NetFoundry

WHITE PAPER

Achieving IEC 62443 Compliance

Learn more at www.netfoundry.io

Executive Summary

For decades, the standard security control for Operational Technology (OT) had been the “air gapped” network. Over time as Industry 4.0 and IIoT have effectively dissolved that gap, the **IEC/ISA 62443** standard has become the new North Star for protecting critical infrastructure. However, a significant rift has formed between the requirements of the standard and the reality of the plant floor.

Traditional networking vendors suggest solving IEC/ISA 62443 compliance by overhauling the existing infrastructure replacing legacy switches, routers, and firewalls with new “security-aware” hardware. In the real world, this approach is a non-starter. Industrial environments are riddled with legacy technical debt: flat Layer 2 networks, unmanaged switches, and sensitive devices that cannot tolerate the disruption of a hardware refresh.

In modern OT, the challenge is no longer just how to connect systems securely, but how to do so without triggering repeated firewall/VLAN changes, MOC cycles, safety reviews, and IT/OT governance friction. This whitepaper details a pragmatic, secure, and operationally simple approach using NetFoundry Software-Defined Zero Trust Overlays that can be fully owned and operated by OT engineers with minimal networking knowhow. NetFoundry ZLAN implements a software-defined network that runs on the existing infrastructure as an identity-first overlay fabric. With it, organizations can implement granular microsegmentation and policy-defined conduits across Purdue Levels 1 through 5 while running on standard COTS hardware without touching the existing underlay.

THE STANDARD

Deep Dive into IEC/ISA 62443-3-3

While other parts of the IEC/ISA 62443 series focus on the *process* or the *components*, **IEC/ISA 62443-3-3** is the "System Security Requirements and Security Levels" section. It is the technical heart of the standard. It defines seven Foundational Requirements (FRs), each with System Requirements (SRs), that are used to assess whether a system meets its target Security Level (SL).

The "Zones and Conduits" Mandate

The most critical architectural concept in 62443-3-3 is the division of the system into **Zones** (groups of assets with similar security requirements) and **Conduits** (secure communication paths between zones).

For higher target Security Levels (SL3 or SL4), the following requirements are especially important:

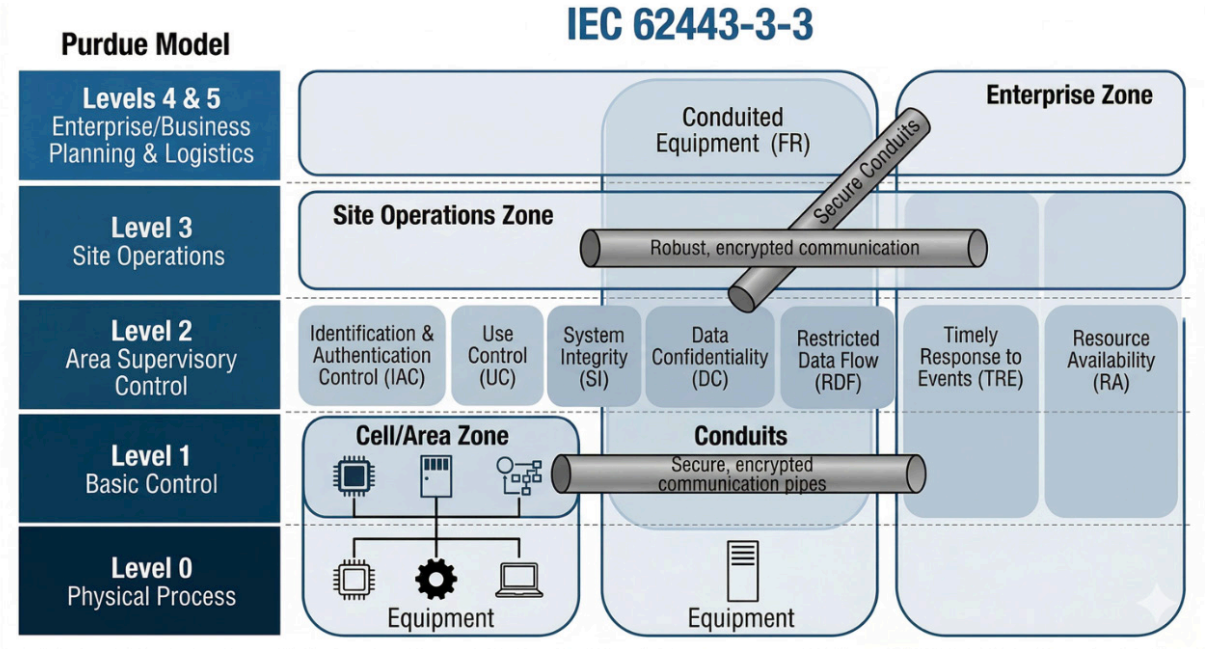
SR 5.1 (Network Segmentation)
The system must support the partition of the network into zones.

SR 5.2 (Conduits)
All communication between zones must occur through defined conduits that provide protection and control.

SR 3.1 (Communication Integrity)
Ensuring that traffic between zones hasn't been tampered with.

SR 4.1 (Data Confidentiality)
Encrypting sensitive data as it moves between segments.

Achieving this across the Purdue Model (from L1 PLCs to L5 Enterprise/Cloud) is the primary goal of any OT security architect.



To visualize how the standard maps to the operational hierarchy, we must look at the Purdue Model through the lens of IEC/ISA 62443 requirements.

Why "Underlay-First" Approaches Fail in OT

The traditional approach to IEC/ISA 62443 championed by hardware-centric vendors relies on "fixing" the physical network. This approach fails because it ignores the unique operational constraints of the OT world:

1 **Legacy Technical Debt & Flat Networks**

Most plants were built for connectivity, not security. They feature "Flat L2" networks where every device can talk to every other device. These rely on **unmanaged switches** that lack VLAN or ACL capabilities.

2 **The "Rip and Replace" Nightmare**

To implement underlay-based segmentation, you must replace every unmanaged switch with a managed one. This isn't just a hardware cost; it's an operations continuity disaster. Scheduling downtime for a complete network overhaul is often impossible for 24/7 manufacturing or utility operations.

3 **The Expertise Gap**

Configuring underlay segmentation (e.g., TrustSec, VRFs, complex Firewall rules) requires high-level networking certifications. OT teams are experts in automation, not BGP or RADIUS. Forcing them to rely on IT for every "move, add, or change" creates friction and delays.

4 **Multi-Vendor Fragmentation**

Plants typically operate a mix of equipment from many vendors, such as Siemens, Rockwell, ABB, and Schneider. Underlay security features are often proprietary to the vendor, leading to "lock-in" and interoperability failures with legacy OT assets. This also makes it very difficult if not impossible to achieve a 'unified governance' operating model.

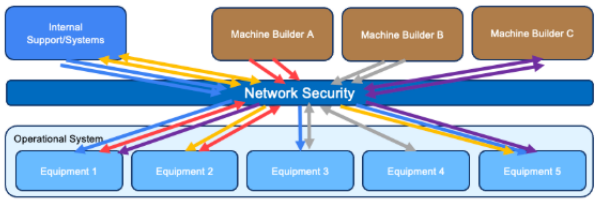
5 **Complex Integrations**

Every new telemetry, AI, vendor-support, or IT/OT integration project triggers firewall/VLAN changes, MOC cycles, safety review, and approval overhead.

6 **Re-IPing Challenges**

Multiple vendor overlays, identity systems, and access models create governance sprawl, inconsistent controls, fragmented audit, and growing pressure for underlay change.

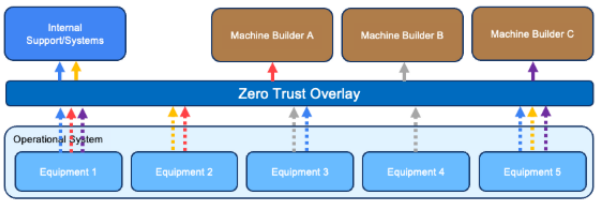
Today | Mixed Governance and Overlay Sprawl



Multiple vendor tunnels & identities → inconsistent controls + governance risk + risk to critical operation

- Plants need external access (telemetry, diagnostics, IT/OT, SRA), but **each brings its own VPN, certs, firewall rules, and support path**, creating inconsistent controls and breaking 62443 governance.
- Operators **cannot enforce zones, conduits, JIT access or session-level audit** across multiple external overlays.
- Mixed governance forces **underlay changes** (FW/VLAN edits, MOC cycles), slowing innovation and raising operational risk.
- Safety teams lose visibility due to **inconsistent logs, identities, and across paths**.

NetFoundry Model | Identity-Bound Overlay



Unified governance, per-service least privilege, protected critical operations, no underlay changes

- **Egress-only Zero Trust overlay** replaces all vendor tunnels - each connection becomes **identity > assett . protocol/port > duration** conduit.
- Governance becomes **centralized and consistent**: JIT approvals, immutable audit, plant-side kill-switches, and least priviledge for internal + OEM + automation access.
- Vendors **no longer infulence the network**; they connect only through **policy-defined conduits**, eliminating underlay changes and reducing safety burden.
- Mixed governance becomes **single governance**: unified policy model, unified audit trial, **plant sovereignty retained**.

THE NETFOUNDRY SOLUTION

zLAN + Zero Trust Overlay

NetFoundry's approach solves the problem from the top down. Instead of asking you to replace your "Underlay" (switches, routers, and firewalls), it builds a **Software-Defined Overlay** enabling plant owned governance by the OT engineers who can control the connectivity and access policies independently of the underlying physical network topology and hardware lifecycle.

Introducing NetFoundry zLAN

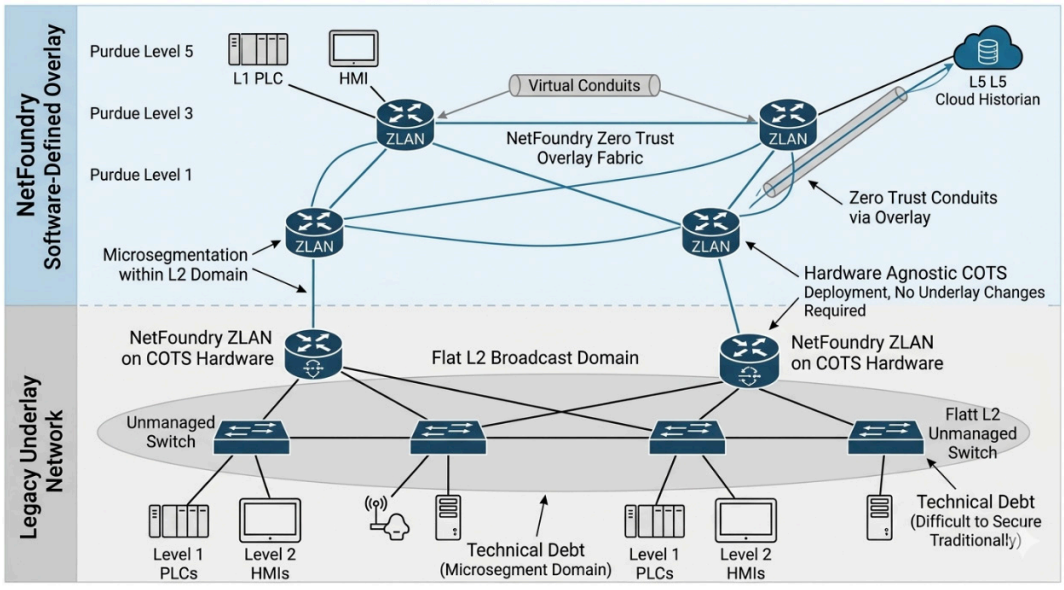
At the heart of the solution is **NetFoundry zLAN (Zero Trust LAN)**. zLAN is a lightweight piece of software that runs on **COTS (Commercial Off-The-Shelf)** hardware such as an industrial PC, a NUC, or a virtual machine. zLAN acts as the "Software-Defined Gateway" that transforms your legacy, flat network into a secure, policy driven overlay that can be independently managed by OT engineers.

A | Microsegmentation Within the Broadcast Domain (Intra-zLAN)

One of the most powerful features of ZLAN is its ability to segment devices *connected to the same unmanaged switch*. By acting as the identity-based enforcement point, zLAN ensures that a PLC and an HMI in the same L2 broadcast domain can only communicate with each other if a specific Zero Trust policy (rule) exists. This is microsegmentation without requiring VLAN redesign or underlay changes.

B | Inter-Zone Connectivity (The Overlay Fabric)

For communication across different plant areas or from the plant floor (L1) to the cloud (L5), the NetFoundry Overlay Fabric creates a secure, governed and encrypted "conduit" that inherently implements zero trust principles of strong identity, least privilege access, continuous authorization, end to end encryption and deep visibility. This conduit is invisible to any network elements that are not part of the fabric. It has no open inbound ports and thus is unreachable from the underlay network. It uses **Just-In-Time (JIT)** connectivity, where the path is only established when an authenticated and authorized identity requests access.



NetFoundry Overlay sits on top of a flat, "dumb" underlay.

Key Compliance Benefits

As policy enforcement is overlay-based, it decouples governance from underlay network changes. This means new use cases, capabilities or changes can be enabled without firewall/VLAN change, MOC churn, or rework of the physical network. It also does not materially alter the zones/conduits security model, reducing reassessment churn.

Mapping IEC/ISA 62443-3-3 Requirements to NetFoundry

IEC/ISA 62443-3-3 SR	Standard Requirement Summary	NetFoundry Solution
SR 1.1: IAC	**Identification & Authentication** Verify identities of all users/devices.	**Identity-First** Access is based on unique cryptographic identity rather than IP addresses, network location or pre-shared credentials.
SR 2.1: UC	**Use Control** Enforce authorized access to assets.	**Micro-segmentation** Least Privileged Access is granted by OT governed policy at the service level (e.g., Modbus/TCP on Port 502 only).
SR 3.1: SI	**Communication Integrity** Protect against tampering and replay.	**Signed Packets** All traffic in the overlay is cryptographically signed and verified.
SR 4.1: DC	**Data Confidentiality** Encrypt communication across conduits.	**MTLS Encryption** Confidentiality is enforced through E2E encrypted overlay communications and mutual authentication (mTLS) between authorized participants.
SR 5.1: RDF	**Network Segmentation** Partition the network into Zones.	**Software Zones** The NetFoundry solution creates logical zones in a flat, unmanaged L2 network without VLANs.
SR 5.2: RDF	**Network Conduits** Securely connect different zones.	**Overlay Fabric** Provides an "invisible," outbound-only conduit across the Purdue Model (L1-L5).
SR 6.1: TRE	**Audit Logging** Record and monitor security-relevant events.	**Deep Visibility** Unified audit trail, identity-to-service traceability, and session-level visibility, with every connection attempt, success, or failure logged in real time for SOC/SIEM and operational review.

The Strategic Advantages of the NetFoundry Approach

- **Unified Governance Across Vendors and Use Cases**
  Instead of each OEM, vendor, or cloud service introducing its own tunnel, identity source, certificate model, and audit trail, NetFoundry provides a single, plant-governed policy model for zones, conduits, least privilege, and session control - reducing governance sprawl without requiring underlay changes.
- **Zero Infrastructure Changes**
  No need for a multi-million dollar hardware refresh. Keep your existing unmanaged switches and flat L2 architecture.
- **Non-Disruptive Deployment**
  Unlike firewalls that must be "inline" and require cutting cables, NetFoundry can be deployed in parallel. Start with one machine and scale as you go.
- **Operational Continuity**
  Avoid the dreaded "cut-over" downtime. NetFoundry microsegmentation solution can be deployed with minimal disruption to operations.
- **Multi-Vendor Underlay Support**
  NetFoundry solution is completely agnostic of the underlay network and runs on COTS hardware. It is truly hardware-agnostic.
- **No Re-IPing Required**
  Because NetFoundry handles NAT and overlapping IP spaces in the software overlay, you can keep your legacy IP addresses exactly as they are.
- **Easy for OT Engineers**
  The NetFoundry console uses business logic (e.g., "Allow HMI-A to talk to PLC-B") rather than complex CLI networking commands. This enables self governance by OT engineers without requiring deep networking knowhow.
- **Automation and Scale**
  Manual certificate, firewall, and rule management does not scale to large industrial estates. Identity and policy lifecycle automation are essential for large environments.
- **Strong Zero Trust Everywhere**
  Whether it is Secure Remote Access for vendors, Edge-to-Cloud telemetry, Cloud-to-Edge Control or Internal Segmentation, the same platform handles every OT, IT-OT convergence use case.

What Good Looks Like

What "good" looks like in modern OT is not a wholesale redesign of the plant network, but a plant-owned, identity-first overlay that enforces egress-only connectivity, default-deny at the cell, and explicit, policy-defined conduits for every approved interaction. Human users, vendors, and headless systems are governed through a unified policy model, with time-bound access, local kill-switch control, and audit-ready records. The result is a practical target state that supports IEC/ISA 62443-3-3 system requirements while allowing innovation to scale without surrendering plant authority or forcing repeated changes to the underlay.

Conclusion and Call to Action

The mandate of IEC/ISA 62443-3-3 is clear, but the path to compliance should not be a financial and operational trap. While the Purdue Model remains useful as a classification and risk lens, the modern connectivity and security enforcement should move to an 'identity' bound overlay that can be independently governed by OT engineers. Trying to "secure the underlay" is an outdated, hardware-centric mindset that does not fit the realities of the modern OT environment.

By moving to a **Software-Defined Zero Trust Overlay**, organizations can simplify and strengthen how they achieve and demonstrate IEC/ISA 62443-3-3 system requirements and target security levels. NetFoundry also produces operational artifacts - including policies, logs, and access records that can support the customer's IEC/ISA 62443 evidence preparation, internal governance, and broader system assessment activities.The result is a practical target state that supports IEC/ISA 62443-3-3 system requirements while allowing innovation to scale without surrendering plant authority or forcing repeated changes to the underlay.

Next Steps for IEC/ISA 62443 Compliance

1. **IDENTIFY** your most critical L2 broadcast domains.
2. **DEPLOY** a NetFoundry ZLAN instance on an existing Industrial PC (IPC) or COTS hardware.
3. **DEFINE** your first secure conduit.
4. **VALIDATE** How NetFoundry can simplify governance, and accelerate IEC/ISA 62443 alignment

Contact NetFoundry for a Technical Deep Dive into your OT Architecture.

About NetFoundry

NetFoundry helps businesses secure connectivity between components of their widely distributed workloads, across any set of networks. Founded by the inventors and maintainers of the world's most used open source zero trust software, OpenZiti, NetFoundry's Identity-First Connectivity™ enables zero trust connectivity with no VPNs, no open inbound ports, and no firewall changes. Software and IoT solution providers use it for secure communications with workloads at their customers' sites. Enterprises secure access to their APIs and agentic AI services in order to avoid any opening that can be leveraged by an attacker. They also use NetFoundry to simplify the operation of hybrid IT/OT segmentation and enable identity-based microsegmentation.

Learn more at www.netfoundry.io

NetFoundry