ISA/IEC-62443-3-3

A Cybersecurity Framework to Protect Industrial Automation and Control Systems



© 2024 Cisco and/or its affiliates. All rights reserved.

Contents

Overview 3

The ISA/IEC 62443-3-3 security principles 4

Leveraging secure components 7

ISA/IEC-62443-3-3 foundational requirements 8

Starting your ISA/IEC-62443-3 journey 22

Summary 25

Links and references 25

For more information 25

© 2024 Cisco and/or its affiliates. All rights reserved.

Overview

Protecting Industrial Automation and Control Systems (IACS) from cyberthreats is top of mind for industrial organizations. But converting good intentions to action can be a daunting task. As IACS and underlying networks are often very complex, with legacy technologies and poor security procedures, one could wonder where to start.

Fortunately, the International Society of Automation (ISA) put together the ISA99 set of standards and technical reports. The International Electrotechnical Commission (IEC) worked with the ISA to publish most of them as IEC documents and developed additional parts that are being added to the common series of ISA/IEC-62443.

The ISA/IEC-62443 Series standards and technical reports are arranged in four groups, corresponding to different focuses and audiences. Part 3-3 defines system security requirements and security capability levels to build an IACS that meets the target security level and evaluate your practice for each requirement. It gives IT and operations teams common ground to work together in building industrial infrastructures that are effectively protected against both cyberthreats and casual or coincidental events, and that drive continuous improvement.

Cisco is best known for enterprise networking and cybersecurity. Fewer people know that for more than 15 years we've also been helping industrial organizations around the globe to digitize their operations. We've worked with manufacturers, energy and water utilities, mines, ports, railways, roadways, and more. In fact, Cisco leads every segment of the industrial networking market.

With our deep understanding of Operational Technology (OT) requirements plus our leading cybersecurity portfolio, Cisco is an ideal partner to help industrial organizations secure their IACS to achieve compliance with the ISA/IEC-62443-3-3 standard. This document explains the requirements listed in the standard and illustrates how Cisco can help.

© 2024 Cisco and/or its affiliates. All rights reserved.

The ISA/IEC 62443-3-3 security principles

Part 3-3 of the standard defines essential security requirements (system requirements – SR and requirement enhancements – RE) derived from the Foundational Requirements (FR) to comply with the cybersecurity principles defined in Part 1-1, including:

Least privilege

This principle gives users only the rights they need to perform their work, in order 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 defense techniques to delay or prevent a cyberattack 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 new. It is already 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. ISA/IEC-62443-3-2 describes a security risk assessment methodology for an IACS.

Compensating security measures

In many cases, the components of an IACS do not provide the capabilities required to meet a given security level. In such scenarios, the use of compensating security measures, technical or procedural, can help to facilitate the needed capability. The combination of multiple techniques found within a security solution is designed to fulfill such a role.

Zones and conduits

Based on these principles, ISA/IEC-62443 proposes an industrial control system architecture that leverages the Purdue reference model used in ISA95 (Figure 1), segmenting these functional levels into zones and conduits (Figure 2). The segmentation is an outcome of the security risk assessment as specified in ISA/IEC-62443-3-2.

© 2024 Cisco and/or its affiliates. All rights reserved.

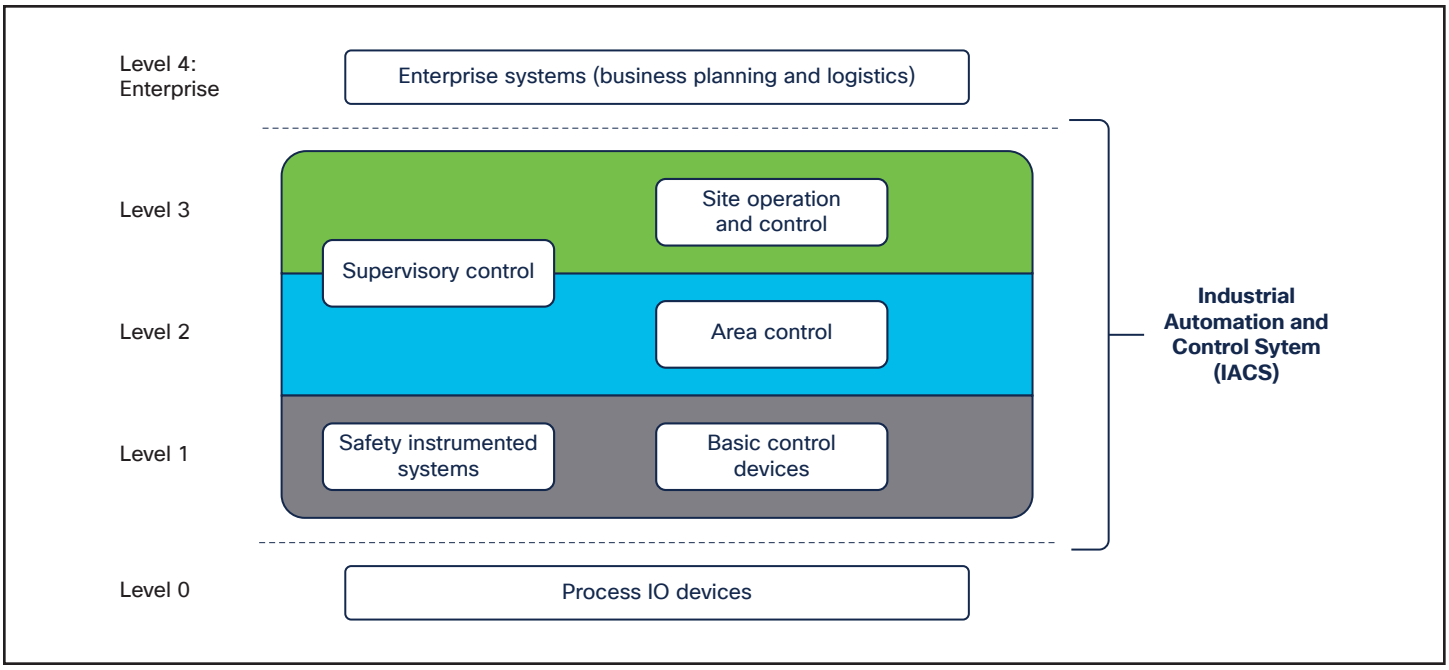


Figure 1. ISA/IEC 62443 functional reference model (source: IEC-62443-3-3 standard)

According to the standard, a **zone** is a collection of physically and/or functionally united assets that have common security requirements. These zones are defined based on the physical and functional models of the industrial system control architecture. All assets in an IACS must be positioned in a zone.

Conduits support communication between zones. A conduit is a logical grouping of communication channels between two or more zones.

© 2024 Cisco and/or its affiliates. All rights reserved.

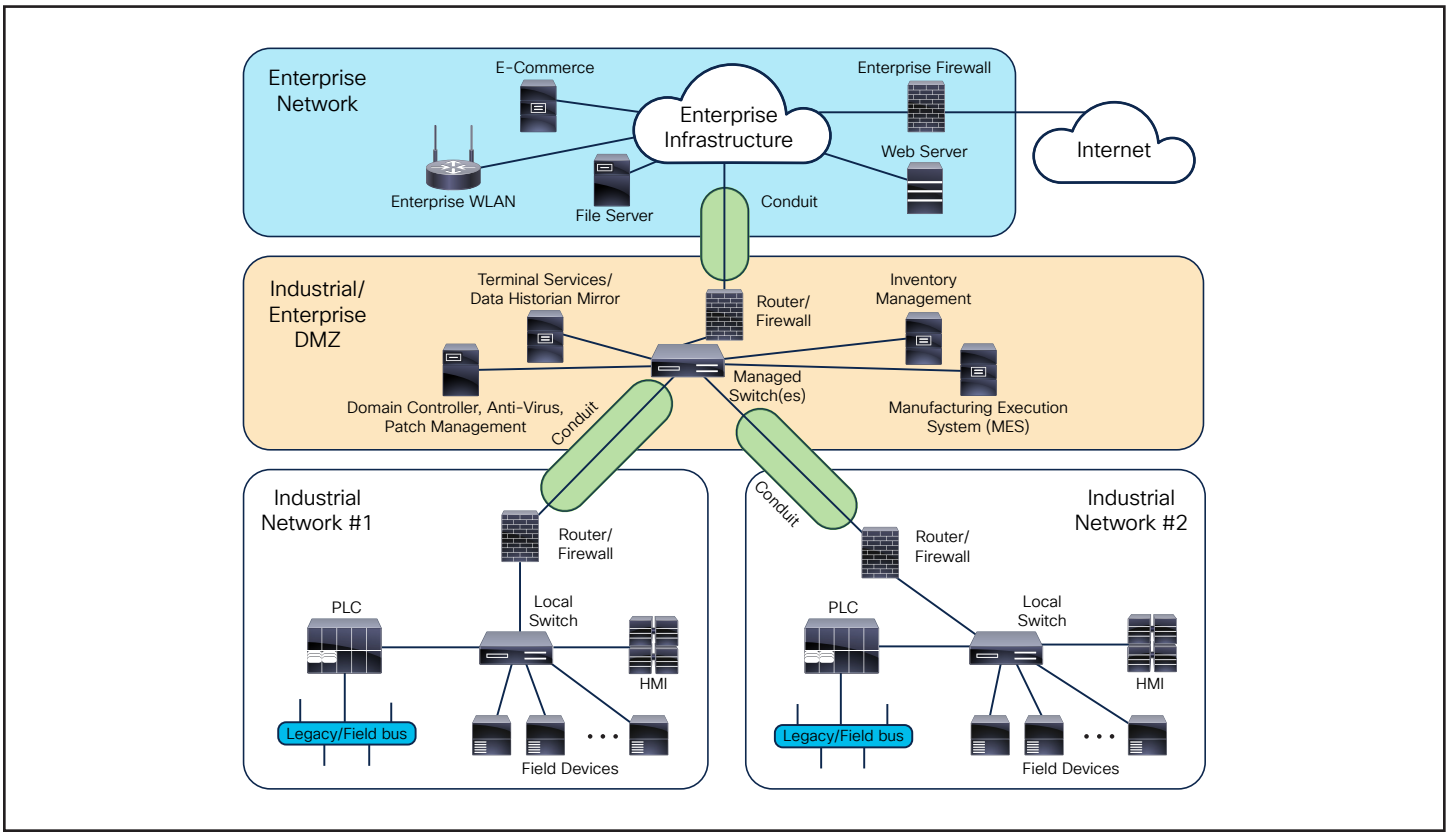


Figure 2. Example of industrial network zones and conduits (source: IEC 62443-3-3 standard)

© 2024 Cisco and/or its affiliates. All rights reserved.

Leveraging secure components

ISA/IEC-62443-3-3 focuses on the principle of a secure IACS but leverages other parts of the standard series. For instance, it assumes that a security program has been established and is being operated in accordance with IEC 62443-2-1: Security Program Requirements for IACS Asset Owners.

ISA/IEC-62443-3-3 also assumes that secure components will be deployed, or that additional measures will be put in place, to meet its requirements and address the current and future vulnerability and threat landscape. Component and development requirements are defined in Parts 4-2 and 4-1, which are essential to achieve compliance.

ISA/IEC-62443-4-1: Secure Product Development Lifecycle Requirements

This part of the ISA/IEC-62443 series comprises process requirements for the secure development of products used to assemble an IACS as well as maturity levels to set benchmarks for compliance. The content pertains to the following processes: requirement, management, design, use of coding guidelines, implementation, verification and validation, defect management, patch management, and product end of life. These requirements are essential to the security capabilities of a component and the underlying secure-by-design approach of the IACS solution. The overall focus of Part 4-1 is on continuous improvement, which is essential to address velocity in product development and release.

Cisco software and hardware products are developed according to the Cisco Secure Development Lifecycle (Cisco SDL), which enforces a secure-by-design philosophy from product planning through end of life. Cisco has obtained IEC-62443-4-1 certification for Cisco SDL that applies to the development of all Cisco industrial products.

ISA/IEC 63443-4-2: Technical Security Requirements for IACS Components

This part contains requirements for technical control system components associated with the seven Foundational Requirements (FRs). It extends the System Requirements (SRs) and Requirement Enhancements (REs) defined in ISA/IEC-62443-3-3 into a series of Component Requirements (CRs) and related REs for the components contained within an IACS. The objective is to support selection and procurement of control system components to build and integrate an IACS solution.

In this regard, the standard specifies security capabilities that enable a component to be integrated into the system environment of an IACS at a given Security Level (SL). Part 4-2 contains requirements for four types of components: software application, embedded device, host device, and network device, tailored to the specifics of these assets. In essence, a secure IACS solution needs to be built based on secure components and by applying compensating security measures if needed.

Several Cisco products have already achieved IEC-62443-4-2 certification. In combination with a 62443-certified development process (Cisco SDL), Cisco offers trustworthy communication products, which is essential for IACS deployment in critical infrastructures.

© 2024 Cisco and/or its affiliates. All rights reserved.

ISA/IEC-62443-3-3 foundational requirements

This chapter details the System Requirements (SRs) defined in IEC-62443-3-3 for each Foundational Requirement (FR) and how Cisco can help achieve compliance. The FRs themselves are defined in ISA/IEC 62443-1-1 (Terminology, Concepts, Models).

According to the scope of the standard, these requirements pertain to all components used to build and operate an IACS. Cisco can typically support an asset owner in meeting the requirements and the desired security level for network and security components.

The standard defines five different Security Levels (SLs) organizations can choose to reach for each FR, depending on their risk analysis:

- **Level 0:** No specific requirements or security protection necessary.
- **Level 1:** Protecting against casual or coincidental events.
- **Level 2:** Protecting against intentional events from malicious users using simple means, low resources, generic skills, and low motivation.
- **Level 3:** Protecting against intentional events from malicious users using sophisticated means, moderate resources, specific skills, and moderate motivation.
- **Level 4:** Protecting against intentional events from malicious users using sophisticated means, extensive resources, specific skills, and high motivation.

These security levels allow an organization to define the needed protection based on security controls for increasingly complex types of threats.

FR1: Identification, authentication control, and access control (AC)

Rationale

This part of the standard describes requirements for identifying and authenticating users (humans, software processes, and devices) before allowing them access to the industrial control system or a particular component. It acknowledges that some components might require stronger authentication mechanisms than others and recommends minimizing controls within a single zone.

How can Cisco help?

Cisco Identity Services Engine (ISE) works with network devices (both wired and wireless) to create an all-encompassing contextual identity with attributes such as user, time, location, threat, vulnerability, and access type. This identity, human or otherwise, can be used to enforce a highly secure access policy that matches the identity's business role. Administrators can apply precise controls over who, what, when, where, and how endpoints are allowed on the network. ISE integrates with multiple external identity providers such as Microsoft Active Directory.

Cisco ISE additionally offers an easy-to-deploy internal certificate authority. ISE supports both standalone deployments and ones in which the certificate authority is integrated with your existing enterprise public key infrastructure and facilitates the manual creation of bulk or single certificates and key pairs to connect devices to the network with a high degree of security.

For human users accessing Windows workstations on the plant floor or entering the network remotely, Cisco Secure Access by Duo offers Multifactor Authentication (MFA) to verify user identity before granting access. Installing Duo authentication for Windows logons adds MFA to all interactive user Windows login attempts, whether at a local console or over Remote Desktop Protocol (RDP), unless you select the "Only prompt for Duo authentication when logging in via RDP" option in the installer.

Cisco Cyber Vision primarily provides asset inventory and visibility into flow data. It can also detect the presence of credentials being sent using cleartext protocols, giving administrators a chance to remedy the situation before a man-in-the-middle attack occurs.

© 2024 Cisco and/or its affiliates. All rights reserved.

Table 1. System requirements for identification, authentication control, and access control

SR	Description	What should you look for?
1.1	Human user identification and authentication	• Cisco ISE provides contextual identity across both wired and wireless networks. • Cisco Duo provides MFA to connections as needed, such as for added protection for remote-access users.
1.2	Software process and device identification and authentication	• Cisco ISE uses MAC Authentication Bypass (MAB) to authenticate devices on the network by their MAC address. • Cisco Cyber Vision identifies IT and OT devices and their associated firmware. The device inventory built by Cyber Vision is shared with ISE, which can additionally be used for authentication.
1.3	Account management	• Cisco ISE can be used as a standalone account management tool or can be integrated with Microsoft Active Directory to manage both individual and group accounts.
1.4	Identifier management	• Cisco ISE stores the posture of every human and device in the network, which can be supplemented with Cyber Vision for additional OT-specific context on the devices.
1.5	Authenticator management	• Cisco ISE can force users to change their password after first login and subsequently change their password after a set cycle. • Cyber Vision detects passwords sent in cleartext protocols to inform administrators that passwords are subject to man-in-the-middle attacks.
1.6	Wireless access management	• Cisco ISE is consistent across both wired and wireless networks.
1.7	Strength of password-based authentication	• Cisco ISE provides configurable password strength based on minimum length and variety of character types when users log in to the network. • Cyber Vision detects default user credentials and clear (not ciphered) passwords.

© 2024 Cisco and/or its affiliates. All rights reserved.

SR	Description	What should you look for?
1.8	Public key infrastructure (PKI) certificates	• For device-to-device communication, Cisco ISE supports both standalone PKI deployments and ones in which the certificate authority is integrated with your existing enterprise PKI.
1.9	Strength of public key authentication	• Cisco ISE provides the ability to validate certificates, establish user control of the corresponding private key, and map the authenticated identity to a user.
1.10	Authenticator feedback	• Passwords are obscured when providing credentials to Cisco network equipment.
1.11	Unsuccessful login attempts	• Cisco ISE will log all network login attempts, both successful and unsuccessful. • Cisco Duo also logs all login information when using MFA to protect access. • Cyber Vision identifies login attempts when using unencrypted protocols and logs them. Multiple failures can be checked.
1.12	System use notification	• This requirement applies to IACS developers.
1.13	Access via untrusted networks	• Cisco Secure Firewall, in conjunction with the Cisco AnyConnect client, provides remote-access VPN capabilities along with policy enforcement capabilities to restrict what traffic can cross the boundary from an untrusted network. • Cisco Secure Equipment Access is a purpose-built remote access application that resides on Cisco industrial network equipment such as the Cisco Catalyst IR1101 Rugged Router to provide secure remote connectivity to individual IACS devices. • Cyber Vision captures all network communications, including remote access potentially from untrusted networks.

© 2024 Cisco and/or its affiliates. All rights reserved.

FR2: Use control (UC)

Rationale

This foundational requirement is about enforcing the proper privileges for a user (human, software process or device) once identified and authenticated to protect a component against unauthorized action (reading/writing data, downloading programs, setting configurations, etc.). It also cares about monitoring user actions and recommends adapting user privileges based on time of day, date, location, and means by which access is made.

How can Cisco help?

Cisco Identity Services Engine (ISE) is an Authentication, Authorization, and Accounting (AAA) server that is used for access control in both wired and wireless industrial networks. Authentication provides a way to identify a user, typically by having the user enter a valid username and password before access is granted. However, most devices in the network are not human and therefore do not have the capability to provide a username or password.

ISE provides the capability to do MAC Authentication Bypass (MAB), which uses the MAC address of a device to determine the level of network access to provide. Before MAB authentication, the identity of the endpoint is unknown, and all traffic is blocked. The switch examines a single packet to learn and authenticate the source MAC address. After MAB succeeds, the identity of the endpoint is known and traffic from that endpoint is allowed. The switch performs source MAC address filtering to help ensure that only the MAB-authenticated endpoint is allowed to send traffic.

Authorization is the process of enforcing policies and determining what type of activities, resources, or services a user or device is permitted to access. All controlled from a central location, Cisco ISE distributes enforcement across the entire network infrastructure. Administrators can centrally define a policy that differentiates vendors from registered users and grant access based on least privilege. ISE provides a range of access control options, such as Downloadable Access Control Lists (dACLs), VLAN assignments, and Security Group Tags (SGT) or Cisco TrustSec. These technologies are explained further in FR5, where network segmentation is addressed. Cisco Secure Firewall provides more granular policy across network boundaries for capabilities such as read/write enforcement.

Accounting measures the resources a user consumes during access, which may include the amount of system time or the amount of data that a user sent or received during a session. Accounting is carried out through the logging of session statistics and usage information, which is used for authorization control, resource utilization, and capacity planning activities.

Audit logs are supplemented by Cisco Cyber Vision, as all packets that flow through the network infrastructure undergo deep packet inspection, providing OT specific data when reviewing events in the network.

© 2024 Cisco and/or its affiliates. All rights reserved.

Table 2. System requirements for use control

SR	Description	What should you look for?
2.1	Authorization enforcement	• Cisco ISE is an AAA server that is used for access control across both wired and wireless networks. • Cisco Secure Firewall provides more granular policy across network boundaries for capabilities such as read/write enforcement.
2.2	Wireless use control	• Cisco ISE authorization enforcement is consistent regardless of access technology. • Cyber Vision can monitor wireless network activities (at the access point level).
2.3	Use control for portable and mobile devices	• Cisco ISE, Secure Firewall, and Duo can all enforce based on the posture of a device, such as type of device, whether the device is managed, or contextual information linked to a device (firmware version, for example). • Cyber Vision detects and can alert on new connected components (including portable and mobile devices).
2.4	Mobile code	• This requirement applies to IACS developers.
2.5	Session lock	• Although possible, it is not recommended to constantly ask a user or device to reauthenticate to the network, and this system requirement applies better to timing out application access, which is out of scope for Cisco. • However, Cisco Secure Equipment Access, the secure remote access tool for critical networks, can be configured to allow access only to a specified endpoint (device, application, etc.) for a specified amount of time.
2.6	Remote session termination	• Cisco Secure Firewall, the VPN concentrator for remote access into the network, can terminate active sessions to kick a user off the network. • Cisco Secure Equipment Access provides the ability to limit remote access between a specified time window and can be killed at any time.

© 2024 Cisco and/or its affiliates. All rights reserved.

SR	Description	What should you look for?
2.7	Concurrent session control	• Cisco ISE can be configured to allow only a single MAC address to be connected to any given network port on the network, disabling the ability for a rogue device to be connected to the network in place of a legitimate device. • Cyber Vision can monitor simultaneous connections (flows) to and from every device on the network.
2.8	Auditable events	• Cisco ISE, Secure Firewall, Duo, and Cyber Vision all provide event logging, auditing, and export features.
2.9	Audit storage capacity	• Logs across all Cisco products mentioned in this guide are archived within the product and can be exported using standard formats. Retention policy and storage capacity are configurable.
2.10	Response to audit processing failures	• This requirement applies to IACS developers.
2.11	Timestamps	• All Cisco logs and activities are timestamped.
2.12	Nonrepudiation	• When using Cisco ISE, accounting is carried out through the logging of session statistics and usage information, which is used for authorization control, resource utilization, and capacity planning activities. • Cisco Secure Firewall additionally has identity awareness and can include user identity when logging activity that crosses the firewall.

© 2024 Cisco and/or its affiliates. All rights reserved.

FR3: System Integrity (SI)

Rationale

The objective of this foundational requirement is to ensure the integrity of each component of the IACS by hindering unauthorized manipulations throughout the component's lifecycle, that is, during testing, operational, and nonoperational phases. Integrity of data transmission is also a key requirement to prevent manipulation of measurement values or command parameters, for instance.

How can Cisco help?

In addition to security controls, hardened and ruggedized equipment is required to address specific physical and environmental effects and to preclude impact from Electromagnetic Interference (EMI) and other harsh conditions. This includes cabling, interfaces, and the design of the communication equipment. A perfect example in this regard is the IEC-61850-3 standard for equipment installed in electrical substations. Cisco's ruggedized industrial switches used in substation automation networks are all certified against Part 3 of IEC-61850.

Furthermore, a robust, reliable, and in some cases redundant network architecture is key to ensure high availability of data and to minimize effects from environmental conditions.

To gain insight into the integrity of data transmission, Cisco recommends the use of endpoint software and an Intrusion Detection System (IDS) to prevent, detect, report, and mitigate the effects of malicious code or unauthorized software. Cisco Snort is an open-source IPS/IDS that is integrated into both Cisco Secure Firewall and Cyber Vision. Cisco Secure Endpoint is an endpoint protection tool that can detect and prevent malware on workstations, Windows-based Human-Machine Interfaces (HMIs), and tablets used within industrial networks.

Table 3. System requirements for system integrity

SR	Description	What should you look for?
3.1	Communication integrity	• Cyber Vision can check protocols used and distinguish clear and encrypted flows.
3.2	Malicious code protection	• Snort is an open-source IPS/IDS offered by Cisco. It is capable of real-time traffic analysis and packet logging on IP networks. It can perform protocol analysis and content searching and matching, and can be used to detect a variety of attacks and probes, such as buffer overflows, stealth port scans, Server Message Block (SMB) probes, OS fingerprinting attempts, and much more. • Snort IDS is integrated with Cyber Vision. • Snort IDS/IPS is integrated with Cisco Secure Firewall. • Cisco Secure Endpoint is an endpoint protection tool that can detect and prevent malware on desktop and mobile endpoints used within industrial networks.

© 2024 Cisco and/or its affiliates. All rights reserved.

SR	Description	What should you look for?
3.3	Security functionality verification	• Cyber Vision both contributes to this requirement and is able to help verify proper operation of other security features, such as firewalls, logging system, backup solutions, etc.
3.4	Software and information integrity	• Cyber Vision provides operational insights into control system activities. It detects and reports all changes that have occurred over the network. • If configured correctly, Cisco Secure Firewall and ISE will block unauthorized changes from occurring in the network. However, if used for monitoring only, both the firewall and ISE logs will add user context to any unauthorized changes to the network.
3.5	Input validation	• While Cisco provides input validation for its own tools, this requirement mainly applies to IACS developers. Cisco could leverage Snort rules to detect out-of-range values for a defined field type to perform input validation on data that crosses the network.
3.6	Deterministic output	• This requirement applies to IACS developers.
3.7	Error handling	• This requirement applies to IACS developers.
3.8	Session integrity	• This requirement applies to IACS developers.
3.9	Protection of audit information	• While Cisco can limit the modification and deletion of logs within its own tools to administrator accounts, we recommend that you back up all logs in a Security Information and Event Manager (SIEM). Additionally, Cisco Secure Endpoint could be used to add further protection to the endpoint in which the audit tool resides.

© 2024 Cisco and/or its affiliates. All rights reserved.

FR4: Data Confidentiality (DC)

Rationale

The objective of this foundational requirement is to protect data from unauthorized disclosure, either when being transmitted or while stored. Not only does this imply protecting communication channels and storage, it also requires organizations to define what data must be protected and who should have access to it.

How can Cisco help?

MACsec is the IEEE 802.1AE standard for authenticating and encrypting packets between two MACsec-capable devices. Cisco Catalyst IE3400 Rugged Series switches, for example, support 802.1AE encryption with MACsec Key Agreement (MKA) on switch-to-host links for encryption between the switch and capable host devices. The switch also supports MACsec encryption for switch-to-switch security using Cisco TrustSec Network Device Admission Control (NDAC), Security Association Protocol (SAP), and MKA-based key exchange protocol.

Protecting data while stored is out of scope for Cisco, and further considerations should be applied to do so.

Table 4. System requirements for data confidentiality

SR	Description	What should you look for?
4.1	Information confidentiality	• Cisco industrial switches, such as the Catalyst IE3400, support MACsec for hosts that can do so. • Cyber Vision lets users know whether information is communicated as cleartext (or binary) or as ciphered information. • Cisco Secure Firewall and Cisco industrial routers additionally support the transmission of data over an encrypted link.
4.2	Information persistence	• This requirement applies to IACS developers.
4.3	Use of cryptography	• Cisco industrial switches such as the Catalyst IE3400 support 802.1AE encryption with MKA on switch-to-host links for encryption between the switch and capable host devices. The switch also supports MACsec encryption for switch-to-switch security using Cisco TrustSec NDAC, SAP, and MKA-based key exchange protocol.

© 2024 Cisco and/or its affiliates. All rights reserved.

FR5: Restricted Data Flow (RDF)

Rationale

The objective of this foundational requirement is to restrict seamless communications between components to enforce the least privilege principle that the standard recommends. Restricting communications is achieved by segmenting the IACS network to support the zones and conduits defined by each organization based on its risk assessment and the security level it wants to reach. Network segmentation is acknowledged as an efficient way to reduce the exposure of the control system to cyberthreats and limit the spread of attacks. It is also leveraged to respond to an incident by breaking connections between different network segments.

How can Cisco help?

The industrial demilitarized zone (IDMZ) is the buffer between critical environments or production floor systems and the enterprise network. All shared services between the industrial zone and the enterprise zone will be located at the IDMZ. Cisco provides boundary or “edge” security appliances such as the Cisco Secure Firewall that can inspect traffic as it enters and exits each security zone, as well as replication services such as the Cisco Telemetry Broker to bridge the gap between the critical network and the noncritical network while maintaining a segmented network.

Within the plant itself, and to support the zones and conduits model proposed by IEC 62443, Cisco ISE uses TrustSec technology to logically segment control system networks. Cisco TrustSec classification and policy enforcement functions are embedded in Cisco switching, routing, wireless LAN, and firewall products. At the point of network access, a Cisco TrustSec policy group called a Security Group Tag (SGT) is assigned to an endpoint, typically based on that endpoint’s user, device, and location attributes. The SGT denotes the endpoint’s access entitlements, and all traffic from the endpoint will carry the SGT information. The SGT is used by switches, routers, and firewalls to make forwarding decisions. Because SGT assignments can denote business roles and functions, Cisco TrustSec controls can be defined in terms of business needs and not underlying networking detail.

Cisco Cyber Vision helps define these business roles. Cyber Vision leverages a unique combination of passive and active discovery to identify all your assets with no risk to devices and processes. As discovery is performed by your industrial network elements, inquiries are not blocked by firewalls or Network Address Translation (NAT) boundaries, resulting in 100% visibility. Cyber Vision shows assets and their communications in maps that operations teams can easily relate to their industrial processes. This gives them the opportunity to group assets into zones (production cells, for example) and define the network segmentation logic. Cyber Vision automatically shares this information with ISE to build security policies accordingly.

To meet compliance requirements, Cyber Vision maintains the history of all events and application flows, including variable accesses, so you can easily run forensic searches and build reports.

© 2024 Cisco and/or its affiliates. All rights reserved.

Table 5. System requirements for restricted data flow

SR	Description	What should you look for?
5.1	Network segmentation	• Cisco Secure Firewall is used to create segments that delineate network boundaries, such as the enterprise zone and the industrial zone. It is the primary enforcement mechanism when crossing the IDMZ. • Within the plant itself, and to support the zones and conduits model proposed by IEC 62443, Cisco ISE uses TrustSec technology to logically segment control system networks.
5.2	Zone boundary protection	• Cyber Vision provides the capability to group assets into logical zones and visualize the data that crosses the conduits. • The logical compartmentalization that is created in Cyber Vision is shared with ISE to influence enforcement policies across logical zone boundaries, as per the risk-based zones and conduits model.
5.3	General-purpose person-to-person communication restrictions	• Cisco Secure Firewall will detect and prevent the use of general-purpose person-to-person messages such as connecting to email servers from the industrial zone or connecting to social media.
5.4	Application partitioning	• This requirement applies to IACS developers.

© 2024 Cisco and/or its affiliates. All rights reserved.

FR6: Timely Response to Events (TRE)

Rationale

The objective of this foundational requirement is to ensure that IACS components are properly monitored to ensure that they remain secure. These requirements are designed so that organizations implement the tools and procedures to collect forensic evidence and respond to security violations. The five security levels set different expectations for how quickly the proper authorities get notified when an event impacts the security of the systems.

How can Cisco help?

Cisco Cyber Vision maintains the history of all events and application flows. It enables you to quickly understand your current security status, identify anomalies and vulnerabilities, and respond to threats. Cyber Vision offers various dashboards, reports, and event histories to easily spot security concerns. Additionally, Cyber Vision integrates the Snort IDS engine leveraging Cisco Talos threat intelligence to detect known and emerging threats such as malware or malicious traffic.

Cyber Vision is preintegrated with leading SIEM and Security, Orchestration, Automation, and Response (SOAR) platforms such as IBM QRadar and Splunk and can forward OT events and alerts to any other tool using syslog. To avoid event fatigue, it even lets you choose which event types should be shared.

Cisco SecureX aggregates intelligence from both Cisco security product and third-party sources to identify whether observables such as file hashes, IP addresses, domains, and email addresses are suspicious. When you start an investigation, context is automatically added from integrated Cisco security products, so you know instantly which of your systems was targeted and how. It brings that knowledge back from intel sources and security products, displaying results in seconds. Cisco SecureX also provides security operations teams the ability to act immediately by triggering custom workflows or continue their investigation with the tools provided.

Table 6. System requirements for timely response to events

SR	Description	What should you look for?
6.1	Audit log accessibility	• Cyber Vision provides role-based access for read-only access to audit logs. • Cisco Secure Firewall, Cyber Vision, and Duo allow administrators to export logs for sharing with users who do not require access to the tools.
6.2	Continuous monitoring	• Cisco Cyber Vision continuously monitors the OT network activity to identify new and modified assets, communication patterns, and abnormal events, as well as performs IDS monitoring in supported hardware. • Cisco Secure Firewall provides additional security monitoring when deployed at selected perimeter locations. • Cisco Secure Endpoint continuously monitors all endpoints in which it has been deployed and reacts to suspicious activity.

© 2024 Cisco and/or its affiliates. All rights reserved.

FR7: Resource Availability (RA)

Rationale

The objective of this foundational requirement is to ensure that IACS components will still provide essential functions to ensure continued safe operations when running in a degraded environment, such as when a Denial-of-Service (DoS) attack occurs. This means being able to prioritize network traffic, detect deviations from baselines, recover systems from backups, and more. For all this to become feasible, organizations must maintain a detailed inventory of all their IACS components.

How can Cisco help?

The entire objective of Cisco's industrial security architecture is to help ensure the integrity and availability of IACS resources. This is achieved through various techniques as described in the table below.

In addition, Cisco network infrastructure provides the ability to configure Quality of Service (QoS) to protect against DoS attacks. Users can select specific network traffic and prioritize it according to its relative importance. Implementing QoS in the network makes network performance more predictable and bandwidth utilization more effective. If a network segment is compromised, QoS will help ensure that the resource utilization of other network segments on the same physical infrastructure is unaffected.

Table 7. System requirements for resource availability

SR	Description	What should you look for?
7.1	DoS protection	• While Cisco does offer DoS protection, this requirement, which is to run in a degraded mode during a DoS attack, applies to IACS developers.
7.2	Zone boundary protection	• Cisco recommend the use of QoS policies in the network infrastructure to ensure that critical systems always take precedence in the network and are not affected by DoS attacks targeting network infrastructure.
7.3	Control system backup	• Cisco provides the ability to back up network configurations when using a centralized management tool such as Cisco DNA Center.
7.4	Control system recovery and reconstitution	• Cyber Vision can be used to detect what system has been compromised to reduce the time needed to reconstruct the IACS network. • Cyber Vision helps to prove that the system was able to reach a known secure state after recovery.

© 2024 Cisco and/or its affiliates. All rights reserved.

SR	Description	What should you look for?
7.5	Emergency power	• The Cisco Industrial Ethernet (IE) switches provide the ability to switch to and from an emergency power supply to help ensure that the network stays operational during a primary power failure.
7.6	Network and security configuration settings	• Network configuration can be checked live on the control system by Cisco DNA Center and compared against recommended network and security configurations.
7.7	Least functionality	• Cisco Secure Firewall can be used to prohibit the use of unnecessary functions, ports, protocols, and/or services across network boundaries. • Cisco ISE can be used to prohibit the same services laterally as it crosses the network infrastructure using ACLs and/or SGTs. • Cyber Vision helps to detect prohibited or unexpected network communications (flows, ports, shadow communications, network pollution, etc.).
7.8	Control system component inventory	• Cyber Vision passively detects installed components and their properties whenever they communicate on the network. • Cyber Vision has the ability to actively query components on the network using the semantic of the protocols at play to collect additional details on their characteristics and configurations.

© 2024 Cisco and/or its affiliates. All rights reserved.

Starting your ISA/IEC-62443-3 journey

For over 15 years, Cisco has been helping industrial organizations around the globe digitize their operations by developing a market-leading networking portfolio that is purpose-built for industrial use cases. Our deep understanding of OT requirements plus a comprehensive cybersecurity portfolio is a rare combination.

Cisco believes that a solid and flexible network architecture is a key success criterion for robust security. Poor network design can create a huge vulnerability and hinders the concepts of segmentation and extensibility, as well as the integration of cybersecurity controls and physical security measures.

However, our experience shows that building a secure industrial network will not happen overnight. To help ensure success, Cisco promotes a phased approach in which each phase builds the foundation for the next so that you can enhance your security posture at your own pace and demonstrate value to all stakeholders as you embark on this journey.

Building on the ISA/IEC-62443-3 zones and conduits concept, Cisco has developed a reference architecture that describes the various steps organizations should follow to secure their industrial control systems while building compliance with the standard. The Cisco Industrial Security Validated Design (CVD) meets the needs of operations as defined by ISA/IEC-62443-3 and also leverages the NIST cybersecurity framework that IT and security teams are more familiar with.

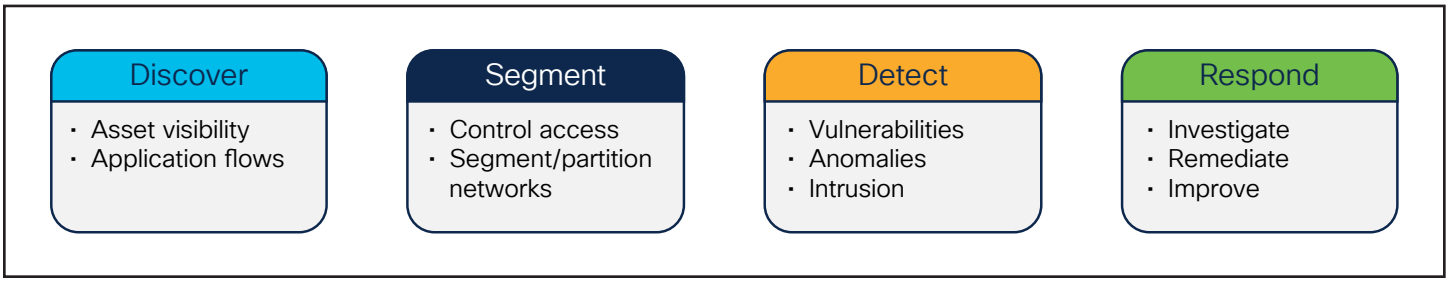


Figure 3. The pillars of the NIST cybersecurity framework

© 2024 Cisco and/or its affiliates. All rights reserved.

Discover

Visibility into all industrial assets and their application flows is provided by Cisco Cyber Vision. It creates dynamic inventories with detailed information on all connected devices, tracks communication activities to monitor zones and conduits, and helps drive risk assessments by identifying the IACS exposure to cyberthreats. Cyber Vision sensors are embedded into the cell/area network equipment to provide visibility at scale.

Segment

The industrial network is segmented from the enterprise network by an Industrial Demilitarized Zone (IDMZ) implemented by Cisco Secure Firewalls. It can also be used to segment the various parts of the industrial network so that each segment forms a semiautonomous zone to limit and contain security incidents within a zone.

For more granular segmentation and dynamic access control, Cisco Identity Services Engine (ISE) automatically enforces security policies at the device level. It leverages zones configured by control engineers in Cyber Vision to instruct the network to restrict communication flows accordingly.

Cisco ISE can also restrict activities from remote users gaining VPN access to the industrial network using Cisco Secure Client (which includes AnyConnect). Cisco Secure Equipment Access is another remote-access solution that grants access only to individual devices. Both solutions can leverage MFA using Cisco Duo.

Detect

Cisco Cyber Vision alerts you to hardware and software vulnerabilities that need to be patched for each OT device and also integrates a Snort IDS engine to detect intrusions and malicious traffic. This comprehensive visibility into OT network activities lets you build baselines to detect any deviations from normal behaviors.

Cisco Secure Network Analytics (formerly Cisco Stealthwatch) also helps detect anomalies by collecting telemetry from network devices and monitoring network flows.

Cisco Secure Firewall integrates Cisco Secure IPS, Secure Firewall Malware Defense, advanced distributed DoS (DDoS) mitigation, and URL filtering to offer comprehensive intrusion detection and protection. It can also leverage Talos signature files to block vulnerability exploits.

Cisco Secure Endpoint offers advanced malware protection for your various endpoints (workstations, servers, laptops, tablets, etc.) and can identify which processes on the protected endpoint are talking on the network.

Respond

Cisco SecureX accelerates investigations by aggregating threat intelligence and data from multiple security technologies—Cisco and otherwise—into one unified view. It streamlines remediations by offering comprehensive case management and enabling custom playbooks for your specific environment.

Cyber Vision and other security tools can export log events to SIEM platforms for further investigation and correlation.

The Cisco Validated Design (CVD)

Cisco's OT security reference design is a blueprint for a secured, robust, and reliable industrial network. It leverages Cisco's comprehensive networking and security technologies to provide industrial asset visibility, macro/zone segmentation, zone access control, threat detection, and response. It enables coordination with information security for consistent access policy management and aggregation of industrial security events in the Security Operations Center (SOC).

As shown in Figure 4, this design follows the Purdue/ISA95 model and provides detailed design and implementation guidelines to achieve compliance with ISA/IEC-62443-3.

© 2024 Cisco and/or its affiliates. All rights reserved.

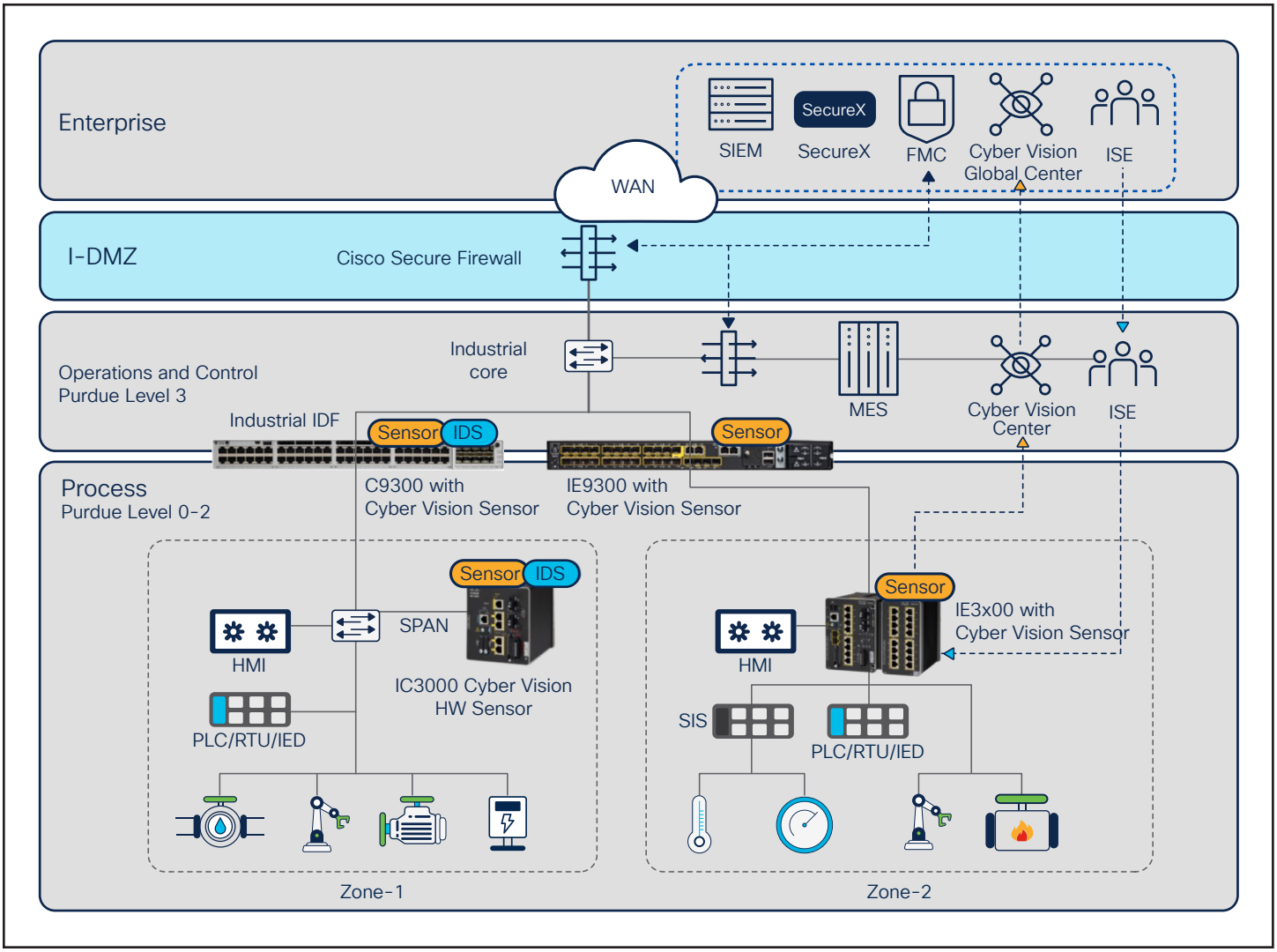


Figure 4. Cisco's industrial security architecture (source: Cisco OT Security Validated Design)

© 2024 Cisco and/or its affiliates. All rights reserved.

Summary

As with any other security measure, the protection of industrial automation and control systems is not a product, it is a continuous process. This applies to component development comprising hardware and software, operation, maintenance, and any other related activity. Cisco is addressing this essential paradigm not only in product development based on Cisco SDL but also in improving architectural and deployment references such as the Cisco Validated Designs.

Links and references

ISA99 standard committee

IEC62443-3-3 standard download

Cisco Validated Design for industrial security

Cisco Industrial Threat Defense solution for securing industrial networks

Cisco Secure Development Lifecycle (Cisco SDL)

For more information

Contact Cisco to discuss your industrial security needs

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

C11-3185108-01 08/24