IEC TS 62443-1-5

Edition 1.0 2023-09

TECHNICAL SPECIFICATION

Security for industrial automation and control systems – Part 1-5: Scheme for IEC 62443 security profiles

IEC TS 62443-1-5:2023-09(en)

IEC Secretariat
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
info@iec.ch
www.iec.ch

About the IEC
The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications
The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigendum or an amendment might have been published.

IEC publications search - webstore.iec.ch/advsearchform
The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee, …). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished
Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and once a month by email.

IEC Customer Service Centre - webstore.iec.ch/csc
If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: sales@iec.ch.

IEC Products & Services Portal - products.iec.ch
Discover our powerful search engine and read freely all the publications previews. With a subscription you will always have access to up to date content tailored to your needs.

Electropedia - www.electropedia.org
The world's leading online dictionary on electrotechnology, containing more than 22 300 terminological entries in English and French, with equivalent terms in 19 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC TS 62443-1-5

Edition 1.0 2023-09

TECHNICAL SPECIFICATION

Security for industrial automation and control systems – Part 1-5: Scheme for IEC 62443 security profiles

INTERNATIONAL ELECTROTECHNICAL COMMISSION

ICS 25.040.40

ISBN 978-2-8322-7499-6

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

SECURITY FOR INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS –

Part 1-5: Scheme for IEC 62443 security profiles

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.

IEC TS 62443-1-5 has been prepared by IEC technical committee 65: Industrial-process measurement, control and automation. It is a Technical Specification.

The text of this Technical Specification is based on the following documents:

Draft	Report on voting
65/947/DTS	65/1009/RVDTS

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 Technical Specification 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.

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

INTRODUCTION

This document specifies a scheme for defining security profiles for the IEC 62443 series.

The scheme is applicable to IEC 62443 security profiles intended to be published as part of the upcoming IEC 62443 dedicated security profiles sub-series). The document can also be used for the definition of security profiles outside of the IEC 62443 series.

IEC 62443 security profiles can be used by interested parties (e.g., organizations, interested groups/ sectors) to contextually map a defined set of requirements specified in the IEC 62443 series. Examples for the necessity of security profiles include the industry sector specific (area of application) contextual mapping of IEC 62443 terminology and requirements.

NOTE The ISO/IEC 15408 series also uses a concept of profiles (called "Protection Profiles"), but those profiles are based on a different scheme, specific to ISO/IEC 15408.

SECURITY FOR INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS –

Part 1-5: Scheme for IEC 62443 security profiles

1 Scope

This part of IEC 62443 specifies a scheme for defining (selecting, writing, drafting, creating) IEC 62443 security profiles.

This scheme and its specified requirements apply to IEC 62443 security profiles which are planned to be published as part of the upcoming IEC 62443 dedicated security profiles sub-series.

IEC 62443 security profiles can support interested parties (e.g. during conformity assessment activities) to achieve comparability of assessed IEC 62443 requirements.

2 Normative references

There are no normative references in this document.

3 Terms, definitions, abbreviated terms, and acronyms

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in IEC TS 62443-1-1:2009 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at https://www.electropedia.org/
- ISO Online browsing platform: available at https://www.iso.org/obp

3.1.1
contextual mapping
declaration and rationale of how a selected requirement is applied within a specific environment

Note 1 to entry: A contextual mapping is neither intended to undermine principles and concepts of the underlaying IEC 62443 document(s) nor to alter / modify the definition / rationale of a selected requirement.

EXAMPLE 1:

Detailing requirements, e.g.

- the applicable framework for a security risk assessment methodology (e.g. IEC 62443-2-4, SP.03.01 BR)
- required security training courses for service provider staff, subcontractors, or consultants in a particular industry sector (e.g. IEC 62443-2-4, SP.01.01, SP.01.02)
- the central identification and authentication system that should be supported by a component (see IEC 62443-4-2, CR 1.1)

EXAMPLE 2: Detailing roles and responsibilities (e.g. within the oil & gas industry the asset owner could be the owner of an oil drilling platform)

3.1.2
interested party
organization, group / sector, association, conformity assessment body, etc. which has an interest in the definition or use of a profile

[SOURCE: ISO/IEC GUIDE 59:2019, 3.5, modified – wording adapted to focus on profiles]

3.1.3
profile
subset of characteristics from a common defined framework for specific applications

Note 1 to entry: The number of profiles shall be limited, and profiles defined only when essential to meet technical, regional or application needs.

EXAMPLE 1 Application specific variants for contextual mapping of a standard or a set of standards to a specific industry or application.

EXAMPLE 2 User profiles, which are a defined subset that is valid for a specific type of user.

EXAMPLE 3 A subset of characteristics designed for one specific function.

EXAMPLE 4 An IEC 62443 security profile specifying that all requirements of IEC 62443-4-1 are fulfilled at minimum to a maturity level of 2 (ML 2).

EXAMPLE 5 An IEC 62443 security profile specifying a subset of relevant IEC 62443-4-2 requirements for a specific product type.

[SOURCE: ISO/IEC Directives, Part 2, 2021, Clause 6.6, modified – wording adapted to be useable for a definition]

3.1.4
risk
expectation of loss expressed as the likelihood that a particular threat will exploit a particular vulnerability with a particular consequence

[SOURCE: IEC 62443-3-2:2020, 3.1.14]

3.1.5
security
condition of system resources being free from unauthorized access and from unauthorized or accidental change, destruction, or loss

3.1.6
security context
security provided to the product, control system or automation solution by the environment (e.g. asset owner deployment) in which the product, control system or automation solution is intended to be used

Note 1 to entry: The security provided to the product, control system or automation solution by its intended environment can effectively restrict the threats that are applicable to the product, control system or automation solution.

[SOURCE: IEC 62443-4-1:2018, 3.1.23, modified – broadened scope to include control systems and automation solutions]

3.1.7
security level
<as defined in IEC 62443-4-2> level corresponding to the required set of countermeasures and inherent security properties of devices and systems for a zone or conduit based on assessment of risk for the zone or conduit

[SOURCE: IEC 62443-4-2:2019, 3.1.37]

3.1.8
security level
<as defined in IEC 62443-3-3> 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.

[SOURCE: IEC 62443-3-3:2013, 3.1.38]

3.2 Abbreviated terms and acronyms

The following abbreviated terms and acronyms are used in this document.

IACS	Industrial Automation and Control System
IS	International Standard
PR	Profile Requirement
TR	Technical Report
TS	Technical Specification

4 Security profile

An IEC 62443 security profile is a defined subset of IEC 62443 requirements, which are contextually mapped e.g., to:

- a specific application domain (e.g., discrete manufacturing, process industry);
- an area of activity (e.g., integration, patch management);
- the intended operational environment and the security context of a product (component, system) or automation solution within that environment; or
- particular type(s) of product(s).

A security profile which is planned to be published as a part of the IEC 62443 series (upcoming IEC 62443-5-x) shall comply with all requirements specified in Clause 5.

The process activities for the creation and validation of IEC 62443 security profiles are defined in Clause 6.

Figure 1 illustrates the relation between the standards and the security profiles within the IEC 62443 series.

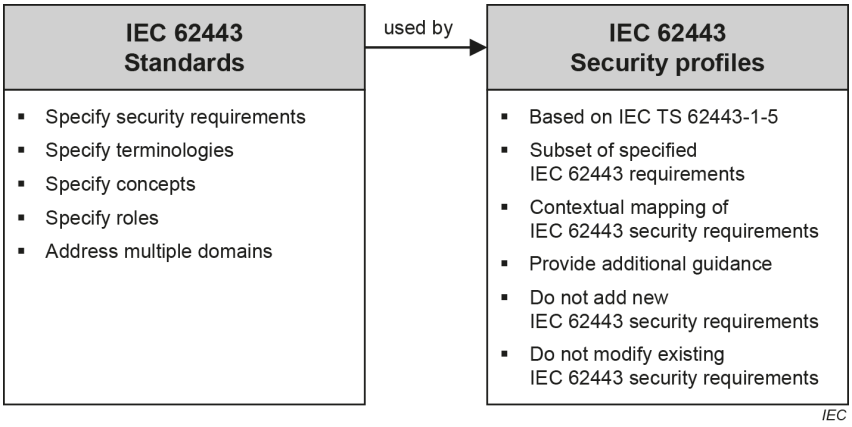

Figure 1 – Relationship between standards and security profiles within the IEC 62443 series

5 Security profile requirements

5.1 General

Clause 5 specifies the mandatory requirements for the content of security profiles (Profile Requirements, PRs). Where relevant, additional rationale and supplemental guidance are provided for each requirement.

Figure 2 shows a flowchart illustrating relations between security profile requirements outlined in the following subclauses.

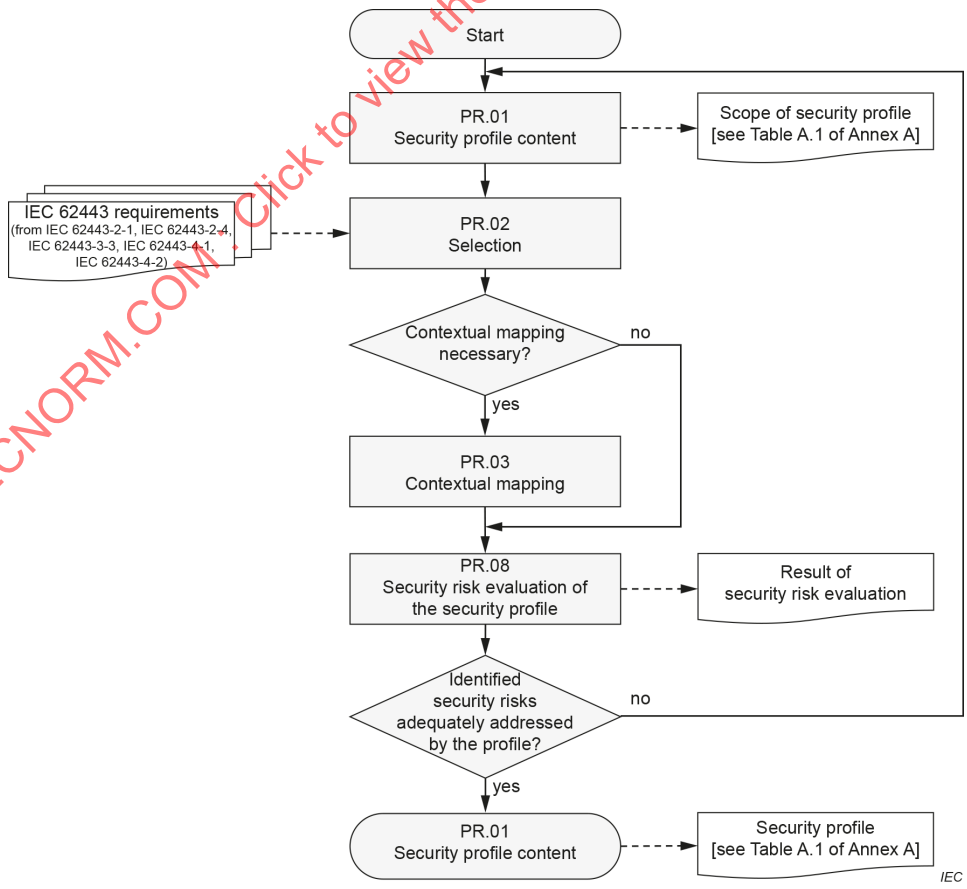

Figure 2 – Relations between security profile requirements

5.2 PR.01: Security profile content

5.2.1 Requirement

Annex A gives the IEC 62443 security profile content. At a minimum, the security profile content specified in Table A.1 shall be documented. Related justification shall be provided for content topics deemed as "not applicable".

5.2.2 Rationale and supplemental guidance

Table A.1 provides the minimum content that is addressed by a security profile. This information is important to understand the need and purpose of a security profile and to support comparability of different security profiles.

5.3 PR.02: Selection

5.3.1 Requirement

The security profile shall refer to a single IEC 62443 document or multiple IEC 62443 documents and select a subset of requirements from one or more of the following IEC 62443 documents:

- IEC 62443-2-1
- IEC 62443-2-4
- IEC 62443-3-3
- IEC 62443-4-1
- IEC 62443-4-2

The security profile shall clearly identify which requirements and requirement enhancements are included and provide justification for those requirements which are not included in the selection.

If a list of requirements and requirement enhancements exists in the standard (e.g. IEC 62443-4-2:2019, Annex B), it should be used as a basis for the selection.

5.3.2 Rationale and supplemental guidance

Due to the interrelationship of the various parts of IEC 62443, the evaluation of the requirements specified by a security profile may also involve the consultation of other parts of the IEC 62443 series. Related results may be documented within the profile.

5.4 PR.03: Contextual mapping

5.4.1 Requirement

Where necessary the security profile should contextually map a requirement to a specific application domain, area of activity and/or intended operational environment, and detail how the requirement is applied in that context.

A contextual mapping shall

- provide context facilitating to relate concepts (including processes, technology, and terminology in the specific application domain, area of activity and the intended operational environment) to the processes, technology, and terminology identified in the requirement;
- provide contextual information on the relation between
  - the applied concepts (including processes, technology, and terminology in the specific application domain, area of activity or the intended operational environment) and
  - the processes, technology, and terminology specified by the requirement;

- not introduce concepts that would extend, reduce, or eliminate the scope and function of the requirement in the specific application domain, area of activity and the intended operational environment; and
- ensure its equivalence to the original requirement in the specific application domain, area of activity and the intended operational environment.

5.4.2 Rationale and supplemental guidance

Contextual mapping may for example be used to:

- align requirements with the terminology used in particular domains;
- explain the application of a requirement in a particular domain or area of activity;
- define preconditions on intended operational environments and the security context; or
- detail certain security mechanisms, e.g. in support of functional interoperability.

A contextual mapping is neither intended to undermine principles and concepts of the underlaying IEC 62443 document(s) nor to alter / modify the definition / rationale of a selected requirement.

EXAMPLE If a profile for 2-4 would contextually map the role of an asset owner to an organization which is not adequately empowered, this could introduce additional security risks.

5.5 PR.04: No new requirements

5.5.1 Requirement

The security profile shall not introduce new requirements in addition to the requirements specified in the selected IEC 62443 document(s) (see 5.3).

5.5.2 Rationale and supplemental guidance

When specifying a security profile, it is important to ensure that no new requirements are introduced, in addition to those already specified in the selected IEC 62443 document(s) (e.g., by a contextual mapping).

5.6 PR.05: No modification of IEC 62443 requirements

5.6.1 Requirement

The security profile shall neither alter / modify the definition nor the corresponding rationale of a selected requirement (see 5.3).

5.6.2 Rationale and supplemental guidance

When specifying a security profile and contextually mapping requirements, it is important not to modify the selected requirements.

5.7 PR.06: Maturity level

5.7.1 Requirement

Where applicable, the security profile may select a minimum maturity level for

- individual requirements;
- a group of requirements (e.g., for a functional area in IEC 62443-2-4, a practice in IEC 62443-4-1); or
- the entire security profile.

NOTE For maturity levels see IEC 62443-2-4:2017, 4.2 and IEC 62443-4-1:2018, 4.2.

EXAMPLE A security profile addressing IEC 62443-4-1 requirements specifies that a secure product development lifecyle must meet all requirements of that standard with at least a particular specified maturity level.

5.7.2 Rationale and supplemental guidance

IEC 62443-2-4 and IEC 62443-4-1 define a maturity level model. The specification of the minimum maturity level in a security profile can support interested parties (e.g. during conformity assessment activities) to achieve comparability of assessed requirements. It can be used, for example, in conformity assessments to verify a minimum level of process maturity for the selected requirements.

5.8 PR.07: Security level

5.8.1 Requirement

Where applicable the security profile may select a minimum security level for

- individual requirements;
- a group of requirements (e.g. for a foundational requirement); or
- all requirements of the respective IEC 62443 document(s).

5.8.2 Rationale and supplemental guidance

IEC 62443-3-3 and IEC 62443-4-2 define a security level model outlining which requirements and requirement enhancements have to be fulfilled for a particular security level (e.g. IEC 62443-4-2:2019, Annex B).

The specification of the minimum security level in a security profile can support interested parties (e.g. during conformity assessment activities) to achieve comparability of assessed requirements.

5.9 PR.08: Security risk evaluation of the security profile

5.9.1 Requirement

Where applicable the security profile shall be based on a documented security risk evaluation that is appropriate to the specific application domain, area of activity and the intended operational environment to:

- identify potential security risks;
- show that the security profile does not introduce additional risks e.g. by the selected subset of requirements; and
- verify that the profile does not undermine the principles of the IEC 62443 series.

NOTE Depending on the scope of a security profile, a security risk evaluation may not be appropriate (see also 5.2.1).

5.9.2 Rationale and supplemental guidance

The security risk evaluation ensures that security risks are identified, adequately addressed, and no new security risks are introduced by the security profile. The security risk evaluation may be used to ensure consistency with the principles, fundamental concepts, and requirements of the IEC 62443 series.

5.10 PR.09: Document type

5.10.1 Requirement

Depending on the envisaged IEC document type for the IEC 62443 security profile (e.g., TR, TS, IS), the proposed security profile shall be submitted to IEC following the related applicable requirements of IEC for that envisaged document type.

5.10.2 Rationale and supplemental guidance

None

6 Process for the creation, validation, and application of IEC 62443 security profiles

6.1 General

The following subclauses define specific process activities for the preparation, validation, and application of IEC 62443 security profiles.

6.2 Creation phase

The author/interested party of a security profile shall ensure that the security profile

- complies with this document;
- meets specific technical, regional or application needs; and
- does not overlap with existing IEC 62443 security profiles which meets their needs.

NOTE Authors/interested parties of a security profile may contact IEC central office or IEC TC 65 for support related to those topics

6.3 Validation phase

A submitted IEC 62443 security profile shall be validated according to the applicable rules of IEC for the related IEC document type of the IEC 62443 security profile (e.g., TR, TS, IS) and particularly according to:

- formal verification of the requirements defined in Clause 5 of this document; and
- technical judgement (purpose, plausibility, reasoning, completeness).

6.4 Application phase

A formally released IEC 62443 security profile shall be applied in total, for example to support interested parties (e.g. during conformity assessment activities) to achieve comparability of assessed requirements.