2 Cybersecurity involves process, people, and technology

It is commonly accepted that cybersecurity involves technical as well as organizational measures. Cybersecurity always relies on three legs: technology, process, and people. The activities and measures differ significantly if they are conducted for a site-specific automation project of an operating facility or if they are performed to improve the security capabilities of automation products.

Holistic security concept for products

For the product supplier the technology side of the triangle represents the security features of the products – components or systems – the supplier is delivering, see Figure 2.1. In general, products are specified to fulfill requirements of target markets to be served by these products; they are not dedicated to a specific customer-project. Product suppliers integrate security capabilities in their products which can be used in many different automation solutions. A common situation is that the same controller can be included in machine tools or in complex automation solutions, such as those typically deployed in the oil and gas industry.

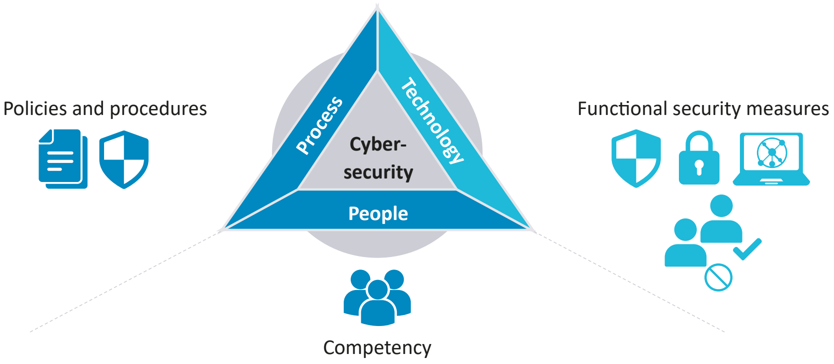


Figure 2.1 Cybersecurity involves technology, process, and people.

The “process” and “people” areas are addressing the necessity to integrate cybersecurity in all phases of the product lifecycle. The product supplier should establish a holistic security concept for its products. It includes to integrate cybersecurity in the typical phases of the product development process – specification, design, implementation and test – with the objective to avoid as much as possible the generation of vulnerabilities during the development activities. The product supplier should also offer a support during commercialization of the product, by providing guidelines supporting the secure use of the product, and by establishing processes for vulnerability management, incident handling, and patch / update management. Finally, a holistic security concept includes taking care of the integrity of the delivered products by protecting the development environment as well as the production facilities against manipulation of the onboard firmware and software.

Security protection scheme for operating facilities

In a site-specific environment, the standard IEC 62443 addresses the security measures of the so-called "Industrial Automation and Control System (IACS)". The term IACS includes all elements which are necessary to ensure a reliable and secure operation of an automated industrial equipment. An IACS consists basically of two complementary and matched parts, see Figure 2.2:

- a technical solution, the ***automation solution*** which is connected to the operating facility
- ***organizational measures*** to operate the IACS via the automation solution

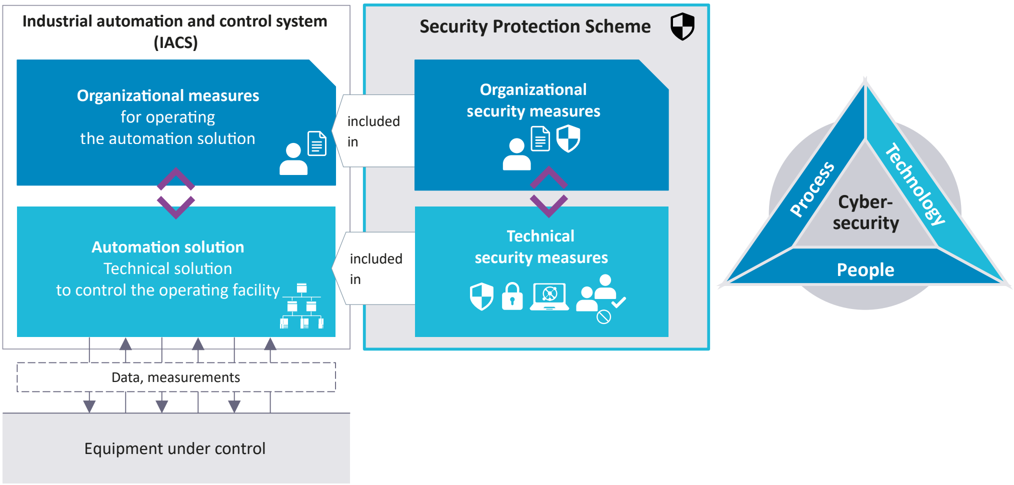

Industrial automation and control system (IACS)
Organizational measures for operating the automation solution
Automation solution Technical solution to control the operating facility
included in
included in
Data, measurements
Equipment under control
Security Protection Scheme
Organizational security measures
Technical security measures
Process
Technology
People
Cyber-security

Figure 2.2 Integration of a security protection scheme in an IACS

IACS control typically manufacturing lines, continuous processes, railway infrastructures, power distribution networks or automated building equipment. The automation solution exchanges signals and data with the equipment under control and consists of connected products to perform monitoring and controlling functions. Products can be hardware/ software components like controllers, firewalls, gateways, SCADA systems or PC-based host devices but also software components and applications. Products can also be systems, like control systems, machine controls or robot controls. They consist of connected components, which are combined to realize system functionalities.

In the environment of a specific operating facility, the cybersecurity activities have the purpose of implementing a security protection scheme for each IACS of the operating facility in order to prevent an intentional or unintentional misuse during operation.

> A **Security Protection Scheme (SPS)** is a set of technical and organizational security measures with the aim to protect an IACS against cyberthreats during operation.

The technology leg represents the technical security measures implemented in the automation solution. The aim is that the security capabilities of the automation solution allow to meet the desired security requirements, when the organizational security measures are practiced during operation. They are implemented by deploying and configuring the security capabilities of the products used in the automation solution. Additional compensating technical security measures may be necessary in order to meet the desired security requirements.

“Process” and “People” are about practicing organizational security measures during operation. They should be matched with the technical security measures and must be aligned with the capabilities provided by the automation solution.

The development of organizational security measures includes the generation of security policies and procedures, the definition of responsibility chains and escalation processes as well as the qualification of the personnel in charge. Compensating organizational security measures may be developed, if the security capabilities provided by the automation solution are not sufficient to meet the desired security requirements.

3 Roles and responsibilities in IEC 62443

The standard IEC 62443 is based on the fundamental understanding that the protection of an automated operating facility against intentional or unintentional violation needs a set of balanced security measures, which must be implemented by different involved actors. To be independent from any specific organizational structure or legal entities, the actors will be described in this book according to their roles.

A role is defined by responsibilities and/or accountabilities as well as associated activities to be fulfilled by an organization. An organization can be an individual, a legal entity, such as a company or government agency, or a subdivision of the legal entity, such as a department.

An organization can fulfill one or multiple roles. For example, it is not unusual that the same company is responsible for the operational activities as well as for the design, implementation and validation of an automation solution. On the other hand, a role can be fulfilled by one or several organizations. It is not unusual that the maintenance activities are performed by different organizations.

The implementation of a security protection scheme for an IACS requires the contribution and collaboration of all involved actors according to their designated role.

The role asset owner (AO) is accountable for the protection of the automated operating facility against cyberthreats and all associated risks throughout its lifecycle, see Figure 3.1. The AO defines the tolerable residual cybersecurity risk for each IACS and implements a security protection scheme according to this risk. Whilst remaining accountable, the organization fulfilling this role delegates many responsibilities and their associated activities to organizations fulfilling other roles. The second part assigned to the role AO, is the responsibility for the operational activities. Concerning cybersecurity, this part focusses on

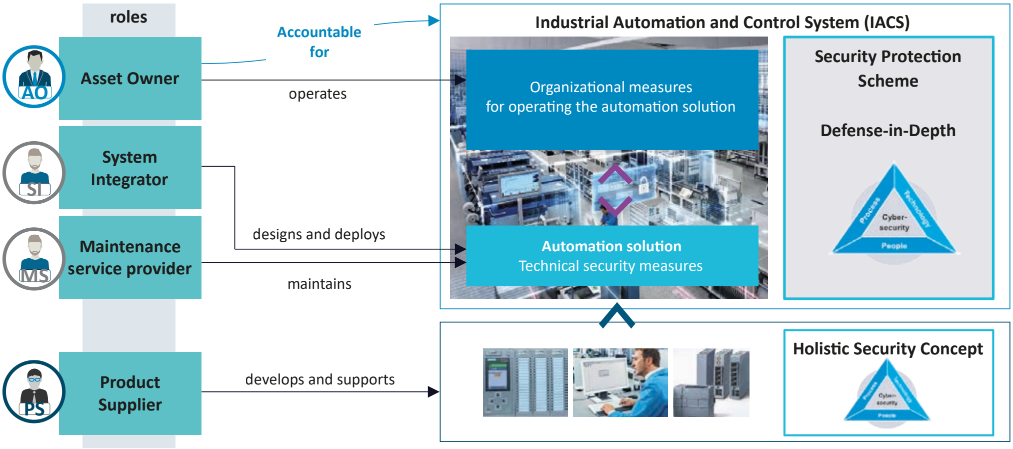


Figure 3.1 Principal roles in IEC 62443

the practice of the organizational security measures according to defined security policies and procedures. Combining these two parts in the role AO reflects that in many cases the organization which operates the operating facility is also the legal owner and is accountable for all risks associated with the operating facility.

The role integration service provider (SI) is responsible for the design and implementation as well as commissioning and validation of the technical security measures. The activities cover the development and validation of a security protection scheme, with the goal to match the tolerable residual cybersecurity risk defined by the AO. These include the development of technical security measures as well as generating recommendations for the organizational security measures to be practiced during operation. 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 activities.

The maintenance service provider (MS) is mainly responsible for eventually updating the security protection scheme during the operation phase. The updating activities have the purpose to eventually improving the measures of the security protection scheme, in case of a change in the threat situation or a modification of the automation solution. An update phase is triggered by the result of a cybersecurity risk assessment showing that the measures of the security protection scheme no longer provide the desired protection. In general, the improvements cover technical security measures implemented in the automation solution as well as the organizational security measures to be practiced during operation. The role MS also includes to ensure to match the tolerable residual cybersecurity risk during or after the decommissioning of parts or the whole automation solution.

The product supplier (PS) is responsible for the development and support of products used in the automation solution. The activities include the development of security capabilities following an established product development lifecycle process, including supplying integration, hardening, operational and decommissioning guidelines for the products used in the automation solution. The product supplier must also establish a process to support its customers if a vulnerability is discovered during the commercialization phase of the product.

Organizations fulfilling these roles can vary from one project to another, and the terms used for naming these organizations may be different in various market sectors, branches or countries, for example:

- Role AO: plant owner, regulator organization, operations department, operation service provider, etc.
- Role MS: maintenance department, technical service, etc.
- Role SI: plant setup and commissioning department, integrator, EPC company, machine builder, etc.
- Role PS: manufacturer, producer, OEM, etc.

4 Structure of IEC 62443

In this chapter, we will list the main documents which are relevant for the purpose of this book. We have intentionally left out the documents addressing the specification of profiles (part 1-5) and the evaluation methodologies (parts 6-1 and 6-2). The annexes provide an overview on the content and the status of the relevant documents of the series at the point of time of publication of this book*.

In the first block overall aspects like concepts, terminologies and methods are described in the part 1-1 and a glossary is given in part 1-2. The aim of part 1-3 is to provide possible key performance indicators for the evaluation of the efficiency of cybersecurity. In part 1-4 it is planned to describe use cases to support the implementation of cybersecurity along the IACS lifecycle.

The second block is dedicated to process requirements. Part 2-1 defines requirements to the security program (SP) of the asset owner (role AO). The security program is a set of security practices of the asset owner, having the purpose of ensuring that security protection schemes are developed and operated for all IACS in its operating facility. Part 2-2 describes the use of relevant parts of the series for the development, practice and maintenance of IACS security protection schemes. The document describes the cooperation of the various roles and the rating of the protection provided by the security protection scheme with so-called Security Protection Ratings (SPR). Part 2-3 contains recommendations for the qualification and deployment of patches during the operation phase, involving the principal roles. Part 2-4 addresses service providers for integration and maintenance (roles SI and MS), and includes requirements for applying security measures to automation solutions. It is planned to generate a part 2-5 containing recommendations for the implementation of security programs by asset owners.

The third block focusses on security measures for systems. Part 3-1 is a technical report on state-of-the-art technologies used against cyberthreats. Part 3-2 describes a risk-based approach for partitioning automation solutions in zones and conduits. The document describes process steps of a risk assessment, with the purpose of developing security measures for each zone and conduit fulfilling a desired set of security requirements. Part 3-3 specifies the requirements to security capabilities of systems. On the one hand, the document addresses capabilities of products like control systems or blueprints and is relevant for product suppliers (role PS) offering. On the other hand, the system security requirements of part 3-3 are the base for the design of technical security measures and are relevant for service providers for integration or maintenance (roles SI and MS), as well as for the asset owners (role AO) for IACS during operation, including the practice of organizational security measures.

The fourth block is relevant for product suppliers. Part 4-1 specifies the integration of cybersecurity practices in all the phases of a product lifecycle. It addresses the development of products as well as their support during commercialization. Part 4-2 specifies technical requirements for components. Four categories are considered:

* 2025

- embedded devices like controllers or remote terminal units,
- host based devices like operator stations or engineering stations,
- network devices like firewalls, gateways or switches, and
- software applications like HMI applications or historians.

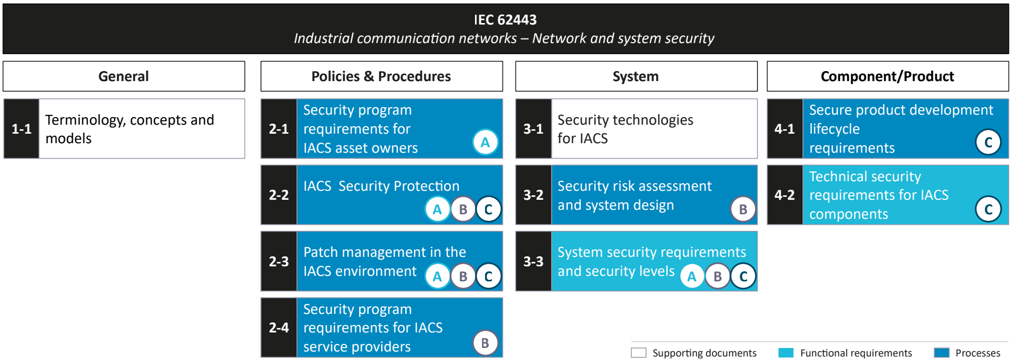
The standard has found a large practical acceptance. Based on the concepts described in IEC 62443-2-2 [7] this book is intended to help in the implementation of security protection schemes. Following documents are core for the development of holistic protection concepts for operating facilities:

- **IEC 62443-2-1, Security program requirements for IACS asset owners** [6].
  The edition 2 has been published in 2024, and is the basis for the considerations of this book. Edition 1 included requirements for a security management system. In edition 2 all requirements to the content for a security management have been removed. Instead, it is assumed that the asset owner has an established information security management system (ISMS) in place. We assume that the ISMS of the asset owner is based on the standards ISO 27001 [2] and ISO 27002 [3].
- **IEC 62443-2-4, Security program requirements for IACS service providers** [9].
  Specifies the requirements for the policies and procedures for service providers for integration or maintenance. The document was adopted in 2015 as international standard, edition 2 has been published in 2023.
- **IEC 62443-3-2, Security risk assessment and system design** [11].
  Specifies process steps for a risk-based partitioning in zones and conduits and design of security measures for each zone and conduit. The document was adopted in 2020 as international standard.
- **IEC 62443-3-3, System security requirements and security levels** [12].
  Specifies functional requirements for control systems and blueprints. The document should also be used by integration service providers to develop security capabilities of automation solutions. The document was adopted in 2013 as international standard, edition 2 is currently under development.
- **IEC 62443-4-1, Secure product development lifecycle requirements** [13].
  Specifies the cybersecurity requirements to be integrated in the product lifecycle. The document was adopted in 2018 as international standard.
- **IEC 62443-4-2, Technical security requirements for IACS components** [14].
  Specifies functional requirements to components. The document was adopted in 2019 as international standard.

To give a first orientation, we have grouped in Figure 4.1 the documents according to their main relevance for the primary roles:

- Group C – parts 3-3, 4-1, 4-2, 2-2 and 2-3 – is mainly relevant for product suppliers in the development and support of products
- Group B – parts 2-4, 3-2, 3-3, 2-2 and 2-3 – is mainly relevant for service providers designing or maintaining security measures in automations solutions.

- Group A – parts 2-1, 3-3, 2-2 and 2-3 – is mainly relevant for asset owners implementing security programs and ensuring the development and practice of security protection schemes



IEC 62443
Industrial communication networks – Network and system security

General	Policies & Procedures	System	Component/Product
1-1 Terminology, concepts and models	2-1 Security program requirements for IACS asset owners A	3-1 Security technologies for IACS	4-1 Secure product development lifecycle requirements C
	2-2 IACS Security Protection A B C	3-2 Security risk assessment and system design B	4-2 Technical security requirements for IACS components C
	2-3 Patch management in the IACS environment A B C	3-3 System security requirements and security levels A B C	
	2-4 Security program requirements for IACS service providers B		

□ Supporting documents ■ Functional requirements ■ Processes

Figure 4.1 Main relevant documents of IEC 62443