138
8.4.1 Exigence 138
8.4.2 Justification et recommandations supplémentaires 138
8.4.3 Améliorations d'exigences 139
8.4.4 Niveaux de sécurité 139
8.5 SR 4.3 – Utilisation de la cryptographie 139
8.5.1 Exigence 139
8.5.2 Justification et recommandations supplémentaires 139
8.5.3 Améliorations d'exigences 140
8.5.4 Niveaux de sécurité 140
9 FR 5 – Flux de données réduit 140
9.1 Objectif et descriptions du SL-C(RDF) 140
9.2 Justification 140
9.3 SR 5.1 – Segmentation des réseaux 140
9.3.1 Exigence 140
9.3.2 Justification et recommandations supplémentaires 140
9.3.3 Améliorations d'exigences 141
9.3.4 Niveaux de sécurité 141
9.4 SR 5.2 – Protection des limites de zone 142
9.4.1 Exigence 142
9.4.2 Justification et recommandations supplémentaires 142
9.4.3 Améliorations d'exigences 142
9.4.4 Niveaux de sécurité 142
9.5 SR 5.3 – Restrictions de communication de personne à personne à visée générale 143
9.5.1 Exigence 143
9.5.2 Justification et recommandations supplémentaires 143
9.5.3 Améliorations d'exigences 143
9.5.4 Niveaux de sécurité 144
9.6 SR 5.4 – Partitionnement d'application 144
9.6.1 Exigence 144
9.6.2 Justification et recommandations supplémentaires 144
9.6.3 Améliorations d'exigences 144
9.6.4 Niveaux de sécurité 144
10 FR 6 – Réponse rapide aux événements 144
10.1 Objectif et descriptions du SL-C(TRE) 144
10.2 Justification 145
10.3 SR 6.1 – Accessibilité du journal d'audit 145
10.3.1 Exigence 145

10.3.2 Justification et recommandations supplémentaires 145
10.3.3 Améliorations d'exigences 145
10.3.4 Niveaux de sécurité 145
10.4 SR 6.2 – Surveillance permanente 146
10.4.1 Exigence 146
10.4.2 Justification et recommandations supplémentaires 146
10.4.3 Améliorations d'exigences 146
10.4.4 Niveaux de sécurité 146
11 FR 7 – Disponibilité des ressources 146
11.1 Objectif et descriptions du SL-C(RA) 146
11.2 Justification 147
11.3 SR 7.1 – Protection contre le refus de service 147
11.3.1 Exigence 147
11.3.2 Justification et recommandations supplémentaires 147
11.3.3 Améliorations d'exigences 147
11.3.4 Niveaux de sécurité 147
11.4 SR 7.2 – Gestion des ressources 148
11.4.1 Exigence 148
11.4.2 Justification et recommandations supplémentaires 148
11.4.3 Améliorations d'exigences 148
11.4.4 Niveaux de sécurité 148
11.5 SR 7.3 – Sauvegarde du système de commande 148
11.5.1 Exigence 148
11.5.2 Justification et recommandations supplémentaires 148
11.5.3 Améliorations d'exigences 149
11.5.4 Niveaux de sécurité 149
11.6 SR 7.4 – Récupération et reconstitution du système de commande 149
11.6.1 Exigence 149
11.6.2 Justification et recommandations supplémentaires 149
11.6.3 Améliorations d'exigences 149
11.6.4 Niveaux de sécurité 149
11.7 SR 7.5 – Alimentation d'urgence 150
11.7.1 Exigence 150
11.7.2 Justification et recommandations supplémentaires 150
11.7.3 Améliorations d'exigences 150
11.7.4 Niveaux de sécurité 150
11.8 SR 7.6 – Paramètres de configuration de sécurité et de réseau 150
11.8.1 Exigence 150
11.8.2 Justification et recommandations supplémentaires 150
11.8.3 Améliorations d'exigences 150
11.8.4 Niveaux de sécurité 151
11.9 SR 7.7 – Moindre fonctionnalité 151
11.9.1 Exigence 151
11.9.2 Justification et recommandations supplémentaires 151
11.9.3 Améliorations d'exigences 151
11.9.4 Niveaux de sécurité 151
11.10 SR 7.8 – Inventaire de composants du système de commande 151
11.10.1 Exigence 151
11.10.2 Justification et recommandations supplémentaires 151

11.10.3 Améliorations d'exigences 152
11.10.4 Niveaux de sécurité 152
Annexe A (informative) Analyse du vecteur SL 153
Annexe B (informative) Mapping des SR et RE aux FR SL 1-4 164
Bibliographie 168

Figure 1 – Structure de la série IEC 62443 93
Figure A.1 – Exemple d'industrie de traitement de haut niveau représentant les zones et conduits 157
Figure A.2 – Exemple de fabrication de haut niveau représentant les zones et conduits 158
Figure A.3 – Schéma de corrélation de l'utilisation de différents types de SL 159

Tableau B.1 – Mapping des SR et RE aux niveaux FR SL 1-4 *(1 sur 4)* 164

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

RÉSEAUX INDUSTRIELS DE COMMUNICATION – SÉCURITÉ DANS LES RÉSEAUX ET LES SYSTÈMES –

Partie 3-3: Exigences de sécurité des systèmes et niveaux de sécurité

AVANT-PROPOS

1) La Commission Électrotechnique 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 62443-3-3 a été établie par le comité d'études 65 de l'IEC: Mesure, commande et automation dans les processus industriels.

La présente version bilingue (2019-01) correspond à la version anglaise monolingue publiée en 2013-08.

Le texte anglais de cette norme est issu des documents 65/531/FDIS et 65/540/RVD.

Le rapport de vote 65/540/RVD donne toute information sur le vote ayant abouti à l'approbation de cette norme.

La version française de cette norme n'a pas été soumise au vote.

Cette publication a été rédigée selon les Directives ISO/IEC, Partie 2.

Une liste de toutes les parties de la série IEC 62443, publiées sous le titre général *Réseaux industriels de communication – Sécurité dans les réseaux et les systèmes*, peut être consultée sur le site web de l'IEC.

Le comité a décidé que le contenu de cette publication 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 à la publication recherchée. À cette date, la publication sera

- reconduite,
- supprimée,
- remplacée par une édition révisée, ou
- amendée.

Le contenu du corrigendum d'avril 2014 est inclus dans la présente copie.

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 ce document en utilisant une imprimante couleur.

0 Introduction

0.1 Vue d'ensemble

NOTE 1 La présente norme fait partie d'une série de normes traitant de la sécurité des systèmes d'automatisation et de commande industrielles (IACS). Elle a été élaborée par le groupe de travail 4, sous-groupe de travail 2 du comité 99 de l'IEC, en coopération avec le GT 10 du CE 65 de l'IEC. Le présent document spécifie les exigences de sécurité des systèmes de commande associées aux sept exigences fondamentales définies dans l'IEC 62443-1-1, et assigne des niveaux de sécurité (SL - *security level*) de système aux systèmes à l'étude (SuC - *system under consideration*).

NOTE 2 Le format de la présente norme suit les exigences de l'ISO/IEC traitées dans les directives ISO/IEC, Partie 2 [11].[1] Ces directives spécifient le format de la norme ainsi que l'utilisation des termes comme «devoir», «il convient» et «pouvoir». Les exigences spécifiées dans les articles normatifs utilisent les conventions traitées dans l'Appendice H des directives de l'ISO/IEC.

Les organismes de système d'automatisation et de commande industrielles (IACS) utilisent de plus en plus de dispositifs de réseau commerciaux (COTS - *commercial-off-the-shelf*) peu coûteux, efficaces et très automatisés. Les systèmes de commande sont également de plus en plus interconnectés avec des réseaux non IACS pour des raisons commerciales valables. Ces dispositifs, les technologies de réseau ouvertes, ainsi que la connectivité croissante augmentent le risque de cyberattaque contre le matériel et le logiciel du système de commande. Cette faiblesse peut avoir des conséquences au niveau de la santé, sécurité et environnement (HSE - *health, safety and environmental*), des conséquences financières et/ou des conséquences au niveau de la réputation dans les systèmes de commande déployés.

Les organismes qui déploient des solutions de cybersécurité pour le traitement de l'information (IT - *information technology*) commerciale pour traiter de la sécurité des équipements IACS peuvent ne pas pleinement concevoir les résultats de ces décisions. Nombre des applications IT commerciales et solutions de sécurité peuvent être appliquées aux équipements IACS, mais elles doivent l'être de façon appropriée afin d'éviter toute conséquence indésirable. Pour cette raison, l'approche utilisée pour définir les exigences système doit se baser sur une combinaison d'exigences fonctionnelles et d'appréciation du risque, comprenant également le plus souvent une connaissance des problèmes fonctionnels.

Il convient que les mesures de sécurité des IACS n'aient pas la capacité de causer la perte des services et fonctions essentiels, procédures d'urgence incluses. (Ce qui est le cas des mesures de sécurité IT le plus souvent déployées.) Les objectifs de la sécurité IACS se concentrent sur la disponibilité du système de commande, sur la protection des installations et sur leur fonctionnement (même en mode dégradé), et sur la réponse système limitée dans le temps. Les objectifs de la sécurité IT n'accordent généralement pas la même importance à ces aspects. Ils peuvent être plus tournés vers la protection des informations que vers les actifs physiques. Ces objectifs différents doivent être clairement établis en tant que qu'objectifs de sécurité, sans tenir compte du degré d'intégration des installations. Il convient que l'identification des services et fonctions essentiels au fonctionnement, telle qu'exigée par l'IEC 62443-2-1[2], soit une étape clé de l'appréciation du risque. (Par exemple, dans certaines installations, le soutien technique peut être défini comme étant une fonction ou un service non essentiel.) Dans certains cas, il peut être acceptable qu'une action de sécurité cause une perte temporaire d'une fonction ou d'un service non essentiel, contrairement à une fonction ou un service essentiel qu'il convient de ne pas compromettre.

La présente norme part du principe qu'un programme de sécurité a été établi et qu'il est fonctionnel conformément à l'IEC 62443-2-1. En outre, la gestion des correctifs est par principe mise en œuvre conformément aux recommandations détaillées dans l'IEC/TR 62443-2-3 [5], en utilisant les exigences de système de commande appropriées et les améliorations d'exigences, comme décrit dans la présente norme. De plus, l'IEC 62443-3-2 [8] décrit la façon dont un projet définit les niveaux de sécurité (SL) basés

---

1 Les chiffres entre crochets se réfèrent à la Bibliographie.

2 De nombreux documents de la série IEC 62443 sont actuellement à l'étude ou en cours d'élaboration.

sur le risque. Ces derniers sont ensuite utilisés pour sélectionner des produits avec les capacités de sécurité techniques appropriées, comme cela est détaillé dans la présente norme. L'apport majeur de la présente norme inclut l'ISO/IEC 27002 [15] et le NIST SP800-53, rév. 3 [24] (voir l'Article 2 et la Bibliographie pour une liste plus complète des sources documentaires).

La série IEC 62443 a principalement pour objet de fournir un cadre flexible qui facilite le traitement des vulnérabilités actuelles et futures dans l'IACS et l'application des atténuations nécessaires de manière systématique et défendable. Il est important de comprendre que l'intention de la série IEC 62443 est de construire des extensions à la sécurité des entreprises qui adaptent les exigences pour les systèmes IT commerciaux et les combinent avec les exigences uniques pour la disponibilité forte dont l'IACS a besoin.

0.2 Objectif et public visé

Le public de la communauté IACS visé par la présente norme est constitué des propriétaires d'actif, des intégrateurs de système, des fournisseurs de produit, des fournisseurs de service et, lorsque cela est approprié, des autorités de conformité. Les autorités de conformité comprennent les agences et régulateurs gouvernementaux ayant l'autorité légale à réaliser des audits permettant de vérifier la conformité aux lois et régulations en vigueur.

Les intégrateurs de système, fournisseurs de produit et fournisseurs de service utilisent la présente norme pour évaluer la capacité de fourniture de sécurité fonctionnelle de leurs produits et services afin de satisfaire aux exigences de niveau de sécurité cible (SL-T - *target security level*) du propriétaire d'actif. Comme pour l'évaluation des SL-T, l'applicabilité des exigences de système de commande individuelles (SR - *system requirement*) et des améliorations d'exigences (RE - *requirement enhancement*) doivent se baser sur les politiques de sécurité, procédures et appréciation du risque du propriétaire d'actif dans le contexte de leur site spécifique. Il est à noter que certaines SR contiennent des conditions spécifiques pour les exceptions admissibles, comme lorsque la conformité aux SR enfreint les exigences fondamentales de fonctionnement d'un système de commande (ce qui peut entraîner des contre-mesures compensatoires).

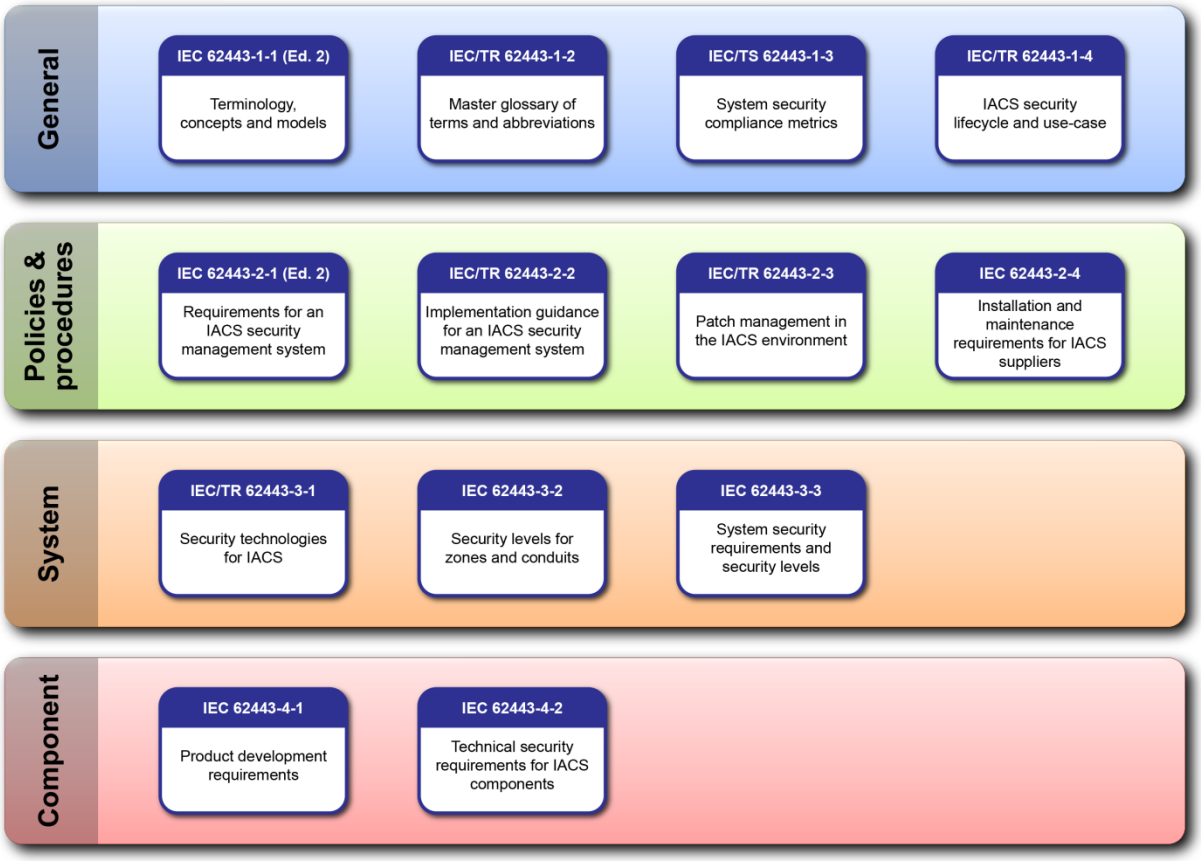
Lors de la conception d'un système de commande conformément à l'ensemble des SR associées aux SL-T spécifiques, il n'est pas nécessaire que chaque composant du système de commande proposé prenne en charge chaque exigence système au niveau imposé dans la présente norme. Des contre-mesures compensatoires peuvent être employées afin de fournir les fonctionnalités nécessaires à d'autres sous-systèmes, de façon à ce que les exigences générales SL-T soient satisfaites au niveau du système de commande. Il convient que l'inclusion des contre-mesures compensatoires lors de la phase de conception soit accompagnée par une documentation complète de façon à ce que le SL et le SL-A (système de commande) du système de commande atteint reflètent pleinement les capacités de sécurité prévues inhérentes à la conception. De même, lors de l'essai de certification et/ou des audits post-installation, des contre-mesures compensatoires peuvent être utilisées et documentées afin de satisfaire au SL général du système de commande.

La présente norme n'est pas assez détaillée pour concevoir et construire une architecture de sécurité intégrée. Cela exige une analyse supplémentaire au niveau du système et l'élaboration d'exigences dérivées qui sont le sujet d'autres normes de la série IEC 62443 (voir 0). Il est à noter que la présente norme n'a pas pour objet de fournir des spécifications assez détaillées pour construire une architecture de sécurité. L'objectif est de définir un ensemble d'exigences minimales et communes pour atteindre progressivement des niveaux de sécurité plus élevés. La conception effective d'une architecture qui satisfait à ces exigences relève des intégrateurs de système et des fournisseurs de produit. Ces derniers disposent d'une liberté de choix individuels, ce qui renforce la compétition et l'innovation. Ainsi, la présente norme adhère strictement aux exigences fonctionnelles spécifiques, et ne traite pas de la manière dont il convient de satisfaire à ces exigences.

0.3 Utilisation dans d'autres parties de la série IEC 62443

La Figure 1 donne une représentation graphique de la série IEC 62443 lors de la rédaction de la présente norme.

L'IEC 62443-3-2 utilise les SR et RE comme liste de vérification. Après que le système à l'étude (SuC) a été décrit en matière de zones et conduits, et qu'un SL cible individuel a été assigné à ces zones et conduits, les SR et RE dans la présente norme, ainsi que leur mapping aux SL de capacité (SL-C), sont utilisés pour dresser une liste d'exigences auxquelles la conception du système de commande doit satisfaire. L'intégrité de la conception de système de commande donnée peut alors être vérifiée, et ainsi fournir les SL-A.



Anglais	Français
General	Généralités
Policies & procedures	Politiques et procédures
System	Système
Component	Composant

Figure 1 – Structure de la série IEC 62443

L'IEC/TS 62443-1-3 [2] utilise les exigences fondamentales (FR - *foundational requirement*), les SR, les RE et le mapping aux SL-C comme liste de vérification pour l'essai d'intégrité de la spécification des critères quantitatifs. Les critères quantitatifs de conformité à la sécurité dépendent du contexte. Avec l'IEC 62443-3-2, les évaluations SL-T du propriétaire d'actif sont traduites en critères quantitatifs pouvant être utilisés pour la prise en charge de l'analyse du système, pour la conception d'études de compromis, et pour l'élaboration d'une architecture de sécurité.

L'IEC 62443-4-1 [9] traite des exigences générales lors de l'élaboration de produits. Comme telle, l'IEC 62443-4-1 est centrée sur le fournisseur de produit. Les exigences de sécurité des produits sont issues de la liste des exigences de base et des RE spécifiées dans la présente norme. Les spécifications normatives de qualité de l'IEC 62443-4-1 sont utilisées lors de l'élaboration des capacités de ces produits.

L'IEC 62443-4-2 [10] contient des ensembles d'exigences dérivées qui fournissent un mapping détaillé des SR spécifiées dans la présente norme aux sous-systèmes et composants du SuC. Au moment de la rédaction de la présente norme, les catégories de composants traités dans l'IEC 62443-4-2 étaient: les appareils intégrés, les appareils hôtes, les dispositifs de réseau et les applications. En tant que telle, l'IEC 62443-4-2 est centrée sur le fournisseur (de produit et de service). Les exigences de sécurité des produits sont d'abord issues de la liste des exigences de base et des RE spécifiées dans la présente norme. Les exigences et critères de sécurité de l'IEC 62443-3-2 et de l'IEC/TS 62443-1-3 sont utilisés pour approfondir ces exigences normatives dérivées.

RÉSEAUX INDUSTRIELS DE COMMUNICATION – SÉCURITÉ DANS LES RÉSEAUX ET LES SYSTÈMES –

Partie 3-3: Exigences de sécurité des systèmes et niveaux de sécurité

1 Domaine d'application

La présente partie de la série IEC 62443 fournit des exigences système (SR) de commande techniques détaillées associées aux sept exigences fondamentales (FR) décrites dans l'IEC 62443-1-1, y compris la définition des exigences des niveaux de sécurité de capacité du système de commande, SL-C (système de commande). Ces exigences sont utilisées par plusieurs membres de la communauté des systèmes d'automatisation et de commande industrielles (IACS) ainsi que les zones et conduits définis pour le système à l'étude (SuC), tout en développant le SL cible du système de commande approprié, SL-T (système de commande) pour un actif spécifique.

Comme cela est défini dans l'IEC 62443-1-1, il existe sept FR au total:

a) Commande d'identification et d'authentification (IAC - *identification and authentication control*),
b) Commande d'utilisation (UC - *use control*),
c) Intégrité du système (SI - *system integrity*),
d) Confidentialité des données (DC - *data confidentiality*),
e) Flux de données réduit (RDF - *restricted data flow*),
f) Réponse rapide aux événements (TRE - *timely response to events*),
g) Disponibilité des ressources (RA - *ressource availability*).

Ces sept exigences constituent le fondement des SL de capacité du système de commande, SL-C (système de commande). La présente norme a pour objet de définir la capacité de sécurité au niveau du système de commande. Les SL cible (SL-T) ou les SL atteints (SL-A), quant à eux, ne relèvent pas du domaine d'application de la présente norme.

Voir l'IEC 62443-2-1 pour un ensemble équivalent de SR de capacité non techniques et relatives au programme nécessaires pour atteindre pleinement un SL cible de système de commande.

2 Références normatives

Les documents suivants sont cités dans le texte de sorte qu'ils 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 62443-1-1:2009, *Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models* (disponible en anglais seulement)

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*