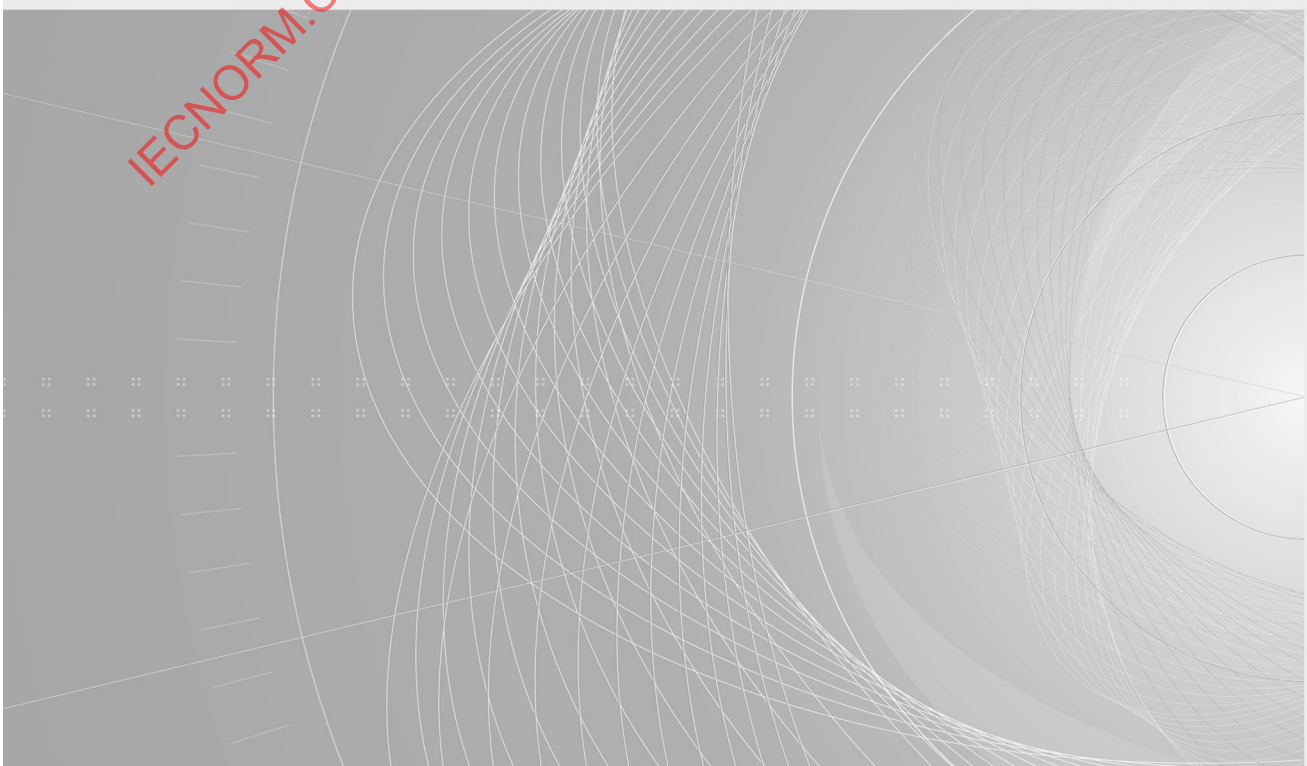
IEC TS 62443-6-1

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 62443-6-1:2024-03(en)

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

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

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

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

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 It also gives information on projects, replaced and withdrawn publications.

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

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

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

Electropedia - www.electropedia.org
The world's leading online dictionary on electrotechnology, containing more than 22 500 terminological entries in English and French, with equivalent terms in 25 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

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.

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	1) The service provider shall have a process that can be performed for the asset owner to inform and assign personnel to the automation solution 2) The process includes a verification/validation step that only informed personnel is assigned to 3) The training content shall include IEC 62443-2-4 topics 4) The service provider personnel shall accept their responsibility to comply with the security aspects that they have been informed about	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) Initial training materials / records of participation (i.e. first participants are trained), automated training logs 3) Security manual / handbook / policy or other documentation that are required reading for personnel prior to their assignment to the solution	1) List of all the staff involved in the project who have been security role-based trained 2) Solution staffing list matches with trained personnel at training record	1) KPI: Training coverage statistics 2) Periodical review of training contents 3) 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	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 2) The process includes a verification/validation step that only informed subcontractor or consultant personnel is assigned to 3) The training content shall include IEC 62443-2-4 topics 4) The service provider subcontractor or consultant personnel shall accept their responsibility to comply with the security aspects that they have been informed about	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) Initial training materials / records of participation (i.e. first participants are trained), automated training logs 3) Security manual / handbook / policy or other documentation that are required reading for personnel prior to their assignment to the solution	1) List of all the staff involved in the project who have been security role-based trained 2) Solution staffing list matches with trained personnel at training record	1) KPI: Training coverage statistics 2) Periodical review on training contents

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	The service provider shall have a process that can be performed for the asset owner to: 1) determine the asset owner's security requirements, policies and procedures, 2) make its personnel aware of their responsibilities to comply with these security requirements, policies and procedures, 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) Verification / validation step that these obtained requirements will be respected / followed by the personnel, for example checklist template for obtaining asset owner's requirements 3) Policy on subcontractors or subcontractor agreement template 4) Training materials / records /security manual / handbook or other documentation that are required reading for personnel prior to their assignment to the solution	1) Participant list / attestation of personnel for the asset owner required training about its responsibilities, policies and procedures 2) Asset owner agreement 3) Subcontractor agreement 4) Completed checklist for particular automation solution	1) The service provider agrees with asset owner(s) on a feedback channel on a continuous basis 2) The service provider demonstrates continuous improvements related to the feedback from asset owner(s) 3) 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 for changes involving devices, workstations, and servers and connections between them	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: 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: 1) Project documentation 2) Interviews	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.	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	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: 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: 1) Project documentation 2) Interviews	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	1) Background checks were performed according to the applicable legal framework and usual industry specific rules	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: 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: 1) Project documentation 2) Interviews	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	1) Background checks were performed according to the applicable legal framework and usual industry specific rules for subcontractor / consultants / representatives	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	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. 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.	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.	Examples of execution that the service provider has met the requirement at least for one customer for example: 1) Project documentation 2) Interviews	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)	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	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)**
		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. 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					

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	The service provider shall have a process that can be performed for the asset owner to inform the asset owner of changes to: 1) New personnel who need to get access to the solution 2) Personnel who no longer need access to the 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) Documented process for promptly notifying the asset owner about the change of personnel 2) Documented process agreed with the asset owner of which personnel changes require notification 3) Form / template for personnel change notification	1) Completed form for personnel change notification 2) Central repository of personnel with access to the automation solution, for example ticketing system 3) Secure e-mail notifications 4) Agreed organigram with the asset owner 5) Documented communication to the asset owner about new personal trainings conducted	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	The service provider shall have a process that can be performed for the asset owner to identify: 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	Examples of execution that the service provider has met the requirement at least for one customer for example: 1) Project documentation 2) Interviews	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: 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.	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	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	The service provider shall have the capability to recommend security analysis tools (e.g. network scanning tools) for use with the automation solution and: 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	The service provider shall have a process that can be performed for the asset owner: 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 The documentation shall include the points covered in points 1) to 3) of the 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) 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	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	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	The service provider shall have a process that can be performed for the asset owner: 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	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 to identify security analysis tools that can be used to for example 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	1) Live demo of the security analysis tools during conformity assessment 2) Asset owner approval for compliance with its standard operating procedures	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	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 2) The service provider shall specify which criteria applies for normal operation of the components in a solution or particular reference architecture	Examples of execution that the service provider has met the requirement at least for one customer for example: 1) Project documentation 2) Interviews	1) Defined normal operation / essential control system function for the related automation solution 2) Process to implement technical test cases for verification to withstand scanning by system or network scans under normal operation	1) Security certificates or similar declarations for secure components, fuzz testing, communications robustness, etc. 2) System or network scan test results as they relate to the component 3) Applicable product supplier test results	1) KPI: Test results for control system components for robustness are verified periodically 2) Continuous improvement on the methods to ensure robustness 3) Improvement continuous monitoring of the test results 4) Improvement on identifying and mitigation of vulnerabilities that might affect robustness 5) Continuous improvement of ability to maintain operation 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.02.03 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	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 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.	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 2) The service provider shall have personnel (employees, consultants, contractors subcontractors) capable of leading or actively participating in a risk assessment of the solution 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	Examples of execution that the service provider has met the requirement at least for one customer for example: 1) Project documentation 2) Interviews	1) Written procedures for conducting risk assessments including definition of risk, impact and level of acceptable risk including: – training courses for risk assessment – written templates or appropriate tools for risk assessments 2) Process for using asset owner risk assessment methodologies 3) Personnel with expertise in risk assessments: resumes, training records	1) Risk assessment report 2) Documented cooperation with asset owner on risk assessment	1) Continuous improvements of risk assessment methodology 2) Improvement of the expertise of staff related to risk assessment 3) Positive feedbacks from asset owners on risk assessment co-operations

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)**
			Example of such risk parameters are: – 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.	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	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 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	1) Reported risk assessment results for example: – Completed communication template 2) Documentation of risk mitigation mechanisms and procedures for asset owner	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	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 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	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 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 2) Reference architecture documentation and procedures / checklist for adapting it to the asset owner's automation solution 3) Checklist for identification of network segments and interfaces, and for determination of trustworthiness of interfaces	1) Documentation of network segments including interfaces and designation of trusted or untrusted 2) As-built drawings of network segmentation	1) Continuous improvement of process to determine interfaces as trusted or untrusted 2) Feedback from project member personnel is continuously integrated into network segmentation architecture for trusted or untrusted interfaces

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)	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: 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)	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	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 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	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	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)**
		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. NOTE 2 Depending on the automation solution, Level 2 / Level 3 interfaces can be "External" interface.	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).				

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	The service provider shall have capabilities for handling vulnerabilities that affect the automation solution, including its related policies and procedures. These capabilities shall address: 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	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	Examples of execution that service provider has met the requirement at least for one customer for example: 1) Project documentation 2) Interviews	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/	1) Reports on identified and handled vulnerabilities 2) Remediation solutions for vulnerabilities	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	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 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	Examples of execution that service provider has met the requirement at least for one customer for example: 1) Project documentation 2) Interviews	1) Documented process on analysing and identifying weaknesses in communication protocols (e.g., by robustness tests), on mitigating those weaknesses and on documenting them 2) Documented process on the communication with the asset owner related to communication protocol risks and weaknesses, including related recommendations for protection measures 3) Robustness testing results and their mitigation for a reference architecture	1) Documentation as approved by the asset owner describing the implemented mitigations and weaknesses for the communication protocols 2) Robustness testing results for a specific solution	1) Continuous positive feedback from asset owner about the quality of the documentation on the mitigation of the security weaknesses related to communication protocols

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.03.04 BR	The service provider shall have the capability to ensure that time distribution / synchronization for the automation solution is performed from a secure and accurate source that uses a protocol that is commonly accepted by both the security and industrial automation communities	For the solution or used reference architecture the service provider shall: 1) describe that time synchronization is performed from a reliable source, 2) identify the time distribution protocol used, 3) show that it is commonly accepted by the security and industrial automation communities	Examples of execution that the service provider has met the requirement at least for one customer for example: 1) Project documentation 2) Interviews	1) Description or diagram, or both that illustrate(s) the security of the time source 2) Identification of the recommended time distribution protocol and explanation of its reliability 3) Procedure for selecting and approving time distribution protocol 4) Evidence (articles, papers, studies) showing that the protocol is commonly accepted and current, and not obsolete or unacceptable	1) Documentation and test record of the used time distribution / synchronization 2) Documentation of approval of the used time distribution / synchronization by communities or asset owner	1) Up to date usage and integration of commonly accepted protocol over a period of time 2) KPI: No. of timing-related issues in deployed solutions
Solution hardening	SP.03.05 BR	The service provider shall have the capability to ensure that only software and hardware features required by the automation solution or approved by the asset owner are enabled in the automation solution. At a minimum, this includes ensuring that:	The service provider shall have a process that can be performed for the asset owner: 1) To reduce the attack surface of components / devices used in the solution at least according to the points 1) to 5) of the 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 that verifies / validates the implementation of the least functionality principle 2) Hardening guidelines including least functionality of points 1), 3) and 4) of the requirement and related installation software / procedures 3) Documented process to obtain approval of network addresses	1) Test record that unnecessary software applications and services, USB ports, USB devices etc. are disabled 2) Authorization of network addresses by asset owner	1) The service provider demonstrates continuous improvements related to the attack surface reduction of the points 1) to 5) of the requirement related to the used components / systems

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)**
		1) unnecessary software applications and services (e.g. email, office applications, games) and their associated communication access points (e.g. TCP / UDP ports), USB devices (e.g. mass storage), Bluetooth and wireless communications are disabled or removed unless required by the automation solution, 2) network addresses in use are authorized, 3) physical and logical access to diagnostic and configuration ports is protected from unauthorized access and use,	2) To ensure that the initial reduction of the attack surface is not weakened during maintenance procedures		4) Documented process for retaining the hardening state during and after maintenance 5) Maintenance manual	3) Installation records like logs / reports that reflect the reduced attack surface 4) Records showing that required functions enabled for maintenance activities were disabled after maintenance to ensure initial reduction of attack surface	2) KPI: No. of cases of unnecessary software applications, ports and services identified by asset owner or third parties

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)**
		4) unused ports on network devices (e.g. switches and routers) are configured to prevent unauthorized access to the automation solution's network infrastructure, 5) maintenance processes maintain the hardened state of the automation solution during its lifetime					

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.03.05 RE(1)	The service provider's hardening guidelines and procedures shall ensure that only necessary, authorized, and documented digital certificates for certificate authorities (CAs) are installed.	The service provider shall have a process that can be performed for the asset owner that: 1) digital certificates pre-installed or installed automatically by the component are removed if they are not necessary, 2) digital certificates are removed when they are no longer used by the solution, 3) only necessary, authorized and documented digital certificates are permitted to be installed	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 that identifies needed (CA) certificates 2) Documented process that require and verifies removal of unused digital (CA) certificates 3) Documented process to use protection against or prevent installation of unnecessary certificates 4) Checklist for verification	1) Documented needed (CA) certificates 2) Validation activity result that unused digital certificate have been removed from the automation solution prior to or during installation	1) KPI: No. of cases of unnecessary, unauthorized or undocumented (CA) certificates identified by asset owner or third parties

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.03.06 BR	The service provider shall have the capability to support the use of session locking for automation solution workstations as required by the asset owner. This requirement applies only to the workstations for which the service provider is responsible. Session locking: 1) prevents information on the logged on user's display device from being viewed, and 2) blocks input from the user's input device (e.g. keyboard, mouse) until unlocked by the session user or an administrator NOTE Locking the user input device means that the user at the workstation is not able to use the keyboard except for unlocking the keyboard.	For the solution or used reference architecture the service provider shall have a process that can be performed for the asset owner to describe its session locking mechanism or equivalent and how to use it. If the session locking mechanism is provided by the operating system, then the service provider needs only to specify which operating system is used and that it provides session locking	Examples of execution that the service provider has met the requirement at least for one customer for example: 1) Project documentation 2) Interviews	1) Checklist that workstations used in automation solution have session locking mechanism 2) Description of the session locking mechanism (or compensating controls) and how to use it (this may be used by web applications or other applications to which a user connects) 3) Operating system reference to session locking capability	1) Record of session locking validation 2) Log / record of session locking enforcement by operating system configuration	1) KPI: No. of cases of missing or non-implemented session locking mechanisms identified by asset owner or third parties 2) Continuous positive feedback from asset owner about the session locking implementation for workstations in the responsibility of the service provider

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.03.07 BR	The service provider shall have the capability to ensure that wired and wireless workstations, including handhelds, used for maintenance and engineering of wired and wireless control / instrumentation devices do not circumvent the: 1) automation solution's access controls for these devices, 2) network security safeguards (e.g. network security devices) at the automation solution's boundary with Level 3 NOTE 1 Direct access to these devices by handhelds that bypass access controls of the automation solution is prohibited. NOTE 2 Direct access by a handheld to a wireless device in Level 3 that bypasses the Level 2 / 3 network security device is prohibited.	1) For the solution or used reference architecture the service provider shall have a process that can be performed for the asset owner to describe the access control mechanisms of workstations and handhelds used for maintenance and engineering. 2) The service provider shall particularly make sure that these mechanisms prevent unauthorized access to the control devices by workstations and handhelds.	Examples of execution that the service provider has met the requirement at least for one customer for example: 1) Project documentation 2) Interviews	1) Reference architecture drawings / descriptions that identify access paths or controls, or both, that enforce specified access paths 2) Documented process to verify restriction of access paths, so that access paths are blocked which would circumvent the access control 3) Documents (e.g. design documents, user manuals, installation manuals, hardening guide, etc) that describe how engineering and maintenance workstations are able to access the control system or its components, or both, and are not able to bypass user access controls of the solution	1) Test records / reports related to performed verification activities for access control 2) Application of documents outlined for ML-2 within projects	1) KPI: No of circumvented access controls of automation solutions 2) KPI: No. of circumvented network security safeguards of automation solutions

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.03.07 RE(1)	The service provider shall have the capability to support the use of multi-factor authentication for automation solution workstations as required by the asset owner. This requirement applies only to the workstations for which the service provider is responsible	For the solution or used reference architecture the service provider shall have a process that can be performed for the asset owner to describe its process for applying / integrating / configuring multifactor authentication according to the requirements of asset owners	Examples of execution that the service provider has met the requirement at least for one customer for example: 1) Project documentation 2) Interviews	1) Description of the multi-factor authentication mechanism and how it is used 2) Operating system reference to multi-factor authentication feature 3) Checklist that records configuration of multi-factor authentication for workstations	1) Verification of application of multi factor authentication in project 2) Asset owner approvals of multi factor authentication mechanisms including key management	1) Continuous positive feedback from asset owner about the multifactor authentication for workstations in the responsibility of the service provider
Network security	SP.03.08 BR	The service provider shall have the capability to ensure that the least privilege is used for the administration of network devices for which the service provider is responsible	The service provider shall have a process that can be performed for the asset owner to: 1) identify the mechanisms used to enforce the least privilege (e.g. role-based access controls) in network devices 2) configure and validate the least privilege for the administration of network devices	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 that describes the usage and validation of least-privilege for the administration of network devices 2) Description of validated least-privilege mechanisms 3) Documented application concept for network device least-privilege mechanisms 4) Validation checklist for least-privilege mechanisms	1) Documentation of application of least-privilege concepts in projects 2) Implementation and test record for example role-based access controls 3) Completed validation checklist for least-privilege mechanisms for a project	1) KPI: No. of identified violations of least privilege in projects (target = 0 over a certain period of 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.03.08 RE(1)	The service provider shall have the capability to ensure that access controls used for the administration of network devices and wireless networks include role-based access controls. NOTE Normally network devices are only accessed by administrators so only a single role for them will be defined. However, if the asset owner's operating procedures allow access to the network devices by administrators and others, then multiple roles can be defined.	For the solution or used reference architecture the service provider shall have a process that can be performed for the asset owner: 1) To support role-based access controls for network devices and wireless networks 2) To configure, validate, verify and test network devices and wireless networks to use role-based access control as required	Examples of execution that the service provider has met the requirement at least for one customer for example: 1) Project documentation 2) Interviews	1) Documentation and checklists / templates that describe the implementation and verification of role-based access control for the administration of network devices and wireless networks	1) Completed templates or checklists on the application of role-based access control in projects 2) Records of configuration, verification, validation and testing of role-based access control of network devices and wireless networks according to the documented process	1) KPI: No. of identified issues related to roles-based access control in projects (target = 0 over a certain period of time) 2) FAT / SAT task approvals or continuous positive feedback, or both, from asset owner about the configuration and verification of role-based access control for network devices and wireless networks in the responsibility of the service provider

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.03.08 RE(2)	The service provider shall have the capability to ensure that encryption is used to protect data, whether in transit or at rest, that is used in the administration of network device (e.g. passwords, configuration data) that is identified as data requiring safeguarding (see SP.03.10 BR and its REs). NOTE See SP.03.10 RE(3) for cryptographic requirements.	For the solution or used reference architecture the service provider shall have a process that can be performed for the asset owner to: 1) identify the cryptographic mechanisms used to protect data used in the administration of network devices, 2) protect sensitive data in transit or at rest; for example to use cryptographic hashes to protect passwords NOTE If cryptographic mechanisms are not supported by the components, the service provider will describe compensating controls that are used to protect the data.	Examples of execution that the service provider has met the requirement at least for one customer for example: 1) Project documentation 2) Interviews	1) Template that identifies the types of data used for administration of network devices (e.g. credentials, config data identified as sensitive data) to be protected and the cryptographic mechanisms used to protect them 2) Procedures / templates / checklists for the use of cryptographic mechanisms to protect data used for the administration of network devices	1) Documentation on identified types of data requiring safeguarding and the applied protection mechanisms in a project 2) Documentation of implementation (e.g. screenshots) of cryptographic mechanisms to protect these data (e.g. passwords) in a project	1) The cryptographic mechanisms used are always state of the art over a period of time 2) Continuous improvement of the applied protection mechanisms for example: – more efficiency by automation – timely updates of the mechanisms used for protection

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.03.08 RE(3)	The service provider shall have the capability to ensure that access controls used for the administration of network devices include mutual authentication	For the solution or used reference architecture, the service provider shall have a process that can be performed for the asset owner to: 1) apply mutual authentication mechanisms for administration of the network devices, 2) configure, validate, verify and test its mutual authentication mechanisms NOTE If this mechanism is provided by the operating system or an application, such as a web server via HTTPS, then the service provider will specify which operating system / application is used, that it provides mutual authentication, and if provided by HTTPS or TLS, how the certificates for the server are generated and installed.	Examples of execution that the service provider has met the requirement at least for one customer for example: 1) Project documentation 2) Interviews	1) Description of the mutual authentication mechanism and how it is used, for example https / tls / ssh or similar technologies 2) Validation activity, for example checklist that records configuration of mutual authentication for administration of network devices 3) Documented concept of the application of mutual authentication features provided by operating system / applications	1) Documentation of application of mutual authentication mechanisms in a project, for example use of techniques like challenge / response, user password / device certificate, and Kerberos (IETF RFC 1510), etc. 2) Validation records of their correctness and effectiveness in the solution	1) The mutual authentication mechanisms used are always state of the art over a period of time 2) Continuous improvement of the applied mutual authentication mechanisms for example: – more efficiency by automation – timely updates of the mechanisms used for access control

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)**
Data protection	SP.03.09 BR	The service provider shall have the capability to ensure that the automation solution is configured to verify that all control actions and data flows in the automation solution (e.g. between workstations and controllers), including configuration changes, are: 1) valid, 2) initiated or approved by an authorized user, and 3) transferred over an approved connection in the approved direction	For the solution or used reference architecture the service provider shall have a process that can be performed for the asset owner describing that data and commands are properly validated, authorized and transferred in a protected manner over approved connections in the approved directions. This process shall include configuration, verification and testing for: 1) Account authentication 2) Account authorization 3) Integrity of commands and / or data 4) Access control at network or application layer 5) Data flows only occurring over approved connections in the approved directions	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 procedure to identify and verify commands / data flows and their validity, authorizations, compliance and approved directions 2) Documented procedure that verify that control actions and data flows of the automation solution implement: a) verification of control actions and data flows for example DMZ, data diodes b) verification of user authorization for that action c) verification that the action is received from the right source	Test records of application of the documented procedure for example that the identified data flows have been protected according to ML2 evidence 2a), 2b), and 2c)	1) KPI: No of identified control actions and data flows violating points 1) to 3) of the requirement (target = 0 over a certain period of time) 2) Positive FAT / SAT deviation reviews related to control actions and data flows over a period of time 3) Continuous improvement on the method of the related verification procedures for example related to automations, efficiency

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)**
Data protection	SP.03.10 BR	The service provider shall have the capability to ensure that data storage points and data flows within the automation solution that require safeguarding, as defined or approved by the asset owner, are documented, including the security requirements for their safeguarding (e.g. confidentiality, integrity).	The service provider shall have a process that can be performed for the asset owner to: 1) identify data requiring safeguarding inherent to the automation solution or associated reference architecture, or both, 2) identify the asset owner's data requiring safeguarding, 3) determine the security requirements for the data requiring safeguarding, and 4) obtain related asset owner's 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 identifying / obtaining asset owner's data and defining their security requirements 2) Documented process to create and maintain automation solution / reference architecture documentation that identifies its data requiring safeguarding, and defines their security requirements 3) Related checklist used by the process	1) Documentation of identified data requiring safeguarding and their protection mechanisms in a project 2) Documentation of related communication with asset owner on the definition or approval, or both 3) Completed related checklist used by the process	1) Continuous positive feedback from asset owner about documentation and protection of data requiring safeguarding 2) Continuous improvement on the method of the related documentation and protection of data requiring safeguarding procedures, for example related to automations, efficiency 3) KPI: No. of identified compromises of confidentiality, integrity of data requiring safeguarding (target = 0 over a certain period of 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)**
Data protection	SP.03.10 RE(1)	The service provider shall have the capability to ensure that data within the automation solution requiring safeguarding, as described in SP 03.10 BR, is protected from unauthorized disclosure or modification, whether at rest or in transit	For the automation solution or used reference architecture the service provider shall have a process that can be performed for the asset owner to protect data requiring safeguarding against disclosure or modification (confidentiality or integrity)	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 describing the protection mechanisms used in the automation solution or reference architecture to ensure confidentiality and integrity of data at rest and data in transit 2) Documented mechanisms for configuring and verifying the automation solution or reference architecture to protect confidentiality and integrity of data requiring safeguarding 3) Related checklist used by the process	1) Documentation of applied data protection mechanisms and their verification of implementation in a project 2) Completed related checklist used by the process	1) KPI: No. of identified unauthorized disclosures or modifications of data requiring safeguarding (target = 0 over a certain period of time) 2) The applied mechanisms for confidentiality and integrity protection are all state of the art over a period of time, particularly related to the applied cryptography

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)**
Data protection	SP.03.10 RE(2)	The service provider shall have the capability to provide documentation to the asset owner that describes the retention capabilities provided by the automation solution for storing / archiving sensitive data. This documentation includes capacities, pruning and purging functions, retention timeouts, etc	The service provider shall have a process that can be performed for the asset owner to: 1) create and maintain documentation on the data retention capabilities of the solution that can be used to store / archive sensitive data, 2) make sure that this documentation includes capacities, pruning and purging functions, retention timeouts, etc., 3) provide this documentation to 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) Documented process for creating the documentation of data retention capabilities and for transferring it to the asset owner 2) Documentation of resources (capacities / data volumes) and of functionalities for storing and maintaining data, including pruning and purging functions, retention timeouts, etc. 3) Process to keep documentation up-to-date and to keep the asset owner informed about the latest document	1) Documentation provided to an asset owner describing data retention capabilities including used capacity, pruning and purging functions or retention timeouts	1) Continuous positive feedback from asset owner about documentation and handover process of data retention capabilities 2) Increased level of detail or improved structure of the documentation about data retention capabilities and its functionality 3) Continuously improved process to keep documentation up-to-date

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)**
Data protection	SP.03.10 RE(3)	The service provider shall have the capability to ensure that the cryptographic mechanisms used in the automation solution, including algorithms and key management / distribution / protection, are commonly accepted by both the security and industrial automation communities	For the solution or used reference architecture the service provider shall have a process that can be performed for the asset owner to be able to: 1) identify the cryptographic mechanisms used in the automation solution or that can be configured, 2) show that they are commonly accepted and not self-developed or obscure or obsolete or compromised or insecure.	Examples of execution that the service provider has met the requirement at least for one customer for example: 1) Project documentation 2) Interviews	1) Description / diagrams of where cryptographic mechanisms are used, and their identity, such as a) operating system software, that contain built-in cryptographic mechanisms b) open source cryptographic mechanisms embedded into the automation solution 2) Process to ensure that cryptographic mechanisms used in the automation solution are accepted by the industry as current and not obsolete or unacceptable	1) Documentation of used implementations of cryptographic mechanisms in a project 2) Provided evidence (e.g. articles in trustworthy media, scientific papers, studies, security institutions like NIST) showing the implementation of the cryptographic mechanisms as current and not obsolete or unacceptable	1) Zero outdated cryptographic mechanisms in the components of automation solutions over a period of time 2) Regular review of the acceptance of cryptographic mechanisms integrated in automation solutions over the lifecycle 3) Systematic and comprehensive review of the state of the art of cryptographic mechanisms

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)**
Data protection	SP.03.10 RE(4)	The service provider shall have the capability to ensure that when it removes a component from the automation solution, that all data in the component requiring safeguarding, as described in SP 03.10 BR, is permanently destroyed / deleted.	The service provider shall have a process that can be performed for the asset owner to permanently destroy all data requiring safeguarding from the devices / components that it removes from service	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 that verifies / validates that sensitive data in devices / components that are removed from the automation solution are permanently destroyed 2) Checklist used by the process to verify permanent destruction of sensitive data after uninstallation of component from the automation solution	1) Completed checklist stating decommissioned component and destruction of data 2) Documentation of applied mechanisms for data clearance and destruction of memory in a project	1) Continuous improvement of the mechanisms to validate and test the deletion of sensitive data in components being removed from an automation solution 2) Continuous automation and improvement of the efficiency of the mechanisms applied for data deletion
Wireless	SP.04.01 BR	The service provider shall have the capability to ensure that its automation solution architecture documentation describing wireless systems is current in its description of the following. 1) Data exchange between a Level 1 network and wireless instrumentation 2) Data exchange between a Level 2 network and a Level 3 network through a secure wireless link	The service provider shall have a process that can be performed for the asset owner to describe: 1) its process to document the architecture of its wireless networks and data flows according to topics 1) and 2) of the requirement, and to keep the documentation current,	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 the installation / maintenance of wireless systems and their configured security mechanisms 2) Documented process to ensure that the architecture documentation of the wireless networks is kept current, for example addition / deletion of devices	Evidence that related processes and documentation have been applied in projects for example: 1) Architectures 2) Flow diagrams 3) Security design 4) Network design	1) Systematic and comprehensive review of the state of the art of architecture documentation describing wireless systems over a significant period of time 2) Continuous improvement of the zones and conduits concepts used in the architecture documentation associated with wireless access to wired devices / workstations in the Automation Solution

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)**
		3) Security mechanisms that prevent an intruder from gaining access to the Automation Solution using the wireless system 4) Security mechanisms that restrict access within the Automation Solution by workers with handheld wireless devices 5) Where required, security mechanisms that provide protection for remote management of wireless systems NOTE The term "Level" refers to the position in the Purdue Reference Model as standardized by IEC 62264-1 (see 5.3).	2) its implemented security mechanisms to prevent intrusion or bypass of specified access restrictions to the Automation Solution via wireless devices, according to topics 3) to 5) of the requirement		3) Documentation of the security mechanism to prevent bypass of specified access restrictions to the Automation Solution, for example wireless bridges, wireless handhelds 4) Checklists for documenting new installations and changes related to points 1) to 5) of the requirement		

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)**
Wireless	SP.04.02 BR	The service provider shall have the capability to ensure that access to wireless devices is protected by authentication and access control mechanisms that are commonly accepted by both the security and industrial automation communities	For the solution or used reference architecture the service provider shall have a process that can be performed for the asset owner to be able to: 1) ensure that authentication and access control mechanisms are used to protect its wireless devices, 2) show that the applied mechanisms are commonly accepted and strong according to the state of the art	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 procedures that include configuration and verification for the applied authentication and access control technology 2) Process to ensure that authentication and access control mechanisms used for wireless devices in the automation solution are accepted by the industry as current and not weak or unacceptable	1) Documentation of applied commonly accepted authentication and access control mechanisms to wireless devices in a project 2) Documentation of successful verification that applied authentication and access control mechanisms are commonly accepted according to the state of the art in a project	1) Regular review of the acceptance of authentication and access control mechanisms integrated in automation solutions over the lifecycle 2) Systematic and comprehensive review of the state of the art of authentication and access control mechanisms

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)**
Wireless	SP.04.02 RE(1)	The service provider shall have the capability to ensure that wireless communications are protected by cryptographic mechanisms that are commonly accepted by both the security and industrial automation communities	For the solution or used reference architecture the service provider shall have a process that can be performed for the asset owner: 1) to configure, validate, verify and test cryptographic mechanisms to protect its wireless devices, 2) show that these cryptographic mechanisms are commonly accepted	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 procedures that include configuration and verification for the cryptographic mechanisms used to protect communications 2) Process to ensure that cryptographic mechanisms used for wireless devices (e.g. wireless bridges, wireless handhelds, used protocols) in the automation solution are accepted by the industry as current and not weak or unacceptable	1) Documentation of used implementations of cryptographic mechanisms for wireless communication in a project 2) Provided evidence (e.g. articles in trustworthy media, scientific papers, studies, security institutions like NIST) showing the implementation of the cryptographic mechanisms for wireless communications as current and not obsolete or unacceptable	1) Zero outdated cryptographic mechanisms for wireless communication in the components of automation solutions over a period of time 2) Regular review of the acceptance of cryptographic mechanisms for wireless communication integrated in automation solutions over the lifecycle 3) Systematic and comprehensive review of the state of the art of cryptographic mechanisms for wireless communication

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)**
Wireless	SP.04.03 BR	The service provider shall have the capability to ensure that wireless protocols used in the automation solution are compliant with standards commonly used within the industrial security community and with applicable regulations	For the solution or used reference architecture the service provider shall have a process that can be performed for the asset owner to be able to: 1) ensure that wireless protocols and their configured security mechanisms are compliant with commonly accepted standards, 2) ensure that the wireless protocols used are compliant with applicable local regulations	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 to select, configure and apply wireless protocols 2) Documented process to test, verify and validate compliance of the wireless protocols with applicable standard and local regulations 3) Template for wireless protocols showing compliance with commonly used standards and regulations	1) Provided evidence (e.g. articles in trustworthy media, scientific papers, studies, security institutions like NIST) showing used wireless protocols were according to standards used in the OT security community and with applicable regulations 2) Documentation list of used wireless protocols implemented in an automation solution and related verifications of compliance 3) Completed template for wireless protocols showing compliance with commonly used standards and regulations	1) Continuous improvement of the process to verify compliance of wireless protocols with standards and regulations for example: - optimization of the verification process like automation and acceleration - improved mechanisms to detect deviations or to apply related corrections, or both

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)**
Wireless	SP.04.03 RE(1)	The service provider shall have the capability to ensure that unique, automation solution-specific identifiers are used for wireless networks and that all wireless identifiers are descriptive acronyms that are not obviously associated with the asset owner's site.	The service provider shall have a process that can be performed for the asset owner to make sure that its rules for naming wireless network identifiers provide unique identifiers and prevent an easy identification of the associated site or function	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 / checklists / templates for creating wireless identifiers (the rules for the value of the identifiers and the process for creating them) 2) Documented process of review of identifiers with the asset owner	1) Completed checklists / templates for creating wireless identifiers 2) Records or protocols on the cooperation activities with asset owners related to wireless identifiers	1) KPI: No. of issues related to wireless network identifiers for example duplicated / disclosing SSIDs (target = 0 over a certain period of time)) 2) Continuous positive feedback from asset owner about cooperation related to wireless identifiers
Wireless	SP.04.03 RE(2)	The service provider shall ensure that the automation solution's wireless devices that have IP addresses use static addressing and have dynamic address assignment mechanisms (e.g. DHCP) disabled.	For the solution or used reference architecture the service provider shall have a process that can be performed for the asset owner: 1) for assigning static IP addresses to wireless devices, 2) to disable dynamic IP addressing	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 verifying that IP addresses to wireless devices assigned are static 2) Checklists / template of assigned IP addresses of wireless devices 3) Documented process to check that dynamic address assignment is disabled	1) Completed checklists / template of assigned IP addresses of wireless devices 2) Verification records showing that dynamic address assignment is disabled	1) Continuous improvement of the process to verify allocation of addresses for wireless devices 2) KPI: No. of identified dynamically allocated IP addresses for wireless devices (target = 0 over a certain period of 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)**
SIS	SP.05.01 BR	The service provider shall have the capability to verify that security architecture reviews or security risk assessments of the communications of the SIS used in the automation solution have been conducted and addressed.	The service provider shall have a process that can be performed for the asset owner that communication of SIS is considered and addressed during risk assessment and security architecture reviews	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 that can include checklists and have a verification step that communication of SIS is addressed during risk assessment 2) Template of SIS communications / data flows and checklist of related risk assessment	1) Record on security architecture review including SIS 2) Risk assessment report including SIS communication review	1) Continuous improvement on the detection and mitigation of security risks related to SIS communications in automation solution 2) Improvement of the expertise of staff related to risk assessment
SIS	SP.05.02 BR	The service provider shall have the capability to ensure that SIS safety communications and SIS safety functions are protected from the BPCS or any other automation solution communications NOTE This requirement does not require that communications not critical to safety functions between the SIS and the BPCS (e.g. configuration downloads, status monitoring, logging) be shielded from other Automation Solution communications.	For the solution or used reference architecture the service provider shall have a process that can be performed for the asset owner to make sure that SIS safety-critical communications: 1) are protected from other communications, 2) are not subject to interference by non-safety critical communications	Examples of execution that service provider has met the requirement at least for one customer for example: 1) Project documentation 2) Interviews	1) Design / architecture documents that describe segmentation between the SIS and other communications 2) SIS certification that addresses this security requirement 3) Checklists / templates for verifying that SIS safety-critical communications are protected from other communications	1) Completed checklists / templates for verifying that SIS safety-critical communications are protected from other communications 2) Documentation of applied network architecture with separation and protection of SIS	1) Continuous improvement of network architectures and protection concepts for SIS safety communication / functions 2) KPI: No. of critical safety functions / communication being impacted by interfering other communications (target = 0 over a certain period of 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)**
SIS	SP.05.03 BR	The service provider shall have the capability to ensure that communications external to the automation solution, including remote access communications, are not able to interfere with the operation of the SIS.	For the solution or used reference architecture the service provider shall have a process that can be performed for the asset owner to describe the protection of SIS functions from interference: 1) by communications originating and / or terminating external to the automation solution, 2) by remote access communications	Examples of execution that the service provider has met the requirement at least for one customer for example: 1) Project documentation 2) Interviews	1) Design / architecture documents that show how SIS operations are protected from interference from external communications, including which external communications are not to be allowed 2) SIS certification that addresses this requirement 3) Checklists / templates that prohibit configurations that allow external communications from interfering with SIS operations.	1) Completed design / architecture documents 2) Completed checklists / templates 3) Evidence of non-interference in operation, for example penetration or command flooding test results showing non-interference	1) Continuous improvement of network architectures for protection of SIS against interference by external communications / remote access communications 2) KPI: No. of interferences of SIS by external communications (target = 0 over a certain period of 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)**
SIS	SP.05.04 BR	The service provider shall have the capability to ensure that applications, (e.g. control system applications) external to the SIS are not able to participate in or disrupt or otherwise interfere with SIS communications that are critical to safety functions	For the solution or used reference architecture the service provider shall have a process that can be performed for the asset owner to protect SIS safety-critical communications, for example from external applications NOTE SP.05.03 BR addresses protecting SIS operations and this requirement addresses protecting SIS communications.	Examples of execution that the service provider has met the requirement at least for one customer for example: 1) Project documentation 2) Interviews	1) Design / architecture documents that describe logical or physical segmentation, or both, between the SIS and the BPCS 2) SIS certification that addresses this requirement, 3) Checklists / templates for verifying that SIS safety-critical communications cannot be impacted by SIS-external applications	1) Completed design / architecture documents 2) Completed checklists / templates 3) Evidence of non-participation and non-disruption in operation, for example penetration or command flooding test results showing non-participation and non-disruption	1) Continuous improvement of protection of SIS-communications against SIS-external applications 2) KPI: No. of interferences of SIS communications by SIS-external applications (target = 0 over a certain period of 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)**
SIS	SP.05.05 BR	The service provider shall have the capability to ensure that SIS EWSs that reside outside the SIS (external to SIS interface with the control system) cannot be compromised by communications from Level 3 or above. NOTE The term "Level" refers to the position in the Purdue Reference Model as standardized by IEC 62264-1 (see 5.3)	For the solution or used reference architecture the service provider shall have a process and mechanisms that can be performed for the asset owner to make sure that SIS EWSs which are external to the SIS are protected through a network security device or equivalent mechanisms against communications to / from devices / workstations form Level 3 and above.	Examples of execution that the service provider has met the requirement at least for one customer for example: 1) Project documentation 2) Interviews	1) Design / architecture documents showing that: – Level 2 and Level 3 are segmented using a network security device, that there are no unauthorized communications paths around it that show the SIS EWS in Level 2 2) Design / architecture documents that show how SIS EWSs external to SIS are protected from unauthorized communications from Level 3 and Level 4 devices / workstations 3) Checklists / templates that verify the design / architecture ensuring that all communications between the SIS engineering workstation and Level 3 (and above) applications pass through a network security device	1) Completed design / architecture documents 2) Completed checklists / template 3) Documentation of the network security device (including applied protection rules) which has been used in an automation solution or reference architecture to ensure the protection of communication from Level 3 and above 4) Evidence of EWS effective separation from architecture Level 3 and above, for example demonstrated by penetration test results	1) Continuous improvement of protection of SIS EWSs against interfering communications from Level 3 and above 2) KPI: No. of identified compromises of SIS EWSs by interfering communications from Level 3 and above (target = 0 over a certain period of 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)**
SIS	SP.05.05 RE(1)	The service provider shall have the capability to ensure that the automation solution's SIS EWS that reside within the SIS (internal to SIS interface with the control system) cannot be compromised by remote access (e.g. RDP)	For the solution or used reference architecture, the service provider shall have a process that can be performed for the asset owner to make sure that the SIS EWSs that are internal to the SIS are protected from compromise by remote access communications	Examples of execution that the service provider has met the requirement at least for one customer for example: 1) Project documentation 2) Interviews	1) Design / architecture documents showing that remote access paths to internal SIS EWSs are blocked or disabled or restricted 2) Process / architecture documents showing that remote access has to be disabled (not accessible) or restricted 3) Risk assessment methodology addressing the risks of SIS EWSs being compromised by remote access to the SIS EWSs	1) Completed design / architecture documents 2) Documentation showing that remote access has been disabled for SIS EWSs in a project 3) Results / reports of related risk assessment in a project 4) Evidence of EWS effective separation from remote architecture, for example demonstrated by penetration test and port discovery results	1) Continuous improvement of protection of SIS EWSs against exploitation via remote access connections 2) KPI: No. of identified compromises of SIS EWSs by exploitation of remote access connections (target = 0 over a certain period of 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)**
SIS	SP.05.06 BR	The service provider shall have the capability to ensure that all access to the automation solution's SIS from outside the SIS is mediated and authorized at the interface to the SIS	For the solution or used reference architecture, the service provider shall have a process that can be performed for the asset owner to make sure that all connections to the SIS are mediated (e.g. via a firewall, gateway, or something similar)	Examples of execution that the service provider has met the requirement at least for one customer for example: 1) Project documentation 2) Interviews	1) Design / architecture documents showing the mediating component, for example gateway 2) Checklists / templates for installation, configuration, or maintenance of the mediating component 3) Documentation showing that SIS is physically connected only to SIS EWSs	1) Completed design / architecture documents 2) Completed checklists / templates 3) Documentation showing that SIS was only physically connected to SIS EWSs in a project or automation solution 4) Evidence of correct access and block of functions from outside the SIS, for example demonstrated by penetration test results from non-EWS addresses	1) Continuous improvement of mediation and authorization solution for the access to the SIS 2) KPI: No. of identified unauthorized accesses to SIS (target = 0 over a certain period of 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)**
SIS	SP.05.07 BR	The service provider shall have the capability to ensure that SIS functions performed by the automation solution's SIS EWS are protected from compromise by other SIS EWS software	For the solution or used reference architecture, the service provider shall have a process that can be performed for the asset owner to protect the SIS EWS safety software from other software running in the SIS EWS (least functionality concept)	Examples of execution that the service provider has met the requirement at least for one customer for example: 1) Project documentation 2) Interviews	1) Design documents that show that the SIS EWS is configured to perform only SIS functions 2) Descriptions of mechanisms that prohibit the SIS EWS from being configured to perform non-SIS functions 3) Checklists / templates that prohibit the SIS EWS from being configured to perform non-SIS functions 4) Descriptions of mechanisms that isolate and protect SIS EWS software from other software running in the SIS EWS	1) Specifications of SIS EWSs used in a project, including their least functionality concept 2) Completed checklists / template 3) Documentation of applied mechanisms that isolate and protect SIS EWS software from other software running in the SIS EWS 4) Evidence of effective prevention of malware or unauthorized software on the EWS, for example by test of effective mechanism such as whitelist controls or EWS hardening	1) Continuous improvement and update of specifications against other SIS EWSs software that could intentionally or inadvertently cause harm to the SIS 2) Continuous improvement of mechanisms for isolation and protection of SIS EWS software from other software running in the SIS EWS 3) KPI: No. of identified compromises of SIS EWSs by other SIS EWSs software (target = 0 over a certain period of 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)**
SIS	SP.05.08 BR	The service provider shall have the capability to verify that unauthorized wireless devices are not used as an integral part of SIS safety functions	The service provider shall have a process that can be performed for the asset owner to prevent unauthorized wireless devices from participating in SIS safety functions	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 to document the design showing that unauthorized wireless devices are not permitted in the operation of SIS functions 2) Description of mechanisms to identify and authorize wireless devices for SIS safety functions 3) Checklists / templates that prohibit unauthorized wireless devices from being used as part of SIS functions in the guideline	1) Documentation of application of mechanisms to identify and authorize wireless devices for SIS functions in a project 2) Documentation of applied protection concept for SIS safety functions against unauthorized wireless devices 3) Completed checklists / template	1) Continuous improvement and update of mechanisms for identification and authorization of the access of wireless devices to SIS safety functions 2) Continuous improvement of protection concept for SIS safety functions against unauthorized wireless devices

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)**
SIS	SP.05.09 BR	The service provider shall have the capability to ensure that the SIS configuration mode can be enabled and disabled. While disabled, this interface shall prohibit the SIS from being configured NOTE This interface will typically prevent configuration messages from being delivered to the SIS.	For the solution or used reference architecture, the service provider shall have a process that can be performed for the asset owner to make sure that its SIS interface can be locked to prevent SIS from being configured.	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 and documentation describing how to lock the SIS interface 2) Checklists / templates for ensuring that once SIS interface is locked, the configuration mode is disabled 3) Documentation of mechanism used to prevent SIS from being configured in disabled mode	1) Documentation of application of mechanisms to lock / unlock the SIS configuration interface in a project 2) Documentation of application of protection concepts against unintended / unauthorized configurations in disabled mode (e.g software-controlled locks) 3) Completed checklists / template	1) Continuous improvement and update of mechanisms to enable and disable SIS configuration 2) Ensuring that protection concepts, for example software controlled locks are always state of the art over a period of 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)**
SIS	SP.05.09 RE(1)	The service provider shall have the capability to provide a hardware implementation of the configuration mode interface required by SP.05.09 BR and to ensure that this hardware implementation is capable of being physically locked while configuration mode is disabled	For the solution or used reference architecture, the service provider shall have a process that can be performed for the asset owner that its SIS interface can be locked by a physical switch or equivalent physical mechanism to prevent SIS from being configured in disabled mode	Examples of execution that the service provider has met the requirement at least for one customer for example: 1) Project documentation 2) Interviews	1) User documentation that describes hardware implementation to lock the SIS interface to prevent configuration changes from being made in disabled mode 2) Process and documentation describing how to use the physical locking mechanism used to prevent unintended configuration changes at the SIS interface 3) Checklists / templates for locking / disabling hardware configuration mode	1) Documentation of application of mechanisms to physically lock / unlock the SIS configuration interface in a project 2) Documentation of application of protection concepts against unintended / unauthorized configurations in disabled mode by physical key switches 3) Completed checklists / template	1) Continuous improvement and update of physical locking mechanisms to enable and disable SIS configuration 2) Ensuring that protection concepts using physical key switches are always state of the art over a period of 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)**
SIS	SP.05.09 RE(2)	The service provider shall have the capability to have an independent third party verify that it is not possible to change the configuration of the SIS when the hardware interface described in SP.05.09 RE(1) is locked in the "disable" configuration mode	The service provider shall have a process that can be performed for the asset owner to appoint and cooperate with independent third parties to verify its configuration mode locking mechanism	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 having independent third parties to verify that the locking mechanism operates as intended 2) Documentation of certification process performed by independent third party for this requirement	1) Application of third party verification process in a project 2) Audit reports or certifications from independent third party	1) Positive feedback from independent third party about the cooperation on the verification of configuration locking mechanisms 2) KPI: No of identified unintended configuration changes of the SIS in disabled mode (target = 0 over a certain period of 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)**
Configura-tion manage-ment	SP.06.01 BR	The service provider shall have the capability to provide accurate logical and physical infrastructure drawings / documentation of the automation solution, including its network devices, internal interfaces, and external interfaces. The documentation and drawings shall be maintained as an accurate representation of the automation solution. 1) Documented process for baseline design documentation including physical infrastructure drawings; also considering versioning during commissioning and maintenance stages	The service provider shall have a process that can be performed for the asset owner to generate, deliver, and maintain drawings / descriptions of the solution's network infrastructure that clearly identifies internal and external interfaces to which devices can be connected (e.g. switches, routers, firewalls, network interface cards)	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 on the generation, delivery, and maintenance of the network architecture representing the automation solution, including physical and logical network infrastructure 2) Checklists / templates to ensure the correctness and completeness of the physical / logical infrastructure drawings of the automation solution	1) Application of the documentation of the network architecture of a specific automation solution 2) Completed checklists / template 3) Detailed network architecture drawings including interfaces, addresses and segmentations by zones and conduits	1) Systematic and comprehensive review of the state of the art of architecture documentation over a significant period of time 2) Continuous improvement of the zones and conduits concepts used in the architecture documentation in the automation solution 3) KPI: Accuracy and completeness of the infrastructure drawings / network architecture documentation. Target: No. of missing elements (e.g. interfaces) or errors in the architecture drawings=0 over a certain period of 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)**
Configura-tion manage-ment	SP.06.01 RE(1)	The service provider shall have the capability to keep the as-built and installed equipment connection and configuration documents current	The service provider shall have a process that can be performed for the asset owner to make sure that the architecture drawings, connection diagrams, and configuration file (as-built) documentation always reflect the current operational equipment and their network connections	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 which ensures that configuration of all equipment and network connections – as built and installed – is documented and kept current 2) Related checklists / templates	1) Documentation that connection and configuration documents were updated according to related changes in the automation solution 2) Completed checklists / templates	1) Continuous improvement of the applied updating process to keep the documentation current, for example: – more efficiency by automation, – timeliness of updates of the documentation according to the related changes in the automation solution

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)**
Configura-tion manage-ment	SP.06.02 BR	The service provider shall have the capability to create and maintain an inventory register, including version numbers and serial numbers, of all devices and their software components in the automation solution for which the service provider is responsible	The service provider shall have a process that can be performed for the asset owner to make sure that all installed equipment and the software (if any) that runs on them are documented as required by 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 to establish and maintain an inventory register and keep it current including version numbers and serial numbers of all devices and software components 2) Checklists / template of inventory register	1) Inventory register used in a project 2) Completed checklists / templates	1) KPI: Accuracy and completeness of the inventory register. Target: No. of missing inventory information (e.g. version numbers or serial numbers) or errors in the inventory register =0 over a certain period of time 2) Continuous improvement of the establishment of the inventory register, for example: – more efficiency of the establishment by automation, – cooperation between inventory register and patch management particularly to use the inventory to check which components have to be patched, – timeliness of patching based on information from the inventory

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)**
Configura-tion manage-ment	SP.06.03 BR	The service provider shall have the capability to verify that wired and wireless devices used for control and instrumentation have been configured correctly with their approved values	The service provider shall have a process that can be performed for the asset owner to make sure that field devices retrieve correct configuration parameters with approved values downloaded / written to the device	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 used for verification of field device configuration 2) Related checklists / templates	1) Applied process verification of field device configuration in a project 2) Completed checklists / templates	1) KPI: No. of unauthorized or erroneous configuration changes in wired / wireless devices (target = 0 over a certain period of time) 2) Continuous improvement of concepts to ensure integrity of device configurations, for example – efficiency of cooperation with related workstation, – automation of verification of configuration values

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)**
Remote access	SP.07.01 BR	The service provider shall have the capability to ensure that all remote access applications used in the automation solution are commonly accepted by both the security and industrial automation communities	The service provider shall have a process that can be performed for the asset owner: 1) To identify remote access applications that it has approved for use in its solutions 2) To systematically select and approve them 3) To verify that they are commonly accepted	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 to identity the remote access applications that it is prepared to use in solutions 2) Documented process to verify that selected and planned remote access applications are commonly accepted by both the security and industrial automation communities	1) Documentation of applied remote access applications (e.g. RDP) in a project and their security verifications 2) Provided evidence (e.g. articles in trustworthy media, scientific papers, studies, security institutions like NIST) showing that only state of the art security mechanisms are used in the remote access applications	1) Zero outdated remote access applications in automation solutions over a period of time 2) Regular review of the acceptance of remote access applications used in automation solutions over the lifecycle 3) Systematic and comprehensive review of the state of the art of remote access applications

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)**
Remote access	SP.07.02 BR	The service provider shall have the capability to provide detailed instructions for the installation, configuration, operation, and termination of the remote access applications used in the automation solution	For each remote access application in the solution or reference architecture, the service provider shall have a process that can be performed for the asset owner for providing / referencing a user manual that includes the description to install / configure, operate, and terminate the remote access application	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 to create, maintain and provide the appropriate documentation 2) Documented process to provide instructions to the asset owner on the termination of remote access connections 3) Related checklists / templates	1) Documentation of installed and configured remote access connections in a project according to the related process 2) Documentation of cooperation with asset owners on the installation and configuration of remote access applications 3) Completed checklists / templates	1) Positive feedback from asset owners on cooperation about remote access applications 2) Systematic and comprehensive review of reaching a state of the art level of protection to the automation solution provided by remote access applications (e.g. by applied risk analysis and related verifications)

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)**
Remote access	SP.07.03 BR	The service provider shall have the capability to provide information about all proposed remote access connections to the asset owner that includes, for each connection: 1) its purpose, 2) the remote access application to be used, 3) how the connection will be established (e.g. via the Internet through a VPN), and 4) the location and identity of the remote client	The service provider shall have a process that can be performed for the asset owner to identify and describe each remote access connection proposed for the Solution covering all points of the 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 to list all proposed remote access connections to the asset owner containing information as stated in the requirement 2) Related checklists / template of all proposed remote access connections including points 1) to 4) of the requirement	1) Documentation of installed and configured remote access connection at asset owner's site 2) Completed checklists / templates	1) Continuous and Positive feedback from asset owners on cooperation about remote access connections
Remote access	SP.07.04 BR	The service provider shall have the capability to ensure that it obtains approval from the asset owner prior to using each and every remote access connection	The service provider shall have a process that can be performed for the asset owner to make sure that each remote access connection proposed for the solution is 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) Documented process to obtain asset owner's approval prior to the use of remote access connections 2) Related checklists 3) Template for approval about remote access connection by asset owner	1) Completed checklists 2) Signed templates by asset owners	1) Continuous and Positive feedback from asset owners on approval process related to remote access connections

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)**
Remote access	SP.07.04 RE(1)	The service provider shall have the capability to ensure that all remote access connections conducted over the Internet or over other publicly accessible media that are used to support remote access to the automation solution by the service provider (e.g. from a service provider facility) are authenticated and encrypted,.	The service provider shall have a process that can be performed for the asset owner to make sure that each remote access connection using public communication networks is authenticated and encrypted	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 assurance that remote access connections that use public communications networks are authenticated and encrypted 2) Related checklists / templates 3) Documented process to select suitable authentication and encryption mechanisms for remote access	1) Documentation of application of authentication and encryption mechanisms for remote access connections in a project, for example lists of related applied mechanisms 2) Completed checklists / template	1) Systematic and comprehensive review of the state of the art of authentication and encryption mechanisms used for remote access connections

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)**
Event manage-ment	SP.08.01 BR	The service provider shall have capabilities for handling cyber-security incidents that affect the automation solution that include: 1) detecting cyber-security compromises and incidents, 2) reporting cyber-security incidents to the asset owner, 3) responding to cyber-security compromises and incidents, including supporting an incident response team. NOTE 1 Logging of security-related events is addressed by SP.08.02 BR. NOTE 2 Logging and reporting of alarms and events is addressed by SP.08.03 BR.	The service provider shall have a process that can be performed for the asset owner to describe its: 1) incident handling process, 2) criteria for analysis of incidents and resulting / applied actions, particularly for those incidents that could adversely affect the automation solution, 3) reporting of incidents to the asset owner, 4) supporting of an incident response team.	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 defining criteria to manage security incidents and to filter and prioritize a security incident, for example reaction / response time 2) Documented process that describes how it detects, reports, and responds to cyber-security incidents and compromises 3) Description of how its response to cyber-security incidents and compromises supports an incident response team 4) Checklists and related actions to be performed in case of a security incident	1) Successful and comprehensive dry run of incident management process 2) Documentation of handled security incidents in an automation solution according to related process 3) Completed checklists	1) Successful handling and closing of security incidents over a period of time 2) Continuous and positive feedback from asset owners on cooperation on security incidents 3) Continuous improvement of the applied incident handling mechanisms, for example: – more efficiency by automation, – transparency of incident handling activities for the asset owners, – shorter reaction / response 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)**
Event manage-ment	SP.08.01 RE(1)	The service provider shall have the capability to ensure that security compromises that have been automatically detected can be reported through a communications interface that is accessible to the asset owner and that is commonly accepted by both the security and industrial automation communities	For the solution or used reference architecture, the service provider shall have a process that can be performed for the asset owner to identify and verify: 1) communications interfaces that can be used to report automatically detected security compromises to the asset owner, 2) agreed procedures with the asset owners on how to use them, 3) that they are commonly accepted	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 on the communication interface with the asset owner, which also describes how these interfaces can be used by the asset owner to obtain information about the security incidents 2) Documented process to verify that planned communication interfaces are commonly accepted and current, and not obsolete or unacceptable (e.g. based on state of the art SIEM solutions)	1) List of communications interfaces that were used for automatically detected compromises 2) Provided evidence (e.g. articles in trustworthy media, scientific papers, studies) showing that applied communication interfaces are commonly accepted and current, and not obsolete or unacceptable	1) Regular review of the quality and acceptance of the communication interface solution used for the incident reporting over the period of time 2) Systematic and comprehensive review of the state of the art of communication interface solution 3) Continuous and positive feedback from asset owners on the accessibility of the communication interface and the related cooperation with the service provider

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)**
Event manage-ment	SP.08.02 BR	The service provider shall have the capability to ensure that the automation solution is configured to write all security-related events, including user activities and account management activities, to an audit log that is kept for the number of days specified by the asset owner,. NOTE Logging and reporting of process-related events, such as setpoint changes and other operational / configuration data changes, is addressed by SP.08.03 BR.	For the solution or used reference architecture the service provider shall have a process that can be performed for the asset owner to: 1) identify all security-related events 2) write them to audit logs 3) configure their retention capabilities as specified 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) Documented process for identifying security-related events and the audit logs to which they will be written 2) Checklists / templates to verify the related configuration of automation solutions 3) Documented process and criteria to select audit logging solutions	1) Audit logs which have been created / compiled in automation solutions according to the related process 2) Completed checklists / template 3) Completed forensics analysis based on audit logs	1) Continuous verification of effectiveness of configuration of automation solution to detect and log all security related events 2) Continuous and positive feedback from the asset owner on the applied audit logging solutions

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)**
Event manage-ment	SP.08.02 RE(1)	The service provider shall have the capability to ensure that security-related data and events can be accessed through one or more interfaces that are commonly accepted by both the security and industrial automation communities	For the solution or used reference architecture the service provider shall have a process that can be performed for the asset owner to: 1) identify the interfaces supported by the automation solution that particularly asset owners can use to obtain security-related data and events, 2) show that they are commonly accepted	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: – selection of access interfaces for security related data and events, – verification that the interfaces are commonly accepted and current, and not obsolete or unacceptable 2) Checklists / templates to ensure that security-related data and events can be accessed	1) Provided evidence of acceptable interfaces (e.g. articles in trustworthy media, scientific papers, studies) showing that they are commonly accepted and current, and not obsolete or unacceptable 2) Completed checklists / templates	1) Regular review of the quality and acceptance of the interfaces solution used for event logging and reporting over the period of time 2) Systematic and comprehensive review of the state of the art of the related interface solution

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)**
Event manage-ment	SP.08.02 RE(2)	The service provider shall have the capability to verify that, using a simulated security-related event approved by the asset owner, security-related events can be written to an audit log	The service provider shall have a process that can be performed for the asset owner to simulate a security event and to write security related data to an audit log according to a scenario selected by an 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) Documented process to verify that simulated security-related event / data is written in an audit log 2) Training process for simulating a security-event and writing security data to an audit log according to requirements of an asset owner	1) Documentation of performed related simulations approved by asset owner in a project 2) Completed related trainings	1) Continuous improvement of the related simulation process, for example: – more efficiency by automation, – cooperation with the asset owner on the related simulation process, – accuracy of simulation to reflect event logging mechanisms in operational automation solutions 2) Continuous and positive feedback from the asset owner on the applied simulations

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)**
Event manage-ment	SP.08.03 BR	The service provider shall have the capability to ensure that the automation solution is configured to log and notify the operator of process-related events as required by the asset owner. The types of events include state changes / operating condition changes / configuration changes that can be due to manual or automated (those without human intervention) operation. NOTE Logging of security-related events is addressed by SP.08.02 BR.	For the solution or used reference architecture, the service provider shall have a process that can be performed for the asset owner to configure process-related events to be logged and notified to the operator according to the details of the 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) Training process for configuring process-related events to be logged and reported to the operator 2) Checklists / templates for the used technology	1) Completed related training 2) Event log files and documentation of reporting used in a project 3) Completed checklists / templates	1) Continuous and positive feedback from the operator and the asset owner on the event reporting and alarm notification solution 2) KPI: Percentage of process-related events which have been reported to operators according to the requirements of the asset owner (target = 100 % over a certain period of 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)**
Event manage-ment	SP.08.03 RE(1)	The service provider shall have the capability to ensure that alarms / alerts / events can be securely reported through an interface that is commonly accepted by both the security and industrial automation communities	For the solution or used reference architecture, the service provider shall have a process that can be performed for the asset owner to: 1) verify that alarms / alerts / events can be reported via secure interfaces supported by the automation solution, 2) show that these are commonly accepted.	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 risk assessment procedure to ensure that all relevant alarms / alerts / events requiring safeguarding are protected in transfer via a secure reporting interface 2) Documented process and criteria to verify effectiveness of safeguarding 3) Documented process showing that the reporting interface is commonly accepted and current, and not obsolete or unacceptable	1) Provided evidence on the security of applied reporting interfaces (e.g. articles in trustworthy media, scientific papers, studies) showing that they are commonly accepted and current, and not obsolete or unacceptable 2) Related risk assessment report	1) Regular review of the quality and acceptance of the security of the reporting interfaces used for event logging and reporting over a period of time 2) Systematic and comprehensive review of the state of the art of the related reporting interface solution

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)**
Event manage-ment	SP.08.04 BR	The service provider shall have the capability to document the automation solution's ability to withstand the near-simultaneous occurrence of large numbers of events, typically referred to as event storms	For the solution or used reference architecture, the service provider shall have a process that can be performed for the asset owner to verify and document that an automation solution is able to withstand event storms	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 of conducting tests (e.g. robustness test, stress test) at an automation solution to verify that it withstands event storms 2) Evaluation concept / procedure for architectural features (including rate-limiting network devices) of an automation solution with regard to their capabilities to protect against event storms 3) Risk assessment procedure that considers event storms and includes proper protection	1) Related test report / results / certification for particular automation solution 2) Related risk assessment report for particular automation solution	1) Continuous improvement of applied testing methodology for the robustness of automation solutions against event storms

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)**
Account manage-ment	SP.09.01 BR	The service provider shall have the capability to ensure that the automation solution supports: 1) the use of a single, integrated data base, which may be distributed or redundant, for defining and managing user and service accounts, 2) restricted management of accounts to authorized users, 3) decentralized access to this data base for the management of accounts, 4) decentralized enforcement of the account settings (e.g. passwords, operating system privileges, and access control lists) defined in this data base	For the solution or used reference architecture, the service provider shall have a process that can be performed for the asset owner to ensure that account management supports the points 1) to 4) of the 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 to select account management application(s) satisfying points 1) to 4) of the requirement (e.g. LDAP product) 2) Documentation of evaluation criteria related to 1) to 4) of the requirement for account management applications in the automation solution	1) Applied and verified account management applications in an automation solution	1) Continuous improvement of the related applied account management applications, for example: – more efficiency by centralization of account management functions 2) Simplifications of account management by administrators 3) Efficiency and automation of evaluation method of account management solutions

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)**
Account manage-ment	SP.09.02 BR	The service provider shall have the capability to ensure that unique accounts can be created and maintained for users	For the solution or used reference architecture, the service provider shall have a process that can be performed for the asset owner for creating and maintaining a unique user account for each automation solution user	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 to select unique user accounts for each user of an automation solution 2) Documentation of evaluation criteria to verify that unique user accounts are provided in an automation solution	1) Applied account management with unique user accounts for each user of an automation solution	1) KPI: No. of users for which no unique account is provided (only shared account available – target = 0 over a certain period of time)
Account manage-ment	SP.09.02 RE(1)	The service provider shall provide documentation to the asset owner that: 1) identifies all default user and service accounts, 2) describes the tools and procedures used to set / reset passwords for all default user and service accounts	The service provider shall have a process that can be performed for the asset owner for generating a list of all user and service accounts and providing instructions to the asset owner that describes how to change their passwords	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 on: – the identification of default accounts, – on the tools and procedures to set / reset password, – on the relate reporting to the asset owner 2) Cooperation procedures with asset owners to ensure that there are no hidden accounts nor are there passwords that cannot be changed	1) Documentation of related application for a solution: – list of users on all devices, – reference to description to set / reset password, – description to set / reset passwords	1) Continuous and positive feedback from the asset owners on documentation of user and service accounts

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)**
Account manage-ment	SP.09.02 RE(2)	The service provider shall have the capability to ensure that if an account / password is automatically generated for a user, other than operators and service groups, both the generated account and password are unique	For the solution or used reference architecture, the service provider shall have a process that can be performed for the asset owner to ensure the automatic generation of unique passwords for users, other than operators and service groups	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 of selection of related account management application(s) 2) Documented process to ensure that the account management solution does not generate the same password for two different users and that each generated user account is unique and has a unique identifier	1) Documentation of accepted and applied account management application(s) in an automation solution	1) KPI: No. of identified cases where same password is generated for multiple user accounts (target = 0 over a certain period of time)
Account manage-ment	SP.09.02 RE(3)	The service provider shall have the capability to ensure that service, auto-login and operator accounts, and other accounts required for essential functions and / or continuous operations, or as required by the asset owner have been configured so that they never expire nor become disabled automatically	For the solution or used reference architectureThe service provider shall have a process that can be performed for the asset owner to prevent these essential accounts from expiring or automatic disabling	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 to ensure that essential permanent accounts in the automation solution are configured to not expire or become automatically disabled or deleted. 2) Related checklists / templates for accounts and their lifetime and their retention procedures 3) Related documented verification / validation step for the implementation / configuration	1) Documentation of verification / validation record on identified accounts 2) Completed checklists / templates	1) KPI: No. of identified essential accounts which have expired or being deleted unintendedly (target = 0 over a certain period of 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)**
Account manage-ment	SP.09.02 RE(4)	The service provider shall have the capability to ensure that the built-in administrator account is disabled, and if that is not possible, that it is renamed or otherwise made difficult to exploit	The service provider shall have a process that can be performed for the asset owner to disable the administrator account or otherwise protect it from exploitation	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 ensuring the protection of administrator account against unauthorized use or exploitation 2) Related checklists / templates 3) Related documented verification / validation steps that built-in administrator accounts are disabled if possible	1) Documentation of applied verification / validation in a project that administrator accounts were disabled or protected against exploitation 2) Completed checklists / templates	1) Continuous improvement of the protection concept related to the administrator account over a period of time 2) KPI: No. of identified cases of attackers gaining administrative privileges using the built-in administrator account (target = 0 over a certain period of time)
Account manage-ment	SP.09.03 BR	The service provider shall have the capability to ensure that unused system default accounts have been removed or disabled,.	The service provider shall have a process that can be performed for the asset owner to identify and remove / disable the unused system default accounts	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 on the identification and disabling / removing of unused system default accounts 2) Related checklists / templates / trainings 3) Related documented verification / validation steps that unused system default accounts are removed or disabled	1) Documentation of applied verification / validation in a project that unused system default accounts were identified and disabled / removed 2) Completed checklists / templates / trainings	1) Continuous improvement of the applied removal / disabling mechanisms, for example: – more efficiency by automation 2) KPI: No. of identified cases of attackers gaining access to the automation solution through unused system default accounts (target = 0 over a certain period of 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)**
Account manage-ment	SP.09.04 BR	The service provider shall have the capability to ensure that all user accounts are removed once they are no longer needed. This includes: 1) temporary accounts under the control of the service provider, such as those used for integration or maintenance, 2) user accounts for service provider personnel who are no longer assigned to the automation solution (see SP.01.07 BR for notifying the asset owner of the removal of service provider personnel from the automation solution	The service provider shall have a process that can be performed for the asset owner to identify and remove / disable the user accounts that are no longer needed	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 on the identification and disabling / removing of user accounts that are no longer needed 2) Related checklists / templates / trainings 3) Related documented verification / validation steps for the removal of user accounts that are no longer needed	1) Documentation of applied verification / validation in a project for the removal of user accounts that are no longer needed 2) Completed checklists / templates / trainings	1) Continuous improvement of the applied removal / disabling mechanisms, for example: – more efficiency by automation 2) KPI: No. of identified cases of attackers gaining access to the automation solution through outdated user accounts (target = 0 over a certain period of 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)**
Account manage-ment	SP.09.04 RE(1)	The service provider shall have the capability to generate an audit log report after the completion of integration / maintenance activities that shows that accounts used to support these activities have been removed from the automation solution if they are no longer needed	The service provider shall have a process that can be performed for the asset owner to generate audit log that contains the entries for the removed user accounts that are no longer needed	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 generating audit logs 2) Related checklists / templates 3) Documented process for patching of an automation solution	1) Generated log file for entries recording the removal of accounts 2) Completed checklists / templates of removed integration / maintenance accounts 3) Related patch report	1) Continuous improvement of the applied removal / disabling mechanisms, for example: – more efficiency by automation 2) KPI: No. of identified cases of attackers gaining access to the automation solution through outdated integration / maintenance accounts (target = 0 over a certain period of 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)**
Account manage-ment	SP.09.05 BR	The service provider shall have the capability to ensure that password policies can be set to achieve a minimum complexity commonly accepted by both the security and industrial automation communities. NOTE At the time of this writing, minimal password complexity is: 1) at least eight characters in length, and 2) a combination of at least three of the following four character sets: lowercase, uppercase, numeric digit, and special characters (e.g.% and #).	For the solution or used reference architecture, the service provider shall have a process that can be performed for the asset owner: – to identify the account management application(s) used to set password policies that meet this requirement, – show that they are commonly accepted	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 setting the related password policy 2) Documented process for selection of and acceptance of account management application(s), that supports this requirement 3) Documented process showing that used password policy is commonly accepted and current, and not obsolete or unacceptable	1) Verification / validation record policy of this process, for example application of tools to verify minimum complexity of passwords 2) List of used account management application(s) in a project 3) Provided evidence on the applied minimum complexity policy for passwords (e.g. articles in trustworthy media, scientific papers, studies) showing that they are commonly accepted and current, and not obsolete or unacceptable	1) Regular review and continuous improvement of the quality and acceptance of password policies 2) Systematic and comprehensive review of the state of the art of the related minimum password complexity

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)**
Account manage-ment	SP.09.06 BR	The service provider shall have the capability to ensure that passwords for local and system-wide (e.g. domain) user accounts are configured to automatically expire after they have been in use for a period of time specified by the asset owner	For the solution or used reference architecture, The service provider shall have a process that can be performed for the asset owner to: – retrieve the expiry period requirements from the asset owner, – configure password expiry to meet those requirements NOTE Defining an expiration period to "infinite" (no expiry) is a possible choice for 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) Documented process on the configuration of password expiry policies to meet this requirement 2) Related checklists / templates 3) Documented process of verification / validation step for this requirement	1) verification / validation record on implementation of this policy 2) Documentation of successful cooperation with asset owner on password expiries in a project 3) Completed related checklists / templates	1) Continuous and positive feedback from the asset owners on applied password policy 2) KPI: No. of identified passwords which have not expired after their identified time period of usage (target = 0 over a certain period of 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)**
Account manage-ment	SP.09.06 RE(1)	The service provider shall have the capability to ensure that password policies are set to prompt users to change passwords N days before they expire, where N is specified by the asset owner. This requirement does not apply to passwords that are not set to expire	For the solution or used reference architecture, the service provider shall have a process that can be performed for the asset owner to: – retrieve the number of days for prompting users before password expiry from the asset owner – configure password expiry to meet that 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 on the configuration of password expiry policies to meet this requirement 2) Related checklists / templates 3) Documented process of verification / validation step for this requirement	1) Verification / validation record on implementation of this policy 2) Completed related checklists / templates 3) Documentation of successful cooperation with asset owner on user prompting	1) Continuous and positive feedback from the asset owners on applied user prompting 2) KPI: No. of users which have not been prompted N days before password expiry (target = 0 over a certain period of time)
Account manage-ment	SP.09.07 BR	The service provider shall have the capability to ensure that default passwords are changed as required by the asset owner	The service provider shall have a process that can be performed for the asset owner to identify and change the default passwords according to the requirements of 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) Documented process on the identification and changing of default passwords 2) Related checklists / templates / trainings 3) Related documented verification / validation steps that default passwords are changed	1) Documentation of applied verification / validation in a project that default passwords were changed according to the requirements of the asset owner 2) Completed checklists / templates / trainings	1) Continuous and positive feedback from the asset owners on the cooperation related to applied default password changes 2) KPI: No. of identified default passwords which have not been changed according to the requirements of the asset owners (target = 0 over a certain period of 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)**
Account manage-ment	SP.09.08 BR	The service provider shall have the capability to ensure that password policies are set to prevent users from reusing their last N passwords, where N is specified by the asset owner	For the solution or used reference architecture, The service provider shall have a process that can be performed for the asset owner to: – retrieve the number "N" of passwords from the asset owner, – configure password reuse to meet the related requirements	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 on the prevention of password reuses 2) Related checklists / templates / trainings 3) Related documented verification / validation steps that previous N passwords are not reused	1) Documentation of applied verification / validation in a project that password re-usages are prevented according to the requirements of the asset owner 2) Completed checklists / templates / trainings	1) Continuous and positive feedback from the asset owners on the cooperation related to password reuse prevention 2) KPI: No. of identified re-usages of passwords from the last N passwords which were not detected (target = 0 over a certain period of 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)**
Account manage-ment	SP.09.08 RE(1)	The service provider shall have the capability to ensure that password policies are set to prevent users from changing their passwords more frequently than once every N days, where N is specified by the asset owner	For the solution or used reference architecture, the service provider shall have a process that can be performed for the asset owner to: – retrieve the number N of days from the asset owner, – configure password changing to meet the related requirements NOTE Defining the number N days as "zero" (no restriction on frequency of change) is a possible choice for 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) Documented process on the prevention of password changes 2) Related checklists / templates / trainings 3) Related documented verification / validation steps that passwords are not changed more than once every N days	1) Documentation of applied verification / validation in a project that passwords are not changed more than once every N days 2) Completed checklists / templates / trainings	1) Continuous and positive feedback from the asset owners on the cooperation related to password change prevention 2) KPI: No. of identified changes of passwords more than once in N days (target = 0 over a certain period of 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)**
Account manage-ment	SP.09.09 BR	The service provider shall have the capability to ensure that accounts whose passwords have been approved by the asset owner to be shared with the service provider are securely documented and maintained.	The service provider shall have a process that can be performed for the asset owner to: – retrieve passwords approved for sharing from the asset owner, – document and maintain retrieved passwords securely	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 to ensure secure handling and documentation of shared passwords 2) Related checklists / templates 3) Description of used password management tools and criteria for their selection and maintenance	1) Documentation of application of protection of shared passwords in a project (e.g. encrypted archive or database of password manager) 2) Completed checklists / templates	1) Continuous and positive feedback from the asset owners on the cooperation related to shared passwords 2) Continuous improvement of the applied password protection mechanisms, for example: – more efficiency by automation, – strong encryption of stored passwords, – improved logging of password usages

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)**
Account manage-ment	SP.09.09 RE(1)	The service provider shall have the capability to report to the asset owner passwords that were 1) shared and no longer need to be shared, 2) knowingly divulged, or 3) knowingly compromised, and to support the asset owner in changing passwords as necessary	The service provider shall have a process that can be performed for the asset owner to: – report to the asset owner about outdated, divulged or compromised passwords, – change related passwords in cooperation with 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) Documented process for identifying passwords that need to be changed and reporting them to the asset owner 2) Documented process for cooperating with the asset owner related to password management according to the requirement 3) Related checklists / templates	1) Documentation of application of password management process (identification, reporting and changing) in a project 2) Records of related cooperation with asset owner 3) Completed checklists / templates	1) Continuous and positive feedback from the asset owners on the cooperation related to password management 2) Continuous improvement of the applied password management mechanisms, for example: – more efficiency by automation, – timeliness of reaction and resolution in case of outdated, divulged or compromised passwords

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)**
Malware protection	SP.10.01 BR	The service provider shall have the capability to provide the asset owner with documented instructions for the proper installation, configuration and update of malware protection mechanisms that are tested and verified for the automation solution.	For the solution or used reference architecture, the service provider shall have a process that can be performed for the asset owner to: – provide instructions to the asset owner for the use and maintenance of anti-malware mechanisms that it uses in the solution, – ensure that related mechanisms were verified and tested, – document how they were verified and tested (e.g. by the control system supplier or by the service provider itself)	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 delivering the relevant documentation and for related cooperation with the asset owner, for example including antimalware tools or whitelisting 2) Related checklists / templates 3) Training program for the service provider regarding malware protection testing and verification 4) Control system documentation from supplier for anti-malware mechanisms delivered with the Solution that describes how to maintain them and how they were verified	1) Documentation of application of installation and maintenance of malware protection mechanisms in a project 2) Completed checklists / templates 3) Completed related trainings	1) Continuous improvement of the applied malware protection mechanisms for example: – more efficiency by automation, – compatibility with the automation solution 2) Malware protection mechanisms are always state of the art over a period of time 3) Continuous and positive feedback from the asset owners on the cooperation related to malware protection mechanisms

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)**
Malware protection	SP.10.02 BR	The service provider shall have the capability to ensure that: 1) malware protection mechanisms have been correctly installed / updated and properly configured in accordance with the service provider's approved procedures, 2) malware definition files are installed within the time period agreed to with the asset owner, 3) malware configurations are maintained and kept current.	The service provider shall have a process that can be performed for the asset owner to make sure that: 1) ensure correct installation and configuration of malware protection mechanisms, 2) maintenance and update of the installed malware protection mechanisms (e.g. keeping malware definition files current) in cooperation with 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) Documented process for related installation / configuration / maintenance of anti-malware mechanisms 2) Training program for the service provider regarding malware protection installation / configuration / maintenance 3) Related checklists / template (e.g. final verification step that configuration and definitions file are up-to-date) 4) Documented process for updating configuration and definition files including time frame agreement with asset owner	1) Documentation of application of pattern update log during integration or maintenance in a project 2) Time frame agreement for maintenance service with the asset owner 3) Completed checklists / templates 4) Completed related trainings	1) Malware protection mechanisms are always state of the art over a period of time 2) Continuous and positive feedback from the asset owners on the cooperation related to malware protection mechanisms particularly to time period for related installation / maintenance

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)**
Malware protection	SP.10.02 RE(1)	The service provider shall create and maintain the documentation that describes the use of malware protection mechanisms in the automation solution for which the service provider is responsible. this documentation shall include for each component used in the automation solution: 1) the installation state of malware protection mechanisms or a statement that it is not technically possible to install malware protection mechanisms on the component, 2) the current configuration settings of the installed malware protection mechanism,	The service provider shall have a process that can be performed for the asset owner to document and maintain the antimalware software status for each component of the automation solution according points 1) to 4) of the requirement	Examples of execution that service provider has met the requirement at least for one customer for example: 1) Project documentation 2) Interviews	1) Documented process for use of malware protection mechanism of each component in an automation solution, fulfilling points 1) to 4) of requirement 2) Documented process for alternative mitigation measures where malware protection mechanisms are not feasible / available / applicable 3) Related checklists / templates	1) Established documentation of used malware protection mechanisms in a project 2) Complete checklists / templates 3) Documentation of applied other mitigation mechanisms according to point 4) of the requirement	1) Continuous improvement of the documentation of malware protection mechanisms, for example: – Continuous timely updating of documentation – Quality and comprehensiveness of documentation related to points 1) to 4) of the requirement

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)**
		3) the current status of malware definition files approved for installation on the component, 4) the use of other mitigating features and functions used to reduce the risk of infection or mitigate the effect of infections, or both, (e.g. isolating infections, reporting infections)					
Malware protection	SP.10.03 BR	The service provider shall have the capability to verify that malware, other than zero-day malware, can be detected and properly handled by the installed malware protection mechanisms.	For the solution or used reference architecture, the service provider shall have a process that can be performed for the asset owner to verify the correct operation of the antimalware mechanisms at the component, systems and solution level (e.g. configuration, detection, mitigation, logging / , notifications) to provide protection against known malware	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 on the verification proper malware operation 2) Related checklists / templates	1) Documentation of application of the verification of malware protection mechanisms in a project (e.g. EICAR, IDS / IPS, whitelisting tests, security gateway) 2) Completed checklists / templates	1) Malware protection verification mechanisms are always state of the art and current over a period of time 2) Continuous improvement of the verification of malware protection mechanisms and the associated process, for example: – timeliness of testing and verification, – cooperation with antimalware vendors related to malware definitions and updates

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)**
Malware protection	SP.10.04 BR	The service provider shall have the capability to provide to the asset owner documentation that describes: 1) how malware definition files for the automation solution are evaluated and approved, 2) reporting the status of malware definition files to the asset owner within N days after release of the files by the manufacturer, where N has been agreed to by the service provider and asset owner. This status includes the applicability (e.g. component and version) and approval state (e.g. approved, installed, disapproved, etc.) for each malware definition file	The service provider shall have a process that can be performed for the asset owner to: – document and maintain the information about malware definition files, – inform the asset owner of the related results within a mutually agreed time period after their release by the anti-malware software manufacturer. – inform the asset owner about the applicability and approval state of the new malware definition file	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 to create documentation about approval of malware definition files and reporting of the status to the asset owner 2) Related checklists / template for reporting on the approval stage	1) Documentation of applied verification of new malware definition files 2) Reporting agreement with asset owner 3) Completed checklists / templates	1) Continuous and positive feedback from the asset owners on the cooperation related to malware definition files and related reporting process 2) Continuous improvement of the documentation on malware definition files and reporting process to asset owner, for example: – continuous timely updating of documentation, – quality and comprehensiveness of documentation – efficiency of approval process for new malware definition files

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)**
Malware protection	SP.10.05 BR	The service provider shall have the capability to ensure that all devices, including workstations, supplied to the automation solution by the service provider are free of known malware prior to use in the automation solution.	The service provider shall have a process that can be performed for the asset owner to make sure that components / workstations are free of known malware when integrated into 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) Documented process ensuring that components / workstations are scanned for malware prior to integrating it into the automation solution 2) Related checklists / templates 3) Related training process for service provider 4) Documented process for supply chain assurances from component suppliers that the components delivered to the automation solution are free of known malware	1) Malware scan logs for all components / workstations performed in a project 2) Agreement with suppliers 3) Completed checklists / trainings 4) Completed trainings	1) Continuous improvement of technical competence related to malware scans over period of time 2) KPI: No. of identified malware in components / workstations integrated in an automation solution (target = 0 over a certain period of 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)**
Malware protection	SP.10.05 RE(1)	The service provider shall have the capability to ensure that for the portable media that it uses for system testing, commissioning, or maintenance, it uses this portable media for this purpose only	The service provider shall have a process that can be performed for the asset owner to make sure portable media is used only for its intended purpose	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 requiring that the portable media that the service provider uses in the automation solution is not used for any other purpose 2) Documented process of using automated mechanisms that recognize service provider portable media and restrict its use to authorized uses 3) Documented process of cooperation with the asset owner about usage of portable media for testing, commissioning or maintenance	1) Documentation of applied process for using portable media in a project 2) Test report on effectiveness of automated mechanism in a project 3) Related framework agreement with the asset owner	1) KPI: No. of identified portable media used in an automation solution being also used in an unauthorized way outside the project (target = 0 over a certain period of time)
Malware protection	SP.10.05 RE(2)	The service provider shall have the capability to ensure that all portable media used in or connected to the automation solution by the service provider is free of known malware prior to use in the automation solution	The service provider shall have a process that can be performed for the asset owner to make sure that portable media are free of malware when 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) Documented process ensuring that portable media are scanned for malware prior to use in the automation solution 2) Related checklists / templates 3) Automated mechanisms that recognize portable media and allow its use only if free of known malware	1) Documented results of antimalware scans of portable media 2) Completed checklist / templates	1) KPI: No. of identified malware-infected portable media being used in an automation solution (target = 0 over a certain period of time)