

AS IEC 62443.4.2:2025
IEC 62443-4-2:2019



STANDARDS
Australia



Security for industrial automation and control systems

Part 4.2: Technical security requirements for IACS components



currently in preview, click buy full version

AS IEC 62443.4.2:2025

This Australian Standard® was prepared by IT-006, Industrial Process Measurement, Control and Automation. It was approved on behalf of Standards Australia's Standards Development and Accreditation Committee on 13 January 2025.

This Standard was published on 31 January 2025.

The following are represented on Committee IT-006:

- Australia Safety Critical Systems Association
- Australian Computer Society
- Australian Energy Producers
- Australian Industry Group
- Engineers Australia
- ISACA Sydney
- Institute of Instrumentation, Control & Automation Australia

This Standard was issued in draft form for comment as DR AS IEC 62443.4.2:2024.

Keeping Standards up-to-date

Ensure you have the latest versions of our publications and keep up-to-date about Amendments, Rulings, Withdrawals, and new projects by visiting:

www.standards.org.au

ISBN 978 1 76175 009 0

Security for industrial automation and control systems

Part 4.2: Technical security requirements for IACS components

First published as AS IEC 62443.4.2: 025



© IEC Geneva Switzerland 2025 — All rights reserved
© Standards Australia Limited 2025

All rights are reserved. No part of this work may be reproduced or copied in any form or by any means, electronic or mechanical, including photocopying, without the written permission of either the IEC or the publisher, unless otherwise permitted under the Copyright Act 1968 (Cth). If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please see the contact details on the back cover or the contact us page of the website for further information.

Preface

This Standard was prepared by the Standards Australia Committee IT-006, Industrial Process Measurement, Control and Automation.

The objective of this document is to provide detailed technical control system component requirements (CRs) associated with the seven foundational requirements (FRs) described in IEC TS 62443-1-1, including defining the requirements for control system capability security levels and their components, SL-C(component).

This document is identical with, and has been reproduced from IEC 62443-4-2:2019, *Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components*.

As this document has been reproduced from an international document, a full point substitutes for a comma when referring to a decimal marker.

Australian or Australian/New Zealand Standards that are identical adoptions of international normative references may be used interchangeably. Refer to the online catalogue for information on specific Standards.

The terms “normative” and “informative” are used in Standards to define the application of the appendices or annexes to which they apply. A “normative” appendix or annex is an integral part of a Standard, whereas an “informative” appendix or annex is only for information and guidance.

Contents

Preface	ii
FOREWORD	xi
INTRODUCTION	xiii
0.1 Overview	xiii
0.2 Purpose and intended audience	xiii
1 Scope	1
2 Normative references	1
3 Terms, definitions, abbreviated terms, acronyms, and conventions	2
3.1 Terms and definitions	2
3.2 Abbreviated terms and acronyms	8
3.3 Conventions	10
4 Common component security constraints	10
4.1 Overview	10
4.2 CCSC 1: Support of essential functions	11
4.3 CCSC 2: Compensating countermeasures	11
4.4 CCSC 3: Least privilege	11
4.5 CCSC 4: Software development process	11
5 FR 1 – Identification and authentication control	11
5.1 Purpose and SL-C(IAC) descriptions	11
5.2 Rationale	11
5.3 CR 1.1 – Human user identification and authentication	12
5.3.1 Requirement	12
5.3.2 Rationale and supplemental guidance	12
5.3.3 Requirement enhancements	12
5.3.4 Security levels	12
5.4 CR 1.2 – Software process and device identification and authentication	13
5.4.1 Requirement	13
5.4.2 Rationale and supplemental guidance	13
5.4.3 Requirement enhancements	13
5.4.4 Security levels	13
5.5 CR 1.3 – Account management	14
5.5.1 Requirement	14
5.5.2 Rationale and supplemental guidance	14
5.5.3 Requirement enhancements	14
5.5.4 Security levels	14
5.6 CR 1.4 – Identifier management	14
5.6.1 Requirement	14
5.6.2 Rationale and supplemental guidance	14
5.6.3 Requirement enhancements	15
5.6.4 Security levels	15
5.7 CR 1.5 – Authenticator management	15
5.7.1 Requirement	15
5.7.2 Rationale and supplemental guidance	15
5.7.3 Requirement enhancements	16
5.7.4 Security levels	16
5.8 CR 1.6 – Wireless access management	16
5.9 CR 1.7 – Strength of password-based authentication	16
5.9.1 Requirement	16
5.9.2 Rationale and supplemental guidance	16
5.9.3 Requirement enhancements	17
5.9.4 Security levels	17
5.10 CR 1.8 – Public key infrastructure certificates	17

5.10.1	Requirement	17
5.10.2	Rationale and supplemental guidance	17
5.10.3	Requirement enhancements	17
5.10.4	Security levels	17
5.11	CR 1.9 – Strength of public key-based authentication	18
5.11.1	Requirement	18
5.11.2	Rationale and supplemental guidance	18
5.11.3	Requirement enhancements	19
5.11.4	Security levels	19
5.12	CR 1.10 – Authenticator feedback	19
5.12.1	Requirement	19
5.12.2	Rationale and supplemental guidance	19
5.12.3	Requirement enhancements	19
5.12.4	Security levels	19
5.13	CR 1.11 – Unsuccessful login attempts	19
5.13.1	Requirement	19
5.13.2	Rationale and supplemental guidance	20
5.13.3	Requirement enhancements	20
5.13.4	Security levels	20
5.14	CR 1.12 – System use notification	20
5.14.1	Requirement	20
5.14.2	Rationale and supplemental guidance	20
5.14.3	Requirement enhancements	21
5.14.4	Security levels	21
5.15	CR 1.13 – Access via untrusted networks	21
5.16	CR 1.14 – Strength of symmetric key-based authentication	21
5.16.1	Requirement	21
5.16.2	Rationale and supplemental guidance	21
5.16.3	Requirement enhancements	22
5.16.4	Security levels	22
6	FR 2 – Use control	22
6.1	Purpose and SL-C(UC) descriptions	22
6.2	Rationale	22
6.3	CR 2.1 – Authorization enforcement	23
6.3.1	Requirement	23
6.3.2	Rationale and supplemental guidance	23
6.3.3	Requirement enhancements	23
6.3.4	Security levels	24
6.4	CR 2.2 – Wireless use control	24
6.4.1	Requirement	24
6.4.2	Rationale and supplemental guidance	24
6.4.3	Requirement enhancements	24
6.4.4	Security levels	24
6.5	CR 2.3 – Use control for portable and mobile devices	25
6.6	CR 2.4 – Mobile code	25
6.7	CR 2.5 – Session lock	25
6.7.1	Requirement	25
6.7.2	Rationale and supplemental guidance	25
6.7.3	Requirement enhancements	25
6.7.4	Security levels	25
6.8	CR 2.6 – Remote session termination	25
6.8.1	Requirement	25
6.8.2	Rationale and supplemental guidance	25
6.8.3	Requirement enhancements	26
6.8.4	Security levels	26
6.9	CR 2.7 – Concurrent session control	26
6.9.1	Requirement	26
6.9.2	Rationale and supplemental guidance	26

6.9.3	Requirement enhancements	26
6.9.4	Security levels	26
6.10	CR 2.8 – Auditable events	26
6.10.1	Requirement	26
6.10.2	Rationale and supplemental guidance	27
6.10.3	Requirement enhancements	27
6.10.4	Security levels	27
6.11	CR 2.9 – Audit storage capacity	27
6.11.1	Requirement	27
6.11.2	Rationale and supplemental guidance	27
6.11.3	Requirement enhancements	28
6.11.4	Security levels	28
6.12	CR 2.10 – Response to audit processing failures	28
6.12.1	Requirement	28
6.12.2	Rationale and supplemental guidance	28
6.12.3	Requirement enhancements	28
6.12.4	Security levels	29
6.13	CR 2.11 – Timestamps	29
6.13.1	Requirement	29
6.13.2	Rationale and supplemental guidance	29
6.13.3	Requirement enhancements	29
6.13.4	Security levels	29
6.14	CR 2.12 – Non-repudiation	29
6.14.1	Requirement	29
6.14.2	Rationale and supplemental guidance	30
6.14.3	Requirement enhancements	30
6.14.4	Security levels	30
6.15	CR 2.13 – Use of physical diagnostic and test interfaces	30
7	FR 3 – System integrity	30
7.1	Purpose and SL-C(SI) descriptions	30
7.2	Rationale	30
7.3	CR 3.1 – Communication integrity	31
7.3.1	Requirement	31
7.3.2	Rationale and supplemental guidance	31
7.3.3	Requirement enhancements	31
7.3.4	Security levels	32
7.4	CR 3.2 – Protection from malicious code	32
7.5	CR 3.3 – Security functionality verification	32
7.5.1	Requirement	32
7.5.2	Rationale and supplemental guidance	32
7.5.3	Requirement enhancements	32
7.5.4	Security levels	33
7.6	CR 3.4 – Software and information integrity	33
7.6.1	Requirement	33
7.6.2	Rationale and supplemental guidance	33
7.6.3	Requirement enhancements	33
7.6.4	Security levels	33
7.7	CR 3.5 – Input validation	34
7.7.1	Requirement	34
7.7.2	Rationale and supplemental guidance	34
7.7.3	Requirement enhancements	34
7.7.4	Security levels	34
7.8	CR 3.6 – Deterministic output	34
7.8.1	Requirement	34
7.8.2	Rationale and supplemental guidance	34
7.8.3	Requirement enhancements	35
7.8.4	Security levels	35
7.9	CR 3.7 – Error handling	35

7.9.1	Requirement	35
7.9.2	Rationale and supplemental guidance	35
7.9.3	Requirement enhancements	35
7.9.4	Security levels	35
7.10	CR 3.8 – Session integrity	36
7.10.1	Requirement	36
7.10.2	Rationale and supplemental guidance	36
7.10.3	Requirement enhancements	36
7.10.4	Security levels	36
7.11	CR 3.9 – Protection of audit information	36
7.11.1	Requirement	36
7.11.2	Rationale and supplemental guidance	36
7.11.3	Requirement enhancements	37
7.11.4	Security levels	37
7.12	CR 3.10 – Support for updates	37
7.13	CR 3.11 – Physical tamper resistance and detection	37
7.14	CR 3.12 – Provisioning product supplier roots of trust	37
7.15	CR 3.13 – Provisioning asset owner roots of trust	37
7.16	CR 3.14 – Integrity of the boot process	37
8	FR 4 – Data confidentiality	37
8.1	Purpose and SL-C(DC) descriptions	37
8.2	Rationale	38
8.3	CR 4.1 – Information confidentiality	38
8.3.1	Requirement	38
8.3.2	Rationale and supplemental guidance	38
8.3.3	Requirement enhancements	38
8.3.4	Security levels	38
8.4	CR 4.2 – Information persistence	39
8.4.1	Requirement	39
8.4.2	Rationale and supplemental guidance	39
8.4.3	Requirement enhancements	39
8.4.4	Security levels	39
8.5	CR 4.3 – Use of cryptography	39
8.5.1	Requirement	39
8.5.2	Rationale and supplemental guidance	40
8.5.3	Requirement enhancements	40
8.5.4	Security levels	40
9	FR 5 – Restricted data flow	40
9.1	Purpose and SL-C(RLE) descriptions	40
9.2	Rationale	40
9.3	CR 5.1 – Network segmentation	41
9.3.1	Requirement	41
9.3.2	Rationale and supplemental guidance	41
9.3.3	Requirement enhancements	41
9.3.4	Security levels	41
9.4	CR 5.2 – Zone boundary protection	41
9.5	CR 5.3 – General-purpose person-to-person communication restrictions	42
9.6	CR 5.4 – Application partitioning	42
10	FR 6 – Timely response to events	42
10.1	Purpose and SL-C(TRE) descriptions	42
10.2	Rationale	42
10.3	CR 6.1 – Audit log accessibility	42
10.3.1	Requirement	42
10.3.2	Rationale and supplemental guidance	42
10.3.3	Requirement enhancements	43
10.3.4	Security levels	43
10.4	CR 6.2 – Continuous monitoring	43

10.4.1	Requirement	43
10.4.2	Rationale and supplemental guidance	43
10.4.3	Requirement enhancements	43
10.4.4	Security levels	43
11	FR 7 – Resource availability	44
11.1	Purpose and SL-C(RA) descriptions	44
11.2	Rationale	44
11.3	CR 7.1 – Denial of service protection	44
11.3.1	Requirement	44
11.3.2	Rationale and supplemental guidance	44
11.3.3	Requirement enhancements	44
11.3.4	Security levels	44
11.4	CR 7.2 – Resource management	45
11.4.1	Requirement	45
11.4.2	Rationale and supplemental guidance	45
11.4.3	Requirement enhancements	45
11.4.4	Security levels	45
11.5	CR 7.3 – Control system backup	45
11.5.1	Requirement	45
11.5.2	Rationale and supplemental guidance	45
11.5.3	Requirement enhancements	45
11.5.4	Security levels	46
11.6	CR 7.4 – Control system recovery and reconstitution	46
11.6.1	Requirement	46
11.6.2	Rationale and supplemental guidance	46
11.6.3	Requirement enhancements	46
11.6.4	Security levels	46
11.7	CR 7.5 – Emergency power	46
11.8	CR 7.6 – Network and security configuration settings	46
11.8.1	Requirement	46
11.8.2	Rationale and supplemental guidance	47
11.8.3	Requirement enhancements	47
11.8.4	Security levels	47
11.9	CR 7.7 – Least functionality	47
11.9.1	Requirement	47
11.9.2	Rationale and supplemental guidance	47
11.9.3	Requirement enhancements	47
11.9.4	Security levels	47
11.10	CR 7.8 – Control system component inventory	48
11.10.1	Requirement	48
11.10.2	Rationale and supplemental guidance	48
11.10.3	Requirement enhancements	48
11.10.4	Security levels	48
12	Software application requirements	48
12.1	Purpose	48
12.2	SAR 2.4 – Mobile code	48
12.2.1	Requirement	48
12.2.2	Rationale and supplemental guidance	49
12.2.3	Requirement enhancements	49
12.2.4	Security levels	49
12.3	SAR 3.2 – Protection from malicious code	49
12.3.1	Requirement	49
12.3.2	Rationale and supplemental guidance	49
12.3.3	Requirement enhancements	49
12.3.4	Security levels	49
13	Embedded device requirements	50
13.1	Purpose	50

13.2	EDR 2.4 – Mobile code	50
13.2.1	Requirement.....	50
13.2.2	Rationale and supplemental guidance.....	50
13.2.3	Requirement enhancements.....	50
13.2.4	Security levels.....	50
13.3	EDR 2.13 – Use of physical diagnostic and test interfaces.....	51
13.3.1	Requirement.....	51
13.3.2	Rationale and supplemental guidance.....	51
13.3.3	Requirement enhancements.....	51
13.3.4	Security levels.....	51
13.4	EDR 3.2 – Protection from malicious code.....	51
13.4.1	Requirement.....	51
13.4.2	Rationale and supplemental guidance.....	51
13.4.3	Requirement enhancements.....	52
13.4.4	Security levels.....	52
13.5	EDR 3.10 – Support for updates.....	52
13.5.1	Requirement.....	52
13.5.2	Rationale and supplemental guidance.....	52
13.5.3	Requirement enhancements.....	52
13.5.4	Security levels.....	52
13.6	EDR 3.11 – Physical tamper resistance and detection.....	53
13.6.1	Requirement.....	53
13.6.2	Rationale and supplemental guidance.....	53
13.6.3	Requirement enhancements.....	53
13.6.4	Security levels.....	53
13.7	EDR 3.12 – Provisioning product supplier roots of trust.....	53
13.7.1	Requirement.....	53
13.7.2	Rationale and supplemental guidance.....	53
13.7.3	Requirement enhancements.....	54
13.7.4	Security levels.....	54
13.8	EDR 3.13 – Provisioning asset owner roots of trust.....	54
13.8.1	Requirement.....	54
13.8.2	Rationale and supplemental guidance.....	54
13.8.3	Requirement enhancements.....	55
13.8.4	Security levels.....	55
13.9	EDR 3.14 – Integrity of the boot process.....	55
13.9.1	Requirement.....	55
13.9.2	Rationale and supplemental guidance.....	55
13.9.3	Requirement enhancements.....	55
13.9.4	Security levels.....	55
14	Host device requirements.....	56
14.1	Purpose.....	56
14.2	HDR 2.4 – Mobile code.....	56
14.2.1	Requirement.....	56
14.2.2	Rationale and supplemental guidance.....	56
14.2.3	Requirement enhancements.....	56
14.2.4	Security levels.....	56
14.3	HDR 2.13 – Use of physical diagnostic and test interfaces.....	57
14.3.1	Requirement.....	57
14.3.2	Rationale and supplemental guidance.....	57
14.3.3	Requirement enhancements.....	57
14.3.4	Security levels.....	57
14.4	HDR 3.2 – Protection from malicious code.....	57
14.4.1	Requirement.....	57
14.4.2	Rationale and supplemental guidance.....	57
14.4.3	Requirement enhancements.....	58
14.4.4	Security levels.....	58
14.5	HDR 3.10 – Support for updates.....	58

14.5.1	Requirement.....	58
14.5.2	Rationale and supplemental guidance.....	58
14.5.3	Requirement enhancements.....	58
14.5.4	Security levels.....	58
14.6	HDR 3.11 – Physical tamper resistance and detection.....	58
14.6.1	Requirement.....	58
14.6.2	Rationale and supplemental guidance.....	59
14.6.3	Requirement enhancements.....	59
14.6.4	Security levels.....	59
14.7	HDR 3.12 – Provisioning product supplier roots of trust.....	59
14.7.1	Requirement.....	59
14.7.2	Rationale and supplemental guidance.....	59
14.7.3	Requirement enhancements.....	60
14.7.4	Security levels.....	60
14.8	HDR 3.13 – Provisioning asset owner roots of trust.....	60
14.8.1	Requirement.....	60
14.8.2	Rationale and supplemental guidance.....	60
14.8.3	Requirement enhancements.....	61
14.8.4	Security levels.....	61
14.9	HDR 3.14 – Integrity of the boot process.....	61
14.9.1	Requirement.....	61
14.9.2	Rationale and supplemental guidance.....	61
14.9.3	Requirement enhancements.....	61
14.9.4	Security levels.....	61
15	Network device requirements.....	61
15.1	Purpose.....	61
15.2	NDR 1.6 – Wireless access management.....	62
15.2.1	Requirement.....	62
15.2.2	Rationale and supplemental guidance.....	62
15.2.3	Requirement enhancements.....	62
15.2.4	Security levels.....	62
15.3	NDR 1.13 – Access via untrusted networks.....	62
15.3.1	Requirement.....	62
15.3.2	Rationale and supplemental guidance.....	62
15.3.3	Requirement enhancements.....	63
15.3.4	Security levels.....	63
15.4	NDR 2.4 – Mobile code.....	63
15.4.1	Requirement.....	63
15.4.2	Rationale and supplemental guidance.....	63
15.4.3	Requirement enhancements.....	63
15.4.4	Security levels.....	64
15.5	NDR 2.13 – Use of physical diagnostic and test interfaces.....	64
15.5.1	Requirement.....	64
15.5.2	Rationale and supplemental guidance.....	64
15.5.3	Requirement enhancements.....	64
15.5.4	Security levels.....	64
15.6	NDR 3.2 – Protection from malicious code.....	65
15.6.1	Requirement.....	65
15.6.2	Rationale and supplemental guidance.....	65
15.6.3	Requirement enhancements.....	65
15.6.4	Security levels.....	65
15.7	NDR 3.10 – Support for updates.....	65
15.7.1	Requirement.....	65
15.7.2	Rationale and supplemental guidance.....	65
15.7.3	Requirement enhancements.....	65
15.7.4	Security levels.....	65
15.8	NDR 3.11 – Physical tamper resistance and detection.....	66
15.8.1	Requirement.....	66

15.8.2	Rationale and supplemental guidance.....	66
15.8.3	Requirement enhancements.....	66
15.8.4	Security levels.....	66
15.9	NDR 3.12 – Provisioning product supplier roots of trust.....	66
15.9.1	Requirement.....	66
15.9.2	Rationale and supplemental guidance.....	66
15.9.3	Requirement enhancements.....	67
15.9.4	Security levels.....	67
15.10	NDR 3.13 – Provisioning asset owner roots of trust.....	67
15.10.1	Requirement.....	67
15.10.2	Rationale and supplemental guidance.....	67
15.10.3	Requirement enhancements.....	68
15.10.4	Security levels.....	68
15.11	NDR 3.14 – Integrity of the boot process.....	68
15.11.1	Requirement.....	68
15.11.2	Rationale and supplemental guidance.....	68
15.11.3	Requirement enhancements.....	68
15.11.4	Security levels.....	68
15.12	NDR 5.2 – Zone boundary protection.....	69
15.12.1	Requirement.....	69
15.12.2	Rationale and supplemental guidance.....	69
15.12.3	Requirement enhancements.....	69
15.12.4	Security levels.....	69
15.13	NDR 5.3 – General purpose, person-to-person communication restrictions.....	70
15.13.1	Requirement.....	70
15.13.2	Rationale and supplemental guidance.....	70
15.13.3	Requirement enhancements.....	70
15.13.4	Security levels.....	70
Annex A	(informative) Device categories.....	71
Annex B	(informative) Mapping of CRs and REs to FR SLs 1-4.....	74
Bibliography		78

List of Figures

Figure 1 — Parts of the IEC 62443 series.....	xv
---	----

List of Tables

Table B.1 — Mapping of CRs and REs to FR SL levels 1-4.....	74
---	----

FOREWORD

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

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

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

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

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

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

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

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

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

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

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

The contents of the corrigendum 1 (2022-08) only applies to the French version.

INTRODUCTION

0.1 Overview

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

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

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

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

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

0.2 Purpose and intended audience

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

System integrators will use this document to assist them in procuring control system components that make up an IACS solution. The assistance will be in the form of helping system integrators specify the

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

2 Numbers in square brackets refer to the bibliography.

appropriate security capability level of the individual components they require. The primary standards for system integrators are IEC 62443-2-1 [1], IEC 62443-2-4 [3], IEC 62443-3-2 [5]³ and IEC 62443-3-3 that provide organizational and operational requirements for a security management system and guide them through the process of defining security zones for a system and the target security capability levels (SL-T) for those zones. Once the SL-T for each zone has been defined, components that provide the necessary security capabilities can be used to achieve the SL-T for each zone.

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

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

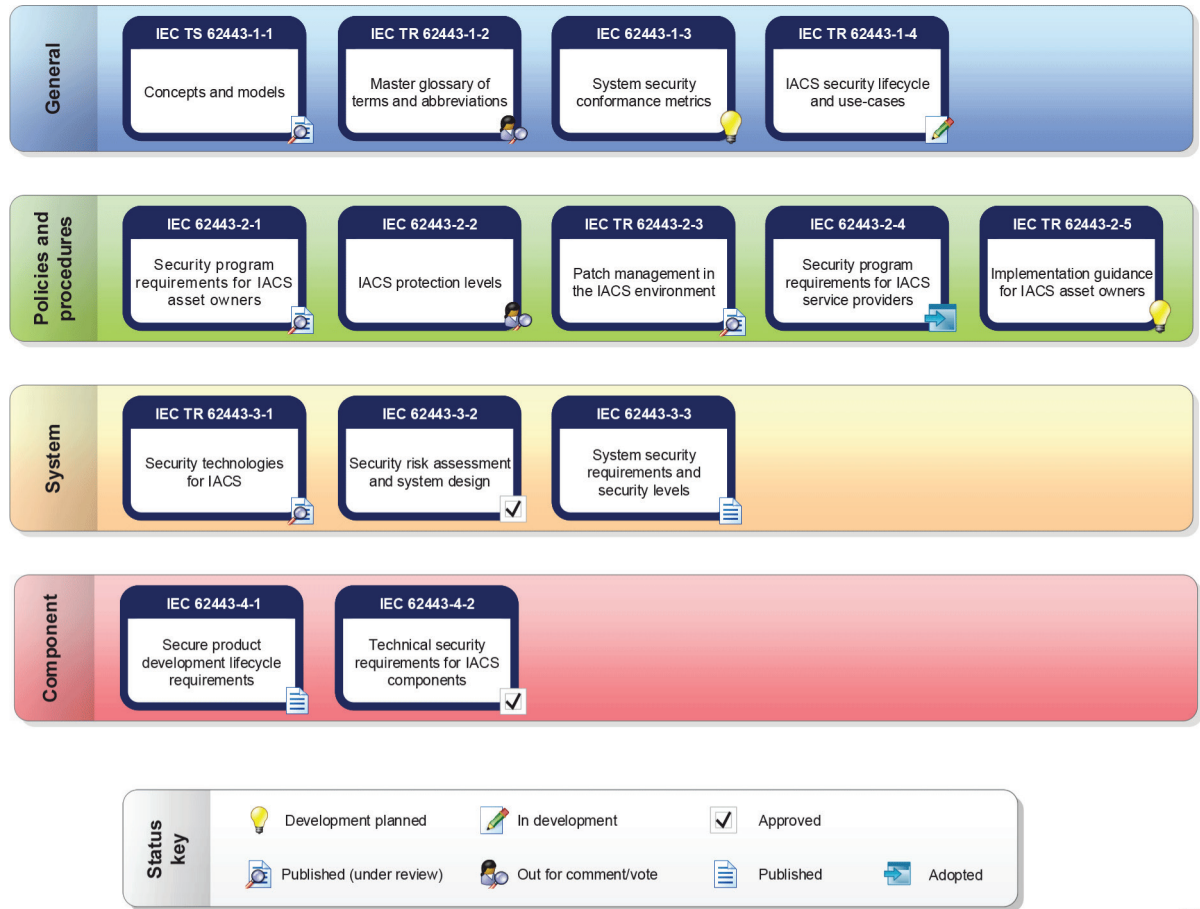
This document provides component requirements for four types of components: software application, embedded device, host device and network device. Thus, the CRs for each type of component will be designated as follows:

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

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

[Figure 1](#) shows a graphical depiction of the IEC 62443 series when this document was written.

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



IEC

Figure 1 — Parts of the IEC 62443 series

NOTES

Australian Standard®

Security for industrial automation and control systems

Part 4.2: Technical security requirements for IACS components

1 Scope

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

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

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

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

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

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

2 Normative references

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

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

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

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