Securing industrial networks: What is ISA/IEC 62443?

Antoine Amirault (amrt@cisco.com)

Itamar Ferreira dos Santos (itamarf@cisco.com)

Cisco IoT Security Research Lab

cisco.com/go/iotsecuritylab

© 2021 Cisco and/or its affiliates. All rights reserved.

Introduction

For a long time, cyber attacks were not considered a real risk in the industrial world. Only the protection of processes and facilities was supported by security, introduced by IEC 61508. In addition, the many manufacturers of industrial products that primarily use proprietary protocols and processes have introduced their own vision of protection into embedded systems, making automation more difficult to understand.

In order to improve interconnection and compatibility between industrial systems, manufacturers are increasingly using standard communication protocols and complying with the requirements of international standards agencies. This is the role of the International Society of Automation (ISA), the International Organization for Standardization (ISO), and the International Electrotechnical Commission (IEC).

There are significant differences between the worlds of OT and IT, which means having security standards tailored to this area, as IT solutions do not address the diversity and specificity of the problems encountered in the industrial world.

Establishing a cybersecurity management system (CSMS) requires a holistic approach (workforce, organizational, and technological) that is consistent with other aspects of security (information systems security and functional security) and is economically reasonable, sustainable over time and tailored to the specific data of a particular company or facility.

Hence the value of a single framework for introducing rationality into a subjective domain, being consistent in assessments, and dealing with problems in an economically reasonable way. Another advantage of prescriptive frameworks is the assurance of compliance with regulatory requirements based on a country or region, which are usually based on international standards. A list of normative repositories is given below:

- SI Generic Repository: ISA/IEC 27000 Series
- IACS Repository: ISA/IEC 62443 Series
- NIST Guidelines: Guide to Industrial Control Systems (ICS) Security - 800-82 (2011)
- ENISA Guides: Good Practices for Security of the Internet of Things in the context of Smart Manufacturing (2018)

It should be noted that there are also industry standards, based on their fields of activity (nuclear, energy, transport, pharmaceutical, financial, etc.).

A global series of standards

The ISA/IEC 62443 series of standards, based on ISA-99, is a collaborative effort between several regulators, the main ones being:

- IEC TC65 / WG10
- ANSI / ISA-62443
- ISO / IEC-JTC1-SC27

The motivation to pay close attention to the security of industrial automation and control systems emerged in the United States in 2001 following the events of 9/11. In fact, if terrorists learned how to operate sophisticated airplanes, it was likely that they could learn how control systems in critical infrastructures such as water supply, power stations, and transportation operate, as well as sensitive facilities such as chemicals, food processing, and pharmaceuticals.

© 2021 Cisco and/or its affiliates. All rights reserved.

As a result of these risks and the emergence of attacks on the industrial world, managers have become convinced that they need to protect their systems from cyberterrorism, industrial espionage, or just malicious intent. This prompted the need for best practices, benchmarks, tools, and assessment services for the world of process control, initially started by ISA-99.

The ISA works on the basis of rules set by the American National Standards Institute (ANSI) and these documents are voted on by the voting members who are chosen based on their application and expertise in the field. The working documents are available to "information members" who can also comment on them. After approval, the ISA forwards its documents to ANSI and IEC for review before becoming a standard. Figure 1 shows the overall organization of the documents in the standard.

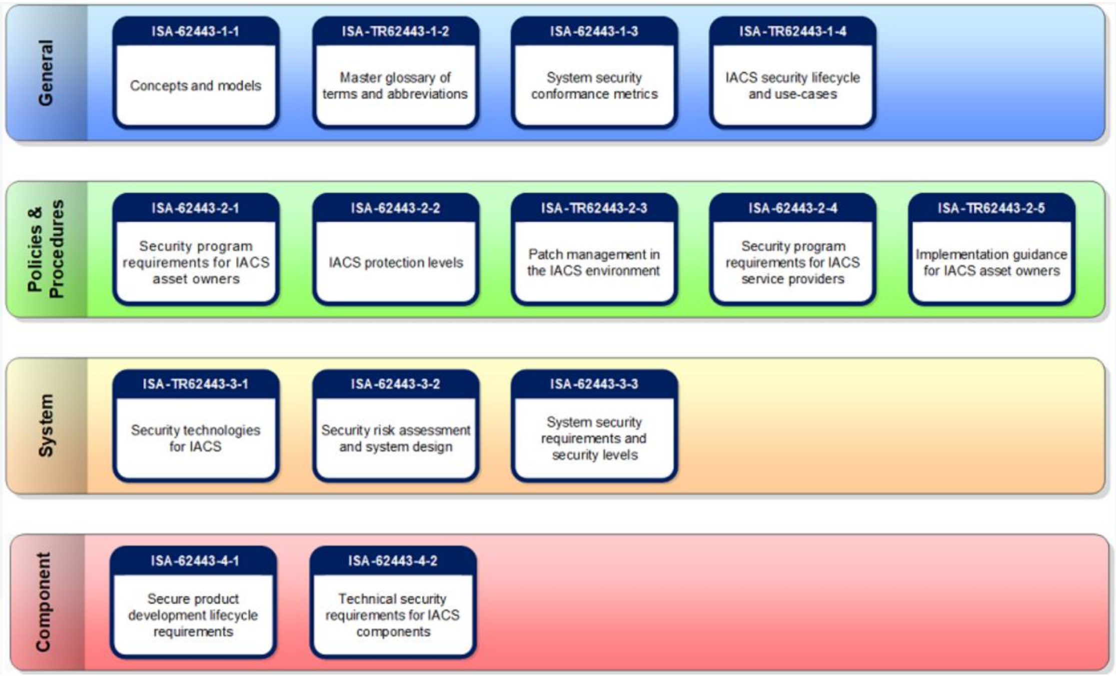

General
ISA-62443-1-1
Concepts and models
ISA-TR62443-1-2
Master glossary of terms and abbreviations
ISA-62443-1-3
System security conformance metrics
ISA-TR62443-1-4
IACS security lifecycle and use-cases
Policies & Procedures
ISA-62443-2-1
Security program requirements for IACS asset owners
ISA-62443-2-2
IACS protection levels
ISA-TR62443-2-3
Patch management in the IACS environment
ISA-62443-2-4
Security program 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

Figure 1. List of documents for ISA/IEC 62443

ISA/IEC 62443 concepts

To understand ISA/IEC 62443; it is important to introduce the three basic roles that help protect industrial facilities from cyber attacks.

- Product Supplier (PS)
- System Integrator (SI)
- Asset Owner (AO)

Each of these actors has a unique role to play in the design, development, marketing, operation, and maintenance of industrial cybersecurity solutions.

All requirements of the standard address these three groups because the equipment used is usually developed independently of a particular application. To take the example of programmable logic controllers (PLCs), these are integrated into a large number of solutions that can be very different, ranging from automation of an air conditioning system to very complex systems as found in the oil industry.

© 2021 Cisco and/or its affiliates. All rights reserved.

The security of industrial control systems is based on three main areas of the organization: people, procedures (process) and technology used. These three pillars of cybersecurity must meet the following general requirements:

- Must not affect the security functions of industrial systems,
- Apply countermeasures to achieve the required level of security, or even prevent attacks.

The standard defines the principles to be followed in the OT sector:

- **The principle of least privilege**
  The purpose of this practice is to give users only the rights they need to perform their work, to prevent unwanted access to data or programs and to block or slow an attack if an account is compromised.
- **Defense in Depth**
  This technique allows multiple layered defenses techniques to delay or prevent a cyber attack in the industrial network. The standard also requires that systems be separated into groups called “zones” that will be able to communicate with each other through communication channels called “conduits” whether they are physical, electronic, or process-based.
- **Risk analysis**
  The concept of risk analysis, based on criticality, likelihood, and impact, is not a new concept in industry. In fact, this practice is used to address risks related to production infrastructure, production capacity (production downtime), impact on people (injury, death), and the environment (pollution). However, this technique must extend to cybersecurity to address the risks inherent in industrial information systems.

The ISA/IEC 62443 reference model

Based on these three principles, ISA/IEC 62443 defines the concept of an industrial control system, introducing a five-level functional reference model, segmenting these functional levels into **zones** and **conduits**, and defining the essential requirements (Foundational Requirements - FR) for system security.

Considered to be an industrial automation and control system (IACS) is any control system and its associated means of communication (level 2 or 3 of the OSI model) as well as the interfaces useful for its implementation. Local and/or distributed industrial control systems (also known as SCADA) are typically composed of the following:

- DCS (Distributed Control System)
- PLC (Programmable Logic Controller)
- RTU (Remote Terminal Unit)
- BPCS (Basic Process Control System)
- Safety Instrumented System (SIS)
- Communication systems (L2 and L3 OSI model, such as switches, modems, routers, wireless communication devices, firewalls, etc.).

The standard also provides functional reference models (Figure 2), reference models for local systems, distributed systems (SCADA) (Figure 3), and a zone and conduit segmentation model (Figure 4).

© 2021 Cisco and/or its affiliates. All rights reserved.

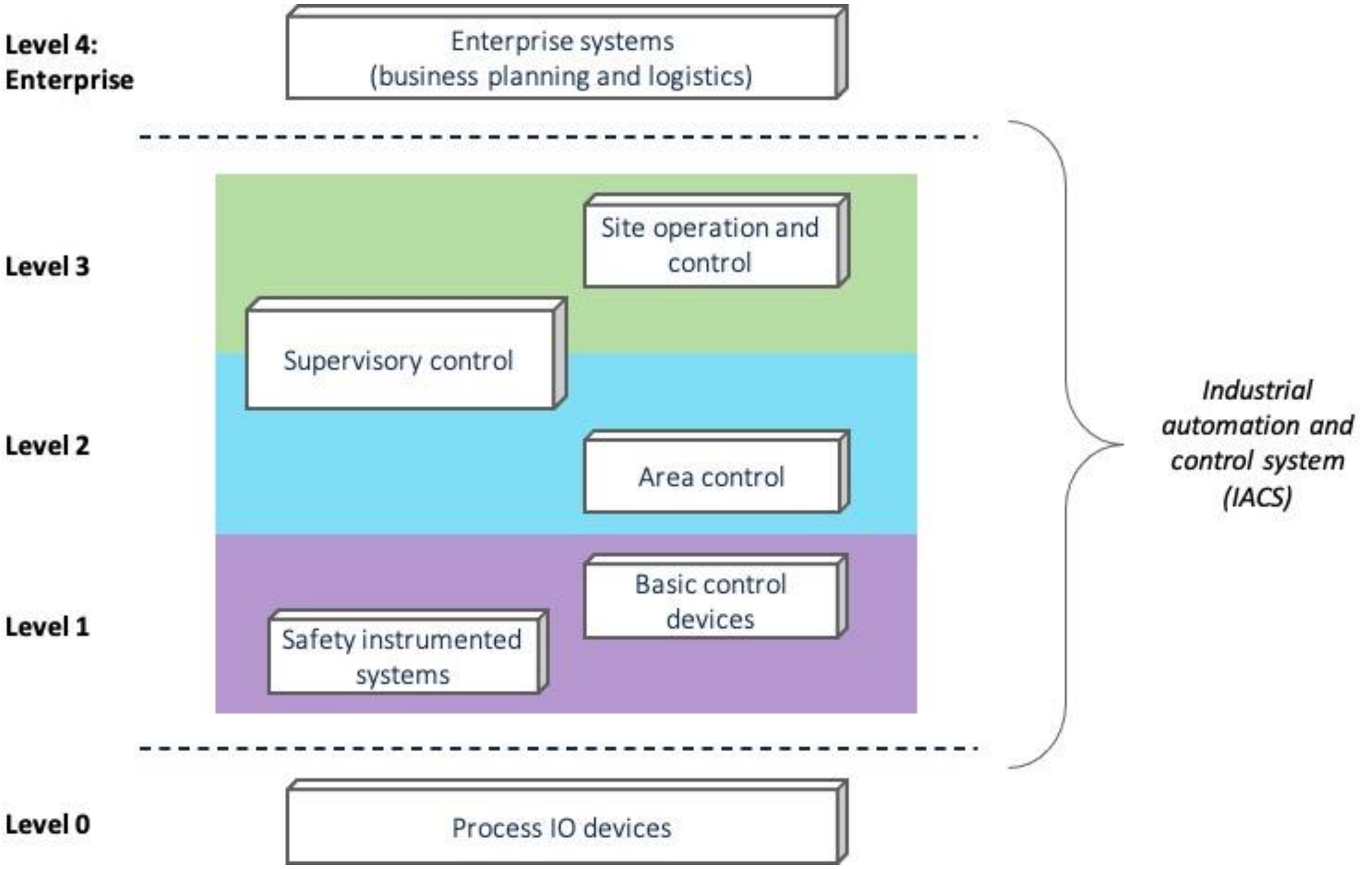


Figure 2. ISA/IEC 62443 Functional reference model

© 2021 Cisco and/or its affiliates. All rights reserved.

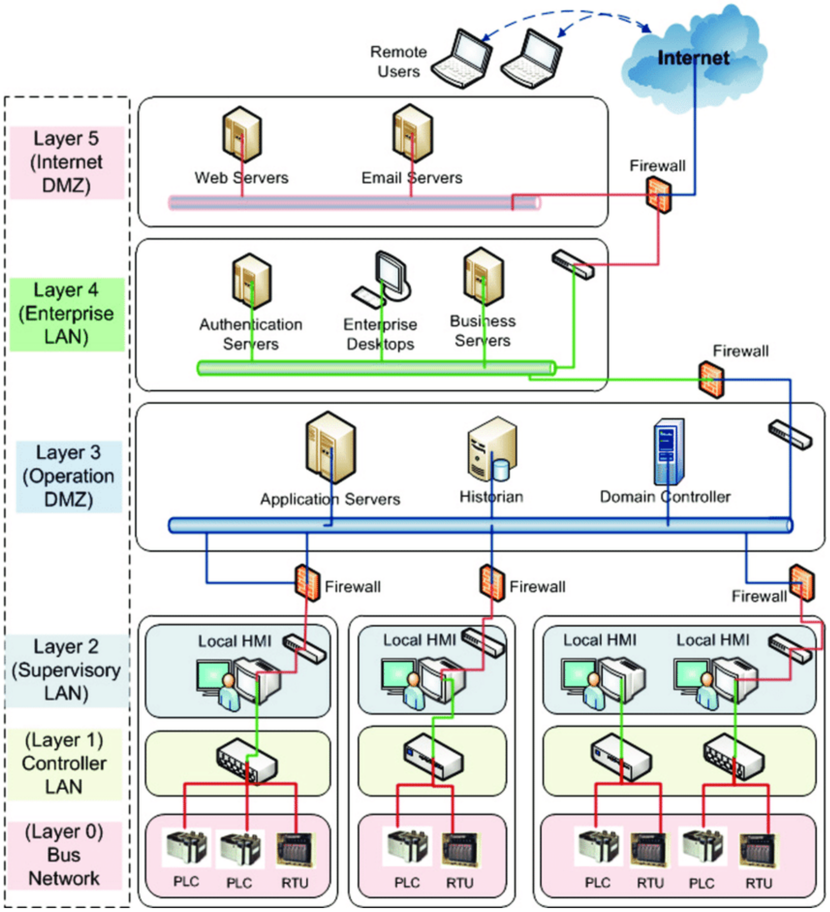


Figure 3. Physical architecture model of an industrial network

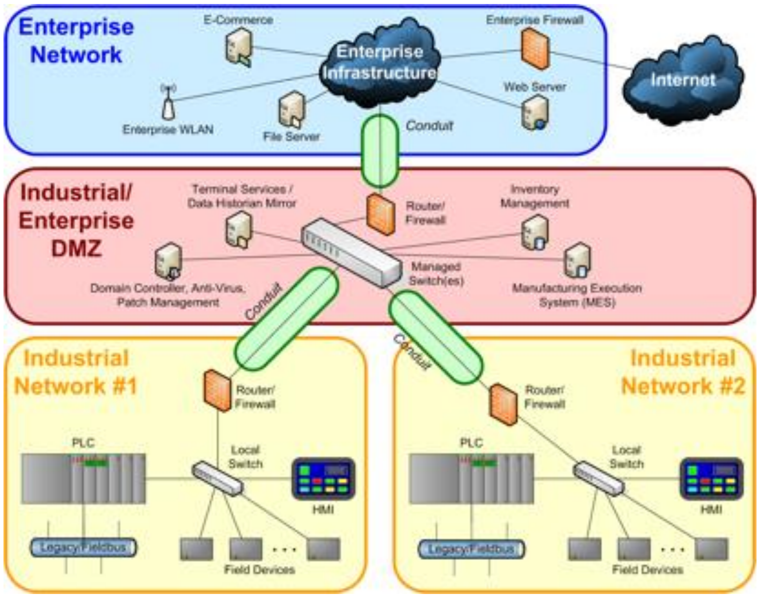


Figure 4. Industrial network model of zones and conduits

© 2021 Cisco and/or its affiliates. All rights reserved.

Security requirements

These models are proposed to improve understanding of the standard and provide concrete elements to guide automation engineers in managing their digital protection projects. It is important to remember that standards define a set of requirements at organizational (governance) and technical levels.

ISA/IEC 62443 establishes seven requirements (Foundational Requirements – FR):

- **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.

Operators must define the level at which each of these requirements must be met based on the outcome of risk analyzes. These expected levels of security will help build Security Levels (SLs).

Essential concepts

The isolated initiatives of various countries and/or organizations are consolidated today with the international standard ISA/IEC 62443, which is specifically dedicated to the security of industrial systems. Because the role of a repository is to provide the rules for setting up and managing a cybersecurity management system (CSMS), the key concepts for its implementation are:

- Key roles
- The CSMS lifecycle
- Security levels (SLs)
- Zones and conduits
- Evaluating a cybersecurity program

Key roles

The standard has defined three primary roles for IACS security:

- Product Supplier (PS),
- System Integrator (SI),
- Asset Owner.

The standard also defines the three roles into which all users of the manufacturing system are divided: management, technical group, and other users. All three groups need to be aware of cybersecurity best practices based on their roles.

© 2021 Cisco and/or its affiliates. All rights reserved.

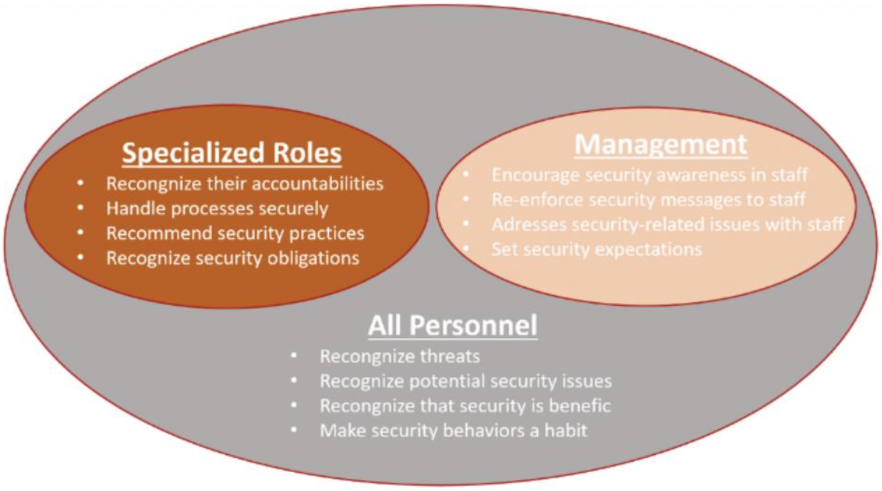

Specialized Roles
Recongnize their accountabilities
Handle processes securely
Recommend security practices
Recognize security obligations
Management
Encourage security awareness in staff
Re-enforce security messages to staff
Adresses security-related issues with staff
Set security expectations
All Personnel
Recongnize threats
Recognize potential security issues
Recongnize that security is benefic
Make security behaviors a habit

Figure 5. Distribution of user roles in an industrial computer system

The CSMS lifecycle

The definition of a Cybersecurity Management System (CSMS) should be part of an overall corporate security policy. It should be based on the most comprehensive and consistent analysis of all risks to a business. It involves raising the awareness of business leaders at the highest level and raising awareness at all levels with instructions that are as operational as possible.

Cybersecurity, like quality, is built step by step, based on risk analysis, experience, feedback, and evaluation. Effective protection against cyber attacks must become a significant part of any industrial or commercial organization's legacy, along with compliance with environmental standards, for example.

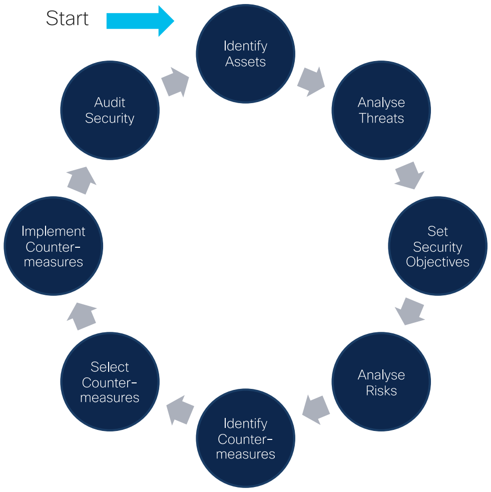
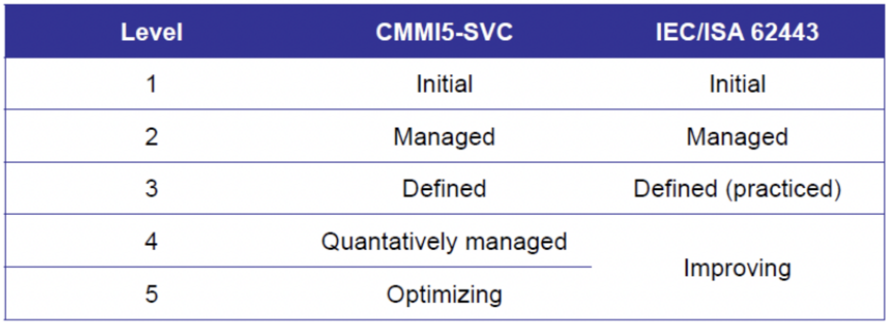


Figure 6. CSMS lifecycle

In this continuous improvement loop lifecycle approach, the repository introduces via document 62443-1-1 a maturity model, derived from the CMMI for services model (CMU/SEI-2010-TR-034, ESC-TR -2010-034). It is about characterizing an organization's level of cybersecurity control based on its practices as defined by the standard.

© 2021 Cisco and/or its affiliates. All rights reserved.



Level	CMMI5-SVC	IEC/ISA 62443
1	Initial	Initial
2	Managed	Managed
3	Defined	Defined (practiced)
4	Quantatively managed	Improving
5	Optimizing	

Figure 7. Comparing CMMI and ISA/IEC 62443 security levels

As shown in Figure 7, ISA/IEC 62443 has limited itself to four levels of maturity, encompassing levels 4 and 5 of the CMMI model into a single level 4 called “Improving”. The goal is to make it clear that cybersecurity is a complex topic that needs to be continually improved.

Security levels defined in the standard:

- **Level 1 - Initial:** The company is lagging behind in cybersecurity. Few measures are in place or if they exist, they are not documented.
- **Level 2 - Managed:** Security measures are in place, documented, but the process is not adopted by the entire ecosystem. Best practices are not yet in the DNA of users.
- **Level 3 - Defined (practiced):** Measures are in place, documented, and well integrated across the organization.
- **Level 4 - Improving:** Safeguards exist, are documented, CSMS is regularly audited. Regular system updates are performed to improve governance and technical solutions.

Security levels (SLs)

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.

Security levels are defined according to their typology:

- **Target** - This is the level of protection to be achieved for each area and path using a number of countermeasures **(SL-T)**.
- **Capability** - This is the level of protection specific to a component or system that allows the desired level of security to be expected. **(SL-C)**
- **Achieved**: This is the level actually achieved by the intrinsic properties of the components that make up a zone or conduit and the potential contribution of countermeasures. **(SL-A)**

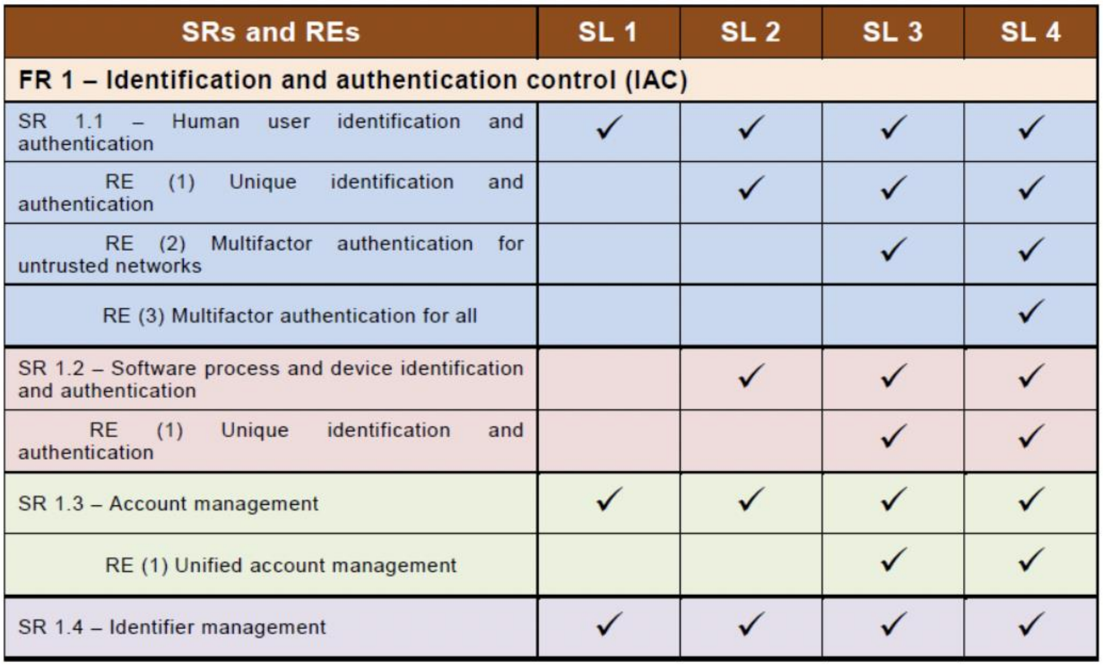
These security levels should be matched to each essential requirement (Foundational Requirements - FRs) based on the relevance to the particular industrial system.

The security levels are divided into five levels:

- **SL 0:** Protection below level 1
- **SL 1:** Protection against usual or coincidental violations
- **SL 2:** Protection against intentional violations using simple resources
- **SL 3:** Protection against intentional violations using sophisticated measures
- **SL 4:** Protection against intentional violations using extreme measures

© 2021 Cisco and/or its affiliates. All rights reserved.

The security levels to be achieved (SL-T) are defined for each essential requirement (FR) based on their criticality within the system. Figure 8 summarizes these expectations.



SRs and REs	SL 1	SL 2	SL 3	SL 4
FR 1 – Identification and authentication control (IAC)				
SR 1.1 – Human user identification and authentication	✓	✓	✓	✓
RE (1) Unique identification and authentication		✓	✓	✓
RE (2) Multifactor authentication for untrusted networks			✓	✓
RE (3) Multifactor authentication for all				✓
SR 1.2 – Software process and device identification and authentication		✓	✓	✓
RE (1) Unique identification and authentication			✓	✓
SR 1.3 – Account management	✓	✓	✓	✓
RE (1) Unified account management			✓	✓
SR 1.4 – Identifier management	✓	✓	✓	✓

Figure 8. Standard requirements based on desired security level

ISA/IEC 62443-3-3 defines the system requirements (SR) for a given system. In this example, we observe the requirements that must be in place to achieve the desired level of security based on the techniques used. To ensure compatibility of the standard, correspondence tables have been established for requirements of other standards, such as ISO 27002, NISTSP800-53r3, NERC CIP002-2.

Zones and conduits

ZONES

According to the standard, a security zone is a collection of physically and functionally united assets that have similar security requirements. These areas are defined from the physical and functional models of the industrial system control architecture.

The definition of a “zone” is based on the physical model of the industrial information system, which will be supplemented with features and activities, such as operations, maintenance, adjustments, and so on. When an asset supports multiple functions (or activities), it is assigned to a zone corresponding to the most stringent function or a separate zone is created with a specific security policy.

Security zones are characterized 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.

© 2021 Cisco and/or its affiliates. All rights reserved.

All assets in an industrial system (IACS) must be positioned in an area and all of these areas and paths must be produced in a schematic form, illustrating the system partition.

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.

These attributes should be documented:

- 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)

CONDUITS

Reference document ISA/IEC 62443-3-2 also describes that conduits are a special form of zone. They support communication between zones. This is because a conduit is a security zone that contains communication channels between two or more zones. More often than not, a conduit comprises a communication network and the components that support it (cabling, routers, switches, firewalls, etc.). Conduits can combine different communication techniques and have multiple communication channels.

Conduits are used in potential risk analyzes related to the level of communication within a zone, however, this specific type of zone cannot have subzones, or sub-conduits. The set of physical devices, and the applications that use these communication channels, are the terminal devices of the conduits.

Like a zone, each conduit has a set of characteristics and security requirements that are its attributes:

- Name and/or identifier (unique)
- The zones interconnected by the conduit
- List of access points and end devices
- Type of data (dataflows) supported
- Connected zones and conduits
- List of assets and related risks
- Applicable security requirements (general and specific)
- Target security level (SL-T)
- Applicable security policies and procedures (general and specific)
- Dependence on external factors

© 2021 Cisco and/or its affiliates. All rights reserved.

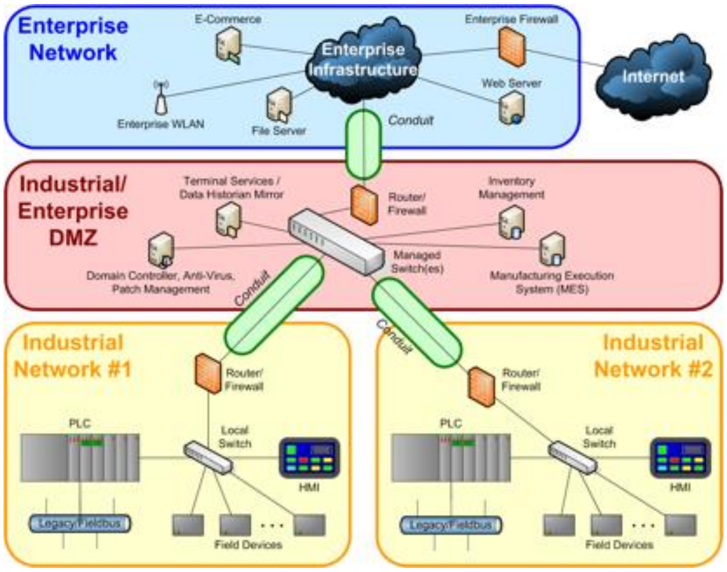


Figure 9. Model of zones and conduits

Evaluating a cybersecurity program

The standard also establishes audit rules for the evaluation of the security program for industrial systems, based on the rules defined in the company's general and specific programs. The security policy is established by the CISO (Chief Information Security Officer) and enforced at the highest level of the organization. Hierarchical involvement and user awareness are key to the success of a successful cybersecurity program.

Technically, if the requirements of the standard are not met by a component, appropriate and documented countermeasures must be taken to enable the component to be integrated into a system with a given level of security. One of the roles of the audit is to verify compliance with these requirements.

© 2021 Cisco and/or its affiliates. All rights reserved.