GLOBAL CYBERSECURITY ALLIANCE

Quick Start Guide: An Overview of ISA/IEC 62443 Standards

Security of Industrial Automation and Control Systems

THE TIME IS NOW

June 2020

www.isa.org/ISAGCA

Quick Start Guide:
An Overview of ISA/IEC 62443 Standards
Security of Industrial Automation and Control Systems

Executive Summary

This document is intended to provide the reader with a detailed overview of the ISA/IEC 62443 Series of standards and technical reports. The ISA/IEC 62443 Series addresses the Security of Industrial Automation and Control Systems (IACS) throughout their lifecycle. These standards and technical reports were initially developed for the industrial process sector but have since been applied to building automation, medical devices, and transportation sectors.

There are several trends that have made cybersecurity an essential property of IACS, along with safety, integrity, and reliability. First, over the last two decades, IACS technologies have migrated from vendor-proprietary to commercial off-the-shelf technologies such as Microsoft Windows™ and TCP/IP networking. Second, the value of data residing in the IACS for the business has significantly increased the interconnectivity of IACS both internal and external to the organization. Finally, the means, resources, skills, and motivation of cyberattackers have significantly increased. The combination of these trends has made IACS more vulnerable to cyberattack. Figure 1 shows some of the notable cyberattacks that have impacted IACS.

Date	Target	Method
2000	Australian Sewage Plant	Insider
2010	Iran Uranium Enrichment	Stuxnet
2013	ICS Supply Chain attack	Havex
2014	German Steel Mill	
2015	Ukraine Power Grid	BlackEnergy, KillDisk
2016	Ukraine Substation	CrashOverride
2017	Global shipping company	NotPetya
2017	IoT DDos attack	BrickerBot
2017	Health care, Automotive, many others	WannaCry
2017	Saudi Arabia Petrochemical	TRITON/TRISIS
2019	Norwegian Aluminum Company	LockerGaga

Source: www.awa.csis.org/programs/technology-policy-program/significant-cyber-incidents

Table 1: Some notable cyberattacks impacting IACS

Initially, the ISA99 committee considered IT standards and practices for use in the IACS. However, it was soon found that this was not sufficient to ensure the safety, integrity, reliability, and security of an IACS. This is because the consequences of a successful cyberattack on an IACS are fundamentally different. While the primary consequences of a successful cyberattack on IT systems is financial and privacy loss due to information disclosure, the consequences for an IACS may additionally include loss of life or health, damage to the environment, or loss of product integrity. There are several other differences between IT and IACS such as performance requirements, availability requirements, change management, the time between maintenance windows, and equipment lifetime. [1]

The International Society of Automation (ISA) and the International Electrotechnical Commission (IEC) have joined forces to address the need to improve the cybersecurity of IACS. The ISA99 Committee and the IEC Technical Committee 65/ Working Group 10 develop and publish the ISA/ IEC 62443 Series. These documents describe a methodical engineered approach to addressing the cybersecurity of IACS. They can be purchased from either organization; the technical content is identical. The benefits of using a standards-based approach include reducing the likelihood of a successful cyberattack, the use of a common set of requirements among stakeholders, security throughout the lifecycle, and a reduction in overall lifecycle cost.

Introduction

This document provides an overview of the ISA/IEC 62443 Series of standards and technical reports (referred to as the ISA/IEC 62443 Series) which specifies requirements for the Security of Industrial Automation and Control Systems (IACS). The goal of the ISA/IEC 62443 Series is to improve the safety, reliability, integrity, and security of Industrial Automation and Control Systems (IACS) using a risk-based, methodical, and complete process throughout the entire lifecycle. The ISA/IEC 62443 Series describes a set of common terms and requirements that can be used by asset owners, product suppliers, and service providers to secure their Control Systems and the Equipment Under Control.

Scope and Purpose

The scope of the ISA/IEC 62443 Series is the Security of Industrial Automation and Control Systems (IACS). An IACS is defined as a:

> **collection of personnel, hardware, software, and policies involved in the operation of the industrial process and that can affect or influence its safe, secure, and reliable operation.**

Note that an IACS includes more than the technology that comprises a control system; it also includes the people and work processes needed to ensure the safety, integrity, reliability, and security of the control system. Without people who are sufficiently trained, risk-appropriate technologies and countermeasures, and work processes throughout the security lifecycle, an IACS could be more vulnerable to cyberattack.

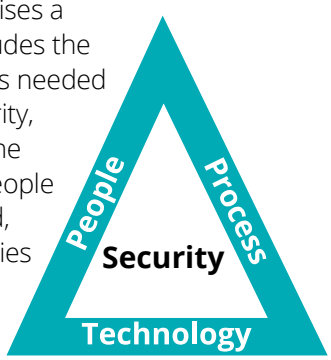

Figure 1:
The Security Triad

Table of Contents

Because IACS are physical-cyber systems, the impact of a cyberattack could be severe. The consequences of a cyberattack on an IACS include, but are not limited to:

- Endangerment of public or employee safety or health
- Damage to the environment
- Damage to the Equipment Under Control
- Loss of product integrity
- Loss of public confidence or company reputation
- Violation of legal or regulatory requirements
- Loss of proprietary or confidential information
- Financial loss
- Impact on entity, local, state, or national security

The first four consequences in the above list are unique to physical-cyber systems and are not typically present in traditional IT systems. Indeed, it is this difference that fundamentally results in the need for different approaches to securing physical-cyber systems and caused standards development organizations to identify the need for standards that are unique to IACS. Some other characteristics of IACS that are not typical in IT systems include: [1]

- more predictable failure modes
- tighter time-criticality and determinism
- higher availability
- more rigorous management of change
- longer time periods between maintenance
- significantly longer component lifetimes
- Safety, Integrity, Availability, and Confidentiality (SIAC) instead of CIA

Cyber threat actors include but are not limited to insiders (accidental or intentional), hacktivists, cybercriminals, organized crime, and state-sponsored attackers. Types of cyberattacks include but are not limited to ransomware, destructive malware, directed remote access attacks, and coordinated attacks on control systems and associated support infrastructure. Table 1 lists several noteworthy directed and non-directed cyberattacks impacting IACS.

ISA/IEC 62443 Series Standards Development Organizations

There are two standards development organizations involved in the development of the ISA/IEC 62443 Series of standards and technical reports:

- International Society of Automation – ISA99 Committee
- International Electrotechnical Commission – IEC TC65/WG10 Committee

There is a formal liaison agreement between these two standards development organizations. The ISA/IEC 62443 Series of standards and technical reports are developed primarily by the ISA99 Committee with input, review and simultaneous adoption by both the ISA and IEC. The one exception is ISA/IEC 62443-2-4, which was developed by the IEC TC65/WG10 Committee and adopted by ISA. As a result, whether an ISA/IEC 62443 document is published by ISA or IEC, the content is identical except for the non-normative preface and foreword.

The United Nations Economic Commission for Europe (UNECE) confirmed at its annual meeting in late 2018 that it will integrate the widely used ISA/IEC 62443 Series into its forthcoming Common Regulatory Framework on Cybersecurity (CRF). The CRF will serve as an official UN policy position statement for Europe, establishing a common legislative basis for cybersecurity practices within the European Union trade markets. [2]

Refer to the *Published Standards and Technical Reports* section at the end of this document for a complete list of ISA and IEC cybersecurity-related documents currently available.

Summary of ISA/IEC 62443 Series Standards and Technical Reports

These documents are arranged in four groups, corresponding to the primary focus and intended audience. [4]

1. **General**—This group includes documents that address topics that are common to the entire series.
   - **Part 1-1: Terminology, concepts, and models** introduces the 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.

- **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 cybersecurity management system. The intended audience includes asset owners who have responsibility for the design and implementation of such a program.
   - **Part 2-2: IACS 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. This standard was developed by IEC TC65/WG10.
   - **Part 2-5: Implementation guidance for IACS asset owners** provides guidance on what is required to operate an effective IACS cybersecurity program. The intended audience includes asset owners who have responsibility for the operation of such a program.
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

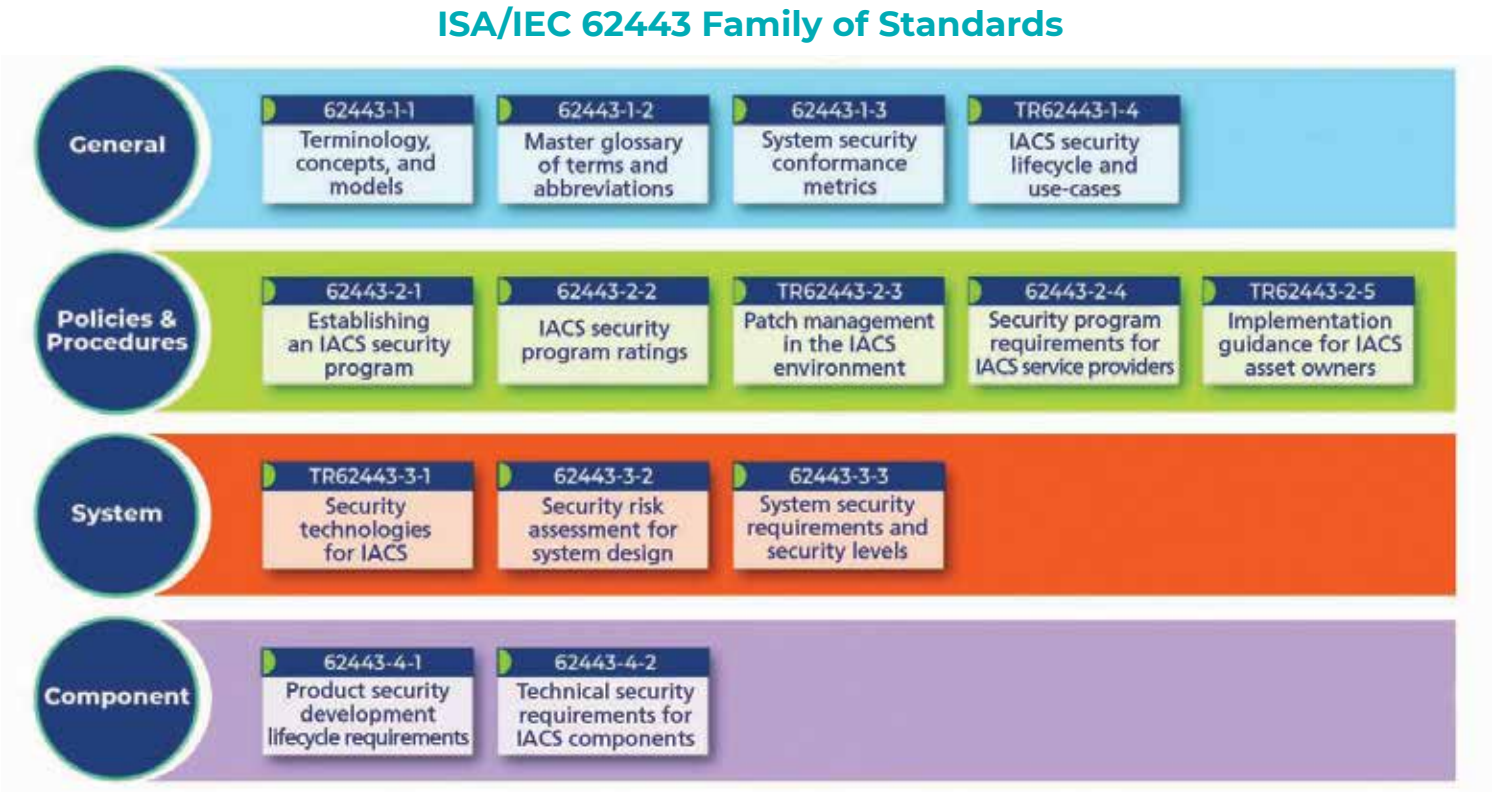

Figure 2: The ISA/IEC 62443 Series

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: Product security development life cycle requirements** describes the requirements for a product developer's security development 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.

	Part	Type	Title	Date
Overview	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	
Systems	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

Table 2: ISA/IEC 62443 Series Status

Table 2 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.

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.

Fundamental Concepts

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 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 countermeasures 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. 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, as mentioned above, the IACS is significantly different from IT systems, so there are additional requirements and considerations for its Security Program.

Risk Management

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 3 shows the 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 cyber-attack. 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
- Should separate temporarily connected devices
- Should separate wireless devices
- Should separate devices connected via external networks

Cybersecurity Requirements Specification

Part 3-2 also requires that required security countermeasures from the Risk Assessment as

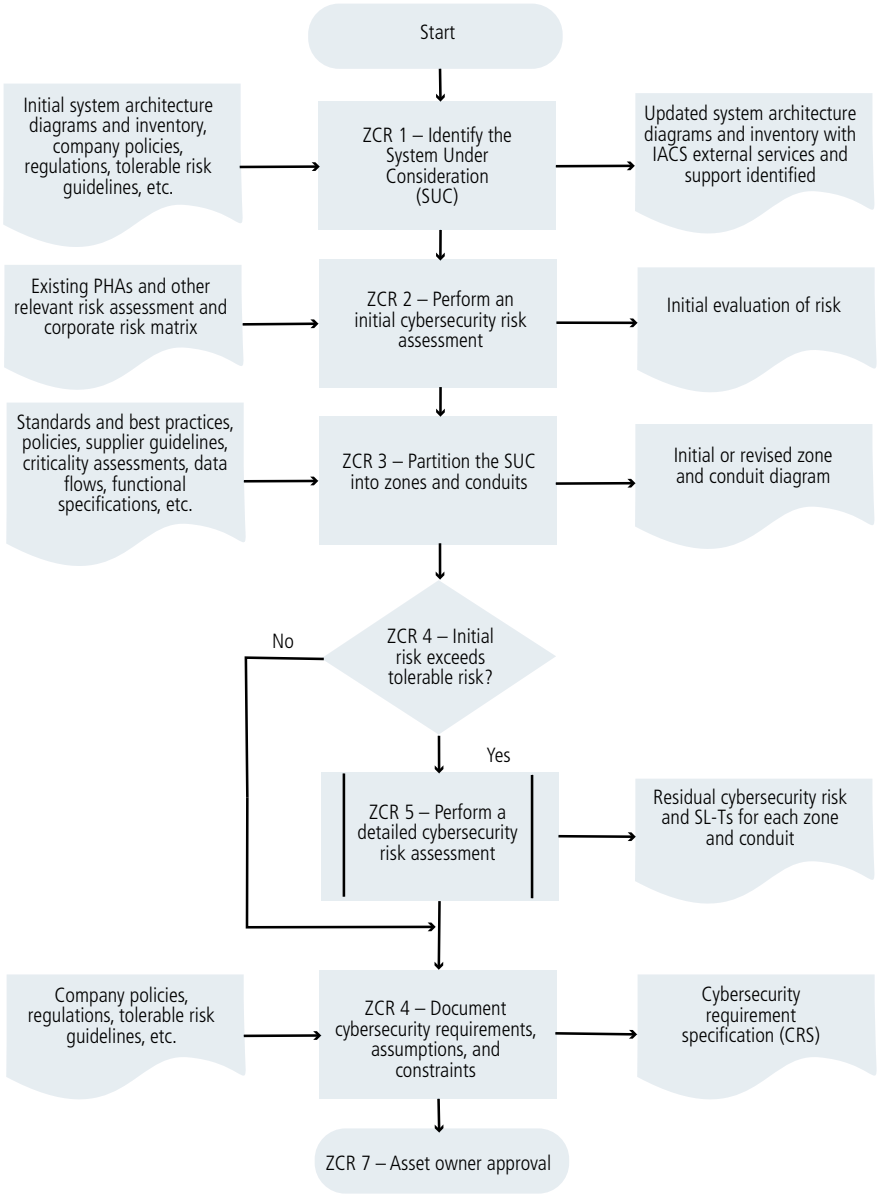

Figure 3: Risk Assessment Process

well as security requirements based on company or facility-specific policies, standards, and relevant regulations are documented in a Cybersecurity Requirements Specification (CRS). The CRS does not have to be a standalone document; it can be included as a section in other relevant IACS documents.

The CRS includes information such a description of the System Under Consideration, Zone and Conduit drawings, threat environment, and countermeasures from risk assessments.

Threat Modeling

Part 4-1 describes the requirements for the security development lifecycle (SDL) of Control System and Component products. One of the key processes in the product SDL is threat modeling which is a systematic process to identify data flows, trust boundaries, attack vectors, and potential threats to the control system. The security issues identified in the threat model must be addressed in the final release of the product and the threat model itself must be periodically updated during the product's lifecycle.

Foundational Requirements

Foundational Requirements (FRs) form the basis for technical requirements throughout the ISA/IEC 62443 Series. All aspects associated with meeting a desired IACS security level (people, processes, and technology) are derived through meeting the requirements associated with the seven following Foundational Requirements:

- FR 1 – Identification and Authentication Control (IAC)
- FR 2 – Use Control (UC)
- FR 3 – System Integrity (SI)
- FR 4 – Data Confidentiality (DC)
- FR 5 – Restricted Data Flow (RDF)
- FR 6 – Timely Response to Events (TRE)
- FR 7 – Resource Availability (RA)

Foundational Requirements are used to organize the requirements for IACS Systems (Part 3-3) and Components (Part 4-2).

The combination of FR 1 and FR 2 is sometimes called Access Control; they were split into two FRs to keep the total number of requirements at a manageable level.

Security Levels

Security Level is defined as the *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 Table 3. 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 natively without additional compensating countermeasures.
- ***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 additional countermeasures during the Integration phase of the IACS lifecycle.
- ***Achieved Security Levels (SL-A)*** are the actual levels of security for a particular Automation

Security Level	Definition	Means	Resources	Skills	Motivation
1	Protection against casual or coincidental violation	simple	low	generic	low
2	Protection against intentional violation using simple means with low resources, generic skills, and low motivation				
3	Protection against intentional violation using sophisticated means with moderate resources, IACS-specific skills, and moderate motivation	sophisticated	moderate	IACS-specific	moderate
4	Protection against intentional violation using sophisticated means with extended resources, IACS-specific skills, and high motivation	sophisticated	extended	IACS-specific	high

Table 3: Security Level Definition

Solution. These are measured after the Automation Solution is commissioned and in operation. Part 2-2 combines SL-A with operational and maintenance policies and procedures to form the Security Program Rating for a particular Automation Solution.

Maturity Model

While Security Levels are a measure of the strength of technical requirements, Maturity Levels are a measure of processes (people, policies, and procedures). Parts 2-1, 2-2, 2-4, and 4-1 use Maturity Levels to measure how thoroughly requirements are met.

As shown in Table 4, the Maturity Model is based on the Capability Maturity Model Integration (CMMI), with Levels 4&5 combined into Level 4.

Design Principles

Secure by Design

Secure by design is a design principle where security measures are implemented early in the lifecyle of the IACS. The intent is that robust security policies, security architectures, and secure practices are established early in development and implemented throughout the lifecycle. This design principle applies to both product development and Automation Solution development. When using a secure by design philosophy, security measures operate natively within the Control System or Component without requiring the addition of compensating countermeasures.

Reduce Attack Surface

Reducing the attack surface is a design principle where the physical and functional interfaces of an IACS that can be accessed and exposed to potential attack are minimized, making it more difficult for an attack to succeed. Reducing attack surface includes design principles such as:

- Access control—restricting physical and logical access to IACS systems and networks
- Network segmentation—segmenting IACS networks and controlling the traffic between them
- Least function—hardening IACS systems and networks by removing unneeded functions
- Least privilege—limiting privileges to the minimum necessary for the role or function

Defense in Depth

Defense in depth is defined as the *provision of multiple security protections, especially in layers, with the intent to delay or prevent an attack.* Defense in depth implies layers of security and detection, even on single systems, and requires attackers to break through or bypass multiple layers without being detected. The IACS is still protected even if a vulnerability in one layer is compromised. Special attention must be paid to a single vulnerability that allows the potential compromise of multiple layers.

Essential Functions

Essential functions are defined as *functions or capabilities that are required to maintain health, safety, the environment, and availability of the Equipment Under Control.* Essential functions include:

- the Safety Instrumented Function (SIF)
- the control function
- the ability of the operator to view and manipulate the Equipment Under Control

The loss of essential functions is commonly termed: loss of protection, loss of control, and loss of view respectively. In some use cases additional functions such as history may be considered essential.
Part 3-3 requires that security measures shall not adversely affect essential functions of a high-

Level	CMMI	62443	Description
1	Initial	Initial	• Product development typically ad-hoc and often undocumented • Consistency and repeatability may not be possible
2	Managed	Managed	• Product development managed using written policies • Personnel have expertise and are trained to follow procedures • Processes are defined but some may not be in practice
3	Defined	Defined (Practiced)	• All processes are repeatable across the organization • All processes are in practice with documented evidence
4	Quantitively Managed	Improving	• CMMI Levels 4 and 5 are combined • Process metrics are used control effectiveness and performance
5	Optimizing		• Continuous improvement

Table 4: Maturity Level Definition

availability IACS unless it is supported by a Risk Assessment. The concept of essential functions places some design constraints on the design of IACS security measures:

- Access control shall not prevent the operation of essential functions
- Essential functions shall be maintained if the Zone boundary protection (firewall) goes into a fail close/island mode
- A denial of service event on the Control System or Safety Instrumented System network shall not prevent safety instrumented functions from acting

Roadmap for the ISA/IEC 62443 Series

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 4 visualizes this relationship.

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

- ***Asset Owner*** is the organization that 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*** is the individual or organization that provides support activities for an Automation Solution.
- ***Integration Service Provider*** is the organization that 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*** is the organization that manufactures and supports a hardware and/or software product. Products may include Control Systems, Embedded Devices, Host Devices, Network Devices, and/or Software Applications.

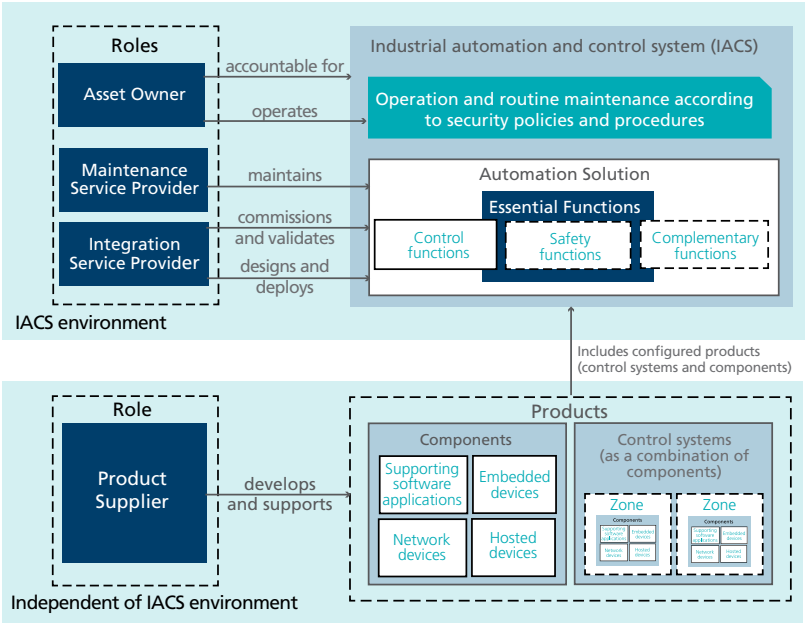

Figure 4: Roles, Products, Automation Solution, and IACS

Component, System, Automation Solution, and IACS

The right-hand side of the figure 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
- ***IACS System (or Control System)*** consists of an integrated set of Embedded Devices (e.g. PLC), Host Devices, Network Devices, and Software Applications provided by one or more Product Suppliers.
- ***Automation Solution*** is the realization of a Control System 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 Industrial Automation and Control System (IACS)*** includes the Automation

Solution and the operational and maintenance policies and procedures necessary to support it.

Hierarchical View

Figure 5 shows the hierarchical relationships among the ISA/IEC 62443 Series of 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. In particular, it describes the Foundational Requirements, which are used to organize technical requirements throughout the series.
- **Part 2-1** sets the requirements for the Security Program of an Asset Owner. All of the other standards in the ISA/IEC 62443 Series derive their requirements from Part 2-1 and expand upon them in more detail.
- **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 4-1** is used by the Product Supplier to establish and sustain a Security Development Lifecycle, which is used to create Control System and Component products.

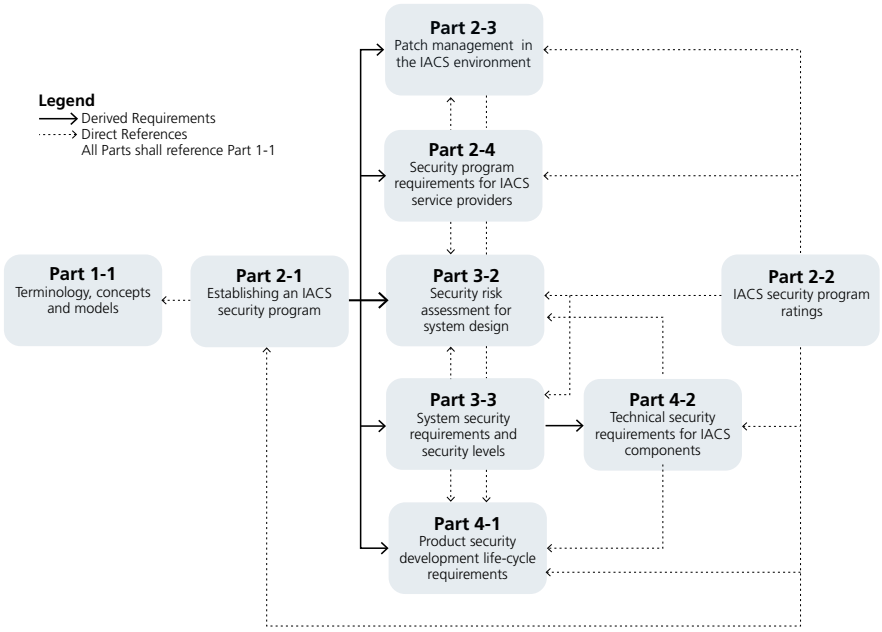

Figure 5: ISA/IEC 62443 Standards – Hierarchical View

- **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 2-3** sets the requirements for the patch management process, which is used to reduce cybersecurity vulnerabilities in the Automation Solution.

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 Development Lifecycle and the Automation

<table>
<tr><th rowspan="2">Product Development Lifecycle</th><th colspan="2">Automation Solution Lifecycle</th></tr>
<tr><th>Integration</th><th>Operation and Maintenance</th></tr>
<tr><td colspan="3">Part 1-1: Terminology, Concepts, and Models</td></tr>
<tr><td rowspan="6"></td><td colspan="2">Part 2-1: Establishing an IACS Security Program</td></tr>
<tr><td colspan="2">Part 2-2: IACS Security Program Rating</td></tr>
<tr><td colspan="2">Part 2-3: Patch Management in the IACS Environment</td></tr>
<tr><td colspan="2">Part 2-4: Security program requirements for IACS service providers</td></tr>
<tr><td colspan="2">Part 3-2: Security Risk Assessment for System Design</td></tr>
<tr><td colspan="3">Part 3-3: System security requirements and Security levels</td></tr>
<tr><td>Part 4-1: Product Security Development Lifecycle Requirements</td><td colspan="2" rowspan="2"></td></tr>
<tr><td>Part 4-2: Technical security requirements for IACs components</td></tr>
</table>

Figure 6: ISA/IEC 62443 Standards - Lifecycle View

Solution Lifecycle. The Automation Solution Lifecycle is further divided into an Integration Phase and an Operation and Maintenance Phase. Table 6 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 Development Lifecycle and the Integration Phase of the Automation Solution Lifecycle. This is because while the Product Supplier is the main audience for Part 3-3, the Integration Service Provider may also combine Components to create Control Systems. An example would be a SCADA system, where the Integration Service Provider integrates the SCADA system with Embedded Devices (e.g., PLC) to create an Automation Solution.

ISA/IEC 62443 Series for Asset Owners

Asset Owner activities:

- Establish and sustain a Security Program that includes IACS-specific requirements
- Partition Zones and Conduits and perform associated Risk Assessments
- Document IACS requirements in the Cybersecurity Requirements Specification
- Procure products and services that meet IACS requirements
- Operate and maintain the IACS
- Assess the effectiveness of the IACS Security Program

Applicable ISA/IEC 62443 standards:

- ISA/IEC 62443-2-1, *Establishing an IACS security program*
- ISA/IEC 62443-2-2, *Security Program ratings*
- ISA/IEC 62443-2-3, *Patch management in the IACS environment*
- ISA/IEC 62443-2-4, *Requirements for IACS service providers*
- ISA/IEC 62443-3-2, *Security risk assessment for system design*
- ISA/IEC 62443-3-3, *System security requirements and security levels*

ISA/IEC 62443 Series for Product Suppliers

Product Supplier activities:

- Establish and sustain a Security Development Lifecycle
- Provide Control System products that meet Security Level capabilities
- Provide Component products that meet Security Level capabilities
- Provide ongoing lifecycle support for their Control System and Component products

Applicable ISA/IEC 62443 standards:

- ISA/IEC 62443-4-1, *Product security development lifecycle requirements*
- ISA/IEC 62443-3-3, *System security requirements and security levels*
- ISA/IEC 62443-4-2, *Technical security requirements for IACS Components*
- ISA/IEC 62443-3-2, *Security risk assessment for system design*

ISA/IEC 62443 Series for Service Providers

Integration Service Providers

Integration Service Provider activities:

- Establish and sustain a Security Program for Automation Solution integration
- Design and implement Automation Solutions that meet the requirements in the Cybersecurity Requirements Specification
- Apply security patches during the Integration Phase of the Automation Solution lifecycle

Applicable ISA/IEC 62443 standards:

- ISA/IEC 62443-2-1, *Establishing an IACS security program*
- ISA/IEC 62443-2-3, *Patch management in the IACS environment*
- ISA/IEC 62443-2-4, *Requirements for IACS service providers*
- ISA/IEC 62443-3-2, *Security risk assessment for system design*
- ISA/IEC 62443-3-3, *System security requirements and security levels*

Maintenance Service Providers

Maintenance Service Provider activities:

- Establish and sustain a Security Program for maintenance services
- Provide services and capabilities that meet the IACS security policies and procedures specified by the Asset Owner

Applicable ISA/IEC 62443 standards:

- ISA/IEC 62443-2-3, *Patch management in the IACS environment*
- ISA/IEC 62443-2-2, *IACS Security Program ratings*
- ISA/IEC 62443-2-4, *Requirements for IACS service providers*

Certification and Training

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 Development 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.

Certified System ISASecure®

- ***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

Certified Component ISASecure®

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

IECEE Certification

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.

ISA Cybersecurity Training

The following cybersecurity-related training courses are offered by ISA:

- Cybersecurity awareness training for Water/ Wastewater Industry Professionals (IC31)
- Using the ISA/IEC 62443 Standards to Secure Your Control System (IC32, IC32M)
- Introduction to Industrial Automation Security and the ISA/IEC 62443 Standards (IC32C)
- Cybersecurity for Automation, Control and SCADA Systems (IC32E)
- Assessing the Cybersecurity of New or Existing IACS Systems (IC33, IC33E, IC33M)
- IACS Cybersecurity Design and Implementation (IC34, IC34M)
- IACS Cybersecurity Operation and Maintenance (IC37, IC37M)
- Overview of ISA/IEC 62443 for Product Suppliers (IC46C, IC46M)

The last letter of the course code designates the type of course as follows:

- <none> - Multi-day classroom course
- C – One-day overview course
- E – Online, instructor-assisted course
- M – On-demand, computer-based training

ISA Cybersecurity Certificates

ISA offers the following cybersecurity certificates for students who have completed the training courses listed above. Certificates are not to be confused with product certifications offered by ISASecure®.

- ISA/IEC 62443 Cybersecurity Fundamentals Specialist
- ISA/IEC 62443 Cybersecurity Risk Assessment Specialist
- ISA/IEC 62443 Cybersecurity Design Specialist
- ISA/IEC 62443 Cybersecurity Maintenance Specialist
- ISA/IEC 62443 Cybersecurity Expert

Certificate 1 **Certificate 2** **Certificate 3** **Certificate 4** **Expert**

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
   ANSI/ISA-62443-4-1-2018 / IEC 62443-4-1:2018 – SECURITY FOR INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS, PART 4-1: PRODUCT SECURITY DEVELOPMENT LIFE-CYCLE REQUIREMENTS
8. 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
9. IEC TR 63069:2019 – INDUSTRIAL-PROCESS MEASUREMENT, CONTROL AND AUTOMATION – FRAMEWORK FOR FUNCTIONAL SAFETY AND SECURITY
10. IEC TR 63074:2019 – SAFETY OF MACHINERY – SECURITY ASPECTS RELATED TO FUNCTIONAL SAFETY OF SAFETY-RELATED CONTROL SYSTEMS

References

1. NIST SP 800-82 REVISION 2, GUIDE TO INDUSTRIAL CONTROL SYSTEMS (ICS) SECURITY
2. UNITED NATIONS COMMISSION TO INTEGRATE ISA/IEC 62443 INTO CYBERSECURITY REGULATORY FRAMEWORK, ISA INTECH MAGAZINE, JAN-FEB, 2019
3. THE 62443 SERIES OF STANDARDS: INDUSTRIAL AUTOMATION AND CONTROL SECURITY, ISA99 COMMITTEE
4. FREQUENTLY ASKED QUESTIONS: THE ISA99 COMMITTEE AND 62443 STANDARDS, ISA99 COMMITTEE
5. INSTRUMENTATION AND CONTROL SYSTEMS SECURITY EXPLAINED: THE WHAT AND THE WHY, ISA99 COMMITTEE

This document contains some information that is based on ISA99 Committee draft documents. Please refer to the published documents for the definitive set of requirements currently available.