IEC TS 62443-6-1

Edition 1.0 2024-03

TECHNICAL SPECIFICATION

colour inside

Security for industrial automation and control systems – Part 6-1: Security evaluation methodology for IEC 62443-2-4

IEC TS 62443-6-1

Edition 1.0 2024-03

TECHNICAL SPECIFICATION

colour inside

Security for industrial automation and control systems – Part 6-1: Security evaluation methodology for IEC 62443-2-4

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 25.040.40

ISBN 978-2-8322-8328-8

Warning! Make sure that you obtained this publication from an authorized distributor.

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

____

SECURITY FOR INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS –

Part 6-1: Security evaluation methodology for IEC 62443-2-4

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 TS 62443-6-1 has been prepared by IEC technical committee TC 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
65/1030/DTS	65/1042A/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 https://www.iec.ch/members_experts/refdocs. The main document types developed by IEC are described in greater detail at https://www.iec.ch/standardsdev/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, 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

Repeatable and comparable evaluations of the security program according to IEC 62443-2-4[1] require a common understanding for acceptable evaluation criteria and conformance evidence.

This document supports service providers and evaluators to do a conformity assessment by evaluating the security program against the requirements of IEC 62443-2-4.

This document specifies the evaluation methodology to support interested parties, for example during conformity assessment activities to achieve repeatable and reproducible evaluation results against IEC 62443-2-4 requirements.

[1] Throughout the document, when reference is being made to IEC 62443-2-4 (undated), this means IEC 62443-2-4:2015 and IEC 62443-2-4:2015/AMD1:2017 (Ed.1). A consolidated version of IEC 62443-2-4 is available.

SECURITY FOR INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS –

Part 6-1: Security evaluation methodology for IEC 62443-2-4

1 Scope

This part of IEC 62443 specifies the evaluation methodology to support interested parties (e.g. during conformity assessment activities) to achieve repeatable and reproducible evaluation results against IEC 62443-2-4 requirements. This document is intended for first-party, second-party or third-party conformity assessment activity, for example by product suppliers, service providers, asset owners and conformity assessment bodies.

NOTE 1 62443-2-4 specifies requirements for security capabilities of an IACS service provider. These security capabilities can be offered as a security program during integration and maintenance of an automation solution.

NOTE 2 The term “conformity assessment” and the terms first-party conformity assessment activity, second-party conformity assessment activity and third-party conformity assessment activity are defined in ISO/IEC 17000.

2 Normative references

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

IEC 62443-2-4:2015*, Security for industrial automation and control systems – Part 2-4: Security program requirements for IACS service providers*
IEC 62443-2-4:2015/AMD1:2017

3 Terms, definitions and abbreviated terms

3.1 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

IEC and ISO 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
acceptable evaluation criteria
criteria which may be used for an evaluation

Note 1 to entry: Acceptable evaluation criteria indicated in this document are only examples, which are by no means complete and where also other or alternative evidence can be used to demonstrate the fulfilment of, or conformity to, the related requirement.

3.1.2
evaluator
individual or organisation that performs an evaluation

Note 1 to entry: An evaluator can act in the context of first-party, second-party or third-party conformity assessment activity according ISO/IEC 17000.

[SOURCE: ISO/IEC 25000:2014, 4.10, modified – the note has been added.]

3.1.3
evaluation
systematic determination of the extent to which the subject under evaluation (SuE) meets its specified requirements

[SOURCE: ISO/IEC 12207:2008, 4.12, modified – “an entity” has been replaced with “the subject under evaluation (SuE)".]

3.1.4
evidence of existence
EoE
documentation showing evidence that a process, procedures, templates or checklists had been created to support service provider activities

3.1.5
examine, verb
generate a verdict by analysis using evaluator expertise

[SOURCE: ISO/IEC 18045:2022, 3.9, modified – the note has been removed.]

3.1.6
key performance indicator
KPI
quantifiable measure that an organization uses to gauge or compare performance in terms of meeting its strategic and operational objectives

Note 1 to entry: The key performance indicator can be used to assess the success of applied measures or to demonstrate continuous improvement.

[SOURCE: ISO 18788:2015, 3.2.5, modified – the note has been added.]

3.1.7
overall maturity level
maturity level assigned to the entire security program

Note 1 to entry: Maturity levels are specified in IEC 62443-2-4:2015 and IEC 62443-2-4:2015/AMD1:2017, Table 1.

3.1.8
process
set of interrelated or interacting activities that transform input to output

[SOURCE: ISO 9000:2015, 3.4.1, modified – “use inputs to deliver an intended result” has been replaced with “transform input to output” and the notes have been removed.]

3.1.9
project
integration or maintenance service execution for an asset owner

3.1.10
proof of execution
PoE
documentation or other evidence showing the accomplishment of activities performed as a service provider for an automation solution

Note 1 to entry: In general, evidence of existence is the baseline documentation used during the execution.

3.1.11
reference architecture
generic control system, consisting of hardware and software components, used as a basis for an automation solution

3.1.12
subject under evaluation
SuE
subject agreed to be evaluated, related to conformity to the requirements of the document

Note 1 to entry: ‘Subject under evaluation’ is similar to the term ‘object of conformity assessment’ specified in ISO/IEC 17000.

EXAMPLE 1 Processes.

EXAMPLE 2 Systems.

EXAMPLE 3 Solutions.

EXAMPLE 4 Components.

3.1.13
security program
portfolio of security services, including integration services and maintenance services, and their associated policies, procedures, and products that are applicable to the IACS

Note 1 to entry: The security program for IACS service providers refers to the policies and procedures defined by them to address security concerns of the IACS.

[SOURCE: IEC 62443-2-4:2015, 3.1.18]

3.1.14
trustworthiness
ability to meet stakeholders expectations in a verifiable way

[SOURCE:ISO/IEC 30145-2:2020, 3.9, modified – the notes have been removed.]

3.2 Abbreviated terms

EICAR	European Institute for Computer Antivirus Research (www.eicar.com)
EoE	evidence of existence
EWS	engineering workstation
FAT	factory acceptance test
KPI	key performance indicator
ML	maturity level
NDA	non-disclosure agreement
NIST	National Institute of Standards and Technology
PoE	proof of execution
RDP	remote desktop protocol

SAT	site acceptance test
SIEM	security information and event management
SIS	safety instrumented system
SuE	subject under evaluation

4 Overview

This document contains two parts:

- Clause 5 specifies the evaluation methodology for the conformity assessment of IEC 62443-2-4 requirements. Subclause 5.1 to subclause 5.3 are applicable to all maturity levels (ML 1-4). Subclause 5.4 is only applicable to maturity level 4 (ML 4).
- Clause 6 provides guidance that shall be used to evaluate the IEC 62443-2-4 requirements according to the respective maturity level. Table 1 shows acceptable evaluation criteria and examples for conformance evidence for each requirement.

5 Methodology for the evaluation

5.1 Scoping of the subject under evaluation (SuE)

The evaluation starts with the scope of the SuE containing at least the following information:

- security program to which conformance to IEC 62443-2-4 is claimed for an integration service, a maintenance service or both,
- organization (unit, department(s)) that implements the security program as part of its integration service, a maintenance service or both,
- security requirements of IEC 62443-2-4 for which the service provider is claiming conformity; those may be all requirements, or a particular requirements subset as specified by an IEC 62443-5-x security profile,
- requested maturity level, i.e. ML-1, ML-2, ML-3 or ML-4, for each requirement in the scope.

Evaluations shall be performed according to the selected maturity levels for various particular requirements of IEC 62443-2-4. It is not required that service providers have to select a particular overall (summary) ML-value for the evaluation of a SuE. Evaluations in the context of ISO/IEC 17000 third-party conformity assessment activities shall only be performed with ML-2 or higher.

NOTE Requirements for cyber security profiles are specified in IEC TS 62443-1-5.

5.2 Content of conformity statements and conformance evidence

To support claims of conformance, evidence shall be provided to support the maturity level for each requirement for which conformance is claimed. A conformity statement can be used to explain how the evidence provided supports the service provider SuE meeting a requirement at a specific maturity level. Table 1 provides examples for conformance evidence. Where the applicant requests evaluation with requirements as not-applicable, this shall be accompanied with justification of this non-applicability to the SuE.

For requirements not in scope:

- they shall be marked accordingly, and
- the provision of conformity statement and conformance evidence as specified in Table 1 is not required.

For requirements which are in the scope and not applicable:

– they shall be marked accordingly,

– a rationale or other evidence to support the scope specification for each requirement deemed as Not Applicable shall be provided, and

– the provision of conformance evidence as specified in Table 1 is not required.

5.3 Evaluation of conformity statement and conformance evidence

The SuE and related evidence specified and documented according to 5.2 shall be the basis for the evaluation. The provided SuE scoping, conformity statements and conformance evidence are used to evaluate the SuE. The evaluation process consists of an evaluation of each requirement of IEC 62443-2-4 within the specified scope (including those not applicable) using the following procedure:

a) Examine that the conformity statement, if provided, explains how the evidence fulfils the requirement completely for the requested maturity level within the specified scope (see 5.1). Table 1 contains acceptable evaluation criteria, which are intended to lead to an objective verdict.

b) Examine that the conformance evidence is valid, consistent, veritable, trustworthy and that the requirements for conformance evidence of the requested maturity level in 6.2 to 6.5 are also fulfilled, and that if the conformity statement is not provided, then the evidence stands independently without the need of any further explanation. Table 1 contains examples of conformance evidence for each maturity level for guidance.

c) If the requirement is marked as not applicable, then the validity of this decision is examined on the basis of the rationale or evidence provided.

NOTE 1 How often the evaluation process is repeated, for example to get a result, is beyond the scope of this document.

NOTE 2 The assignment of an overall level of ML-X (1-4) for an SuE is presently not defined within the IEC 62443 series, but the ML is evaluated for each individual IEC 62443-2-4 requirement. However, future profiles related to IEC 62443 can specify that each requirement of IEC 62443-2-4 are fulfilled at least with ML-X.

5.4 Particular requirements for evaluations related to ML-4

According to the specification of maturity level ML-4 in IEC 62443-2-4, and as outlined further in 6.6, evaluations of SuE related to a declared maturity level ML-4 require a systematic control of the effectiveness and performance of the fulfilment of the requirements by the SuE, and the demonstration of a continuous improvement of that fulfilment over a period of time. An evaluation of SuE for a maturity level of ML-4 is therefore only performed for a significant period of time after achieving maturity level ML-3 for the particular requirement. By default, such a "period of time" typically is one year.

6 Table used for evaluation

6.1 Overview

Table 1 shall be used for the evaluation as described in Clause 5. It provides the following columns:

- Columns A to C are the requirements of the standard IEC 62443-2-4. Each row in column C of Table 1 specifies a requirement for a process that the service provider can perform for the asset owner for the integration or maintenance of the automation solution.
- Column D describes the evaluation criteria for these requirements.

NOTE 1 The text of each evaluation criteria description, begins with “The service provider shall have a process that can be performed for the asset owner to” to clarify that the IEC 62443-2-4 requirements cannot be interpreted as requirements for technical capabilities. Whether an asset owner requires the service provider to perform the process is beyond the scope of this document.

- Columns E to H provide examples of conformance evidence which may be taken into account to support the related claims for compliance to those criteria for ML-1, ML-2, ML-3 and ML-4.

In addition to the examples for conformance evidence provided in Table 1 itself, 6.3 to 6.6 provide further considerations, which can help to understand and apply the related examples of conformance evidence outlined in Table 1.

NOTE 2 For details on the definition of maturity levels ML-1, ML-2, ML-3 and ML-4, see IEC 62443-2-4 and Annex A.

6.2 Evaluation criteria

The evaluation criteria are intended to be an orientation for the evaluator in order to achieve a comparable evaluation result as far as possible. Since the requirements are usually very long and can contain “multiple shalls”, the acceptable evaluation criteria are often divided into several points. This division of the criteria is intended to increase the comprehensibility of the requirement and to achieve an as equal as possible interpretation of the requirement.

6.3 Conformance evidence related to maturity level ML-1

For maturity level ML-1, the service provider typically performs the service in an ad-hoc and often undocumented (or not fully documented) manner. Therefore, the related process documentation for a requirement often does not exist or is incomplete and correspondingly evidence of execution is used to determine if a requirement is met, for example the record from an evaluation interview or a statement of work under contract with the asset owner.

6.4 Conformance evidence related to maturity level ML-2

For maturity level ML-2, the service provider is required by IEC 62443-2-4 to provide its service process according to repeatable, written policies. Evaluation activities for maturity level ML-2 therefore particularly focus on the examination of the availability and validity of documented processes for those services, and of the availability of training materials and training records demonstrating that the personnel (including subcontractors and consultants) follow those processes in a repeatable way, and that they possess the required qualifications. The related documentation is referred to as evidence of existence (EoE).

6.5 Conformance evidence related to maturity level ML-3

According to the specification of maturity level ML-3 in IEC 62443-2-4, processes that are claimed to meet requirements related to a declared maturity level ML-3 are required to have been practiced for an asset owner.

For conformity to maturity level ML-3, the conformity of the SuE to ML-2 shall be successfully evaluated first, or all relevant ML-2 aspects shall be successfully evaluated in parallel in the actual ML-3 evaluation. In addition, conformance evidence shall show that the ML-2 conformance process was performed for at least one asset owner. The related documentation is referred to as proof of execution (PoE).

For conformance evidence related to maturity level ML-3, the following constraints shall be considered:

- ML-3 conformance evidence cannot always be internally available at the service provider's organization but can be under the control of the respective asset owner, or other third parties. For example, the service provider has to respect the non-disclosure agreement (NDA) conditions of its clients. Hence, availability of such evidence can depend on the consent of its respective owner.
- For particular requirements, it will not be possible to generate relevant artefacts as ML-3 conformance evidence.
- Certain requirements depend on the availability of input that is under the responsibility of the asset owner (e.g. written Management-of-Change processes, or asset owner policies

which need to be followed). It can be the case that such input from the asset owner's side has not been made available to the service provider, or ML-3 conformance evidence is provided in an anonymized or sanitized form.

- For particular requirements, ML-3 conformance can be demonstrated by technical means that ensure that a requirement is always fulfilled. For example, the validity of configuration changes (SP.03.09) can be ensured using digital signatures.

In particular, implicit conformance evidence which can be generated by the service provider itself without dependencies on any third-party that are not involved in the evaluation shall be considered.

6.6 Conformance evidence related to maturity level ML-4

For conformity to maturity level ML-4, the conformity of the SuE shall be successfully evaluated to ML-3. In addition, conformance evidence shall show the following:

- The specification of the performance indicators or similar metrics for the SuE which are used to measure the delivery, effectiveness and performance related to IEC 62443-2-4.
- The documented process or procedure specifying the application of those performance indicators or similar metrics for continuous improvement.
- Conformance evidence demonstrating the continuous improvements related to those performance indicators or metrics over a significant period of time. Such a continuous improvement is determined and documented at a related internal audit or management meeting. The detailed report of those audit/meetings demonstrating the improvement is an acceptable ML-4 conformance evidence.