



BSI Standards Publication

Security for industrial automation and control systems

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

National foreword

This Published Document is the UK implementation of CLC IEC/TS 62443-6-1:2024. It is identical to IEC TS 62443-6-1:2024. It supersedes PD IEC TS 62443-6-1:2024, which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee GEL/65, Measurement and control.

A list of organizations represented on this committee can be obtained on request to its committee manager.

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

This publication is not to be regarded as a British Standard.

© The British Standards Institution 2024
Published by BSI Standards Limited 2024

ISBN 978 0 539 34691 6

ICS 25.040.40

Compliance with a Published Document cannot confer immunity from legal obligations.

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 31 March 2024.

Amendments/corrigenda issued since publication

Date	Text affected
31 December 2024	This corrigendum renumbers PD IEC TS 62443-6-1:2024 as PD CLC IEC/TS 62443-6-1:2024

English Version

Security for industrial automation and control systems - Part 6-1:
Security evaluation methodology for IEC 62443-2-4
(IEC/TS 62443-6-1:2024)

Sécurité des automatismes industriels et des systèmes de
commande - Partie 6-1: Méthodologie d'évaluation de la
sécurité pour la IEC 62443-2-4
(IEC/TS 62443-6-1:2024)

IT-Sicherheit für industrielle Automatisierungssysteme -
Teil 6-1: Security-Evaluierungsmethodik für IEC 62443-2-4
(IEC/TS 62443-6-1:2024)

This Technical Specification was approved by CENELEC on 2024-12-09.

CENELEC members are required to announce the existence of this TS in the same way as for an EN and to make the TS available promptly at national level in an appropriate form. It is permissible to keep conflicting national standards in force.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and the United Kingdom.



European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

European foreword

This document (CLC IEC/TS 62443-6-1:2024) consists of the text of document IEC/TS 62443-6-1:2024, prepared by IEC/TC 65 "Industrial-process measurement, control and automation".

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CENELEC shall not be held responsible for identifying any or all such patent rights.

Any feedback and questions on this document should be directed to the users' national committee. A complete listing of these bodies can be found on the CENELEC website.

Endorsement notice

The text of the International Technical Specification IEC/TS 62443-6-1:2024 was approved by CENELEC as a European Technical Specification without any modification.

In the official version, for Bibliography, the following notes have to be added for the standard indicated:

IEC/TS 62443-1-5	NOTE	Approved as CLC IEC/TS 62443-1-5
ISO/IEC 17000:2020	NOTE	Approved as EN ISO/IEC 17000:2020 (not modified)
ISO/IEC 18045:2022	NOTE	Approved as EN ISO/IEC 18045:2023 (not modified)
ISO 9000:2015	NOTE	Approved as EN ISO 9000:2015 (not modified)

Annex ZA

(normative)

Normative references to international publications with their corresponding European publications

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.

NOTE 1 Where an International Publication has been modified by common modifications, indicated by (mod), the relevant EN/HD applies.

NOTE 2 Up-to-date information on the latest versions of the European Standards listed in this annex is available here: www.cenelec.eu.

<u>Publication</u>	<u>Year</u>	<u>Title</u>	<u>EN/HD</u>	<u>Year</u>
IEC 62443-2-4	2015	Security for industrial automation and control systems – Part 2-4: Security program requirements for IACS service providers	EN 62443-2-4	2019
+ A1	2017		+ A1	2019

CONTENTS

FOREWORD.....	3
INTRODUCTION.....	5
1 Scope.....	6
2 Normative references	6
3 Terms, definitions and abbreviated terms	6
3.1 Terms and definitions.....	6
3.2 Abbreviated terms.....	8
4 Overview	9
5 Methodology for the evaluation.....	9
5.1 Scoping of the subject under evaluation (SuE).....	9
5.2 Content of conformity statements and conformance evidence	9
5.3 Evaluation of conformity statement and conformance evidence.....	10
5.4 Particular requirements for evaluations related to ML-4.....	10
6 Table used for evaluation	10
6.1 Overview	10
6.2 Evaluation criteria	11
6.3 Conformance evidence related to maturity level ML-1	11
6.4 Conformance evidence related to maturity level ML-2	11
6.5 Conformance evidence related to maturity level ML-3	11
6.6 Conformance evidence related to maturity level ML-4	12
6.7 Overview of evaluation criteria and examples of conformance evidence (Table 1).....	13
Annex A (informative) Legend for maturity levels	131
Bibliography.....	132
Table 1 – Overview of evaluation criteria and examples of conformance evidence	13

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 62443-2-4¹ 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.

6.7 Overview of evaluation criteria and examples of conformance evidence (Table 1)

Table 1 – Overview of evaluation criteria and examples of conformance evidence

A	B	C	D	E	F	G	H
Summary Level	IEC 62443-2-4 ID	IEC 62443-2-4 requirement	Evaluation criteria	Examples for ML-1 conformance evidence (see 6.3)	Examples for ML-2 conformance evidence (see 6.4) EoE	Examples for additional ML-3 conformance evidence (see 6.5) EoE + PoE	Examples for additional ML-4 conformance evidence of continuous process improvement (see 6.6)
Solution staffing	SP.01.01 BR	The service provider shall have the capability to ensure that it assigns only service provider personnel to automation solution related activities who have been informed of and comply with the responsibilities, policies, and procedures required by this document	<ol style="list-style-type: none"> The service provider shall have a process that can be performed for the asset owner to inform and assign personnel to the automation solution The process includes a verification/validation step that only informed personnel is assigned to The training content shall include IEC 62443-2-4 topics The service provider personnel shall accept their responsibility to comply with the security aspects that they have been informed about 	<p>Examples of execution that the service provider has met the requirement at least for one customer for example:</p> <ol style="list-style-type: none"> Project documentation Interviews 	<ol style="list-style-type: none"> Documented process Initial training materials / records of participation (i.e. first participants are trained), automated training logs Security manual / handbook / policy or other documentation that are required reading for personnel prior to their assignment to the solution 	<ol style="list-style-type: none"> List of all the staff involved in the project who have been security role-based trained Solution staffing list matches with trained personnel at training record 	<ol style="list-style-type: none"> KPI: Training coverage statistics Periodical review of training contents Periodic reviews of meeting minutes showing improvements of solution staffing list matching with the latest training records

A	B	C	D	E	F	G	H
Summary Level	IEC 62443-2-4 ID	IEC 62443-2-4 requirement	Evaluation criteria	Examples for ML-1 conformance evidence (see 6.3)	Examples for ML-2 conformance evidence (see 6.4) EoE	Examples for additional ML-3 conformance evidence (see 6.5) EoE + PoE	Examples for additional ML-4 conformance evidence of continuous process improvement (see 6.6)
Solution staffing	SP.01.01 RE(1)	The service provider shall have the capability to ensure that it assigns only subcontractor or consultant personnel to automation solution related activities who have been informed of and comply with the responsibilities, policies, and procedures required by this document	<p>1) The service provider shall have a process that can be performed for the asset owner to inform and assign subcontractor or consultant personnel to the automation solution</p> <p>2) The process includes a verification/validation step that only informed subcontractor or consultant personnel is assigned to</p> <p>3) The training content shall include IEC 62443-2-4 topics</p> <p>4) The service provider subcontractor or consultant personnel shall accept their responsibility to comply with the security aspects that they have been informed about</p>	<p>Examples of execution that the service provider has met the requirement at least for one customer, for example:</p> <p>1) Project documentation</p> <p>2) Interviews</p>	<p>1) Documented process</p> <p>2) Initial training materials / records of participation (i.e. first participants are trained), automated training logs</p> <p>3) Security manual / handbook / policy or other documentation that are required reading for personnel prior to their assignment to the solution</p>	<p>1) List of all the staff involved in the project who have been security role-based trained</p> <p>2) Solution staffing list matches with trained personnel at training record</p>	<p>1) KPI: Training coverage statistics</p> <p>2) Periodical review on training contents</p>

A	B	C	D	E	F	G	H
Summary Level	IEC 62443-2-4 ID	IEC 62443-2-4 requirement	Evaluation criteria	Examples for ML-1 conformance evidence (see 6.3)	Examples for ML-2 conformance evidence (see 6.4) EoE	Examples for additional ML-3 conformance evidence (see 6.5) EoE + PoE	Examples for additional ML-4 conformance evidence of continuous process improvement (see 6.6)
Solution staffing	SP.01.02 BR	The service provider shall have the capability to ensure that it assigns only service provider, subcontractor or consultant personnel to automation solution related activities who have been informed of and comply with the security-related responsibilities, policies, and procedures required by the asset owner	<p>The service provider shall have a process that can be performed for the asset owner to:</p> <ol style="list-style-type: none"> determine the asset owner's security requirements, policies and procedures, make its personnel aware of their responsibilities to comply with these security requirements, policies and procedures, direct its subcontractors and consultants to comply with this requirement 	<p>Examples of execution that the service provider has met the requirement at least for one customer for example:</p> <ol style="list-style-type: none"> Project documentation Interviews 	<ol style="list-style-type: none"> Documented process Verification / validation step that these obtained requirements will be respected / followed by the personnel, for example checklist template for obtaining asset owner's requirements Policy on subcontractors or subcontractor agreement template Training materials / records / security manual / handbook or other documentation that are required reading for personnel prior to their assignment to the solution 	<ol style="list-style-type: none"> Participant list / attestation of personnel for the asset owner required training about its responsibilities, policies and procedures Asset owner agreement Subcontractor agreement Completed checklist for particular automation solution 	<ol style="list-style-type: none"> The service provider agrees with asset owner(s) on a feedback channel on a continuous basis The service provider demonstrates continuous improvements related to the feedback from asset owner(s) Subcontractor re-evaluation and conformance check to asset owner policies, procedures might be adequate

A	B	C	D	E	F	G	H
Summary Level	IEC 62443-2-4 ID	IEC 62443-2-4 requirement	Evaluation criteria	Examples for ML-1 conformance evidence (see 6.3)	Examples for ML-2 conformance evidence (see 6.4) EoE	Examples for additional ML-3 conformance evidence (see 6.5) EoE + PoE	Examples for additional ML-4 conformance evidence of continuous process improvement (see 6.6)
Solution staffing	SP.01.02 RE(1)	The service provider shall have the capability to ensure that it assigns only service provider, subcontractor or consultant personnel to automation solution related activities who have been informed of and comply with the asset owner's Management-of-Change (MoC) and Permit to Work (PtW) processes,	The service provider shall have a process that can be performed for the asset owner to: 1) determine the asset owner's Management-of-Change (MoC) and Permit to Work (PtW) processes, 2) make its personnel aware of their individual responsibilities required to support these processes, 3) direct its subcontractors and consultants to comply with this requirement	Examples of execution that the service provider has met the requirement at least for one customer for example: 1) Project documentation 2) Interviews	1) Documented process 2) Checklists for following related asset owner(s) processes 3) Policy on subcontractors or subcontractor agreement template 4) Training materials / records/security manual / handbook or other documentation on MoC and PtW processes, that are required reading for personnel prior to their assignment to the Solution 5) Checklist for obtaining asset owner's requirements	1) Record on MoC of the customer was followed 2) Record on PtW of customer was followed especially on asset owner's site 3) Subcontractor agreements, if subcontractors were involved	1) The service provider agrees with asset owner(s) on a feedback channel related to MoC and PtW on a continuous basis 2) The service provider demonstrates continuous improvements related to the feedback based on MoC and PtW from asset owner(s)

A	B	C	D	E	F	G	H
Summary Level	IEC 62443-2-4 ID	IEC 62443-2-4 requirement	Evaluation criteria	Examples for ML-1 conformance evidence (see 6.3)	Examples for ML-2 conformance evidence (see 6.4) EoE	Examples for additional ML-3 conformance evidence (see 6.5) EoE + PoE	Examples for additional ML-4 conformance evidence of continuous process improvement (see 6.6)
Solution staffing	SP.01.03 BR	The service provider shall have the capability to ensure that it assigns only service provider personnel to automation solution related activities who have been informed of and comply with the policies, procedures, and contractual obligations required to protect the confidentiality of the asset owner's data	The service provider shall have a process that can be performed for the asset owner to: <ol style="list-style-type: none"> 1) protect the confidentiality of asset owner's data, 2) make its personnel aware of the confidentiality agreements with the asset owner, 3) direct its personnel to comply with this requirement 	Examples of execution that the service provider has met the requirement at least for one customer for example: <ol style="list-style-type: none"> 1) Project documentation 2) Interviews 	<ol style="list-style-type: none"> 1) Documented process about confidentiality protection 2) Data classification policy 3) HR related policies and procedures such as training materials/record template, including process to be used to identify and protect sensitive data 4) Security manual for confidentiality requirements 5) Confidentiality agreement template, for example NDA template 5) Evidence of internal audit by the service provider conducted on a regular basis on its employees for verification of asset owner's data in their custody. 6) Policies in place restricting use of personal laptops and portable drives when providing services to the asset owners. 	<ol style="list-style-type: none"> 1) NDA stating protection of the confidentiality of asset owner's data 2) Training records for assigned personnel about protection of sensitive data 3) Policy enforcement like work contract for assigned personnel 	<ol style="list-style-type: none"> 1) KPI: amount and severity of detected confidentiality breaches 2) Confidentiality issues reach the value "0" over a period of time 3) Satisfaction of asset owner (via feedback) on confidentiality protection by service provider continuously improves

A	B	C	D	E	F	G	H
Summary Level	IEC 62443-2-4 ID	IEC 62443-2-4 requirement	Evaluation criteria	Examples for ML-1 conformance evidence (see 6.3)	Examples for ML-2 conformance evidence (see 6.4) EoE	Examples for additional ML-3 conformance evidence (see 6.5) EoE + PoE	Examples for additional ML-4 conformance evidence of continuous process improvement (see 6.6)
Solution staffing	SP.01.03 RE(1)	The service provider shall have the capability to ensure that it assigns only subcontractors, consultants, and representatives to automation solution related activities who have been informed of and comply with the policies and procedures required to protect the confidentiality of the asset owner's data	The service provider shall have a process that can be performed for the asset owner to assign subcontractors or consultant personnel to: 1) protect the confidentiality of asset owner's data, 2) make its subcontractors, consultants, and representatives aware of the confidentiality agreements with the asset owner, 3) direct its subcontractors, consultants, and representatives to comply with this requirement	Examples of execution that the service provider has met the requirement at least for one customer for example: 1) Project documentation 2) Interviews	1) Subcontractor agreement template including enforcement of protecting asset owner's data 2) Checklists / templates used by subcontractors or consultants, or both, for protection of asset owner data	1) NDA between service provider and subcontractor stating protecting the confidentiality of asset owner's data 2) Subcontractor agreements like work contracts with confidentiality clauses	1) KPI: amount and severity of detected confidentiality breaches by subcontractors / consultants 2) Confidentiality issues reach the value "0" over a period of time 3) Satisfaction of asset owner (via feedback) on confidentiality protection by subcontractors/consultants continuously improves

A	B	C	D	E	F	G	H
Summary Level	IEC 62443-2-4 ID	IEC 62443-2-4 requirement	Evaluation criteria	Examples for ML-1 conformance evidence (see 6.3)	Examples for ML-2 conformance evidence (see 6.4) EoE	Examples for additional ML-3 conformance evidence (see 6.5) EoE + PoE	Examples for additional ML-4 conformance evidence of continuous process improvement (see 6.6)
Solution staffing	SP.01.04 BR	The service provider shall have the capability to ensure that it assigns only service provider personnel to automation solution related activities who have successfully passed security-related background checks, where feasible, and to the extent allowed by applicable law	The service provider shall have a process that can be performed for the asset owner to ensure that assigned personnel: <ol style="list-style-type: none"> 1) have successfully passed security related background checks 	Examples of execution that service provider has met the requirement at least for one customer for example: <ol style="list-style-type: none"> 1) Project documentation 2) Interviews 	<ol style="list-style-type: none"> 1) Documented process for conducting background checks 2) Background check template used by the service provider 3) Documents like service contracts, work contracts, etc., which include related sections for background checks 	<ol style="list-style-type: none"> 1) Background checks were performed according to the applicable legal framework and usual industry specific rules 	<ol style="list-style-type: none"> 1) Background checks successfully and consistently applied and continuously improved for a significant time frame
Solution staffing	SP.01.04 RE(1)	The service provider shall have the capability to ensure that it assigns only subcontractors, consultants, and representatives to automation solution related activities who have successfully passed security-related background checks where feasible, and to the extent allowed by applicable law	The service provider shall have a process that can be performed for the asset owner that assigned subcontractor / consultants / representatives: <ol style="list-style-type: none"> 1) have successfully passed security related background checks 	Examples of execution that service provider has met the requirement at least for one customer for example: <ol style="list-style-type: none"> 1) Project documentation 2) Interviews 	<ol style="list-style-type: none"> 1) Documented process for conducting background checks for subcontractor / consultants / representatives 2) Background check template used for subcontractor / consultant / representative 3) Third party contract for performing background checks on subcontractor / consultants / representatives 4) Usage of blacklists for subcontractors / consultants / representatives 	<ol style="list-style-type: none"> 1) Background checks were performed according to the applicable legal framework and usual industry specific rules for subcontractor / consultants / representatives 	<ol style="list-style-type: none"> 1) Background checks successfully and consistently applied and continuously improved for a significant time frame for subcontractors / consultants / representatives

A	B	C	D	E	F	G	H
Summary Level	IEC 62443-2-4 ID	IEC 62443-2-4 requirement	Evaluation criteria	Examples for ML-1 conformance evidence (see 6.3)	Examples for ML-2 conformance evidence (see 6.4) EoE	Examples for additional ML-3 conformance evidence (see 6.5) EoE + PoE	Examples for additional ML-4 conformance evidence of continuous process improvement (see 6.6)
Solution staffing	SP.01.05 BR	<p>The service provider shall have the capability to assign a security contact in its organization to the automation solution who is responsible and accountable for the following activities.</p> <ol style="list-style-type: none"> 1) Acting as liaison with the asset owner, as appropriate, about the service provider's and the automation solution's adherence to the IEC 62443-2-4 requirements that are required by the asset owner. 2) Communicating the service provider's point-of-view on IACS security to the asset owner's staff. 	<p>The service provider shall have a process that can be performed for the asset owner that security contacts have been assigned and qualified. This includes defined role(s) meeting the items 1) to 4) of the requirement. The security contact shall accept its responsibility.</p>	<p>Examples of execution that the service provider has met the requirement at least for one customer for example:</p> <ol style="list-style-type: none"> 1) Project documentation 2) Interviews 	<ol style="list-style-type: none"> 1) Role description including related support by the management 2) Documented process for selecting a qualified individual (e.g. management or human resources policy for staffing positions) 	<ol style="list-style-type: none"> 1) Solution organization chart showing this position 2) Role assignment letter and acceptance of the person in the project organization in the form of a meeting protocol or a declaration of consent 	<ol style="list-style-type: none"> 1) No. of projects with allocated security contact is 100 % for a longer period of time 2) Role description for security contact is continuously improved based on experiences from projects, discussions and feedback from asset owner 3) Increasing and maintaining the capability of the security contact such as keeping up to date with security issues

A	B	C	D	E	F	G	H
Summary Level	IEC 62443-2-4 ID	IEC 62443-2-4 requirement	Evaluation criteria	Examples for ML-1 conformance evidence (see 6.3)	Examples for ML-2 conformance evidence (see 6.4) EoE	Examples for additional ML-3 conformance evidence (see 6.5) EoE + PoE	Examples for additional ML-4 conformance evidence of continuous process improvement (see 6.6)
		<p>3) Ensuring that tenders to the asset owner are aligned and in compliance with the IEC 62443-2-4 requirements specified as required by the asset owner and the service provider's internal IACS security requirements.</p> <p>4) Communicating to the asset owner deviations from, or other issues not conforming with, the IEC 62443-2-4 requirements that are required by the asset owner. This includes deviations between these requirements and the service provider's internal requirements</p>					

A	B	C	D	E	F	G	H
Summary Level	IEC 62443-2-4 ID	IEC 62443-2-4 requirement	Evaluation criteria	Examples for ML-1 conformance evidence (see 6.3)	Examples for ML-2 conformance evidence (see 6.4) EoE	Examples for additional ML-3 conformance evidence (see 6.5) EoE + PoE	Examples for additional ML-4 conformance evidence of continuous process improvement (see 6.6)
Solution staffing	SP.01.06 BR	The service provider shall have documented minimum IACS cyber-security qualifications for security lead positions and the capability to assign security leads to automation solutions who meet these qualifications	The service provider shall have a process that can be performed for the asset owner that security leads for automation solution are assigned and are qualified for this role	Examples of execution that the service provider has met the requirement at least for one customer for example: 1) Project documentation 2) Interviews	1) Documented role description including minimum IACS cyber-security qualifications 2) Documented process for selecting a qualified individual (e.g. management or human resources policy for staffing positions) 3) Appointment letter template or similar document which includes checks of qualification	1) Solution organization chart showing this position 2) Role assignment letter	1) For a longer period of time all projects have an allocated security lead unless for agreed exceptions 2) Increase of cyber security expertise of security leads for example by experiences, trainings and certifications 3) Role description for security lead is continuously improved based on experiences from projects, including feedback from asset owner

A	B	C	D	E	F	G	H
Summary Level	IEC 62443-2-4 ID	IEC 62443-2-4 requirement	Evaluation criteria	Examples for ML-1 conformance evidence (see 6.3)	Examples for ML-2 conformance evidence (see 6.4) EoE	Examples for additional ML-3 conformance evidence (see 6.5) EoE + PoE	Examples for additional ML-4 conformance evidence of continuous process improvement (see 6.6)
Solution staffing	SP.01.07 BR	The service provider shall have the capability to notify the asset owner of changes in the service provider, subcontractor, or consultant personnel who have access to the automation solution	<p>The service provider shall have a process that can be performed for the asset owner to inform the asset owner of changes to:</p> <ol style="list-style-type: none">1) New personnel who need to get access to the solution2) Personnel who no longer need access to the solution	<p>Examples of execution that the service provider has met the requirement at least for one customer for example:</p> <ol style="list-style-type: none">1) Project documentation2) Interviews	<ol style="list-style-type: none">1) Documented process for promptly notifying the asset owner about the change of personnel2) Documented process agreed with the asset owner of which personnel changes require notification3) Form / template for personnel change notification	<ol style="list-style-type: none">1) Completed form for personnel change notification2) Central repository of personnel with access to the automation solution, for example ticketing system3) Secure e-mail notifications4) Agreed organigram with the asset owner5) Documented communication to the asset owner about new personal trainings conducted	<ol style="list-style-type: none">1) KPI: Execution time until asset owner is informed about change of personnel

A	B	C	D	E	F	G	H
Summary Level	IEC 62443-2-4 ID	IEC 62443-2-4 requirement	Evaluation criteria	Examples for ML-1 conformance evidence (see 6.3)	Examples for ML-2 conformance evidence (see 6.4) EoE	Examples for additional ML-3 conformance evidence (see 6.5) EoE + PoE	Examples for additional ML-4 conformance evidence of continuous process improvement (see 6.6)
Assurance	SP.02.01 BR	The service provider shall have the capability to provide documentation that verifies that automation solution components identified by the asset owner (e.g. as result of a security assessment, threat analysis, or security testing, or both) have adequate security for their level of risk	<p>The service provider shall have a process that can be performed for the asset owner to identify:</p> <ol style="list-style-type: none"> 1) The level of risk adequate for the components in the security context of the automation solution 2) The documentation that it has or that it can generate (e.g. via a risk assessment – see SP.03.01BR) to confirm that components have adequate security for their level of risk in the asset owner's automation solution 	<p>Examples of execution that the service provider has met the requirement at least for one customer for example:</p> <ol style="list-style-type: none"> 1) Project documentation 2) Interviews 	<ol style="list-style-type: none"> 1) Risk analysis procedure to identify critical components and their level of risk, or obtain them from the asset owner 2) One or more of the following: <ol style="list-style-type: none"> a) Evidence of existence for the component, such as security requirements, defence-in-depth designs b) Description of compensating counter measures used to bring the component to the adequate security for their risk level as applicable. 	<ol style="list-style-type: none"> 1) Security certificates or similar declarations of conformity that components have adequate security for their level of risk 2) Security testing results 3) Performed security assessments such as risk assessments, threat analysis or vulnerability assessments that indicate an acceptable risk for a component 	<ol style="list-style-type: none"> 1) KPI: Continuous improvement of security test results for components 2) Continuous risk mitigation related to components of automation solution 3) Continuous improvement of security of components as documented by related declarations of conformity

A	B	C	D	E	F	G	H
Summary Level	IEC 62443-2-4 ID	IEC 62443-2-4 requirement	Evaluation criteria	Examples for ML-1 conformance evidence (see 6.3)	Examples for ML-2 conformance evidence (see 6.4) EoE	Examples for additional ML-3 conformance evidence (see 6.5) EoE + PoE	Examples for additional ML-4 conformance evidence of continuous process improvement (see 6.6)
Assurance	SP.02.02 BR	<p>The service provider shall have the capability to recommend security analysis tools (e.g. network scanning tools) for use with the automation solution and:</p> <ol style="list-style-type: none"> 1) provide instructions on how to use them 2) identify any known adverse effects they can have on the automation solution's performance 3) provide recommendations for how to avoid adverse effects 	<p>The service provider shall have a process that can be performed for the asset owner:</p> <ol style="list-style-type: none"> 1) To identify security analysis tools that it has validated and are prepared to be used 2) To create and maintain the associated documentation that describes how to use them safely <p>The documentation shall include the points covered in points 1) to 3) of the requirement</p>	<p>Examples of execution that the service provider has met the requirement at least for one customer for example:</p> <ol style="list-style-type: none"> 1) Project documentation 2) Interviews 	<ol style="list-style-type: none"> 1) Process of recommending security analysis tools including the creation and maintenance of documentation for points 1) to 3) of the requirement 2) List of recommended security analysis tools for particular reference architecture 3) User manuals or references to online user manuals 4) Descriptions of potential adverse effects, including instructions for avoiding these adverse effects 	<ol style="list-style-type: none"> 1) A list of tools that the service provider has approved for use for an automation solution 2) Documentation including how identified adverse effects have been avoided 	<ol style="list-style-type: none"> 1) Maintenance and continuous update of the list of recommended security analysis tools, when applicable also based on experiences from identified adverse effects 2) List of recommended security analysis tools are always state of the art 3) KPI: No. and severity of occurred adverse effects

A	B	C	D	E	F	G	H
Summary Level	IEC 62443-2-4 ID	IEC 62443-2-4 requirement	Evaluation criteria	Examples for ML-1 conformance evidence (see 6.3)	Examples for ML-2 conformance evidence (see 6.4) EoE	Examples for additional ML-3 conformance evidence (see 6.5) EoE + PoE	Examples for additional ML-4 conformance evidence of continuous process improvement (see 6.6)
Assurance	SP.02.02 RE(1)	The service provider shall have the capability to ensure that it obtains approval from the asset owner prior to using security analysis tools (e.g. network scans) at the asset owner's site.	The service provider shall have a process that can be performed for the asset owner that security analysis tools are used only with asset owner approval	Examples of execution that the service provider has met the requirement at least for one customer for example: 1) Project documentation 2) Interviews	1) Documented process for obtaining asset owner's approval 2) Checklist for obtaining asset owner's approval used by this process 3) Approval template for the asset owner	1) Documented approval / agreement between service provider and asset owner for using security analysis tool at asset owner's site 2) Completed related checklists or templates 3) Tool approval by the asset owner	1) KPI: No. of tool usages without the prior approval of the asset owner

A	B	C	D	E	F	G	H
Summary Level	IEC 62443-2-4 ID	IEC 62443-2-4 requirement	Evaluation criteria	Examples for ML-1 conformance evidence (see 6.3)	Examples for ML-2 conformance evidence (see 6.4) EoE	Examples for additional ML-3 conformance evidence (see 6.5) EoE + PoE	Examples for additional ML-4 conformance evidence of continuous process improvement (see 6.6)
Assurance	SP.02.02 RE(2)	The service provider shall have the capability to schedule and use security analysis tools to discover undocumented or unauthorized systems or vulnerabilities in the automation solution. This capability shall include the ability to use these tools in accordance with the asset owner's standard operating procedures	<p>The service provider shall have a process that can be performed for the asset owner:</p> <ol style="list-style-type: none"> 1) To identify security analysis tools that can be used to discover hidden devices (IP addresses) 2) To identify the security analysis tools for identifying running applications (e.g. application finger print) 3) To ensure that these tools can be used only at times approved by the asset owner and in a way that is consistent with asset owner practices 	<p>Examples of execution that the service provider has met the requirement at least for one customer for example:</p> <ol style="list-style-type: none"> 1) Project documentation 2) Interviews 	<ol style="list-style-type: none"> 1) Documented process to identify security analysis tools that can be used to discover hidden devices and TCP/UDP ports 2) Process directing solution personnel to use these tools only at the times approved by the asset owner 3) Process directing solution personnel to ensure the use of these tools does not interfere with asset owner practices and standard operating procedures 	<ol style="list-style-type: none"> 1) Live demo of the security analysis tools during conformity assessment 2) Asset owner approval for compliance with its standard operating procedures 	<ol style="list-style-type: none"> 1) Continuous improvement of the recommended scanning tools with regard to having the most recent updates, and being generally accepted and tested against adverse effects. 2) Continuous improvement of the capabilities to run the tools consistently upon approval by the asset owner.

A	B	C	D	E	F	G	H
Summary Level	IEC 62443-2-4 ID	IEC 62443-2-4 requirement	Evaluation criteria	Examples for ML-1 conformance evidence (see 6.3)	Examples for ML-2 conformance evidence (see 6.4) EoE	Examples for additional ML-3 conformance evidence (see 6.5) EoE + PoE	Examples for additional ML-4 conformance evidence of continuous process improvement (see 6.6)
Assurance	SP.02.02 RE(3)	The service provider shall have the capability to ensure the control system components used in the automation solution have the ability to maintain operation of essential control system functions in the presence of system or network scans, or both, during normal operation	<p>1) The service provider shall have a process that can be performed for the asset owner for selecting and using control system components for solution or particular reference architecture which can withstand scanning by system or network scans</p> <p>2) The service provider shall specify which criteria applies for normal operation of the components in a solution or particular reference architecture</p>	<p>Examples of execution that the service provider has met the requirement at least for one customer for example:</p> <p>1) Project documentation</p> <p>2) Interviews</p>	<p>1) Defined normal operation / essential control system function for the related automation solution</p> <p>2) Process to implement technical test cases for verification to withstand scanning by system or network scans under normal operation</p>	<p>1) Security certificates or similar declarations for secure components, fuzz testing, communications robustness, etc.</p> <p>2) System or network scan test results as they relate to the component</p> <p>3) Applicable product supplier test results</p>	<p>1) KPI: Test results for control system components for robustness are verified periodically</p> <p>2) Continuous improvement on the methods to ensure robustness</p> <p>3) Improvement continuous monitoring of the test results</p> <p>4) Improvement on identifying and mitigation of vulnerabilities that might affect robustness</p> <p>5) Continuous improvement of ability to maintain operation as documented by related declarations of conformity</p>

A	B	C	D	E	F	G	H
Summary Level	IEC 62443-2-4 ID	IEC 62443-2-4 requirement	Evaluation criteria	Examples for ML-1 conformance evidence (see 6.3)	Examples for ML-2 conformance evidence (see 6.4) EoE	Examples for additional ML-3 conformance evidence (see 6.5) EoE + PoE	Examples for additional ML-4 conformance evidence of continuous process improvement (see 6.6)
Assurance	SP.02.03 BR	The service provider shall have the capability to provide documentation to the asset owner that describes how to harden the automation solution	The service provider shall have a process that can be performed for the asset owner to create and maintain hardening documentation for the automation solution, that is based on hardening documentation for the included control system / components	Examples of execution that service provider has met the requirement at least for one customer for example: 1) Project documentation 2) Interviews	Process which includes for instance one or more of the following: 1) Hardening guide 2) Reference defense-in-depth architecture with configuration instructions 3) Recommended component / system security configurations	Checking of hardening documentation as built for a project, including implementation of defense-in-depth configuration strategy (firewall rules, least privilege, least functionality, etc.)	1) KPI: Continuous improvement on attack surface reduction in hardening guide / reference architecture / recommended configurations
Assurance	SP.02.03 RE(1)	The service provider shall have the capability to verify that its security hardening guidelines and procedures are followed during automation solution related activities	The service provider shall have a process that can be performed for the asset owner to verify that its hardening guidelines are followed	Examples of execution that service provider has met the requirement at least for one customer for example: 1) Project documentation 2) Interviews	1) Procedures for validation completion of hardening activities for example during FAT / SAT 2) Verification checklist to be completed during hardening activities	1) Completed checklist about completed hardening activities 2) Hardening report	1) KPI: Completeness of performed hardening activities 2) KPI: Hardening issues reach the value "0" for a significant period of time. Examples of hardening issue are: – Undocumented identified TCP / UDP ports, unintended accessible services

A	B	C	D	E	F	G	H
Summary Level	IEC 62443-2-4 ID	IEC 62443-2-4 requirement	Evaluation criteria	Examples for ML-1 conformance evidence (see 6.3)	Examples for ML-2 conformance evidence (see 6.4) EoE	Examples for additional ML-3 conformance evidence (see 6.5) EoE + PoE	Examples for additional ML-4 conformance evidence of continuous process improvement (see 6.6)
Solution hardening	SP.03.01 BR	<p>The service provider shall have the capability to conduct a security risk assessment of the automation solution or contribute to (participate in) a security risk assessment conducted by the asset owner or its agent</p> <p>NOTE The asset owner can additionally require the service provider to document its assessment. The “Doc?” column is set to “No” because this is a requirement to have the capability to perform the assessment and not a requirement to provide documentation.</p>	<p>1) The service provider shall have a process that can be performed for the asset owner for conducting a risk assessment and defined triggers when to do so</p> <p>2) The service provider shall have personnel (employees, consultants, contractors subcontractors) capable of leading or actively participating in a risk assessment of the solution</p> <p>3) The service provider shall have a process that can be performed for the asset owner to obtain the risk parameters from the asset owner</p>	<p>Examples of execution that the service provider has met the requirement at least for one customer for example:</p> <p>1) Project documentation</p> <p>2) Interviews</p>	<p>1) Written procedures for conducting risk assessments including definition of risk, impact and level of acceptable risk including:</p> <ul style="list-style-type: none"> – training courses for risk assessment – written templates or appropriate tools for risk assessments <p>2) Process for using asset owner risk assessment methodologies</p> <p>3) Personnel with expertise in risk assessments: resumes, training records</p>	<p>1) Risk assessment report</p> <p>2) Documented cooperation with asset owner on risk assessment</p>	<p>1) Continuous improvements of risk assessment methodology</p> <p>2) Improvement of the expertise of staff related to risk assessment</p> <p>3) Positive feedbacks from asset owners on risk assessment co-operations</p>

A	B	C	D	E	F	G	H
Summary Level	IEC 62443-2-4 ID	IEC 62443-2-4 requirement	Evaluation criteria	Examples for ML-1 conformance evidence (see 6.3)	Examples for ML-2 conformance evidence (see 6.4) EoE	Examples for additional ML-3 conformance evidence (see 6.5) EoE + PoE	Examples for additional ML-4 conformance evidence of continuous process improvement (see 6.6)
			<p>Example of such risk parameters are:</p> <ul style="list-style-type: none"> – Possible financial damage on unavailability of the automation solution – Compromises of integrity and confidentiality of automation solution data – Breaches of regulatory requirements 				
Solution hardening	SP.03.01 RE(1)	The service provider shall inform the asset owner of the results of security risk assessments that it performs on the automation solution, including risk mitigation mechanisms and procedures.	<p>1) The service provider shall have a process that can be performed for the asset owner to report risk assessment results (including risk mitigation mechanisms / procedures and not mitigated residual risks) to the asset owner</p>	<p>Examples of execution that the service provider has met the requirement at least for one customer for example:</p> <ol style="list-style-type: none"> 1) Project documentation 2) Interviews 	<ol style="list-style-type: none"> 1) Process for reviewing and reporting risk assessments 2) Policies for using asset owner risk assessment methodologies 3) Training courses for risk assessment review and reporting 4) Templates for communication of risk assessment results 	<ol style="list-style-type: none"> 1) Reported risk assessment results for example: <ul style="list-style-type: none"> – Completed communication template 2) Documentation of risk mitigation mechanisms and procedures for asset owner 	<ol style="list-style-type: none"> 1) Positive feedbacks from asset owners on communication about risk assessment

A	B	C	D	E	F	G	H
Summary Level	IEC 62443-2-4 ID	IEC 62443-2-4 requirement	Evaluation criteria	Examples for ML-1 conformance evidence (see 6.3)	Examples for ML-2 conformance evidence (see 6.4) EoE	Examples for additional ML-3 conformance evidence (see 6.5) EoE + PoE	Examples for additional ML-4 conformance evidence of continuous process improvement (see 6.6)
Solution hardening	SP.03.01 RE(2)	The service provider shall have the capability to verify that security architecture reviews or security assessment or threat analysis of the control system used in the automation solution have been conducted by a third party	The service provider shall have a process that can be performed for the asset owner to verify to the asset owner that a security assessment / threat analysis was conducted by a third party on the control system used in the automation solution	Examples of execution that the service provider has met the requirement at least for one customer for example: 1) Project documentation 2) Interviews	1) Process for obtaining a third party assessment 2) Process to select third party 3) List of potential third parties	1) Third party assessment report / results	1) Continuously improved monitoring of third party performance

A	B	C	D	E	F	G	H
Summary Level	IEC 62443-2-4 ID	IEC 62443-2-4 requirement	Evaluation criteria	Examples for ML-1 conformance evidence (see 6.3)	Examples for ML-2 conformance evidence (see 6.4) EoE	Examples for additional ML-3 conformance evidence (see 6.5) EoE + PoE	Examples for additional ML-4 conformance evidence of continuous process improvement (see 6.6)
Network security	SP.03.02 BR	The service provider shall have the capability to ensure that the physical network segmentation architecture used in the automation solution, including its use of network security devices or equivalent mechanisms, is implemented according to the automation solution design approved by the asset owner	The service provider shall have a process that can be performed for the asset owner that approved network segmentation is implemented and verified according to the automation solution design approved by the asset owner	Examples of execution that the service provider has met the requirement at least for one customer for example: 1) Project documentation 2) Interviews	1) Process for the implementation of the approved network segmentation architecture and the configuration of its network security devices and related checklist 2) Security test cases that verify the network segmentation for example during FAT / SAT 3) Verification process / checklist to ensure that changes do not negatively impact the approved network segmentation	1) Network segmentation design / architecture, 2) Completed checklists / test records 3) As-built drawings of network segmentation	1) KPI: Network segmentation architectures meeting design requirement of the asset owner 2) Network security devices or equivalent mechanisms used in the network segmentation are always state of the art and are improved continuously 3) Continuous positive feedback from asset owner in accordance with network segment architecture with approved design for the automation solution 4) Feedback from project member personnel is continuously integrated into network segmentation architecture

A	B	C	D	E	F	G	H
Summary Level	IEC 62443-2-4 ID	IEC 62443-2-4 requirement	Evaluation criteria	Examples for ML-1 conformance evidence (see 6.3)	Examples for ML-2 conformance evidence (see 6.4) EoE	Examples for additional ML-3 conformance evidence (see 6.5) EoE + PoE	Examples for additional ML-4 conformance evidence of continuous process improvement (see 6.6)
Network security	SP.03.02 RE(1)	The service provider shall have the capability to identify and document the network segments of the automation solution and their interfaces to other segments, including external networks, and for each interface designate whether it is trusted or untrusted	<p>1) The service provider shall have a process that can be performed for the asset owner to identify and document the network segmentation architecture for the solution</p> <p>2) The service provider shall have a process that can be performed for the asset owner to identify interfaces as trusted or untrusted for example by risk assessments</p>	<p>Examples of execution that the service provider has met the requirement at least for one customer for example:</p> <p>1) Project documentation</p> <p>2) Interviews</p>	<p>1) Process identifies and documents network segments and the interfaces between them, including the criteria it uses for determining which interfaces of the solution are considered untrusted</p> <p>2) Reference architecture documentation and procedures / checklist for adapting it to the asset owner's automation solution</p> <p>3) Checklist for identification of network segments and interfaces, and for determination of trustworthiness of interfaces</p>	<p>1) Documentation of network segments including designation of trusted or untrusted</p> <p>2) As-built drawings of network segmentation</p>	<p>1) Continuous improvement of process to determine interfaces as trusted or untrusted</p> <p>2) Feedback from project member personnel is continuously integrated into network segmentation architecture for trusted or untrusted interfaces</p>

A	B	C	D	E	F	G	H
Summary Level	IEC 62443-2-4 ID	IEC 62443-2-4 requirement	Evaluation criteria	Examples for ML-1 conformance evidence (see 6.3)	Examples for ML-2 conformance evidence (see 6.4) EoE	Examples for additional ML-3 conformance evidence (see 6.5) EoE + PoE	Examples for additional ML-4 conformance evidence of continuous process improvement (see 6.6)
Network security	SP.03.02 RE(2)	<p>The service provider shall have the capability to ensure that interfaces of the Automation Solution that have been identified as untrusted are protected by network security devices or equivalent mechanisms, with documented and maintained security rules. At a minimum, the following shall be protected:</p> <ol style="list-style-type: none"> 1) External interfaces 2) Level 2 / Level 3 interfaces (see NOTE 2 below) 3) Interfaces between the BPCS and the SIS 4) Interfaces connecting wired and wireless BPCS networks 5) Interfaces connecting the BPCS to data warehouses (e.g. enterprise historians) 	<ol style="list-style-type: none"> 1) The service provider shall have a process that can be performed for the asset owner to conduct risk assessment to verify that identified untrusted network interfaces have adequate protection 2) The protection mechanisms for example air gapping or one way firewalls or firewall configurations shall be documented and their effectiveness shall be ensured 3) The process shall as a minimum ensure protection related to points 1) to 5) of the requirement 	<p>Examples of execution that the service provider has met the requirement at least for one customer for example:</p> <ol style="list-style-type: none"> 1) Project documentation 2) Interviews 	<ol style="list-style-type: none"> 1) Documented process for risk assessment to protect untrusted interfaces, at least covering the interfaces of points 1) to 5) of the requirement 2) Process for the implementation, configuration, and test of identified protection mechanisms 3) Template for security rules on used network security devices or equivalent mechanisms, or both, for example firewall configurations 4) Checklist used for implementation, configuration and test 	<ol style="list-style-type: none"> 1) Used protection mechanisms on untrusted interfaces as-built 2) Record on configuration and testing of these mechanisms 3) Documented security rules on used network security devices and/or equivalent mechanisms 	<ol style="list-style-type: none"> 1) The mechanisms used for protection of untrusted interfaces are reviewed and improved periodically 2) Maintenance and continuous improvement of suitable reference architectures 3) Both firewalls and configured rules are always state of the art and are improved continuously

A	B	C	D	E	F	G	H
Summary Level	IEC 62443-2-4 ID	IEC 62443-2-4 requirement	Evaluation criteria	Examples for ML-1 conformance evidence (see 6.3)	Examples for ML-2 conformance evidence (see 6.4) EoE	Examples for additional ML-3 conformance evidence (see 6.5) EoE + PoE	Examples for additional ML-4 conformance evidence of continuous process improvement (see 6.6)
		<p>NOTE 1 For some, responsibility for maintaining firewall rules and documentation transfers to the asset owner prior to or at automation solution turnover. In this case, the service provider's role can be, as required by the asset owner, only to support verification that the firewall rules are accurate and up-to-date.</p> <p>NOTE 2 Depending on the automation solution, Level 2 / Level 3 interfaces can be "External" interface.</p>	<p>NOTE The term "Level" in point 2) of the requirement refers to the position in the Purdue Reference Model as standardized by IEC 62264-1 (see 5.3).</p>				

A	B	C	D	E	F	G	H
Summary Level	IEC 62443-2-4 ID	IEC 62443-2-4 requirement	Evaluation criteria	Examples for ML-1 conformance evidence (see 6.3)	Examples for ML-2 conformance evidence (see 6.4) EoE	Examples for additional ML-3 conformance evidence (see 6.5) EoE + PoE	Examples for additional ML-4 conformance evidence of continuous process improvement (see 6.6)
Solution hardening	SP.03.03 BR	<p>The service provider shall have capabilities for handling vulnerabilities that affect the automation solution, including its related policies and procedures. These capabilities shall address:</p> <ol style="list-style-type: none"> 1) The handling of vulnerabilities newly discovered in the automation solution or in its related policies and procedures for which the service provider is responsible 2) The handling of publicly disclosed vulnerabilities affecting the automation solution 	<ol style="list-style-type: none"> 1) The service provider shall have a process that can be performed for the asset owner to describe its vulnerability handling process 2) The handling of newly discovered and publicly disclosed vulnerabilities shall be included 	<p>Examples of execution that service provider has met the requirement at least for one customer for example:</p> <ol style="list-style-type: none"> 1) Project documentation 2) Interviews 	<ol style="list-style-type: none"> 1) Process for vulnerability handling including who (by role / position) in the organization is responsible for handling them including defined evaluation if automation solution is affected 2) Monitoring process to identify publicly disclosed vulnerabilities that can affect the automation solution, including list of identified sources of information being monitored for example https://cve.mitre.org/cve/ 	<ol style="list-style-type: none"> 1) Reports on identified and handled vulnerabilities 2) Remediation solutions for vulnerabilities 	<ol style="list-style-type: none"> 1) KPI: Effectiveness of vulnerability handling mechanisms including reaction time

A	B	C	D	E	F	G	H
Summary Level	IEC 62443-2-4 ID	IEC 62443-2-4 requirement	Evaluation criteria	Examples for ML-1 conformance evidence (see 6.3)	Examples for ML-2 conformance evidence (see 6.4) EoE	Examples for additional ML-3 conformance evidence (see 6.5) EoE + PoE	Examples for additional ML-4 conformance evidence of continuous process improvement (see 6.6)
Network security	SP.03.03 RE(1)	The service provider shall have the capability to provide documentation to the asset owner that describes how to mitigate security weaknesses inherent in the design or implementation, or both, of communication protocols used in the automation solution that were known prior to automation solution integration or maintenance activities	<p>1) The service provider shall have a process that can be performed for the asset owner to reduce the impact of communications protocols that are vulnerable to attack or how it can protect them from being attacked</p> <p>2) The service provider shall have a process that can be performed for the asset owner to communicate the weaknesses and associated mitigation result with the asset owner</p>	<p>Examples of execution that service provider has met the requirement at least for one customer for example:</p> <p>1) Project documentation</p> <p>2) Interviews</p>	<p>1) Documented process on analysing and identifying weaknesses in communication protocols (e.g., by robustness tests), on mitigating those weaknesses and on documenting them</p> <p>2) Documented process on the communication with the asset owner related to communication protocol risks and weaknesses, including related recommendations for protection measures</p> <p>3) Robustness testing results and their mitigation for a reference architecture</p>	<p>1) Documentation as approved by the asset owner describing the implemented mitigations and weaknesses for the communication protocols</p> <p>2) Robustness testing results for a specific solution</p>	<p>1) Continuous positive feedback from asset owner about the quality of the documentation on the mitigation of the security weaknesses related to communication protocols</p>