FORESCOUT®

How to Effectively Implement ISA 99/IEC 62443

Table of Contents

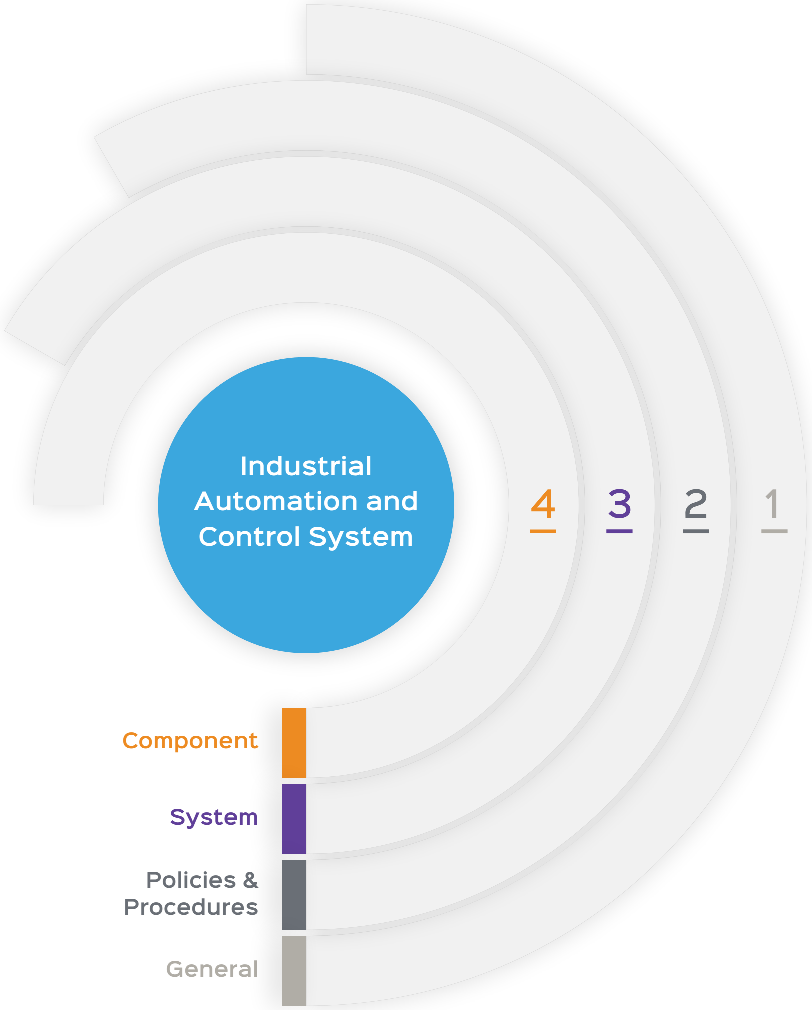
ISA 99/IEC 62443

IEC 62443, formerly known as ISA 99, is the worldwide de facto standard for security of industrial control system (ICS) networks. The standard was created by the International Society of Automation (ISA) and was taken over by the International Electrotechnical Commission (IEC), who is responsible for further developing it.

IEC 62443 assists in the evaluation of existing and potential vulnerabilities within ICS and aids in applying the necessary mitigations. The overall goal of this standard is to reduce the risk of threats and failures within ICS networks. The standard consists of 13 documents organized into four groups: General, Policies & Procedures, System and Component.

The following pages list some of the key technical requirements of IEC 62443 and explain how eyeInspect (formerly SilentDefense) helps ICS network operators to comply with them.

Industrial Automation and Control System



GENERAL

- 1-1 Terminology, concepts and models
- 1-2 Master glossary of terms and abbreviations
- 1-3 System security compliance metrics
- 1-4 IACS security lifecycle and use-case

POLICIES & PROCEDURES

- 2-1 Requirements for an IACS security management system
- 2-2 Implementation guidance for an IACS security management system
- 2-3 Patch management in the IACS environment
- 2-4 Installation and maintenance requirements for IACS suppliers

SYSTEM

- 3-1 Security technologies for IACS
- 3-2 Security levels for zones and conduits
- 3-3 System security requirements and security levels

COMPONENT

- 4-1 Product development requirements
- 4-2 Technical security requirements for IACS components

IEC 62443-3-3 and IEC 62443-4-2

IEC 62443-3-3 describes general system security requirements such as authentication, data confidentiality and system integrity.

IEC 62443-4-2 specifies the technical requirements for securing the individual components of an ICS network.

GENERAL	1-1	Terminology, concepts and models
	1-2	Master glossary of terms and abbreviations
	1-3	System security compliance metrics
	1-4	IACS security lifecycle and use-case
POLICIES & PROCEDURES	2-1	Requirements for an IACS security management system
	2-2	Implementation guidance for an IACS security management system
	2-3	Patch management in the IACS environment
	2-4	Installation and maintenance requirements for IACS suppliers
SYSTEM	3-1	Security technologies for IACS
	3-2	Security levels for zones and conduits
	3-3	System security requirements and security levels
COMPONENT	4-1	Product development requirements
	4-2	Technical security requirements for IACS components

FR 1 - Identification and Authentication Control

IEC 62443-3-3	IEC 62443-4-2	How eyeInspect helps you comply
SR 1.1 The control system shall provide the capability to identify and authenticate all human users on all interfaces that provide human user access to the control system.	**CR 1.1** All human users need to be identified and authenticated for all access to applications and devices. This includes access through network protocols HTTP, HTTPS, FTP, SFTP, and protocols used by device configuration tools.	eyeInspect monitors remote network access and authentication attempts over several clear-text OT & IT protocols including HTTP, FTP, SMB, and Telnet. Both failed and successful authentication attempts are logged for analysis and to ensure that all critical systems are accessed using individual user credentials. Real-time alerts are raised in case authentication occurs through default or insecure credentials (e.g. admin/admin), or in case of brute-force attempts.
SR 1.7 For control systems utilizing password-based authentication, the control system shall provide the capability to enforce configurable password strength based on minimum length and variety of character types. Additionally, control systems shall prevent password reuse for a configurable number of generations and enforce minimum and maximum password lifetime restrictions.	**CR 1.7** Components that use password-based authentication shall provide the capability to enforce configurable password strength based on minimum length and variety of character types. Additionally, components shall prevent password reuse for a configurable number of generations and enforce minimum and maximum password lifetime restrictions.	eyeInspect features out-of-the-box checks and real-time alerts for the use of default or insecure credentials (e.g. admin/admin) and brute-force attempts over several clear-text OT & IT protocols, including HTTP, FTP, SMB, and Telnet. Additional checks can be defined to monitor and alert for the use of weak passwords (e.g. based on length and variety of character types), password reuse and exceeded password lifetime.

IEC 62443-3-3	IEC 62443-4-2	How eyeInspect helps you comply
SR 1.8 Where PKI is utilized, the control system shall provide the capability to operate a PKI according to commonly accepted best practices or obtain public key certificates from an existing PKI	**CR 1.9** Components that utilize public-key based authentication shall ensure certificate validity and that the strength of the cipher suite used complies with cryptographic requirements.	eyeInspect performs several checks on TLS/SSL communications and certificates to ensure the security of information exchange. These include checks on certificate dates validity, trustworthiness of certificate authorities, SSL client applications, and strength of the cipher suite. All checks can be tuned to ensure compliance of encrypted communications and certificates with recognized best practices and/or company policies.
SR 1.13 The control system shall provide the capability to monitor and control all methods of access to the control system via untrusted network.	**CR 1.13** The network devices supporting device access into a network shall provide the capability to monitor and control all methods of access to the network device via untrusted networks.	eyeInspect continuously monitors all network traffic and visualizes device access and communications in the form of an interactive network map, which the user can browse and analyze to understand device behavior and information exchange across the network. Furthermore, eyeInspect automatically generates a baseline of active network communications which is presented to the user as intuitive access rules. This combination of visualizations gives the user a quick and simple way to identify illegitimate access to devices or to the network, with additional details such as who performed the access and over which protocol. Once reviewed and approved, the automatically generated baseline can be used as network whitelist, in order to alert in real time in case of access violations and other network anomalies.

FR 2 Use Control

IEC 62443-3-3

SR 2.8 The control system shall provide the capability to generate audit records relevant to security for the following categories: access control, request errors, operating system events, control system events, backup and restore events, configuration changes, potential reconnaissance activity and audit log events.

IEC 62443-4-2

CR 2.8 Components shall provide the capability to generate audit records relevant to security for the following categories: access control, request errors, control system events, backup and restore events, configuration changes, audit log events. Individual logs shall include: timestamp, source device, category, type, event ID, and event result.

How eyeInspect helps you comply

eyeInspect continuously monitors network and device activity in real time and alerts and/or logs events of interest such as network reconnaissance activity, unauthorized access and communications, failed and successful remote login attempts, error and malfunction indicators from field devices, noteworthy control system events (e.g. maintenance operations) and ICS device configuration changes (e.g. program and firmware updates). Alerts and logs contain all details required to analyze and respond to the event, such as timestamp, source and target information, event type, potential causes, impact and recommendations. Alerts and logs can be filtered and exported for offline analysis or inclusion in audit records.

> “eyeInspect continuously monitors network and device activity in real-time”

FR 3 System Integrity

IEC 62443-3-3	IEC 62443-4-2	How eyeInspect helps you comply
SR 3.2 The control system shall provide the capability to employ protection mechanisms to prevent, detect, report and mitigate the effects of malicious code or unauthorized software transported by electronic mail, Internet access, removable media, network connections, infected laptops or other common means.	**CR 3.2** The network device shall provide for protection from malicious code. If a network device is able to utilize a compensating control, it need not directly support protection from malicious code.	eyeInspect leverages a combination of signature- and anomaly-based detection to detect and alert in real time for both known and unknown malware and exploit attempts over the network. The activity of malicious actors and code is detected at the earliest stage, i.e. during reconnaissance and spread. The alert information provided by eyeInspect contains clear information about the source, target and nature of the threat, enabling immediate response and to prevent the malware from carrying out the actual attack.
SR 3.5 The control system shall validate the syntax and content of any input which is used as an industrial process control input or input that directly impacts the action of the control system.	**CR 3.5** Components shall validate the syntax and content of any input that is used as an industrial process control input.	eyeInspect features full deep packet inspection (DPI) capability on industrial protocol communications. It verifies the validity of process control messages at two levels: first, it verifies whether the message is syntactically well-formed (i.e. whether it complies with the protocol specification); second, it applies more restrictive verification to ensure that the content is valid and expected (i.e. is "normal" for the process under consideration and/or complies with process-specific restrictions). Failure of these verification steps result in real-time alerts reporting clear information required for analysis and response.

“Users are empowered with the ability to perform effective predictive maintenance”

IEC 62443-3-3

SR 3.7 The control system shall identify and handle error conditions in a manner such that effective and timely troubleshooting and remediation can occur.

IEC 62443-4-2

CR 3.7 Components shall identify and handle error conditions in a manner such that effective and timely troubleshooting and remediation can occur.

How eyeInspect helps you comply

eyeInspect monitors and detects error conditions and malfunction indicators of ICS devices and control systems, such as the inability to process requests, the presence of corrupt configurations or unexpected restarts. eyeInspect reports this intelligence to the user in real time, and provides the ability to correlate it with other network activity that might have caused the error condition to ensure timely troubleshooting and response with minimal effort. As a result, users are empowered with the ability to perform effective predictive maintenance.

FR 4 Data Confidentiality

IEC 62443-3-3

SR 4.1 The control system shall protect the confidentiality of information at rest and in transit.

IEC 62443-4-2

CR 4.1 Components shall protect the confidentiality of information at rest and in transit.

How eyeInspect helps you comply

eyeInspect enables users to verify that sensitive information is communicated using secure encrypted protocols and cipher suites. This verification can be performed by the user in several ways:

- Leveraging eyeInspect’s interactive network map and automatically generated communications baseline, users can easily identify critical control systems and servers and see whether their communication with other critical devices is encrypted.
- Leveraging eyeInspect’s Industrial Threat Library (ITL), users receive real-time alerts if insecure protocols are used to exchange sensitive information. The alerts include information about source and destination devices, so that remediation actions can be taken (e.g. insecure versions of SSL can be disabled on the host).
- Furthermore, the ITL also alerts the user if weak cipher suites or encryption keys are being used by network devices.

“Built-in controls ensure that encrypted communications follow international standards and recognized security practices.”

IEC 62443-3-3

SR 4.3 If cryptography is required, the control system shall use cryptographic algorithms, key size and mechanisms for key establishment and management according to internationally recognize and proven security practices.

IEC 62443-4-2

CR 4.3 If cryptography is required, components shall use cryptographic security mechanisms according to internationally recognized and proven security practices.

How eyeInspect helps you comply

The use of obsolete and insecure protocol versions and weak cipher suites enables attackers to leverage known exploits to compromise the security of communications. eyeInspect features several built-in controls to ensure that encrypted communications in the monitored network follow international standards and recognized security practices and alerts the user if:

- Insecure protocols or protocol versions are being used (e.g. SSHv1, SSLv2, etc.).
- Weak cipher suites or encryption keys are used in TLS/SSL communications.
- TLS/SSL certificates issued by untrustworthy certificate authorities are being used.
- Network devices use client applications associated with known malware and exploit kits.

FR 5 Restricted Data Flow

IEC 62443-3-3	IEC 62443-4-2	How eyeInspect helps you comply
SR 5.1 The control system shall provide the capability to logically segment control system networks from non-control system networks and to logically segment critical control system networks from other control system networks.	**CR 5.1** Components shall support a segmented network to support the broader network architecture based on logical segmentation and criticality.	eyeInspect provides valuable support throughout multiple stages of the network segmentation process: • At design stage, it generates an automatic and accurate visualization of all active network IP-connected devices and traffic flows, facilitating the identification of security perimeters, access points, and groups of functionally and logically related devices. Leveraging eyeInspect’s interactive network map, users can more easily (and visually) understand the network operation and accordingly define risk-based zones and conduits. • At enforcement time, eyeInspect supports the enforcement of network segmentation into zones and conduits, helping to guarantee that no undesired communication or information flow occurs. Real-time alerts are raised in case violations are detected.
SR 5.2 The control system shall provide the capability to monitor and control communications at zone boundaries to enforce the compartmentalization defined in the risk-based zone and conduits model.	**CR 5.2** A network device at a zone boundary shall monitor and control communications at zone boundaries to enforce the compartmentalization defined in the risk-based zones and conduits model.	eyeInspect enables users to monitor communications at zone boundaries and detect violations of network compartmentalization defined by zones and conduits in multiple ways: • Visually, through its interactive network map and visual threat scenarios, users can observe communications at zone boundaries and highlight the presence of communications across undesired zones. • Through automatically generated network baselines used as a network whitelist (upon approval by the user) to ensure that only legitimate communications occur in the network and at zone boundaries, or that all communications to/from a zone occur through appropriate boundary protection devices (e.g. gateways, firewalls, etc.). Actionable, real-time alerts are raised if violations occur.

> “eyeInspect provides real-time alerts if undesired communications or protocols are observed.”

IEC 62443-3-3	IEC 62443-4-2	How eyeInspect helps you comply
SR 5.3 The control system shall provide the capability to prevent general purpose person-to-person messages from being received from users or systems external to the control system. These includes e-mails, social media, or other message systems that permit the transmission of any type of executable file.	**CR 5.3** A network device at a zone boundary shall provide the capability to prevent general purpose, person-to-person messages from being received from users or systems external to the control system. These includes e-mails, social media, or other message systems that permit the transmission of any type of executable file.	eyeInspect monitors communications within and across zone boundaries and provides real-time alerts if undesired communications or protocols are observed (e.g. e-mail protocols). Furthermore, it can track file operations and alert if specific files or extensions (e.g. executables or other critical system files) are transmitted, edited or deleted.
SR 5.4 The control system shall support partitioning of data, applications and services based on criticality to facilitate implementing a zoning model.		eyeInspect provides visibility into the services in use by each device. This visibility can be used both to support users in defining appropriate zones and conduits at design stage (e.g. based on the functionality offered by devices), and to validate services and communications at enforcement time, with additional real time alerting capability if policy violations or the use of undesired services are detected.

FR 6 Timely Response to Events

IEC 62443-3-3	IEC 62443-4-2	How eyeInspect helps you comply
SR 6.1 The control system shall provide the capability for authorized humans and/or tools to access audit logs on a read-only basis.	**CR 6.1** Components shall provide the capability for authorized humans and/or tools to access audit logs on a read-only basis.	eyeInspect monitors remote access and communications to control systems and components as well as file transfer operations, to help ensure that information and audit logs are accessed only from authorized users and workstations. Real-time alerts are raised if unauthorized access and communications are detected.
SR 6.2 The control system shall provide the capability to continuously monitor all security mechanism performance using commonly accepted security industry practices and recommendations to detect, characterize and report security breaches in a timely manner. Monitoring can be achieved through a variety of tools and techniques such as IDS, IPS, network monitoring mechanisms, etc.	**CR 6.2** Components shall provide the capability to be continuously monitored to detect, characterize and report security breaches in a timely manner. Monitoring can be achieved through a variety of tools and techniques such as IDS, IPS, network monitoring mechanisms, etc.	eyeInspect continuously monitors network traffic and alerts in real time for any threat to the network and its components. It features over 1,600 built-in ICS-specific signatures and checks and combines them with powerful anomaly detection engines to help ensure that both known and unknown threats are identified at the earliest stage. These threats include the use of insecure protocols and configurations, network reconnaissance activity, possible data breach, known and unknown malware and exploits, as well as error and malfunction indicators of ICS devices and other undesired process operations that can put operational continuity at risk. All detected threats result in real time alerts containing comprehensive details and information that can lead to effective analysis and timely response.

FR 7 Resource Availability

IEC 62443-3-3	IEC 62443-4-2	How eyeInspect helps you comply
SR 7.1 The control system shall remain operative in a degraded mode during a DoS event.	**CR 7.1** Components shall maintain essential functions in a degraded mode during a DoS attack.	eyeInspect includes built-in controls for real-time detection of several types of Denial of Service attacks. Alert information includes details on the source and target hosts as well as the DoS attack technique being used, enabling quick response before control systems' and components' essential functions are compromised. In addition, eyeInspect allows users to easily monitor traffic loads to/from control systems at any time, to prevent DoS events caused by system overload.
SR 7.7 The control system shall restrict the use of unnecessary functions, ports, protocols and/or services.	**CR 7.7** Components shall restrict the use of unnecessary functions, ports, protocols and/or services.	eyeInspect automatically fingerprints network devices, and creates an inventory of open ports, protocols and services in use for each device, to match this information with desired configurations and/or company policies. In addition, it features automatic generation of network baselines that can be used to detect and alert in real time if new or undesired communications, ports, services and protocols are used in the network.
SR 7.8 The control system shall provide the capability to report the current list of installed components and their associated properties.	**CR 7.8** Components shall provide the capability to support a control system component inventory.	eyeInspect automatically generates an inventory of all active network IP-connected devices and communications, with accurate device fingerprinting including details such as IP and MAC addresses, host names, OS version, open ports, protocols and services in use, and for ICS devices, firmware version, serial number, device modules information and known vulnerabilities. The inventory information is available to the users through eyeInspect's interactive network map, which features filtering and highlight capabilities, as well as the ability to visualize devices currently exposed to security threats. Furthermore, the complete network inventory can be exported by the user for offline analysis and archiving.

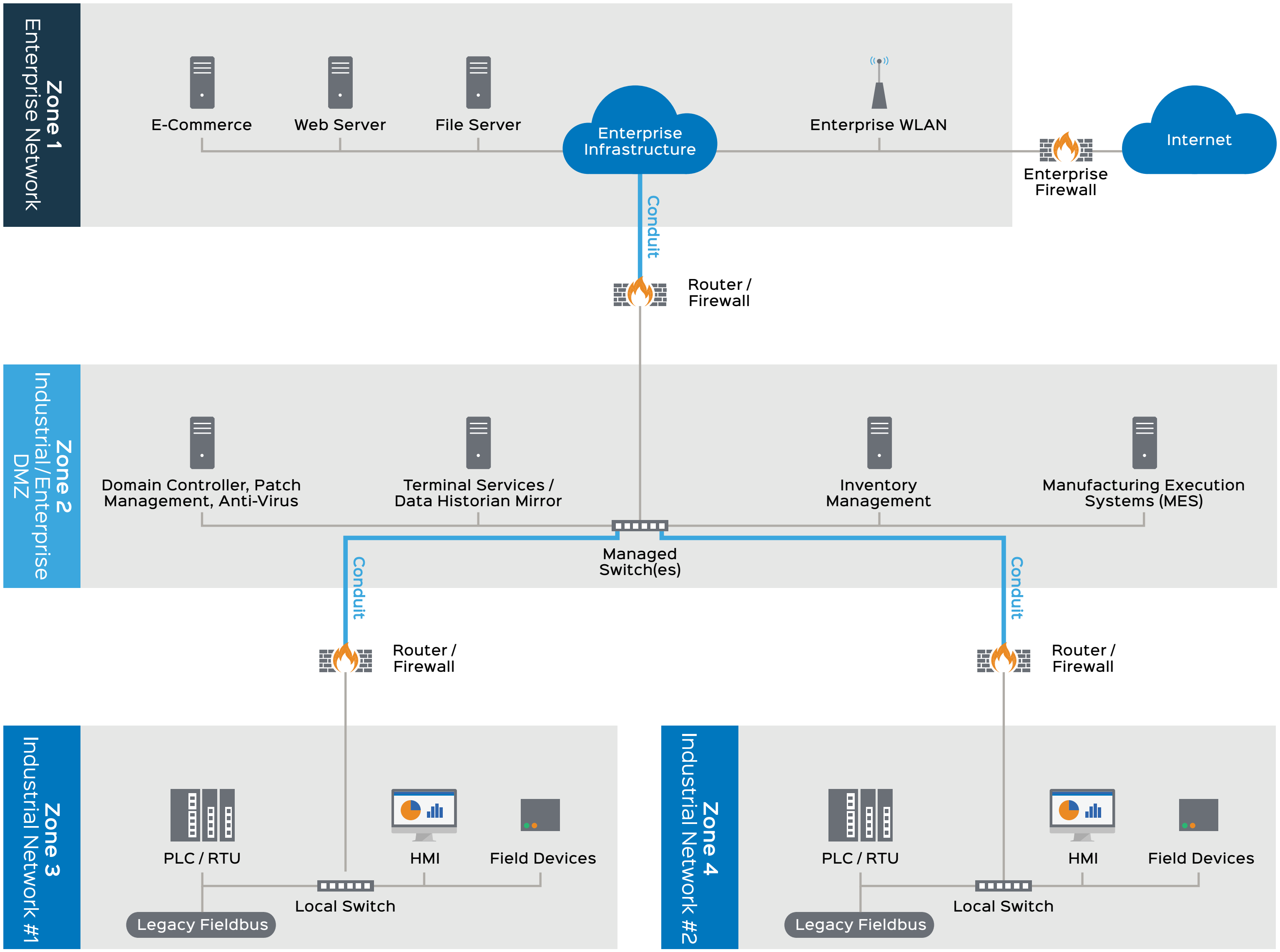
IEC 62443-3-2

Zones, Conduits and Risk Assessments

IEC 622443-3-2 addresses security risk assessment and network design. It suggests how organizations should segment their network into zones and conduits, grouping systems which are similar in functionality and restricting access to limit threat exposure and propagation.

GENERAL	1-1	Terminology, concepts and models
	1-2	Master glossary of terms and abbreviations
	1-3	System security compliance metrics
	1-4	IACS security lifecycle and use-case
POLICIES & PROCEDURES	2-1	Requirements for an IACS security management system
	2-2	Implementation guidance for an IACS security management system
	2-3	Patch management in the IACS environment
	2-4	Installation and maintenance requirements for IACS suppliers
SYSTEM	3-1	Security technologies for IACS
	3-2	Security levels for zones and conduits
	3-3	System security requirements and security levels
COMPONENT	4-1	Product development requirements
	4-2	Technical security requirements for IACS components

Manufacturing Network Example Showing Zones and Conduits



ZCR 1 Identification of the system under consideration (SuC)

IEC 62443-3-2

ZCR 1.1 The organization shall clearly identify the System under Consideration (SuC), including clear definition of the security perimeter and identification of all access points to the SuC.

How eyeInspect helps you comply

eyeInspect automatically generates and visualizes an inventory of all active IP-connected network devices and communications, and presents it to the user in the form of an interactive network map and clear network baselines. This enables users to:

- At design stage, identify the current (or define the intended) security perimeter and access points (e.g. gateways, firewalls, etc.).
- At enforcement time, ensure that all communications accessing a network (the SuC) and its devices pass from the intended access points. Real-time alerts are raised if communications violate flow and perimeter restrictions.

ZCR 2 High-level cyber security risk assessment

IEC 62443-3-2

ZCR 2.1 The organization shall perform a high-level cybersecurity risk assessment of the SuC in order to identify the worst-case unmitigated cybersecurity risk that could result from the interference with, disruption of, or disablement of mission critical IACS operations.

How eyeInspect helps you comply

eyeInspect supports and facilitates risk assessments through a combination of automated asset inventory, vulnerability assessment, and a library of over 1,600 ICS-specific operational and security threats. As soon as eyeInspect is connected to a network, it starts passively creating the inventory of all IP-connected network devices, communications, and their vulnerabilities, and identifying whether the network and its IP-connected devices are subject to any of the 1,600 built-in operational and security threats. It then presents this information as an intuitive and interactive network map, where the user can visualize the major risks and threats to the network and prioritize mitigation actions.

> “A library of over 1,600 ICS-related operational and security threats”

ZCR 3 Partition the SuC into zones and conduits

IEC 62443-3-2	How eyeInspect helps you comply
ZCR 3.1 The organization shall establish zones and conduits by grouping IACS and related assets. Grouping shall be used upon the results of the high-level cybersecurity risk assessment or other criteria, such as criticality of assets, operational function, physical or logical location, required access or responsible organization.	eyeInspect's interactive network map and threat visualizations allow users to easily understand the network operation and its major risks. The network map groups devices by function and/or network, facilitating the identification of security perimeters, access points, and groups of functionally and logically related devices. Users can leverage this information to define risk-based zones and conduits to be used as a basis for network segmentation.
ZCR 3.2 IACS shall be grouped into zones that are logically or physically separated from business or enterprise system assets. **ZCR 3.3** Safety related assets shall be grouped into zones that are logically or physically separated from zones with non-safety related assets.	Users can easily investigate network devices' activity and communications on eyeInspect's interactive network map. Dedicated visual threat scenarios allow users to quickly identify open links and communications between control system and business networks, or between safety and non-safety related assets, so that mitigation actions can be taken and communications can be stopped.
ZCR 3.4 Devices that are permitted to make temporary connections to the SuC should be grouped into a separate zone or zones from assets that are intended to be permanently connected to the IACS. **ZCR 3.6** Devices that are permitted to make connections to the SuC via networks external to the SuC should be grouped into a separate zone or zones.	eyeInspect allows users to visualize communications across network zones on its interactive network map. For each communication, eyeInspect records when it was first and last seen active. Through the map filters and dedicated visual threat scenarios, users can (a) verify whether two network segments/zones have active communications, and (b) ensure that connections from certain zones to the IACS were not active at undesired times. Additionally, if connections are to be allowed only at pre-determined times, eyeInspect allows the definition of custom checks and real-time alerts for access time violations.

IEC 62443-3-2	How eyeInspect helps you comply
ZCR 3.7 The organization shall (a) produce a drawing that illustrates the zone and conduit partitioning of the entire SuC, (b) assign each asset in the SuC to a zone or a conduit.	eyeInspect's interactive network map automatically groups devices based on their function or network segment. Users can adopt or edit these groups to define desired zones and visualize active communications across zones (i.e. the conduits). The map allows users to easily spot devices which have yet to be assigned to a zone, and conduits which should or should not be present. The network map can be exported by the user as a high-resolution image for printing or inclusion in reports.
ZCR 3.8 The organization shall identify and document for each zone and conduit: name and/or unique identifier, accountable organization(s), definition of logical boundary, definition of physical boundary (if applicable), safety designation, list of all logical and physical access points, list of data flow associated with each access point, connected zones and conduits, list of assets and their classification, criticality and business value, applicable security requirements and policies, assumptions and external dependencies.	The interactive network map and asset inventory information provided by eyeInspect allows users to easily identify logical boundaries and network access points, list of data flows associated with each access point, connected zones and conduits, and to generate a list of assets and their classification, criticality and business values. All the information automatically collected by eyeInspect can be exported by the user and integrated with additional information such as accountable organization(s), safety designation, applicable security requirements and policies in order to make it available for internal or external compliance audits.

"eyeInspect's interactive network map automatically groups devices based on their function or network segment."

ZCR 5 Perform a detailed cybersecurity risk assessment

IEC 62443-3-2

DRAR 1 A list of threats that could affect the assets contained within the zone or conduit shall be developed. A threat description shall include a description of the threat source, threat vectors and potentially affected assets.

DRAR 2 The zone or conduit shall be analyzed in order to identify and document the known vulnerabilities in the assets contained within the zone or conduit including the access point.

DRAR 12 The results of the cyber risk assessment shall be documented and reported. Documentation that was instrumental in performing the cyber risk assessment (such as architecture diagrams, vulnerability assessments and source of threat information) shall be recorded and archived along with the cyber risk assessment.

How eyeInspect helps you comply

eyeInspect features a library of over 600 known ICS vulnerabilities and over 1,600 ICS-related operational and security threats. These vulnerabilities and threats are automatically matched with the asset inventory information collected by eyeInspect and the observed network communications, to determine which of them are applicable to the monitored network. Applicable threats and vulnerabilities can be visualized by the user within eyeInspect (visual threat scenarios on the network map) or exported as a list with associated severity. This list contains further details about the source, target and nature of the threat, enabling an informed analysis and mitigation.

eyeInspect allows users to visualize risks, threats and vulnerabilities on its interactive network map in order to determine which devices and networks are most at risk and prioritize mitigation actions. The network map, including threat visualizations, can be exported by the user as an image and included in reports along with the list of threats and vulnerabilities applicable to the monitored network.

ZCR 5 Document cybersecurity requirements, assumptions and constraints

IEC 62443-3-2

ZCR 5.3 Cyber security requirements specifications (CSRS) shall identify and document the physical and logical environment in which the SuC is located or planned to be located. This shall provide a clear understanding of the networks, information technology, protocols and IACS systems that may interface with the SuC.

How eyeInspect helps you comply

eyeInspect’s network map provides the user with full visibility over the monitored environment (the SuC), including details about:

- All active IP-connected network devices, their function and their properties.
- Communications and links across networks/zones.
- All protocols and services in use in each network/zone and by each device within that zone.

This information can be exported by the user as an image (the network map) and lists (of assets and protocols) for inclusion in external documentation.

ZCR 5.4 CSRS shall include a description of the threat environment that impacts the SuC. The description shall include the source(s) of threat intelligence and include both current and emerging threats.

eyeInspect’s known vulnerability and ICS threat libraries include Common Vulnerabilities and Exposures (CVEs) and threat intelligence coming from ICS-CERT, IACS vendor advisories, and Forescout’s own field knowledge and experience. These libraries are used to determine, based on the assets and communications observed in the monitored environment, which risks, threats and vulnerabilities apply to the SuC. Applicable threats and vulnerabilities can be visualized by the user within eyeInspect (visual threat scenarios on the network map) or exported for inclusion in external documentation. Each threat and vulnerability obtained from external sources contains a clear reference to the threat intelligence source or identifier.

Forescout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591

Learn more at Forescout.com