WHITE PAPER

Building a Resilient Network Security Foundation for IEC 62443-3-3 Compliance

Theo Lai
Product Manager

MOXA®

Security as a Systemic Engineering Task

Industrial IoT (IIoT) has continued to expand in recent years, with more and closer integration of IT and OT assets. Inevitably, this trend has also fundamentally shifted the industrial cyberthreat landscape. The need for comprehensive network protection is more dire than ever. However, building comprehensive OT cybersecurity is more than just a matter of buying OT security-focused products. It's a complex and multifaceted endeavor that requires a systemic mindset for developing a comprehensive defense-in-depth strategy. Knowing where to start is half the journey.

A Guide to Robust Cybersecurity – IEC 62443

The IEC 62443 framework is the world's most authoritative set of standards for OT cybersecurity. It covers security measures on multiple layers to create holistic protection against cyberthreats, including device-level components (IEC 62443-4-2) and secure product development lifecycle processes (IEC 62443-4-1). In this white paper, we will take a closer look at the IEC 62443-3-3 standard, which offers a guiding framework for integrating multiple system components into industrial automation and control systems (IACS).

IEC 62443-3-3 bridges the gap between the vendor's product capabilities and the integrator's implementation of those products, outlining the requirements necessary to meet a set of predefined system-wide security objectives.

The standard defines four distinct Security Levels (SL) based on the attacker's motivation, skills, and resources. The following overview gives a brief description of each level:

Level	Description
Security Level 1	Protection against casual or coincidental violations.
Security Level 2	Protection against intentional violations using simple means with low resources and generic skills.
Security Level 3	Protection against intentional violations using sophisticated means with moderate resources and specific IACS skills.
Security Level 4	Protection against intentional violations using sophisticated means with extended resources and highly specialized skills.

Table 1: IEC 62443 Security Levels summary

IEC 62443-3-3 defines seven Foundational Requirements (FRs), that are tied to a separate set of additional conditions. These are System Requirements (SRs), which specify the technical capabilities the system should have, and Requirement Enhancements (REs), which provide additional controls for complying with higher SLs. Refer to the following table for a summary of FRs and their main objective.

Requirement	Objective
FR 1: Identification & Authentication	Ensure all users (human, software process, or device) are identified and authenticated before gaining access.
FR 2: Use Control	Enforce assigned privileges to ensure users only perform actions they are authorized to do, preventing "privilege creep".

Requirement	Objective
FR 3: System Integrity	Protect the IACS against unauthorized changes to hardware, firmware, and software.
FR 4: Data Confidentiality	Protect sensitive information from unauthorized disclosure in communication channels and data storage.
FR 5: Restricted Data Flow	Segment the network into zones and conduits to limit the spread of a cyberattack across the system.
FR 6: Timely Response to Events	Ensure the system can notify authorities, log data, and provide forensics when a security violation is detected.
FR 7: Resource Availability	Ensure the IACS remains operational and resilient against degradation or Denial of Service (DoS) attacks.

Table 2: IEC 62443-3-3 Foundational Requirements summary

Which SL to pursue depends on the threat environment, system criticality, and availability of resources, as the number and complexity of compliance requirements expands with each SL. For most modern industrial applications, SL2 strikes a good balance between security against more complicated intentional attacks and implementation feasibility.

The Pitfalls of Traditional OT Networks

As industries embrace converged IT/OT infrastructure to boost operational efficiency and manageability, industrial control systems inevitably become exposed to a new dimension of cross-domain cyberattacks. This development has made rudimentary OT cybersecurity inadequate to handle rapidly evolving cyberthreats. The transition to converged networks has fueled a surge in IT-originated exploitation attempts targeting popular OT protocols, up to 84% in 2025, with most threats aimed at Modbus and EtherNet/IP[1]. These vulnerabilities are highlighted even more by the fact that most OT networks are traditionally designed in a "flat" architecture (Figure 1). In such setups, a concentrated security barrier protects connected network components against basic attacks, creating an exploitable single point of failure. When breached, attacks can easily spread to any other component in the network. Developing a multi-layered defense strategy helps mitigate many of the weaknesses of traditional OT networks.

[1] Forescout Research – Vedere Labs: 2025 Threat Roundup Report: 2025 Threat Report: Exploitation Grows Across IT, IoT, and OT

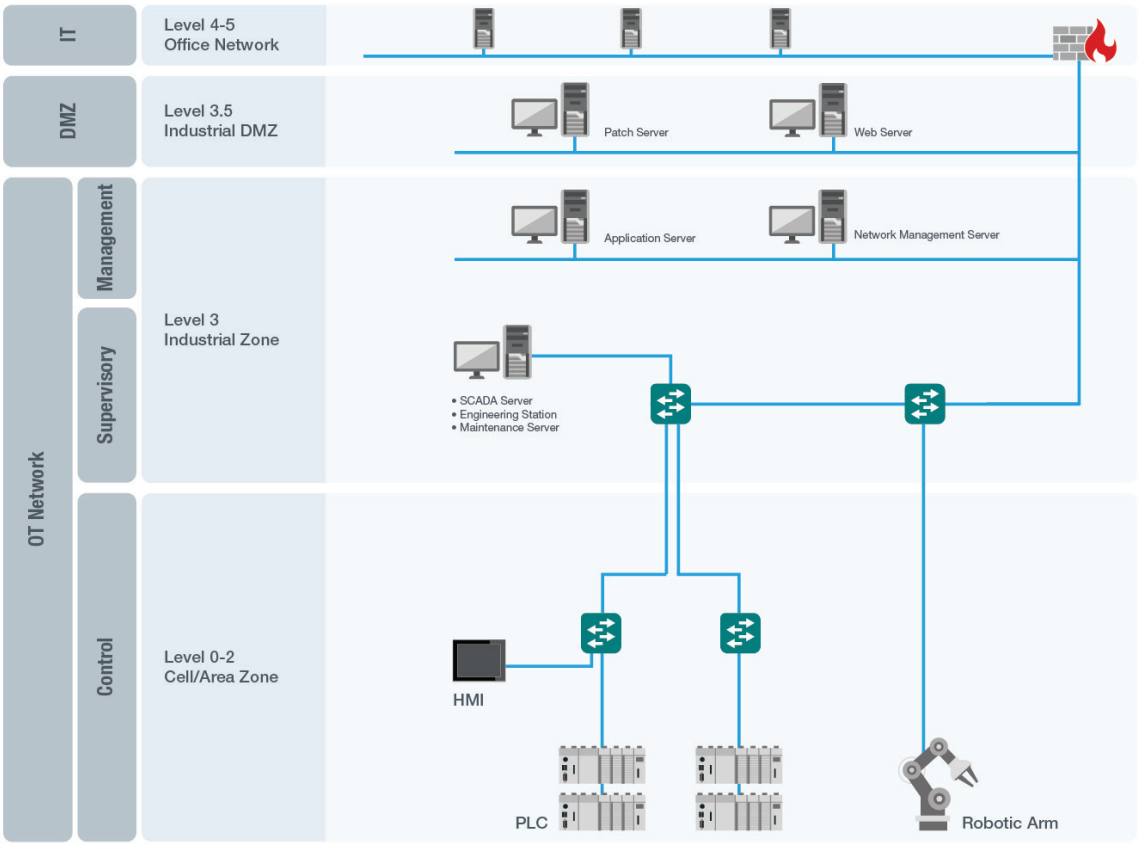

Figure 1: Traditional flat OT network architecture

Implementing IEC 62443-3-3 From a Networking Perspective

As introduced earlier, IEC 62443 is a comprehensive suite of standards covering cybersecurity requirements for IACS components, systems, and integration. While Moxa focuses on delivering security-hardened devices compliant with IEC 62443-4-2 SL 2, system integrators and asset owners must address the system-level requirements of IEC 62443-3-3. We understand the challenges our industrial partners are facing. By redesigning vulnerable networks according to these rigid standards, we carry out our commitment to helping integrators build resilient network security and advance their efforts to achieve IEC 62443-3-3 system-wide compliance.

For the purposes of this white paper, we will explore how Moxa can assist system integrators in meeting IEC 62443-3-3 Foundational Requirements for SL2 from a networking perspective. While these recommendations address some of the System Requirements (SRs) and Requirement Enhancements (REs), this is not an exhaustive list of measures required to achieve compliance.

FR 1: Identification and Authentication

An important tenet of cybersecurity is ensuring that only authorized users have access to network systems. There are multiple mechanisms available to verify the identity of users, either locally or remotely. Some of the most common methods of remote authentication and authorization are TACACS+ and RADIUS. Implementing remote authentication allows system integrators to move away from vulnerable shared credentials towards centralized, multifactor user authentication. Encrypting authentication data safeguards data integrity and enhances security even further. Proper user authentication ensures that anyone attempting to access control systems from an untrusted network is verified and authorized, minimizing the risk of tampering by bad actors.

FR 2: Use Control

Besides making sure anyone allowed on your network is authorized to do so, it is just as important to limit access for each user to only systems and functions relevant to their responsibilities. Here is where the principle of "least privilege" comes into play, which dictates that a user should only have access to the bare minimum required to fulfill their role. This helps prevent both accidental misconfiguration and intentional tampering by users operating outside the scope of their assigned tasks. Measures such as role-based access control (RBAC) allow administrators to define access permissions based on user role, providing only the absolute minimum required system privileges.

FR 3: System Integrity

Guaranteeing the integrity of systems and data in transition is another cornerstone of a robust security framework to prevent unauthorized changes and tampering. At the device level, secure boot and trusted firmware serve as baseline checks to make sure only authentic, unmodified code can execute on your controllers and I/O devices. The next step is ensuring the integrity of communication channels by using encrypted, secure protocols such as HTTPS, TLS, SSH, and SNMPv3 to prevent data from being intercepted or manipulated during transit. Disabling unused or unsecure physical and logical interfaces also reduces the attack surface and mitigates the risk of unauthorized entry points being exploited.

FR 4: Data Confidentiality

Data in transmission can be highly vulnerable to interception, especially when it involves sensitive control parameters or system credentials. Ensuring the confidentiality of such data is a fundamental requirement to protect it from unauthorized disclosure. For system integrators, protecting data across different network layers is often a major architectural challenge. Leveraging industry-proven cryptographic mechanisms provides a standards-compliant method for encrypting moving data. It's crucial to have measures in place that protect confidentiality on different levels, such as MACsec for hop-by-hop Layer 2 encryption within the LAN, and secure VPN tunnelling (IPsec) for routing across untrusted networks. Equally important is ensuring that stored device configuration files are securely encrypted to prevent malicious actors from extracting network information and credentials. Deploying these mechanisms side-by-side ensures data confidentiality across the entire system architecture.

FR 5: Restricted Data Flow

Data freely moving across a network is more vulnerable as it passes through more devices, offering potential attackers more opportunities to intercept or manipulate the traffic. In industrial network environments, there are many types of data of different criticality being processed by an equally broad range of devices, including production equipment, control systems, and management devices. Segmenting data to prevent the lateral movement of threats is another key pillar of sound network security. By separating the network, integrators can create operational areas with their own dedicated security measures (zones) and controlled communication paths (conduits) between these zones. In a segmented structure, if one network zone is compromised, the breach is contained and will not affect other networking zones. The easiest way to create networking zones is by implementing a VLAN architecture, which logically groups networking devices into a single LAN environment. Deploying industrial firewalls with Deep Packet Inspection (DPI) capabilities creates a robust defense layer that monitors and blocks any unauthorized traffic moving across zone boundaries based on user-defined policies.

FR 6: Timely Response to Events

Maintaining a secure control environment relies heavily on the ability to respond quickly to security events and incidents occurring on the network. Device- and network-level visibility plays a critical role in enabling administrators to identify and mitigate potential threats. Traffic monitoring functions and event logging provide supervisors with valuable insights into network activity, while configurable notifications alert of issues as they happen. Meanwhile, powerful network management software offers more holistic, network-wide visibility via real-time dashboards, topologies, and security asset management.

FR 7: Resource Availability

This requirement states that control systems should remain operational in the face of a network attack or failure. Good resource management is critical for system reliability and security, as sudden operational disruptions not only incur heavy costs, but also expose the network to potential attacks. Optimizing network availability requires thoughtful

implementation of both software and hardware measures. Communication load management functions such as rate limiters and storm control regulate incoming and outbound traffic volumes to prevent overloading, data loss, and DoS attacks. Quality of Service (QoS) prioritization, in turn, ensures that critical data such as input from control systems is reliably transmitted, even in heavy traffic conditions. Not to be overlooked is support for redundant protocols and architectures to provide communication failover capabilities in the event of a failure. At the hardware level, availability can be enhanced through robust redundancy built into the product design, such as redundant dual power supplies.

From a Vulnerable to a Hardened Architecture

Implementing the Foundational Requirements helps transform vulnerable networks into a resilient and secure foundation that brings integrators one step closer to designing IEC 62443-3-3 compliant IACS systems. Figure 2 illustrates a hardened architecture where security is embedded into the fabric of the network. The system now features protected zones and boundaries, encrypted communication, and real-time visibility. In such a security-hardened architecture, if one segment is compromised, other segments stay secure, enabling more resilient system-wide operations.

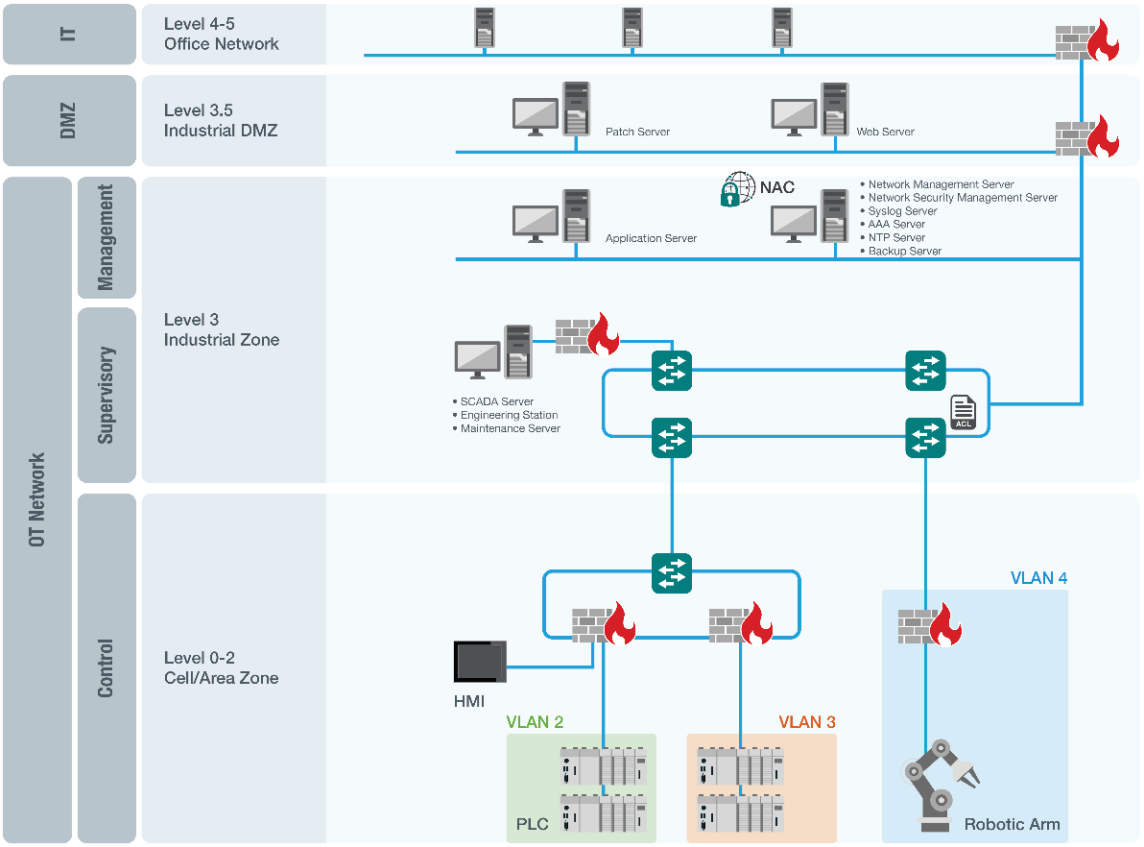

Figure 2: Security-hardened OT network architecture

Conclusion: A United Front for Industrial Security

Adopting a systemic view of cybersecurity is the only way to ensure long-term operational resilience in the digital age. When you design your network according to IEC 62443-3-3 principles, you aren't just checking a compliance box; you are building a defensible fortress for your assets. By starting with pre-validated building blocks, integrators can reduce complexity,

lower compliance costs, and build systems that are truly secure by design. Selecting a reliable solutions partner can significantly simplify this journey. Moxa, with its ample expertise in IEC 62443-4-1 secure development and strong portfolio of -4-2 certified hardware, offers integrators the tools they need to build secure systems for the next generation of industrial operations.

For more information about Moxa's industrial network security solutions, visit Industrial Network Security | Moxa.