GLOBAL CYBERSECURITY ALLIANCE

Cybersecurity is a Global Imperative

THE TIME IS NOW

Announcing the Creation of the ISA Global Cybersecurity Alliance

# OT Cybersecurity for Maritime Transportation System using ISA/IEC 62443 Standards to Assess, Implement, Operate and Maintain for vessels

April 2023 K.Chatziargyros

Steps to start for Securing the OT devices:

- start with the Risk Assessment to identify and categorize the nodes and scan what objects are on networks .

- determine security Level targets

- utilize the 7 FR’s Foundational requirements .

62443 Lifecyle is
-Assess
-Develop and Implement
-Operate and Maintain

In Policies and Procedures on ISA-IEC 62443-2-3 is the patch management we have to follow for all of our devices.
While patching is necessary evil ,it is not the only thing we have to focus on .

Some steps of how i am Securing OT devices:

-Network Segmentation on a Managed ethernet switch .
-Configure Bond Interfaces on the Firewall .
-Use 1 bond port for incoming connection traffic .
-Use another bond port for outgoing traffic .
-Connection of all OT devices  on the Managed Switch .
ex.VDR VLAN10 ,AMS VLAN20 etc (avoid using VLAN 1 which is default on many devices) .
-Make sure that you have :
i)inquire every mitigation action as the ICS/OT systems have many interdependencies.
ii) that tag servers and OPC systems are within the same VLANs as the PLCS and CPUS.
iii)Serial ports might be encapsulated ethernet via gateways .
-Installing Fend data diode products .
-Patch management “of VDR” and any other OT device as per IEC-TR-63443-2-3 .
-Image backup of OT devices using Windows O.S to an encrypted external disk (disks in raid 1) .
-Use of encrypted USB disks onboard only .
-Use of OSINT tools.
-SOC .
-End Point Protection.
-In case of detection on OT device or an anomaly that will appear on traffic the safest way is to disable the LAN port of the device and not to block the object  from Firewall .

**Let's See now in detail how we can do that by using**

**ISA/IEC 62443 Standards to Assess, Implement, Operate and Maintain for vessels**

# ISA/IEC 62443 Global Automation Cybersecurity Standards

The ISA/IEC 62443 series of standards define requirements and processes for asses, implementing, operate and maintain electronically secure Industrial Automation and Control Systems (IACS).

These standards set best practices for security and provide a way to assess the level of security performance.

International Society of Automation, ISA (www.isa.org) is a non-profit professional association founded in 1945 of engineers, technicians who are engaged to improve the management, safety and Cyber Security of automation, control systems and critical infrastructure across Industry .Its purpose is to sets the Standards to create a better and technologically safer world through automation.

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.

***We cannot talk about Automation, if we don't take into consideration the Global ISA/IEC 62443 Standards.***

# Overview of ISA/IEC 62443 Standards for the Security of Industrial Automation and Control Systems

There are several trends that have made cybersecurity a substantial property of IACS, along with safety, integrity, and reliability.

last  decades, IACS technologies have migrated from vendor-proprietary to commercial off-the-shelf technologies

also, 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, cyberattacks have been significantly increased.

All of these trends has made IACS more vulnerable to cyberattack.

Initially, the ISA99 committee considered IT standards and practices for use in the IACS. However, it ware realized that this was not sufficient to ensure the safety, integrity, reliability, and security of an IACS.
This because the consequences of a successful cyberattack on an IACS are different.

While the primary consequences of a successful cyberattack on IT systems are economic loss and loss of privacy due to information disclosure, the consequences for an IACS may additionally include loss of life or health, damage to the environment .

There are many other differences between IT and IACS such as performance requirements, availability requirements, change management, the time of maintenance windows, and the equipment lifetime.

## 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:

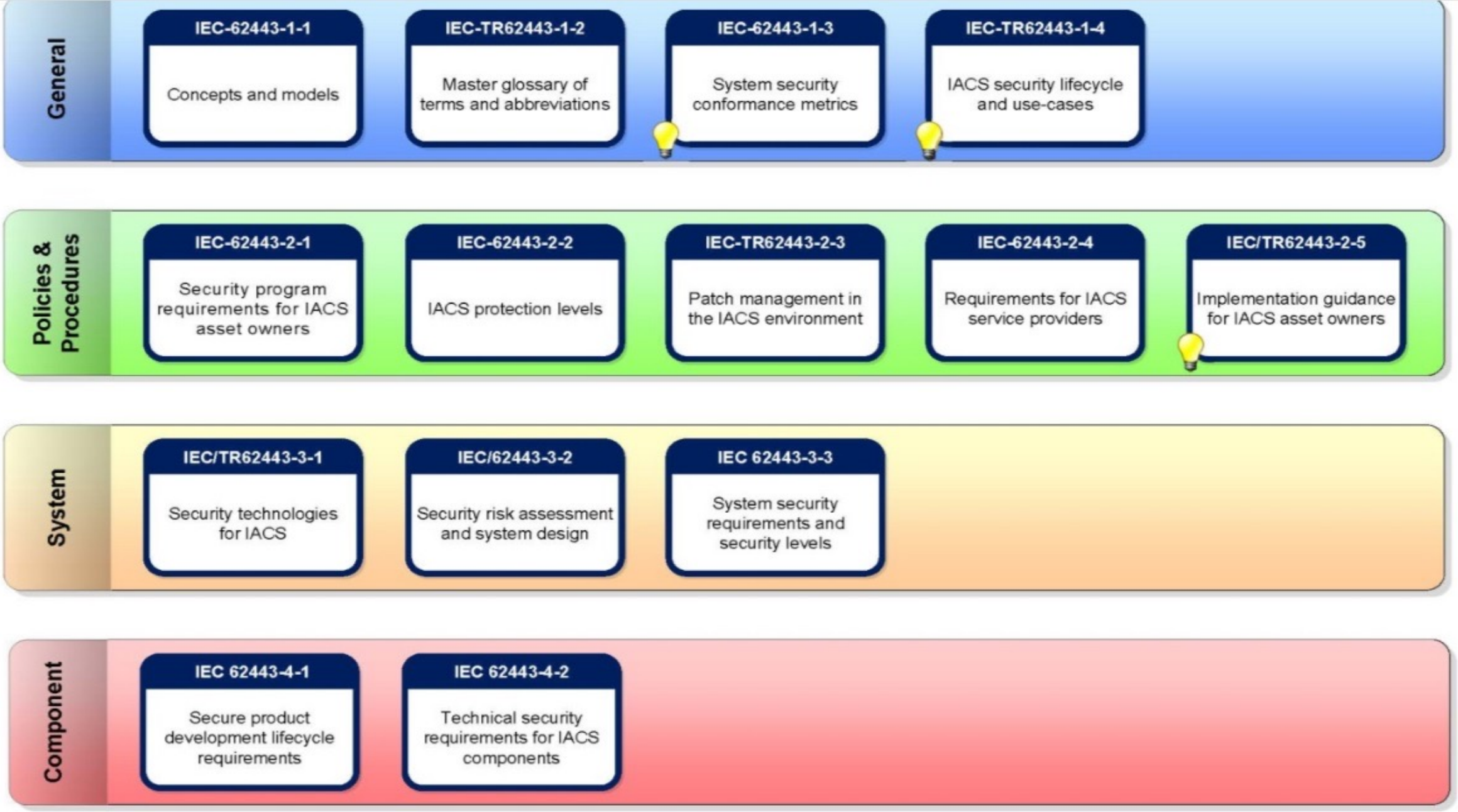
- International Society of Automation – ISA99 Committee
- International Electrotechnical Commission – IEC TC65/WG10 Committee

## Scope and Purpose

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

An IACS is considered follow:

**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**.


General
IEC-62443-1-1
Concepts and models
IEC-TR62443-1-2
Master glossary of terms and abbreviations
IEC-62443-1-3
System security conformance metrics
IEC-TR62443-1-4
IACS security lifecycle and use-cases
Policies & Procedures
IEC-62443-2-1
Security program requirements for IACS asset owners
IEC-62443-2-2
IACS protection levels
IEC-TR62443-2-3
Patch management in the IACS environment
IEC-62443-2-4
Requirements for IACS service providers
IEC/TR62443-2-5
Implementation guidance for IACS asset owners
System
IEC/TR62443-3-1
Security technologies for IACS
IEC/62443-3-2
Security risk assessment and system design
IEC 62443-3-3
System security requirements and security levels
Component
IEC 62443-4-1
Secure product development lifecycle requirements
IEC 62443-4-2
Technical security requirements for IACS components

## General

- Part 1-1: Terminology, ideas, and models introduces the ideas and models used throughout 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

- Part 2-1: Establishing an IACS security program

what is required to define and implement an effective IACS cybersecurity management system.

.

- 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. 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.

## 3. System Requirements

- Part 3-1: Security technologies for IACS

describes the application of various security technologies to an IACS 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.

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

• 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.

On table 2 presents the complete list of ISA/IEC 62443 standards and technical reports.

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

| | 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**

**Fundamental ideas**

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.

On this section 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.

**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.**

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

**Risk Management**

-Part 3-2 describes the requirements of cybersecurity risks in an IACS, including the use of Zones and Conduits, and Security Levels. While it includes the requirements for the risk assessment ,does not specify the methodology which must be used. Methodology must be established by the Asset Owner and should be consistent with the overall risk assessment methodology of the organization.

-Zones and Conduits
A Zone is considered 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 considered as a logical grouping of communication channels that share common security requirements connecting two or more zones.

A basic step in the Risk Assessment process is to partition the System Under Consideration into separate Zones and Conduits. The intention is to identify those assets that share common security to establish a set of common security requirements that reduce cybersecurity risk.
Part 3-2 requires or recommends that some assets are partitioned as follows:

- to separate business and control system assets
- to separate safety related assets
- to separate temporarily connected devices
- to separate wireless devices
- to separate devices connected via external networks

-Cybersecurity Requirements Specification
Part 3-2 also requires that required security countermeasures from the Risk Assessment are documented in a Cybersecurity
Requirements Specification (CRS).

The CRS must not be a standalone document,But it can be included as a section in other relevant IACS documents.

The CRS include the following information :

description of the System Under Consideration, Zone Conduit drawings, threat environment and countermeasures from risk assessments.

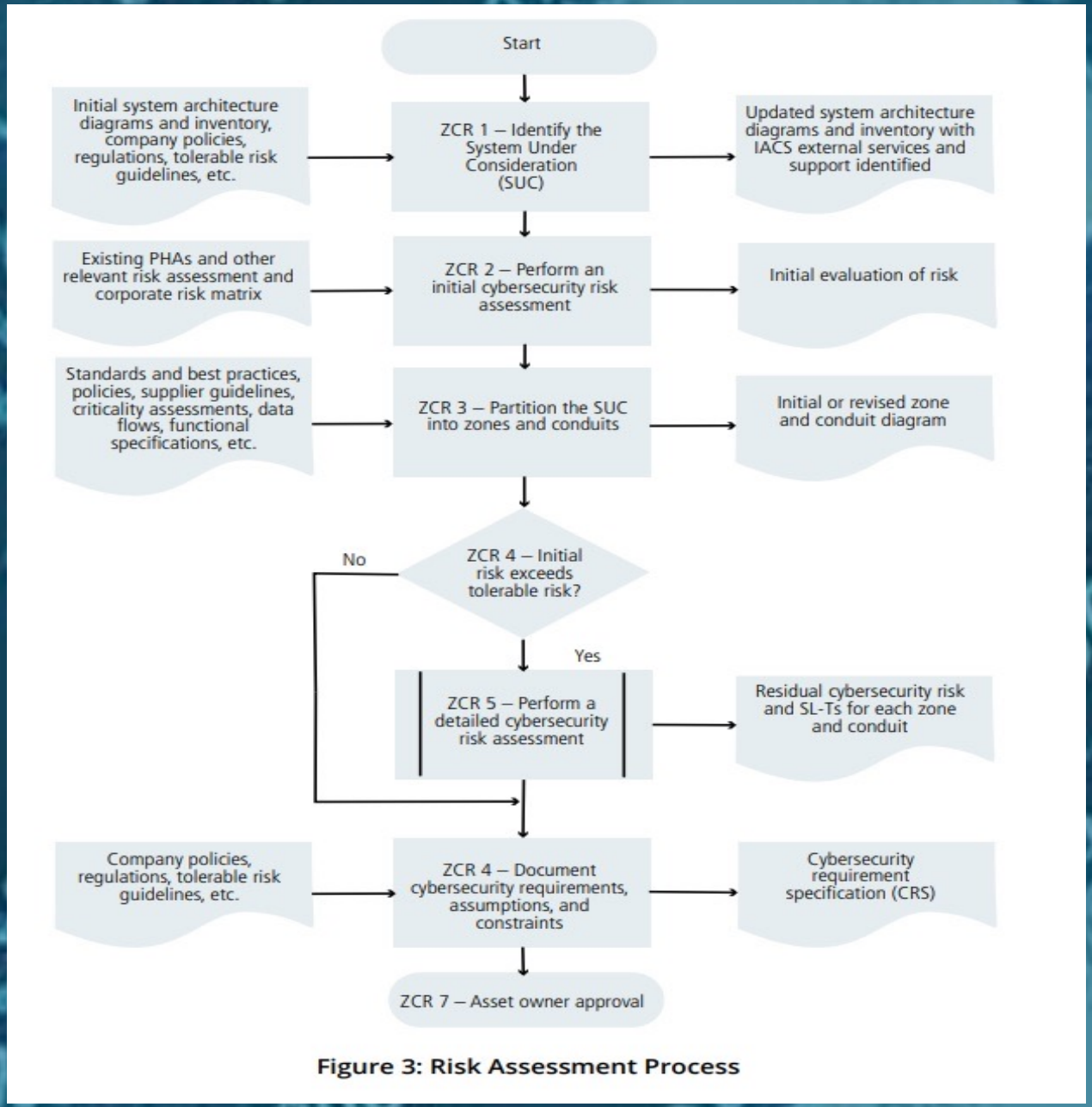



**Figure 3: Risk Assessment Process**

-Threat Modeling

Part 4-1 describes the requirements for the security development lifecycle (SDL) of Control System and Component products.

The security issues that are identified in the threat model must be reported in the final release
of the product and the threat model itself must be periodically updated during the product's lifecycle.

Foundational Requirements
(FRs) form the basis for technical requirements throughout the ISA/IEC 62443 Series. All aspects associated with achieve a desired IACS security level (people,
processes, and technology) are obtained  by complying with 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 called Access Control and they were split into two FRs to remain the total number of requirements at a manageable level.

## Security Levels

Security Level is considered 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 to differentiate 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)
- Target Security Levels (SL-T)
- Achieved Security Levels (SL-A)

| 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

# Maturity Model

While Security Levels are considere as 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 in a thorough manner..
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.

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

**Table 4: Maturity Level Definition**

**Design Principles.**

Secure by design is a design principle where security measures are implemented early in the lifecycle of the IACS.

-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**

Those are considered as the provision of multiple security protections.
Defense in depth indicate layers of security and detection, even on single systems, and requires attackers to break through or bypass multiple layers without being detected. Special attention must be paid to a single vulnerability that allows the potential compromise of multiple layers.

**-essential functions**

Those are considered as functions or capabilities that are required to maintain health, safety, the environment, and availability of the Equipment Under Control, they 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 substantial.
Part 3-3 requires that security measures do not affect essential functions of a high availability IACS unless it is supported by a Risk Assessment. The idea of essential functions places some design constraints on the design of IACS security measures:

- Access control shall not impede 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 impede safety instrumented functions from acting

# Roadmap for the ISA/IEC 62443 Series

## Principal Roles

To understand how to use the ISA/IEC 62443 Series you have toto understand the relationship between Roles, Control System, Automation Solution, and IACS.

Figure 4 visualizes this relationship.

• 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 expedite and assist in the activity to partition the System Under Consideration into Zones and Conduits and perform the Risk Assessment.

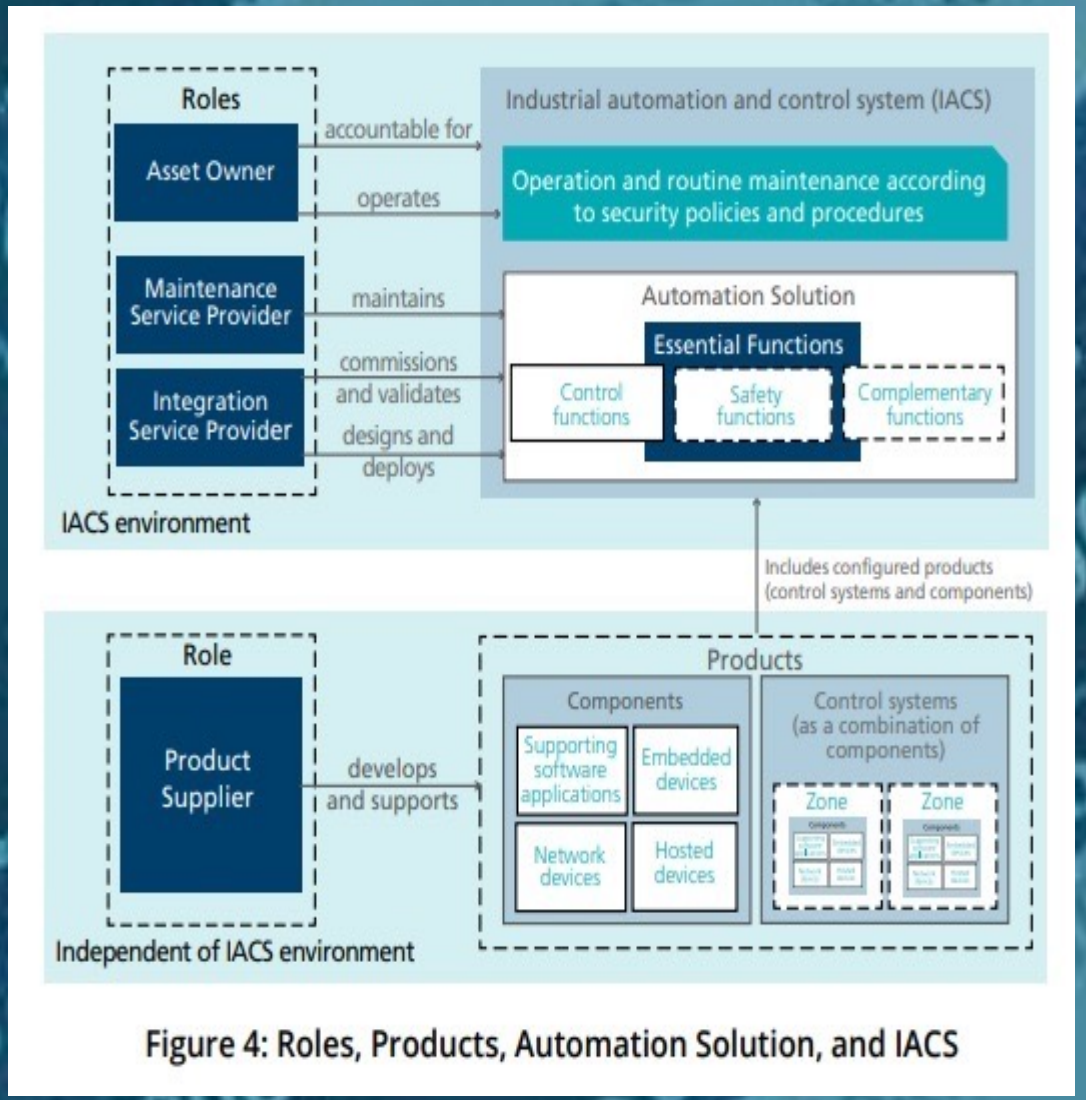



Figure 4: Roles, Products, Automation Solution, and IACS

• 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.

**Component, System, Automation Solution, and IACS**

- **IACS Components** are provided by a Product Supplier and include the following types:
• Embedded
• Host device
• Network device
• Software application

-Automation Solution is the accomplishment 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 .

**-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.

## Hierarchical View

Figure 5 presents 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 presents the direction of derivation.

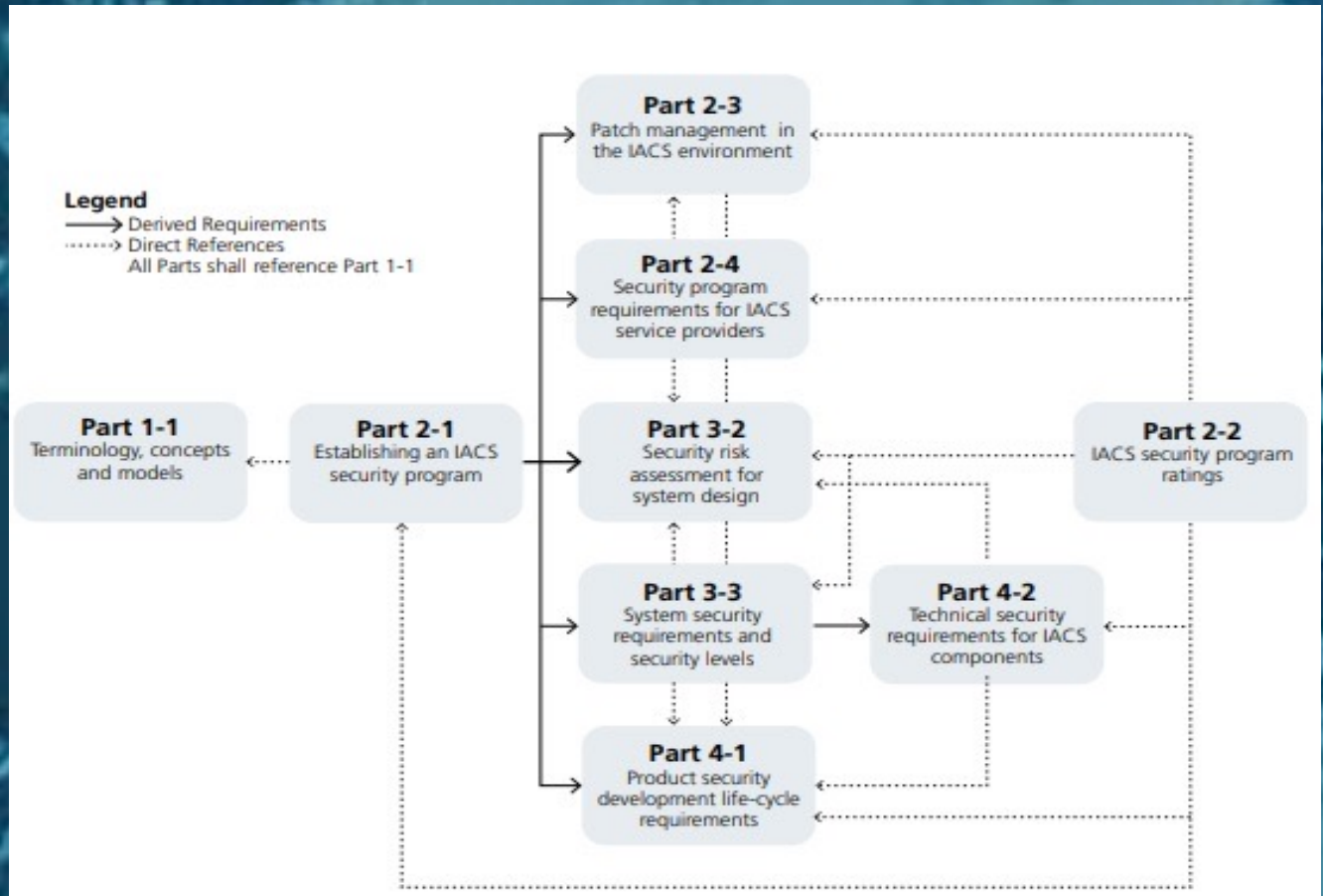



Figure 5: ISA/IEC 62443 Standards – Hierarchical View

• Part 1-1 introduces the ideas 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 considered 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.

•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

There are two independent lifecycles described in the series: the Product Development Lifecycle and the Automation Solution Lifecycle. The Automation Solution Lifecycle is further divided into an Integration Phase and an Operation and Maintenance Phase.

Table 6 presents the relationship between the Parts of the ISA/IEC 62443 Series and the various lifecycles and phases.

| Product Development Lifecycle | Automation Solution Lifecycle | |
|---|---|---|
| | Integration | Operation and Maintenance |
| 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 6: ISA/IEC 62443 Standards - Lifecycle View**

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**

**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**

## ISA/IEC 62443 Series for Service Providers

-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

Vessel consists mainly with number of OT devices .
(VDR, AMS, Main Engine /MOP PC, Digital Flow meter devices, ECDIS ,Loading PC, Ballast PC ,AIS)

I referred above some of the most important devices. As an **Administrator** have come across many times with issues by finding them with Legacy O.S ,unpatched ,without Antivirus installed, windows not activated ,having no password to logon as a user and unknown Administrator Password .

Basis on the regulations for Cybersecurity and in effort to protect IT and OT devices onboard I will explain to you, the ways and how I have implemented a more secure environment for these devices and what I recommend, that should be done on the part of the makers according to the ISA/IEC 62443 standards.

OT devices to Secure and Isolate .
Isolation of O.S (for those that have Windows installed )and Network Isolation .On OT we usually observe specific traffic protocols such as Profinet, Profibus, Modbus and BACnet RS-232,Canbus ,

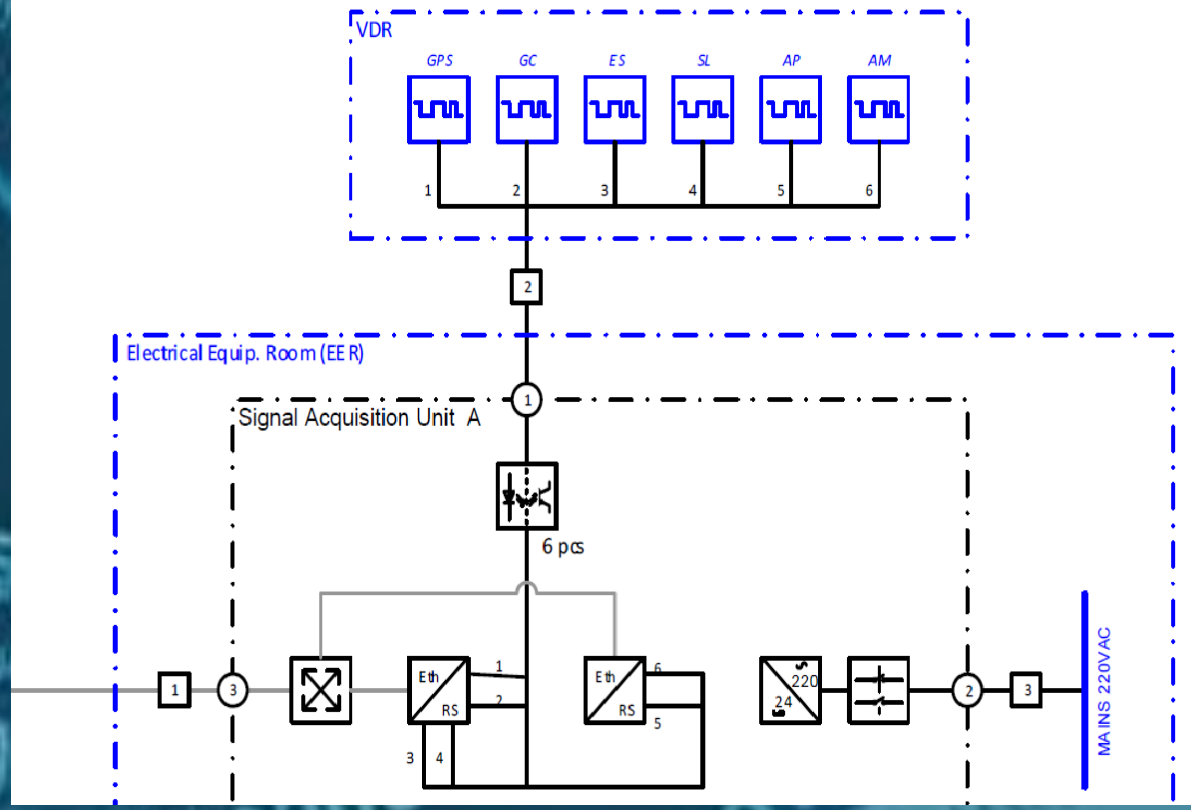
1. VDR
usually, vessels that have IoT Applications onboard then have the IoT device connected to take signals from SAU unit from : (GPS/GC/ES/SL/AP/AM)

2. AMS (Alarm Monitoring System)
We have AMS Computers or
AMS system Devices without Win OS

3a. PMI (Main Engine Program)
3b. Main Engine PC or Flow meter or Cylmate PC
3c. MOP PC

4. ECDIS
Usually Windows installed

*Global Position System*
*Gyrocompass*
*Echo Sound*
*Speed Log*
*Auto Pilot*
*Anemometer*



# examples of sub-components and equipment info of OT/ICS devices.

| Vessel | Sub-Components | Source of measurement | | | EQUIPMENT INFO | |
|---|---|---|---|---|---|---|
| Container | *SAU1 (ECR)* | | | | Device Model | Description |
| | [redacted] | Port 1: Shaft Measuring System | | | [redacted] | 4-RS to ethernet gateway |
| | | Port 3: Mass Flow Meter (Main Engine) | | | [redacted] | 2-RS to ethernet gateway |
| | | Port 4: Mass Flow Meter (Aux Engine) | | | [redacted] | 1-CAN to ethernet gateway |
| | [redacted] | Port 1: Alarming Monitoring System | | | [redacted] | 4-HART to ethernet gateway |
| | *SAU2 (Bridge)* | | | | [redacted] | 8ch analogue to ethernet gateway |
| | [redacted] | Port 1: GPS | | | [redacted] | 8ch discrete + pulses/freq counter to ethernet gateway |
| | | Port 2: Anemometer | | | | |
| | | Port 3: Gyrocompass | | | | |
| | | Port 4: Auto Pilot | | | | |
| | [redacted] | Port 1: Echo Sounder | | | | |
| | | Port 2: Speed Log | | | | |
| Bulk | *SAU1 (ECR)* | | | | | |
| | [redacted] | Port 2: Shaft Measuring System | | | | |
| | | Port 3: Mass Flow Meter (Main Engine) | | | | |
| | | Port 4: Mass Flow Meter (Aux Engine) | | | | |
| | [redacted] | Port 1: Alarming Monitoring System | | | | |
| | *SAU2 (Bridge)* | | | | | |
| | [redacted] | Port 1: GPS | | | | |
| | | Port 2: Anemometer | | | | |
| | | Port 3: Gyrocompass | | | | |
| | | Port 4: Auto Pilot | | | | |
| | [redacted] | Port 1: Echo Sounder | | | | |
| | | Port 2: Speed Log | | | | |

**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

**Published Standards and Technical Reports**

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 COMMITTE