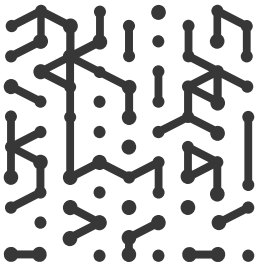
WHITE PAPER

Using Armis To Align With IEC 62443 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, and impact operational resilience. To 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 white paper will outline the IEC 62443 standard and how Armis helps you to implement and align with these critical standards.

What Is The IEC 62443 Standard?

The IEC 62443 standard is a globally recognized set of guidelines developed by the International Electrotechnical Commission (IEC) for industrial cybersecurity. It defines a framework to secure Industrial Automation and Control Systems (IACS), which are commonly found in manufacturing, critical infrastructure, and operational technology (OT) environments.

Key Aspects of IEC 62443 include:

1. Holistic Security - IEC 62443 covers security for the entire lifecycle of industrial systems, from design and development to operation and maintenance.
2. Defense-in-Depth - It advocates for a layered security strategy to mitigate risks from both internal and external threats.
3. Role-Based Compliance – With specific sections that are relevant for different stakeholders, including asset owners, system integrators, and product suppliers.

ARMIS.

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?

Why is IEC 62443 Important?

IEC 62443 is crucial for securing industrial environments, as cyber threats targeting Industrial Automation and Control Systems (IACS) have grown significantly in both frequency and sophistication. Unlike traditional IT environments, OT systems are often designed for reliability and longevity rather than security, making them vulnerable to cyberattacks that can lead to operational disruptions, safety hazards, and financial losses. By providing a structured framework, IEC 62443 helps organizations implement a **defense-in-depth** strategy that reduces risk across industrial networks. The standard ensures that cybersecurity is integrated from the design phase of industrial components to their deployment and ongoing operation, enabling asset owners, system integrators, and product vendors to build and maintain resilient systems.

IEC 62443 also supports regulatory compliance. Many industries, such as energy, manufacturing, and healthcare, are subject to strict cybersecurity regulations, including **NIST 800-82, NERC CIP, and FDA** guidelines. By aligning with IEC 62443, organizations can demonstrate adherence to global best practices, reducing legal and financial risks associated with non-compliance. IEC 62443 facilitates vendor risk management, ensuring that suppliers and system integrators adhere to strong security principles when developing and deploying industrial solutions. This is particularly important as supply chain attacks have become more prevalent, with adversaries targeting vulnerabilities in third-party components to compromise critical infrastructure.

The standard promotes a risk-based approach to cybersecurity by defining **security levels (SL1 to SL4)** and zones and conduits for network segmentation. These concepts allow organizations to tailor their security measures based on the criticality of different assets, ensuring that the most sensitive systems receive the highest level of protection. By following IEC 62443, organizations can establish proactive cybersecurity programs that mitigate risks, improve resilience, and enable secure digital transformation in industrial sectors.

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.

ARMIS

Can you see all the assets in your 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 are running unpatched OSs or applications?

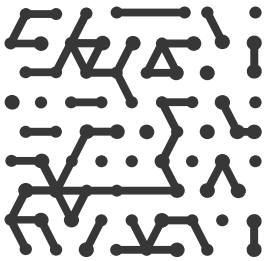
The standard is split into four levels:

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.

Armis Alignment with IEC 62443-3-2 Requirements:

IEC 62443-3-2 Requirement	Description	How Armis helps
ZCR 1.1 Asset Inventory & Classification	Organizations must maintain an accurate and complete inventory of all assets in the industrial environment.	Armis enables the compliance assessment itself with 62443, from the single asset level, to the machine, site and entire organization level, including monitoring and reporting. Armis provides real-time asset discovery and classification, identifying all OT, IT, and IoT devices, including managed or unmanaged and physical and virtual assets.
ZCR 2.1 Network Segmentation & Security Zones	Industrial networks must be segmented into security zones based on risk levels, ensuring that critical assets are protected.	Armis maps communication flows, helping enforce IEC 62443 zone and conduit principles, detecting unauthorized connections, and supporting segmentation strategies.
ZCR 3.2 Threat Monitoring	Organizations must implement continuous monitoring to detect cyber threats and unauthorized access.	Armis provides AI-driven threat detection, identifying early warning threats, suspicious behaviors, policy violations, and potential breaches in real time.
ZCR 3.3 Intrusion Detection & Response	Industrial systems must have mechanisms for detecting and responding to security intrusions.	Armis detects anomalies and attacks across OT networks and integrates with SIEM/SOAR platforms as well as the entire tech stack for a cooperative and automated response.
ZCR 3.4 Anomaly Detection & Behavioral Analysis	Systems must track normal behavior and detect deviations that may indicate cyber threats.	Armis continuously monitors device behavior, leveraging machine learning and the billions strong proprietary asset intelligence engine to detect deviations from baseline activity and alert on potential threats.

IEC 62443-3-2 Requirement	Description	How Armis helps
ZCR 3.6 Vulnerability Assessment & Management	Security vulnerabilities in industrial systems must be continuously identified, assessed, and mitigated.	Armis performs automated vulnerability assessment, correlating asset risks with known exploits and identifying, deduplicating prioritizing assigning and remediating based on impact and exposure.
ZCR 3.7 Logging & Security Event Analysis	Security-related events must be logged and analyzed to detect potential threats.	Armis logs all asset activities and security events, providing forensic insights and integrating with SIEM platforms for in-depth analysis.
ZCR 3.8 Access Control & Least Privilege Enforcement	Access to critical assets must be restricted based on need-to-know principles.	Armis detects unauthorized access attempts and helps enforce least privilege (Zero Trust) policies by identifying risky asset communication.
DRAR 1 Risk Assessment for Security Zones	Organizations must perform risk assessments to determine security levels for different zones.	Armis continuously evaluates security risks, providing insights into potential threats and vulnerabilities affecting different zones. Microsegmentation can also limit the lateral creep of attacks via east west traffic.
DRAR 2 Risk-Based Security Level Assignment	Each security zone must be assigned an appropriate security level (SL1–SL4) based on risk assessment.	Armis helps organizations determine appropriate security levels by analyzing asset criticality, network exposure, and threat intelligence.
DRAR 12 Incident Response & Recovery Planning	Organizations must develop and maintain an incident response plan.	Armis enhances incident response by providing real-time threat intelligence, forensic insights, and automated remediation recommendations.
ZCR 5.3 Secure Remote Access	Remote access to industrial systems must be controlled and monitored to prevent unauthorized access.	Armis identifies and monitors all remote access sessions, detecting unauthorized connections and ensuring compliance with remote access policies.
ZCR 5.4 Secure Communication Channels	Communication between industrial assets must be protected against interception and tampering.	Armis detects insecure protocols, unauthorized communications, and potential man-in-the-middle attacks, ensuring secure data exchange.

How Armis Assists Organizations With IEC 62443-3-3 Compliance

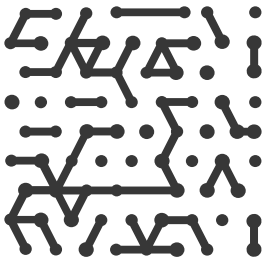
The 62443-3-3 section relates to general systems security requirements, which include authentication, data confidentiality, and system integrity.

IEC 62443-3-3 Requirement	Description	How Armis helps
SR 1.1 Identification & Authentication Control	All users and devices accessing the system must be uniquely identified and authenticated.	Armis continuously monitors asset identities and access behaviors, detecting unauthorized devices and credential misuse.
SR 1.2 Strength of Authentication Mechanisms	Strong authentication mechanisms must be enforced.	Armis detects weak authentication methods, such as shared credentials or default passwords, and flags them for remediation.
SR 1.6 Remote Access Security	Remote access to industrial systems must be controlled and monitored.	Armis detects and analyzes all remote access activity, ensuring compliance with security policies.
SR 1.7 Session Integrity	Session security must be enforced to prevent hijacking and replay attacks.	Armis identifies anomalous session behaviors and flags potential session hijacking attempts.
SR 1.8 Use of Unambiguous Identifiers	Devices and users must be uniquely identifiable.	Armis automatically inventories and assigns unique identifiers to all OT, IT, and IoT assets.
SR 1.9 Strength of Password-Based Authentication	Password security requirements must be enforced.	Armis detects weak credentials and unauthorized login attempts.
SR 1.10 Authenticator Management	Authentication mechanisms must be centrally managed.	Armis integrates with identity management solutions to ensure proper enforcement of authentication policies.

IEC 62443-3-3 Requirement	Description	How Armis helps
SR 1.13 Access Privileges	Least privilege access must be enforced.	Armis detects excessive permissions and improper privilege escalations.
SR 2.1 Authorization Enforcement	Systems must enforce access control policies.	Armis continuously monitors user and device access, identifying policy violations and unauthorized actions.
SR 2.3 Use Control for Network Communications	Access to networked systems must be restricted based on roles.	Armis enforces network segmentation, blocking unauthorized communication flows.
SR 2.4 Mobile Code Security	Mobile code execution must be restricted and monitored.	Armis detects unauthorized script execution and potentially malicious mobile code.
SR 2.8 Auditable Events	Security-related events must be logged and analyzed.	Armis generates detailed logs and integrates with SIEMs & SOARs for event correlation.
SR 2.11 Use of Cryptography	Cryptographic protections must be implemented where required.	Armis detects unencrypted data flows and insecure cryptographic implementations.
SR 2.12 Information Persistence	Sensitive information must be securely stored and accessed.	Armis identifies data at risk, ensuring sensitive information is not exposed in insecure environments.
SR 3.1 Asset Inventory	Organizations must maintain an up-to-date asset inventory.	Armis provides real-time asset discovery and classification, ensuring accurate inventory management.
SR 3.2 Patch Management	Security patches must be applied in a timely manner.	Armis identifies unpatched devices, prioritizing remediation based on risk exposure.
SR 3.3 Security Functionality Verification	Security functions must be regularly tested.	Armis performs continuous security monitoring, identifying misconfigurations and security control failures.
SR 3.4 Use of Secure Communication Protocols	Secure communication protocols must be enforced.	Armis detects unencrypted protocols and ensures secure data exchanges.

IEC 62443-3-3 Requirement	Description	How Armis helps
SR 3.5 Input Validation	Systems must validate input to prevent injection attacks.	Armis detects anomalies in network traffic, identifying potential injection attacks.
SR 3.6 Deterministic Output Processing	Systems must process outputs securely.	Armis monitors industrial control commands, detecting anomalies and potential tampering.
SR 3.7 Error Handling	Systems must manage error conditions securely.	Armis identifies misconfigurations and software errors, helping prevent exploitation.
SR 3.8 Session Termination	Sessions must be terminated securely after use.	With Secure Remote Access, Armis can ensure secure termination of sessions after use.
SR 3.9 Protection Against Replay Attacks	Systems must prevent replay attacks.	Armis detects suspicious repeated request patterns, mitigating replay attack risks.
SR 4.1 Information Confidentiality	Data must be protected from unauthorized access.	With Secure Remote Access, Armis detects unauthorized data access attempts, ensuring compliance with security policies.
SR 4.2 Information Integrity	Data integrity must be maintained.	Armis detects unauthorized modifications and alerts on potential data tampering.
SR 4.3 Information Availability	Systems must ensure availability against cyber threats.	Armis detects DDoS attacks and abnormal traffic patterns, helping maintain system uptime. The solution also validates that security controls and assets are configured properly to prevent such attacks proactively.
SR 5.1 Network Segmentation	Segmentation must prevent unauthorized lateral movement.	Armis maps assets and associated traffic and flags unauthorized connections between zones.
SR 5.2 Zone Boundary Protection	Network perimeters must be secured.	Armis continuously analyzes zone boundaries, detecting policy violations and security gaps.

IEC 62443-3-3 Requirement	Description	How Armis helps
SR 5.3 Public Access Control	Publicly accessible systems must be controlled and monitored.	With Secure Remote Access, Armis ensures that publicly accessible systems can be secured with granular access policies. Furthermore, Armis identifies and monitors publicly exposed assets, reducing attack surfaces.
SR 5.4 Control System Protection from External Networks	Access from external networks must be tightly controlled.	Armis detects external threats, such as unauthorized VPN access or exposed industrial systems.
SR 6.1 Audit Log Availability	Audit logs must be retained and accessible for compliance.	Armis logs all security events, ensuring compliance with IEC 62443 logging requirements.
SR 6.2 Continuous Monitoring	Continuous monitoring of security events is required.	Armis provides real-time security monitoring, identifying threats as they emerge.
SR 7.1 Operational Resilience & Recovery	Systems must be resilient against cyber threats and recover quickly.	Armis is resilient against cyber threats and is hardened platform that can perform backup validation. Additionally, Armis assists in post-incident analysis and recovery, reducing downtime.
SR 7.7 Weakness Identification & Response	Security weaknesses must be identified and remediated.	Armis continuously scans for vulnerabilities and provides risk-based mitigation recommendations.
SR 7.8 Security Updates & Patching	Security patches must be applied consistently.	Armis prioritizes patching based on real-time threat intelligence, reducing exposure.



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:

IEC 62443-4-2 Requirement	Description	How Armis helps
CR 1.1 Identification & Authentication Control	Devices and users must be uniquely identified and authenticated.	Armis provides real-time asset visibility and detects unauthorized devices or anomalous authentication attempts.
CR 1.7 Session Integrity	Sessions must be protected against hijacking and replay attacks.	Armis monitors session behavior and detects replay attacks, session hijacking, and unauthorized access attempts.
CR 1.9 Strength of Password-Based Authentication	Password-based authentication must meet security best practices.	Armis detects weak or default credentials and provides risk-based insights to enforce strong authentication.
CR 1.13 Access Privileges	Access control must follow the principle of least privilege.	Armis continuously analyzes access levels, detecting excessive permissions and unauthorized privilege escalations.
CR 2.8 Auditable Events	Security-relevant events must be logged and reviewed.	Armis generates detailed security logs and integrates with SIEM and SOAR tools to ensure compliance with logging requirements.
CR 3.2 Patch Management	Security patches must be applied and managed effectively.	Armis identifies unpatched vulnerabilities, prioritizes remediation based on risk, and provides patching insights.
CR 3.5 Input Validation	Systems must validate all external inputs to prevent injection attacks.	Armis inspects network traffic and detects anomalous inputs that could indicate injection attacks or data manipulation.

IEC 62443-4-2 Requirement	Description	How Armis helps
CR 3.7 Session Termination	Sessions must be securely terminated after use.	Armis monitors active sessions, detecting and flagging persistent, unauthorized, or abnormal session behavior.
CR 4.1 Information Confidentiality	Sensitive information must be protected from unauthorized access.	Armis detects unencrypted traffic, flags data exfiltration attempts, and ensures data confidentiality.
CR 4.3 Information Availability	Systems must ensure uptime and resilience against cyber threats.	Armis identifies threats such as DDoS attacks, ransomware, or anomalous events that could impact availability.
CR 5.1 Network Segmentation	Network segmentation must prevent unauthorized lateral movement.	Armis maps traffic flows and enforces network segmentation policies to block unauthorized communications.
CR 5.2 Zone Boundary Protection	Systems must secure boundaries between security zones.	Armis detects unauthorized cross-zone traffic, ensuring proper network segmentation and policy enforcement.
CR 5.3 Public Access Control	Systems exposed to public networks must be controlled and monitored.	Armis identifies publicly exposed assets, monitors external access, and mitigates exposure risks.
CR 6.1 Audit Log Availability	Logs must be available for security monitoring and compliance.	Armis provides centralized logging and reporting, ensuring audit logs are accessible and secure.
CR 6.2 Continuous Monitoring	Continuous monitoring of security events is required.	Armis continuously monitors OT, IT, and IoT environments, detecting anomalous behavior and threats in real time.
CR 7.1 Operational Resilience & Recovery	Systems must be resilient against cyberattacks and support recovery.	Armis assists in incident response, providing forensic insights to support rapid recovery.

IEC 62443-4-2 Requirement	Description	How Armis helps
CR 7.7 Weakness Identification & Response	Security weaknesses must be continuously identified and addressed.	Armis performs continuous vulnerability assessments and prioritizes remediation based on risk.
CR 7.8 Security Updates & Patching	Security patches must be consistently applied and verified.	Armis automates vulnerability detection, ensuring timely patching and reducing exposure to exploits.

Armis and IEC 62443 Compliance at Scale

Armis empowers organizations to achieve and maintain compliance with IEC 62443 by providing comprehensive asset visibility, continuous risk assessment, and automated security controls across industrial environments. As cyber threats targeting OT, ICS, and critical infrastructure continue to evolve, Armis enables organizations to align with IEC 62443's rigorous security standards by ensuring:

- **Full Asset Discovery and Inventory** – Identifying and classifying all OT, IT, and IoT assets in real time.
- **Risk-Based Vulnerability Management** – Continuously assessing vulnerabilities and prioritizing remediation efforts based on risk.
- **Segmentation and Access Control** – Enforcing network segmentation and monitoring access to prevent unauthorized communication.
- **Threat Detection and Response** – Detecting anomalous behavior and responding to cyber threats without disrupting operations.
- **Regulatory Alignment** – Supporting IEC 62443 requirements, including security levels, system hardening, and incident response.

Armis ensures that security and compliance efforts do not interfere with critical operations. By automating compliance workflows and delivering actionable insights, Armis helps organizations scale their cyber resilience strategy, ensuring they meet IEC 62443 requirements while safeguarding their industrial environments against modern cyber exposure threats.