# IEC 62443 Compliance Support

Make verified hardware identity part of industrial cyber resilience

## The Challenge

IEC 62443-aligned programs depend on knowing which assets participate in industrial automation and control system environments. Yet many OT networks still rely on declared identity, manual inventories, network scans, or traffic visibility that can miss unmanaged, spoofed, dormant, or physically hidden hardware.

## Why It Matters Now

Industrial environments are expanding through remote access, IIoT, engineering workstations, supplier connectivity, and connected operational assets. When hardware identity is assumed rather than verified, zones and conduits can be weakened, unauthorized devices can persist, and response teams may lack the evidence needed to act quickly.

## Sepio's Solution

Sepio supports IEC 62443 programs by extending visibility and control to the hardware layer. Using AssetDNA and physical-layer intelligence, Sepio helps discover connected assets, validate true device identity, detect rogue or masquerading hardware, provide precise location context, and trigger policy-driven mitigation through existing security operations.

# How Sepio Supports IEC 62443

Sepio strengthens key IEC 62443 control areas that depend on trusted asset identity:

**1**

### Asset Discovery

Continuously identify IT, OT, IoT, USB, peripherals, unmanaged devices, and shadow assets that traditional tools may miss.

**2**

### Identity Validation

Verify what a device really is using physical-layer and AssetDNA evidence, not only MAC, IP, hostname, or self-declared attributes.

**3**

### Zones & Conduits

Support segmentation assurance by showing what is connected, where it is located, and whether it belongs in a given industrial zone.

**4**

### Risk-Based Prioritization

Prioritize response using exposure, criticality, confidence of evidence, policy context, and hardware risk indicators.

**5**

### Detect & Mitigate

Trigger alerts, restrictions, quarantine, denial, or automated workflows before unauthorized hardware can operate unchecked.

## Where Sepio Applies

- IEC 62443-2-1 security program support: improves asset inventory confidence and provides evidence for ongoing governance.
- IEC 62443-3-2 risk assessment: helps identify hardware exposure, unauthorized assets, and gaps that affect zone-level risk.
- IEC 62443-3-3 system requirements: supports restricted data flow, system integrity, timely response, auditability, and resource availability through hardware visibility and response.
- EC 62443-4-2 component security context: helps validate connected components and detect anomalous or masquerading device behavior in operational environments.

## Why Sepio

- Trafficless discovery suitable for sensitive OT environments
- Hardware identity validation using AssetDNA and physical-layer evidence
- Precise asset location context across network, USB, and endpoint attachment points
- Detection of rogue, spoofed, unauthorized, dormant, and vulnerable hardware
- Integration-ready alerts and evidence for SIEM, SOAR, CMDB, NAC, and operational workflows

## Business Outcomes

**With Sepio, organizations can:**

- Close hardware-level blind spots across industrial and critical infrastructure environments
- Strengthen IEC 62443-aligned governance with continuous hardware evidence
- Reduce operational risk before unauthorized devices can affect industrial operations

## IEC 62443 programs need trusted asset identity.

Sepio helps organizations extend Zero Trust to the physical layer - enabling them to discover, verify, validate, prioritize, and enforce trust at the hardware level.