Aligning Network Security with IEC 62443

How Network Service Edge (NSE) Supports Industrial Cybersecurity

Executive Summary

The convergence of operational technology (OT), IT, and cloud-managed systems is increasing cyber risk across industrial, critical infrastructure, and cloud environments. To address these risks, the IEC 62443 series of standards defines a globally recognized framework for securing industrial automation and control systems.

This white paper explains the intent and structure of the IEC 62443 standard and describes how the Network Service Edge (NSE) platforms from Cambium Networks help organizations implement IEC 62443 aligned security controls. It provides a capability-based mapping, not a certification claim, and is intended to support customer risk assessments, procurement evaluations, and regulatory- or framework-driven programs such as NIS2.

Understanding IEC 62443

What is IEC 62443?

IEC 62443 is an international series of standards developed by the International Electrotechnical Commission (IEC) to address cybersecurity for industrial automation and control systems (IACS). Unlike generic IT security frameworks, IEC 62443 is designed specifically for environments where availability, safety, and operational continuity are critical.

The standard applies across the lifecycle of industrial systems and addresses:

- Secure product development
- Secure system design and integration
- Operational security and monitoring
- Risk-based segmentation and access control

Foundational Requirements

At its core, IEC 62443 defines seven Foundational Requirements (FR) that represent the essential security objectives for industrial systems and components:

1. Identification and Authentication Control (IAC)
2. Use Control (UC)
3. System Integrity (SI)
4. Data Confidentiality (DC)
5. Restricted Data Flow (RDF)
6. Timely Response to Events (TRE)
7. Resource Availability (RA)

These FRs describe what security outcomes must be achieved, while lower-level requirements (System Requirements [SR] and Requirement Enhancements describe how those outcomes may be implemented.

Capability Alignment

This white paper documents how the NSE appliance capabilities can help organizations implement the intent and requirements of the IEC 62443.

Scope of This Whitepaper

- **Products:** Cambium Networks' NSE
- **Management Platform:** cnMaestro™ Network Management
- **IEC 62443 Parts Referenced:**
  - IEC 62443 4 2 – Technical security requirements for components
  - IEC 62443 4 1 – Secure product development lifecycle (capability alignment)

IEC 62443 Foundational Requirements Mapping

FR1 – Identification and Authentication Control (IAC)

Objective: Ensure that users, devices, and systems are uniquely identified and authenticated.

How NSE Helps:

- Role-based administrative access
- Multi factor authentication for administrators
- Unique identification of devices and users through centralized management
- Secure remote access using WireGuard® based VPNs and IKEv2/IPsec VPNs

FR2 – Use Control (UC)

Objective: Ensure authenticated entities can only perform authorized actions.

How NSE Helps:

- Granular role-based authorization via cnMaestro
- Controlled administrative access to configuration and operational functions
- Centralized policy enforcement and auditability

FR3 – System Integrity (SI)

Objective: Protect systems and communications from unauthorized modification.

How NSE Helps:

- Controlled firmware update mechanisms
- Centralized configuration management with rollback to last known good state
- Default hardening and explicit enablement of services
- Continuous identification of integrity risks through the Always ON Vulnerability Scanner

FR4 – Data Confidentiality (DC)

Objective: Prevent unauthorized disclosure of information.

How NSE Helps:

- Encrypted management access using HTTPS and SSH
- Secure remote and site-to-site site connectivity using WireGuard and IKEv2/IPsec VPNs
- Encrypted communications across segmented network zones
- Protection of credentials and sensitive configuration data

FR5 – Restricted Data Flow (RDF)
Objective: Limit data flows to only those explicitly permitted.

How NSE Helps:

- VLAN based segmentation of networks and critical assets
- Stateful firewall policies for inter-VLAN and WAN/LAN traffic
- Default deny posture with explicit allow rules

FR6 – Timely Response to Events (TRE)
Objective: Detect security-relevant events and support timely response.

How NSE Helps:

- Centralized logging and event visibility
- Log export via syslog and APIs for SIEM integration
- Alerts for anomalous activity, failed access attempts, and security events
- Always ON Vulnerability Scanner providing continuous, low-impact detection of emerging vulnerabilities

FR7 – Resource Availability (RA)
Objective: Ensure system availability and resilience during faults or attacks.

How NSE Helps:

- WAN redundancy to maintain connectivity during link failures
- High-availability support for critical deployments
- Configuration backup and automatic rollback
- Least functionality posture to reduce attack surface

Secure Development and Supply Chain Practices (IEC 62443 4 1 Alignment)

Cambium Networks follows secure development and maintenance practices aligned with IEC 62443 4 1 principles, including:

- Firmware review against known vulnerabilities prior to release
- Regular security and maintenance updates
- Documented vulnerability handling and remediation processes
- Ongoing product lifecycle support

These practices support customer supply chain assurance and secure-by-design objectives.

Management Platform Assurance: cnMaestro

cnMaestro, the centralized management platform for NSE devices, operates under SOC 2–compliant security and operational controls. SOC 2 provides independent assurance of cnMaestro functions related to access control, monitoring, availability, incident handling, and operational security.

While SOC 2 is not an IEC 62443 certification, it complements IEC 62443 aligned product capabilities and supports organizational governance and aligned product capabilities and supports organizational governance and supply chain risk management requirements, including those under NIS2.

Relationship to NIS2

The NIS2 Directive requires organizations to implement proportionate technical and organizational measures for cybersecurity risk management. IEC 62443 provides a recognized technical framework for demonstrating such measures in industrial and operational environments.

NSE capabilities mapped in this whitepaper can serve as technical evidence supporting broader NIS2 compliance programs.

Conclusion

IEC 62443 provides a structured, risk based approach to securing industrial networks. Cambium's Network Service Edge platforms help organizations implement the intent of the IEC 62443 Foundational Requirements through integrated security, segmentation, monitoring, resilience, and continuous vulnerability awareness.

This capability-based alignment enables organizations to strengthen cyber resilience while maintaining operational simplicity and regulatory confidence

ABOUT CAMBIUM NETWORKS

Cambium Networks empowers millions of people with wireless connectivity worldwide. Its wireless portfolio is used by commercial and government network operators as well as broadband service providers to connect people, places and things. With a single network architecture spanning fixed wireless and Wi-Fi, Cambium Networks enables operators to achieve maximum performance with minimal spectrum. End-to-end cloud management transforms networks into dynamic environments that evolve to meet changing needs with minimal physical human intervention. Cambium Networks empowers a growing ecosystem of partners who design and deliver gigabit wireless solutions that just work.

cambiumnetworks.com