GLOBAL CYBERSECURITY ALLIANCE

Security Lifecycles in the ISA/IEC 62443 Series

Security of Industrial Automation and Control Systems

THE TIME IS NOW

October 2020

www.isa.org/ISAGCA

Security Lifecycles in the ISA/IEC 62443 Series

Security of Industrial Automation and Control Systems

Executive Summary

This document provides an overview of the security lifecycles that are described in the ISA/IEC 62443 Series of standards and technical reports, which specifies the requirements for the Security of Industrial Automation and Control System (IACS). There are two security lifecycles that are included in the ISA/IEC 62443 Series: the *Product Security Lifecycle,* and the *Automation Solution Security Lifecycle.*

The *Product Security Lifecycle* specifies the security requirements for the *technical and organizational security measures* used to design, develop, and support IACS System and Component products. It includes *secure by design* aspects such as threat modeling and defense-in-depth strategies, *secure implementation* such as secure coding standards, *security verification & validation testing*, and *security update management. Technical security measures* based on *Security Levels* allow the Product Supplier to deliver *IACS Systems* and *IACS Components* that are capable of meeting specified security requirements, provided the Asset Owner maintains associated *organizational security measures.*

The *Automation Solution Security Lifecycle* is shown in Figure 1 and specifies the *technical and organizational security measures* used throughout the lifecycle of the IACS Automation Solution, which is the realization of IACS Systems and IACS Components at a particular facility.

Asset Owner, Product Supplier, and *Service Provider* are roles that are defined later in this document. Roles are not the same as organizations. An organization can have multiple roles, and the responsibilities of a role can be split between multiple organizations. While this document presents typical roles and responsibilities throughout the security lifecycles, it is important to note that the Asset Owner must determine and document the *actual roles and responsibilities* used for their organization and IACS Product Suppliers and Service Providers.

There are a few key messages that the reader should understand from this document:

- The Asset Owner is *accountable* for the cybersecurity risk of the IACS and the Equipment Under Control
- IACS cybersecurity is a *shared responsibility* between Asset Owner, Product Supplier, and Service Providers
- IACS cybersecurity is required *throughout the Automation Solution Security Lifecycle*
- IACS cybersecurity is required throughout the *Product Security Lifecycle*

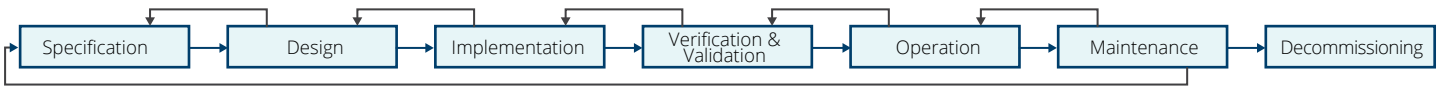


Figure 1 – ISA/IEC 62443 IACS Automation Solution Security Lifecycle

Introduction

This document provides an overview of the security lifecycles that are described in the ISA/IEC 62443 Series of standards and technical reports, which specifies the requirements for the Security of Industrial Automation and Control System (IACS). There are two security lifecycles that are included in the ISA/IEC 62443 Series: the Product Security Lifecycle and the Automation Solution Security Lifecycle.

Note: *The Product Security Lifecycle is based on ISA/IEC-62443-4-1:2018 [8]. The Automation Solution Security Lifecycle is based on a ISA99 Committee draft of ISA/IEC-62443-2-2 [23] and is subject to change.*

IEC/ISA 62443 Series

In order to understand the IACS Security Lifecycles, we must first understand the ISA/IEC 62443 Series of standards upon which they are based. The following topics are excerpts from *Quick Start Guide: An Overview of ISA/IEC 62443 Standards* [16] that provides a user-friendly high-level description of the ISA/IEC 62443 Series of Standards. The Quick Start Guide can be found at: **http://www.isa.org/cyberguide**

Summary

Figure 2 shows the 62433 standards and technical reports arranged in four groups, corresponding to the primary focus and intended audience [19].

1. **General** – This group includes documents that address topics that are common to the entire series.

Table of Contents

Table of Figures

- **Part 1-1: Terminology, concepts and models** introduces the terminology, concepts and models used throughout the series. The intended audience includes anyone wishing to become familiar with the fundamental concepts that form the basis for the series.
- **Part 1-2: Master glossary of terms and definitions** is a list of terms and abbreviations used throughout the series. The master glossary will likely be delivered in an online format.
- **Part 1-3: System security conformance metrics** describes a methodology to develop quantitative metrics derived from the process and technical requirements in the standards.
- **Part 1-4: IACS security lifecycle and use cases** provides a more detailed description of the underlying lifecycle for IACS security, as well as several use cases that illustrate various applications.

2. **Policies and Procedures** – Documents in this group focus on the policies and procedures associated with IACS security.
   - **Part 2-1: Establishing an IACS security program** describes what is required to define and implement an effective IACS Security Program. The intended audience includes asset owners who have responsibility for the design and implementation of such a program.
   - **Part 2-2: Security Program Ratings** provides a methodology for evaluating the level of protection provided by an operational IACS against the requirements in the ISA/IEC 62443 Series of standards.
   - **Part 2-3: Patch management in the IACS environment** provides guidance on patch management for IACS. The intended audience includes anyone who has responsibility for the design and implementation of a patch management program.
   - **Part 2-4: Security Program requirements for IACS service providers** specifies requirements for IACS service providers such as system integrators or maintenance providers.
   - **Part 2-5: Implementation guidance for IACS asset owners** provides guidance on what is required to operate an effective IACS Security Program. The intended audience includes asset owners who have responsibility for the operation of such a program.

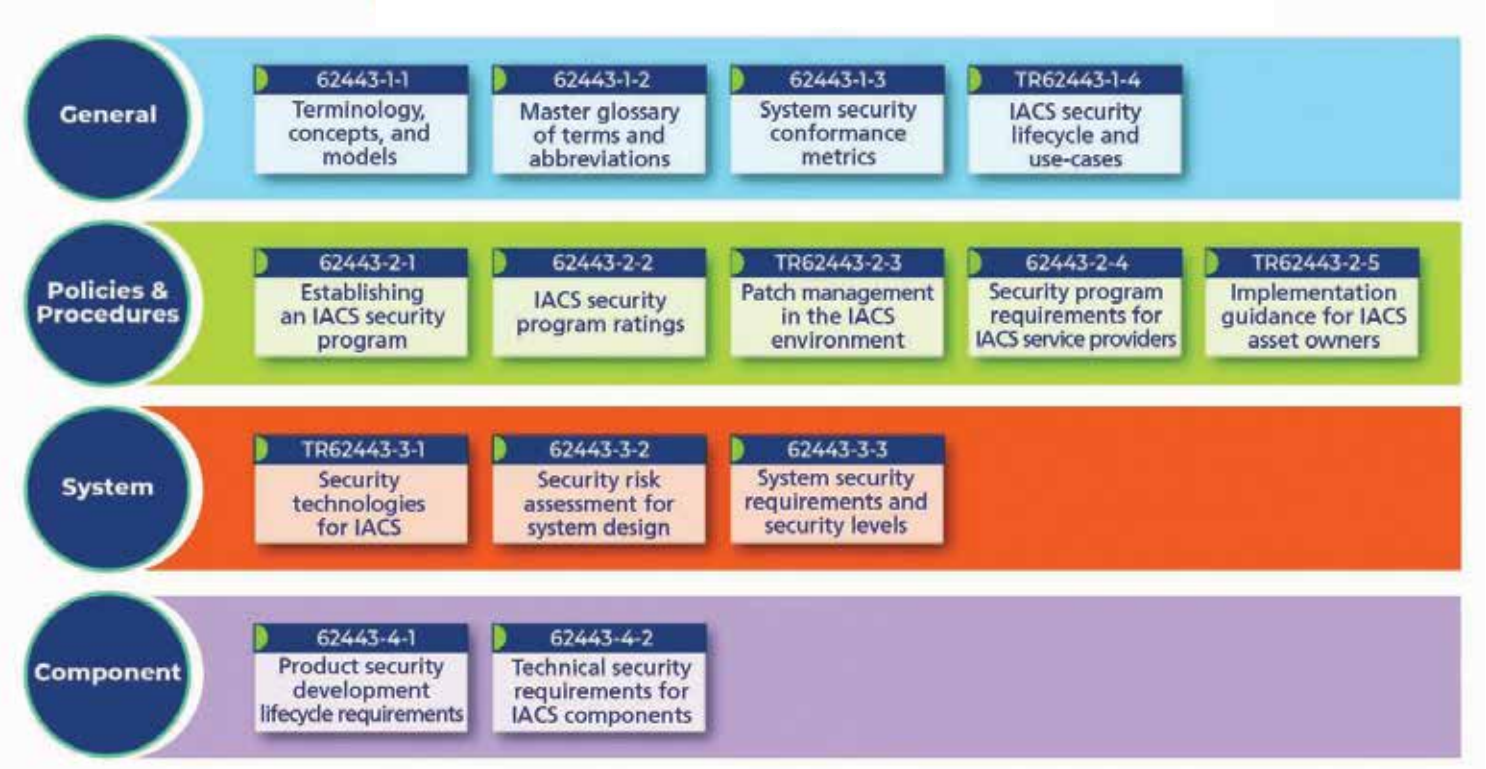


Figure 2 – ISA/IEC 62443 Series

3. **System Requirements** – The documents in the third group address requirements at the system level.
   - **Part 3-1: Security technologies for IACS** describes the application of various security technologies to an IACS environment. The intended audience includes anyone who wishes to learn more about the applicability of specific technologies in a control systems environment.
   - **Part 3-2: Security risk assessment for system design** addresses cybersecurity risk assessment and system design for IACS. The output of this standard is a Zone and Conduit model and associated Risk Assessments and Target Security Levels. These are documented in the Cybersecurity Requirements Specification. This standard is primarily directed at asset owners and system integrators.
   - **Part 3-3: System security requirements and security levels** describes the requirements for an IACS system based on security level. The principal audience include suppliers of control systems, system integrators, and asset owners.

4. **Component Requirements** – The fourth and final group includes documents that provide information about the more specific and detailed requirements associated with the development of IACS products.
   - **Part 4-1: Secure Product development lifecycle requirements** describes the requirements for a product developer's security lifecycle. The principal audience include suppliers of Control System and Component products.
   - **Part 4-2: Technical security requirement for IACS components** describes the requirements for IACS Components based on security level. Components include Embedded Devices, Host Devices, Network Devices and Software Applications. The principal audience include suppliers of Component products that are used in control systems.

Figure 3 shows the complete list of ISA/IEC 62443 standards and technical reports. The Part can be derived from the document number; for example, ISA/IEC 62443-2-1 is referred to as Part 2-1 in this document.

Part	Type	Title	Date
General			
1-1	TS	Terminology, Concepts, and Models	2007
1-2	TR	Master glossary of terms and abbreviations	
1-3		System cybersecurity conformance metrics	
1-4		IACS security lifecycle and use cases	
Policies & Procedures			
2-1	IS	Establishing an IACS security program	2009
2-2		IACS security program ratings	
2-3	TR	Patch management in the IACS environment	2015
2-4	IS	Security program requirements for IACS service providers	2018
2-5	TR	Implementation guidance for IACS asset owners	
System			
3-1	TR	Security technologies for IACS	
3-2	IS	Security risk assessment for system design	2020
3-3	IS	System security requirements and security levels	2013
Component			
4-1	IS	Product security development life-cycle requirements	2018
4-2	IS	Technical security requirements for IACS components	2019

Figure 3 – ISA/IEC 62443 Series Status

The document types are:
- IS – International Standard
- TR – Technical Report
- TS – Technical Specification

Finally, the publication date is shown for each document as of the publication date of this document. ISA/IEC standards are on a five-year update cycle, so many of the published documents are currently in revision. Documents where the date is blank have not been published yet. Documents where the type cell is blank have not been determined yet.

Hierarchical View

Figure 4 shows the hierarchical relationship between ISA/IEC 62443 Series standards. A hierarchical relationship means that one standard derives its requirements from the requirements in another standard. The arrowhead shows the direction of derivation.

- **Part 1-1** introduces the concepts and models that are used throughout the ISA/IEC 62443 Series.
- **Part 2-1** sets the requirements for the Security Program of an Asset Owner. The other standards in the ISA/IEC 62443 Series derive their requirements from Part 2-1 and expand upon them in more detail.

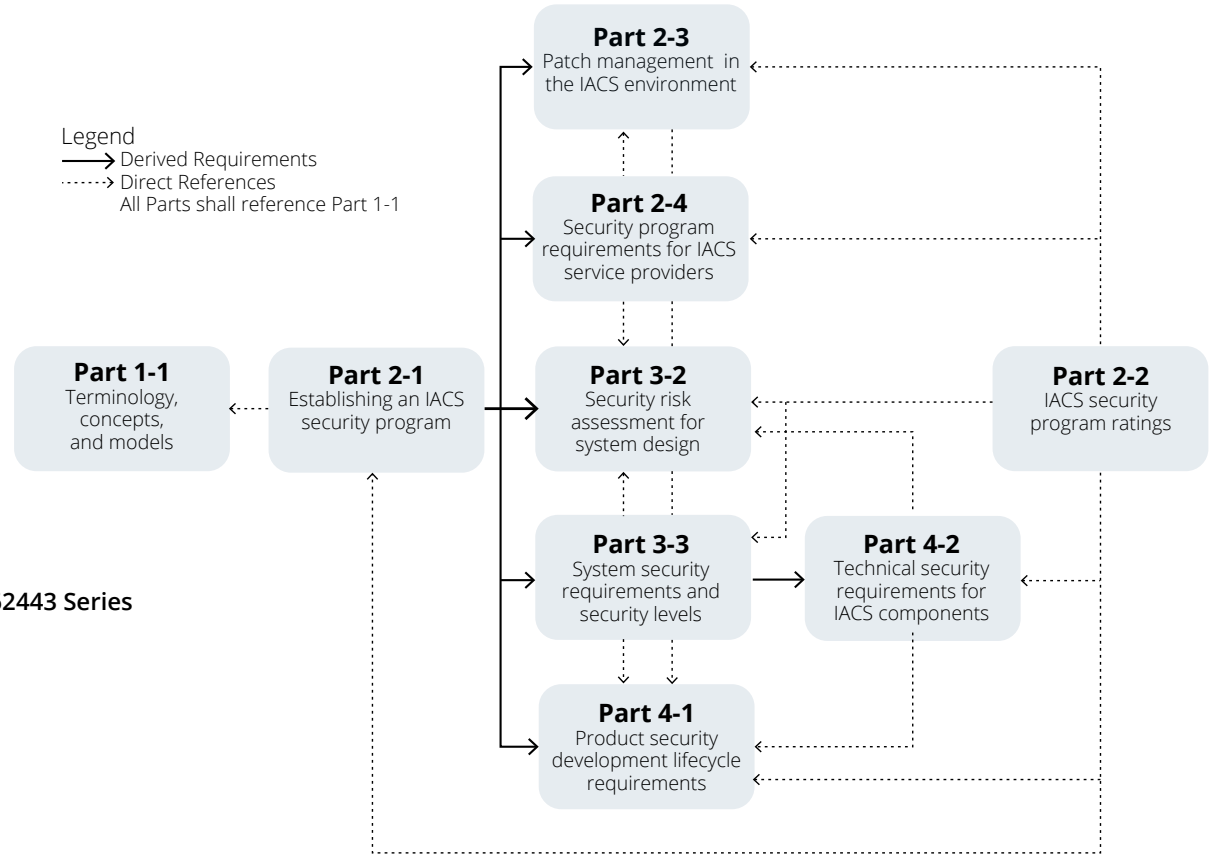


Figure 4 – ISA/IEC 62443 Series Hierarchical View

- **Part 2-2** refers to the other standards in the 62443 series to create an assessment methodology for an IACS in operation.
- **Part 2-3** sets the requirements for the patch management process, which is used to reduce cybersecurity vulnerabilities in the Automation Solution.
- **Part 2-4** sets the requirements for Service Providers that are involved in support of the IACS. Integration Service Providers provide integration services for the Automation Solution, and Maintenance Service Providers provide maintenance services for the IACS.
- **Part 3-2** sets the requirements for the partitioning of the System Under Consideration into Zones and Conduits and their Risk Assessment. The risk assessment defines the Target Security Level (SL-T) which is used to procure Systems and Components that have the capabilities defined in Part 3-3 and Part 4-2 respectively. Part 3-2 also requires a Cybersecurity Requirements Specification, which is used to create the Automation Solution.
- **Part 3-3** sets the technical requirements for IACS Systems based on capability security levels.
- **Part 4-1** is used by the Product Supplier to establish and sustain a Security Lifecycle, which is used to create Control System and Component products.
- **Part 4-2** sets the technical requirements for IACS Components based on capability security levels.

Lifecycle View

Another view of the ISA/IEC 62443 Series is the lifecycle view. There are two independent lifecycles described in the series: the Product Security Lifecycle and the Automation Solution Security Lifecycle. The Automation Solution Security Lifecycle is further divided into an Integration Phase and an Operation and Maintenance Phase. Figure 5 shows the relationship between the Parts of the ISA/IEC 62443 Series and the various lifecycles and phases.

Note that Part 3-3 spans the Product Security Lifecycle and the Automation Solution Security Lifecycle. Part 3-3 describes the technical requirements for IACS systems and is used by the Product Supplier to develop systems, the Integration Service Provider to integrate systems into an Automation Solution, and the Asset

Product Security Lifecycle	Automation Solution Security Lifecycle						
	Integration				Operation and Maintenance		
	Specify	Design	Implement	Verify & Validate	Operate	Maintain	Decommission
Part 1-1: Terminology, Concepts, and Models							
	Part 2-1: Establishing an IACS Security Program						
	Part 2-2: IACS Security Program Rating						
	Part 2-3: Patch Management in the IACS Environment						
	Part 2-4: Security Program Requirements for IACS Service Providers						
	Part 3-2: Security Risk Assessment for System Design						
Part 3-3: System Security Requirements and Security Levels							
Part 4-1: Product Security Development Lifecycle Requirements							
Part 4-2: Technical Security Requirements for IACs Components							

Figure 5 – ISA/IEC 62443 Series Lifecycle View

Owner to assess the technical security measures of the IACS throughout the Automation Solution Security Lifecycle.

Key Concepts

Principal Roles

To understand how to use the ISA/IEC 62443 Series, it is first necessary to understand the relationship between Roles, Control System, Automation Solution, and IACS. Figure 6 visualizes this relationship.

The left-hand side of Figure 6 shows the roles that are identified in the ISA/IEC 62443 Series:

- ***Asset Owner*** is accountable and responsible for the IACS. The Asset Owner is also the operator of the IACS and the Equipment Under Control.
- ***Maintenance Service Provider*** provides support activities for an Automation Solution.
- ***Integration Service Provider*** provides integration activities for an Automation Solution including design, installation, configuration, testing, commissioning, and handover to the Asset Owner. The Integration Service Provider may also facilitate and assist in the activity to partition the System Under Consideration into Zones and Conduits and perform the Risk Assessment.
- ***Product Supplier*** manufactures and supports a hardware and/or software product. Products may include Control Systems, Embedded Devices, Host Devices, Network Devices, and/or Software Applications.

It is important to understand that a role is not necessarily an organization. An organization can have multiple roles, and the responsibilities for a particular role can be split among multiple organizations. For example, an Asset Owner organization can have the Operations role and all or part of the Maintenance Service Provider role. It is also not uncommon that a Product Supplier organization has the Product Supplier role, the Integration Service Provider role and portions of

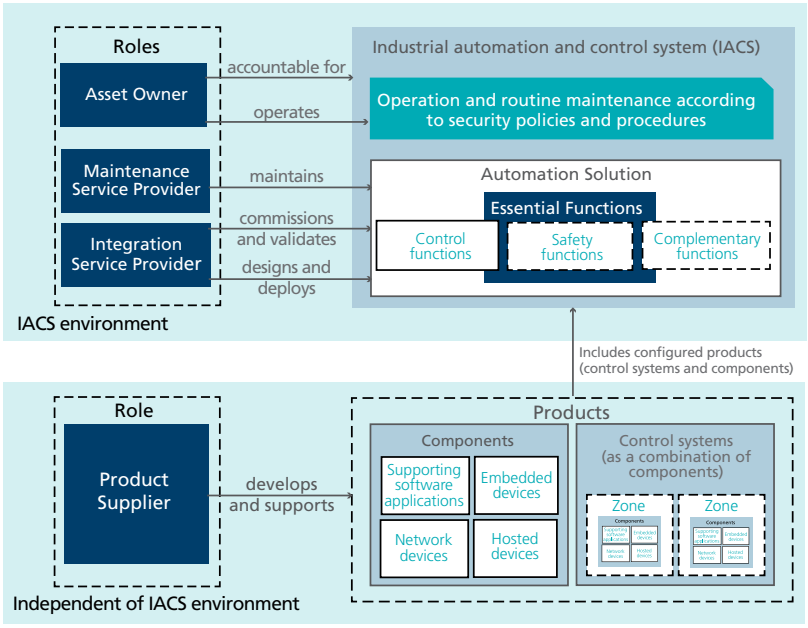


Figure 6 – IACS Principal Roles and Responsibilities

the Maintenance Service Provider role. Finally, while all or part of the responsibilities in a role can be delegated to other organizations, the accountability for the IACS must remain with the Asset Owner organization.

IACS and Automation Solution

The right-hand side of Figure 6 shows the types of systems that are identified in the ISA/IEC 62443 Series:

- ***IACS Components*** are provided by a *Product Supplier* and include the following types:
  - *Embedded device* – special purpose device designed to directly monitor or control an industrial process
  - *Host device* – general purpose device running an operating system capable of hosting one or more software applications, data stores or functions from one or more suppliers
  - *Network device* – device that facilitates data flow between devices, or restricts the data flow, but may not directly interact with a control process
  - *Software application* – one or more software programs and their dependencies that are used to interface with the process or the control system itself

  Note that a single device may include functions for more than one component type.
- ***IACS System (or Control System)*** consists of an integrated set of Embedded Devices (e.g. PLC), Host Devices, Network Devices, and Software Applications that is provided by one or more Product Suppliers.
- ***Automation Solution*** is the realization of one or more Control Systems at a particular facility. It includes essential functions such as safety functions and control functions and other supporting functions such as historization and engineering. The *Automation Solution* is portioned into Zones and Conduits as part of the risk assessment process.
- ***The Industrial Automation and Control System (IACS)*** includes the Automation Solution and the organizational security measures for its operation and maintenance.

Figure 7 shows a visualization of the taxonomy for the term Industrial Automation and Control System (IACS).

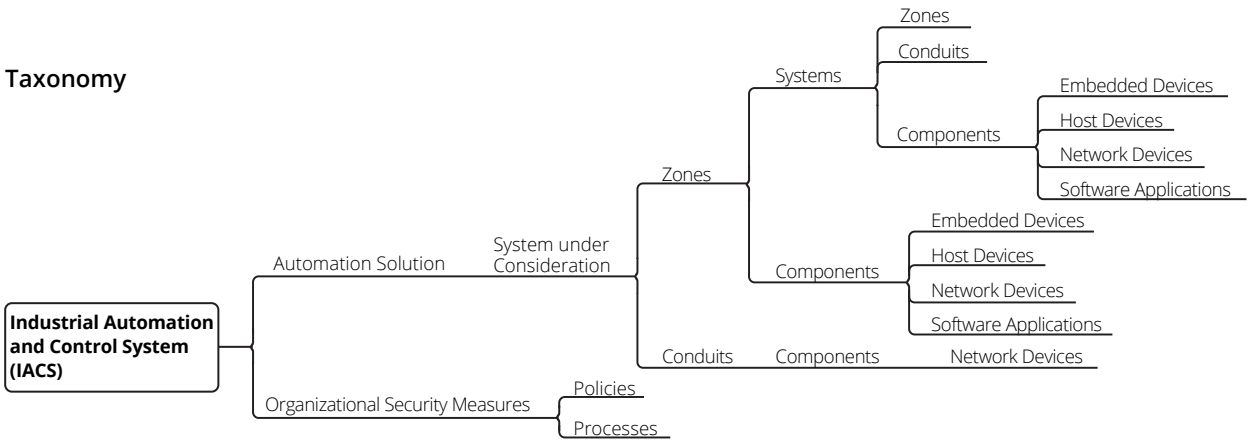
Security Program

Part 2-1 specifies Asset Owner Security Program requirements for the IACS. A Security Program consists of the implementation and maintenance of personnel, policy, & procedural and technology-based capabilities that reduce the cybersecurity risk of an IACS.

In the context of Part 2-1, the Asset Owner is also the Operator of the IACS and the Equipment Under Control (the process equipment or manufacturing equipment being controlled by the IACS). The Security Program covers the entire lifecycle of the IACS. Because the lifetime of an IACS can be longer than the product supplier support timeframe, the standard recognizes that not all requirements can be met by legacy systems, so compensating security measures may be needed to secure the IACS.

Although the Asset Owner is ultimately accountable for the secure operation of the IACS, implementation of security capabilities requires the support of product suppliers and service providers.

Figure 7 – IACS Taxonomy



The Asset Owner must include requirements for security throughout the supply chain to meet the overall Security Program requirements.

The Security Program for the IACS must be coordinated with the overall Information Security Management System (ISMS) of the organization. The ISMS sets the overall security governance and policies for the organization. However, the IACS is significantly different from IT systems, so there are additional requirements and considerations for its Security Program.

Risk Assessment

Part 3-2 describes the requirements for addressing the cybersecurity risks in an IACS, including the use of Zones and Conduits, and Security Levels. While Part 3-2 includes the requirements for the risk assessment process, it does not specify the exact methodology to be used. The methodology used must be established by the Asset Owner and should be consistent with the overall risk assessment methodology of the organization. Examples using the risk matrix methodology are included as informative content. Figure 8 shows the risk assessment process.

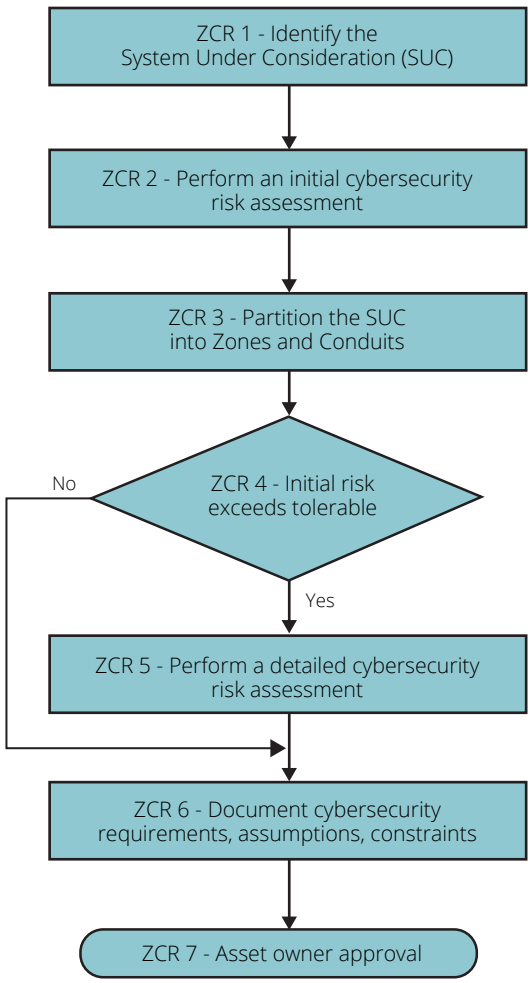


Figure 8 – Risk Assessment Process

Zones and Conduits

A Zone is defined as *a grouping of logical or physical assets based upon risk or other criteria such as criticality of assets, operational function, physical or logical location, required access or responsible organization.*

A Conduit is defined as *a logical grouping of communication channels that share common security requirements connecting two or more zones.*

A key step in the Risk Assessment process is to partition the System Under Consideration into separate Zones and Conduits. The intent is to identify those assets which share common security characteristics in order to establish a set of common security requirements that reduce cybersecurity risk.

Partitioning the System Under Consideration into Zones and Conduits can also reduce overall risk by limiting the scope of a successful cyberattack. Part 3-2 requires or recommends that some assets are partitioned as follows:

- Shall separate business and control system assets
- Shall separate safety related assets from non-safety related assets
- Should separate temporarily connected devices
- Should separate wireless devices
- Should separate devices connected via external networks

Security Measure

The concept of *security measures* is central to understanding the ISA/IEC 62443 series.

> *A security measure is an action, device, procedure, or technique that reduces a threat, a vulnerability or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken.*

Other terms used interchangeably for *security measure* are *security control* or *countermeasure.*

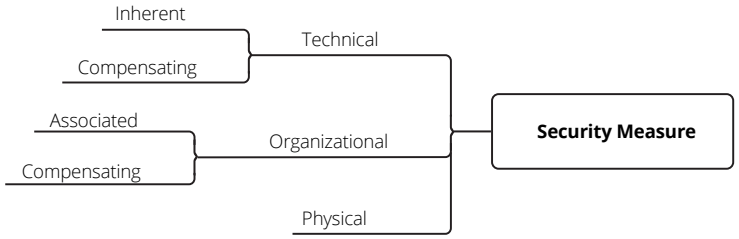


Figure 9 – Security Measure Taxonomy

The taxonomy for *security measure* is shown in Figure 9. There are three types of security measures:

- ***Technical security measures*** are implemented in IACS hardware and software and typically execute without human intervention
- ***Organizational security measures*** involve a person that executes one or more processes (policies and procedures)
- ***Physical security measures*** restrict physical access to IACS Systems and Components through security measures such as locked doors or cabinets

There is a second level of granularity to the taxonomy of *security measure:*

- An ***inherent*** technical security measure is a technical capability that is incorporated in or native to an IACS System or Component. An example would be role-based access control which is incorporated into an IACS System.
- An ***associated*** organizational security measure is a process (policy or procedure) that is necessary to securely implement a technical security measure. An example would be a process to add a new account or reset the password of an account for a role-based access control ***technical security measure***.
- A ***compensating*** security measure is a security measure in lieu of or in addition to ***inherent*** or ***associated*** security measures that is required to meet the overall target security requirement. An example of a ***compensating technical security measure*** would be a logical access point (e.g. firewall) that is added to restrict access to vulnerable communication protocols on an IACS network. An example of a ***compensating organizational security measure*** would be a process to scan removable media devices before use in an IACS System or Component that has no other means to prevent the execution of malware.

Security Level

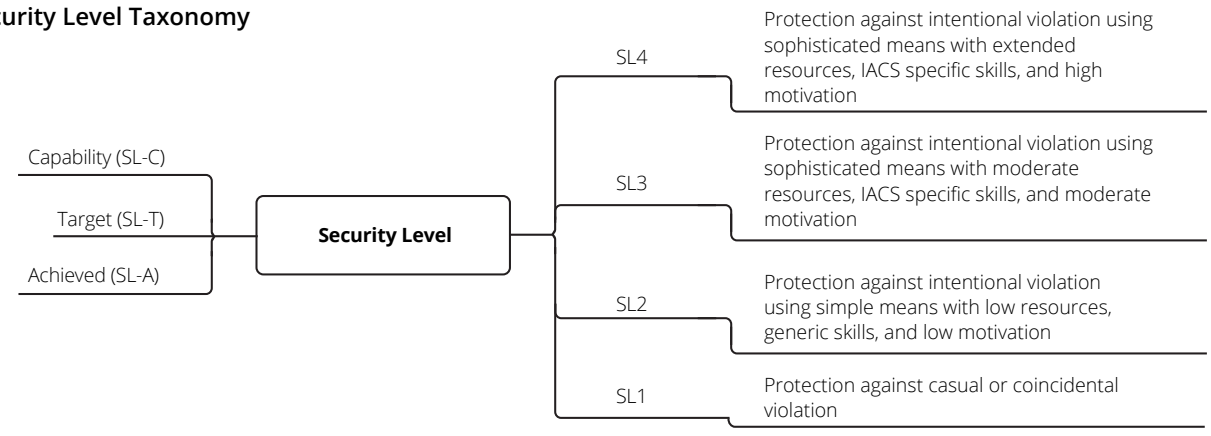
Security Level is defined as t*he measure of confidence that the System Under Consideration, Zone* or *Conduit is free from vulnerabilities and functions in the intended manner.*

Part 3-3 further defines the Security Level in terms of the means, resources, skills, and motivation of the threat actor, as shown in Figure 10. It is used as a means to discriminate between requirement enhancements for systems (Part 3-3) and Components (Part 4-2).

There are three types of Security Levels that are used throughout the ISA/IEC 62443 Series:

- ***Capability Security Levels (SL-C)*** are the security levels that Systems (Part 3-3) or Components (Part 4-2) can provide when properly integrated and configured. These levels state that a particular System or Component is capable of meeting the SL-T

Figure 10 – Security Level Taxonomy



natively without additional compensating security measures.

- ***Target Security Levels (SL-T)*** are the desired level of security for a particular Automation Solution. They are determined as the result of the Risk Assessment process (Part 3-2) and are documented in the Cybersecurity Requirements Specification. SL-T are used to select products and design compensating security measures during the Integration phase of the Automation Solution Security Lifecycle.
- ***Achieved Security Levels (SL-A)*** are the actual levels of security for a particular Automation Solution. These are measured after the Automation Solution is commissioned and in operation.

Maturity Level

While Security Levels are a measure of the strength of technical security measures, Maturity Levels are a measure of organizational security measures (people, policies, and procedures).

A Maturity Level is defined as the *degree to which a procedural capability (a process) is performed, formalized, practiced, and optimized.* Figure 11 shows the taxonomy of the term Maturity Level.

Parts 2-1, 2-2, 2-4 and 4-1 use Maturity Levels to measure how thoroughly security requirements are met and maintained.

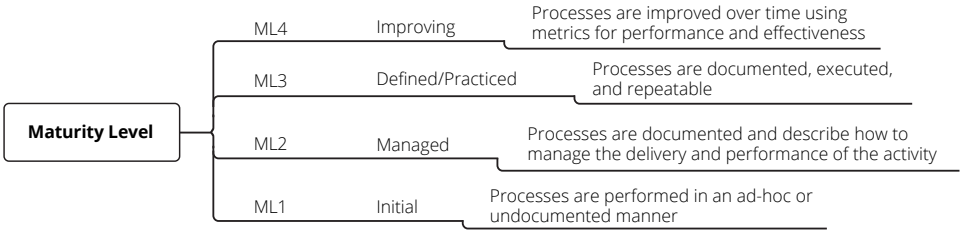


Figure 11 – Maturity Level Taxonomy

IACS Security Lifecycles

Product Security Lifecycle

Part 4-1 defines the security requirements for the Security Lifecycle of IACS System and Component product development and support. Part 4-1 describes process security requirements (e.g., policies and procedures) rather than technical security requirements.

Part 4-1 uses a Maturity Model, based on Capability Maturity Model Integration for Development (CMMI-DEV) [22], to define Maturity Levels that are used to assess the level of rigor used to develop products.

The technical security requirements for IACS Systems and Components are specified in Part 3-3 for IACS Systems [7] and Part 4-2 for IACS Components [9]. These requirements allow the Product Supplier to deliver and support a product that has the capability to meet the technical security requirements for a specified Security Level-Capability (SL-C).

Figure 12 shows the 8 security practices that are included in the IACS Product Security Lifecyle:

- Security management
- Specification of security requirements
- Secure by design
- Secure implementation
- Security verification and validation testing
- Management of security-related issues
- Security update management, and
- Security guidelines

Practice	Title	Requirements
1	Security management (SM)	13
2	Specification of security requirements (SR)	5
3	Secure by design (SD)	4
4	Secure implementation (SI)	2
5	Security verification and validation testing (SW)	5
6	Management of security-related issues (DM)	6
7	Security update management (SUM)	5
8	Security guidelines (SG)	7

Figure 12 – IACS Product Security Lifecycle Practices

Security management (SM)

The processes in the *security management practice* are intended to ensure that the security-related activities are adequately planned, documented and executed throughout the product's lifecycle.

Security management practice requirements include the following processes:

1. Development process
2. Identification of responsibilities
3. Identification of applicability
4. Security expertise
5. Process scoping
6. File integrity
7. Development environment security
8. Controls for private keys
9. Security requirements for externally provided components
10. Custom developed components from 3rd party suppliers
11. Assessing and addressing security-related issues
12. Process verification
13. Continuous improvement

Specification of security requirements (SR)

The processes in the *specification of security requirements practice* are intended to define and document the security capabilities of the product and the expected product security context. The technical security capabilities of the product are defined in Part 3-3 for Systems and Part 4-2 for Components. The product security context describes the expectations and assumptions about the security environment where the product is used, including threats, risks, and additional compensating security measures.

Specification of security requirements practice requirements include the following processes:

1. Product security context
2. Threat model
3. Product security requirements
4. Product security requirements content
5. Security requirements review

Secure by design (SD)

The processes in the *secure by design practice* are intended to ensure that the appropriate security considerations have been included throughout the specification and design phases of product development. The *secure by design practice* is based on the defense in depth strategy, which provides multiple layers of security to thwart security threats.

Secure by design practice requirements include the following processes:

1. Secure design principles
2. Defense in depth design
3. Security design review
4. Secure design best practices

Secure implementation (SI)

The processes specified in the *secure implementation practice* are intended to ensure that product functionality and security measures are implemented securely.

Secure implementation practice requirements include the following processes:

1. Security implementation review
2. Secure coding standards

Security verification & validation testing (SVV)

The processes specified in the *security verification & validation testing practice* are intended to ensure that the security requirements have been met for the product, and security of the product is maintained when it is used in its security context and configured according to the defense in depth strategy.

Security verification & validation testing practice requirements include the following processes:

1. Security requirements testing
2. Threat mitigation testing
3. Vulnerability testing
4. Penetration testing
5. Independence of testers

Management of security-related issues (DM)

The processes specified in the *management of security-related issues practice* are used for handling security-related issues of a product that has been configured to employ its defense in depth strategy within the product security context.

Management of security-related issues practice requirements include the following processes:

1. Receiving notifications of security-related issues
2. Reviewing security-related issues
3. Assessing security-related issues
4. Addressing security-related issues
5. Disclosing security-related issues
6. Periodic review of security defect management practice

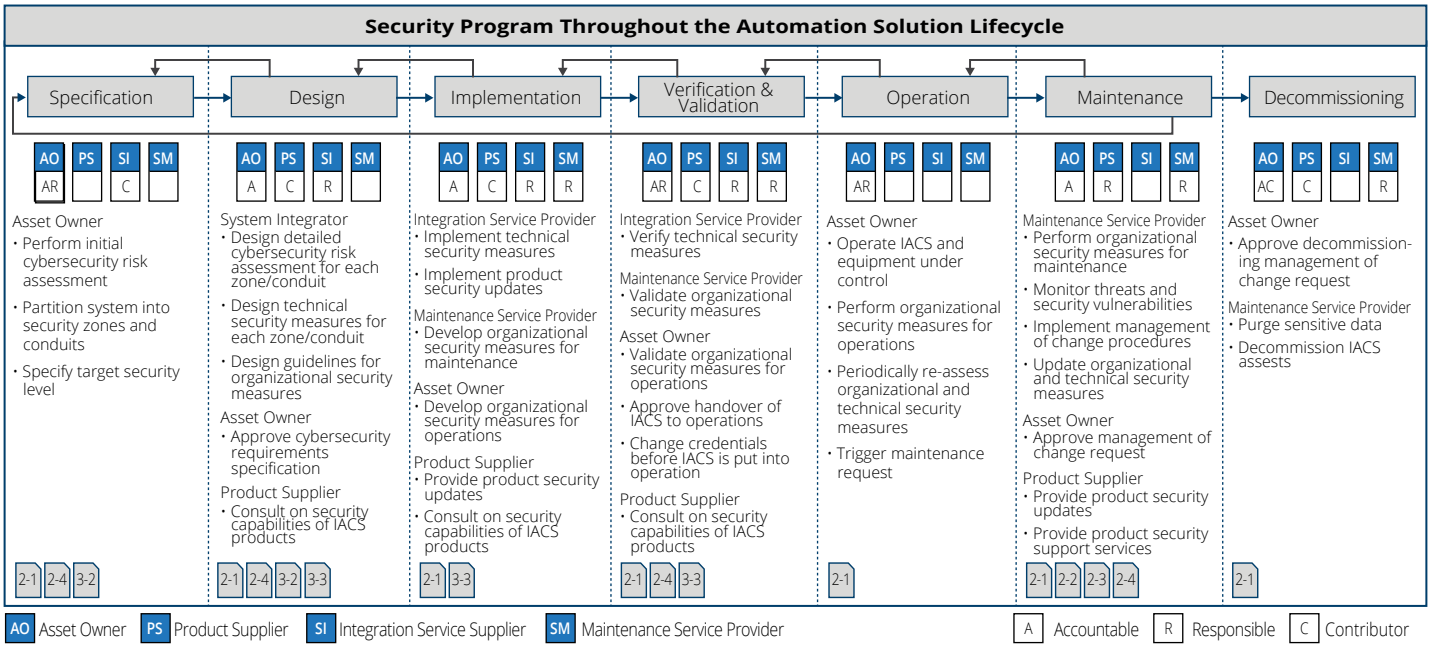


Figure 13 – IACS Automation Solution Security Lifecycle

Security update management (SUM)

The processes specified in the *security update management practice* are intended to ensure security updates (hardware, software, firmware) associated with the product are tested for regressions and made available to product users in a timely manner.

Security update management practice requirements include the following processes:

1. Security update qualification
2. Security update documentation
3. Dependent component or operating system update documentation
4. Security update delivery
5. Timely delivery of security patches

Security guidelines (SG)

The processes specified in the *security guidelines practice* are intended to provide user documentation that describes how to integrate, configure, and maintain the defense in depth strategy of the product in accordance with its product security context.

Security guidelines practice requirements includes the following processes:

1. Product defense in depth
2. Defense in depth measures expected in the environment
3. Security hardening guidelines
4. Secure disposal guidelines
5. Secure operation guidelines
6. Account management guidelines
7. Documentation review

Automation Solution Security Lifecycle

The Automation Solution Security Lifecycle is shown in Figure 13 and is currently documented in ISA/IEC-62443-2-2 Annex A (draft). It is based on the system lifecycle from *ISO/IEC/IEEE 24748-1 – Systems and software engineering – Lifecycle management Part 1: Guidelines for lifecycle management [12].*

Security Program

Before the Automation Solution Security Lifecycle begins, the Asset Owner must first establish the IACS Security Program for the organization. The security requirements for an Asset Owner Security Program is specified in Part 2-1 [2] and is based on the overall security policies of the organization with consideration for the security requirements of IACS. IACS-specific security policies for the organization include, but are not limited to:

- Establishing the roles and responsibilities for Product Suppliers and Service Providers

- A risk assessment methodology that is based on the organization's risk assessment methodology and includes the consequences for an IACS failure or compromise
- The minimum set of technical and organizational security measures for IACS across the organization
- The use of IACS-specific standards and practices such as ISA/IEC 62443
- The use of IACS-specific certifications such as ISASecure®

IACS-specific Security Program policies for the organization are typically documented in an organization's standards and practices, project-specific specifications, and contractual agreements with product suppliers and service providers.

Specification

The *Specification Phase* of the Automation Solution Security Lifecycle is documented in *Part 3-2 Security risk assessment for system design [6]* clauses ZCR 1 through 3 as shown in Figure 8. This phase of the lifecycle includes identifying the System Under Consideration, performing an initial high-level risk assessment, and partitioning the System into security zones and conduits. The result of this process is the Target Security Levels for each Zone and Conduit in the System Under Consideration.

Roles and Responsibilities:
- Asset Owner is accountable and responsible
- Integration Service Provider is consulted

Key activities:
- Perform initial cybersecurity risk assessment
- Partition the System Under Consideration into Zones and Conduits
- Specify the Target Security Level used for the Design phase

Design

The *Design Phase* of the Automation Solution Security Lifecycle is documented in *Part 3-2 Security risk assessment for system design [6]* clauses ZCR 4 through 7 as shown in Figure 8. This phase of the lifecycle is the detailed design of the System Under Consideration and includes for each Zone and Conduit:
- the *technical security measures* based on the Security Level from Part 3-3 System security requirements and Security Levels [7]
- the *organizational security measures* that are *associated with* the selected technical security measures
- additional *compensating* technical and organizational security measures

The key deliverable from the Design Phase is the *Cybersecurity Requirements Specification*, which must be approved by the Asset Owner before the Implementation Phase can start.

Roles and Responsibilities:
- Asset Owner is accountable
- Integration Service Provider is responsible
- Product Supplier is consulted

Key activities:
- Perform detailed cybersecurity risk assessment for each Zone and Conduit
- Design technical security measures based on the Target Security Level for each Zone and Conduit
- Design guidelines for the development of Organizational Security Measures
- Approval of the Cybersecurity Requirements Specification

Implementation

The *Implementation Phase* of the Automation Solution Security Lifecycle is when the technical security measures that are specified in the Cybersecurity Requirements Specification are implemented in the Automation Solution. In this Phase, the organizational security measures required for the *Operations Phase* and the *Maintenance Phase* are developed so that they are available during the *Verification & Validation Phase.*

It is important that the security of the Automation Solution is maintained during the *Implementation Phase* by the Integration Service Provider. This includes, but is not limited to, maintaining physical and logic access controls, installing product security updates in a timely manner, data confidentiality, and protecting against malware. Refer to *Part 2-4 Security program requirements for IACS service providers [4]* for additional security requirements.

Roles and responsibilities:
- Asset Owner is accountable
- Integration Service Provider is responsible for technical security measures
- Maintenance Service Providers are

responsible for organizational security measures for maintenance
- Asset Owner is responsible for organizational security measures for operations

Key activities:
- Implement technical security measures based on Target Security Level
- Implement product security updates during the integration phase
- Develop organizational security measures for maintenance phase
- Develop organizational security measures for operations phase

Verification & Validation

The *Verification & Validation Phase* of the Automation Solution Lifecycle is when the Automation Solution is tested to ensure that the technical and organizational security measures meet the security requirements specified in the Cybersecurity Requirements Specification. In some industry sectors these tests are called *Factory Acceptance Tests (FAT)* or *Site Acceptance Tests (SAT).* Examples of security-related tests in this phase include vulnerability scans, penetration tests, intrusion detection tests and access control tests. Part 2-2 can be used to determine the Security Program Rating – Capability (SPR-C) before the Automation Solution is put into operation.

The last step in the Verification & Validation Phase is the formal handover of the Automation Solution to the Asset Owner. Immediately after the handover, the Asset Owner is responsible for preparing the Automation Solution for the Operation Phase. Particular attention should be paid to changing the access controls (e.g., passwords, encryption keys) implemented by the Integration Service Provider or Product Supplier before placing the Automation Solution in service. This may be the last time that certain accounts/credentials for some essential functions can be changed before the Automation Solution is put in operation.

Roles and responsibilities:
- Asset Owner is accountable
- Integration Service Provider is responsible for implementing technical security measures
- Maintenance Service Providers are responsible for organizational security measures for maintenance
- Asset Owner is responsible for organizational security measures for operations

Key activities:
- Verify technical security measures
- Validate organizational security measures for operations
- Validate organizational security measures for maintenance

Handover to Operations
- Key activity at the end of the V&V phase
- Formal acceptance of the IACS by the Asset Owner
- Must change credentials (accounts, passwords, keys) before putting the IACS into operation

Operation

The *Operation Phase* of the Automation Solution Lifecycle is when the Automation Solution is placed into service and all of the organizational and technical security measures are executed. The organizational security measures, technical security measures, and associated IACS risk assessment must be periodically reviewed and updated.

Roles and Responsibilities:
- Asset Owner is accountable and responsible for Operations

Key activities:
- Operate the IACS and the Equipment Under Control
- Perform organizational security measures for operations, such as incident response and recovery
- Periodically re-assess the organizational and technical security measures
- Trigger maintenance requests

Maintenance

The *Maintenance Phase* of the Automation Solution Lifecycle is triggered by Operations requests or the monitoring of security threats and security vulnerabilities. Addressing security threats or vulnerabilities may require changes to the organizational or technical security measures of the IACS and must be implemented using a Management of Change process that includes risk assessment.

The security requirements for product updates to address security vulnerabilities is specified in Part 2-3: Patch management in the IACS environment. The patch management process involves the Asset Owner, Product Supplier and Maintenance Service Provider roles.

Roles and Responsibilities:
- Asset Owner is accountable
- Maintenance Service Provider responsible for organizational security measures for maintenance
- Product supplier is responsible for product support and security updates

Key activities:
- Perform organizational security measures for maintenance
- Monitor threats and security vulnerabilities
- Implement Management of Change procedures including reviewing risk assessments
- Update organizational and technical security measures

Decommissioning

The *Decommissioning Phase* of the Automation Solution Lifecycle can be triggered by a maintenance activity (e.g. replacing a hard drive) or by a major upgrade to the IACS. In either case, the decommissioning must be done in such a way that the Asset Owner's on-going operations are not compromised. A key activity in this phase is the destruction or purging of sensitive data.
Roles and Responsibilities:
- Asset Owner approves decommissioning Management of Change requests
- Maintenance Service Provider decommissions the assets

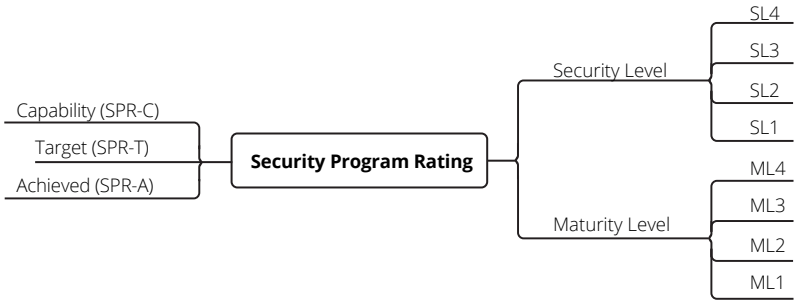


Figure 14 – Security Program Rating Taxonomy

Key activities:
- Purge sensitive data
- Decommission the IACS assets

Integrated Safety/Security Lifecycle

There is a joint working group between the ISA84 and ISA99 Committees that is working together to align the Safety Lifecycle described in *IEC 61511 Functional safety - Safety instrumented systems for the process industry sector [13]* and the security lifecycle described in various parts of *ISA/IEC 62443 Security for Industrial Automation and Control Systems.* The result of this work will be documented in a future edition of *ISA-TR84.00.09-2017,* Cybersecurity Related to *Functional Safety Lifecycle [14].*

IACS Assessment and Certification

Security Program Rating

ISA/IEC-62443-2-2 – Security for Industrial Automation and Control Systems – Part 2-2: IACS security program ratings (draft) specifies a methodology for the evaluation of security for each Zone in an IACS Automation Solution. Figure 14 shows the taxonomy for the Security Program Rating, which a combination of the Security Level of technical security measures, and the Maturity Level of organizational security measures.

Similar to Security Levels, there are three types of Security Program Ratings: Capability (SPR-C), Target (SPR-T), and Achieved (SPR-A). Capability and Target SPRs are used during the Specification, Design, Implementation, and Verification & Validation phases of the Automation Solution Security Lifecycle. Achieved SPR can only be determined during the Operation and Maintenance phases of the Lifecycle.

The Security Program Ratings for each security requirement in the overall IACS Security Program (as defined in Part 2-1) are evaluated to determine the overall effectiveness of the IACS Security Program.

ISASecure® Certification

The ISA Security Compliance Institute is a non-profit organization that has developed several product certification programs for Controls

Systems and Components. Currently available ISASecure® certification programs are:

- ***Security Development Lifecycle Assurance (SDLA)*** which certifies that the Security Lifecycle of a Product Supplier meets the requirements in Part 4-1.
- ***System Security Assurance (SSA)*** which certifies that Control System products have the capability to meet the requirements in Part 3-3 and have been developed in accordance with an SDLA program.
- ***Component Security Assurance (CSA)*** which certifies that Component products have the capability to meet the requirements in Part 4-2 and have been developed in accordance with an SDLA program. Certified Component products can be: Embedded Devices, Host Devices, Network Devices, and Software Applications.

ISASecure® certification programs can be found at ISASecure.org.

Figure 15 – ISASecure® Product Certifications

Other IACS Assessment Options

Other IACS assessment and certification options that are based on the ISA/IEC 62443 Series of standards include the following.

IECEE

IEC also offers a system of conformity assessment schemes called IECEE. IECEE currently offers conformance assessment schemes for the following IEC 62443 standards:

- IEC 62443-2-4:2015/AMD1:2017
- IEC 62443-3-3:2013
- IEC 62443-4-1:2018
- IEC 62443-4-2:2019

IECEE can be found at IECEE.org.

CISA CSET®

The Cyber Security Evaluation Tool (CSET®) is a desktop software tool developed by the US Cybersecurity & Infrastructure Security Agency (CISA) for the evaluation of an organization's security posture. The CSET® tool currently incorporates ISA/IEC 62443 Part 2-1 [2] and Part 3-3 [7].

Information about CSET® can be found at www.us-cert.gov/ics/Downloading-and-Installing-CSET.

Published Standards and Technical Reports

1. ISA-62443-1-1-2007 / IEC TS 62443-1-1:2009 – SECURITY FOR INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS, PART 1-1: TERMINOLOGY, CONCEPTS AND MODELS
2. ISA-62443-2-1-2009 / IEC 62443-2-1:2010 – SECURITY FOR INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS, PART 2-1: ESTABLISHING AN INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS SECURITY PROGRAM
3. ANSI/ISA-TR62443-2-3-2015 / IEC TR 62443-2-3:2015 – SECURITY FOR INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS, PART 2-3: PATCH MANAGEMENT IN THE IACS ENVIRONMENT
4. ANSI/ISA-62443-2-4-2018 / IEC 62443-2-4:2015+AMD1:2017 CSV – SECURITY FOR INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS, PART 2-4: SECURITY PROGRAM REQUIREMENTS FOR IACS SERVICE PROVIDERS
5. IEC TR 62443-3-1:2009 - SECURITY FOR INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS, PART 3-1: SECURITY TECHNOLOGIES FOR INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS
6. ISA-62443-3-2-2020 – SECURITY FOR INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS, PART 3-2: SECURITY RISK ASSESSMENT FOR SYSTEM DESIGN
7. ANSI/ISA-62443-3-3-2013 / IEC 62443-4-2:2013 – SECURITY FOR INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS, PART 3-3: SYSTEM SECURITY REQUIREMENTS AND SECURITY LEVELS
8. ANSI/ISA-62443-4-1-2018 / IEC 62443-4-1:2018 – SECURITY FOR INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS, PART 4-1: SECURE PRODUCT DEVELOPMENT LIFECYCLE REQUIREMENTS
9. ANSI/ISA-62443-4-2-2018 / IEC 62443-4-2:2019 – SECURITY FOR INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS, PART 4-2: TECHNICAL SECURITY REQUIREMENTS FOR IACS COMPONENTS
10. IEC TR 63069:2019 – INDUSTRIAL-PROCESS MEASUREMENT, CONTROL AND AUTOMATION – FRAMEWORK FOR FUNCTIONAL SAFETY AND SECURITY
11. IEC TR 63074:2019 – SAFETY OF MACHINERY – SECURITY ASPECTS RELATED TO FUNCTIONAL SAFETY OF SAFETY-RELATED CONTROL SYSTEMS
12. ISO/IEC/IEEE 24748-1 – SYSTEMS AND SOFTWARE ENGINEERING – LIFE CYCLE MANAGEMENT PART 1: GUIDELINES FOR LIFE CYCLE MANAGEMENT
13. ISA-84.00.01-2004 PART 1 / IEC 61511-1:2016 – FUNCTIONAL SAFETY – SAFETY INSTRUMENTED SYSTEMS FOR THE PROCESS INDUSTRY SECTOR – PART 1 FRAMEWORK, DEFINITIONS, SYSTEM, HARDWARE AND APPLICATION PROGRAMMING REQUIREMENTS
14. ISA-TR84.00.09-2017, CYBERSECURITY RELATED TO THE FUNCTIONAL SAFETY LIFECYCLE
15. IEC 61508 (ALL PARTS) – FUNCTIONAL SAFETY OF ELECTRICAL/ELECTRONIC/PROGRAMMABLE ELECTRONIC SAFETY-RELATED SYSTEMS

References

16. QUICK START GUIDE: AN OVERVIEW OF ISA/IEC 62443 STANDARDS, ISA GLOBAL CYBERSECURITY ALLIANCE, https://gca.isa.org/blog/download-the-new-guide-to-the-isa/iec-62443-cybersecurity-standards
17. NIST SP 800-82 REVISION 2, GUIDE TO INDUSTRIAL CONTROL SYSTEMS (ICS) SECURITY
18. THE 62443 SERIES OF STANDARDS: INDUSTRIAL AUTOMATION AND CONTROL SECURITY, ISA99 COMMITTEE
19. FREQUENTLY ASKED QUESTIONS: THE ISA99 COMMITTEE AND 62443 STANDARDS, ISA99 COMMITTEE
20. INSTRUMENTATION AND CONTROL SYSTEMS SECURITY EXPLAINED: THE WHAT AND THE WHY, ISA99 COMMITTEE
21. THE SECURITY DEVELOPMENT LIFE-CYCLE: SDL A PROCESS FOR DEVELOPING DEMONSTRABLY MORE SECURE SOFTWARE, HOWARD, MICHAEL AND LIPNER, STEVE, 2006, MICROSOFT PRESS
22. CAPABILITY MATURITY MODEL INTEGRATION, CMMI INSTITUTE, www.cmmiinstitute.com
23. ISA-62443-2-2: DC 3/2020 SECURITY FOR INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS, PART 2-2: IACS SECURITY PROGRAM RATINGS (DRAFT)