



BSI Standards Publication

Industrial communication networks – Network and system security

Part 3-3: System security requirements and security levels (IEC 62443-3-3:2013)

National foreword

This British Standard is the UK implementation of EN IEC 62443-3-3:2019. It is identical to IEC 62443-3-3:2013, incorporating corrigendum April 2014. It supersedes BS IEC 62443-3-3:2013, which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee GEL/65/3, Industrial communications: process measurement and control, including fieldbus.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2019
Published by BSI Standards Limited 2019

ISBN 978 0 539 01944 5

ICS 25.040.40; 35.110

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 October 2013.

Amendments/corrigenda issued since publication

Date	Text affected
31 May 2014	Implementation of IEC corrigendum April 2014: first bullet point in clause 7.6.4 updated and both rows for SR 3.4 in Table B.1 updated
31 May 2019	This corrigendum renumbers BS IEC 62443-3-3:2013 as BS EN IEC 62443-3-3:2019

English Version

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

Réseaux industriels de communication - Sécurité dans les
réseaux et les systèmes - Partie-3: Exigences relatives à la
sécurité dans les systèmes et niveaux de sécurité
(IEC 62443-3-3:2013)

Industrielle Kommunikationsnetze - IT-Sicherheit für Netze
und Systeme - Teil 3-3: Systemanforderungen zur IT-
Sicherheit und Security-Level
(IEC 62443-3-3:2013)

This European Standard was approved by CENELEC on 2019-04-03. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.



European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

European foreword

This document (EN IEC 62443-3-3:2019) consists of the text of IEC 62443-3-3:2013 prepared by IEC/TC 65 "Industrial-process measurement, control and automation".

The following dates are fixed:

- latest date by which the document has to be implemented at national level by publication of an identical national standard or by endorsement (dop) 2020-04-03
- latest date by which the national standards conflicting with the document have to be withdrawn (dow) 2022-04-03

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CENELEC shall not be held responsible for identifying any or all such patent rights.

Endorsement notice

The text of the International Standard IEC 62443-3-3:2013 was approved by CENELEC as a European Standard without any modification.

In the official version, for Bibliography, the following notes have to be added for the standards indicated:

IEC 62443-2-4	NOTE	Harmonized as EN IEC 62443-2-4
IEC 62443-4-1	NOTE	Harmonized as EN IEC 62443-4-1
IEC 62443-4-2	NOTE	Harmonized as EN IEC 62443-4-2
ISO/IEC 27002	NOTE	Harmonized as EN ISO/IEC 27002

Annex ZA

(normative)

Normative references to international publications with their corresponding European publications

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.

NOTE 1 Where an International Publication has been modified by common modifications, indicated by (mod), the relevant EN/HD applies.

NOTE 2 Up-to-date information on the latest versions of the European Standards listed in this annex is available here: www.cenelec.eu.

<u>Publication</u>	<u>Year</u>	<u>Title</u>	<u>EN/HD</u>	<u>Year</u>
IEC 62443-2-1	-	Industrial communication networks -- Network and system security - Part 2-1: Establishing an industrial automation and control system security program		-
IEC/TS 62443-1-1	2009	Industrial communication networks -- Network and system security - Part 1-1: Terminology, concepts and models		-

This page deliberately left blank

CONTENTS

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

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

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

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

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

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

11.10.4 Security levels	66
Annex A (informative) Discussion of the SL vector	67
Annex B (informative) Mapping of SRs and REs to FR SL levels 1-4	75
Bibliography	79
Figure 1 – Structure of the IEC 62443 series	13
Figure A.1 – High-level process-industry example showing zones and conduits	69
Figure A.2 – High-level manufacturing example showing zones and conduits	70
Figure A.3 – Schematic of correlation of the use of different SL types	71
Table B.1 – Mapping of SRs and REs to FR SL levels 1-4 (1 of 4)	75

INTERNATIONAL ELECTROTECHNICAL COMMISSION

**INDUSTRIAL COMMUNICATION NETWORKS –
NETWORK AND SYSTEM SECURITY –****Part 3-3: System security requirements and security levels**

FOREWORD

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

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

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

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

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

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

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

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

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

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

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 62443-2-1², 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).

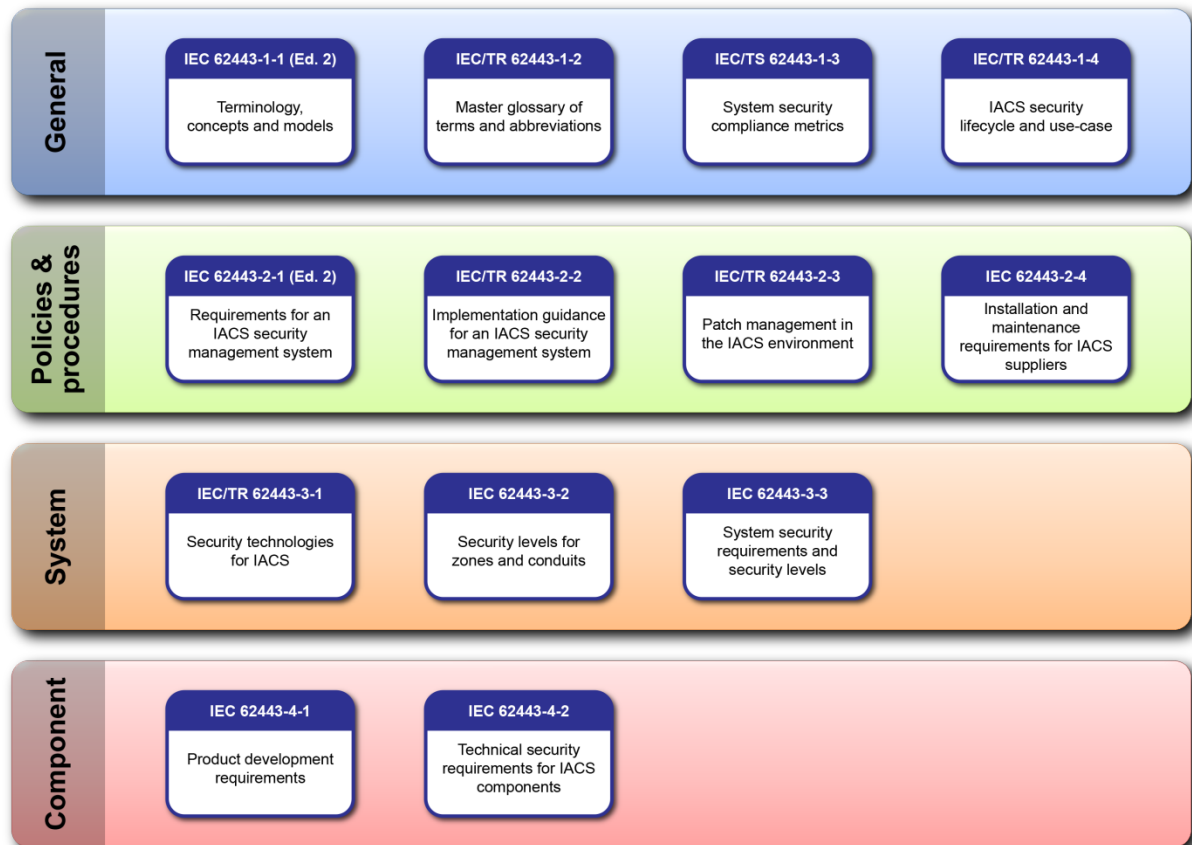
When designing a control system to meet the set of SRs associated with specific SL-Ts, it is not necessary that every component of the proposed control system support every system requirement to the level mandated in this standard. Compensating countermeasures can be employed to provide the needed functionality 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.



IEC 2031/13

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*

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

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in IEC 62443-1-1 and in IEC 62443-2-1, as well as the following, apply.

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

3.1.1

asset

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

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

3.1.2

asset owner

individual or company responsible for one or more IACS

Note 1 to entry: The term "asset owner" is used in place of the generic term "end user" to provide differentiation.

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

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

3.1.3

attack

assault on a system that derives from an intelligent threat

Note 1 to entry: For example, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system

Note 2 to entry: There are different commonly recognized classes of attack:

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

3.1.4

authentication

provision of assurance that a claimed characteristic of an identity is correct

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

3.1.5

authenticator

means used to confirm the identity of a user (human, software process or device)

Note 1 to entry: For example, a password or token may be used as an authenticator.

3.1.6

authenticity

property that an entity is what it claims to be

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

3.1.7

automatic

process or equipment that, under specified conditions, functions without human intervention

3.1.8

availability

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

3.1.9

communication channel

specific logical or physical communication link between assets

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

3.1.10

compensating countermeasure

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

Note 1 to entry: Examples include:

- (component-level): locked cabinet around a controller that doesn't have sufficient cyber access control countermeasures;
- (control system/zone-level): physical access control (guards, gates and guns) to protect a control room to restrict access to a group of known personnel to compensate for the technical requirement for personnel to be uniquely identified by the IACS; and
- (component-level): a vendor's programmable logic controller (PLC) can't meet the access control capabilities from an end-user, so the vendor puts a firewall in front of the PLC and sells it as a system.

3.1.11

compliance authority

entity with legal jurisdiction to determine the adequacy of a security assessment, implementation or effectiveness as specified in a governing document

3.1.12

conduit

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

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

3.1.13

confidentiality

preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information

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

3.1.14

connection

association established between two or more endpoints which supports the establishment of a session

3.1.15

consequence

condition or state that logically or naturally follows from an event

3.1.16

control system

hardware and software components of an IACS

3.1.17**countermeasure**

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

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

3.1.18**degraded mode**

mode of operation in the presence of faults which have been anticipated in the design of the control system

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

3.1.19**demilitarized zone**

common, limited network of servers joining two or more zones for the purpose of controlling data flow between zones

Note 1 to entry: Demilitarized zones (DMZs) are typically used to avoid direct connections between different zones.

3.1.20**device**

asset incorporating one or more processors with the capability of sending or receiving data/control to or from another asset

Note 1 to entry: Examples include controllers, human-machine interfaces (HMIs), PLCs, remote terminal units (RTUs), transmitters, actuators, valves, network switches, etc.

3.1.21**environment**

surrounding objects, region or circumstances which may influence the behavior of the IACS and/or may be influenced by the IACS

3.1.22**essential function**

function or capability that is required to maintain health, safety, the environment and availability for the equipment under control

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

3.1.23**event**

occurrence of or change to a particular set of circumstances

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

3.1.24**firecall**

method established to provide emergency access to a secure control system

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

3.1.25

identifier

symbol, unique within its security domain, that identifies, indicates or names an entity which makes an assertion or claim of identity

3.1.26

identify

assertion of an identity

3.1.27

impact

evaluated consequence of a particular event

3.1.28

incident

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

3.1.29

industrial automation and control system

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

3.1.30

integrity

property of protecting the accuracy and completeness of assets

3.1.31

least privilege

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

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

3.1.32

mobile code

program transferred between a remote, possibly “untrusted” system, across a network or via removable media that can be executed unchanged on a local system without explicit installation or execution by the recipient

Note 1 to entry: Examples of mobile code include JavaScript, VBScript, Java applets, ActiveX controls, Flash animations, Shockwave movies, and Microsoft Office macros.

3.1.33

non-repudiation

ability to prove the occurrence of a claimed event or action and its originating entities

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

3.1.34

product supplier

manufacturer of hardware and/or software product

Note 1 to entry: This term is used in place of the generic word “vendor” to provide differentiation.

3.1.35**remote access**

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

3.1.36**role**

set of connected behaviors, privileges and obligations associated with all users (humans, software processes or devices) of an IACS

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

3.1.37**safety instrumented system**

system used to implement one or more safety-related functions

3.1.38**security level**

measure of confidence that the IACS is free from vulnerabilities and functions in the intended manner

Note 1 to entry: Vulnerabilities can either be designed into the IACS, inserted at any time during its lifecycle or result from changing threats. Designed-in vulnerabilities may be discovered long after the initial deployment of the IACS, for example an encryption technique has been broken or an improper policy for account management such as not removing old user accounts. Inserted vulnerabilities may be the result of a patch or a change in policy that opens up a new vulnerability.

3.1.39**service provider**

organization (internal or external organization, manufacturer, etc.) that has agreed to undertake responsibility for providing a given support service and obtaining, when specified, supplies in accordance with an agreement

Note 1 to entry: This term is used in place of the generic word “vendor” to provide differentiation.

3.1.40**session**

semi-permanent, stateful and interactive information interchange between two or more communicating devices

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

3.1.41**session ID**

identifier used to indicate a specific session entry

3.1.42**set point**

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

3.1.43**system integrator**

person or company that specializes in bringing together component subsystems into a whole and ensuring that those subsystems perform in accordance with project specifications

3.1.44**threat**

circumstance or event with the potential to adversely affect operations (including mission, functions, image or reputation), assets, control systems or individuals via unauthorized access, destruction, disclosure, modification of data and/or denial of service

3.1.45

trust

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

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

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

3.1.46

untrusted

not meeting predefined requirements to be trusted

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

3.1.47

zone

grouping of logical or physical assets that share common security requirements

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

3.2 Abbreviated terms and acronyms

AES	Advanced encryption standard
API	Application programming interface
ASLR	Address space layout randomization
BPCS	Basic process control system
CA	Certification authority
CIP	Critical infrastructure protection
COTS	Commercial off the shelf
CRL	Certificate revocation list
DC	Data confidentiality
DEP	Data execution prevention
DHCP	Dynamic host configuration protocol
DMZ	Demilitarized zone
DNS	Domain name service
DoS	Denial of service
EICAR	European Institute for Computer Antivirus Research
EMI	Electromagnetic interference
FAT	Factory acceptance testing
FIPS	<i>[US NIST] Federal Information Processing Standard</i>
FR	Foundational requirement
FS-PLC	Functional safety PLC
FTP	File transfer protocol
GLONASS	Global Navigation Satellite System
GPS	Global Positioning System
HMI	Human-machine interface
HSE	Health, safety and environmental
HTTP	Hypertext transfer protocol

HTTPS	HTTP secure
IAC	Identification and authentication control
IACS	Industrial automation and control system(s)
IAMS	Instrument asset management system
ID	Identifier
IDS	Intrusion detection system
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IM	Instant messaging
IP	Internet Protocol
IPS	Intrusion prevention system
ISA	International Society of Automation
ISO	International Organization for Standardization
IT	Information technology
MES	Manufacturing execution system
NERC	North American Electric Reliability Corporation
NIST	U.S. National Institute of Standards and Technology
NX	No Execute
OCSP	Online certificate status protocol
OWASP	Open Web Application Security Project
PDF	Portable document format
PKI	Public key infrastructure
PLC	Programmable logic controller
RA	Resource availability
RAM	Random access memory
RDF	Restricted data flow
RE	Requirement enhancement
RFC	[IETF] Request for Comment
RJ	Registered jack
RTU	Remote terminal unit
SAT	Site acceptance testing
SHA	Secure hash algorithm
SI	System integrity
SIEM	Security Information and Event Management
SIF	Safety instrumented function
SIL	Safety integrity level
SIS	Safety instrumented system
SL	Security level
SL-A	Achieved security level
SL-C	Capability security level
SL-T	Target security level
SP	[US NIST] Special Publication