Payatu

ALL YOU NEED TO KNOW ABOUT

ISA/IEC 62443 STANDARD

Copyright notice:

Table of Contents

About the Authors

AMIT MUSALE
Director, ICS/SCADA(OT) Security
Payatu

Amit Musale is the Director of ICS/SCADA(OT) Security at Payatu. In his vast experience in OT Security, Amit has made significant contributions towards Industrial Cyber Security, Cyber Security for Products in OT/IoT, Embedded Software Development for Networking Products Technology/Security Management for Products in ICS/SCADA, IoT, and Automotive Embedded.

He has worked with organizations like Kuwait Oil Company, Deloitte, Emerson, and a few MNCs.

ROHIT KUMAR
Senior Scada Security Engineer,
OT Security Engineer - Payatu

A security consultant with over four years of experience, Rohit is an established expert in ICS/SCADA security field experienced in assessing ICS/SCADA systems for vulnerabilities and conducting compliance assessments. Rohit has experience working in oil and gas, mining and metal manufacturing, power plants, and chemical plant vulnerability audits.

INTRODUCTION

OT (Operational Technology) can consist of a complex network of interactive ICS (Industrial Control Systems) or simply a small number of controllers. These systems receive information from remote sensors that measure and monitor process variables. From control valves to pressure gauges, an ICS sends commands and receives alerts from many different components.

It is used in various facilities like:

Nuclear Power Plant

Oil and Gas

Water/Wastewater management

Electrical Grids

Manufacturing Facilities

Pharmaceuticals

Chemical Plants

Mining and Metal

Building Automation

Dams

Defence Industrial Base

Food and Agriculture

Transportation Systems

As we discuss different components in IT such as web/database server and authentication server, we have similar components in OT, a few of which are as follows:

SCADA

SCADA is an abbreviation of Supervisory Control and Data Acquisition. It spans across huge geographical distances.
E.g. - Oil/Gas Pipeline Systems, Power Transmission & Distribution, Transportation, etc.

DCS

Distributed Control System, generally used in continuous processes.
E.g. Petroleum Refinery, Electricity Generation etc.

HMI

Human Machine Interface are Embedded-Computers that are used to monitor site operations.

PLC

The most critical component in a plant is PLCs, the abbreviation of PLC is Programmable Logic Controller which is used to control diverse types of physical equipment such as motors, valves, and thermal controllers.

OPC

OPC (OLE for Process Control) is one of the most important components of the OT technologies as it is useful in achieving interoperability.

RTU

RTU is the abbreviation of the Remote Terminal Unit. It is used to transmit data from the field to the DCS. RTU generally, monitors field analog and digital parameters and transmits data to SCADA Master Station. On pipeline and grid guarding system. Nowadays days PLCs with radio communication capabilities are available. Some are solar-powered RTUs as well.

ES

Engineering Station is mostly used to program the PLC.

Like every IT component, OT is also susceptible to threats. OT security should also be given equal attention. This is because OT consists of hazardous zones that are extremely critical and require human intervention putting human life at risk. Also, OT platforms are designed to work 24/7 365 days, any downtime due to any threat can lead to huge disasters in terms of human life as well as cost.

The ISA/IEC 62443 series is jointly developed by ISA and IEC committee to ensure the safety and security of Industrial Control systems (ICS) throughout their lifespan. There are presently four groups in which this standard is divided.

ISA/IEC 62443 covers not just the technology that makes up a control system, but also the procedures, countermeasures, and people that work on it. ISA/IEC 62443 adopts a risk-based approach to cyber security.

Payatu

THE ISA/IEC 62443 SERIES OF STANDARDS

The ISA/IEC 62443 series of standards is organized into four parts

GENERAL

Part 1 covers topics that are common to the entire series:
1-1 (TS): Terminology, concepts, and models

POLICIES AND PROCEDURES

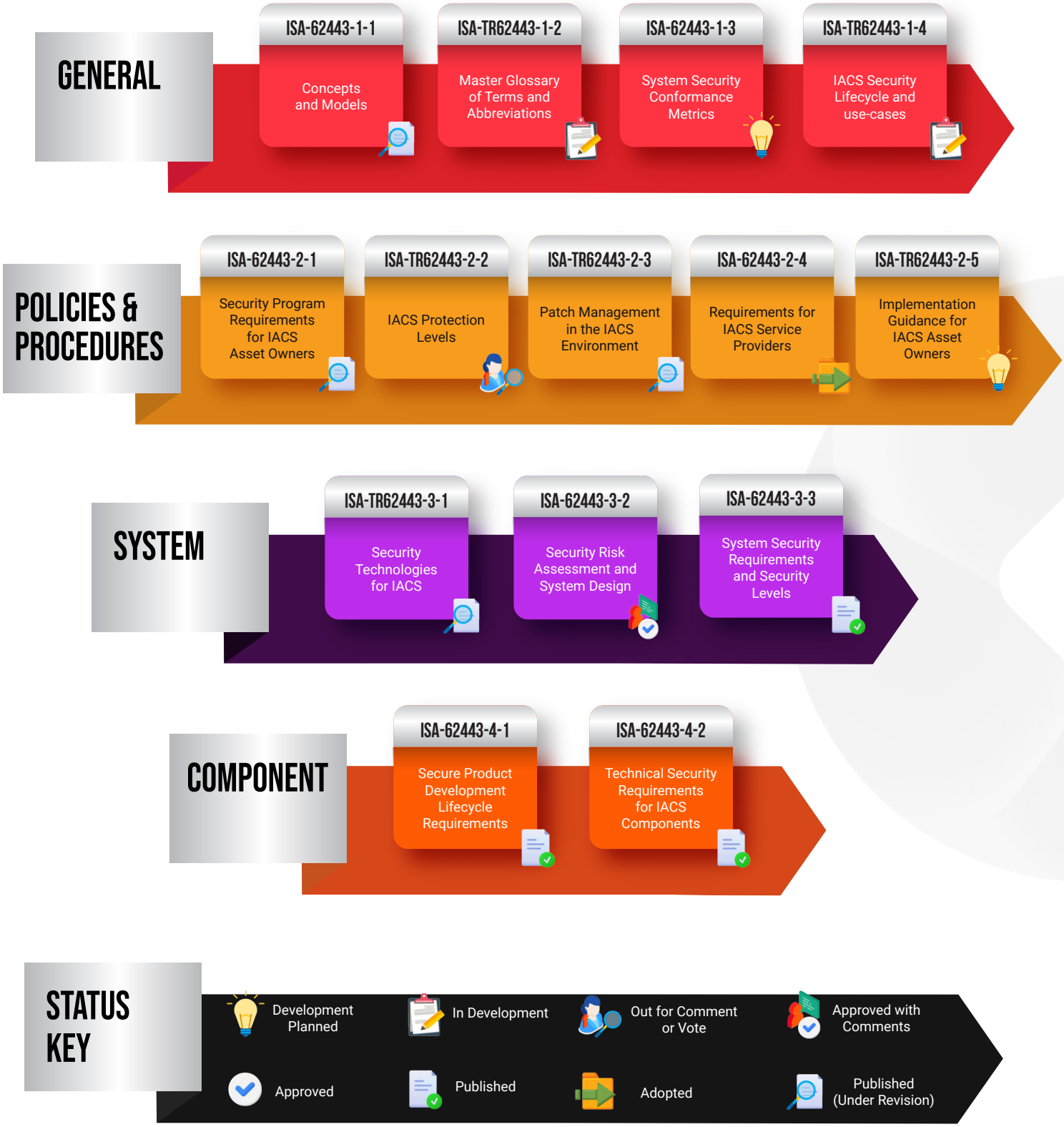
Part 2 focuses on methods and processes associated with IACS security:
2-1: Establishing an I ACS security program
2-3 (TR): Patch management in the IACS environment
2-4: Security program requirements for IACS service providers

SYSTEM

Part 3 is about requirements at the system level:
3-1: Security technologies for IACS
3-2: Security risk assessment for system design
3-3: Sy stem security requirements and security levels

COMPONENTS AND REQUIREMENTS

Part 4 provides detailed requirements for IACS products:
4-1: Secure product development lifecycle requirements
4-2: Technical security requirements for IACS components


GENERAL
ISA-62443-1-1
Concepts and Models
ISA-TR62443-1-2
Master Glossary of Terms and Abbreviations
ISA-62443-1-3
System Security Conformance Metrics
ISA-TR62443-1-4
IACS Security Lifecycle and use-cases
POLICIES & PROCEDURES
ISA-62443-2-1
Security Program Requirements for IACS Asset Owners
ISA-TR62443-2-2
IACS Protection Levels
ISA-TR62443-2-3
Patch Management in the IACS Environment
ISA-62443-2-4
Requirements for IACS Service Providers
ISA-TR62443-2-5
Implementation Guidance for IACS Asset Owners
SYSTEM
ISA-TR62443-3-1
Security Technologies for IACS
ISA-62443-3-2
Security Risk Assessment and System Design
ISA-62443-3-3
System Security Requirements and Security Levels
COMPONENT
ISA-62443-4-1
Secure Product Development Lifecycle Requirements
ISA-62443-4-2
Technical Security Requirements for IACS Components
STATUS KEY
Development Planned
In Development
Out for Comment or Vote
Approved with Comments
Approved
Published
Adopted
Published (Under Revision)

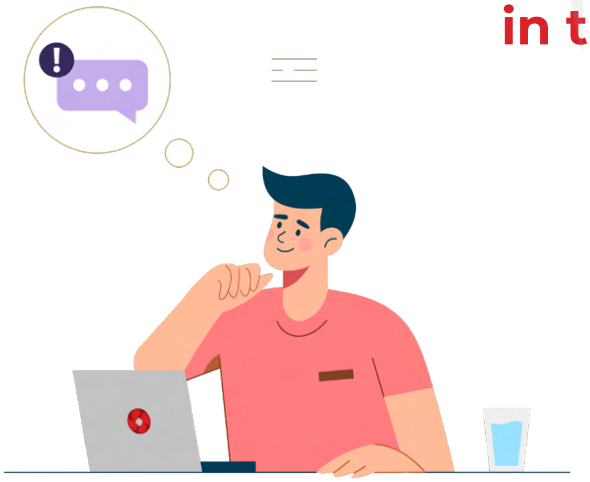
ISA/IEC 62443 is created with the goal of guiding the development of ICS components to secure-by-design and manage by an OT-centric security management system with rules, processes, periodic reviews, specific requirements, and best practices.

However, novice users may be intimidated by its large, comprehensive collection that contains numerous papers and a wealth of information.

ISA/IEC 62443 gives responsibility to everyone:

- Asset Owners (AO)
- System Integrators (SI), Service Providers
- Operators
- Product Supplier (PS)

What is your role in the Ecosystem?



There are two independent lifecycles explained in the series.

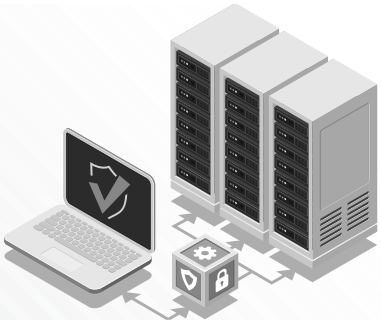
1. **Product Development Lifecycle**
2. **Automation Solution Lifecycle**

- Integration Phase
- Operation & Maintenance Phase

Below table explains the applicability of standard documents:

	Activities	Applicability
ASSET OWNER	• 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	62443-2-1 62443-2-2 62443-2-3 62443-2-4 62443-3-2 6244 3-3-3
INTEGRATION SERVICE PROVIDER	• 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	62443-2-1 62443-2-3 62443-2-4 62443-3-2 62443-3-3
MAINTENANCE SERVICE PROVIDER	• 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	62443-2-3 62443-2-2 62443-2-4
PRODUCT SUPPLIER	• 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	62443-4-1 62443-4-2 62443-3-2 62443-3-3

TO BEGIN WITH, WE NEED TO KNOW OVERALL STRUCTURE OF ISA/IEC 62443



ISA/IEC 62443-1-1: Models and Concepts:
According to the definition ICS is a "collection of processes, persons, hardware, and software that can impact or influence the safe, secure, and reliable functioning of an industrial process,"

ISA/IEC 62443-1-2: Master Glossary of Terms and Abbreviations:
This document sets the core taxonomy and principles for the whole standards collection and should be read before digging into the other standards components.

ISA/IEC 62443-1-3: System Security Compliance Metrics
In accordance with this document, an industrial automation and control system must meet certain high-priority cybersecurity compliance criteria (ICS).

ISA/IEC 62443-1-4: Security Life Cycle and Use Cases
Provides a more detailed description of the underlying lifecycle for ICS security, as well as several use cases that illustrate various application

ISA/IEC 62443-2-1: Requirements for an ICS Security Management System
Gives guidance on how to create the components needed for an industrial automation and control systems (ICS), cyber security management system (CSMS).
The parts of a CSMS outlined in this standard are mostly linked to policy, process, practices, and personnel, and they specify what should or must be included in the organization's final CSMS.

ISA/IEC 62443-2-2: Implementation Guidance for an ICS Security Management System
Provides a methodology for evaluating the level of protection provided by an operational ICS against the requirements in the ISA/IEC 62443 Series of standards.

ISA/IEC 62443-2-3: Patch Management in the ICS Environment
IEC 62443-2-3 recommends a defined format for the distribution of information about security patches from asset owners to IASC product suppliers. It also covers some of the activities associated with the development and deployment of ICS patches.

ISA/IEC 62443-2-4: Requirements for ICS Solution Suppliers
This provides a detailed list of requirements for ICS service providers that may be utilized during integration and maintenance.
It also serves as the foundation for ISA/IEC 62443 standard to create "profiles" that address the

subtleties and reality of various industrial contexts, such as the distinct needs of oil and gas producer's vs those of electricity generation and distribution.

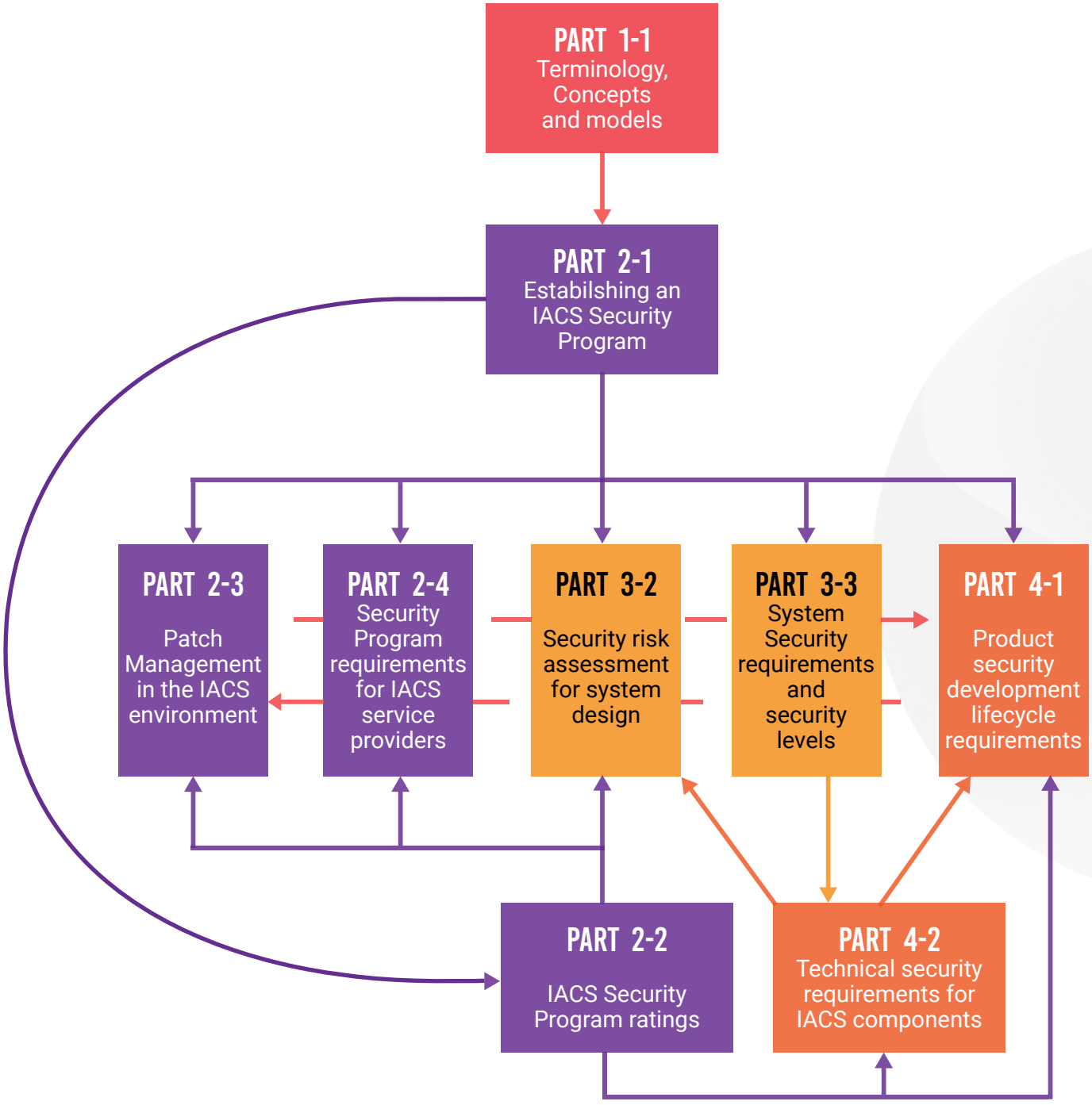
ISA/IEC 62443-3-1: Security Technologies for ICS
Describes the application of various security technologies to an ICS environment. The intended audience includes anyone who wishes to learn more about the applicability of specific technologies in a control systems environment.

ISA/IEC 62443-3-2: Security Risk Assessment, System Partitioning, and Security Levels
This is based on the belief that ICS security is a risk management issue and the fact that risk to an organization is based on the relevant threat impact, vulnerability exposure & likelihood and asset value. Based on such inputs, ISA/IEC 62443-3-2 can assist in solution engineering by directing the identification/application of security countermeasures to decrease risk to acceptable level regarding designated security levels, zones, conduits, and other security principles.

ISA/IEC 62443-3-3: System Security Requirements and Security Levels
This discusses ICS components' Security Levels. Security levels help us understand resilience to purposeful or accidental cyber-attacks.

ISA/IEC 62443-4-1 and ISA/IEC 62443-4-2 : Product Security Development Life-Cycle Requirements
This specifies the process requirements for generating and maintaining secure products in an ICS, as well as a secure development lifecycle for producing and maintaining secure products. These standards can be applied to new or current hardware, software, or firmware development, maintenance, and retirement procedures. The 62443-4-1 and 4-2 lifecycle criteria is primarily directed at developers and suppliers.

Below is the hierarchical relationship between ISA/IEC 62443 Series standards. The arrowhead shows the direction of derivation :



UNDERSTANDING THE TWO(2) LIFECYCLE VIEWS OF ISA/IEC 62443 STANDARD

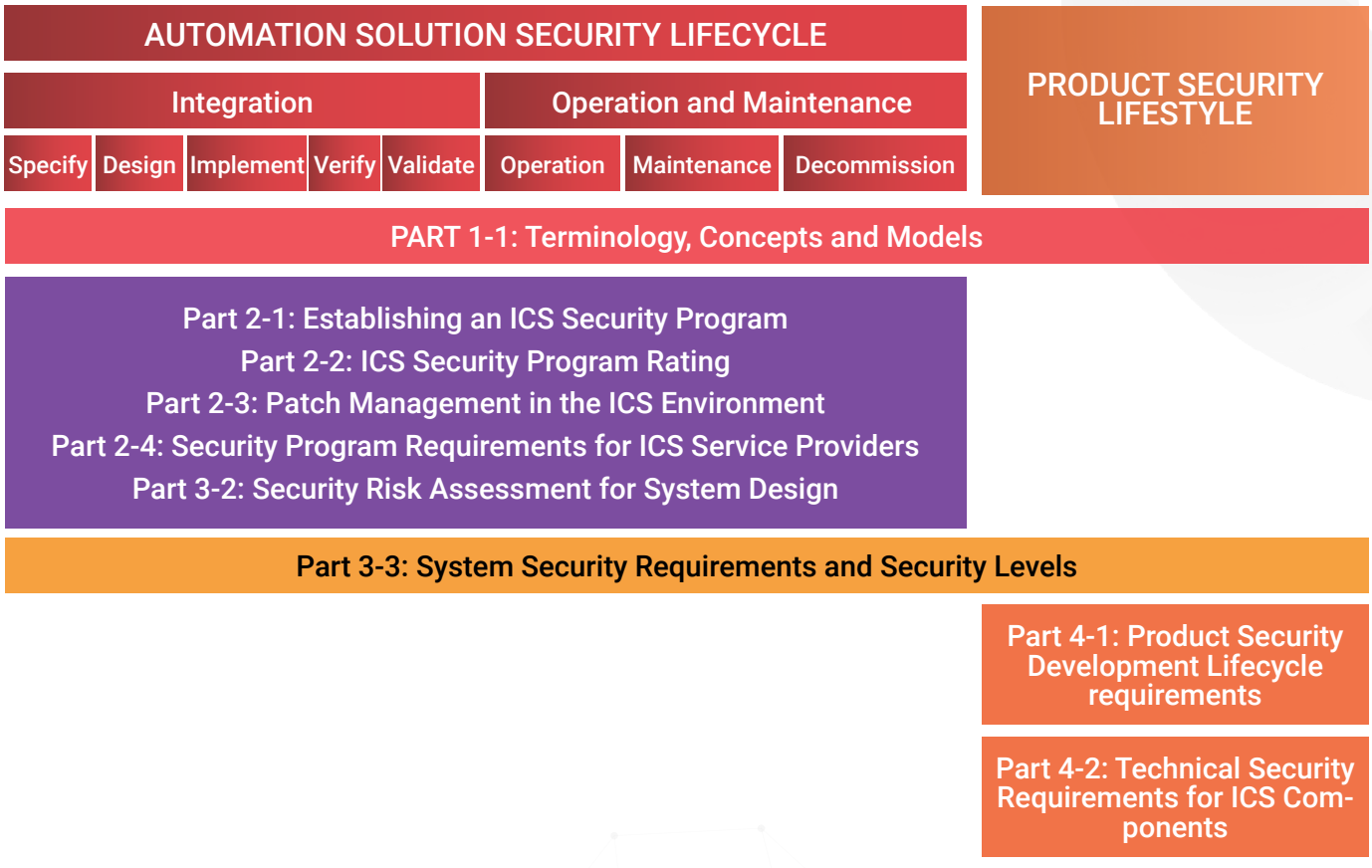
The series outlines two distinct lifecycles:

1. The Automation Solution Security Lifecycle.
2. The Product Security Lifecycle.

Furthermore, there are two subsequent phases that make up the Automation Solution Lifecycle:

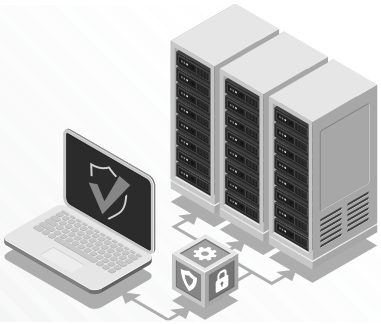
a. Integration phase
b. Operations and Maintenance phase

Below diagram illustrates the connection that exists between the ISA/IEC 62443 Series' Parts and the many different lifecycles and stages :-



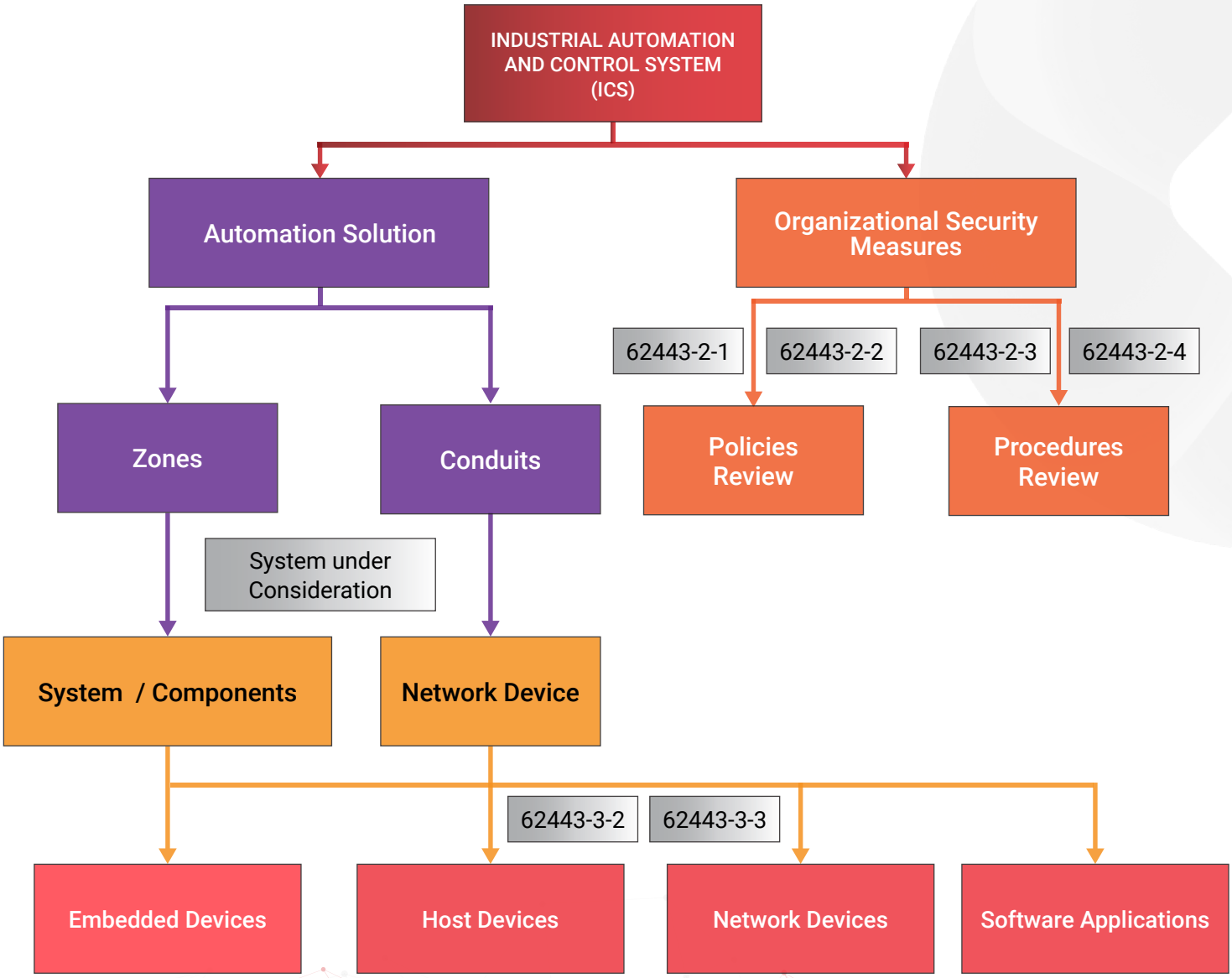
Payatu

HOLISTIC RISK ASSESSMENT BASED ON 62443

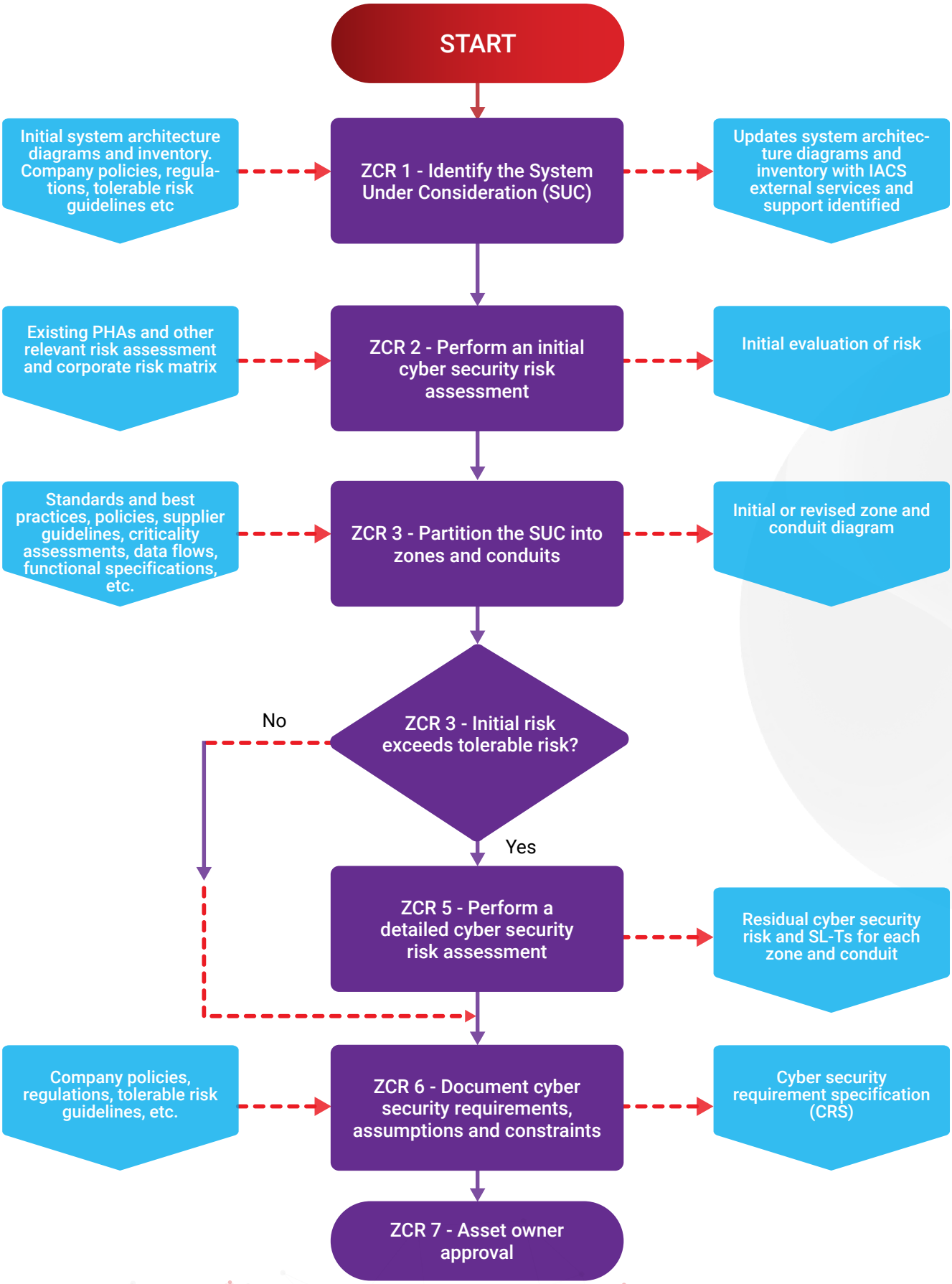


The specifications for handling the cybersecurity concerns in an ICS, including the use of Zones and Conduits and Security Levels, are described in Part 3-2.
Despite the fact that Part 3-2 contains the requirements for the risk assessment process, it does not outline the precise technique to be applied.

The Asset Owner is responsible for developing the methodology, which must be in line with the organization's overall approach to risk assessment.



Process to Assess the Current State :



The flow chart can be simplified into following steps :

STEP 1:
Defining the SuC for an industrial automation and control system (ICS) and its associated networks.

STEP 2:
Partitioning the SuC into zones and conduits.

STEP 3:
Assessing the risk for each zone and conduit and establishing the technical measure security level targets (SL-T) for each zone and conduit.

STEP 4:
Documenting the security requirements needed to design, implement, operate and maintain effective technical security measure.
A furthermore detailed assessment is required if Initial risk exceeds the tolerable risk.

Zones and Conduits

A Zone is described as a collection of logical or physical assets based on risk or other factors like the importance of the assets, their operational purpose, their physical location, their necessary access, or the organization in charge of them.

A logical collection of communication channels that connect two or more zones and have similar security needs is referred to as a conduit.

Partitioning the System Under Consideration into distinct Zones and Conduits is a crucial step in the risk assessment process.

In order to build a set of common security standards that lower cybersecurity risk, it is intended to identify those assets that share common security features.

By reducing the potential impact of a successful cyberattack, partitioning the system under consideration into zones and conduits can help lower overall risk.
Part 3-2 requires or recommends that some assets are partitioned as follows:

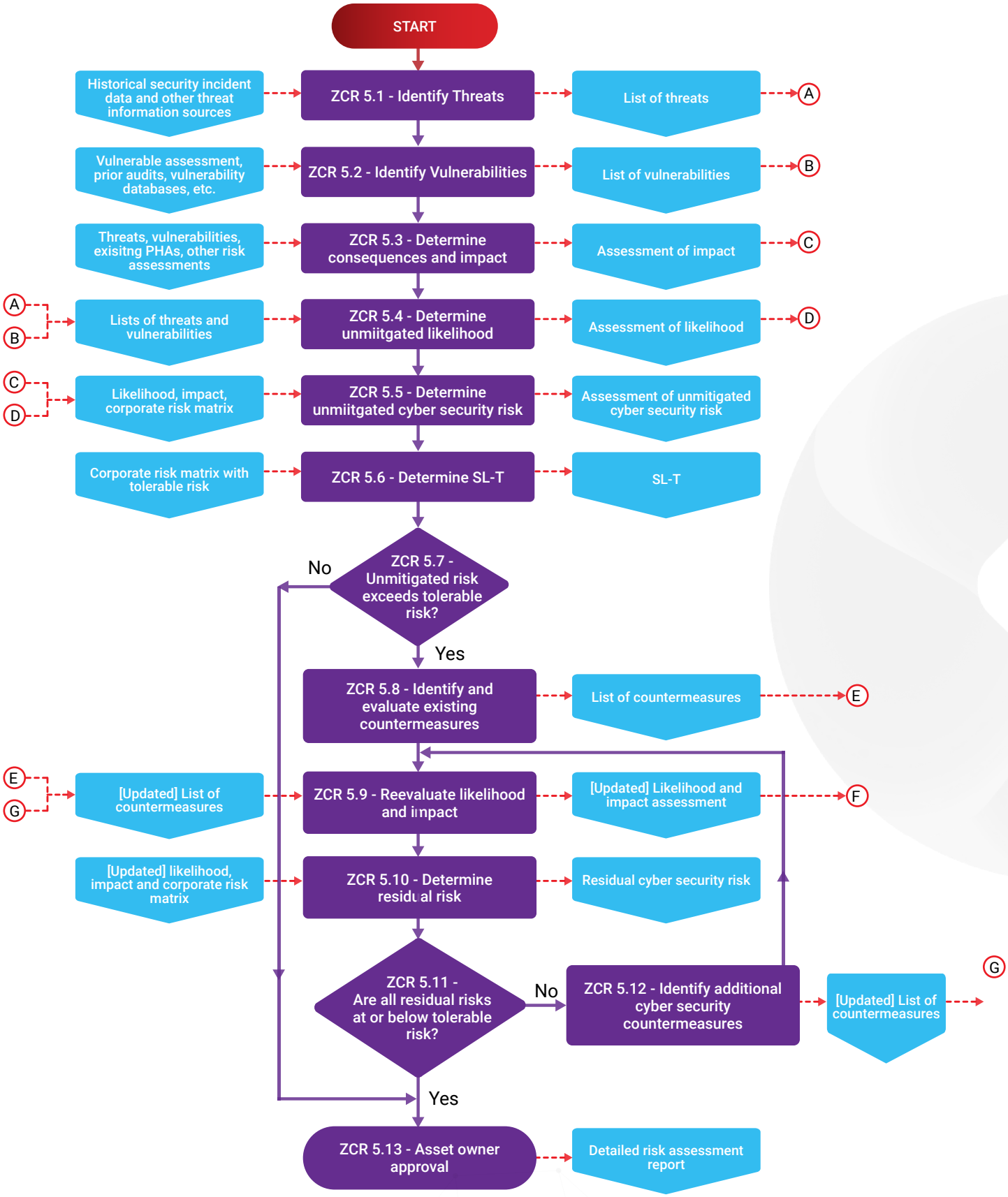
- A zone should have a clear border,
- A zone can have other subzones that meet the security requirements of the primary zone,
- Assets within the zone must be protected to an adequate security level (SL-T)
- Outside assets have a different set of rules,
- The border is used to define access with another zone or outside the system,
- Access is via electronic communication channels or the physical movement of people or equipment.
- Accesses are functionally grouped into conduits.

All of these requirements are documented in ISA/IEC 62443-3-2, including assigning attributes to zones, which have a common set of security features and requirements.

The following attributes should be documented when creating a report based on ISA/IEC 62443-3-2:

- Name and/or identifier (unique)
- Lead organization
- Functional security qualification
- Logical and physical boundaries (if applicable)
- List of border access points and equipment
- List of dataflows associated with each access point
- Connected zones and conduits
- List of assets and related risks
- Target security level (SL-T)
- Applicable security requirements (general and specific)
- Applicable security policies and procedures (general and specific)
- Dependence on external factors (regulations)
- Risk matrix

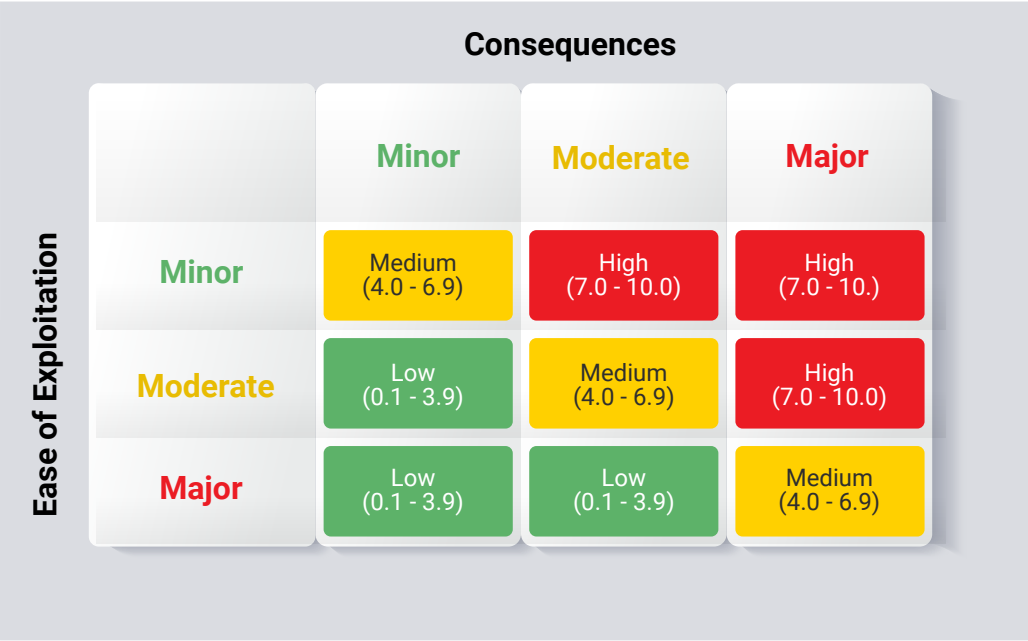
To conduct more detailed security assessment risk, one must refer the following flow chart :



Calculating the Risk matrix

Risk is defined as a measure of human harm, environmental damage, economic loss, intellectual property loss, or loss of privacy in terms of both the chance of the incidence and the severity of the loss or injury.

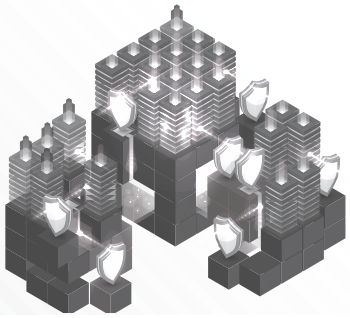
A simplified form of this relationship states risk as the product of the likelihood and consequences of an incidence (i.e., risk = consequence x likelihood).



Minor	Issues that require immediate attention by management. The controls in existence are not able to mitigate these risks.
Medium	Existing controls are not able to mitigate risks, but the risk impact is not high. To improve control or monitor risk consequence, to ensure it does not increase over time.
Low	Issue has been fully or partially mitigated. However, continuous monitoring of controls is needed, i.e. at least quarterly.

Payatu

UNDERSTANDING FOUNDATIONAL REQUIREMENTS AND SECURITY LEVELS



Below listed are the 7 foundational requirements used in series:-

FR1 — IDENTIFICATION, AUTHENTICATION CONTROL AND ACCESS CONTROL (AC)
Identifies and authenticates all users (human, process, and equipment) before allowing access to the IACS.

FR2 — USER CONTROL (UC)
Ensures that all identified users (human, process, and device) have privileges to perform the required actions on the system and monitors the use of those privileges.

FR3 — DATA INTEGRITY (DI)
Ensures the integrity of equipment and information (protection against unauthorized changes) in communication channels and storage directories.

FR4 — DATA CONFIDENTIALITY (DC)
Ensures that information flowing through communication channels and storage directories is not distributed.

FR5 — RESTRICT DATA FLOW (RDF)
Segments the system into zones and conduits to avoid unnecessary data propagation.

FR6 — TIMELY RESPONSE TO EVENTS (TRE)
Responds to security breaches with timely reporting and timely decision making.

FR7 — RESOURCE AVAILABILITY (RA)
Ensures system and asset availability during denial-of-service attacks.

There are a number of specific technical security requirements (SR) and requirement improvements (RE) for each of the foundational requirements, and they are categorised across four security levels based on the degree to which they mitigate threats.

To achieve a specific level of security, it is necessary to meet both the baseline standards (SR) and any modifications to those SR (RE)that have been specified.

A security requirement may be met either directly or by the use of a compensating countermeasure, as both are anticipated by the standard.

Even if some requirements cannot be directly achieved, a certain level of security can be reached thanks to the concept of compensating countermeasures.

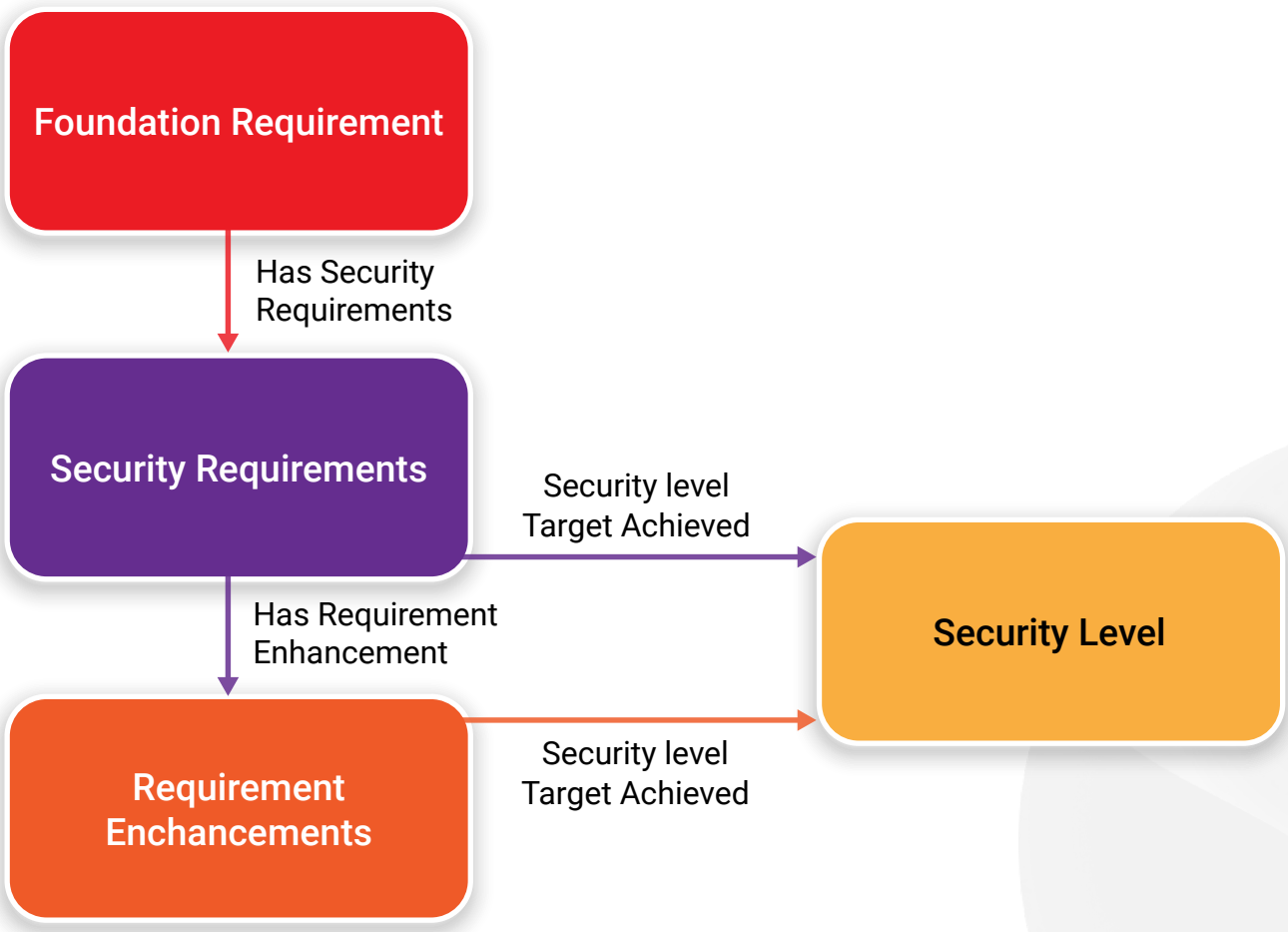
It's possible, for instance, that certain parts, especially older machinery, lack the capability to run the necessary technological functions.

The security levels defined by the standard represent the confidence that a system, zone, and/or its components can provide the desired level of security.

These security levels should be matched to each essential requirement (Foundational Requirements - FRs).

Security Levels	Skills	Motivation	Means	Resources
SL 1 - Staff	No Attack Skills	Mistakes	Non-Intentional	Individual
SL 2 - Low Level Hacker	Generic	Low	Simple	Low
SL 3 - Hacker, Terrorist	System Specific	Moderate	Sophisticated (Attack)	Moderate (Hacker Groups)
SL 4 - Nation State	System Specific	High	Sophisticated (Campaign)	Extended (Multi-Disciplinary Teams)

Below representation can help to co-relate Foundational Requirement, Security Requirements Requirement enhancements and Security level achieved.



Below representations shows the applicability of Foundational requirement and Security level target achieved.

FR 1 - Identification and Authentication

FR 1 - SRs and REs	Security Levels			
	SL1	SL2	SL3	SL4
SR 1.1 - Human User Identification and Authentication	Y	Y	Y	Y
SR 1.1 RE 1 - Unique Identification and Authentication		Y	Y	Y
SR 1.1 RE 2 - Multifactor Authentication for untrusted networks			Y	Y

FR 2 - User Control (UC)

FR 2 - SRs and REs	Security Levels			
	SL1	SL2	SL3	SL4
SR 2.1 - Authorization Enforcement	Y	Y	Y	Y
SR 2.1 RE 1 - Authorization Enforcement for all users		Y	Y	Y
SR 2.1 RE 2 - Permission mapping to roles		Y	Y	Y

FR 3 - System Integrity (SI)

FR 3 - SRs and REs	Security Levels			
	SL1	SL2	SL3	SL4
SR 3.1 - Communication Integrity	Y	Y	Y	Y
SR 3.1 RE 1 - Cryptographic Integrity Protection			Y	Y
SR 3.2 - Malicious Code Protection		Y	Y	Y

FR 4 - Data Confidentiality (DC)

FR 4 - SRs and REs	Security Levels			
	SL1	SL2	SL3	SL4
SR 4.1 - Information Confidentiality	Y	Y	Y	Y
SR 4.1 RE 1 - Protection of Confidentiality at rest or in transit via untrusted networks		Y	Y	Y
SR 4.1 RE 2 - Protection of Confidentiality across zone boundaries			Y	Y

FR 5 - Restricted data flow (RDF)

FR 5 - SRs and REs	Security Levels			
	SL1	SL2	SL3	SL4
SR 5.1 - Network Segmentation	Y	Y	Y	Y
SR 5.1 RE 1 - System Network Segmentation		Y	Y	Y
SR 5.1 RE 2 - Independence from non-control system networks			Y	Y

FR 6 - Timely Response to Events (TRE)

FR 6 - SRs and REs	Security Levels			
	SL1	SL2	SL3	SL4
SR 6.1 - Audit Log Accessibility	Y	Y	Y	Y
SR 6.1 RE 1 - Programmatic Access to Audit Logs			Y	Y
SR 6.2 - Continious Monitoring		Y	Y	Y

FR 7 - Resource Availability (RA)

FR 7 - SRs and REs	Security Levels			
	SL1	SL2	SL3	SL4
SR 7.1 - Denial of Service Protection	Y	Y	Y	Y
SR 7.1 RE 1 - Manage communication loads		Y	Y	Y
SR 7.1 RE 2 - Limit DoS effects to other systems or networks			Y	Y

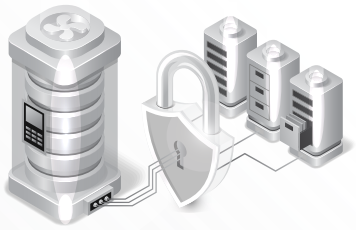
Policy and procedures review based on ISA/IEC 62443-2-1, 2-2, 2-3, 2-4

Policy and procedures review is an important phase in conducting security risk assessment. The ICS policy of the firm must be adhered all of the devices in the ICS environment. The policy must coincide with the organization's overall security objectives and goals in order to guarantee that all of the established security goals have been satisfied.

Below mentioned are some examples of what must be covered under policies and procedures:

1. Network Configuration review
2. Host Configuration review
3. Firewall configuration review
4. Incident response plan
5. Internet and email policy
6. Identification and Authentication
7. Business continuity plan & its annual review
8. Risk management plans
9. Maintenance policy
10. Awareness
11. Training
12. Other documents

PRODUCT SECURITY LIFECYCLE (ISA/IEC 62443-4-1 & 62443-4-2)



ISA/IEC 62443-4-1 Product development requirements

The development life cycle includes defining security requirements, making sure the design is secure, making sure the implementation is secure (which includes coding guidelines), verifying and validating, managing bugs and patches, and deciding when a product is done being used.

The above listed procedures and tasks are applicable to both new and established methods for creating, sustaining, and retiring hardware, software, and firmware. The key practices identified by ISA/IEC 62443-4-1 are:

1. Security Management (SM)
2. Specification for security requirements (SR)
3. Security by design (SD)
4. Secure implementation (SI)
5. Security verification and Validation testing (SVV)
6. Management of Security related issues (DM)
7. Security update management (SUM)
8. Security guidelines (SG)

Further each practice has its own purpose. The purpose of the security management practices is to guarantee that the security-related actions are appropriately planned, recorded, and carried out throughout the entirety of the product's life-cycle.

Each practice has its own purpose and are represented below in the table:

1. Security Management (SM)	
I.	Development process
II.	Identification of responsibilities
III.	Identification of applicability
IV.	Security expertise
V.	Process scoping
VI.	File integrity
VII.	Development environment security
VIII.	Controls of private keys
IX.	Security requirements for externally provided components
X.	Custom developed components from third-party suppliers
XI.	Assessing and addressing security related issues
XII.	Process verification
XIII.	Continuous improvement
2. Specification for security requirements (SR)	
I.	Product security context
II.	Threat model
III.	Product security requirements
IV.	Product security requirements content
V.	Security Requirements review
3. Secure by design (SD)	
I.	Secure design principles
II.	Defence in depth design
III.	Security design review
IV.	Secure design best practices
4. Secure implementation (SI)	
I.	Security Implementation review
II.	Secure coding standards
5. Security verification and validation testing (SVV)	
I.	Security requirement testing
II.	Threat mitigation testing
III.	Vulnerability testing
IV.	Penetration testing
V.	Independence of testers
6. Management of security related issues(DM)	
I.	Receiving notifications of security related issues
II.	Reviewing security related issues
III.	Assessing security related issues
IV.	Addressing security related issues
V.	Disclosing security related issues
VI.	Periodic review of security defect management practice

7. Security update management	
I.	Security update qualification
II.	Security update documentation
III.	Dependent components or operating system security update documentation
IV.	Security update delivery
V.	Timely delivery of security patches
8. Security guidelines	
I.	Product defence in depth
II.	Defence in depth measure expected in the environment
III.	Security hardening guidelines
IV.	Secure disposal guidelines
V.	Secure operations guidelines
VI.	Account management guidelines
VII.	Documentation review

this article is mostly about embedded software applications, which are mostly related to OT.

ISA/IEC 62443-4-2 Technical security requirement for ICS components

ISA/IEC 62443-4-2 defines the requirements for control system capability security levels and their components, as well as providing the technical control system component requirements (CRs) linked with the seven foundational requirements (FRs)

There are a total of seven foundational requirements (FRs):

a) Identification and authentication control (IAC),
b) Use control (UC),
c) System integrity (SI),
d) Data confidentiality (DC),
e) Restricted data flow (RDF),
f) Timely response to events (TRE), and
g) Resource availability (RA).

These seven FRs are the foundation for defining control system security capability levels. Defining security capability levels for the control system component is the goal and objective of ISA/IEC 62443-4-2. The SR(s) defined in ISA/IEC 62443 is represented as CR(s) or Component requirements. CRs, like SRs, contain Requirements Enhancements (REs), which must be completed depending on the security level desired.

The IEC 62443-4-2 standard differentiates between four types of components found in an industrial control system:

- Software applications such as SCADA or antivirus software as Software application requirements (SARs).
- Embedded devices such as PLC, DCS, and IEDs (Intelligent Electronic Devices) as Embedded device requirements (EDRs),
- Host devices such as engineering stations, Data historian and the operations computer as Host device requirements (HDRs),
- Network devices such as firewalls, switches and routers as Network device requirements (NDRs).

Below representation is mapping of FR and SLs.

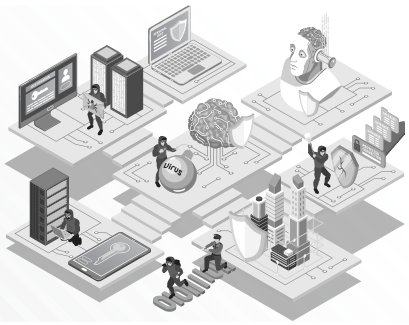
SRs and REs	SL 1	SL 2	SL 3	SL 4
FR 1 - Identification and authentication control (IAC)				
CR 1.1 - Human user identification and authentication	✓	✓	✓	✓
RE (1) Unique identification and authentication:		✓	✓	✓
RE (2) Multifactor authentication for all interfaces			✓	✓
CR 1.2 - Software process and device identification and authentication		✓	✓	✓
RE (1) Unique identification and authentication:			✓	✓
CR 1.3 - Account management	✓	✓	✓	✓
CR 1.4 - Identifier management	✓	✓	✓	✓
CR 1.5 - Authenticator management	✓	✓	✓	✓
RE (1) Hardware security for authenticators			✓	✓
NDR 1.6 - Wireless access management	✓	✓	✓	✓
RE (1) Unique identification and authentication:		✓	✓	✓
CR 1.7 - Strength of password-based authentication	✓	✓	✓	✓
RE (1) Password generation and lifetime restrictions for human users			✓	✓
RE (2) Password lifetime restrictions for all users (human, software process, or device)				✓
CR 1.8 - Public key infrastructire certificates		✓	✓	✓
CR 1.9 - Strength if public key-based authentication		✓	✓	✓
RE (1) Hardware security for public key-based authentication			✓	✓
CR 1.10 - Authenticator feedback	✓	✓	✓	✓
CR 1.11 - Unsuccessful login attempts	✓	✓	✓	✓
CR 1.12 - System use notification	✓	✓	✓	✓
NDR 1.13 - Access via untrusted networks	✓	✓	✓	✓
RE (1) Explicit access request approval			✓	✓
CR 1.14 - Strength of symmetric key-based authentication		✓	✓	✓
RE (1) Hardware security for symmetric key-based authentication			✓	✓

SRs and REs	SL 1	SL 2	SL 3	SL 4
FR 2 - Use control (UC)				
CR 2.1 - Authorization enforcement	✓	✓	✓	✓
RE (1) Authorization enforcement for all users (humans, software processes and devices)		✓	✓	✓
RE (2) Permission mapping to roles		✓	✓	✓
RE (3) Supervisor override			✓	✓
RE (4) Dual approval				✓
CR 2.2 - Wireless use control	✓	✓	✓	✓
CR 2.3 - Use control for portable and mobile devices				
SAR 2.4 - Mobile code	✓	✓	✓	✓
RE (1) Mobile code authenticity check		✓	✓	✓
EDR 2.4 - Mobile code	✓	✓	✓	✓
RE (1) Mobile code authenticity check		✓	✓	✓
HDR 2.4 - Mobile code	✓	✓	✓	✓
RE (1) Mobile code authenticity check		✓	✓	✓
NAR 2.4 - Mobile code	✓	✓	✓	✓
RE (1) Mobile code authenticity check		✓	✓	✓
CR 2.5 - Session lock	✓	✓	✓	✓
CR 2.6 - Remote session termination		✓	✓	✓
CR 2.7 - Concurrent session control			✓	✓
CR 2.8 - Auditable events	✓	✓	✓	✓
CR 2.9 - Audit storage capacity	✓	✓	✓	✓
RE (1) Warn when audit record storage capacity threshold reached			✓	✓
CR 2.10 - Response to audit processing failures	✓	✓	✓	✓
CR 2.11 - Timestamps	✓	✓	✓	✓
RE (1) Time synchronization		✓	✓	✓
RE (2) Protection of time source integrity				✓
CR 2.12 - Non-repudiation	✓	✓	✓	✓
RE (1) Non-repudiation for all users				✓
EDR 2.13 - Use of physical diagnostic and test interfaces		✓	✓	✓
RE (1) Active monitoring			✓	✓
HDR 2.13 - Use of physical diagnostic and test interfaces		✓	✓	✓
RE (1) Active monitoring			✓	✓
NDR 2.13 - Use of physical diagnostic and test interfaces		✓	✓	✓
RE (1) Active monitoring			✓	✓

SRs and REs	SL 1	SL 2	SL 3	SL 4
FR 3 - System Integrity (SI)				
CR 3.1 - Communication integrity	✓	✓	✓	✓
RE (1) Communication authentication		✓	✓	✓
SAR 3.2 - Protection from malicious code	✓	✓	✓	✓
EDR 3.2 - Protection from malicious code	✓	✓	✓	✓
HDR 3.2 - Protection from malicious code	✓	✓	✓	✓
RE (1) Report version of code protection		✓	✓	✓
NDR 3.2 - Protection from malicious code	✓	✓	✓	✓
CR 3.3- Security functionality verification	✓	✓	✓	✓
RE (1) Security functionality verification during normal operation				✓
CR 3.4 - Software and information integrity	✓	✓	✓	✓
RE (1) Authenticity of software and information		✓	✓	✓
RE (2) Automated notification of integrity violations			✓	✓
CR 3.5 - Input violation	✓	✓	✓	✓
CR 3.6 - Deterministic output	✓	✓	✓	✓
CR 3.7 - Error handling	✓	✓	✓	✓
CR 3.8 - Session integrity		✓	✓	✓
CR 3.9 - Protection of audit information		✓	✓	✓
RE (1) Audit record on write-once media				✓
EDR 3.10 - Support for updates	✓	✓	✓	✓
RE (1) Update authenticity and integrity		✓	✓	✓
HDR 3.10 - Support for updates	✓	✓	✓	✓
RE (1) Update authenticity and integrity		✓	✓	✓
NDR 3.10 - Support for updates	✓	✓	✓	✓
RE (1) Update authenticity and integrity		✓	✓	✓
EDR 3.11 - Physical tamper resistance and detection		✓	✓	✓
RE (1) Notification of tampering attempt			✓	✓
HDR 3.11 - Physical tamper resistance and detection		✓	✓	✓
RE (1) Notification of tampering attempt			✓	✓
NDR 3.11 - Physical tamper resistance and detection		✓	✓	✓
RE (1) Notification of tampering attempt			✓	✓
EDR 3.12 - Provisioning product supplier roots of trust		✓	✓	✓
HDR 3.12 - Provisioning product supplier roots of trust		✓	✓	✓
NDR 3.12 - Provisioning product supplier roots of trust		✓	✓	✓
EDR 3.13 - Provisioning asset owner roots of trust		✓	✓	✓
HDR 3.13 - Provisioning asset owner roots of trust		✓	✓	✓
NDR 3.13 - Provisioning asset owner roots of trust		✓	✓	✓
EDR 3.14 - Integrity of the boot process	✓	✓	✓	✓
RE (1) Authenticity of the boot process		✓	✓	✓
HDR 3.14 - Integrity of the boot process	✓	✓	✓	✓
RE (1) Authenticity of the boot process		✓	✓	✓
NDR 3.14 - Integrity of the boot process	✓	✓	✓	✓
RE (1) Authenticity of the boot process		✓	✓	✓

SRs and REs	SL 1	SL 2	SL 3	SL 4
FR 4 - Data confidentiality (DC)				
CR 4.1 - Information confidentiality	✓	✓	✓	✓
CR 4.2 - Information persistence		✓	✓	✓
RE (1) Erase of shared memory resources			✓	✓
RE (2) Erase verification			✓	✓
CR 4.3 - Use of cryptography	✓	✓	✓	✓
FR 5 - Restricted data flow (RDF)				
CR 5.1 - Network segmentation	✓	✓	✓	✓
NDR 5.2 - Zone boundary protection	✓	✓	✓	✓
RE (1) Deny all, permit by exception		✓	✓	✓
RE (2) Island mode			✓	✓
RE (3) Fail close			✓	✓
NDR 5.3 - General purpose, person-to-person communication restrictions	✓	✓	✓	✓
FR 6 - Timely response to events (TRE)				
CR 6.1 - Audti log accessibility	✓	✓	✓	✓
RE (1) Programmatic access to audit logs			✓	✓
CR 6.2 - Continious monitoring		✓	✓	✓
FR 7 - Resource availability (RA)				
CR 7.1 - Denial of service protection	✓	✓	✓	✓
RE (1) Manage communication load from component		✓	✓	✓
CR 7.2 - Resource management	✓	✓	✓	✓
CR 7.3 - Control system backup	✓	✓	✓	✓
RE (1) Backup integrity verification		✓	✓	✓
CR 7.4 - Control system recovery and reconstitution	✓	✓	✓	✓
CR 7.5 - Emergency Power				
CR 7.6 - Network and security configuration settings	✓	✓	✓	✓
RE (1) Machine-readable reporting of current security settings			✓	✓
CR 7.7 - Least functionality	✓	✓	✓	✓
CR 7.8 - Control system component inventory		✓	✓	✓

CONCLUSION



To conclude, there are many reasons and pain points why critical infrastructure organizations must start looking at OT Cyber Security closely and conduct an audit based ISA/IEC 62443.

Some pain points to consider are:

1. Lack of OT Security Strategies, roadmap, and policies
2. Lack of OT Visibility/ OT Monitoring
3. Challenges to perform OT-IT Integration (keeping security in mind)
4. Challenges to perform ICS Pen Testing (It is challenging to test production environments)
5. Limited OT Security Awareness
6. Lack of Risk Mitigation Strategies & Remediation, Limited Patching
7. Sensitive Data may not be secure
8. Challenges to provide Secure Remote Access to OT Environment
9. Lack of OT Security Incident Response Plan
10. OT Security Incident Impact can be catastrophic
11. Challenges to keeping up to date on OT Security in an ever-changing connected world or with emerging technologies or IIoT.
12. Lack of Security Expertise in OT Environments

By combining Maturity Assessments, Risk Assessments, and detailed Technical Assessments, a holistic point of view can be provided to ICS Assessments. This taxonomy can assist OT security experts in Assessing, designing, and implementing OT cybersecurity architecture and solutions, as well as managing cyber risk.

OT SECURITY SERVICE OFFERINGS

HOLISTIC ICS ASSESSMENT (MATURITY REVIEW, RISK BASED MODEL & PASSIVE SCANNING)

A complete approach to addressing an organization's OT security program based on Industry best practices like NIST, ISA/IEC 62443 standard.

As part of Maturity Review, The degree to which an organization is prepared to prevent, recognize, contain, and respond to threats to its information assets will be determined. Our Cyber Maturity Assessment takes into account not just the technological readiness but also the people, processes, and technologies involved.

Risk Assessment comprises reviewing policies and procedures, Network Architecture Review, conducting a security risk assessment based on above standards and conducting passive scanning of OT Environment. A thorough Report will be generated that include real recommendations.

With Our extensive research and years of experience in OT security domain, Payatu have established an effective way to carry out holistic ICS assessments. Our comprehensive cybersecurity program not only makes the process of conducting a ICS security assessment easier, but it also offers extensive coverage across all domains.

ICS SECURITY PROGRAM DESIGN, DEVELOPMENT & IMPLEMENTATION

The development of a cyber security programme which includes program design, development and implementation of security concepts is an activity that is preceded by considerable forethought and is carried out before beginning of any other security-related duties.

When trying to deploy security measures without sufficient planning and direction, you will rapidly get the impression that you are attempting to strike a shifting target. While an organization's objectives and intended security posture should be the primary focus of its security programme, it is nevertheless necessary to comply to widely used and industry-adopted standards while carrying out security measures.

Creating a cyber security program may be a time-consuming process and owing to the extensive list of available criteria outlined in ISA/IEC 62443, NIST 800 can often be difficult to understand.

Payatu provides a streamlined version of the IEC 62443 and NIST based security program development. This framework is not only simple to design and create, but it is also simple for plant staff to accept and comply with.

SOURCING & PROCUREMENT (ICS CYBERSECURITY DURING FAT/SAT)

Factory Acceptance Testing (FAT), as well as Site Acceptance Testing (SAT) are the crucial process to helps verify that newly manufactured ICS equipment meet its intended purpose and is accepted post the implementation in a plant.

FAT entails verifying that systems conform with ICS cybersecurity standards and specifications. This comprises confirming that the appropriate security settings have been setup correctly and that relevant security components are configured correctly.

Testing "delta" adjustments in configuration and network interfaces in accordance with site requirements is a part of SAT, which also entails ensuring that all items on the punch list generated by FAT have been completed.
In some circumstances, testing may also include cybersecurity robustness testing or penetration testing, both of which are aimed to locate and determine the areas of a system that are susceptible to flaws or vulnerabilities.

Our OT security consultant team is able to help reduce the amount of effort required for sourcing and procurement by identifying OT cyber security requirements necessary for a site/plant to achieve their security goals.

SOLUTION IMPLEMENTATION

It can be difficult for an organization to implement complex cybersecurity solutions. Our teams for implementation, assessment and penetration team collaborate in order to produce a solution implementation that is flexible and simply adoptable by any plant staff.

The following is a list of our offerings for solution implementation:

1. SIEM (Security Information and Event Management) Implementation for OT: Design, Development, and Implementation of Centralized Tools for OT Visibility
2. Implementing OT Asset Inventory and Asset Management solutions
3. Firewalls in industrial environments
4. Establishing the setup of unidirectional gateways

TECHNICAL TESTING

ICS Product level Assessments (Hardware to Cloud)

Industrial control system owners and operators may conduct an ICS product level assessment to find out whether their system is vulnerable to a cyber-attack or not. The assessment identifies and seeks to mitigate vulnerabilities that would allow an attacker to disrupt or take control of an ICS product which are connected to other loosely connected networks.

Payatu's expertise in ICS product testing can help you to achieve the same. Our layered security review enables you to mitigate this by building scalable and secure applications & identifying potential vulnerabilities in ICS products.

OTHER SERVICES

Other than offering Consulting, Assessment, and Implementation Payatu also offers Learning and training services. Our Portfolio for offering training services includes the following:

1. ICS Lab Development
2. ICS Training

PAYATU ALSO OFFERS SERVICES LIKE

- Web Security Testing
- Product Security
- Mobile Security Testing
- Cloud Security Assessment
- Code Review
- Red Team Assessment
- IoT Security Testing
- AI/ML Security Audit
- DevSecOps Consulting
- Critical Infrastructure
- Trainings

Payatu Security Consulting Pvt. Ltd.

www.payatu.com

info@payatu.com

+91 20 41207726