IEC PAS 62443-2-2

Edition 1.0 2025-03

PUBLICLY AVAILABLE SPECIFICATION

Security for industrial automation and control systems – Part 2-2: IACS security protection scheme

IEC PAS 62443-2-2:2025-03(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 It also gives information on projects, replaced and withdrawn publications.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 PAS 62443-2-2

Edition 1.0 2025-03

PUBLICLY AVAILABLE SPECIFICATION

Security for industrial automation and control systems – Part 2-2: IACS security protection scheme

INTERNATIONAL ELECTROTECHNICAL COMMISSION

ICS 25.040.40; 35.100.05

ISBN 978-2-8327-0299-4

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

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

SECURITY FOR INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS –

Part 2-2: IACS security protection scheme

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) IEC draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). IEC takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, IEC had not received notice of (a) patent(s), which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at https://patents.iec.ch. IEC shall not be held responsible for identifying any or all such patent rights.

IEC 62443-2-2 has been prepared by IEC technical committee 65: Industrial-process measurement, control and automation. It is a Publicly Available Specification.

IEC PAS 62443-2-2 has been developed by IEC TC 65 and the liaison ISA99: ISA committee on Security for industrial automation and control systems.

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

Draft	Report on voting
65/1051/DPAS	65/1121/RVDPAS

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 Publicly Available 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, and the ISO/IEC Directives, JTC 1 Supplement available at www.iec.ch/members_experts/refdocs. The main document types developed by IEC are described in greater detail at www.iec.ch/publications.

A list of all parts in the IEC 62443 series, published under the general title *Security for industrial automation and control systems*, can be found on the IEC website.

The committee has decided that the contents of this document will remain unchanged until the stability date indicated on the IEC website under webstore.iec.ch in the data related to the specific document. At this date, the document will be

- reconfirmed,
- withdrawn, or
- revised.

NOTE In accordance with ISO/IEC Directives, Part 1, IEC PASs are automatically withdrawn after 4 years.

INTRODUCTION

This document is the part of the IEC 62443 series that provides guidance on the development and validation of a set of technical, physical, and process security measures to address risk associated with cyberthreats when operating IACS. In the context of this document, asset owner also includes the operator of the IACS.

The purpose of the document is to provide input to support asset owners, integration service providers, maintenance service providers as well as product suppliers in their activities to provide a combination of technical, physical, and organizational capabilities for protecting IACS against cyberthreat.

SECURITY FOR INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS –

Part 2-2: IACS security protection scheme

1 Scope

This part of IEC 62443 provides guidance on the development, validation, operation, and maintenance of a set of technical, physical, and process security measures called Security Protection Scheme (SPS). The document's goal is to provide the asset owner implementing an IACS Security Program (SP) with mechanisms and procedures to ensure that the design, implementation and operation of an SPS manage the risks resulting from cyberthreats to each of the IACS included in its operating facility.

The document is based on contents specified in other documents of the IEC 62443 series and explains how these contents can be used to support the development of technical, physical, and process security measures addressing the risks to the IACS during the operation phase.

Figure 1 illustrates the content of this document using a simplified IACS life cycle.

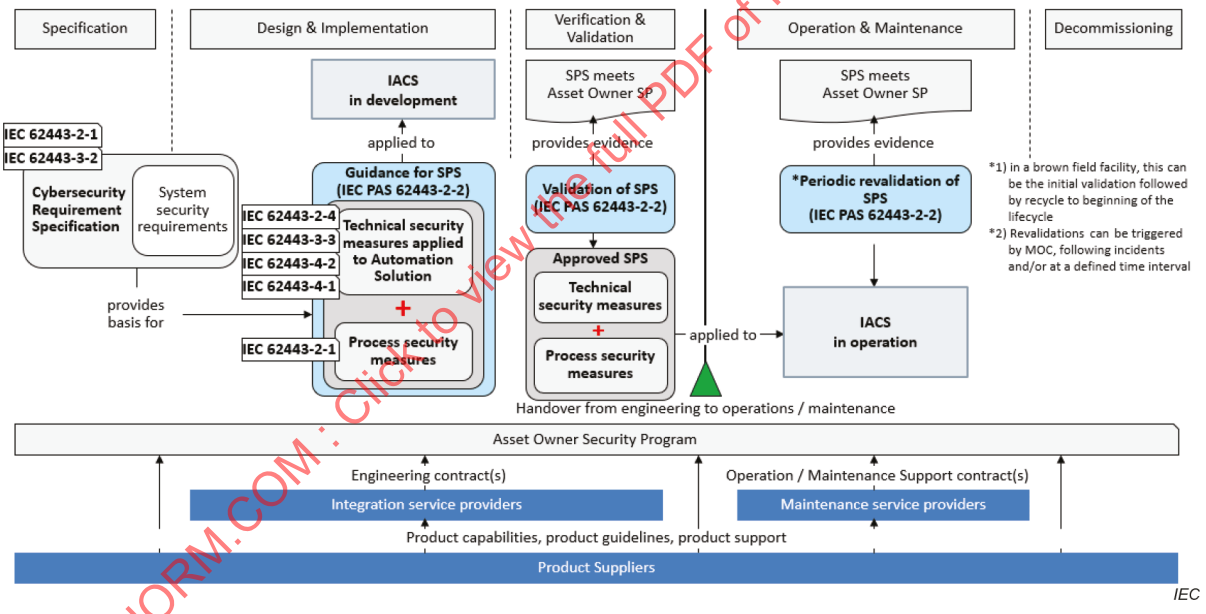

Figure 1 – Simplified asset owner security protection scheme (SPS) life cycle

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 TS 62443-1-1:2009, *Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models*

IEC 62443-2-1:—[1], *Security for industrial automation and control systems – Part 2-1: Security program requirements for IACS asset owners*

IEC 62443-2-4:2023, *Security for industrial automation and control systems – Part 2-4: Security program requirements for IACS service providers*

IEC 62443-3-2:2020, *Security for industrial automation and control systems – Part 3-2: Security risk assessment for system design*

IEC 62443-3-3:2013, *Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels*

3 Terms, definitions, abbreviated terms and acronyms

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

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

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

NOTE Terms and definitions are defined in IEC TS 62443-1-1. The purpose of this clause is to provide supplemental guidance for some key terms used in this document, to improve clarity for the reader.

3.1 Terms and definitions

3.1.1
security program
SP
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 SP for IACS asset owners refers to the policies and procedures defined by them to address cybersecurity concerns of the IACS. This can include technical, process, physical and compensating security measures used to reduce the cybersecurity attack surface.

[SOURCE: IEC 62443-2-1:—, 3.1.15]

3.1.2
security protection scheme
SPS
set of technical, physical, and process security measures designed to address cyber security concerns of an IACS during operation

Note 1 to entry: The SP for IACS asset owners refers to the policies and procedures defined by them to address cybersecurity concerns of the IACS. This can include technical, process, physical and compensating security measures used to reduce the cybersecurity attack surface.

[1] Under preparation. Stage at the time of publication: IEC/FDIS 62443-2-1:2024.

3.1.3
system security requirement
security requirements based on requirements specified in IEC 62443-3-3:2013

Note 1 to entry: When applied to products, the system security requirements are specified in IEC 62443-3-3:2013. Each requirement is formulated as "The control system shall provide the capability to ...".

Note 2 to entry: When applied to automation solutions, the system security requirements are defined as "The zone of the automation solution shall provide the capability to ...", instead of "The control system shall provide the capability to ...":

Note 3 to entry: When applied to IACS in operation, the system security requirements are defined as "The IACS in operation shall provide the capability to ...", instead of "The control system shall provide the capability to ...".

3.1.4
security level
measure of confidence that the IACS is free from vulnerabilities and functions in the intended manner

Note 1 to entry: The definition of security levels is expected to evolve. In the context of this document, the security levels are the levels to which the system security requirements are mapped to according to IEC 62443-3-3.

[SOURCE: IEC 62443-3-3:2013: 3.1.38, modified – The Note to entry has been changed.]

3.1.5
target security protection ratings
levels of the system security requirements that an asset owner desires to be fulfilled during operation

3.1.6
implemented security protection ratings
levels of the system security requirements which can be fulfilled during implementation by the designed technical, physical, and process security measures, under the assumption that the process security measures will be executed during operation with a demonstrated repeatability and effectiveness

3.1.7
operated security protection ratings
levels of system security requirements that have been fulfilled by the technical, physical, and process security measures at a given point of time during operation, with demonstrated process security measures that are repeatable and effective

3.1.8
maturity level
qualitative method of characterizing the capability of an organization to implement security requirements according to documented policies and procedures and their historical performance in doing so

Note 1 to entry: In the context of this document, maturity levels express the level of confidence that process security measures are executed by the personnel in charge during operation of the IACS with a demonstrated repeatability and effectiveness.

[SOURCE: IEC 62443-2-1:—, 3.1.7, modified – The Note to entry has been added.]

3.1.9
security measure
measure taken for an IACS to protect the safety, integrity, availability, and confidentiality

[SOURCE: IEC TS 62443-1-1:—, 3.1.110]

3.2 Abbreviated terms and acronyms

AO	asset owner
CRS	cybersecurity requirements specification
IACS	industrial automation and control systems
IEC	International Electrotechnical Commission
ISA	International Society of Automation
ISO	International Organization for Standardization
KPI	key performance indicator
ML	maturity level
MS	maintenance service provider
NIST	National Institute of Standards and Technology
PS	product supplier
SI	integration service provider
SL	security level
SL-C	security level capability
SP	security program
SPE	security program element
SPR	security protection rating
SPR-I	security protection rating implemented
SPR-O	security protection rating operational
SPR-T	security protection rating target
SPS	security protection scheme
SR	security requirement
SuC	system under consideration

4 Relationship between this document and other documents

The document describes the activities for the design, implementation, and validation of an SPS and the use of IEC 62443-2-1, IEC 62443-2-4, IEC 62443-3-2, IEC 62443-3-3, IEC 62443-4-1, and IEC 62443-4-2 for supporting these activities.

The concepts described in this document are not all reflected in currently published documents of the IEC 62443 series. None of these concepts contradicts contents of the IEC 62443 documents. They provide input for evolutions, which are expected to be reflected in further editions of IEC 62443 series documents.

5 Security program and security protection scheme

5.1 Relationship between security program and security protection scheme

IEC 62443-2-1 specifies security program (SP) requirements for IACS asset owners. The SP of IACS asset owners refers to technical, physical, and process security measures defined by them to address cyber security concerns of all the IACS during their respective life cycle. The SP can include technical, physical, and process security measures to reduce the cyber security attack surface. The SP also includes physical measures to reduce access to the assets of the IACS.

IEC 62443-2-1 has a requirement for the SP to implement an information security management system ensuring the execution of actions to reduce the risks. For an asset owner, risk reduction means the implementation of the necessary security measures for the protection of its operating facility against cyberthreats. It is not unusual that an operating facility includes several IACS, each of them controlling a part of the physical process. According to the criticality for the business of the asset owner, each IACS can have different target levels for security protection. The risk reduction actions include for each IACS the development of a set of technical, physical, and process security measures – the security protection scheme (SPS) – to meet the required target security protection levels. An asset owner establishing a security program ensures that a SPS is designed and applied during operation for each IACS, involving all roles defined in the IEC 62443 series.

The SPS life cycle is identical to the life cycle of the IACS to which the SPS is applied. In addition to security measures applied to each IACS, the SP includes security measures to meet corporate organization requirements of the operating facility. These are linked to the enterprise life cycle of the operating facility which is decoupled from the IACS / SPS life cycles. Examples of those measures are security management policies and procedures, security measurements such as KPIs, escalation procedures, top management reports, etc.

It is necessary to align the corporate organization requirements of the operating facility with those which apply to each IACS.

The latter leads to specific technical, physical, and process security measures for each IACS resulting from a risk-based approach considering the criticality of the considered IACS. In the context of IEC 62443, the asset owner role also includes the operator of each IACS. During operation, the execution of process security measures of the SPS by the personnel in charge are the responsibility of the asset owner.

Figure 2 illustrates the relationship between the SP and the SPS.

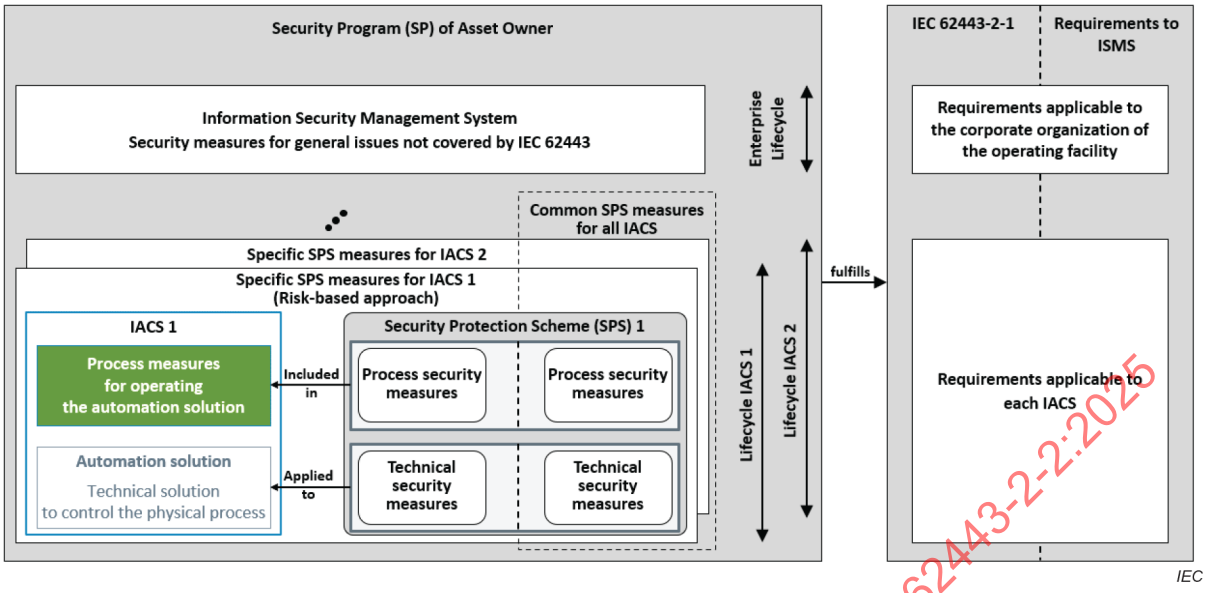

Figure 2 – Security program and security protection scheme

5.2 Process steps for the generation of a Security Protection Scheme

The primary process steps for the generation of an SPS are illustrated in Figure 3. Based on the process steps of IEC 62443-3-2, a partitioning of the IACS in zones and conduits is performed and the technical, physical, and process security measures are designed.

A cybersecurity requirement specification (CRS) is created for documenting the system security requirements for each zone and conduit. These are derived from the application to a specific IACS of the requirements of IEC 62443-2-1, to meet the tolerable cybersecurity residual risks which are specific to the considered IACS. The system security requirements are formulated by applying IEC 62443-3-3 requirements to zones and conduits of the IACS instead of capabilities of control systems. They should be grouped according to the security program elements (SPEs) and sub-SPEs defined in IEC 62443-2-1, to provide tracing to the asset owner security program requirements. The mapping of system security requirements to levels supports the required strength of security measures to meet the tolerable cybersecurity residual risks.

The CRS further includes enterprise, business, and operational constraints which are considered when designing the security measures. They include but are not limited to:

- operating environment assumptions,
- physical access to the assets of the IACS,
- assumptions and external dependencies,
- demarcation between OT and IT,
- company or site-specific policies,
- standards,
- regulatory requirements,
- operational availability and performance constraints,
- safety requirements,
- cost constraints.

The process starts with a risk-based system partitioning along the process steps described in IEC 62443-3-2, leading to zones and conduits.

For each zone and its conduits and SPE / sub-SPE, the CRS includes:

a) applicable IEC 62443-2-1 requirements,

b) derived system security requirements (IEC 62443-3-3) to meet the tolerable cybersecurity residual risks,

c) enterprise, business, and operational constraints.

For each zone and its conduits, a set of technical, physical, and process security measures are designed to fulfil the security requirements of the zone and its conduits. Some of the security measures are specific to only one zone and its conduits, others are effective for several or all zones and conduits. The SPS includes all technical, physical, and process security measures to fulfil the security requirements of each zone and its conduits.

In general, technical security measures, including, if any, compensating technical security measures, are not sufficient to fulfil the system security requirements during the operation of the IACS. The technical capabilities are operated according to associated process security measures. As the operation phase often lasts many years, these associated process security measures significantly impact the fulfilment of the requirements. For example, the implementation of a firewall is a technical security measure supporting the fulfilment of the system security requirement SR 1.13 (see IEC 62443-3-3) to "monitor and control all methods of access via untrusted networks". The security protection is given by the configured firewall according to the asset owner's requirements. During operation, the protection is directly impacted by the management of the firewall configuration, which constitutes the associated process security measures.

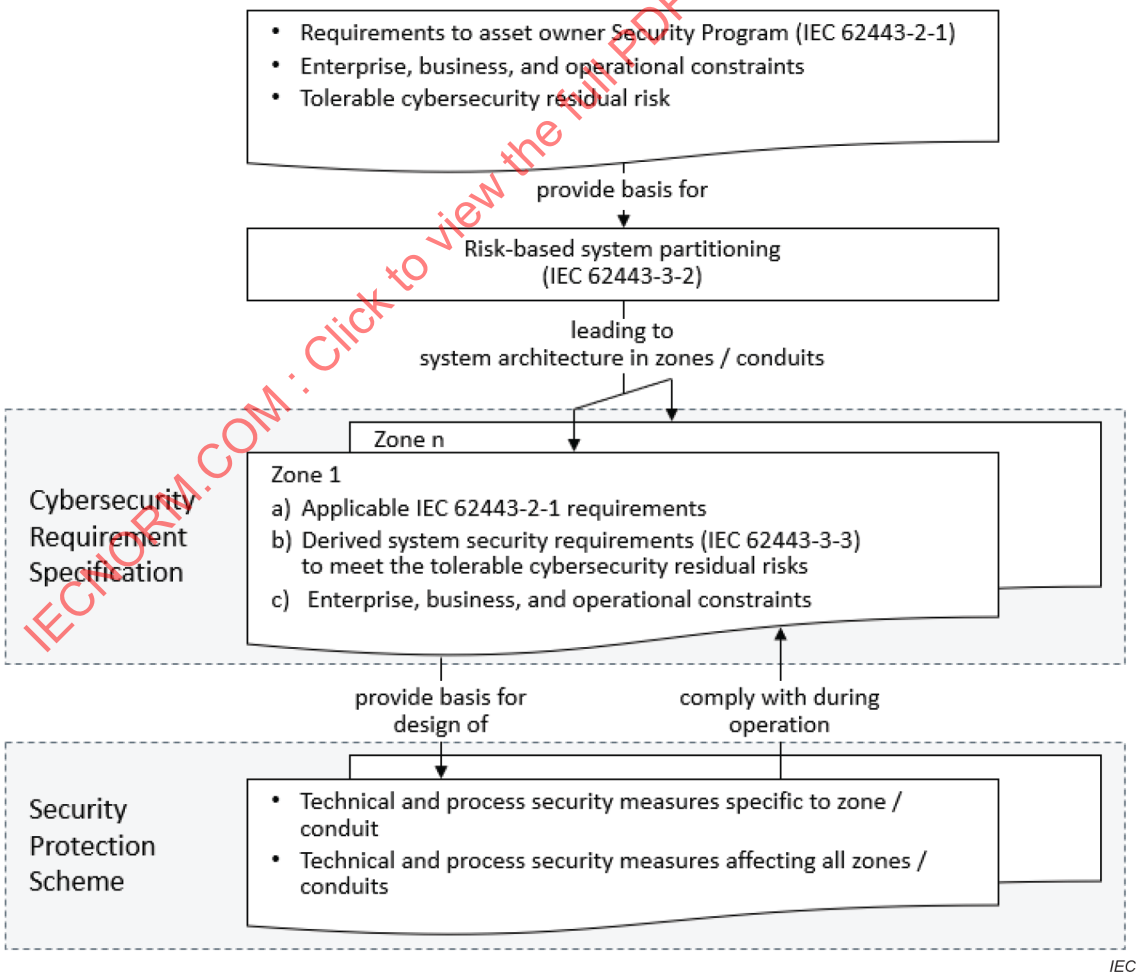

Figure 3 – Process steps for generating a security protection scheme

6 Security protection ratings

6.1 Overview

Security protection ratings (SPR) are used when assessing the fulfilment of system security requirements by the security measures included in the Security Protection Scheme. The content of the system security requirements, including their mapping to security levels (SL), is provided by IEC 62443-3-3.

The goal of the SPR is to support the target risk mitigation determined for the IACS solution during operation. Consequently, the system security requirements are defined as "The IACS in operation shall provide the capability to …", instead of "The control system shall provide the capability to …".

A system security requirement is assessed as fulfilled when the security measures provide the capability to fulfil it and the organizational part of the security measures are practiced reliably. The SPR describes the outcome of the assessment process in values from 0 to 4, which reflect the level of compliance with the system security requirement.

The SPR value combines two parts:

a) the mapping of the considered system security requirement to the security level (SL), and

b) the repeatability to execute the organizational measures necessary to sustain the required security measures during operation.

The first step is to evaluate the capability to fulfil the system security requirement. In many cases the security measures necessary to provide risk mitigation are a combination of technical measures implemented in the automation solution and organizational measures. The organizational measures include those sustaining the technical measures, as well as compensating risk mitigation organizational measures, if any. If the system security requirement can be fulfilled, the SL value is equal to the mapping of the considered system security requirement. The second part focuses on the repeatability of executing the organizational measures necessary to sustain the required security measures. The effectiveness of these is taken as a prerequisite and is not considered in this document. If the process security measures are executed reliably, the SPR value is equal to the mapping of the considered system security requirement.

System security requirements can also be fulfilled by purely organizational measures. In this situation, the assessment focuses on the repeatability of execution. The SL and the SPR values are equal to the mapping of the considered system security requirement if the process security measures are executed reliably.

EXAMPLE Regarding the system security requirement SR 1.1 – which is mapped to SL 1 –, the assessor will evaluate the fulfilment of the requirement: "The IACS in operation shall provide the capability to identify and authenticate all human users". The SL value is equal to 1, if the technical, physical, and process security measures provide the capability to fulfil this requirement. Fulfilment is achieved if the responsible personnel execute reliably the organizational measures necessary for the identification and authentication of human users, thus leading to the SPR value equal to 1.

The assessment evaluates the fulfilment of each system security requirement by one or several security measures, resulting in either "fulfilled" or "not fulfilled". Partial fulfilment is not considered in the determination of the SPR values but could be used to measure progress. How fulfilment is assessed depends on the methodology, which is not specified in this document. Any used methodology should show consistency and repeatability of the assessment results. Annex A provides example(s) of methodologies that could be considered.

6.2 Use of the maturity model defined in IEC 62443-2-1 for the determination of SPR values

Maturity models are commonly used to evaluate organizations regarding the ability of their personnel to repeatably act according to defined policies and procedures. Organizations can apply an existing model or define their own model. A maturity model to be used for the evaluation of the repeatability of execution of the process security measures should satisfy the following criteria, as shown in Figure 4:

- Maturity levels should be described with a clear differentiation of the levels.
- Each level should be progressively more advanced than the previous level.
- The model should include a threshold in the scale defining a repeatable execution of the process security measures when the threshold is exceeded.

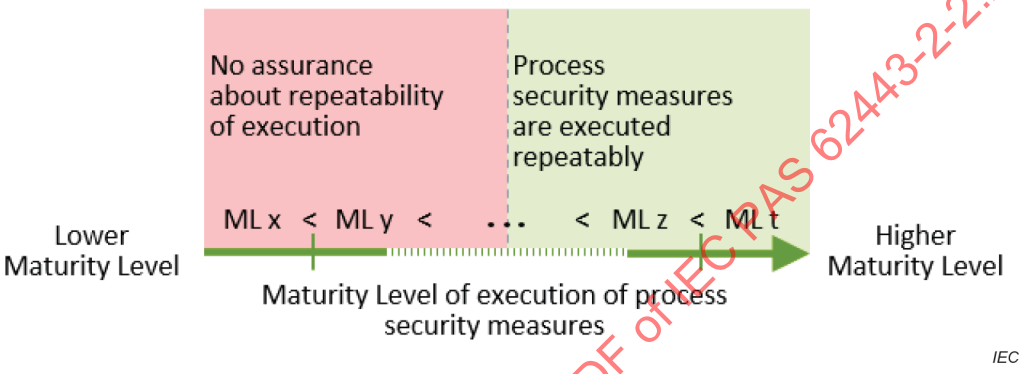

Figure 4 – Maturity model

IEC 62443-2-1 defines a maturity model that sets benchmarks for the execution of the process security measures by the asset owner. Based on this maturity model, the definitions of the maturity levels for the evaluation of the repeatability of execution of the process security measures are:

ML 1: Processes are performed in an ad-hoc and often undocumented (or not fully documented) manner. As a result, consistency over time can be difficult to be shown.

ML 2: Documentation exists and how to manage the delivery and performance of the capability. This documentation can be in form of written procedures or written training programs for performing the capability. There can be a significant delay between defining a process and executing it.

ML 3: A process at Level 3 is a Level 2 process that is being practiced on the IACS. The performance of a Level 3 practice can be shown to be repeatable over time within the IACS.

ML 4: Using suitable process metrics, the effectiveness and/or performance improvements of the process security measures for operation can be demonstrated. This results in a SP that improves the process through technological / procedural / management changes.

According to this maturity model, the threshold defining a repeatable execution of process security measures is between ML 2 and ML 3. At ML 3, documentation exists that describes how to execute the process security measures as well as proof on on-going repeatable execution. This documentation can be in the form of written policies and procedures, and written training programs that establish the basis that the practices are repeatable, even during times of stress. When these practices are in place, measured performance, e.g., training records, focused audits, key performance indicators, etc. provides evidence that their execution is performed and managed according to their documented plans. The execution can be shown to be repeatable over time within the IACS.

Figure 5 shows the determination of the SPR value using a matrix. The horizontal axis represents the security level to which the considered system security requirement is mapped. The vertical axis differentiates the maturity level for the execution of the process security measures. The SPR value is "not defined" if there is no assurance about repeatable execution of the process security measures.

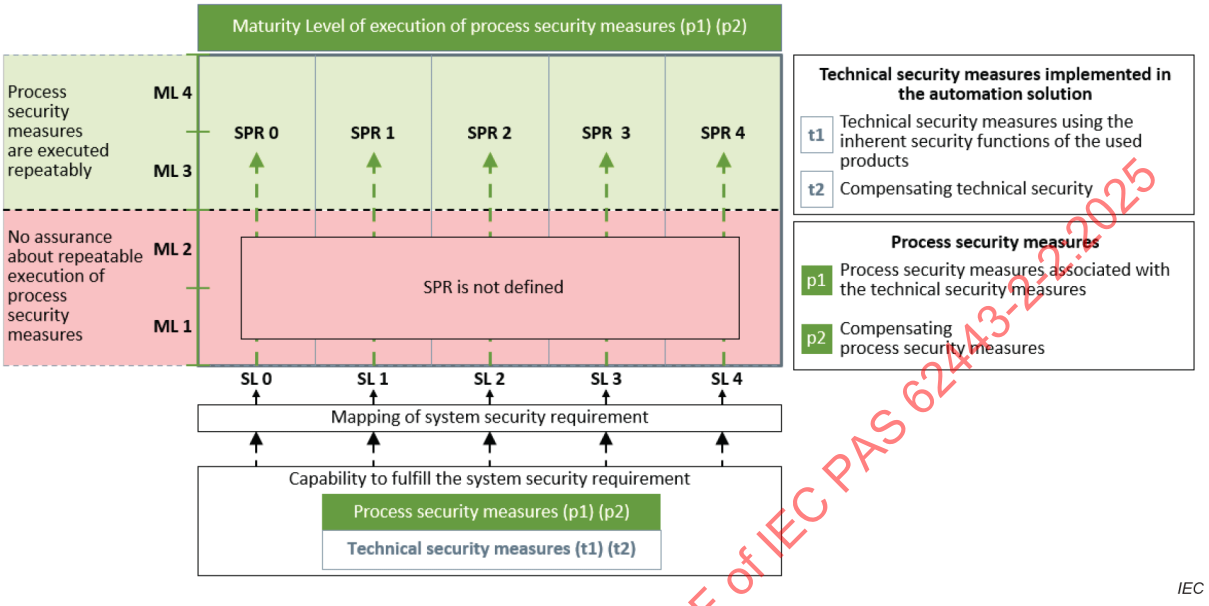

Figure 5 – Determination of the SPR value by using the maturity model of IEC 62443-2-1

As IACS are often operated over many years, it is important to ensure that the process security measures are reliably practiced over time. If this is not the case, the level of protection of the IACS during operation can be degraded. Human behaviour has a great impact on the protection of the IACS during operation and can significantly increase attack surfaces. Referring to the example of identification and authentication, a significant weakness is created if an authorized human user does not handle its credentials confidentially. The reason could be that there is no password policy prescribing the confidential handling of passwords, or that employees are not aware of or don't follow the policy. The ML value would be rated as less than 3. Due to this weakness, the protection of the IACS can be significantly lowered, even if the access control capabilities of the automation solution would allow a higher level of protection to be achieved.

Figure 6 shows the use of the SPR matrix to visualize the assessment of the fulfilment of a system security requirement mapped at Level 3. The first step is to assess if the technical and process security measures provide the capability to fulfil the system security requirement. This leads to a SL value of 3 in case of a positive result. In a second step, the repeatability of execution of the process security measures is assessed, which is reflected in the ML value. When the maturity level is above the threshold (ML 3 or ML 4), the system security requirement is fulfilled, which is reflected by an SPR value of 3.

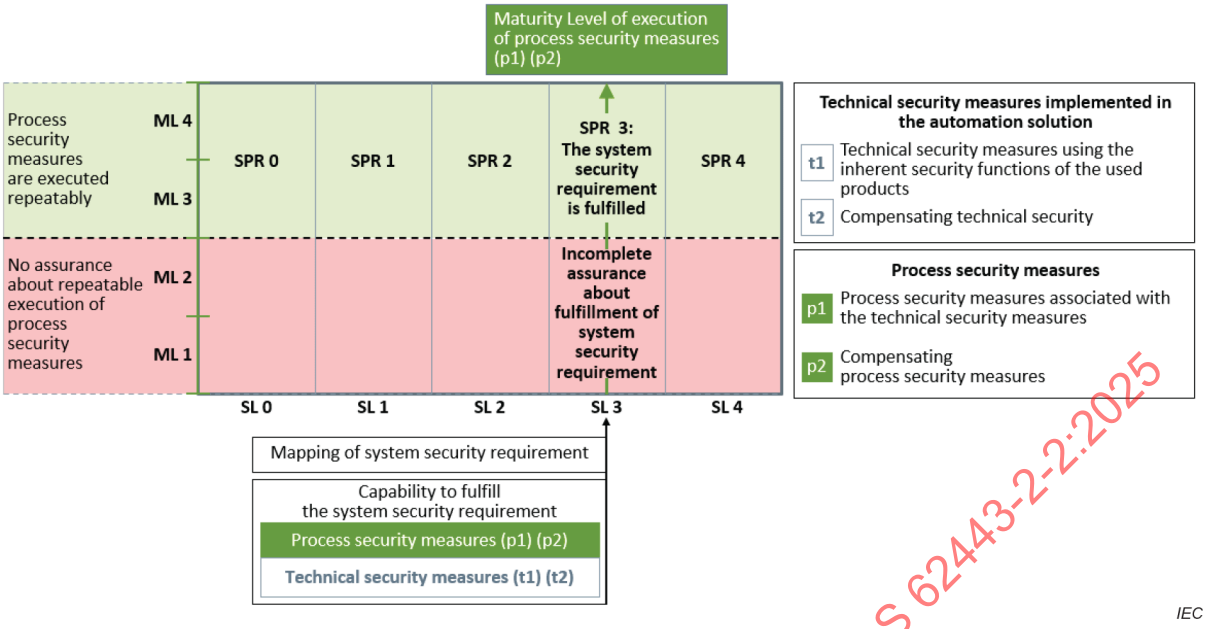

Figure 6 – Example of visualizing the fulfilment of a system security requirement with an SPR value

6.3 Use of alternative SPR matrixes for internal purposes

Some risk reduction should be available even for ML 1 and ML 2; however, it will be less than if ML 3 or ML 4 were applicable for the same SL capability. Organizations can define for internal purposes their own set of SPR values for ML 1 and ML 2, leading to alternative SPR matrixes that are helpful with respect to an asset owner's risk management program when it comes to making recommendations intended to provide improvements. Another benefit of estimating SPR values for all MLs is to show progress in the evolution of the organization's maturity level.

When assigned to fields of the matrix at ML 1 and ML 2, SPR values should match the following rules:

- For a given SL which can be matched, the SPR values should not decrease when the maturity improves, as the maturity level reflects the reliability of the organization to use the capabilities provided by the technical security measures during operation.
- The SPR values in the rows for ML 3 and ML 4 are equal to the corresponding SL values. Organizations can differentiate improvements in effectiveness and performance of the process security measures by claiming ML 4 in addition to the SPR values.

The left side of Figure 7 shows an example of a SPR matrix with SPR values fulfilling the rules.

An alternative possibility to show progress is to visualize in each field below ML 3 the SL values which can be matched and the ML values, as illustrated in the example on the right of Figure 7.

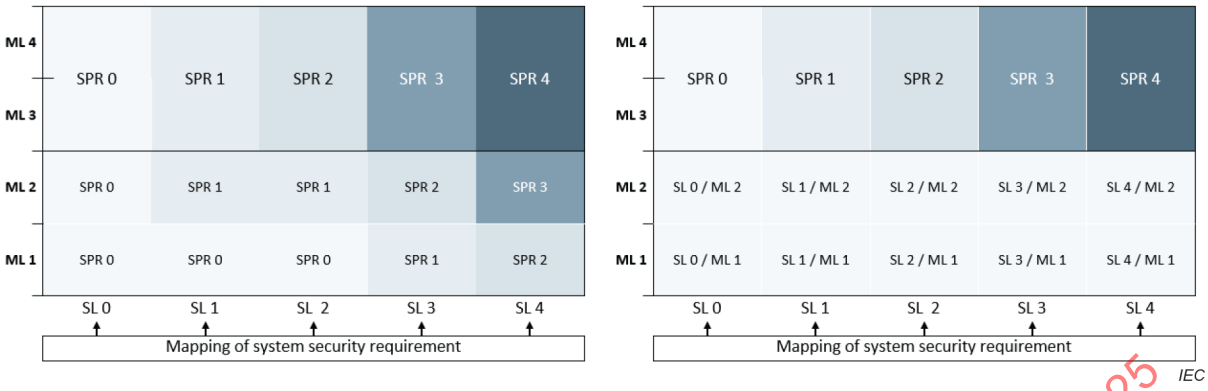

Figure 7 – Examples of alternative SPR matrix for internal purposes

6.4 Grouping of security requirements

The number of system security requirements reflects the large number of security issues to be considered when implementing a holistic security protection scheme. Evaluating the fulfilment of each system security requirement requires security expertise and leads to a high number of SPR values.

The SPR concept can support a systematic approach for the development of the security protection schemes, by building groups of system security requirements and other related requirements of the IEC 62443 series. Each group would include the requirements which address the same security issue. An aggregated SPR value would be generated for each group. For example, the overall SPR can be defined as the minimum level of the fulfilled system security requirements. Alternative aggregating methods can be defined, leading to a different meaning of the aggregated SPR value. The aggregated SPR values cannot be considered as absolute values, but support comparison of different sets of security measures. A tool can be developed to visualize the fulfilment of the system security requirement in aggregated SPR values.

6.5 Tracing to SPEs and sub-SPEs

As all security activities of the involved actors should have the purpose to support the protection of IACS during operation, a reasonable way for the grouping is to use the structure of the document IEC 62443-2-1, which specifies requirements to the security program of IACS asset owners. In the current documents, the requirements for the various actors are spread over different documents of the series, each having a different structure. The requirements in IEC 62443-2-1 are grouped in security program elements (SPE), each having one to three sub-SPE. Tracing all requirements to these elements shows how the requirements of the IEC 62443 series can be used to support asset owners in the implementation of security protection schemes for their IACS.

The grouping traces each relevant requirement of the series to one or more sub-SPE. Asset owners structuring their security programs with the sub-SPEs are able to request service providers to offer capabilities according to their traced requirements. When designing automation solutions, service providers select products with inherent capabilities helping to fulfil their traced requirements in each considered sub-SPE. Product suppliers are able to demonstrate capabilities of their products to support the fulfilment of the requirements of the respective sub-SPE.

A common structure is key for the development, practice and maintenance of a security protection scheme and the evaluation of the level of confidence that the protection matches the tolerable residual risk.

- The requirements of IEC 62443-2-1 apply to the process security measures to be practiced by the asset owner during operation.
- The traced system security requirements of IEC 62443-3-3 apply to the IACS in operation.
- The traced requirements of IEC 62443-2-4 apply to the expected contributions of service providers for integration or maintenance.
- For products, the traced requirements of IEC 62443-3-3 and IEC 62443-4-2 apply to the expected inherent security capabilities.
- The traced requirements of IEC 62443-4-1 apply to the expected contributions of the product suppliers with guidelines, incident handling and vulnerability management.

6.6 Views

The SPR concept can also be used to provide an additional level of simplification with views. Views are typically used by the management level of an organization, for example in the communication with insurance companies or governmental bodies. Views visualize the protection ratings as a handful of SPR number values.

In the same way as for the grouping in sub-SPEs, each element of a view includes the system security requirements which are traced to the considered view element. This can be done by additionally tracing each system security requirement to one or more view elements or by aggregating the SPR values of the sub-SPEs. This can be done as additional features of the tool for the generation of the SPR value in the sub-SPEs.

An organization can define its own views or use views which are defined for an industry sector, a country or any interest group sharing the same issues. For example, the "Framework for Improving Critical Infrastructure Cybersecurity" published by the National Institute of Standards and Technology (NIST) is structured in functions (Identify, Protect, Detect, Respond, Recover) which could be the elements of a view.

To illustrate the concept, the following describes a generic view. Business owners at management level define the SPR targets for each element of the view, based on the impact of a misuse of the IACS to the business under their responsibility. The view dashboard highlights security areas requiring improvements to meet the desired system security requirements. Based on the dashboard, cost and implementation timeline for proposed security measures can be discussed with the management.

- Secure physical access:
  Includes the organizational and technical measures which influence the physical access to the system under consideration.
- Organizational security:
  Includes the policies and procedures to organize the security.
- Secure design:
  Includes the organizational and technical measures which influence the SPR of the designed automation solution.
- Secure operations and maintenance:
  Includes the organizational and technical measures which influence keeping the SPR during operation.
- Secure life cycle management:
  Includes the organizational and technical measures which influence the maintenance of the SPR over the life cycle of the IACS.

Figure 8 illustrates a possible dashboard for the generic view.

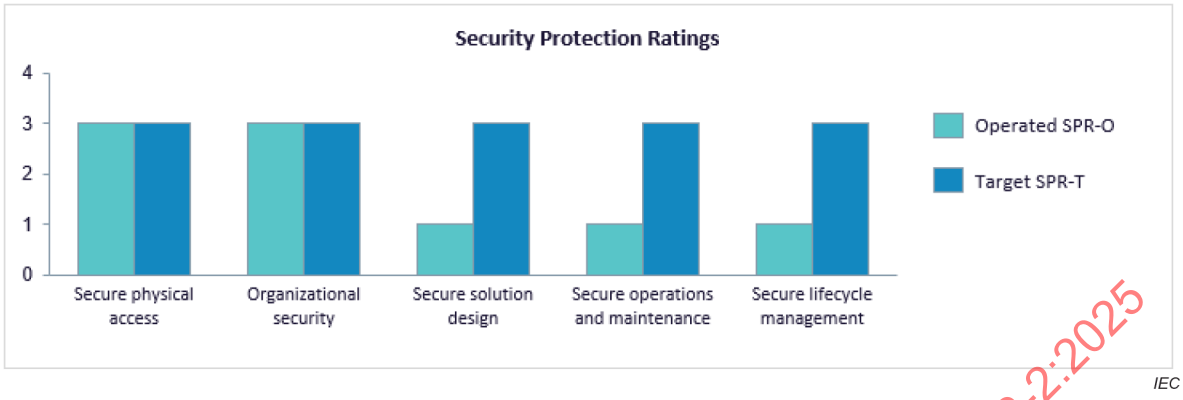

Figure 8 – Example of a dashboard for the generic view

Managers can use views for setting targets as part of requests for quotation. As a response, integration service providers represent their capabilities with a simplified visualization of their offerings.

Views can also be used by integration service providers as inputs for the design activities and the visualization of the security protection ratings that can be attained by the proposed technical and process security measures.

During operation, views can be used to visualize the rated protection of the IACS in operation compared to the initial targets.

6.7 SPR and SL types

6.7.1 General

Security levels are described in IEC 62443-3-3:2013, Annex A. As the concept of SPR is based on the concept of SL, the SPR types are aligned with the security levels. SPR types support the implementation of security protection schemes along the phases of the IACS life cycle, see Figure 9.

6.7.2 SL types for products

When applied to products, the following definition applies:

- Capability SL (product), SL-C (product)
  Security level that a that product can meet without compensating security measures when properly configured and integrated in an automation solution.

6.7.3 SPR types used in an IACS life cycle

In an IACS life cycle, implemented security protection ratings apply to a specific zone of the automation solution.

NOTE A zone can be an entire automation solution or individual segments of an automation solution.

When applied to zone(s) the following definitions apply:

- Target SPR (zone), SPR-T (zone)
  Levels of the system security requirements that an asset owner desires to be fulfilled, considering the procedures necessary to sustain the security measures during operation.
- Implemented SPR (zone), SPR-I (zone)
  Estimation of the security protection ratings SPR-O, which can be met during operation by the implementation of zone related security capabilities, under the assumption that the process security measures will be able to demonstrate repeatability and effectiveness.
- Operated SPR (zone), SPR-O (zone)
  Security protection ratings of the fulfilled system security requirements, considering the repeatability and demonstrated effectiveness of procedures necessary to sustain the same security measures during operation.

Target security protection ratings are used for the development and the update of the security protection scheme. The asset owner considers the tolerable residual cybersecurity risk for his/her business and derives the target protection for the IACS in operation. The target SPR (SPR-T) for each zone is defined along the process steps of the IEC 62443-3-2 detailed risk assessments, by using SPR values in lieu of SL values.

Security measures are expected to be designed to fulfil the desired system security requirements. In addition to the design of technical security measures, recommendations for the process security measures to be practiced during operation are generated. Products with the necessary capability SL (SL-C) are selected to be included in the design of the security protection scheme. Where such products are not available, compensating technical or process security measures shall be developed and implemented. SPR-I values can be used to visualize the system security requirements, which can be potentially fulfilled, based on the designed and implemented security measures. SPR-I indicates the predicted compliance with targeted system requirements of IEC 62443-3-3, which can be fulfilled during operation.

When designing security measures, the system security requirements which can be fulfilled during operation can be estimated. It is assumed that the designed organizational measures are executed repeatably. The estimation is mainly important after verification and validation, but can also be made during design and implementation, to give a prediction of the level of protection which can be achieved during operation.

Before starting operation, the technical and process security measures are validated. The operated security protection ratings SPR-O can be predicted by the implemented security protection rating (SPR-I), under the assumption that process security measures are practiced reliably.

Operated security protection ratings can be evaluated during operation of the IACS. The operated SPR (SPR-O) should be evaluated at defined periodic intervals, considering that the maturity level regarding the practice of operational and maintenance policies and procedures can evolve over time, in either a positive or negative manner. SPR-O indicates the current measured compliance with targeted system requirements of IEC 62443-3-3.

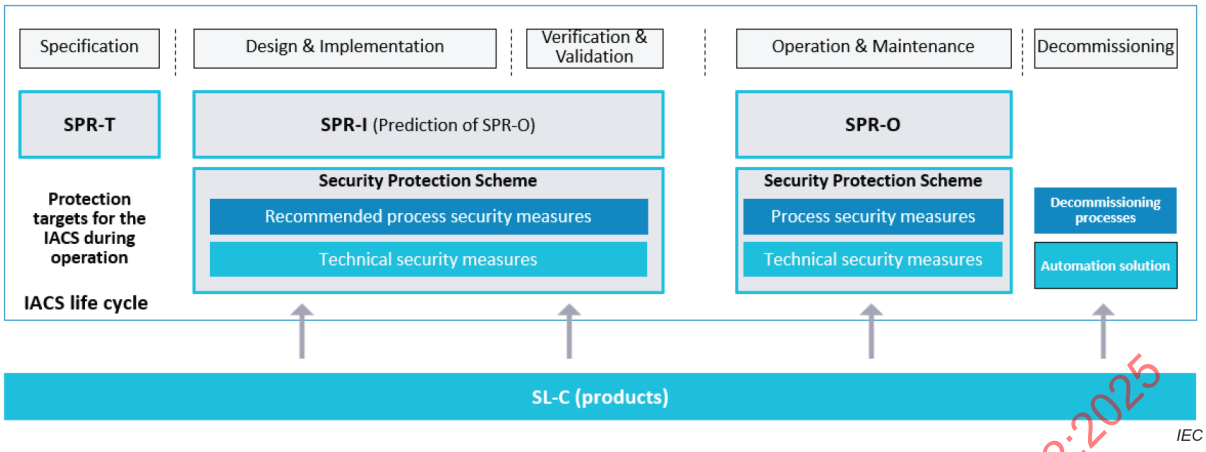

Figure 9 – Use of SPR and SL types in the IACS life cycle

7 Principal roles

7.1 Overview

To understand the development process of a security program, it is necessary to understand the roles involved in the life cycle of an IACS. A role is described in terms of responsibilities, accountabilities, and associated activities to be fulfilled by an organization.

An organization can fulfil one or several roles. For example, the same organization can be responsible for the operation of an IACS as well as for the design, implementation, and validation of the automation solution. On the other hand, a role can be fulfilled by one or several organizations. For example, maintenance activities can be performed by different organizations such as vendors, service providers, asset owners, etc.

The development, operation, and maintenance of a comprehensive security protection scheme (SPS) for an IACS in operation requires the contribution and collaboration of all involved actors according to their role.

Figure 10 summarizes the principal roles and their associated accountabilities and responsibilities concerning the IACS environment.

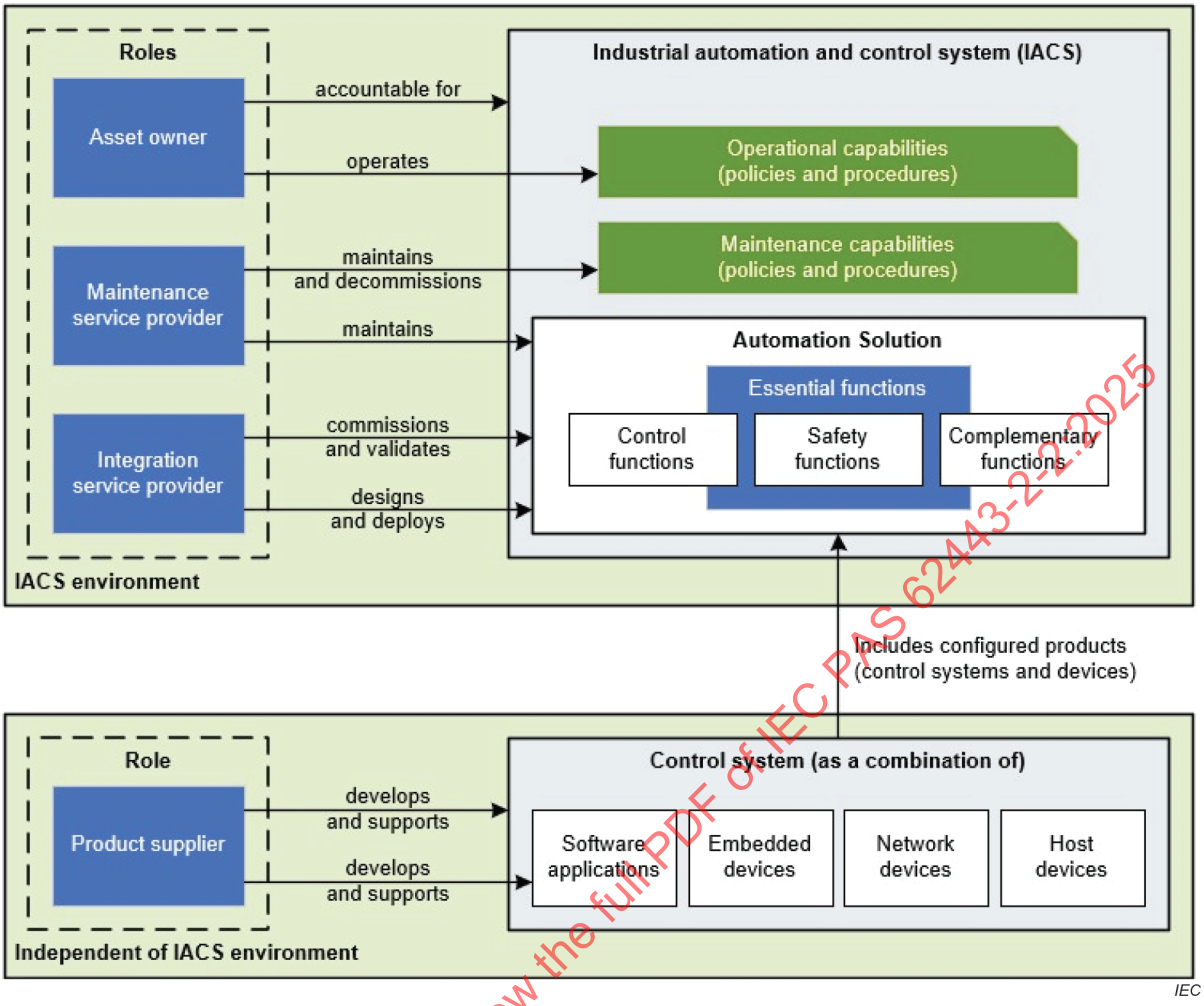

Figure 10 – Roles and responsibilities overview

7.2 Asset owner

The asset owner is fully accountable for the IACS, including the level of cybersecurity and the associated risks throughout the life cycle. This role is responsible for developing and approving the security program (SP) and the security protection scheme (SPS) for all the IACS for which it is accountable. The asset owner defines the tolerable residual cybersecurity risk as an input requirement for all activities along the IACS life cycle. While remaining fully accountable, the organization fulfilling this role can delegate specific responsibilities and the associated activities to organizations fulfilling other roles. The asset owner is also responsible for the operation of the IACS. In many cases, the company which operates the IACS is also the legal owner and is accountable for the IACS. In this case, the accountable role belongs to the business management and responsibility for operation is with the production department of the company.

To claim conformance to the IEC 62443 series, the asset owner should conform to the following standards:

a) IEC 62443-2-1,

b) IEC 62443-2-4,

c) IEC 62443-3-2,

d) IEC 62443-3-3.

7.3 Integration service provider

This role is responsible for providing integration services used in design and deployment as well as commissioning, validation, and periodic revalidation of the security measures of the automation solution. It is not unusual that one or several organizations design and deploy parts or the whole automation solution while another organization is responsible for the commissioning and validation of the automation solution.

To claim conformance to the IEC 62443 series, the integration service provider should conform to the following standards:

a) IEC 62443-2-4,

b) IEC 62443-3-2,

c) IEC 62443-3-3.

7.4 Maintenance service provider

This role is responsible for providing maintenance services triggered by a regular schedule, such as replacing malicious software patterns, reviewing user accounts, or inspection and testing of the security protection scheme to ensure it continues to be compliant with the cybersecurity requirements specification. The maintenance service provider also has the responsibility for decommissioning parts or the whole automation solution. Measures to match the tolerable residual cybersecurity risk during decommissioning typically include actions based on risk assessment as well as the active purging of sensitive data.

To claim conformance to the IEC 62443 series, the maintenance service provider should conform to the following standards:

a) IEC 62443-2-4,

b) IEC 62443-3-2,

c) IEC 62443-3-3.

7.5 Product supplier

This role is responsible for the development and support of products used in the automation solution. The activities include the development of security capabilities to be used for the deployment of the security measures of the security protection scheme. The product supplier is responsible for supplying integration and hardening guidelines as well as establishing a process for incident handling and vulnerability management applied to its products.

To claim conformance to the IEC 62443 series, the product supplier of a control system should conform to the following standards:

a) IEC 62443-3-3,

b) IEC 62443-4-1.

To claim conformance to the IEC 62443 series, the product supplier of a component (as defined in IEC 62443-4-2) should conform to the following standards:

a) IEC 62443-4-1,

b) IEC 62443-4-2.

7.6 Other roles

Other roles that can have some level of involvement or interest in securing the system under consideration (SuC) include:

- Regulatory bodies – Includes government and industry inspection, certification, and audit organizations who impose requirements on asset owners.
- Insurers – Includes providers of cybersecurity insurance policies and general insurers who impose requirements on asset owners.
- Training and certification bodies – Providers of cybersecurity training and certification services, including industry and academic organizations.

8 Duties and activities in the IACS life cycle related to the security protection scheme

8.1 Overview

The life cycle used in the IEC 62443 standards is shown in Figure 11. It is based upon the stages of the general representative system life cycle model in ISO/IEC/IEEE 24748. That standard defines the life cycle as consisting of the following phases:

1) concept;
2) development;
3) production;
4) utilization;
5) support;
6) retirement.

Many sub-work processes can be viewed in the context of this life cycle. For instance, risk management activities occur in the operations and maintenance phases, some of which are cyber-related and some that are not.

Figure 11 describes the levels of involvement of the principal roles described in Clause 7 in the IACS life cycle:

- Accountable:
  Indicates that the organization fulfilling this role is legally responsible for the risks associated with activity.
- Responsible:
  Indicates that the organization fulfilling this role has the duty to execute the activities associated with the role.
- Contributor:
  Indicates that the organization fulfilling this role has the duty to contribute to the activities executed by those identified as the "responsible" role.

The product supplier (PS) is responsible for product development and interfacing with the asset owner (AO), the integration service provider (SI), and the maintenance service provider (MS) throughout the IACS life cycle.

The asset owner is accountable for all risks associated with the IACS under his/her jurisdiction. The AO approves all outputs of the IACS life cycle. While remaining accountable, the organization fulfilling this role can delegate specific responsibilities and the associated activities to organizations fulfilling other roles.

In addition to their liability as accountable, the asset owner is responsible for specifying the IACS cybersecurity requirements. The integration service provider works with product suppliers and the asset owner and is responsible for the design, implementation, and validation of technical security measures to the IACS. The asset owner is responsible for validating the process security measures to the IACS and for operating the IACS. The maintenance service provider is responsible for maintaining the security measures to the IACS, regularly or when required by changes in the IACS solution or the threat environment. The maintenance service provider is responsible for preventing misuse of information in out-of-service assets.

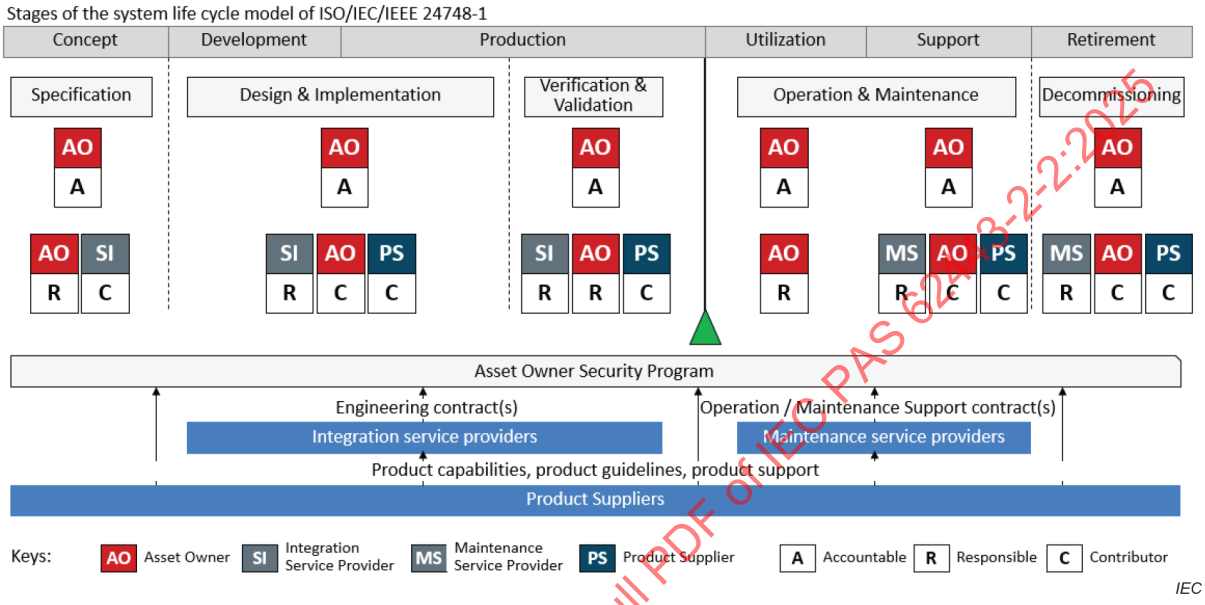

Figure 11 – Life cycle phases and roles

Although Figure 12 presents the progression from specification to decommissioning as a simple, linear life cycle or process, the reality is that it includes several iterations that are the responsibility of specific principal roles. In general, requirements based on experience are passed back to earlier stages of the life cycle. For example, experiences gained in implementation should be considered in design or specification.

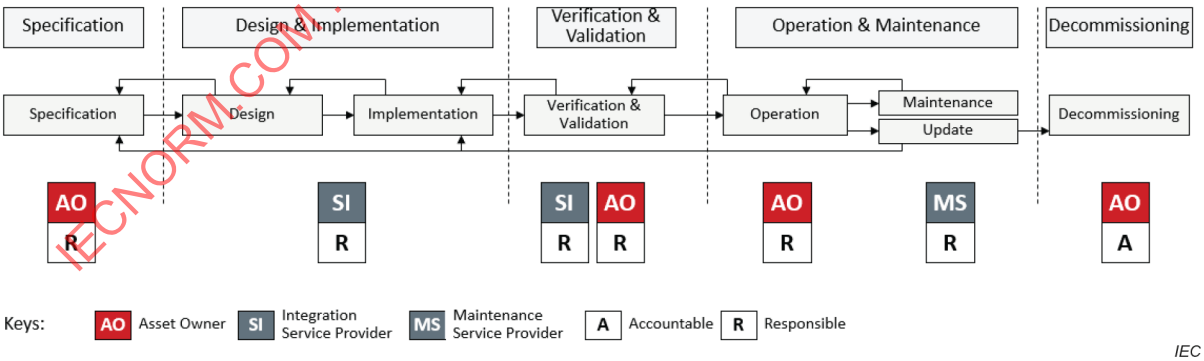

Figure 12 – Iterations in the IACS life cycle

8.2 Generation of the cybersecurity requirement specification (CRS)

The overall responsibility for the generation of the CRS resides with the AO. Cooperation between AO and SI is beneficial when partitioning in zones and conduits and determining system security requirements for each zone and its conduits. Figure 13 shows a simplified view of the activities for the generation of the CRS.

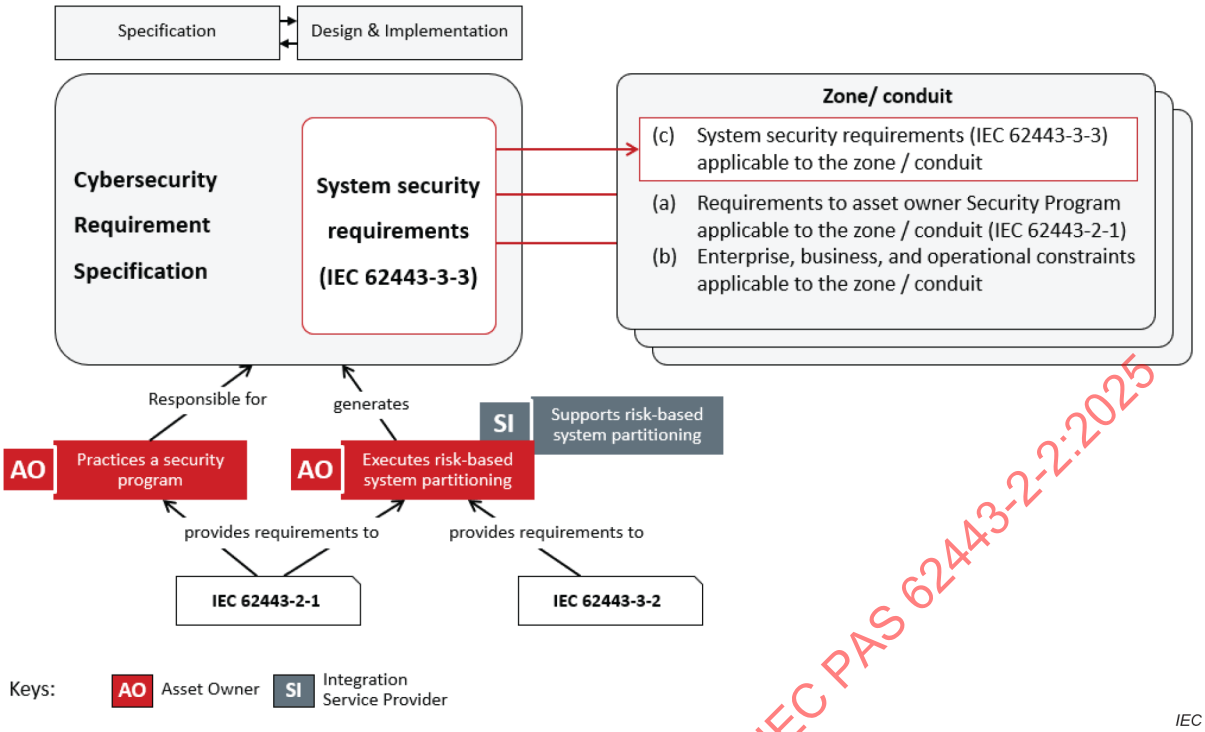

Figure 13 – Activities and responsibilities for the generation of the CRS (simplified view)

The tasks and activities should be based on the process steps described in IEC 62443-3-2. There can be a great deal of iteration and in some cases parallel activities. The design and implementation of security measures can lead to update the CRS based on cost and performance considerations.

8.3 Design and implementation of the security measures

The overall responsibility for the activities in this phase belongs to the SI role. The objective is to design and implement the technical security measures applied to each zone and its conduits of the automation solution. Before starting detailed design, a comparison between the identified initial risk and the tolerable risk is performed (refer to ZCR 4 of IEC 62443-3-2). If the initial risk is below the tolerable risk, there is no need to design additional security measures: the activities should be to modify the CRS to be consistent with the risk assessment. It should be noted that documentation of the CRS is a specification activity, illustrating the iterative nature of the life cycle.

Figure 14 shows a simplified view of the activities and responsibilities for the design and implementation of the security measures applied to the automation solution.

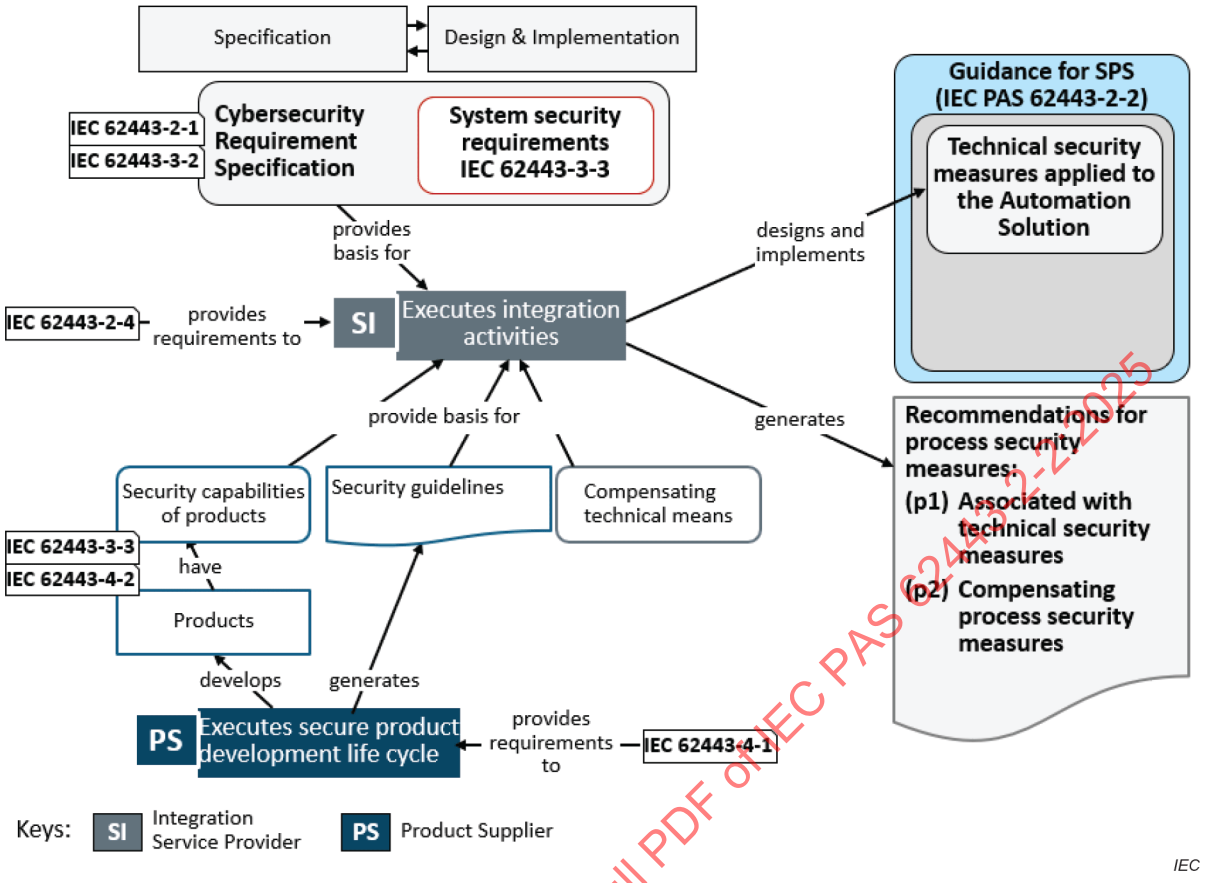

Figure 14 – Activities and responsibilities for the design and implementation of the technical security measures applied to the automation solution (simplified view)

The SI deploys the security capabilities of the products and adds, if necessary, compensating security measures if the system security requirements cannot be natively met by the products. The compensating security measures can be realized technically, for example adding external protection devices. They can also be realized with process security measures, for example monitoring the access to control rooms by a person. In this case, the SI generates recommendations describing how these compensating process security measures can fulfil the system security requirements. The integration activities include the fulfilment of the applicable requirements of IEC 62443-2-4, for example, to harden the products according to the hardening guidelines of the product supplier, to get approval from the asset owner, to change default passwords according to the password policy of the asset owner or to implement least privilege and least functionality.

The SI adopts existing or develops new recommendations for process security measures to be executed during operation. Most of the technical security measures require associated process security measures to support and sustain the technical capabilities. They are closely related to the security measures applied to the automation solution and are adjusted accordingly.

When compensating process security measures are necessary due to lack of technical capabilities, the SI shall work with the AO to resolve. As the AO is accountable for the risk, their involvement is necessary. The fulfilment of system security requirements requires a repeatable practice of these process security measures and belongs to the responsibility of the AO.

Although the overall responsibility for the activities of the design phase belongs to the SI, the contributions of the PS and AO are essential. The MS may be also involved as it is responsible for maintaining the security measures during operation.

The PS contributes by providing the necessary information for the integration and organizational measures to support and sustain the product capabilities during design and operation of the automation solution.

The PS should describe the functional security capabilities of the product. The PS should also describe the list of requirements of IEC 62443-4-2 or IEC 62443-3-3 which can be fulfilled by the product.

In addition, the PS should describe compensating technical and/or process security measures the SI implements, to fulfil security requirements of IEC 62443-4-2 or IEC 62443-3-3 which cannot be fulfilled by the security capabilities of the product.

It is expected that product suppliers comply with IEC 62443-4-1 when developing their products. The product supplier shall provide guidance relative to its products, including:

- the security defense in-depth strategy for the product,
- the security defense in-depth measures expected to be provided by the external environment in which the product is to be used,
- guidelines for hardening the product,
- guidelines for removing the product from use,
- responsibilities and actions necessary for the asset owner to implement and securely operate the product as well as assumptions regarding the behaviour of the user/administrator and their relationship to the secure operation of the product, and
- user account requirements and recommendations associated with the use of the product.

Furthermore, IEC 62443-4-1 requires that the product supplier has a process in place for vulnerability management, incident handling, and update management. This implies that the product supplier provides support if vulnerabilities are discovered during the commercialization phase. Depending on the situation the support can be:

- to provide information on the vulnerability,
- to provide guidelines for workarounds, or
- to deliver updates or patches.

Cooperation between the SI and AO roles are essential, as the decision to fulfil system security requirements by purely technical, purely organizational or a combination of technical and associated process security measures is often a matter of choice, considering cost and benefits aspects. It should be noted that in general, technical measures require management procedures by both SI and AO to support their sustained effectiveness.

NOTE Examples of SI management procedures for technical measures during design and implementation include hardening, patching, etc. Examples of AO management procedures for technical measures during operation include patching, maintenance of the approved configuration, review of access control lists, etc.

The AO is responsible for the requirements included in the CRS and ensures that the SI develops those security measures enabling their fulfilment. In addition, the AO role should be involved with the SI in the generation of the recommendations for process security measures, as the AO is responsible for executing these during operation.

Security measures can be specific to a given zone, several zones, or even to the whole IACS. Proceeding zone by zone means that each security measure should be evaluated as being specific to the zone under consideration or as being effective as well to other zones or the whole IACS. For example, the protection provided by a front-end firewall contributes to the protection of subsequent zones within the IACS for some threat vectors. Many process security measures apply to several zones or the whole IACS. For example the backup and restore processes apply in general for all assets of the IACS.

For each zone or conduit of the automation solution, the output includes:

- design and implementation of technical security measures, and
- recommendations for process security measures to be executed during operation:

  (p1) recommendations for process security measures associated with the technical security measures, including policies and procedures necessary to sustain their effectiveness, and

  (p2) recommendations for compensating process security measures designed to fulfil system security requirements without using technical means.

8.4 Generation and documentation of the process security measures

The overall responsibility for these activities is the role of AO. The AO role uses the recommendations provided by the SI role and the user documentation provided by the PS role to generate and document process security measures to by executed during operation of the IACS.

Documented policies and procedures are prerequisites for the repeatable execution of the process security measures. Documentation should be a combination of defined polices, standards, practices and procedures supported by a training program. Figure 15 shows a simplified view of the activities and responsibilities for the generation and documentation of process security measures.

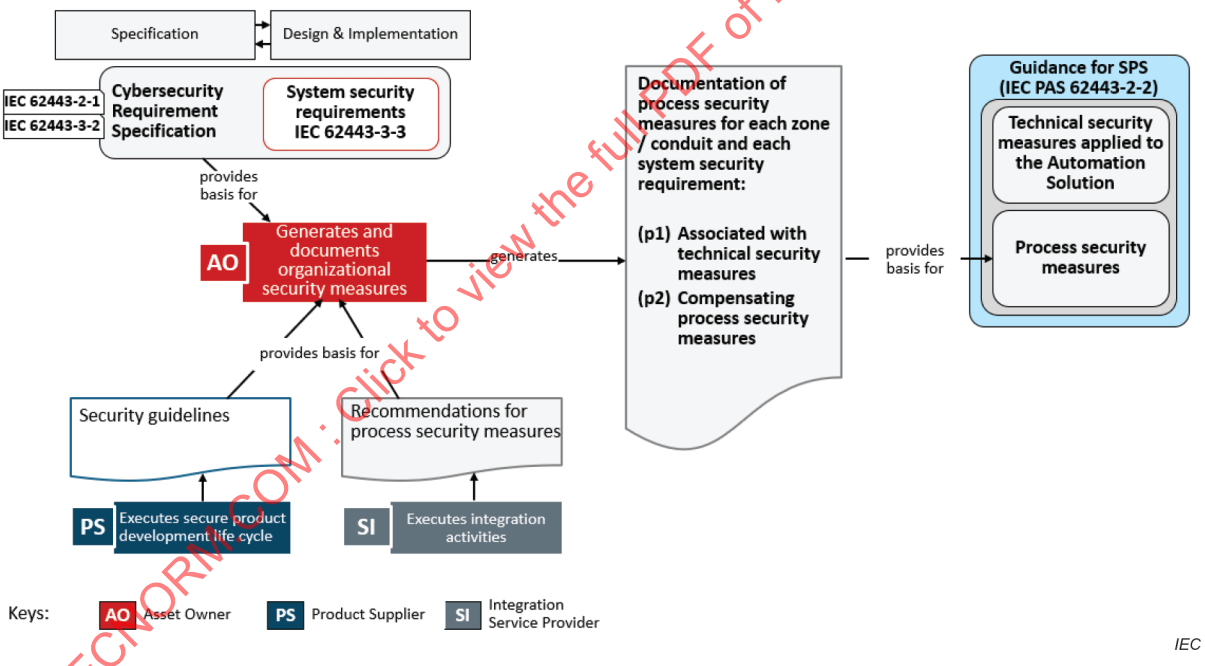

Figure 15 – Activities and responsibilities for the documentation of process security measures (simplified view)

8.5 Validation of the security protection scheme

8.5.1 Overview

The validation of the SPS is the last step before going into operation. The activities are often performed within the scope of a site acceptance test before hand-over to the AO. The SI is responsible for validating the technical security measures applied to the automation solution. The AO is responsible for validating the documented process security measures that are necessary to sustain the effectiveness of the technical measures during operation. During the acceptance activities, the AO can perform its own validation activities.

8.5.2 Validation of the technical security measures

The responsibility for these activities belongs to the SI role. The purpose is to demonstrate that the applied security capabilities within the system provided by the product supplier(s) plus compensating security measures applied to the automation solution can fulfil the desired system security requirements. This is reflected by the SL values for every system security requirement applied within a zone and its conduits of the automation solution.

EXAMPLE 1 To fulfil the system security requirement SR 1.1 from IEC 62443-3-3 "Human user identification and authentication", the SI can implement technical security measures using username and password for the identification and authentication of human users. This would allow to meet the requirement enhancement "SR 1.1 RE 1 – Unique identification and authentication", which is mapped to SL 2. The SL value for the considered system security requirement would be 2.

The SI role provides evidence that the deployment and configuration of product security capabilities as well as of compensating technical security measures provide the capabilities to fulfil the system security requirements. In addition, the SI role provides evidence that the integration activities have been practiced repeatably including the fulfilment of the applicable requirements of IEC 62443-2-4.

For each zone and its conduits and for each SPE / sub-SPE, the SL values which can be met by the capabilities provided by the technical measures are determined. An SL value can be determined if the integration activities have been executed repeatably. If there is no assurance about repeatable execution, significant weaknesses can still exist in the automation solution, thus challenging the security level which can be met by the technical security measures.

EXAMPLE 2 A configured firewall would allow meeting the requirement SR 5.2 from IEC 62443-3-3 "Zone boundary protection". The SL value for the considered system security requirement would be 1. Not hardening the firewall according to the requirement SP.03.05 from IEC 62443-2-4 would challenge this SL value.

Figure 16 illustrates graphically the determination of the SL value when the technical security measures applied to the automation solution provide the capability to fulfil requirements mapped at SL 2.

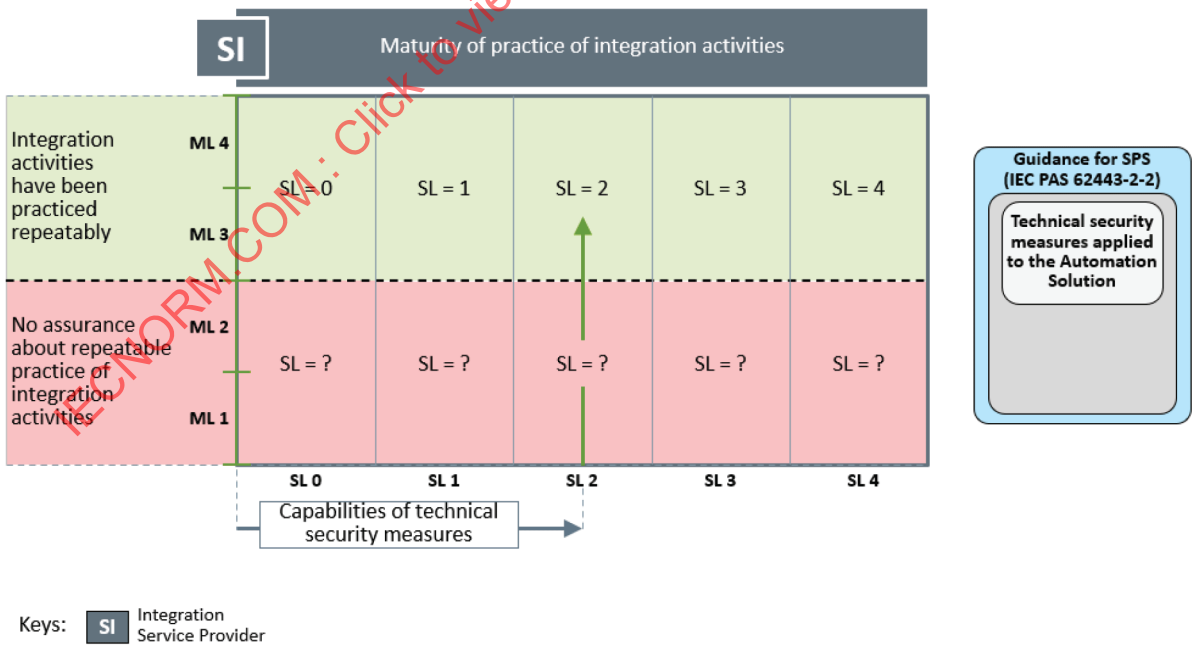

Figure 16 – Example of the determination of the SL value which can be met with capabilities provided by the technical security measures

8.5.3 Validation of the process security measures

The AO is responsible for the validation of the documented process security measures. The SI is responsible for providing input as to what organizational measures are necessary to support and sustain the technical capabilities provided. For each zone and its conduits of the automation solution, the AO evaluates each SPR and provides evidence that the documentation provides the basis for a repeatable execution of the process security measures during operation.

The activities are often performed within the scope of a site acceptance test and combined with the validation of the technical security measures under the responsibility of the SI. The AO can additionally perform its own testing to verify and validate acceptance before starting the operation and maintenance phase.

8.5.4 Prediction of the SPR values, SPR-I

The validation phase is often concluded with a dry run involving the organization responsible for operation which allows a prediction of the SPR, i.e., SPR-I, under the assumption that the validated process security measures are executed repeatably by the AO role during operation.

Figure 17 illustrates graphically an example of the prediction of an SPR value in the use case described in Clause 5.

The predicted SPR (SPR-I) value equals 3 under the assumption that all documented and validated process security measures are executed repeatably during operation.

The SPR values can be aggregated to a SPR value for a zone or conduit. For example, the aggregated SL can be defined as the minimum level of system security requirements, which can be fulfilled.

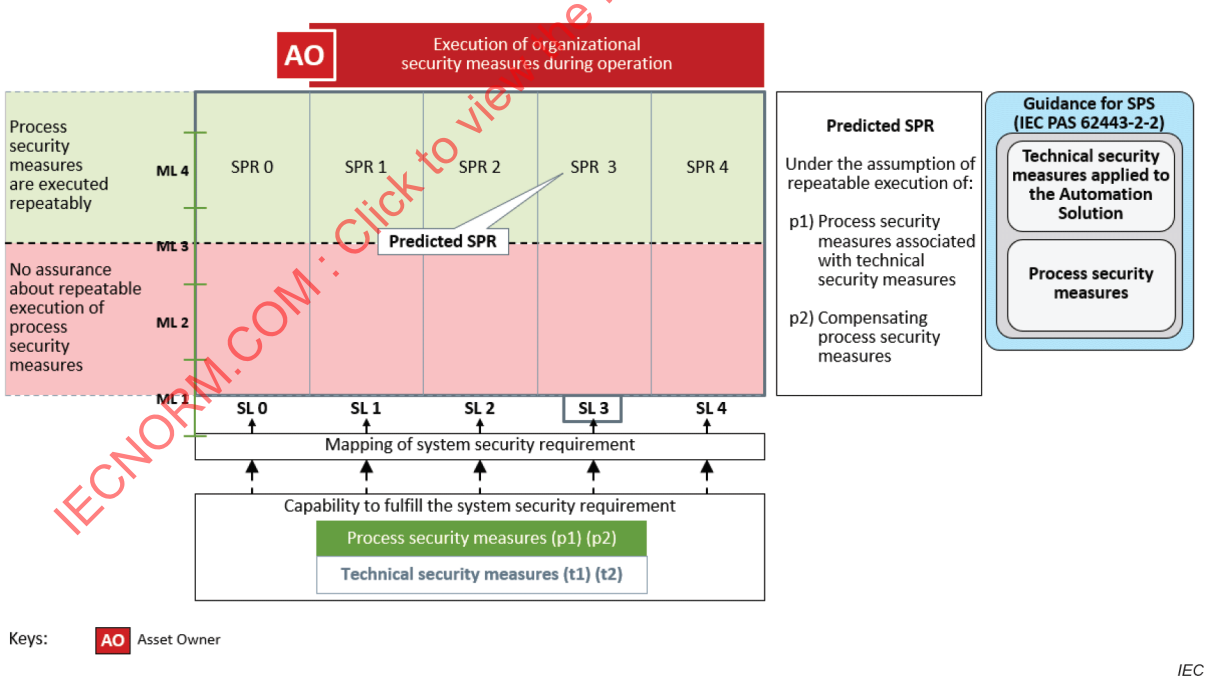

Figure 17 – Example of the prediction of the SPR value

8.6 Periodic revalidation of the SPS during operation

The AO is responsible for the operation of the IACS and for maintaining the continued practice of the technical, physical, and process security measures included in the SPS.

The AO ensures that all users accessing the IACS execute repeatably the validated process security measures of the SPS.

One part is to perform an audit of the quality and completeness of the policies and procedures. The second part is to verify that the personnel in charge executes the process security measures according to the policies and procedures repeatably. Predicted SPR values are confirmed if the maturity level of the organization in charge always meets or exceeds the threshold defining a repeatable practice of the process security measures, typically ML 3.

The audit is regularly performed to ensure stability over time and be presented to the appropriate management with the authority to accept risk.

Even if the operating conditions remain unchanged, the security measures included in the SPS should be regularly maintained to ensure their effectiveness. While the security measures remain unmodified, data used in the security measures should always reflect the actual operating status. The frequency and procedures for updating the current data are described in the process security measures and fine-tuned for each project.

Some examples of such data are:

- virus patterns;
- firewall rules;
- active accounts list;
- backup and restore data.

EXAMPLE 1 A configured front-end firewall is a security measure to control and monitor access from untrusted networks. If the maintenance of an asset of the IACS requires a remote access from an external service provider, the front-end firewall rules are temporarily changed to open a remote connection. After the maintenance cycle of the asset, these rules are changed back to close the remote connection.

All actions should be documented in a change management system.

Unlike the maintenance of unmodified security measures, it is necessary to revalidate the SPS from time to time, to ascertain that the desired SPR values are still met. This should be performed at defined intervals (for example, due to a regulatory process, safety management requirements, during a scheduled maintenance of the industrial facility) or event-triggered due to a change that affects the effectiveness of the security measures.

The AO ensures that the SPS is sufficient and always correct during the life cycle of IACS. The AO triggers a risk assessment to be performed in close collaboration between AO and MS. The purpose of the risk assessment is to evaluate if the security measures still fulfil the desired system security requirements for each zone / conduit. If the requirements are not satisfied, the AO triggers an update phase of the SPS.

Examples of such changes are:

- evolving threat situation,
- vulnerability discovered in the automation solution product(s),
- change in operational conditions,
- modification of the automation solution, or
- decommissioning of assets.

Annex A
(informative)

Example of methodology for SPR verification

A.1 Overview

This document provides a framework for the evaluation of security program ratings. The evaluation methodology is not part of this document. As there is not yet a consensus for mathematical measurements of security, most methodologies are currently based on qualitative evaluation of the measures by experts. The evaluation can be based on a questionnaire that lends itself to a form of self-evaluation by asset owners to determine their level of protection. Third parties can conduct formal evaluations based on an in-depth evaluation of each security requirement in the considered SPE. Evaluation methodologies based on this framework should allow a flexible and scalable approach that can be applied to establish and maintain a defense in-depth strategy for a given IACS or a zone within an IACS.

A.2 Detailed assessment, requirements-based

Detailed assessments will typically be done by auditors in the asset owner's organization or by independent evaluation organizations.

Detailed assessments are useful to find out weaknesses by highlighting requirements which are not fulfilled. These will guide responsible organizations to develop focused organizational or technical measures to remediate to weaknesses.

The assessment is conducted independently for each SPE using four steps, as follows:

a) Determine applicable system security requirements.

b) For each applicable system security requirement, assess the capability of fulfilment by the set of technical, physical, and process security measures.
If the system security requirement can be fulfilled, the SL value is the level to which the system security requirement is mapped to, according to IEC 62443-3-3.

c) For each of the applicable system security requirement, assess the repeatability of execution of the process security measures, the alignment to the technical security measures and the demonstrated effectiveness to fulfil the purpose.
Derive the ML value according to the maturity model described in 6.2.
Reference Annex B – Maturity level assessment, for guidance.

d) Determine the SPR value according to 6.2.

For the generation of aggregated SPR values, refer to 6.3.

If the determined SPR is less than the SPR-T, then consider how to correct the situation, e.g., compensating security measures, improved design, or organizational measures, etc.

The process should be performed until all zones and conduits have been assessed.

Depending upon the life cycle timeline, different SPRs are applicable. These are:

SPR-I – Indicates predicted compliance with targeted system security requirements of IEC 62443-3-3 mapped to Level x (i.e., SPR-I; 1, 2, 3, or 4) and below, which can be fulfilled during operation by:

- technical security measures of a zone of the automation solution including compensating technical security measures,
- and reliably performed and sustained process security measures.

The process security measures include:

a) process security measures to fulfil applicable requirements of IEC 62443-2-1,

b) process security measures associated with technical security measures,

c) and compensating process security measures.

SPR-O – Indicates current measured compliance with targeted system security requirements of IEC 62443-3-3 mapped to Level x (e.g., SPR-O; 1, 2, 3, or 4) and below, which are fulfilled during operation by:

- technical security measures of a zone of the automation solution, including compensating technical security measures,
- and reliably executed and sustained process security measures (ML equal or above 3).

The process security measures include:

a) process security measures to fulfil applicable requirements of IEC 62443-2-1,

b) process security measures associated with technical security measures,

c) and compensating process security measures.

A.3 Detailed assessment, risk-based

Risk assessment methodologies, for example according to NIST SP800 39, may be followed provided the risk assessment requirements are satisfied by the methodology selected.

A.4 Simplified evaluation, questions-based

The simplified evaluation uses questions about performance of technical, physical, and process security measures for the rating of the SPR-value of each SPE instead of evaluating the fulfilment of individual system security requirements included in the SPE. A questionnaire can be developed for the simplified evaluation. The answers to the questions will lead to the rating of SL and ML values thus SPR values.

Annex B
(informative)

Maturity level assessment

B.1 General

NOTE This annex complements the description of the activities described in the main body of this document, to help the reader when assessing the maturity of execution of the process security measures. For convenience, some content of this annex duplicates content of the main body of this document.

The assessment of maturity can be performed to assess the current overall organizational cybersecurity capability or to evaluate those organizational measures and procedures necessary to support the effectiveness of technical measures that are an important component of the determination of security protection ratings (SPR). This annex focuses on the contribution to SPR determination, although it should be relatively easy to see how it can be applied to the entire security program. There are several maturity models that can be found referenced in industry, but they tend to only be slightly different. Table B.1 illustrates the maturity levels based on IEC 62443-2-1.

Table B.1 – Assessment MLs

Assessment MLs
ML 0 – Incomplete / Unaware
ML 1 – Initial
ML 2 – Managed
ML 3 – Defined / Practiced
ML 4 – Improving

B.2 Overall assessment work process

1) Document applicable technical measures applicable to all zones.
2) Document applicable technical measures applicable as a function of specific zones.
3) Document organizational measures and procedures necessary to support specific technical measures.
4) Assess each organizational measure and procedure for its maturity level.
5) Document the results.

B.3 Maturity level assessment procedure

Table B.2 illustrates the maturity level assessment procedure.