MAPPING GUIDE

ISA/IEC 62443 Standards Compliance with the Nozomi Networks Platform

1. Introduction

An increased reliance on industrial automation and the proliferation of IoT assets have made critical infrastructure more vulnerable to cybersecurity threats. As organizations search for ways to ensure the integrity and security of industrial automation and control systems (IACS), the ISA/IEC 62433 standards have risen as the industry benchmark for securing OT systems across sectors.

In this mapping guide we will discuss the ISA/IEC 62443 cybersecurity standards, including what they are and their importance for the cybersecurity of IACS. We will also discuss how Nozomi Networks can help secure and ensure that IACS are in compliance with Parts 2-1 and 3-3 of the ISA/IEC 62443 standards.

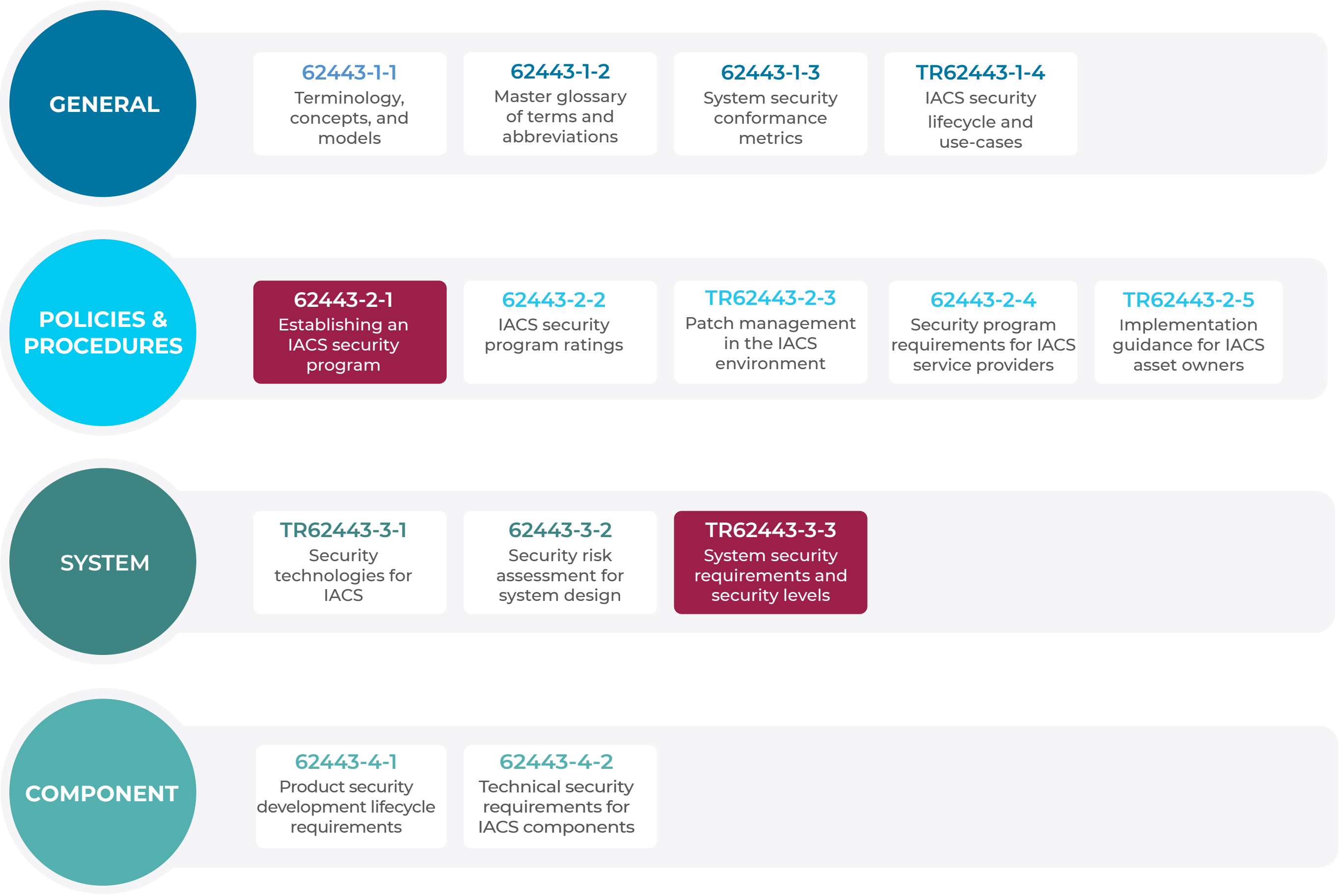
2. What Are the ISA/IEC 62433 Standards & Why Are They Important?

The ISA/IEC 62433 series of standards were developed by the ISA99 Committee and the IEC Technical Committee 65/Working Group 10 to help define best practices and processes for implementing electronically secure manufacturing and control systems within ICS environments. The focus of these standards is to improve manufacturing and control system electronic security, help identify vulnerabilities and provide guidance on how to address them.

Maintaining compliance with ISA/IEC 62433 can help reduce the likelihood of cyberattacks and help organizations avoid serious regulatory, financial and safety consequences while ensuring that operations are achieving comprehensive levels of ICS and cyber-physical security. The standard guidance is applicable for those responsible for the design, implementation and management of control systems, but can be utilized by control users, system integrators, security practitioners, and ICS manufacturers and vendors.

The ISA/IEC 62443 standards and reports are arranged in four groups, corresponding to the primary focus and intended audience. Nozomi Networks helps organizations apply Parts 2-1 and 3-3.

ISA/IEC 62443 Series of Standards



GENERAL

62443-1-1 Terminology, concepts, and models

62443-1-2 Master glossary of terms and abbreviations

62443-1-3 System security conformance metrics

TR62443-1-4 IACS security lifecycle and use-cases

POLICIES & PROCEDURES

62443-2-1 Establishing an IACS security program

62443-2-2 IACS security program ratings

TR62443-2-3 Patch management in the IACS environment

62443-2-4 Security program requirements for IACS service providers

TR62443-2-5 Implementation guidance for IACS asset owners

SYSTEM

TR62443-3-1 Security technologies for IACS

62443-3-2 Security risk assessment for system design

TR62443-3-3 System security requirements and security levels

COMPONENT

62443-4-1 Product security development lifecycle requirements

62443-4-2 Technical security requirements for IACS components

The ISA/IEC 62443 Series

3. How the Nozomi Networks Platform Supports ISA/IEC 62443 Standards

In this section, we discuss the system requirements (SR) for Parts 2-1 and 3-3 of ISA/IEC 62433 framework that the Nozomi Networks Platform supports.

ISA/IEC 62433 – Part 2-1

Security program requirements for asset owners.

4.2 Risk Assessment

Security Control	Nozomi Networks Platform Components	How Nozomi Networks Supports
SR 4.2.3.4 Identify the industrial automation and control systems The organization shall identify the various IACS, gather data about the devices to characterize the nature of the security risk, and group the devices into logical systems.	Guardian, Guardian Air, Vantage, Arc	Nozomi Networks continuously monitors OT and IoT networks to create an accurate asset inventory, providing extensive information about all communicating devices. Tracking of "normal" traffic patterns provides context for more accurate detection of anomalies and vulnerabilities.
SR 4.2.3.5 Develop simple network diagrams The organization shall identify the various IACS, gather data about the devices to characterize the nature of the security risk, and group the devices into logical systems.	Guardian, Guardian Air, Vantage	Nozomi Networks facilitates the identification of IACS assets, their function in the operational process, network zoning, placement within Purdue model levels, the asset risk level, and also allows the addition of custom fields to assign asset priorities. Furthermore, Vantage features Vulnerability Workbooks to help assess risk.
SR 4.2.3.6 Prioritize systems The organization shall develop the criteria and assign a priority rating for mitigating the risk of each logical control system.	Guardian, Vantage	Nozomi Networks provides the capability to add custom fields to assets to assign priorities, ratings, impact levels, or other criteria. Additionally, Vantage includes Vulnerability Workbooks to help prioritize vulnerability mitigations.
SR 4.2.3.7 Perform a detailed vulnerability assessment The organization shall perform a detailed vulnerability assessment of its individual logical IACS, which may be scoped based on the high-level risk assessment results and prioritization of IACS subject to these risks.	Guardian, Vantage, Arc	Nozomi Networks provides vulnerability detection and prioritization for IACS assets. Our threat intelligence provides up-to-date vulnerability data for asset software and firmware. Specific vulnerabilities can be tracked and managed as they are resolved, mitigated, or re-opened.
SR 4.2.3.9 Conduct a detailed risk assessment The organization shall perform a detailed vulnerability assessment of its individual logical IACS, which may be scoped based on the high-level risk assessment results and prioritization of IACS subject to these risks.	Guardian, Guardian Air, Vantage, Arc	Nozomi Networks offers in-depth IACS asset vulnerability data for improved risk assessments. It employs industry-standard metrics like KEVs, VWE, CPE, and CVE for detailed insights and provides both custom and preset vulnerability reports as well as Vulnerability Workbooks to streamline the prioritization of vulnerability mitigation.

Security Control	Nozomi Networks Platform Components	How Nozomi Networks Supports
SR 4.2.3.12 Conduct risk assessments throughout the lifecycle of the IACS Risk assessments shall be conducted through all stages of the technology lifecycle including development, implementation, changes, and retirement.	Guardian, Guardian Air, Vantage, Arc	Nozomi Networks supports risk assessments with asset inventory, network analysis, threat & anomaly detection, and vulnerability detection throughout commissioning and operation stages of the IACS lifecycle.
SR 4.2.3.13 Document the risk assessment The risk assessment methodology and the results of the risk assessment shall be documented.	Guardian, Guardian Air, Vantage, Arc	Reports detailing vulnerabilities, alerts, and other risk factors can be scheduled to run on a regular basis.
SR. 4.2.3.14 Maintain vulnerability assessment records Up-to-date vulnerability assessment records should be maintained for all assets comprising the IACS.	Guardian, Guardian Air, Vantage, Arc	Nozomi Networks maintains and tracks up-to-date vulnerability assessment records for all detected IACS assets.

4.3 Addressing the Risks with Cybersecurity Management Systems

Security Control	Nozomi Networks Platform Components	How Nozomi Networks Supports
SR 4.3.3.3.6 Protect connections	Guardian, Guardian Air, Vantage, Arc	Nozomi Networks detects incoming and outgoing connections with external or undefined networks for further investigation. Our platform also detects signs of weak protection of network traffic, such as presence of insecure protocols and usage of weak passwords.
SR 4.3.3.3.7 Maintain equipment assets	Guardian, Guardian Air, Vantage, Arc	Nozomi Networks helps identify assets that are in the end of sale or end of support state. Additionally, maintenance tasks such as updating, patching, pushing code downloads to IEDs, changing configurations, and asset health states can be tracked.
SR 4.3.3.4.2 Employ isolation or segmentation on high-risk IACS	Guardian, Guardian Air, Vantage, Arc	Nozomi Networks helps detect IACS asset types, zones and their communications for further analysis to determine whether they should be segmented. Segmented networks that are allowing cross-zone traffic are highlighted.
SR 4.3.3.4.3 Block non-essential communications with barrier devices	Guardian, Guardian Air, Vantage, Arc	Nozomi Networks helps detect communications between IACS assets for further inspection, and if needed further configuration of barrier devices or network segmentation.
SR 4.3.3.5.7 Change default passwords	Guardian, Vantage, Arc	Nozomi Networks detects and alerts on default and weak passwords in the network traffic.
SR 4.3.3.6.2 Authenticate all users before system use	Guardian, Vantage, Arc	Nozomi Networks generates alerts for links that have not been authenticated.

Security Control	Nozomi Networks Platform Components	How Nozomi Networks Supports
SR 4.3.3.6.3 Require strong authentication methods for system administration and application configuration	Guardian, Vantage, Arc	Nozomi Networks helps detect signs of weak authentication, such as usage of insecure protocols or weak passwords.
SR 4.3.3.6.4 Log and review all access attempts to critical systems	Guardian, Vantage, Arc	Nozomi Networks detects and alerts on suspicious login activities on the network, as well as capturing logs for further security inspection.
SR 4.3.3.6.6 Develop a policy for remote login and connections	Guardian, Vantage, Arc	Nozomi Networks detects remote (interzone) sessions on the network, as well network communications between IACS assets and untrusted networks. Additionally, remote connection protocols such as RDP, ssh and others are monitored.
SR 4.3.3.7.2 Establish appropriate logical and physical permission methods to access IACS devices	Guardian, Vantage, Arc	Nozomi Networks detects default and weak passwords on the network and provides information on network communications with Authentication, Authorization and Accounting Services to help establish appropriate logical and physical permission for accessing IACS devices.
SR 4.3.4.2.1 Managing IACS risk on an ongoing basis The organization shall adopt a risk management framework that includes selection and implementation of IACS devices and countermeasures to manage risk to an acceptable level over the life of the facility.	Guardian, Vantage, Arc	Nozomi Networks assigns a risk level to each alert and incident, along with a severity for asset vulnerabilities, aiding in the assessment of a facility's risk profile. Risk can also be tracked over time and reported on, ensuring progress is tracked towards facility objectives.
SR 4.3.4.2.2 Employ a common set of countermeasures A common defined set of countermeasures (technical and administrative) to address both physical and cyber security risks should be defined and applied across the organization wherever a specific risk is identified.	Guardian, Vantage, Arc	Nozomi Networks detects security devices on the network such as firewalls, servers, remote access devices, as well as details of assets such as installed antivirus software, hardware present, USB key status, and many other pieces of information that are needed for consistent risk mitigation.
SR 4.3.4.3.2 Develop and implement a change management system A change management system for the IACS environment shall be developed and implemented. The change management process shall follow separation of duty principles to avoid conflicts of interest.	Guardian, Vantage, Arc	Nozomi Networks detects change management events on the network for violations to the change management process. For example, these could include connections that are not from the change management system that perform: Configuration Mismatch, New global function code, New global MAC vendor, New global variable producer, New ARP, New function code, New link, New MAC address, New network device, New node, New target node, New protocol used, New application on link, New confirmed protocol, New OT node, New OT variable value, New OT variable, Configuration change, Device state change, Firmware change, Program change.
SR 4.3.4.3.7 Establish and document a patch management procedure A procedure for patch management shall be established, documented, and followed.	Guardian, Vantage, Arc	Nozomi Networks collects information about firmware, software versions, and vulnerable software/firmware, which helps to support the patch management process.

Security Control	Nozomi Networks Platform Components	How Nozomi Networks Supports
SR 4.3.4.5.1 Implement an incident response plan The organization shall implement an incident response plan that identifies responsible personnel and defines actions to be performed by designated individuals.	Guardian, Vantage	Customizable incident response Playbooks standardize the incident response process.
SR 4.3.4.5.3 Establish a reporting procedure for unusual activities and events The organization should establish a reporting procedure to communicate unusual activities and events that may actually be cyber security incidents.	Guardian, Vantage	Unusual activities and events including anomalies on the network, anomalies in the processes, or usage of the IACS equipment are reported to upstream event management systems, incident response teams, and engineers. The Playbooks should contain a communication plan that details the reporting procedures.
SR 4.3.4.5.6 Identify and respond to incidents If an incident is identified, the organization shall promptly respond in accordance with the established procedures.	Guardian, Vantage	Nozomi Networks can integrate with incident response management systems to help streamline process and accelerate remediation. Additionally, features such as the Time Machine, the Network Graph, and Vantage IQ provide deep insights and details to make recovery easier, and ensure mitigations are effective.
SR 4.3.4.5.7 Identify failed and successful cyber security breaches The organization should have procedures in place to identify failed and successful cyber security breaches.	Guardian, Vantage, Arc	Nozomi Networks detects failed and successful cyber security breaches, including: DDOS attack, Malicious Protocol detected, Multiple Access Denied events, Multiple unsuccessful logins, Malformed Network packet, Network Scan, OT protocol packet injection, Malformed OT protocol packet, TCP flood, Malformed TCP layer, TCP SYN flood, UDP flood, Bad reputation IP, Malicious domain, Bad ip reputation, Malicious URL, Malware detection, MITM attack. Additionally, anomalies on the network, the devices, or in the process are monitored for.

ISA/IEC 62433 – Part 3-3

System security requirements and security levels

Security Control	Security Levels S1	S2	S3	S4	Nozomi Networks Platform Components	How Nozomi Networks Supports
SR 3.3.1.1 Human user identification and authentication Ability to identify and authenticate all human users.	✓	✓	✓	✓	Guardian, Vantage, Arc	By consistently monitoring the network and assets, Guardian, Vantage, and the Arc endpoint sensor identify suspicious login activities and generate reports and alarms. The customization of dashboards permits the operator to be aligned by with custom KPIs and rules associated with IACS components, helping in the enforcement of policies.
SR 3.3.1.5 Authenticator Management	✓	✓	✓	✓	Guardian, Vantage, Arc	Nozomi Networks detects weak and cleartext password in the network.
SR 3.3.1.6 Wireless Access Management Ability to identify and authenticate all users engaged in wireless communications.	✓	✓	✓	✓	Guardian, Guardian Air, Vantage, Arc	Nozomi Networks provides visibility into wireless access points connected to the wired network, and monitors wireless networks to conduct an asset inventory and detect wireless attacks.
SR 3.3.1.7 Strength of password-based authentication Ability to enforce configurable password strength based on minimum length and variety of character types.	✓	✓	✓	✓	Guardian, Vantage, Arc	Nozomi Networks detects weak and cleartext passwords on the network.
SR 3.3.1.8 Public Key infrastructure (PKI) certificates Ability to operate a PKI according to commonly accepted best practices or obtain public key certificates from an existing PRI.	✓	✓	✓	✓	Guardian, Vantage, Arc	Nozomi Networks detects communication between components of Public Key Infrastructure and network certificate exchanges.
SR 3.3.1.9 Strength of public key authentication For control systems utilizing public key authentication, the control system shall provide the capability to: a) validate certificates by checking the validity of the signature of a given certificate; e) validate certificates by constructing a certification path to an accepted CA or in the case of self-signed certificates by deploying leaf certificates to all hosts which communicate with the subject to which the certificate is issued; f) validate certificates by checking a given certificate's revocation status; g) establish user (human, software process or device) control of the corresponding private key; and h) map the authenticated identity to a user (human, software process or device).	✓	✓	✓	✓	Guardian, Vantage, Arc	Nozomi Networks detects communication between components of Public Key Infrastructure and network certificate exchanges.

Security Control	Security Levels				Nozomi Networks Platform Components	How Nozomi Networks Supports
	S1	S2	S3	S4		
SR 3.3.1.11 Access via untrusted networks Ability to monitor and control all methods of access to the control systems via untrusted networks.	✓	✓	✓	✓	Guardian, Vantage, Arc	Nozomi Networks detects communications to/from untrusted networks, as well as remote access devices and protocols used.
SR 3.3.2.2 Wireless use control The control system shall provide the capability to authorize, monitor and enforce usage restrictions for wireless connectivity to the control system according to commonly accepted security industry practices.	✓	✓	✓	✓	Guardian, Guardian Air, Vantage, Arc	Nozomi Networks provides a comprehensive inventory of all wireless assets detected Security teams are alerted in real time of wireless specific threats to help minimize operational impacts. Additionally, assets that may be forbidden by policy from using wireless or wired networks can be detected.
SR 3.3.2.3 Use control for portable and mobile devices Ability to automatically enforce configurable usage restrictions that include: a) preventing the use of portable and mobile devices; b) requiring context specific authorization; and c) restricting code and data transfer to/from portable and mobile devices.	✓	✓	✓	✓	Guardian, Guardian Air, Vantage, Arc	Nozomi Networks helps inventory portable and mobile devices connected to the network, and monitors for portable and mobile device-specific threats.
SR 3.3.2.5 Session lock Ability to prevent further access by initiating a session lock after a configurable time period of inactivity or by manual initiation.	✓	✓	✓	✓	Guardian, Vantage, Arc	Nozomi Networks provides details of user devices connected to the network for further security inspection, such as access control configurations.
SR 3.3.2.6 Remote session termination Ability to terminate a remote session either automatically after a configurable time period of inactivity or manually by the user who initiated the session		✓	✓	✓	Guardian, Vantage, Arc	Nozomi Networks provides details of user devices connected to the network for further security inspection, such as remote session configuration.
SR 3.3.2.8 Auditable events Ability 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. Individual audit records shall include the timestamp, source (originating device, software process or human user account), category, type, event ID and event result	✓	✓	✓	✓	Guardian, Vantage, Arc	Nozomi Networks generates audit records for a variety of types of events, which can be sent to SIEM/SOC for further analysis.
SR 3.3.2.9 Audit storage capacity Allocate sufficient audit record storage capacity for log management and system configuration and accounting for over capacity levels.	✓	✓	✓	✓	Guardian, Vantage, Arc	Nozomi Networks can monitor drive space usage and availability of network assets for capacity related issues.

Security Control	Security Levels				Nozomi Networks Platform Components	How Nozomi Networks Supports
	S1	S2	S3	S4		
SR 3.3.2.11 Timestamps Generate timestamps (including date and time) of audit records using internal system clocks.			✔	✔	Guardian, Vantage, Arc	Nozomi Networks identifies network communications and events in real-time and provides a timestamp for all events.
SR 3.3.3.1 Communications integrity Protection of the integrity of transmitted information	✔	✔	✔	✔	Guardian, Vantage, Arc	Nozomi Networks detects communication integrity violations including: duplicate IP, Invalid IP, OT protocol packet injection, configuration mismatch, MITM attack, configuration change, weak encryption, and others that can indicate misconfiguration or attempts to tamper with the communications.
SR 3.3.3.2 Malicious code protection Protections to prevent detection, reporting and mitigation of the effects of malicious code or unauthorized software with the ability to update the protection mechanisms.	✔	✔	✔	✔	Guardian, Vantage, Arc	Nozomi Networks identifies the status of antivirus software installed on assets and detects malicious code on the network, which could include: Malware detection, Malicious domain, Bad IP reputation, Malicious URL, Malicious Protocol detected, Malformed OT protocol packet, Malicious File, Suspicious Activity, etc. Additionally, Guardian employs an onboard malware sandbox used to detect malware on the network.
SR 3.3.3.4 Software and information integrity Ability to detect, record, report and protect against unauthorized changes to software and information at rest.	✔	✔	✔	✔	Guardian, Vantage, Arc	Nozomi Networks detects and alerts on unauthorized changes to software and information at rest including: Firmware change, program change, program upload, unwanted application payload, etc.
SR 3.3.3.5 Input validation 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.	✔	✔	✔	✔	Guardian, Vantage, Arc	Nozomi Networks detects attempts to tamper with network protocols.
SR 3.3.3.8 Session integrity Ability to protect the integrity of sessions. The control system shall reject any usage of invalid session IDs.	✔	✔	✔	✔	Guardian, Vantage, Arc	Nozomi Networks monitors network sessions and detects attempts of session integrity violation.
SR 3.3.4.1 Information confidentiality Ability to protect the confidentiality of information for which explicit read authorization is supported, whether at rest or in transit.	✔	✔	✔	✔	Guardian, Vantage, Arc	Nozomi Networks detects signs of violation of confidentiality in transit, such as weak and cleartext passwords or insecure protocols in use.
SR 3.3.4.3 Use of cryptography If cryptography is required, the control system shall use cryptographic algorithms, key sizes and mechanisms for key establishment and management according to commonly accepted security industry practices and recommendations.	✔	✔	✔	✔	Guardian, Vantage, Arc	Nozomi Networks detects signs of weak encryption.

Security Control	Security Levels				Nozomi Networks Platform Components	How Nozomi Networks Supports
	S1	S2	S3	S4		
SR 3.3.5.1 Network segmentation Ability to logically segment control system networks from non-control system networks and to logically segment critical control system networks from other control system networks.	✔	✔	✔	✔	Guardian, Vantage, Arc	Nozomi Networks offers visibility and inventory management for assets on control systems and network segments/zones, facilitating the segmentation of critical IACS assets from the rest of the network.
SR 3.3.5.2 Zone boundary protection Ability to monitor and control communications at zone boundaries to enforce the compartmentalization defined in the risk-based zones and conduits model.	✔	✔	✔	✔	Guardian, Vantage, Arc	Nozomi Networks continuously monitors zone boundary devices (such as firewalls) on the network for any anomalies or threats. An alert is generated if anomalies or threats are detected, enabling security teams to quickly investigate and mitigate any impact to operations.
SR 3.3.5.3 General-purpose person-to-person communication restrictions Ability to prevent general purpose person-to-person messages from being received from users or systems external to the control system.	✔	✔	✔	✔	Guardian, Guardian Air, Vantage, Arc	Nozomi Networks detects communication with external systems for further security inspection. Additionally, wireless networks can be monitored for rogue communications.
SR 3.3.6.2 Continuous monitoring Ability to continuously monitor all security mechanism performance and make recommendations to detect, characterize and report security breaches in a timely manner.		✔	✔	✔	Guardian, Guardian Air, Vantage, Arc	Nozomi Networks continuously monitors network (wired and wireless) and endpoint assets. The “real-time” activity of assets is compared against a “known-good” baseline to detect anomalies and vulnerabilities. “New” and “different” behaviors are analyzed to determine whether it is a critical vulnerability and warrants an alert.
SR 3.3.7.1 Denial of service protection Ability to operate in a degraded mode during a DoS event.	✔	✔	✔	✔	Guardian, Vantage, Arc	Nozomi Networks provides alerts for early detection of DDOS attacks on the networks. Playbooks can help to accelerate and standardize remediation steps across teams.
SR 3.3.7.2 Resource management Ability to limit the use of resources by security functions to prevent resource exhaustion.	✔	✔	✔	✔	Guardian, Vantage, Arc	Nozomi Networks detects some attempts of resource exhaustion, such as Network Scan, Flood of MAC addresses, Protocol-based flood, TCP flood, TCP SYN flood, and UDP flood, etc.
SR 3.3.7.4 Control systems and recovery Ability to recover and reconstitute to a known secure state after a disruption or failure.	✔	✔	✔	✔	Guardian, Vantage, Arc	Nozomi Networks provides a Time Machine feature that facilitates the reconstruction of a network by providing snapshots of communications states both before and after a specific incident.
SR 3.3.7.5 Emergency power Ability to switch to and from an emergency power supply without affecting the existing security state or a documented degraded mode.	✔	✔	✔	✔	Guardian, Vantage, Arc	Nozomi Networks provides asset visibility of power source devices (UPS) in the network.

Security Control	Security Levels				Nozomi Networks Platform Components	How Nozomi Networks Supports
	S1	S2	S3	S4		
SR 3.3.7.6 Network and security configuration settings Ability to be configured according to recommended network and security configurations as described in guidelines provided by the control system supplier.	✓	✓	✓	✓	Guardian, Vantage, Arc	Nozomi Networks detects OT device configuration changes on the network. Alerts are generated to ensure that the changes are authorized.
SR 3.3.7.8 Control system component inventory Ability to report the current list of installed components and their associated properties.		✓	✓	✓	Guardian, Vantage, Arc, Asset Intelligence	Nozomi Networks provides a continuous passive and active network asset inventory of control system components. Leveraging our extensive knowledge of OT/IoT systems, Asset Intelligence enhances device profiles with detailed asset information to ensure accurate identify of assets.

4. Conclusion

With the Nozomi Networks platform, ICS security stakeholders can address key aspects, requirements and cybersecurity recommendations defined in the ISA/IEC 62443 standards. Nozomi Networks is committed to helping organizations implement effective ICS cybersecurity controls. Through technology innovations and extensive ICS expertise, the Nozomi Networks platform is built to ensure safety and operational integrity in accordance with all standards, objectives and practices outlined in the ISA/ IEC 62443 standards.

To simplify the initial steps in the journey to compliance, customers can utilize our **ISA/IEC 62443 Content Pack**. This pack includes a foundational set of reports and queries that are ready for customization, designed to help advance their efforts efficiently.

Let's get started

To see the Nozomi Networks platform for yourself, schedule a demo or join our next live group demo.

Custom Demo

nozominetworks.com/demo

Group Demo

nozominetworks.com/resources/live-demo-the-nozomi-networks-platform-in-15-minutes

Nozomi Networks protects the world's critical infrastructure from cyber threats. Our platform uniquely combines network and endpoint visibility, threat detection, and AI-powered analysis for faster, more effective incident response. Customers rely on us to minimize risk and complexity while maximizing operational resilience.

NOZOMI NETWORKS

nozominetworks.com