



Map Every Single Functional Requirement in IEC 62443-3-3

A guide to secure your ICS / OT environments — the compliant way



TABLE OF CONTENTS

Overview..... 3

Building a Resilient Foundation: Your Guide to ISA/IEC 62443 4

ISA/IEC-62443-3 Foundational Requirements 7

- ◆ FR1: Identification and Authentication Control (IAC)7
- ◆ FR2: Use Control (UC).....9
- ◆ FR3: System Integrity (SI)..... 11
- ◆ FR4: Data Confidentiality (DC) 132
- ◆ FR5: Restricted Data Flow (RDF)..... 143
- ◆ FR6: Timely Response to Events (TRE) 155
- ◆ FR7: Resource Availability (RA)..... 16



Overview

The ISA/IEC 62443 series of standards define requirements and processes for implementing and maintaining electronically secure Industrial Automation and Control Systems (IACS). The scope of the ISA/IEC 62443 Series is the Security of Industrial Automation and Control Systems.

An IACS is defined as a:

“Collection of personnel, hardware, software, and policies involved in the operation of the industrial process and that can affect or influence its safe, secure, and reliable operation”.



The standards were developed to establish best practices and provide a way to evaluate the IACS security performance. Organizations can use it to assess existing and potential threats within the industrial environment and take the necessary corrective actions to reduce the overall cyber risk. The standard consists of 13 documents divided into four groups:

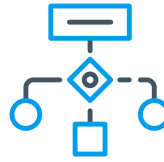
▼
General



▼
Policies



▼
Procedures



▼
System & Component



This document focuses on the ISA/IEC 62443-3-3 and the Functional Requirements (FR) — and explains how the Forescout platform helps organizations implement the standard and establish the necessary controls to monitor and ensure compliance.

Building a Resilient Foundation: Your Guide to ISA/IEC 62443-3-3

When it comes to protecting IACS, the ISA/IEC 62443 series isn't just a set of rules. It is a comprehensive, methodological approach to security that you can adapt to your organization's needs. Rather than rigid guidelines, this standard offers a flexible framework. Learn from each principle and apply them where it truly benefits your operation. Meet compliance requirements and build a security foundation designed to adapt as your organization grows — and as threats evolve. Explore the core concepts of ISA/IEC 62443 and how they can elevate your security strategy.



Cybersecurity as an Ongoing Commitment

Imagine cybersecurity as a continuous journey, where establishing policies is only the beginning. In a world where threats are constantly evolving, staying secure requires an adaptable mindset. By establishing clear KPIs, your organization gains real-time insights into the effectiveness of its security measures, helping you pinpoint areas for improvement and stay agile as new risks appear. Think of monitoring as your organization's 'pulse check' showing you where to adjust and strengthen security practice to stay ahead.



Layered Protection: Defense-in-Depth

In cybersecurity, putting all your defenses in a single layer is a bad move. Defense-in-Depth involves creating multiple layers of security so that if one layer is breached, others are ready to protect critical assets. Think of it as setting up checkpoints at every level of your operations. For example, in a factory setting, a firewall may block unauthorized access to control systems while deep packet inspection (DPI) monitors network traffic, and granular access control policies restrict users based on need. This layered approach minimizes potential impacts, ensuring continuity to maintain security.



Structuring Your Security: Zones & Conduits

Consider Zones & Conduits as the blueprint for managing your IACS environment. Zones group components with similar security requirements and make it easier to apply targeted protections. Conduits act as controlled 'corridors' that regulate data flow between these zones. By segmenting in this way, you create barriers that isolate critical assets —making it easier to detect anomalies and contain security events. For example, using zones helps isolate vulnerable devices in industrial environments where patching can be challenging. Zones add a level of protection where direct fixes may not be feasible.



Matching Defenses to Risks: Security Assurance Levels

Security Assurance Levels (SALs) help you align defenses with specific threats. From basic to advanced, SALs let you ensure each system has the right level of protection. For instance, a high-exposure area may need stringent controls; Lower-risk zones may only need standard protections. By tailoring your protection, you can allocate resources strategically and prioritize areas with the greatest risk. For example, Forescout customers can integrate threat intelligence feeds to better contextualize the risk and apply the right level of protection.

LEVEL	DESCRIPTION	TARGET	SKILLS	MOTIVATION	MEANS
SL1	Protection against casual or accidental violation.	Misconfiguration	Simple or none	None	Nonintentional
SL2	Protection against intentional violation using simple means with low resources, general skills and low motivation.	No security measures in place	Basic	Low	Simple
SL3	Protection against intentional violation using sophisticated tools with limited resources, IACS-specific skills, and moderate motivation.	Moderate security measures	Moderate, IACS-specific	Medium	Sophisticated
SL4	Protection against intentional violations using sophisticated means with extended resources, IACS-specific skills, and high motivation.	Economical or reputational damage	High, IACS-specific	High	Advanced



Managing Access with Precision

In IACS environments, access control goes well beyond password management. Here, it is about ensuring that every user has the appropriate level of access. Nothing more. Through role-based access controls, you can restrict users to only the systems they need. For example, an operator may have permission to monitor systems but not make changes while an administrator has full access. This principle of 'least privilege' minimizes the risk of unintended or unauthorized changes. Furthermore, access is often coupled with layered authentication modes to enhance security as the access level increases.



Protecting Data at Every Stage

In IACS environments, data security is about maintaining the integrity and flow of information in a controlled way. Whether data is stored or in transit, protecting it is essential to keeping operations running smoothly. Imagine handling each piece of data like a valuable asset where only authorized individuals can access or modify it. This protection goes beyond encryption and confidentiality; it involves monitoring access and data pathways to detect and prevent unauthorized usage. For instance, by knowing how your sensitive data should be handled, your organization can better spot and prevent data exfiltration attempts.



Comprehensive Risk Assessment for Industrial Environments

Risk assessments are all about understanding the broader impact on your operation. The IEC 62443 standard guides you through assessing risks across production continuity, safety, and environmental impact. This comprehensive view is essential to prioritizing actions that protect your organization's mission — not just your systems. In industrial and operational settings, understanding risk is particularly challenging, but aligning security efforts with these specific risks helps build a more resilient operation.



Measuring and Maturing Your Security Practices

Based on the [Capability Maturity Model Integration](#) (CMMI), security maturity levels help you assess how deeply security practices are embedded within your organization. These levels range from ad-hoc to fully optimized. They give you a structured way to measure and improve your security posture. This process leaves little room for interpretation and will help you calibrate efforts and investments effectively. By understanding your maturity level, you can chart a clear path for enhancing security, allowing for consistent application and strengthening of practices over time.

LEVEL	CATEGORY	DESCRIPTION
ML1	Initial	Product suppliers usually carry out product development ad hoc and often undocumented (or not fully documented).
ML2	Managed	The product supplier is able to manage the development of a product according to written guidelines. It must be demonstrated that the personnel who carry out the process have the appropriate expertise, are trained and/or follow written procedures. The processes are repeatable.
ML3	Defined	The process is repeatable throughout the supplier's organization. The processes have been practiced and there is evidence that this has been done.
ML4	Improved	Product suppliers use appropriate process metrics to monitor the effectiveness and performance of the process and demonstrate continuous improvement in these areas.



Compensating Controls: Bridging the Gaps

In some cases, ideal security measures may not be available for every system. Compensating controls let you meet essential requirements with alternative solutions. For example, if a device lacks a critical security feature, then a firewall rule could mitigate the vulnerability. These measures can provide quick wins to close security gaps — as long as you have the tools to manage and monitor policies effectively. This approach helps your organization move from a reactive to a proactive defense to reinforce resilience. Keep in mind, however, that a certain level of automation is needed. This isn't feasible manually.

ISA/IEC-62443-3 Foundational Requirements

FOUNDATIONAL REQUIREMENTS	ASSOCIATE PROCESS
♦ FR1 - Identification and Authentication Control (IAC)	User authentication and authorization
♦ FR2 - Use Control (UC)	Enforcement of roles and responsibilities
♦ FR3 - System Integrity (SI)	Change management
♦ FR4 - Data Confidentiality (DC)	Use of encryption
♦ FR5 - Restricted Data Flow (RDF)	Network segmentation
♦ FR6 - Timely Response to Events (TRE)	Audit logs
♦ FR7 - Resource Availability (RA)	System backup and recovery

FR1: Identification and Authentication Control (IAC)

The goal here is straightforward: Ensure every user, application, and device are properly identified and verified before accessing your IACS resources. This process starts with a clear, organized list of users and access protocols tailored to the security needs of each zone. To fully secure access, you'll want the flexibility to define users and policies with precision and integrate with third-party tools to support robust verification measures, allowing only trusted entities to reach your critical systems. This approach reduces the risk of unauthorized access, giving you confidence that your environment is protected.

How Forescout Helps You Meet IEC 62443 IAC Goals

Meeting IEC 62443 requirements means managing access control and authentication across users, devices, and applications. Every device – whether managed, unmanaged, or third-party – must be authenticated before it touches your industrial network. Forescout makes this possible by allowing you to create, test, and enforce policies from a single, centralized platform that integrates seamlessly with your existing IT and security infrastructure. Forescout enforces zero-trust policies rooted in least privilege, ensuring that each device has access only to what it truly needs — no more, no less. This applies across all networks — wired, wireless, and VPN. With Forescout, you have one solution to manage IT, OT, and IoT assets to reinforce your security posture, stay proactive, and maintain complete control over everything accessing your environment.

FR1 is further broken down into 14 sub-levels as “Component Requirements (CR)” outlined in the table below:

CR	DESCRIPTION	HOW FORESCOUT COMPLIES
CR 1.1 User Identification and Authentication	Capability to identify and authenticate all human users. Common user identification and authentication may be accepted.	With Forescout, you gain real-time visibility into the identity and role of every user and device, along with configurations, security status, and risk profiles. This visibility equips you to enforce strong authentication controls across all devices, users, and applications accessing your ICS resources, ensuring that only trusted entities meet your security standards.
CR 1.1 (i)	Unique identification and authentication	
CR 1.1 (ii)	Multifactor authentication for all interfaces	
CR 1.2 Software process and device	Capability to identify itself and authenticate with any other components.	

CR	DESCRIPTION	HOW FORESCOUT COMPLIES
identification and authentication		
CR 1.2 (i)	Unique identification and authentication with other components.	We help you implement comprehensive identity management across IT, IoT, OT, and IoMT networks. Using protocols like 802.1X and RADIUS and integrating with third-party authentication systems, you can validate identities through multiple methods, granting network access based on roles and security requirements across all network types.
CR 1.3 - Account management	Capability to integrate into a system that supports the management of all devices connected in system.	
CR 1.4 - Identifier management	Capability to integrate into a system that supports the management of identifiers.	You'll find managing authentication is straightforward. From third-party identity tools to hardware-based methods, we support diverse authentication needs, including wireless networks. You can monitor and log remote access attempts across OT and IT protocols like HTTP, FTP, SMB, and Telnet, capturing failed <i>and</i> successful authentications.
CR 1.5 - Authenticator management	Capability to support the use of initial authenticator content, support changes to default authenticators and protect unauthorized disclosure and modification when stored, used and transmitted.	To keep your systems secure, real-time alerts notify you of any risky authentication attempts, such as the use of default or weak credentials (like admin/admin) or brute-force attempts, ensuring your critical systems are protected and all access remains accountable.
CR 1.5 (i)	Authentication using hardware mechanisms.	
CR 1.6 - Wireless access management	It should be possible to identify and authenticate all users of wireless communication.	
CR 1.7 - Strength of password-based authentication	Capability to enforce configurable password strength.	Effortlessly integrating with your directory systems (such as AD) or third-party solutions, we make enforcing and managing password policies across your environment simple and immediate.
CR 1.7 (i)	Restrictions on use of old passwords. Enforce password minimum and maximum lifetime restrictions for human users.	With everything pre-configured, you can dive into robust password management without delay. Our platform actively identifies weak security practices, like default or insecure credentials (e.g., admin/admin) and brute-force attempts, monitoring these across OT and IT protocols, including HTTP, FTP, SMB, and Telnet.
CR 1.7 (ii)	Password minimum and maximum lifetime restrictions for all users.	You also have the flexibility to tailor the solution to meet your unique requirements. Set up additional checks for weak credentials (based on length and character variety), prevent password reuse, enforce expiration policies, and address other critical scenarios to keep password management strong, adaptable, and aligned with your organization's needs.
CR 1.8 - Public Key Infrastructure (PKI) certificates	Component shall have the capability to operate within the scope of the PKI.	Integrating with a variety of third-party authentication systems, we support diverse authentication mechanisms to validate unique identities and users before granting network access.
CR 1.9 - Strength of public key authentication	Capability to validate certificates.	Our platform lets you perform comprehensive checks on TLS/SSL communications and certificates to ensure secure information exchange.
CR 1.9 (i)	ISO/IEC 19790 Level 3 security for public key authentication.	This gives you the ability to verify certificate validity dates, assess the trustworthiness of certificate authorities, evaluate SSL client applications, and confirm the strength of the cipher suite.
CR 1.9 (ii)	ISO/IEC 19790 Level 4 security for public key authentication.	
CR 1.10 - Authenticator feedback	Capability to obscure feedback of authentication information.	You can tailor these checks to ensure that encrypted communications and certificates align with recognized best practices and your company's policies.
CR 1.11 – Unsuccessful login attempts	Capability to limit the number of consecutive invalid access.	
CR 1.12 - System use notification	Capability to display a system use notification message (Warnings, system use policy etc.) before authenticating.	Our platform gives you the option to display a message about system usage before authentication—such as warnings or usage guidelines. You can customize these messages to align with your company's policies, ensuring users are fully informed of their responsibilities before accessing the system.
CR 1.13 - Access via untrusted networks	Monitor and control all methods of access from untrusted networks.	

CR	DESCRIPTION	HOW FORESCOUT COMPLIES
CR 1.13 RE 1 - Explicit access request approval	Monitor and terminate remote sessions.	With our platform, you can continuously monitor network traffic and visualize device access and communication through an interactive network map. This dynamic tool lets you easily examine and analyze device behavior and information flow across your network. It also automatically generates a baseline of active communication, displayed as intuitive access rules. Using this interactive view, you can quickly detect unauthorized access to devices or the network, with details on who accessed what and through which protocol. Once you review and approve the generated baseline, it becomes your network's allow-list, triggering real-time alerts for any access violations or anomalies.
CR 1.14 - Strength of symmetric key authentication	Ensure that the algorithms and keys used for the symmetric key authentication comply with CR 4.3	We make tracking accounts and managing access permissions simple and flexible, allowing you to handle identifiers by user, group, role, or control system interface. Identification can be customized to be role-based, group-based, or device-based, giving you precise control over who has access to what, exactly as needed for your security requirements.
CR 1.14 (i)	Hardware security for symmetric keys-based authentication.	The Forescout platform supports this requirement through integration with third-party solutions.

FR2: Use Control (UC)

Securing your IAC is about managing what each user, device, or application can do once they're inside. Use Control (UC) empowers you to set precise permissions ensuring that every entity operates strictly within its designated role and security level. This requires strong authentication measures, a clear role-based access framework, and continuous monitoring to detect and address any inconsistencies or risks.

How Forescout Help You Meet IEC 62443 UC Goals

Our solution supports robust access control, so you can enforce multi-factor authentication (MFA) and integrate third-party tools to create role-based access (RBAC) tailored to each user or device. This approach includes segmenting your network and managing access control lists which is crucial for preventing unauthorized movement and securing each layer of your environment. Beyond setting access permissions, we provide ongoing monitoring to detect any irregularities, such as unauthorized access attempts, unapproved software installations, or configuration changes that could compromise critical systems. You gain real-time visibility into sensitive areas, so you can quickly address potential issues and mitigate risks. When irregularities arise, you have the flexibility to take immediate action. Isolate devices or terminate sessions to contain threats across wired or wireless networks – locally or remotely – instantly.

For compliance, we support workflows for regular access reviews and maintain a detailed audit trail of user actions to make it easy to track activity, conduct security analyses, and meet regulatory requirements. These combined capabilities give you full control over your environment, so you can confidently meet IEC 62443-3-3 goals.

The FR2 is further subdivided (13 sublevels) as “Component Requirements (CR)” outlined in the table below:

CR	DESCRIPTION	HOW FORESCOUT COMPLIES
CR 2.1 - Authorization enforcement	Authorization enforcement mechanism for all human users based on their assigned responsibilities.	Forescout lets you establish granular RBAC policies, so you can precisely manage and limit who has access to the information collected by the platform. This level of control

CR	DESCRIPTION	HOW FORESCOUT COMPLIES
RE 2.1 (i)	Authorization enforcement for all users.	applies to locally authenticated users <i>and</i> those authenticated through external systems, such as LDAP or Active Directory (AD).
RE 2.1 (ii)	Permission mapping to roles.	
RE 2.1 (iii)	Supervisor override: Component shall support a supervisor manual override.	
RE 2.1 (iv)	Dual approval: Component shall support dual approval when action can result in serious impact on the industrial process.	The Forescout platform meets this requirement by integrating with third-party solutions.
CR 2.2 - Wireless use control	If a component supports usage through wireless interfaces, it shall provide the capability to authorize, monitor and enforce usage restrictions according to commonly accepted industry practices.	Forescout enforces flexible controls, including usage restrictions, across wired, wireless, and VPN infrastructure—whether or not 802.1X is in place.
CR 2.3 - Use control for portable and mobile devices	If a component utilizes portable and mobile devices, it shall provide the capability to automatically enforce configurable usage restrictions that including context specific authorization, restricting code and data transfer to/from portable and mobile devices.	Forescout integrates with a wide range of Mobile Device Management (MDM) solutions, providing comprehensive insights into each device's user, configuration, apps, and security posture. This allows the platform to enforce more granular network access and endpoint integrity policies specifically for mobile devices.
CR 2.4 - Mobile code	The mobile code requirements are component specific and can be located as requirements for each specific device type in Cl. 4.3.2.9 through 4.3.2.12	This requirement applies to IACS developers.
CR 2.5 - Session lock	If a component provides an HMI, a session lock should be configurable.	This requirement applies to IACS developers.
CR 2.6 - Remote session termination	Capability to terminate a remote session either automatically after a configurable time period of inactivity or manually by the user who initiated the session.	Our platform can be configured to monitor and detect inactive connections, generate alerts, and notify third-party solutions to terminate remote sessions, ensuring a secure and efficient network environment.
CR 2.7 - Concurrent sessions control	Capability to limit the number of concurrent sessions per interface for any given user (human, software process or device).	Forescout can be configured to monitor network connections, detecting and alerting on concurrent sessions per interface to enhance oversight and control.
CR 2.8 -Auditable events	The component shall provide the capability to generate audit records relevant to security.	Forescout continuously monitors network and device activity in real-time, capturing and logging key events such as unauthorized access attempts, communication attempts, failed and successful remote logins, field device errors, notable control system events (like maintenance operations), and ICS device configuration changes (such as program and firmware updates).
CR 2.9 - Audit storage capacity	Capability of component to allocate audit record storage capacity and to protect failure of component when it reaches or exceeds the audit storage capacity.	
RE 2.9 (i)	Warn when audit record storage capacity threshold reached.	
CR 2.10 - Response to audit processing failures	Capability of component to protect against the loss of essential services and functions in the event of an audit processing failure and to support appropriate actions in response to an audit processing failure.	This requirement applies to IACS developers.
CR 2.11 - Timestamps	Capability to create timestamps (including date and time) for use in audit records.	Users can configure the platform to synchronize internal system clocks with an authoritative time server and/or redundant time sources, with safeguards to protect their integrity. Audit records generated by Forescout include precise timestamps from the internal system clock, capturing date <i>and</i> time for complete accuracy.
RE 2.11 (i)	Time synchronization.	
RE 2.11 (ii)	Protection of time source integrity.	
CR 2.12 - Non-repudiation	Component shall provide the capability to determine whether a given human user took a particular action.	The system monitors and logs user activity related to configuration changes, such as the creation, modification, or deletion of detection parameters, ensuring data integrity and supporting non-repudiation.
RE 2.12 (i)	Non-repudiation for all users.	

CR	DESCRIPTION	HOW FORESCOUT COMPLIES
CR 2.13 Use of physical diagnostic and test interfaces	The use of physical diagnostic and test interfaces.	This requirement applies to IACS developers.

FR3: System Integrity (SI)

System Integrity within IACS includes the protection of all components (hardware, software, firmware, and data) from unauthorized changes that could compromise industrial processes. This requirement is critical for protecting operational continuity and ensuring that vital workflows remain resilient against threats. Achieving system integrity means managing changes effectively, detecting potential threats promptly, and recovering swiftly from critical events to maintain business continuity.

How Forescout Helps You Meet IEC 62443 SI Goals

Forescout enables organizations to maintain system integrity by establishing and maintaining baseline configurations for all components and actively monitoring for deviations. Our platform supports structured change management processes and ensures that changes are approved, tested, and documented in line with your security policies.

For patch management, we help security teams to prioritize vulnerabilities, apply updates, or implement compensating controls for non-patchable systems. Continuous monitoring of your industrial environment detects anomalies and signs of compromise by using DPI for more than 350 protocols in IT, OT, IoT, and IoMT. This includes analyzing traffic load, syntax and content to detect advanced threats, such as malware, zero-day exploits, malformed traffic, and unwanted behavior.

Forescout's baselining and configuration management tools provide a detailed, historical record of your IACS setup. In the event of data corruption, unexpected events, or a cyber-attack, you can verify system integrity and restore operations to their original state. This comprehensive approach ensures that your environment remains reliable, secure, and compliant with IEC 62443 standards.

The FR 3 is further subdivided (14 sublevels) as as "Component Requirements (CR)" outlined in the table below:

CR	DESCRIPTION	HOW FORESCOUT COMPLIES
CR 3.1 - Communication integrity	Capability to protect integrity of transmitted information.	Our users gain the tools to monitor and manage access to sensitive or confidential data, whether it's stored or being transferred. With full visibility into network access and data flow, it's easy to spot unauthorized connections, changes, and data exfiltration attempts. This is particularly crucial in ICS environments, where robust authentication and data protection mechanisms may be lacking.
CR 3.1 (i)	Communication authentication.	
CR 3.2 - Malicious code protection	Prevent malicious code executions on network level.	We combine threat intelligence with signature-based <i>and</i> anomaly-based detection to identify and report known and unknown malware and exploit attempts in real time. Malicious activity is detected at the earliest stages, during reconnaissance and propagations of threats are stopped before they can escalate. Our alerts provide clear event classifications and actionable insights into the threat's source, target, and nature, empowering you to respond immediately and prevent the attack from progressing.

CR	DESCRIPTION	HOW FORESCOUT COMPLIES
CR 3.2 RE 1 - Malicious code protection on entry and exit points	Prevent malicious code executions on host level.	We actively identify and address malicious or high-risk endpoints, reducing the risk of data breaches and malware attacks that could jeopardize your organization. The platform also provides the flexibility to take action, either manually or fully automated, to isolate or remediate compromised hosts, ensuring threats are contained swiftly.
CR 3.3 - Security functionality verification	Capability to support verification of the intended operation of security functions accordingly.	The Forescout platform proactively verifies that essential security components are properly configured and fully operational, reinforcing your overall security (firewalls, switches, log collectors, access controls backup solutions, etc.).
CR 3.3 (i)	Security functionality verification during normal operation.	
CR 3.4 - Software and information integrity	Capability to perform or support integrity checks.	We detect deviations from your software baseline or integrity in real time. This baseline can include critical details like device OS, software or firmware inventory, registry keys, shared and encrypted folders, and more. Once the baseline is established, the platform continuously monitors and generates alerts for any changes, such as OS or firmware updates, application additions or removals, registry modifications, user or role changes, and other key integrity indicators.
CR 3.4 (i)	Capability to perform or support authenticity checks of software and information.	
CR 3.4 (ii)	Automated notification of integrity violations.	
CR 3.5 - Input validation	Capability to validate the syntax, length and content of any input.	Our platform provides comprehensive DPI for industrial protocol communications, ensuring the validity of process control messages through a two-step verification process. First, it verifies that each message aligns with protocol specifications, checking for correct syntax. Next, it performs a deeper validation to confirm that the message content is appropriate and expected for the specific process. If either check fails, real-time alerts are generated, offering detailed information for rapid analysis and response.
CR 3.6 - Deterministic output	Capability to set outputs to a predetermined state.	This requirement applies to IACS developers.
CR 3.7 - Error handling	Capability to identify and handle error conditions.	Our platform continuously monitors ICS devices and control systems, detecting error conditions and malfunction indicators, such as failed request processing, corrupted configurations, or unexpected restarts. Each sensor reports this information to you in real time, enabling you to correlate these events with other network activity that may have triggered the issue. This ensures timely troubleshooting and response with minimal effort, empowering you to perform effective predictive maintenance and keep systems running smoothly.
CR 3.8 - Session integrity	Capability to protect the authenticity of communications sessions including Invalidate session identifiers upon user logout, generate a unique session identifier for each session.	We monitor communications and session identifiers to maintain session integrity, ensuring that each session is secure and properly managed. The platform supports network access control by allowing unique session IDs and configurable expiration times for user credentials, enhancing security across sessions.
CR 3.8 (i)	Invalidation of session IDs after session termination.	
CR 3.8 (ii)	Unique session ID generation.	
CR 3.9 - Protection of audit information	Capability to protect audit information and audit.	Our platform allows you to restrict the modification or deletion of generated logs by setting specific access and management rights for different user profiles, ensuring that log integrity is maintained and only authorized users have control.
CR 3.9 (i)	Audit records on write-once media.	We support this requirement by seamlessly integrating with third-party solutions, enhancing compatibility and expanding functionality across your security ecosystem.

CR	DESCRIPTION	HOW FORESCOUT COMPLIES
CR 3.10 - Support for updates	Support for update requirements are component specific and can be located as requirements for each specific device type in Clauses 4.3.2.9 through 4.3.2.12	This requirement applies to IACS developers.
CR 3.11 - Physical tamper resistance and detection	Physical tamper resistance and detection requirements are component specific and can be located as requirements for each specific device type in Clauses 4.3.2.9 through 4.3.2.12	This requirement applies to IACS developers.
CR 3.12 - Provisioning product supplier root of trust	Provisioning product supplier root of trust requirements are component specific and can be located as requirements for each specific device type in Clauses 4.3.2.9 through 4.3.2.12	This requirement applies to IACS developers.

FR4: Data Confidentiality (DC)

Protecting the confidentiality of sensitive information within IACS is essential for maintaining data integrity and adherence to internal policies. This ensures secure operational workflows by preventing unauthorized access and protecting stored and transmitted data.

How Forescout Helps You Meet IEC 62443 DC Goals

Forescout ensures sensitive information is protected at every stage by securing access, managing communications, and restricting data flow to authorized connections. The platform enforces strict access policies, validates the use of secure protocols— and continuously monitors for unauthorized attempts to access or transfer data. It delivers real-time alerts for immediate response. Our platform takes data leakage prevention further by monitoring or automatically blocking unauthorized USB devices, such as external drives and smartphones — and notifies users of access restrictions. These controls ensure that sensitive data remains secure, preventing unauthorized modifications or transfers.

Forescout monitors communication patterns to detect connections to malicious servers, botnets, or blacklisted IPs by using advanced threat intelligence. This capability mitigates external threats, fortifies data security, and enhances the overall protection of sensitive information. With continuous monitoring and comprehensive insights, Forescout helps organizations protect critical operational data, ensuring alignment with internal security policies and supporting industrial resilience.

The FR 4 is further subdivided (3 sublevels) as “Component Requirements (CR)” as shown in the following table:

CR	DESCRIPTION	HOW FORESCOUT COMPLIES
CR 4.1 - Information confidentiality	Capability to protect the confidentiality of information.	The platform allows you to verify that sensitive information is being transmitted over secure, encrypted protocols and cipher suites. This verification can be performed in several ways: Using the interactive network map and automatically generated communications baseline, you can easily identify critical control systems and servers to determine if their communications with other critical devices are encrypted. Using the integrated Industrial Threat Library (ITL), you receive real-time alerts when insecure protocols are used to exchange sensitive information. These alerts include details about source and destination devices, allowing you to take remedial action, such as disabling insecure versions of SSL on the host. Additionally, the ITL warns you when weak cipher suites or encryption keys are in use by network devices.

CR	DESCRIPTION	HOW FORESCOUT COMPLIES
CR 4.2 - Information persistence	Capability to erase all information when released from active service and/or decommissioned.	This requirement applies to IACS developers.
CR 4.2 (i)	Capability to protect against unauthorized and unintended information transfer via volatile shared memory resources.	Using custom or predefined policies, Forescout can detect and block unauthorized USB mass storage devices—such as memory sticks, external storage devices, smartphones, and cameras—when connected to Windows endpoints. Additionally, it can automatically notify users on Windows endpoints that USB connections are not permitted.
CR 4.3 - Use of cryptography	Cryptographic security mechanisms shall be according to internationally recognized and proven security practices and recommendations.	Our platform includes several built-in controls to ensure that encrypted communications within the monitored network adhere to recognized security practices. It alerts you if insecure protocols or protocol versions, such as SSHv1 or SSLv2, are being used. Additionally, it detects weak cipher suites or encryption keys in TLS/SSL communications, identifies when TLS/SSL certificates are issued by untrustworthy certificate authorities, and flags network devices using client applications linked to known malware or exploit kits.

FR5: Restricted Data Flow (RDF)

Restricted Data Flow is about controlling how information moves between zones, networks, and boundaries to minimize risk. By identifying and applying appropriate methods and controls based on risk analysis and exposure, asset owners can ensure secure communication, maintain compliance, and support operational continuity.

How Forescout Helps You Meet IEC 62443 RDF Goals

Forescout enables organizations to simplify and strengthen network segmentation across diverse IT and OT asset environments, as well as enterprise and industrial domains. Our platform accelerates zero-trust segmentation by providing immediate visibility into communication patterns and enabling dynamic policy enforcement across multi-vendor network environments.

Forescout ensures comprehensive and adaptable protection tailored to your operational needs through seamless integration with existing ecosystems. During the design phase, Forescout automatically maps all active IP-connected devices and their traffic flows. This visualization helps organizations identify logical zones, risk-based boundaries and conduits with precision. The interactive network map provides detailed insights into user, application, and device communications, so you can define segmentation policies that align with business operations and security requirements.

In the enforcement phase, Forescout integrates with existing network ecosystems, such as firewalls and other security tools to apply segmentation policies dynamically — to safeguard authorized communication between zones. The platform continuously enforces controls to reduce the attack surface and maintain compliance. When violations or unauthorized communication attempts are detected, real-time alerts provide actionable insights for swift response. Forescout creates and enforces precise segmentation policies by using device profiles and system baselines to control traffic flows categorized by users, applications, devices, and risk levels. Our platform helps organizations reduce risks, maintain compliance, and ensure operational resilience with continuous monitoring and actionable insights.

The FR 5 is further subdivided (4 sub-levels) as “Component Requirements (CR)” outlined in the following table:

CR	DESCRIPTION	HOW FORESCOUT COMPLIES
CR 5.1 - Network segmentation	Network segmentation and Zoning.	The platform plays a crucial role in various phases of the network segmentation process. During the design phase, it automatically generates an accurate visualization of all active IP-connected network devices and traffic flows, making it easier to identify security perimeters, access points, and groups of functionally or logically related devices. The interactive network map allows users to better understand network operations and define risk-based zones and conduits visually. When it comes to enforcement, the platform aids in implementing network segmentation, ensuring that no unauthorized communication or information flow occurs. If any violations are detected, real-time alerts are immediately issued.
CR 5.1 (i)	Network segments should be physically isolated so that control-system network and non-control system network traffic do not mix.	Forescout accelerates zero-trust segmentation across IT and OT environments by using device profiles and control system baselines to create granular policies. With this approach, your security teams gain immediate visibility into the IT-OT segmentation status of any device, anywhere within the extended ICS environment. The platform enables you to visualize traffic flows through a logical taxonomy of users, applications, services, functions, locations, devices, and risk levels. This comprehensive visibility helps reduce the attack surface and maintain compliance through dynamic segmentation across IT, IoT, and OT networks.
CR 5.2 - Zone boundary protection	The zone boundary protection requirements are network component specific and can be located as requirements for network devices later in Clause 4.3.2.12	
CR 5.2 (i)	Network devices should be set up so that traffic is denied by default and allowed by exception.	
CR 5.2 (ii)	Capability to isolate itself from other networks to reduce the risk of being compromised when an attack is detected.	
CR 5.3 - General purpose person-to-person communication restrictions	The general-purpose person-to-person communication restriction requirements are network component specific and can be located as requirements for network devices later in Clause 4.3.2.12	
CR 5.4 - Application partitioning	Control applications should be partitioned based on criticality to implement a zoning model.	Forescout offers detailed visibility into the services utilized by each device, enabling organizations to define appropriate zones and conduits during the design phase, tailored to device functionality. This capability extends to enforcement where the platform validates services and communications in real time. If policy violations or unauthorized services are detected, immediate alerts provide actionable insights for swift remediation.

FR6: Timely Response to Events (TRE)

Timely Response to Events (TRE) ensures organizations have established policies and procedures to address cyber incidents swiftly and efficiently. It emphasizes the importance of taking prompt response actions to minimize the impact of security events *and* ensure that comprehensive incident data is collected for analysis.

How Forescout Helps You Meet IEC 62443 TRE Goals

Forescout enables organizations to maintain timely responses to security incidents by providing complete visibility into OT/ICS device activity through real-time DPI of all industrial network protocols. Our platform identifies potential vulnerabilities and misconfigurations before they escalate, reducing the risk of downtime and security breaches. By continuously monitoring operational *and* IT environments, our real-time alerts give your security team the insights they need to address critical issues quickly.

Forescout empowers teams to efficiently handle incidents from detection through resolution by automatically collecting incident data and managing through integrated case management tools. The platform tracks asset

lifecycle events, such as changes in risk posture to provide a comprehensive timeline of each asset's status and activity. This visibility reinforces the ability to identify evolving threats and react accordingly.

Forescout also allows organizations to store incident data for a configurable period (90 days by default) to ensure historical data is available for thorough post-event analysis. Detailed event logs and actionable insights can be shared with third-party applications such as SIEM tools for deeper correlation and reporting. Streamline the analysis process and help your team make informed, data-driven decisions faster.

The FR 6 is further subdivided (2 sub-levels) as “Component Requirements (CR)” shown below:

CR	DESCRIPTION	HOW FORESCOUT COMPLIES
CR 6.1 - Audit log accessibility	Capability for authorized humans and/or tools to access audit logs on a read only basis.	Forescout enables asset owners to create and retain system audit logs for a configurable period (default: 90 days), supporting the analysis, investigation, and reporting of dangerous or unauthorized system activity. These logs can also be shared with third-party applications, such as SIEM, for further analysis and correlation.
CR 6.1 (i)	Programmatic access to audit.	
CR 6.2 - Continuous monitoring	Capability to be continuously monitored to detect, characterize and report security breaches in a timely manner.	The platform employs continuous network security monitoring technology specifically designed to detect a wide range of events across IT, IoT, OT networks, and building automation systems (BAS) in real time. By utilizing a combination of hybrid techniques—such as user-defined threat profiles, anomaly detection, queries, and rule-based analysis—the platform can automatically detect and profile security, operational, anomaly, and network-related events. For each detected event, Forescout provides actionable insights, including event type, category, description, severity, possible causes, and mitigation recommendations, along with TTPs information from MITRE ATT&CK.

FR7: Resource Availability (RA)

Ensuring that critical systems remain operational during cyberattacks or disruptions is essential to business continuity. The Resource Availability (RA) requirement specifies the need to maintain system functionality even in the event of a denial-of-service attack or other disruptions. Resource availability ensures that systems continue to operate in degraded modes without compromising safety, compliance, or productivity.

How Forescout Helps You Meet IEC 62443 RA Goals

Forescout helps organizations protect vital operations by delivering real-time visibility into all devices, traffic, and asset configurations across IT and OT environments. With secure access control enforcement and device health monitoring, we establish that only authorized devices interact with your critical infrastructure to reduce risk exposure. The platform continuously tracks baseline configurations. It alerts teams to any deviations that could signal vulnerabilities or security gaps. Be reassured that potential issues are detected and addressed before they cause disruptions, enabling uninterrupted operations.

In addition, Forescout's real-time response capabilities help mitigate risks by automatically isolating non-compliant devices and blocking unauthorized communications. Critical systems remain protected during security incidents. This approach strengthens resilience and gives peace of mind, knowing that your industrial environment can withstand and recover from cyber threats.

The FR 7 is further subdivided (8 sublevels) as “Component Requirements (CR)” shown below:

CR	DESCRIPTION	HOW FORESCOUT COMPLIES
CR 7.1 - Denial of service protection	Capability to maintain essential functions in a degraded mode as the result of a DoS event.	This requirement applies to IACS developers.
CR 7.2 - Resource management	Capability to limit the use of resources by security functions.	The Forescout platform supports role-based access control policies to restrict access to resources based on user, device type, and security posture.
CR 7.3 - Control system backup	Capability to participate in system level backup operations.	Forescout allows security teams to take a snapshot of the monitored system, which contains detailed information about the configuration and interaction of ICS systems and components. This data is particularly useful for verifying the configuration of backup systems, restoring devices to a baseline configuration, or developing contingency plans.
RE 7.3 (i)	Capability to validate the integrity of backed up information prior to the initiation of restore.	
CR 7.4 - Control system recovery and reconstitution	Component shall provide the capability to recover and reconstitute to a known secure state after a disruption or failure.	
CR 7.5 - Emergency power	Capable of running from an emergency power supply without affecting the existing security state or a documented degraded mode.	This requirement applies to IACS developers.
CR 7.6 - Network and security configuration settings	Capability to be configured according to recommended network and security configurations. Capability to Interface to the currently deployed network and security configuration settings.	The Forescout Platform enables organizations to develop, document and maintain a baseline configuration of the systems and components of the ICS environment, and to monitor, review and update changes in real time. Forescout automatically discovers devices and maps communication and data flows with users, roles and responsibilities, for organizational and external entities. Using the GUI, security analysts can easily monitor systems and components, detect new or non-compliant devices, identify deviations from the baseline (device configurations and connections), and identify least functionality configuration issues, such as system ports, protocols, connections, behavior, software, and/or services.
RE 7.6 (i)	Capability to generate a report listing the currently deployed security settings in a machine-readable format.	
CR 7.7 - Least functionality	Capability to specifically prohibit and/or restrict the use of unnecessary functions, ports, protocols and/or services.	The platform enables the enforcement and monitoring of least-privileged access based on device and user identity, device hygiene, and real-time compliance status across diverse networks. The policy engine can be configured to apply usage restrictions, enforce configuration or connection requirements, and issue alerts or automatically take remediation actions, such as isolating or disconnecting a device, when non-compliant assets or connections using unauthorized ports, protocols, or services are detected.
CR 7.8 - Control system component inventory	Components shall provide the capability to support a control system component inventory according to IEC-62443-3-3 SR 7.8	Forescout's real-time asset discovery and vulnerability management system combines passive and active techniques to detect and profile systems on the network, regardless of operating system or form factor. Active discovery probes the network to locate idle devices, while passive discovery monitors traffic to identify active ones. Together, these methods ensure a comprehensive and continuous inventory of all assets in the ICS environment, including physical <i>and</i> software configurations. Whenever a device is installed or reconfigured on the network, the platform immediately detects the change and reassesses the device.

Why Customers Choose Forescout



Complete asset intelligence and control

Managed and unmanaged devices across IT, OT, IoT, IIoT, IoMT



Leader in threat research and intelligence

200+ vulnerabilities identified across hundreds of products



Built for complex, heterogeneous enterprise environments

3000+ customers including 30% of Fortune 100 and 20% of Global 2K



Deep vertical expertise, not one size fits all

Financial services, healthcare, life sciences, government, critical infrastructure, manufacturing



Trusted and proven

20+ years of cybersecurity results



FORESCOUT

Experience the
Forescout Vistaro™ platform
today.

GET STARTED »

About Forescout

As AI-driven vulnerability discovery and exploitation accelerate attack velocity to machine speed, Forescout is a foundational cyber defense layer that allows organizations to segment and isolate compromised systems, block lateral movement, and automate response across IT, OT, IoT, and IoMT environments. The **Forescout Vistaro™ platform**, powered by agentic AI and enhanced with **Vedere Labs** threat intelligence, delivers a Universal Zero Trust Network Access (**UZTNA**) architecture that integrates seamlessly with 180+ security and IT products. With Forescout Vistaro, organizations get comprehensive inventory and classification of both managed and unmanaged assets, continuous exposure management, and real-time protection including dynamic network segmentation and automated threat response.



Forescout Technologies, Inc.

Toll-Free (US) 1-866-377-8771

Tel (Intl) +1-408-213-3191

Support +1-708-237-6591

Learn more at [Forescout.com](https://www.forescout.com)

©2026 Forescout Technologies, Inc. All rights reserved.

Forescout Technologies, Inc. is a Delaware corporation. A list of our trademarks and patents can be found at <https://www.forescout.com/company/legal>. Other brands, products, or service names may be trademarks or service marks of their respective owners.

06_26_V02_RB