

AS IEC 62443.2.1:2025
IEC 62443-2-1:2024



STANDARDS
Australia



Security for industrial automation and control systems

Part 2.1: Security program requirements for IACS asset owners



currently in preview, click buy full version

AS IEC 62443.2.1:2025

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 08 January 2025.

This Standard was published on 17 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 62443.2.1:2024.

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 998 5

Security for industrial automation and control systems

Part 2.1: Security program requirements for IACS asset owners

First published as AS IEC 62443 2.1: 024
Second edition 2025.



© 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, to supersede AS IEC 62443.2.1:2024, *Industrial communication networks — Network and system security, Part 2.1: Establishing an industrial automation and control system security program*.

The objective of this document is to specify asset owner security program (SP) policy and procedure requirements for an industrial automation and control system (IACS) in operation. This document uses the broad definition and scope of what constitutes an IACS as described in IEC TS 62443-1-1. In the context of this document, asset owner also includes the operator of the IACS.

This document is identical with, and has been reproduced from, IEC 62443-2-1:2024, *Security for industrial automation and control systems — Part 2-1: Security program requirements for IACS asset owners*.

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	vii
INTRODUCTION	ix
1 Scope	1
2 Normative references	2
3 Terms, definitions, abbreviated terms and conventions	2
3.1 Terms and definitions	2
3.2 Abbreviated terms and acronyms	6
3.3 Conventions	7
4 Concepts	8
4.1 Use of this document	8
4.1.1 Applicable roles	8
4.1.2 Use of this document by asset owners	8
4.1.3 Use of this document by service providers and product suppliers	10
4.2 Maturity level (ML) definitions	10
4.3 Security levels (SLs)	12
4.4 Requirements definitions	12
4.4.1 Requirements organization	12
4.4.2 Requirements cross-references	13
4.4.3 Requirement conventions	13
5 Conformance and assessment	13
5.1 Overview	13
5.2 Conformity evidence	14
5.3 Requirements evaluation and profiles	15
5.3.1 Overview	15
5.3.2 Evaluation of risk to requirements	15
5.3.3 Profiles	15
5.3.4 Conformity assessment for the asset owner role	16
6 SPE 1 - Organizational security measures	16
6.1 Purpose	16
6.2 ORG 1 - Security related organization and policies	16
6.2.1 ORG 1.1: Information security management system (ISMS)	16
6.2.2 ORG 1.2: Background checks	17
6.2.3 ORG 1.3: Security roles and responsibilities	17
6.2.4 ORG 1.4: Security awareness training	18
6.2.5 ORG 1.5: Security responsibilities training	18
6.2.6 ORG 1.6: Supply chain security	19
6.3 ORG 2 - Security assessments and reviews	19
6.3.1 ORG 2.1: Security risk mitigation	19
6.3.2 ORG 2.2: Processes for discovery of security anomalies	20
6.3.3 ORG 2.3: Secure development and support	21
6.3.4 ORG 2.4: SP reviews	21
6.4 ORG 3 - Security of physical access	21
6.4.1 ORG 3.1: Physical access control	21
7 SPE 2 - Configuration management	22
7.1 Purpose	22
7.2 CM 1 - Inventory management of IACS hardware/software components and network communications	22
7.2.1 CM 1.1: Asset inventory baseline	22
7.2.2 CM 1.2: Infrastructure drawings/documentation	23
7.2.3 CM 1.3: Configuration settings	23
7.2.4 CM 1.4: Change control	24

8	SPE 3 - Network and communications security	24
8.1	Purpose	24
8.2	NET 1 - System segmentation	24
8.2.1	NET 1.1: Segmentation from non-IACS zones	24
8.2.2	NET 1.2: Documentation of zones and network zone interconnections	25
8.2.3	NET 1.3: Network segmentation from safety systems	25
8.2.4	NET 1.4: Network autonomy	26
8.2.5	NET 1.5: Network disconnection from external networks	26
8.2.6	NET 1.6: Internal network access control	26
8.2.7	NET 1.7: Network accessible services	27
8.2.8	NET 1.8: User messaging	27
8.2.9	NET 1.9: Network time distribution	27
8.3	NET 2 - Secure wireless access	28
8.3.1	NET 2.1: Wireless protocols	28
8.3.2	NET 2.2: Wireless network segmentation	28
8.3.3	NET 2.3: Wireless properties and addresses	29
8.4	NET 3 - Secure remote access	29
8.4.1	NET 3.1: Remote access applications	29
8.4.2	NET 3.2: Remote access connections	29
8.4.3	NET 3.3: Remote access termination	30
9	SPE 4 - Component security	30
9.1	Purpose	30
9.2	COMP 1 - Components and portable media	31
9.2.1	COMP 1.1: Component hardening	31
9.2.2	COMP 1.2: Dedicated portable media	32
9.3	COMP 2 - Malware protection	32
9.3.1	COMP 2.1: Malware free	32
9.3.2	COMP 2.2: Malware protection	33
9.3.3	COMP 2.3: Malware protection software validation and installation	33
9.4	COMP 3 - Patch management	34
9.4.1	COMP 3.1: Security patch authenticity/integrity	34
9.4.2	COMP 3.2: Security patch validation and installation	34
9.4.3	COMP 3.3: Security patch status	34
9.4.4	COMP 3.4: Security patch maintenance/retention of security	35
9.4.5	COMP 3.5: Security patch mitigation	35
10	SPE 5 - Protection of data	35
10.1	Purpose	35
10.2	DATA 1 - Protection of data	36
10.2.1	DATA 1.1: Data classification	36
10.2.2	DATA 1.2: Data confidentiality	36
10.2.3	DATA 1.3: Safety system configuration mode	37
10.2.4	DATA 1.4: Data retention policy	37
10.2.5	DATA 1.5: Cryptographic mechanisms	38
10.2.6	DATA 1.6: Key management	38
10.2.7	DATA 1.7: Data Integrity	38
11	SPE 6 - User access control	39
11.1	Purpose	39
11.2	USER 1 - Identification and authentication	39
11.2.1	USER 1.1: User identity assignment	39
11.2.2	USER 1.2: User identity removal	40
11.2.3	USER 1.3: User identity persistence	40
11.2.4	USER 1.4: Access rights assignment	41
11.2.5	USER 1.5: Least privilege	41
11.2.6	USER 1.6: Software service authentication	41
11.2.7	USER 1.7: Software services interactive login rights	42
11.2.8	USER 1.8: Human user authentication	42
11.2.9	USER 1.9: Multifactor authentication (MFA)	42

11.2.10	USER 1.10: Mutual authentication	43
11.2.11	USER 1.11: Password protection	43
11.2.12	USER 1.12: Shared and disclosed/compromised passwords	44
11.2.13	USER 1.13: User login display information	44
11.2.14	USER 1.14: User login failure displays	44
11.2.15	USER 1.15: Consecutive login failures	45
11.2.16	USER 1.16: Session integrity	45
11.2.17	USER 1.17: Concurrent sessions	45
11.2.18	USER 1.18: Screen lock	46
11.2.19	USER 1.19: Component authentication	46
11.3	USER 2 - Authorization and access control	46
11.3.1	USER 2.1: Authorization	46
11.3.2	USER 2.2: Separation of duties	47
11.3.3	USER 2.3: Multiple approvals	47
11.3.4	USER 2.4: Manual elevation of privileges	48
12	SPE 7 - Event and incident management	48
12.1	Purpose	48
12.2	EVENT 1 - Event and incident management	48
12.2.1	EVENT 1.1: Event detection	48
12.2.2	EVENT 1.2: Event reporting	49
12.2.3	EVENT 1.3: Event reporting interfaces	49
12.2.4	EVENT 1.4: Logging	49
12.2.5	EVENT 1.5: Log entries	50
12.2.6	EVENT 1.6: Log access	50
12.2.7	EVENT 1.7: Event analysis	51
12.2.8	EVENT 1.8: Incident handling and response	51
12.2.9	EVENT 1.9: Vulnerability handling	51
13	SPE 8 - System integrity and availability	52
13.1	Purpose	52
13.2	AVAIL 1 - System availability and intended functionality	52
13.2.1	AVAIL 1.1: Continuity management	52
13.2.2	AVAIL 1.2: Resource availability management	52
13.2.3	AVAIL 1.3: Failure state	53
13.3	AVAIL 2 - Backup/restore/archive	53
13.3.1	AVAIL 2.1: Backup	53
13.3.2	AVAIL 2.2: Backup non-interference	54
13.3.3	AVAIL 2.3: Backup verification	54
13.3.4	AVAIL 2.4: Backup media	54
13.3.5	AVAIL 2.5: Backup restoration	54
Annex A	(informative) Cross-references to other standards	56
Annex B	(informative) Establishing and maintaining an IACS SP	99
Annex C	(informative) Evaluating MLs	105
Bibliography		107

List of Figures

Figure 1	— Roles and responsibilities in the IEC 62443 series	2
Figure B.1	— Example of process flow for cybersecurity risk management	103
Figure B.2	— Levels of protection an asset requires	104

List of Tables

Table 1	— ML levels and descriptions	11
Table 2	— Typical conformity evidence types	14
Table A.1	— IEC 62443-2-4 cross-references	56

Table A.2 — Cross-reference of IEC 62443-2-1 to IEC 62443-2-4	59
Table A.3 — IEC 62443-3-3 cross-references	64
Table A.4 — Cross-reference of IEC 62443-2-1 to IEC 62443-3-3	66
Table A.5 — IEC 62443-4-2 cross-references	70
Table A.6 — Cross-reference of IEC 62443-2-1 to IEC 62443-4-2	74
Table A.7 — ISO/IEC 27001:2013 cross-references	78
Table A.8 — Cross-reference of IEC 62443-2-1 to ISO/IEC 27001:2013	83
Table A.9 — NIST CSF cross-references	88
Table A.10 — Cross-reference of IEC 62443-2-1 to NIST CSF	93
Table B.1 — Example risk levels	101

Currently in preview, click buy full version

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) IEC draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). IEC takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, IEC had not received notice of (a) patent(s), which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at <https://patents.iec.ch>. IEC shall not be held responsible for identifying any or all such patent rights.

IEC 62443-2-1 has been prepared by IEC technical committee 65: Industrial process measurement, control and automation, in collaboration with the liaison ISA99: ISA committee on Security for industrial automation and control systems. It is an International Standard.

This second edition cancels and replaces the first edition published in 2010. This edition constitutes a technical revision.

This edition includes the following significant technical changes with respect to the previous edition:

- a) revised requirement structure into SP elements (SPEs),
- b) revised requirements to eliminate duplication of an information security management system (ISMS), and
- c) defined a maturity model for evaluating requirements.

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

Draft	Report on voting
65/1044/FDIS	65/1053/RVD

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

The language used for the development of this International Standard is English.

This document was drafted in accordance with ISO/IEC Directives, Part 2, and developed in accordance with ISO/IEC Directives, Part 1 and ISO/IEC Directives, IEC Supplement, available at www.iec.ch/members_experts/refdocs. The main document types developed by IEC are described in greater detail at www.iec.ch/publications.

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 webstore.iec.ch in the data related to the specific document. At this date, the document will be

- reconfirmed,
- withdrawn, or
- revised.

IMPORTANT — The "colour inside" logo on the cover page of this document 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.

INTRODUCTION

This document is the part of the IEC 62443 series that contains security requirements for industrial automation and control system (IACS) asset owners. In the context of this document, asset owner also includes the operator of the IACS. Its requirements focus on cybersecurity and allow security capabilities that meet them to be provided as a combination of technical, physical, process and compensating security measures.

Cybersecurity is an increasingly important topic in modern organizations. The term cybersecurity is generally used to describe the set of security measures or practices taken to protect a computer or computer system against unauthorized access or attack. In IACS, the most significant concerns include unwanted access or attacks resulting in the IACS not performing the correct functions in the required timeframe.

A very common engineering approach when faced with a challenging problem is to break the problem into smaller pieces and address each piece in a disciplined manner. This approach is a sound one for addressing cybersecurity risks with IACS. However, a frequent mistake is to deal with cybersecurity one system at a time. Cybersecurity is a much larger challenge that should address all IACS components as well as the policies, procedures, practices and personnel that surround and utilize those IACS. Implementing such a wide-ranging management system can require a cultural change within the organization.

Addressing cybersecurity on an organization-wide basis can seem like a daunting task. There is no simple cookbook for security, nor is there a one-size-fits-all set of security practices. Absolute security can be achievable but is probably undesirable because of the loss of functionality that would be necessary to achieve this near perfect state. Security is a balance of risk versus cost.

Each situation will be different. In some situations, the risk can be related to health, safety and environmental (HSE) factors rather than purely economic impact. The risk can have an unrecoverable consequence rather than a temporary financial setback. Therefore, a predetermined set of mandatory security practices can either be overly restrictive and likely quite costly to implement or be insufficient to address the risk.

This document supports the need to address cybersecurity for an IACS in operation by providing requirements for establishing, implementing, maintaining and continually improving an IACS security program (SP). These requirements, when implemented conscientiously, provide security capabilities whose purpose is to reduce IACS security risks to a tolerable level. These requirements are written to be implementation independent, allowing asset owners to select approaches most suitable to their needs. IEC 62443-3-2 [1]¹ describes the methodology for addressing cybersecurity risks in an IACS system design and that assists in the identification of risks and the selection of appropriate security requirements and associated capabilities for an IACS SP.

Commercial-off-the-shelf (COTS) products are often not ruggedized or rigorously engineered enough for IACS environments, where they can introduce additional vulnerabilities and threats to the IACS.

When COTS technologies are used in an IACS, they are often configured to meet IACS specific functional needs and operational constraints. For example, security event handling in COTS products may be configured differently for IACS applications than they are for traditional information technology (IT) applications. Typical COTS equipment is designed for environments where the primary objective is the protection of information. In an IACS environment, the primary objectives are the protection of the HSE of the facility and the minimization of the operational and business impact on facility operation. COTS technologies can be applied to IACS applications, but the risks associated with using these technologies need to be understood by the asset owner.

Some organizations can attempt to use pre-existing IT and business cybersecurity solutions to address security for IACS without understanding the consequences. While many of these solutions can be applied to IACS, it is important to apply them correctly to eliminate inadvertent and undesired

1 Numbers in square brackets refer to the [Bibliography](#).

consequences. For example, in an IACS, availability may have a higher priority than confidentiality, as opposed to typical IT applications.

Asset owners may wish to apply their IACS SP across the organization to address the organization needs and objectives, security requirements, business and work processes, as well as the organization size and structure. All of these influencing factors are dynamic and will likely change over time. Thus, the adoption of an IACS SP is a strategic decision for the organization.

The effectiveness of an IACS SP is often enhanced through coordination or integration with the organization's processes and overall information security management system (ISMS). For example, security can be added to the organization supply chain processes to require security in the design of processes, systems and controls. It is also expected that IACS SP will be scaled in accordance with the needs of the IACS and the organization.

Australian Standard®

Security for industrial automation and control systems

Part 2.1: Security program requirements for IACS asset owners

1 Scope

This part of IEC 62443 specifies asset owner security program (SP) policy and procedure requirements for an industrial automation and control system (IACS) in operation. This document uses the broad definition and scope of what constitutes an IACS as described in IEC TS 62443-1-1. In the context of this document, asset owner also includes the operator of the IACS.

This document recognizes that the lifespan of an IACS can exceed twenty years, and that many legacy systems contain hardware and software that are no longer supported. Therefore, the SP for most legacy systems addresses only a subset of the requirements defined in this document. For example, if IACS or component software is no longer supported, security patching requirements cannot be met. Similarly, backup software for many older systems is not available for all components of the IACS. This document does not specify that an IACS has these technical requirements. This document states that the asset owner needs to have policies and procedures around these types of requirements. In the case where an asset owner has legacy systems that do not have the native technical capabilities, compensating security measures can be part of the policies and procedures specified in this document.

This document also recognizes that not all requirements specified in this document apply to all IACSs. For example, requirements associated with certain technology (such as wireless) or functions (such as remote access) will not apply to IACSs that do not include these technologies or functions. Similarly, not all malware protection requirements apply to systems for which malware protection software is not available for any of their devices. Therefore, this document states that the asset owner needs to identify the IACS security requirements that are applicable to its IACSs in their specific operating environments.

The elements of an IACS SP described in this document define required security capabilities that apply to the secure operation of an IACS. Although the asset owner is ultimately accountable for the secure operation of an IACS, implementation of these security capabilities often includes support from its service providers and product suppliers. For this reason, this document provides guidance for an asset owner when stating security requirements for their service providers and product suppliers, referencing other parts of the IEC 62443 series.

[Figure 1](#) illustrates the roles and responsibilities of the asset owner, service provider(s) and product supplier(s) of an IACS and their relationships to each other and to the Automation Solution. The Automation Solution is a technical solution implementing the control/safety and complementary functions necessary for the IACS. It is composed of hardware and software components that have been installed and configured to operate in the IACS. The IACS is a combination of the Automation Solution and the organizational measures necessary for its design, deployment, operation and maintenance.

Some of these capabilities rely on the appropriate application of integration maintenance capabilities defined in IEC 62443-2-4 [\[2\]](#) and technical security capabilities defined in IEC 62443-3-3 [\[3\]](#) and IEC 62443-4-2 [\[4\]](#).