AS IEC 62443.3.3:2024
IEC 62443-3-3:2013
IEC 62443-3-3:2013/COR1:2014

Australian STANDARD®

STANDARDS Australia

Industrial communication networks — Network and system security

Part 3.3: System security requirements and security levels



AVA Documents
Document Sharing Hub

Full document details: AS IEC 62443.3.3-2024

AS IEC 62443.3.3:2024

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 22 May 2024.

This Standard was published on 14 June 2024.

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 and Automation Australia
Workplace Health and Safety Queensland

This Standard was issued in draft form for comment as DR AS IEC 62443.3.3:2024.

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 76139 658 8

Documents
Document Sharing Hub

Full document details: AS IEC 62443.3.3-2024

AS IEC 62443.3.3:2024
IEC 62443-3-3:2013
IEC 62443-3-3:2013/COR1:2014

Industrial communication networks — Network and system security

Part 3.3: System security requirements and security levels

First published as AS IEC 62443.3.3:2024.

Standards Australia Ltd 2024

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 the publisher, unless otherwise permitted under the Copyright Act 1968 (Cth).

Documents
Document Sharing Hub

Full document details: AS IEC 62443.3.3-2024

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 requirements (SRs) associated with the seven foundational requirements (FRs) described in SA TS IEC 62443.1.1 including defining the requirements for control system capability security levels, SL-C (control system). This document is intended to be used by members of the industrial automation and control system (IACS) community while developing the appropriate control system target SL, SL-T (control system), for a specific asset within the parameters of the defined zones and conduits for the system under consideration (SuC).

As defined in SA TS 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 document as opposed to target SLs, SL-T, or achieved SLs, SL-A, which are out of scope.

Refer to AS IEC 62443.2.1 for an equivalent set of non-technical, program-related, capability SRs necessary for fully achieving a control system target SL.

This document is identical with, and has been reproduced from, IEC 62443-3-3:2013, *Industrial communication networks — Network and system security — Part 3-3: System security requirements and security levels*, and incorporates its Corrigendum 1 (April 2014).

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.

Documents
Document Sharing Hub

© Standards Australia Limited 2024

Full document details: AS IEC 62443.3.3-2024

Contents

Preface ..... **ii**

FOREWORD ..... **ix**

Introduction ..... **xi**

0.1 Overview xi
0.2 Purpose and intended audience xii
0.3 Usage within other parts of the IEC 62443 series xii

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 7
3.3 Conventions 9

4 Common control system security constraints **9**

4.1 Overview 9
4.2 Support of essential functions 10
4.3 Compensating countermeasures 10
4.4 Least privilege 11

5 FR 1 – Identification and authentication control **11**

5.1 Purpose and SL-C(IAC) descriptions 11
5.2 Rationale 11
5.3 SR 1.1 – Human user identification and authentication 11
5.3.1 Requirement 11
5.3.2 Rationale and supplemental guidance 12
5.3.3 Requirement enhancements 12
5.3.4 Security levels 12
5.4 SR 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 14
5.5 SR 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 SR 1.4 – Identifier management 15
5.6.1 Requirement 15
5.6.2 Rationale and supplemental guidance 15
5.6.3 Requirement enhancements 15
5.6.4 Security levels 15
5.7 SR 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 SR 1.6 – Wireless access management 17
5.8.1 Requirement 17
5.8.2 Rationale and supplemental guidance 17
5.8.3 Requirement enhancements 17
5.8.4 Security levels 17
5.9 SR 1.7 – Strength of password-based authentication 17
5.9.1 Requirement 17

AVA Documents
Document Sharing Hub

Full document details: AS IEC 62443.3.3-2024

5.9.2 Rationale and supplemental guidance 17
5.9.3 Requirement enhancements 18
5.9.4 Security levels 18
5.10 SR 1.8 – Public key infrastructure (PKI) certificates 18
5.10.1 Requirement 18
5.10.2 Rationale and supplemental guidance 19
5.10.3 Requirement enhancements 19
5.10.4 Security levels 19
5.11 SR 1.9 – Strength of public key authentication 19
5.11.1 Requirement 19
5.11.2 Rationale and supplemental guidance 19
5.11.3 Requirement enhancements 20
5.11.4 Security levels 20
5.12 SR 1.10 – Authenticator feedback 20
5.12.1 Requirement 20
5.12.2 Rationale and supplemental guidance 20
5.12.3 Requirement enhancements 20
5.12.4 Security levels 21
5.13 SR 1.11 – Unsuccessful login attempts 21
5.13.1 Requirement 21
5.13.2 Rationale and supplemental guidance 21
5.13.3 Requirement enhancements 21
5.13.4 Security levels 21
5.14 SR 1.12 – System use notification 21
5.14.1 Requirement 21
5.14.2 Rationale and supplemental guidance 22
5.14.3 Requirement enhancements 22
5.14.4 Security levels 22
5.15 SR 1.13 – Access via untrusted networks 22
5.15.1 Requirement 22
5.15.2 Rationale and supplemental guidance 22
5.15.3 Requirement enhancements 23
5.15.4 Security levels 23

6 FR 2 – Use control 23
6.1 Purpose and SL-C(UC) descriptions 23
6.2 Rationale 23
6.3 SR 2.1 – Authorization enforcement 24
6.3.1 Requirement 24
6.3.2 Rationale and supplemental guidance 24
6.3.3 Requirement enhancements 24
6.3.4 Security levels 25
6.4 SR 2.2 – Wireless use control 25
6.4.1 Requirement 25
6.4.2 Rationale and supplemental guidance 25
6.4.3 Requirement enhancements 25
6.4.4 Security levels 25
6.5 SR 2.3 – Use control for portable and mobile devices 26
6.5.1 Requirement 26
6.5.2 Rationale and supplemental guidance 26
6.5.3 Requirement enhancements 26
6.5.4 Security levels 26
6.6 SR 2.4 – Mobile code 27
6.6.1 Requirement 27
6.6.2 Rationale and supplemental guidance 27
6.6.3 Requirement enhancements 27
6.6.4 Security levels 27
6.7 SR 2.5 – Session lock 27
6.7.1 Requirement 27

Documents
Document Sharing Hub
Full document details: AS IEC 62443.3.3-2024

6.7.2 Rationale and supplemental guidance 28
6.7.3 Requirement enhancements 28
6.7.4 Security levels 28
6.8 SR 2.6 – Remote session termination 28
6.8.1 Requirement 28
6.8.2 Rationale and supplemental guidance 28
6.8.3 Requirement enhancements 28
6.8.4 Security levels 28
6.9 SR 2.7 – Concurrent session control 29
6.9.1 Requirement 29
6.9.2 Rationale and supplemental guidance 29
6.9.3 Requirement enhancements 29
6.9.4 Security levels 29
6.10 SR 2.8 – Auditable events 29
6.10.1 Requirement 29
6.10.2 Rationale and supplemental guidance 29
6.10.3 Requirement enhancements 30
6.10.4 Security levels 30
6.11 SR 2.9 – Audit storage capacity 30
6.11.1 Requirement 30
6.11.2 Rationale and supplemental guidance 30
6.11.3 Requirement enhancements 30
6.11.4 Security levels 30
6.12 SR 2.10 – Response to audit processing failures 31
6.12.1 Requirement 31
6.12.2 Rationale and supplemental guidance 31
6.12.3 Requirement enhancements 31
6.12.4 Security levels 31
6.13 SR 2.11 – Timestamps 31
6.13.1 Requirement 31
6.13.2 Rationale and supplemental guidance 31
6.13.3 Requirement enhancements 32
6.13.4 Security levels 32
6.14 SR 2.12 – Non-repudiation 32
6.14.1 Requirement 32
6.14.2 Rationale and supplemental guidance 32
6.14.3 Requirement enhancements 32
6.14.4 Security levels 32

7 FR 3 – System integrity 33
7.1 Purpose and SL-C(SI) descriptions 33
7.2 Rationale 33
7.3 SR 3.1 – Communication integrity 33
7.3.1 Requirement 33
7.3.2 Rationale and supplemental guidance 33
7.3.3 Requirement enhancements 34
7.3.4 Security levels 34
7.4 SR 3.2 – Malicious code protection 34
7.4.1 Requirement 34
7.4.2 Rationale and supplemental guidance 34
7.4.3 Requirement enhancements 35
7.4.4 Security levels 35
7.5 SR 3.3 – Security functionality verification 35
7.5.1 Requirement 35
7.5.2 Rationale and supplemental guidance 36
7.5.3 Requirement enhancements 36
7.5.4 Security levels 36
7.6 SR 3.4 – Software and information integrity 36
7.6.1 Requirement 36

Documents
Document Sharing Hub
Full document details: AS IEC 62443.3.3-2024

7.6.2 Rationale and supplemental guidance 37
7.6.3 Requirement enhancements 37
7.6.4 Security levels 37
7.7 SR 3.5 – Input validation 37
7.7.1 Requirement 37
7.7.2 Rationale and supplemental guidance 37
7.7.3 Requirement enhancements 37
7.7.4 Security levels 38
7.8 SR 3.6 – Deterministic output 38
7.8.1 Requirement 38
7.8.2 Rationale and supplemental guidance 38
7.8.3 Requirement enhancements 38
7.8.4 Security levels 38
7.9 SR 3.7 – Error handling 38
7.9.1 Requirement 38
7.9.2 Rationale and supplemental guidance 39
7.9.3 Requirement enhancements 39
7.9.4 Security levels 39
7.10 SR 3.8 – Session integrity 39
7.10.1 Requirement 39
7.10.2 Rationale and supplemental guidance 39
7.10.3 Requirement enhancements 39
7.10.4 Security levels 40
7.11 SR 3.9 – Protection of audit information 40
7.11.1 Requirement 40
7.11.2 Rationale and supplemental guidance 40
7.11.3 Requirement enhancements 40
7.11.4 Security levels 40

8 FR 4 – Data confidentiality 41
8.1 Purpose and SL-C(DC) descriptions 41
8.2 Rationale 41
8.3 SR 4.1 – Information confidentiality 41
8.3.1 Requirement 41
8.3.2 Rationale and supplemental guidance 41
8.3.3 Requirement enhancements 42
8.3.4 Security levels 42
8.4 SR 4.2 – Information persistence 42
8.4.1 Requirement 42
8.4.2 Rationale and supplemental guidance 42
8.4.3 Requirement enhancements 43
8.4.4 Security levels 43
8.5 SR 4.3 – Use of cryptography 43
8.5.1 Requirement 43
8.5.2 Rationale and supplemental guidance 43
8.5.3 Requirement enhancements 43
8.5.4 Security levels 44

9 FR 5 – Restricted data flow 44
9.1 Purpose and SL-C(RDF) descriptions 44
9.2 Rationale 44
9.3 SR 5.1 – Network segmentation 44
9.3.1 Requirement 44
9.3.2 Rationale and supplemental guidance 44
9.3.3 Requirement enhancements 45
9.3.4 Security levels 45
9.4 SR 5.2 – Zone boundary protection 45
9.4.1 Requirement 45
9.4.2 Rationale and supplemental guidance 45

AVA Documents
Document Sharing Hub

Full document details: AS IEC 62443.3.3-2024

9.4.3 Requirement enhancements 46
9.4.4 Security levels 46
9.5 SR 5.3 – General purpose person-to-person communication restrictions 46
9.5.1 Requirement 46
9.5.2 Rationale and supplemental guidance 46
9.5.3 Requirement enhancements 47
9.5.4 Security levels 47
9.6 SR 5.4 – Application partitioning 47
9.6.1 Requirement 47
9.6.2 Rationale and supplemental guidance 47
9.6.3 Requirement enhancements 48
9.6.4 Security levels 48

10 FR 6 – Timely response to events 48
10.1 Purpose and SL-C(TRE) descriptions 48
10.2 Rationale 48
10.3 SR 6.1 – Audit log accessibility 48
10.3.1 Requirement 48
10.3.2 Rationale and supplemental guidance 49
10.3.3 Requirement enhancements 49
10.3.4 Security levels 49
10.4 SR 6.2 – Continuous monitoring 49
10.4.1 Requirement 49
10.4.2 Rationale and supplemental guidance 49
10.4.3 Requirement enhancements 50
10.4.4 Security levels 50

11 FR 7 – Resource availability 50
11.1 Purpose and SL-C(RA) descriptions 50
11.2 Rationale 50
11.3 SR 7.1 – Denial of service protection 50
11.3.1 Requirement 50
11.3.2 Rationale and supplemental guidance 51
11.3.3 Requirement enhancements 51
11.3.4 Security levels 51
11.4 SR 7.2 – Resource management 51
11.4.1 Requirement 51
11.4.2 Rationale and supplemental guidance 51
11.4.3 Requirement enhancements 51
11.4.4 Security levels 51
11.5 SR 7.3 – Control system backup 52
11.5.1 Requirement 52
11.5.2 Rationale and supplemental guidance 52
11.5.3 Requirement enhancements 52
11.5.4 Security levels 52
11.6 SR 7.4 – Control system recovery and reconstitution 52
11.6.1 Requirement 52
11.6.2 Rationale and supplemental guidance 52
11.6.3 Requirement enhancements 53
11.6.4 Security levels 53
11.7 SR 7.5 – Emergency power 53
11.7.1 Requirement 53
11.7.2 Rationale and supplemental guidance 53
11.7.3 Requirement enhancements 53
11.7.4 Security levels 53
11.8 SR 7.6 – Network and security configuration settings 53
11.8.1 Requirement 53
11.8.2 Rationale and supplemental guidance 54
11.8.3 Requirement enhancements 54

Documents
Document Sharing Hub
Full document details: AS IEC 62443.3.3-2024

11.8.4 Security levels 54
11.9 SR 7.7 – Least functionality 54
11.9.1 Requirement 54
11.9.2 Rationale and supplemental guidance 54
11.9.3 Requirement enhancements 54
11.9.4 Security levels 54
11.10 SR 7.8 – Control system component inventory 55
11.10.1 Requirement 55
11.10.2 Rationale and supplemental guidance 55
11.10.3 Requirement enhancements 55
11.10.4 Security levels 55
Annex A (informative) **Discussion of the SL vector** **56**
Annex B (informative) **Mapping of SRs and REs to FRSL levels 1-4** **65**
Bibliography **69**

List of Figures

Figure 1 — Structure of the IEC 62443 series xiii
Figure A.1 — High-level process-industry example showing zones and conduits 59
Figure A.2 — High-level manufacturing example showing zones and conduits 60
Figure A.3 — Schematic of correlation of the use of different SL types 61

List of Tables

Table B.1 — Mapping of SRs and REs to FRSL levels 1-4 65

Documents
Document Sharing Hub
Full document details: AS IEC 62443.3.3-2024

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.

Documents
Document Sharing Hub
© Standards Australia Limited 2024
Full document details: AS IEC 62443.3.3-2024

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.

© Standards Australia Limited 2024

Documents
Document Sharing Hub

Full document details: AS IEC 62443.3.3-2024

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).

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.

---

1) Numbers in square brackets refer to the Bibliography.

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

Documents Document Sharing Hub
© Standards Australia Limited 2024
Full document details: AS IEC 62443.3.3-2024

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.

© Standards Australia Limited 2024

Documents
Document Sharing Hub
Full document details: AS IEC 62443.3.3-2024

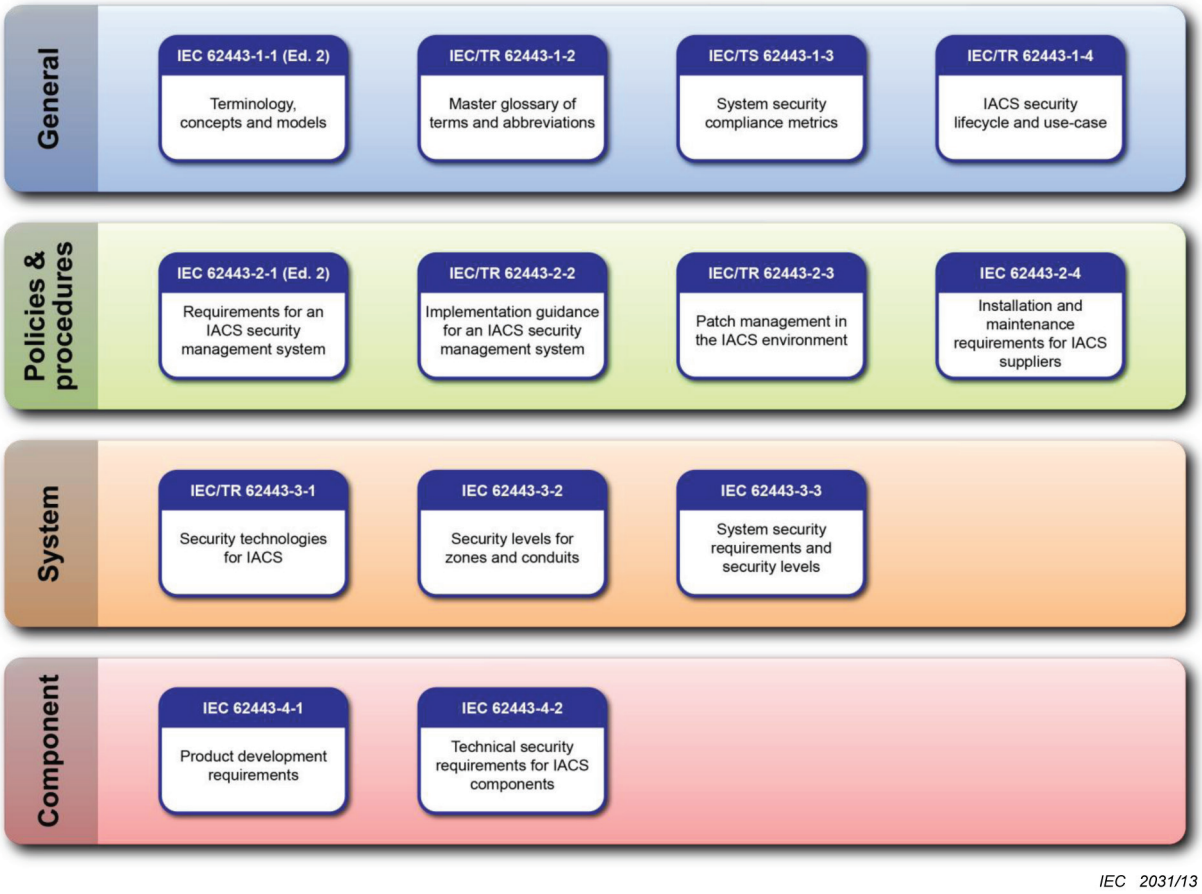


Figure 1 — Structure of the IEC 62443 series

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.

Documents
Document Sharing Hub
© Standards Australia Limited 2024
Full document details: AS IEC 62443.3.3-2024

NOTES

Documents
Document Sharing Hub

Full document details: AS IEC 62443.3.3-2024

Australian Standard®

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*

Documents
Document Sharing Hub
© Standards Australia Limited 2024

Full document details: AS IEC 62443.3.3-2024

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.

© Standards Australia Limited 2024

Documents
Document Sharing Hub

Full document details: AS IEC 62443.3.3-2024

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

Documents
Document Sharing Hub
© Standards Australia Limited 2024

Full document details: AS IEC 62443.3.3-2024

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.

© Standards Australia Limited 2024

Documents
Document Sharing Hub

Full document details: AS IEC 62443.3.3-2024

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.

Documents
Document Sharing Hub
© Standards Australia Limited 2024
Full document details: AS IEC 62443.3.3-2024

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

© Standards Australia Limited 2024

AVA Documents Document Sharing Hub

Full document details: AS IEC 62443.3.3-2024

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	[US NIST] Federal Information Processing Standard
FR	Foundational requirement
FS-PLC	Functional safety PLC

Documents
Document Sharing Hub
© Standards Australia Limited 2024
Full document details: AS IEC 62443.3.3-2024

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

© Standards Australia Limited 2024

Documents
Document Sharing Hub

Full document details: AS IEC 62443.3.3-2024

SP	[US NIST] Special Publication
SR	System requirement
SSH	Secure socket shell
SuC	System under consideration
TCP	Transmission Control Protocol
TPM	Trusted platform module
TRE	Timely response to events
UC	Use control
USB	Universal serial bus
VoIP	Voice over internet protocol
WEP	Wired equivalent privacy
WLAN	Wireless local area network

3.3 Conventions

This standard expands the seven FRs defined in IEC 62443-1–1 into a series of SRs. Each SR has a baseline requirement and zero or more requirement enhancements (REs) to strengthen security. To provide clarity to the reader, rationale and supplemental guidance is provided for each baseline requirement and notes for any associated REs as is deemed necessary. The baseline requirement and REs, if present, are then mapped to the control system capability security level, SL-C(FR, control system) 1 to 4.

All seven FRs have a defined set of four SLs. The control system capability level 0 for a particular FR is implicitly defined as no requirements. For example, the purpose statement for Clause 8, FR 4 – Data confidentiality, is:

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

The associated four SLs are defined as:

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

The individual SR and RE assignments are thus based on an incremental increase in overall control system security for that particular FR.

The SL-C(control system), used throughout this standard, signifies a capability required to meet a given SL rating for a given FR. A complete description of the SL vector concept can be found in Annex A.

4 Common control system security constraints

4.1 Overview

When reading, specifying and implementing the control system SRs detailed in Clauses 5 through 11 of this standard, there are a number of common constraints that shall be adhered to. The introduction of this standard provided some contextual, informative discussion of what this standard is designed to accomplish. This clause and the subsequent FR-specific clauses furnish the normative material

Documents Document Sharing Hub
© Standards Australia Limited 2024

Full document details: AS IEC 62443.3.3-2024

necessary to build extensions to existing enterprise security to support the rigorous integrity and availability requirements needed by IACS.

NOTE The contents of this clause will eventually be incorporated into IEC 62443-1–1.

4.2 Support of essential functions

As documented in 3.1.22, an essential function is a "function or capability that is required to maintain health, safety, the environment and availability for the equipment under control."

- Security measures shall not adversely affect essential functions of a high availability IACS unless supported by a risk assessment.

  NOTE See IEC 62443-2-1 regarding the documentation requirements associated with the risk assessment required to support instances where security measures may affect essential functions.

  When reading, specifying and implementing the SRs described in this standard, implementation of security measures should not cause loss of protection, loss of control, loss of view or loss of other essential functions. After a risk analysis, some facilities may determine certain types of security measures may halt continuous operations, but security measures shall not result in loss of protection that could result in health, safety and environmental (HSE) consequences. Some specific constraints include:

- Access Controls (IAC and UC) shall not prevent the operation of essential functions, specifically:
  - Accounts used for essential functions shall not be locked out, even temporarily (see 5.5, SR 1.3 – Account management, 5.6, SR 1.4 – Identifier management, 5.13, SR 1.11 – Unsuccessful login attempts and 6.7, SR 2.5 – Session lock).
  - Verifying and recording operator actions to enforce non-repudiation shall not add significant delay to system response time (see 6.14, SR 2.12 – Non-repudiation).
  - For high availability control systems, the failure of the certificate authority shall not interrupt essential functions (see 5.10, SR 1.8 – Public key infrastructure (PKI) certificates).
  - Identification and authentication shall not prevent the initiation of the SIF (see 5.3, SR 1.1 – Human user identification and authentication and 5.4, SR 1.2 – Software process and device identification and authentication). Similarly for authorization enforcement (see 6.3, SR 2.1 – Authorization enforcement).
  - Incorrectly timestamped audit records (see 6.10, SR 2.8 – Auditable events and 6.13 SR 2.11 – Timestamps) shall not adversely affect essential functions.
- Essential functions of an IACS shall be maintained if zone boundary protection goes into fail-close and/or island mode (see 9.4, SR 5.2 – Zone boundary protection).
- A denial of service (DoS) event on the control system or safety instrumented system (SIS) network shall not prevent the SIF from acting (see 11.3, SR 7.1 – Denial of service protection).

4.3 Compensating countermeasures

Compensating countermeasures, as used in this standard, shall adhere to the guidelines described in IEC 62443-3-2.

Throughout this standard, the SR normative language states that "the control system shall provide the capability to..." support some specific security requirement. The control system shall provide the capability, but it might be performed by an external component. In such a case, the control system shall provide an 'interface' to that external component. Some examples of compensating countermeasures include user identification (including centralized versus distributed), password strength enforcement,

© Standards Australia Limited 2024

AVA Documents Document Sharing Hub

Full document details: AS IEC 62443.3.3-2024

signature validity checking, security event correlation and device decommissioning (information persistence).

NOTE 1 The control system security requirements detailed in this standard pertain to all technical functions relevant to a control system including tools and applications. However, as noted here, some of these functions can be handled by an external resource.

NOTE 2 In some high resource availability applications (high SL-T(RA, control system)), compensating countermeasures external to the control system (such as additional physical security measures and/or enhanced personnel background checks) will be needed. In these cases, it is possible to see a normally high resource availability SL control system at a lower IAC SL 1 or 2 rating, depending upon the compensating countermeasures. Lockout or loss of control due to security measures is increased, not decreased for very high availability SL control system. Thus higher SLs are not always "better", even where cost is not a significant factor.

4.4 Least privilege

The capability to enforce the concept of least privilege shall be provided, with granularity of permissions and flexibility of mapping those permissions to roles sufficient to support it. Individual accountability should be available when required.

5 FR 1 – Identification and authentication control

5.1 Purpose and SL-C(IAC) descriptions

Identify and authenticate all users (humans, software processes and devices) before allowing them to access to the control system.

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

5.2 Rationale

Asset owners will have to develop a list of all users (humans, software processes and devices) and to determine for each control system component the required level of IAC protection. The goal of IAC is to protect the control system by verifying the identity of any user requesting access to the control system before activating the communication. Recommendations and guidelines should include mechanisms that will operate in mixed modes. For example, some control system components require strong IAC, such as strong authentication mechanisms, and others do not.

5.3 SR 1.1 – Human user identification and authentication

5.3.1 Requirement

The control system shall provide the capability to identify and authenticate all human users. This capability shall enforce such identification and authentication on all interfaces which provide human

Documents Document Sharing Hub
© Standards Australia Limited 2024
Full document details: AS IEC 62443.3.3-2024