appgate

Supporting ISA/IEC 62443 Standards with Universal Zero Trust Network Access (ZTNA)

INTRODUCTION

The manufacturing industry is in the midst of a profound digital transformation, driven by the rapid adoption of Industry 4.0 technologies. This revolution brings with it unprecedented levels of connectivity and automation, promising to optimize processes, boost productivity, and unlock new levels of efficiency. However, this increased interconnectivity also exposes operational technology (OT) environments to a rapidly evolving and increasingly sophisticated threat landscape. OT networks, responsible for controlling critical industrial processes, are particularly vulnerable due to a confluence of factors, including the prevalence of legacy systems, outdated security protocols, and the convergence of IT and OT networks.

This convergence blurs the traditional lines between IT and OT, creating new entry points for malicious actors. Attackers are increasingly targeting manufacturing systems with a diverse arsenal of threats, including:

- **Ransomware attacks:** These attacks can cripple production lines, halting operations and leading to significant financial losses due to downtime and recovery efforts.
- **Targeted intrusions:** Advanced persistent threats (APTs) and state-sponsored actors often engage in targeted espionage aimed at stealing valuable intellectual property, disrupting critical infrastructure, or gaining a competitive advantage.
- **Insider threats:** Malicious or negligent employees with privileged access to sensitive systems can pose a significant risk, whether intentionally or unintentionally.
- **Supply chain vulnerabilities:** Compromised third-party software or hardware components can introduce vulnerabilities that attackers can exploit to gain access to OT networks.

These challenges underscore the critical need for a robust and proactive security approach in the manufacturing sector. The International Society of Automation (ISA) and the International Electrotechnical Commission (IEC) recognized these growing concerns and developed the ISA/IEC 62443 series of standards to provide a comprehensive framework for securing industrial automation and control systems (IACS).

This white paper delves into the significance of ISA/IEC 62443 for manufacturing organizations, emphasizing how aligning security programs with these standards is crucial for protecting OT networks and ensuring business continuity. It also examines how Zero Trust Network Access (ZTNA) can bolster OT security, particularly in remote access scenarios, and how Appgate SDP, a universal ZTNA solution, can help manufacturers achieve and maintain compliance with ISA/IEC 62443 while simultaneously enhancing operational efficiency.

The Importance of ISA/IEC 62443 for Manufacturing

ISA/IEC 62443 is not merely a set of guidelines; it is a comprehensive and detailed series of standards that offer in-depth cybersecurity guidance for the protection of OT systems. The standard is divided into four distinct categories, each addressing specific aspects of OT security:

- **Part 1:** General requirements and concepts for secure product development. This section focuses on the secure design and development lifecycle of IACS products, ensuring that security is embedded from the ground up.
- **Part 2:** Security requirements for system integrators. This part provides guidance for system integrators responsible for designing, implementing, and maintaining secure IACS solutions.
- **Part 3:** Security requirements for industrial automation and control systems. This section outlines the security requirements for the overall IACS, including risk assessment, system design, security controls, and incident response.
- **Part 4:** Security requirements for industrial automation and control system components. This part details the security requirements for individual components within the IACS, such as programmable logic controllers (PLCs), sensors, and actuators.

Each part of the standard provides specific and actionable guidance on different facets of OT security, from conducting thorough risk assessments and implementing secure system designs to establishing effective security controls and developing comprehensive incident response plans.

For asset owners and individuals tasked with the critical responsibility of securing industrial sites, adherence to ISA/IEC 62443 is not just a best practice; it is essential for establishing a multi-layered security approach that:

- **Protects critical infrastructure:** Safeguards vital systems and processes from cyberattacks that could disrupt operations, damage equipment, or compromise sensitive data.
- **Maintains business continuity:** Ensures that manufacturing operations can continue uninterrupted in the face of cyberthreats, minimizing downtime and financial losses.
- **Prevents unauthorized access to sensitive systems:** Restricts access to critical systems and data, preventing unauthorized individuals from gaining control or causing harm.

General	IEC 62443-1-1 Terminology, Concepts and Models	IEC TR-62443-1-2 Master Glossary of Terms and Abbreviations	IEC TR-62443-1-3 Systems Security Conformance Metrics	IEC TR-62443-1-3 IACS Security Lifecycle and Use Cases	
Policies & Procedures	IEC 62443-2-1 Establishing an Industrial Automation and Control System Security Program	IEC TR-62443-2-2 IACS Protection Levels	IEC TR-62443-2-3 Patch Management in the IACS Environment	IEC TR-62443-2-4 Requirement for IACS Service Providers	IEC TR-62443-2-5 Implementation Guidance for IACS Asset Owners
System	IEC TR 62443-3-1 Security Technologies for IACS	IEC TR-62443-3-2 Security Risk Assessment and System Design	IEC TR-62443-3-3 System Security Requirements and Security Levels		
Component	IEC 62443-4-1 Product Development Requirements	IEC 62443-4-2 Technical Security Requirments for IACS Components			

The ISA/IEC 62443 series is organized into four main categories, each focusing on specific security aspects of industrial automation.

Beyond mere compliance, ISA/IEC 62443 represents a valuable opportunity to improve operational efficiencies throughout complex manufacturing infrastructures. By integrating Zero Trust principles alongside these standards, manufacturers can establish a more granular, identity-focused security model that minimizes the attack surface while simultaneously enhancing operational agility. This proactive security framework not only reduces vulnerabilities within OT systems but also supports continuous, secure connectivity across the production environment, fostering a resilient and adaptable manufacturing infrastructure.

With a Zero Trust-aligned ISA/IEC 62443 strategy, organizations can drive business growth, reduce security complexities, and ensure that security enhancements align with broader operational and business objectives.

Strengthening Remote Access in OT Environments Through Zero Trust Principles

In the modern manufacturing landscape, remote access to OT systems is often a necessity, enabling external operators, engineers, and vendors to connect to and manage critical infrastructure from anywhere in the world. However, this convenience also introduces significant security risks if not properly secured. Zero Trust principles offer a robust framework for mitigating these risks, especially when applied to remote access scenarios in OT environments.

Consider the example of an external operator connecting to an engineering workstation or jump server within an industrial demilitarized zone (DMZ). The perimeter of the DMZ serves as the first Zero Trust protected zone and a crucial ISA/IEC 62443 boundary. In this setup, any actor or device outside the DMZ is inherently untrusted, requiring strict authentication, device validation, and secure communication protocols.

Key Zero Trust principles for securing remote access in OT environments include:

- **Strong Authentication:** Multi-factor authentication (MFA) is essential for verifying user identity, ensuring that only authorized personnel with valid credentials can access specific devices and systems.
- **Device Validation:** Before granting access, devices must be authenticated through mechanisms like certificate validation and assessed for compliance with system security policies, including patch levels, antivirus definitions, and other security configurations.

- **Secure Communication:** All data transmitted across the network, especially across the DMZ, must be encrypted to protect sensitive information from interception. Network integrity controls should also be implemented to ensure data integrity and prevent tampering.
- **Real-time Access Control:** Access requests should be evaluated in real-time based on a variety of contextual factors, including user identity, device health, location, time of day, and other risk factors. This dynamic approach ensures that access is granted only when and where it is needed.
- **Network Segmentation:** Establishing secure zones within the OT network is crucial for segmenting critical assets and mitigating the impact of potential breaches. This segmentation limits the lateral movement of attackers, preventing them from gaining access to the entire network even if one area is compromised.
- **Real-time Visibility and Response:** Continuous monitoring of user activities and device behaviors is vital for detecting anomalies and responding swiftly to potential security incidents. Implementing automated threat detection and incident response mechanisms can significantly reduce response times and minimize the impact of security events on operational continuity.

By adhering to these Zero Trust principles, manufacturers can significantly strengthen the security of remote access to their OT environments, ensuring that only authorized entities can interact with critical systems while minimizing the risk of unauthorized access and data breaches.

APPGATE SDP: UNIVERSAL ZTNA FOR OT ENVIRONMENTS

Appgate SDP is a purpose-built solution that delivers universal ZTNA, extending its security coverage to any user, device, and network touchpoint. It is particularly suitable for manufacturing organizations aiming to secure their OT environments in alignment with the ISA/IEC 62443 framework.

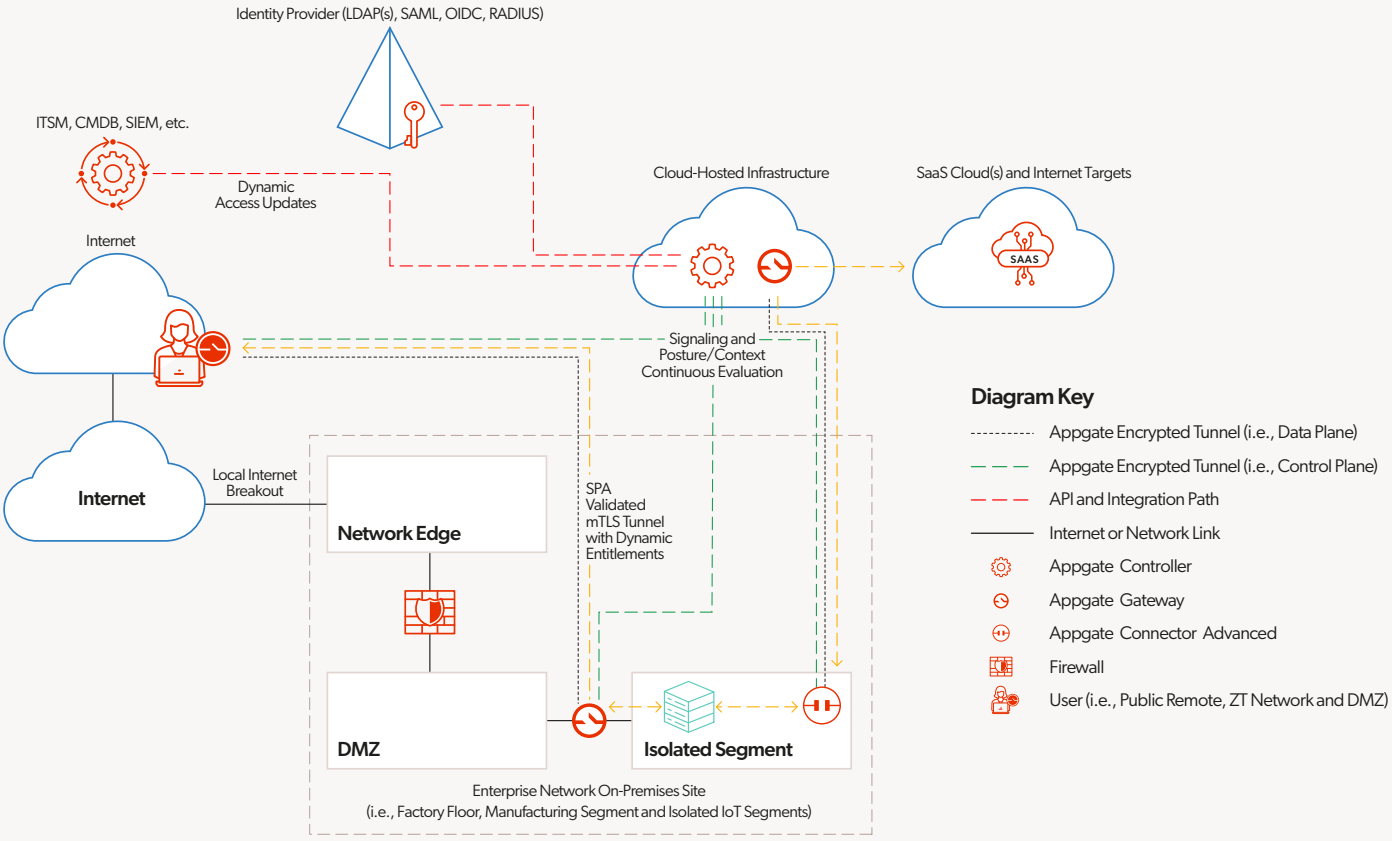
Within the ISA/IEC 62443 framework, there are seven foundational requirements (FRs), each with associated system requirements (SRs) and requirement enhancements designed to achieve one of five target security levels.

SR	FR	Code	Description
1	Identification & Access Control	IAC	Control access to devices, information, or both, to prevent unauthorized interrogation of the device or use of information.
2	Use Control	UC	Control use of selected devices, information, or both to protect unauthorized operation of the device or use of the information.
3	System Integrity	SI	Ensure integrity of data on selected communication channels to protect against unauthorized changes.
4	Data Confidentiality	DC	Ensure the condidentiality of information on communication channels and in data repositories to prevent unauthorized disclosure.
5	Restricted Data Flow	RDF	Segment the control system via zones and conduits to limit the unnecessary flow data.
6	Timely Response to Events	TRE	Respond to security violations by notifying the proper authority reporting needed evidence of the violation and taking timely corrective action when incidents occur.
7	Resources Avalibility	RA	Ensure the availability of the control system against the degradation or denial of essential services.

The seven foundational requirements for IEC 62443.

Appgate SDP provides a comprehensive suite of critical capabilities that support and simplify the implementation of these FRs:

- **FR 1: Identification and Authentication Control:** Appgate SDP enforces strong identity-centric security by authenticating both users and devices before granting network access, supporting an "identify before connect" model. With features like live access entitlements and adaptive policies, Appgate SDP ensures that only verified, trusted entities can access OT systems, providing a foundational layer of identity verification.
- **FR 2: Use Control:** Appgate SDP applies granular, identity-based access control to limit user and device permissions strictly to necessary resources, enforcing the principle of least privilege. Enhanced separation of duties and administrative role controls enable asset owners to govern access precisely, while admin access controls provide further role-based limitations, minimizing the risk of unauthorized actions within OT networks.
- **FR 3: System Integrity:** To preserve the integrity of OT systems, Appgate SDP leverages Single Packet Authorization (SPA) to isolate and cloak network infrastructure, making it invisible to unauthorized users. Additionally, Appgate SDP includes automated defenses against resource overconsumption, dynamically suspending new user connections to the Appgate Gateway (i.e., policy enforcement point) when Java Heap or memory usage exceeds established thresholds, ensuring system stability and resilience.
- **FR 4: Data Confidentiality:** Appgate SDP ensures data confidentiality through end-to-end encryption of data in transit, employing mutual Transport Layer Security (mTLS) to prevent Man-in-the-Middle (MitM) attacks, and utilizing Advanced Encryption Standard (AES)-256 encryption with TLS 1.3 for secure communication channels. Combined with SPA and strict access policies, these capabilities protect OT data from interception or unauthorized disclosure, ensuring secure, confidential network communication.
- **FR 5: Restricted Data Flow:** Appgate SDP enforces precise policies on data movement, segmenting data within secure zones to limit access to designated areas only. Dynamic entitlements further refine data flow control, adjusting accessible targets per user based on inputs from systems like Configuration Management Databases (CMDBs), ticketing systems for just-in-time access, and metadata resolvers. This granular segmentation reduces the risk of unauthorized data exposure or transfer within OT networks.
- **FR 6: Timely Response to Events:** Appgate SDP supports real-time monitoring and rapid policy enforcement, enabling immediate responses to unauthorized access attempts or policy breaches. Appgate SDP's dynamic-conditions feature continuously monitors session activity for changes throughout user sessions, enabling OT security teams to proactively mitigate risks and minimize impact to system stability and security. This capability facilitates rapid response to security events, aligning with the ISA/IEC 62443 framework's emphasis on timely action to maintain system integrity and availability.
- **FR 7: Resource Availability:** Designed for high availability and low latency, Appgate SDP's direct-routed architecture minimizes dependency on external routing. With N+1 redundancy for gateways at each site and a fallback function for site-level failover when all gateways are down or unreachable, Appgate SDP helps ensure continuous, uninterrupted access to critical OT resources, supporting operational continuity and minimizing downtime.



This diagram illustrates Appgate SDP's open, API-first architecture designed for seamless integration with existing technology stacks to deliver scalable, identity-centric security across complex OT environments.

HOW APPGATE SDP WORKS

Appgate SDP universal ZTNA establishes secure connections between users and resources by creating encrypted tunnels. These tunnels are only established after users and devices have been authenticated and authorized. This process ensures that only authorized individuals can access specific resources, regardless of their location.

The key components of Appgate SDP include:

- **Appgate Client:** Installed on user devices (laptops, workstations, mobile devices), the client initiates the connection process and enforces access policies. It acts as a secure gateway, ensuring that only authorized traffic can reach the protected network.
- **Appgate Controller:** The brain of the system, the controller is responsible for authenticating users and devices, authorizing access based on predefined policies, and managing the overall security posture. It acts as a central point of control, enforcing security rules and providing real-time visibility into network activity.
- **Appgate Gateway:** Deployed at the edge of the network, typically within the DMZ or at the perimeter of the OT environment, the gateway enforces access control and provides secure connectivity to resources. It acts as the enforcement point, ensuring that only authorized traffic can pass through to the protected network.

This architecture allows Appgate SDP to provide a seamless and secure user experience while enforcing granular access control and protecting critical OT resources.

Achieving ISA/IEC 62443 Compliance

Achieving ISA/IEC 62443 compliance is not just a checkbox exercise; it is a strategic imperative for manufacturers seeking to establish a robust security posture and protect their critical assets. Compliance with this internationally recognized standard offers numerous benefits:

- **Reduced risk:** A strong security posture, aligned with ISA/IEC 62443, significantly minimizes the likelihood and impact of cyberattacks, protecting valuable assets and minimizing financial losses.
- **Improved operational efficiency:** Secure and reliable systems lead to increased uptime and productivity, ensuring that manufacturing processes can continue without disruptions caused by security breaches.
- **Enhanced reputation:** Demonstrating a commitment to cybersecurity by achieving ISA/IEC 62443 compliance builds trust with customers, partners, and stakeholders, enhancing brand reputation and demonstrating a commitment to security best practices.
- **Competitive advantage:** In a competitive landscape, compliance can be a key differentiator, giving manufacturers an edge by demonstrating a commitment to security and data protection.

Additionally, the certification process for ISA/IEC 62443 typically involves several key steps, including:

- **Gap analysis:** A thorough assessment of the current security posture against the requirements of the standard is conducted to identify any gaps or areas for improvement.
- **Implementation:** Based on the gap analysis, security controls are developed and implemented to address any identified deficiencies and align with the requirements of the standard.
- **Assessment:** An independent audit by a certified body is conducted to evaluate the effectiveness of the implemented security controls and ensure compliance with the standard.
- **Certification:** Upon successful completion of the audit, the organization receives certification, demonstrating its commitment to ISA/IEC 62443 and providing assurance to stakeholders.

Ensuring Security and Operational Success with Universal ZTNA

As manufacturers navigate the complexities of digital transformation, they must prioritize strong security measures to protect their OT environments from the ever-present internal and external cyberthreats. Implementing an adaptable security solution like Appgate SDP enables organizations to confidently leverage innovative technologies while maintaining robust protections against cyberattacks. By aligning security initiatives with industry standards like ISA/IEC 62443, manufacturers can ensure comprehensive protection for their critical infrastructure.

CONCLUSION

The synergy between universal ZTNA and ISA/IEC 62443 standards empowers organizations to not only protect their valuable assets but also reduce security complexity and drive sustainable growth in today's challenging threat landscape. By partnering with Appgate, manufacturers can gain access to the expertise and technology necessary to assess, implement and maintain a suitable defense-in-depth strategy for OT and IACS, ensuring that their security posture remains strong and resilient in the face of evolving threats.

Learn more by exploring the related resources below, or start your 30 day ZTNA Free Trial to experience the power of Appgate SDP in your own environment and test its capabilities firsthand.

About Appgate

Appgate secures and protects an organization's most valuable assets and applications. Appgate is the market leader in Zero Trust Network Access (ZTNA) and online fraud protection. Appgate products include Appgate SDP for Universal ZTNA and 360 Fraud Protection. Appgate services include threat advisory analysis and ZTNA implementation. Appgate safeguards enterprises and government agencies worldwide. Learn more at appgate.com.