ARMIS®

**WHITE** PAPER


# USING ARMIS TO ENABLE THE IEC62443 STANDARD FOR OT SECURITY

 

# Table of contents

# INTRODUCTION

Operational Technology (OT) plays a key role in critical infrastructure as well as industries such as manufacturing, automotive, transportation, oil & gas, energy & utilities, and more.

OT security is critical in helping organizations prevent cyber-attacks and strengthen their defenses against hackers. It protects critical infrastructure against emerging attack vectors and can greatly improve operational and safety metrics.

However, the growth of the Industrial Internet of Things (IIoT) and Industry 4.0 are creating greater security threats for critical systems. Industrial environments face the greater risk of increasingly sophisticated cyber-attacks that could damage their equipment, cause downtime, and result in data leaks. To further protect these systems, a series of security standards known as IEC 62443 has been developed to offer deeper authority and guidance on industrial security.

This whitepaper will outline the IEC 62443 standard and how Armis helps you to implement and deploy these critical standards.

### Can you see all the assets in your environment?

- How many assets do I have— how accurate is my CMDB?
- How many managed vs. unmanaged assets do I have?
- What is the distribution of assets by site or department?
- Do I have any laptops missing an agent?
- Do I have any out-of-warranty devices? If so, where are they and who is using them?
- How many users (by asset type) do I have and where are they located?
- How many unsanctioned applications are in my environment?
- How many cloud assets (by provider) do I have?
- Do I have any users or admins not adhering to password rotation rules?
- Are there any devices reported missing that appear on my network?
- Do I have any AD users whose password needs to change?
- Do my laptops have encryption hard drive enabled?
- How many vulnerable assets do I have (by CVE severity, business unit or location?
- How many devices running unpatched OSs or applications?

# WHAT IS THE **IEC 62443 STANDARD**?

OT systems are protected by a security standard owned by the International Electrotechnical Commission (IEC). The standards were originally created by the International Society of Automation (ISA) and known as ISA 99. However, they were taken over by the IEC and became known as the IEC 62443. The IEC is now responsible for the standards and their further development.

The IEC 62443 standards exist to evaluate the existing and emerging vulnerabilities within Industrial Control Systems (ICS). It assists in applying necessary mitigations to threats against ICS. The overall goal of the standard is to reduce the risk of failures and threats occurring within ICS networks.

IEC 62443 standards provide comprehensive recommendations on how to defend industrial networks and systems against known and emerging security threats. These standards are critical to any organization that has industrial interests and needs to implement strong industrial security processes.

## IEC 62443 standard format

The IEC 62443 standard is formed of 13 comprehensive documents that are split into four distinct groups: General, Policies & Procedures, System, and Components. This ensures a flexible framework that helps organizations address and mitigate security vulnerabilities.

**The standard is split into four levels:**

| | |
|---|---|
| **Level 1** | The first level of IEC 62443 provides an outline of the terminology, concepts, and models (1-1), a master glossary of terms and abbreviations (1-2), system security compliance metrics (1-3), and Industrial Automation & Control Systems (IACS) security lifecycle and use cases (1-4). |
| **Level 2** | The next level up provides requirements and implementation guidelines for IACS systems (2-1 and 2-2), patch management for IACS environments (2-3), and installation and maintenance requirements for IACS suppliers (2-4). |
| **Level 3** | **The system-centric stage.** Covers security technologies for IACS (3-1), security levels for zones and conduits (3-2), and system security requirements and security levels (3-3). |
| **Level 4** | **The component-centric stage.** Adds an advanced component and device-centric state beyond Level 3. Contains product development requirements (4-1) and technical security requirements for IACS components (4-2). |

# HOW ARMIS ASSISTS ORGANIZATIONS WITH **IEC 62443 3-2 COMPLIANCE**

IEC 62443 Level 3 section 2 specifically addresses security risk assessment and network design. This section of the standard advises organizations on how to segment their networks into zones and conduits, which helps to protect OT systems by making it more difficult for attackers to navigate through a network. It groups systems that have similar functionalities, which aim to restrict access, limit threat exposure, and prevent propagation.

## Section 3-2 of IEC 62443 contains 13 pieces of guidance for organizations:

| Category | IEC Category description | How Armis helps |
|---|---|---|
| **ZCR 1.1** | The organization shall clearly identify the System under Consideration (SuC), including a clear definition of the security perimeter and identification of all access points to the SuC. | Armis automatically discovers and catalogs all active connected network devices and their communications to define an SuC. Armis ensures all communications accessing a network (the SuC) and its devices pass within the intended points. Real-time alerts are raised if communications violate flow and perimeter restrictions. |
| **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. | Armis generates a real-time holistic risk score for every device connected to the network based on the Common Vulnerability Scoring System (CVSS). It also provides a risk score for any identified vulnerabilities within that device. |
| **ZCR 3.2** | IACS shall be grouped into zones that are logically or physically separated from business or enterprise system assets. | Armis groups devices based on attributes including physical boundaries, logical boundaries, device type, or function. This ensures users can easily visualize boundaries, evasions, and potential exfiltrations and anomalies. Organizations can then define risk-based zones for network segmentation and policy-based enforcement. |
| **ZCR 3.3** | Safety-related assets shall be grouped into zones that are logically or physically separated from zones with non-safety-related assets. | |

| Category | IEC Category description | How Armis helps |
|---|---|---|
| **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. | Armis discovers devices as soon as they connect to a network. It either permits devices to connect to the SuC and be grouped accordingly or quarantines non-permitted devices. It quickly identifies boundary evasions and remediates open links between control systems and business networks or existing security infrastructure. |
| **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. | The Armis Policy Engine associates new devices to zones with permissions. This ensures alerts are triggered when two network zones have active communications and prevents access to the IACS at undesired times. Armis also enables custom checks and real-time alerts for access time violations and records when each communication was first and last seen active. |
| **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. | The Armis Purdue Model network map automatically groups devices based on their device type, zone or boundary, location, and function. This ensures users can easily spot devices that violate the policy and generates alerts when violations occur. |
| **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. | Armis enables users to easily identify all discovered devices, their logical boundaries, connected zones, and conduits. It also generates a catalog of these assets and their classification, unique attributes, traffic, services, activities, applications, connections, risks, and vulnerabilities. All the information automatically collected by Armis can be used to enrich third-party platforms via pre-built API integrations, json, and syslog. |

| Category | IEC Category description | How Armis helps |
|---|---|---|
| **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. | Armis provides a library of known ICS vulnerabilities, operational and security threats, threat detection engines, NIST database, and the MITRE ATT&CK for ICS framework. This presents a real-time risk profile for every device. Armis can also filter threat vectors, complexity, location, interaction, privileges, impact, and criticality across all sources and targets. |
| **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. | Armis passively detects vulnerabilities within ICS devices by matching device profiles to specific common vulnerabilities and exposures (CVEs) or using vulnerability information from third-party systems. Where permitted, Armis can actively scan devices to improve the vulnerability matching process. |
| **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. | Armis provides reports that can be immediately downloaded or scheduled to be emailed. It also provides multiple customizable dashboards and policies that can generate emails and notifications. These methods ensure users can document and report on the risk assessment of their system. |
| **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 | Armis provides full visibility of the SuC. This includes details of all active and dormant connected network devices, their functions, properties, activities, services, traffic, connections, and risk profiles. It also includes device communications and links, protocols, and services used by each device across all networks and zones. |
| **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. | Armis provides a library of CVEs and threat intelligence from ICS-CERT, IACS vendor advisories, and its own threat detection team. These libraries are used to determine, based on the assets and communications observed in the SuC, which risks, threats and vulnerabilities apply. Links to threats and vulnerabilities are presented for further investigation. |

# HOW ARMIS ASSISTS ORGANIZATIONS WITH **IEC 62443 3-3 COMPLIANCE**

The 62443 3-3 section relates to general systems security requirements, which include authentication, data confidentiality, and system integrity.

| Category | IEC Category description | How Armis helps |
|---|---|---|
| **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. | Armis monitors remote network access and authentication attempts over several clear-text OT and IT protocols. Failed and successful authentication attempts are logged for analysis and to ensure critical systems are accessed using individual user credentials. Real-time alerts are raised in case authentication occurs through insecure credentials or brute-force attempts. |
| **SR 1.2** | The control system shall provide the capability to identify and authenticate all software processes and devices. This capability shall enforce such identification and authentication on all interfaces which provide access to the control system to support the least privilege in accordance with applicable security policies and procedures. | Armis' API can provide device information to the control system. This ensures that only devices with approved security postures can connect. |
| **SR 1.6** | The control system shall provide the capability to identify and authenticate all users (humans, software processes or devices) engaged in wireless communication. | Armis' wireless integration enables organizations to force the authentications of users and devices within the control system. This ensures all wireless devices are identified and authenticated. |
| **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. | Armis features out-of-the-box checks and real-time alerts for the use of insecure credentials and brute-force attempts over several clear-text OT and IT protocols. |

| Category | IEC Category description | How Armis helps |
|---|---|---|
| **SR 1.8** | Where Public Key Infrastructure (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 | Armis performs multiple certificate checks to ensure secure information exchange. This includes checks on certificate validity, certificate reuse, certificate expiration, and the trustworthiness of certificate authorities. |
| **SR 1.9** | For control systems utilizing public-key authentication, the control system shall provide the capability to:<br><br>a) validate certificates by checking the validity of the signature of a given certificate;<br><br>b) 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;<br><br>c) validate certificates by checking a given certificate‘s revocation status;<br><br>d) establish user (human, software process or device) control of the corresponding private key; and<br><br>e) map the authenticated identity to a user (human, software process or device). | Armis performs several checks on certificates to ensure the security of information exchange. These include checks on certificate validity, certificate reuse, certificate expiration, and trustworthiness of certificate authorities. |
| **SR 1.10** | The control system shall provide the capability to obscure feedback of authentication information during the authentication process. | The Armis Policy Engine ensures credentials sent in cleartext and unencrypted are identified. It triggers alerts that identify authentication sessions out of policy. |
| **SR 1.13** | The control system shall provide the capability to monitor and control all methods of access to the control system via an untrusted network. | Armis continuously monitors network traffic and communications to understand device behavior and information exchange across the network. It issues alerts for illegitimate access to devices or the network, which provides additional details like who performed the access, over which protocol, and when. |

| Category | IEC Category description | How Armis helps |
|---|---|---|
| **SR 2.1** | On all interfaces, the control system shall provide the capability to enforce authorizations assigned to all human users for controlling use of the control system to support segregation of duties and least privilege. | Armis detects and assesses every device that connects to the network and helps the control system to determine if a device is properly configured per corporate policies regarding least privilege. |
| **SR 2.2** | The control system shall provide the capability to authorize, monitor and enforce usage<br><br>restrictions for wireless connectivity to the control system according to commonly accepted security industry practices. | The Armis platform detects wireless devices that behave suspiciously or maliciously. It triggers wireless local area network (LAN) controllers to take appropriate action, such as blocking the device from the network or changing which virtual LAN (VLAN) the device is assigned to. |
| **SR 2.3** | The control system shall provide the capability to automatically enforce configurable usage restrictions that include:<br>• Preventing the use of portable and mobile devices;<br>• Requiring context-specific authorization; and<br>• Restricting code and data transfer to/from portable and mobile devices. | Armis continuously monitors all communications for wireless traffic. It protects against wireless devices attempting to join the network based on several attributes, including device type. For wireless devices, Armis uses security platform integrations to alert and block data transfers to or from portable and mobile devices. |
| **SR 2.4** | The control system shall provide the capability to enforce usage restrictions for mobile code technologies based on the potential to cause damage to the control system that include:<br>• Preventing the execution of mobile code;<br>• Requiring proper authentication and authorization for the origin of the code;<br>• Restricting mobile code transfer to/from the control system; and<br>• Monitoring the use of mobile code. | Armis identifies applications, protocols, and file transfer mechanisms, and enforce usage restrictions via integrations into existing security infrastructures. |

| Category | IEC Category description | How Armis helps |
|---|---|---|
| **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. | Armis continuously monitors network and device activity in real-time. It logs and issues alerts for security events such as policy failures, network reconnaissance, unauthorized access and communications, failed and successful remote login attempts, device errors, malfunctions, and configuration changes, and maintenance operations. This enables organizations to analyze and respond to events using data like the timestamp, source, and target, event type, potential causes, impact, and recommendations. Alerts and logs can be filtered and exported to third-party SIEMs and SOARs. |
| **SR 2.11** | The control system shall provide timestamps for use in audit record generation. | Armis logs all activities and services and their timestamps, which can be synced with system network time and their audit record timing. |
| **SR 2.12** | The control system shall provide the capability to determine whether a given human user took a particular action. | Armis tracks all activities, connections from devices on a network and their targets. It also tracks and logs specific programmable logic controllers (PLCs) and other ICS protocols. |
| **SR 3.1** | The control system shall provide the capability to protect the integrity of transmitted information. | Armis enables users to verify that sensitive information is communicated via secure, encrypted protocols and cipher suites. This can be performed in several ways:<br>• Identifying critical control systems and servers to check whether their communication is encrypted.<br>• Real-time alerts when insecure protocols are used to exchange sensitive information from both source and destination devices.<br>• Detection of which encryption suite is being used, which enables users to set policies regulating which to approve and which will trigger alerts or enforcement actions. |

| Category | IEC Category description | How Armis helps |
|---|---|---|
| **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. | Armis provides a combination of signature- and anomaly-based threat detection. This ensures real-time alerts of known and unknown malware and exploit attempts on the network. Malicious activity is detected at the earliest possible stage, such as during reconnaissance and spread. Alerts contain clear information about the source, target, and nature of the threat, enabling immediate response and preventing the attack through integrations with firewalls, network access control (NAC), wireless LAN controllers (WLCs), and networking equipment. |
| **SR 3.4** | The control system shall provide the capability to detect, record, report, and protect against unauthorized changes to software and information at rest. | Armis monitors, detects, records, reports, and protects against unauthorized connections and changes to control system components. It monitors devices for abnormal behavior and triggers policies that prohibit such connections and their actions. |
| **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. | Armis provides full deep packet inspection (DPI) on industrial protocol communications. This verifies whether the message is syntactically well-formed and complies with the protocol specification, and ensures content is valid and expected. Failure of these verification steps triggers real-time alerts containing information for analysis and response. |
| **SR 3.6** | The control system shall provide the capability to set outputs to a predetermined state if the normal operation cannot be maintained as a result of an attack. | Armis provides alerts when device behavior is anomalous or indicates signs of an attack. |
| **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. | Armis provides effective predictive maintenance by monitoring and detecting error conditions of ICS devices and control systems. It issues real-time reports that can be correlated to other network activity that may have caused the error to ensure timely troubleshooting and response with minimal effort. |

| Category | IEC Category description | How Armis helps |
|---|---|---|
| **SR 3.8** | The control system shall provide the capability to protect the integrity of sessions. The control system shall reject any usage of invalid session IDs. | The Armis Policy Engine protects the integrity of sessions by enabling users to create rules that ensure only authorized personnel can access machines, applications, and their activity. |
| **SR 3.9** | The control system shall protect audit information and audit tools (if present) from unauthorized access, modification, and deletion. | Armis' data is stored outside its control systems environment and is protected by multiple security controls. The Armis collector can be configured to be completely passive, which reduces the ability of an adversary to detect its presence and understand that audit records are outside the immediate environment. |
| **SR 4.1** | The control system shall protect the confidentiality of information at rest and in transit. | Armis enables users to verify that sensitive information is communicated using secure encrypted protocols and cipher suites. |
| **SR 4.2** | The control system shall provide the capability to purge all information for which explicit read authorization is supported from components to be released from active service and/or decommissioned. | Users can configure Armis to create an ITSM ticket if a device hasn't been seen on the network for a specific period of time. This ensures IT staff are aware when devices have been removed and require purging. |
| **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 recognized and proven security practices. | Armis features several built-in controls that ensure encrypted network communications follow international standards and recognized security practices. It issues alerts when it detects the use of insecure protocols or protocol versions, weak cipher suites, encryption keys, and untrustworthy certificates in TLS/SSL communications, and known and unknown malware exploit kits. |
| **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. | Armis reports on all active connected devices and traffic flows, which helps to identify security perimeters, access points, and groups of functionally and related devices. Armis supports the enforcement of network segmentation into zones and conduits, which guarantees no undesired communication or information flow occurs, and issues real-time alerts when violations are detected. It also features Cisco ISE and PaloAlto integration that helps assign devices to specific VLANs and subnets. |

| Category | IEC Category description | How Armis helps |
|---|---|---|
| **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. | Armis' Purdue Model map enables users to monitor communications at zone boundaries and detect violations of network compartmentalization defined by zones and conduits. This ensures only legitimate communications occur through appropriate boundary protection devices, such as firewalls and gateways, firewalls, and real-time alerts are raised if violations occur. |
| **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 include emails, social media, or other message systems that permit the transmission of any type of executable file. | Armis monitors communications within and across zone boundaries and provides real-time alerts if undesired communications, protocols, or applications are observed. |
| **SR 5.4** | The control system shall support partitioning of data, applications and services based on criticality to facilitate implementing a zoning model. | Armis provides visibility and real-time alerts into the activity, connections, and services of every device on a network. This helps users to define appropriate zones and conduits, validate activities, connections, and services, activities, and communications. Armis also tags or assigns boundaries to groups of devices, which means alerts can be configured for devices that communicate across unapproved zones. |
| **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. | Armis monitors communications to control systems and components and file transfer operations. This ensures information and audit logs are only accessed by authorized users and workstations. Real-time alerts are raised when 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. | Armis continuously monitors network traffic for vulnerabilities and threats, and issues real-time alerts. It features ICS-specific signatures and checks, Mitre ATT&CK for ICS Frameworks, ICS-Certs, NIST database, and threat detection engines, combined with a powerful behavioral anomaly detection engine to identify known and unknown threats at the earliest stage. Alerts contain comprehensive details that ensure effective analysis and timely response. |

| Category | IEC Category description | How Armis helps |
|---|---|---|
| **SR 7.1** | The control system shall remain operative in a degraded mode during a DoS event. | Armis provides built-in controls for real-time detection and remediation of several types of Denial of Service (DoS) attacks. Alerts include details of the source and target hosts and the DoS attack technique, which enables quick response that prevents control system and component function compromise. Armis helps users to easily monitor traffic loads to and from control systems at any time, which prevents DoS events caused by system overload. |
| **SR 7.7** | The control system shall restrict the use of unnecessary functions, ports, protocols and/or services. | Armis automatically fingerprints network devices and creates an inventory of open ports, protocol, activities, and services in use for each device. It matches this information with desired configurations and/or company policies. |
| **SR 7.8** | The control system shall provide the capability to report the current list of installed components and their associated properties. | Armis automatically generates an inventory of all devices and communications connected to a network. It provides accurate device fingerprinting, including details like IP and MAC addresses, hostnames, OS version, open ports, protocols, services, and associated vulnerabilities in use, and ICS device data like firmware version, serial number, device modules information, and known vulnerabilities. The inventory information is available to users through Armis's Search Query Language (SQL), which features advanced searching and filtering and enables devices to be associated with currently exposed security threats. |

# HOW ARMIS ASSISTS ORGANIZATIONS WITH **IEC 62443 4-2 COMPLIANCE**

IEC 62443 4-2 specifies the technical requirements for securing the individual components of an ICS network. Armis helps organizations comply with the following criteria in this section of the standard:

| Category | IEC Category description | How Armis helps |
|---|---|---|
| **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. | Armis monitors authentication attempts over various clear-text OT and IT protocols, including HTTP, FTP, SMB, and Telnet. Failed and successful authentication attempts are logged for analysis and to ensure all critical systems are accessed using individual user credentials. Real-time alerts are raised in case authentication occurs through default or insecure credentials or brute-force attempts. |
| **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. | Armis provides out-of-the-box checks and real-time alerts for insecure credentials and brute-force attempts over various clear-text OT and IT protocols. |
| **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. | Armis performs multiple certificate checks to ensure secure information exchange. This includes checks on certificate validity, reuse, and expiration, and trustworthiness of certificate authorities. |
| **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. | Armis continuously monitors all network traffic and communications to understand device behavior and information exchange. It issues alerts of illegitimate access of devices and the network, providing additional details like who performed the access, over which protocol, and when. |

| Category | IEC Category description | How Armis helps |
|---|---|---|
| **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. | Armis continuously monitors network and device activity, issues real-time alerts, and logs events of interest, such as network reconnaissance activity, failed and successful remote login attempts, unauthorized access, and device malfunctions. Alerts and logs contain information that helps to analyze and respond to the event, such as timestamp, source and target information, event type, and potential causes, impact, and recommendations, which can be filtered and exported to third-party SIEMs and SOARs. |
| **CR 3.2** | The network device shall provide protection from malicious code. If a network device is able to utilize a compensating control, it need not directly support protection from malicious code. | Armis uses a combination of signature and anomaly- or behavioral-based detection to detect and issue real-time alerts of known and unknown malware and exploit attempts. Alerts contain clear information about the source, target, and nature of the threat, enabling an immediate response that prevents malware from carrying out the actual attack by integrating with firewalls, NACs, WLCs, and networking equipment. |
| **CR 3.5** | Components shall validate the syntax and content of any input that is used as an industrial process control input | Armis provides DPI on industrial protocol communications. It verifies the validity of process control messages by ensuring messages are syntactically well-formed and content is valid and expected. Failure of these verification steps results in real-time alerts that provide clear information for analysis and response. |
| **CR 3.7** | Components shall identify and handle error conditions in a manner such that effective and timely troubleshooting and remediation can occur. | Armis monitors ICS devices and control systems to detect configuration uploads, configuration changes, mode changes, errors, and process request failures. This intelligence is reported to users in real-time and can be correlated with other network activity that may have caused the error to ensure timely troubleshooting and response with minimal effort. |

| Category | IEC Category description | How Armis helps |
|---|---|---|
| **CR 4.1** | Components shall protect the confidentiality of information at rest and in transit. | Armis enables users to verify sensitive information is communicated using secure encrypted protocols and cipher suites. This verification can be performed by ensuring critical control systems and servers are using encrypted communication, or through real-time alerts of insecure protocols being used to exchange sensitive information. Alerts include information about source and destination devices that enable remediation actions. |
| **CR 4.3** | If cryptography is required, components shall use cryptographic security mechanisms according to internationally recognized and proven security practices. | Armis provides built-in controls that ensure encrypted communications in the monitored network follow international standards and recognized security practices. It alerts users of the use of insecure protocols or protocol versions being used, such as HTTP vs. HTTPS, TLS/SSL certificates issued by untrustworthy certificate authorities, and known malware and exploit kits. |
| **CR 5.1** | Components shall support a segmented network to support the broader network architecture based on logical segmentation and criticality. | Armis reports on all active devices and traffic flows connected to the network. This enables the identification of security perimeters, access points, and groups of functionally and logically related devices. It also supports the enforcement of network segmentation into zones and conduits, which prevents undesired communication or information flow, and raises real-time violation alerts. |
| **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. | Armis enables users to monitor communications at zone boundaries and detect violations of network compartmentalization defined by zones and conduits. Its Purdue Model map helps users observe communications at zone boundaries and detect communications across undesired zones. Armis ensures only legitimate communications occur in the network and at zone boundaries using appropriate boundary protection devices like firewalls and gateways and issues actionable real-time alerts if violations occur. |

| Category | IEC Category description | How Armis helps |
|---|---|---|
| **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 include emails, social media, or other message systems that permit the transmission of any type of executable file. | Armis monitors communications within and across zone boundaries and provides real-time alerts if undesired communications, protocols, or applications are observed. It proactively blocks those applications, users, machines, and connections. |
| **CR 6.1** | Components shall provide the capability for authorized humans and/or tools to access audit logs on a read-only basis. | Armis monitors access and communications to control systems and components and file transfer operations. It ensures information and audit logs are only accessed by authorized users and workstations and raises real-time alerts if unauthorized access and communications are detected. Armis also stores logs outside of the environment, providing additional access control to the logs. |
| **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... | Armis continuously monitors network traffic for anomalies, vulnerabilities, and threats, then issues real-time alerts. Armis provides ICS-specific signatures and checks, MITRE ATT&CK for ICS Frameworks, ICS-Certs, NIST database, and threat detection engines combined with a powerful behavioral anomaly detection engine that ensures known and unknown threats are identified as quickly as possible. These threats include the use of insecure protocols and configurations, network reconnaissance activity, possible data breaches, known and unknown malware and exploits, and ICS device errors and malfunctions. Alerts contain comprehensive details that lead to effective analysis and timely response. |

| Category | IEC Category description | How Armis helps |
|---|---|---|
| **CR 7.1** | Components shall maintain essential functions in a degraded mode during a DoS attack. | Armis provides built-in controls for real-time detection and remediation of various DoS attacks. It issues alerts with information on source and target hosts and the DoS attack technique being used. This ensures quick response before control systems and components are compromised. Armis enables users to monitor traffic loads to and from control systems at any time to prevent DoS events caused by system overload. |
| **CR 7.7** | Components shall restrict the use of unnecessary functions, ports, protocols and/or services. | Armis automatically fingerprints network devices, and creates an inventory of open ports, protocol, activities, and services in use for each device. It matches this information with desired configurations and/or company policies. |
| **CR 7.8** | Components shall provide the capability to support a control system component inventory | Armis automatically generates an inventory of all active and historic network devices and communications. It provides accurate device fingerprinting details including IP and MAC addresses, hostnames, OS version, open ports, protocols, services, and associated vulnerabilities in use. It also details ICS device information like firmware version, serial number, device modules information, and known vulnerabilities. Inventory information is available to users through Armis's SQL, which provides advanced searching and filtering, and enables devices to be associated with currently exposed security threats. |

# **SECURE** YOUR CRITICAL INFRASTRUCTURE WITH ARMIS

Armis is perfectly positioned to help your organization implement and abide by the IEC 62443 standard. Armis covers more enterprise requirements across more components and systems than any other vendor. We take into consideration all Building Management System (BMS), Building Automation System (BAS), IT, and IoT devices, in addition to OT requirements. Whereas other, more niche vendors only cover OT devices.

For more information on how Armis can secure your critical infrastructure download our Securing IT & OT in Industrial Environments whitepaper or book a demo.

# About Armis

Armis is the leading unified asset visibility and security platform designed to address the new threat landscape that connected devices create. Fortune 1000 companies trust our real-time and continuous protection to see with full context all managed, unmanaged, and IoT devices, including medical devices (IoMT), operational technology (OT) and industrial control systems (ICS). Armis provides passive and unparalleled cybersecurity asset management, risk management, and automated enforcement. Armis is a privately held company and headquartered in Palo Alto, California.

armis.com

1.888.452.4011

20210825-1