Zero Trust for OT

Applying Zero Trust Principles to Industrial Environments

OT Security Learning Series

Document 308 | January 2026

Contributors: Matthias Niedermaier

Created with AI assistance

LEARNING RESOURCE

Contents

1 Introduction

Information

Zero Trust is a security model based on the principle of "never trust, always verify." Rather than assuming that everything inside a network perimeter is safe, Zero Trust requires continuous verification of every user, device, and connection. Applying these principles to OT environments requires careful adaptation to address real-time requirements, legacy systems, and safety constraints.

Traditional OT security relied heavily on air gaps and perimeter defenses. Once inside the OT network, devices and users were implicitly trusted. This model has proven inadequate as IT/OT convergence, remote access, and sophisticated attacks have eroded the effectiveness of perimeter-based security.

Zero Trust offers a path forward, but OT environments cannot simply adopt IT Zero Trust architectures. The principles must be adapted to work within the constraints of industrial control systems.

2 Zero Trust Principles

2.1 Core Tenets

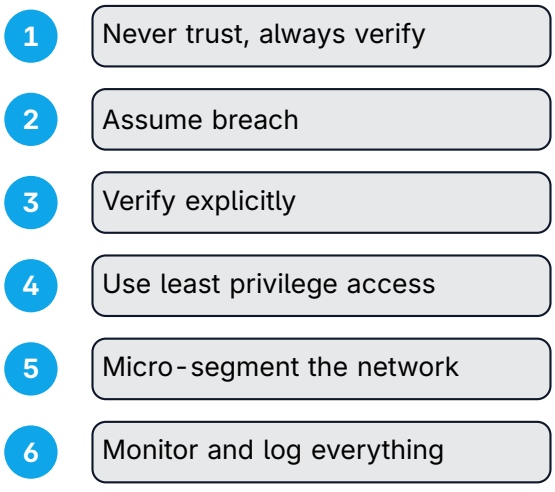

Figure 1: Core Zero Trust principles

2.2 Traditional vs Zero Trust

Aspect	Traditional Model	Zero Trust Model
Trust Boundary	Network perimeter	No implicit trust boundary
Internal Traffic	Trusted by default	Verified for each request
Access Control	Network location-based	Identity and context-based
Segmentation	Flat or minimal zones	Micro-segmentation
Verification	One-time at perimeter	Continuous verification
Breach Assumption	Prevent perimeter breach	Assume breach occurred

Table 1: Traditional perimeter security vs Zero Trust

3 OT-Specific Challenges

Warning

Zero Trust was developed for IT environments with modern devices, frequent updates, and tolerance for latency. OT environments have fundamentally different constraints that require adapted approaches rather than direct implementation of IT Zero Trust solutions.

3.1 Technical Constraints

Constraint	Impact on Zero Trust
Legacy Devices	Cannot support modern authentication or agents
Real-Time Requirements	Verification latency may be unacceptable
Proprietary Protocols	May not support encryption or authentication
Safety Systems	Cannot tolerate disruption from security controls
Long Lifecycles	Devices may be in service for 15–25 years
Limited Compute	PLCs/RTUs cannot run security software

Table 2: OT constraints affecting Zero Trust implementation

3.2 Operational Constraints

- **Availability Priority** – Safety and uptime take precedence over security
- **Change Resistance** – Production systems resist frequent modifications
- **Testing Limitations** – Cannot easily test security changes on live systems
- **Skill Gaps** – OT staff may lack cybersecurity expertise
- **Vendor Dependencies** – Changes may void warranties or support

4 Zero Trust Architecture for OT

4.1 Adapted Model

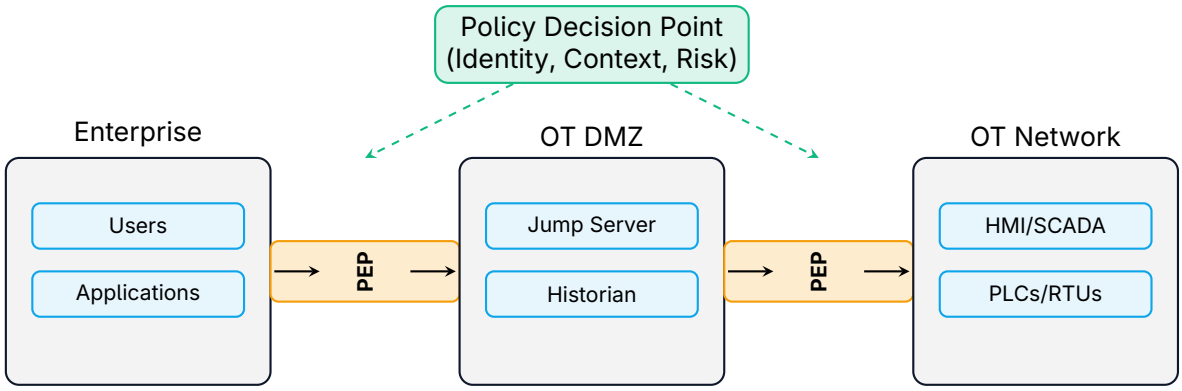

Figure 2: Zero Trust architecture adapted for OT

4.2 Key Components

- **Policy Decision Point (PDP)** – Evaluates access requests against policies
- **Policy Enforcement Point (PEP)** – Enforces decisions at zone boundaries
- **Identity Provider** – Authenticates users and devices
- **Device Inventory** – Maintains authoritative asset database
- **Monitoring System** – Provides context for access decisions

5 Implementation Strategies

5.1 Start at the Boundaries

For OT environments, implement Zero Trust progressively from outside in:

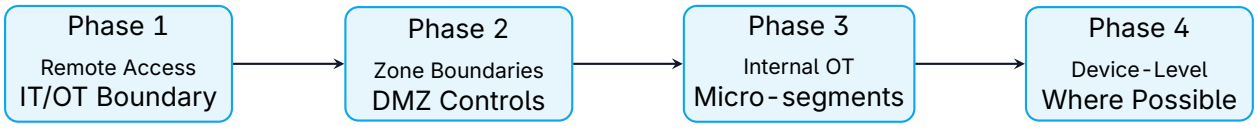

Figure 3: Phased Zero Trust implementation for OT

5.2 Identity and Access

Control	OT Implementation
User Authentication	MFA for all remote and administrative access
Device Authentication	802.1X where supported; MAC-based for legacy
Service Accounts	Vaulted credentials with just-in-time access
Vendor Access	Explicit approval, time-limited, fully monitored
Local Accounts	Minimize; use centralized identity where possible

Table 3: Identity controls for OT Zero Trust

5.3 Network Micro-Segmentation

Divide the OT network into small, controlled segments:

- **By Function** – Separate control, safety, and monitoring systems
- **By Criticality** – Isolate high-impact systems more strictly
- **By Process** – Segment different production lines or units
- **By Vendor** – Contain vendor-specific systems

Tip

Use industrial firewalls or VLANs with ACLs to create micro-segments. Allow only the specific protocols and connections required for each system to function. Default deny all other traffic.

5.4 Continuous Monitoring

Zero Trust requires visibility to make informed access decisions:

- **Network Traffic** – Baseline normal communications, detect anomalies
- **Device Behavior** – Monitor for unexpected process changes
- **User Activity** – Log all actions, especially privileged operations
- **Asset State** – Track configuration changes and patch status

6 Handling Legacy Systems

Critical

Many OT devices cannot participate directly in Zero Trust verification. They lack the capability for modern authentication, encryption, or agent installation. These devices require compensating controls rather than direct Zero Trust implementation.

6.1 Compensating Controls

Legacy Limitation	Compensating Control
No authentication	Network isolation, strict firewall rules
No encryption	Encrypt at network layer (IPsec, MACsec)
No agent support	Network-based monitoring and detection
Static credentials	Segment tightly, monitor all access
No logging	Capture traffic at network level

Table 4: Compensating controls for legacy OT devices

6.2 Protect the Path

When devices cannot verify themselves, protect access to them:

- Authenticate users/devices that *access* the legacy system
- Encrypt the *network path* to the legacy system
- Monitor all *traffic* to and from the legacy system
- Restrict which systems can *communicate* with it

7 Safety Considerations

7.1 Safety System Exemptions

Warning

Safety instrumented systems (SIS) may require exemptions from certain Zero Trust controls. A security measure that could delay or prevent a safety shutdown is unacceptable. Document these exemptions and implement alternative protections.

- Do not place inline security controls that could fail-closed on safety paths
- Use passive monitoring rather than active blocking for safety traffic
- Ensure security failures do not cascade to safety systems
- Test thoroughly in non-production environments

7.2 Fail-Safe Design

Zero Trust controls in OT must fail safely:

- **Fail-Open for Safety** – Safety-critical communications continue if controls fail
- **Graceful Degradation** – Loss of verification reduces access, doesn't halt operations
- **Manual Override** – Operators can bypass controls in emergencies (with logging)

8 Maturity Progression

Level	Characteristics	OT Focus Areas
Initial	Perimeter-focused, implicit trust	Asset inventory, network visibility
Developing	Zone segmentation, some verification	IT/OT boundary controls, MFA
Defined	Micro-segmentation, explicit policies	Internal OT segmentation, PAM
Managed	Continuous verification, automation	Behavioral monitoring, SOAR
Optimized	Adaptive, risk-based decisions	AI/ML anomaly detection

Table 5: Zero Trust maturity levels for OT

Key Point

Most OT environments should target the "Defined" level as a realistic goal. Full Zero Trust implementation at Level 0/1 (field devices) is often impractical with current technology. Focus verification efforts at zone boundaries and human access points.

9 Summary

Key Takeaways

- **Adapted Approach:** Zero Trust principles apply to OT, but implementation must account for legacy systems, real-time requirements, and safety constraints
- **Never Trust:** Eliminate implicit trust based on network location; verify every access request
- **Start at Boundaries:** Implement Zero Trust progressively from remote access inward; IT/OT boundary first
- **Micro-Segment:** Divide OT networks into small, controlled zones with explicit allow rules
- **Compensating Controls:** Protect legacy devices that cannot participate in verification by controlling access paths
- **Safety First:** Never compromise safety system availability; use fail-safe designs and document exemptions

10 Further Reading

Standards and Guidelines

- **NIST SP 800-207** – Zero Trust Architecture
  https://csrc.nist.gov/pubs/sp/800/207/final
- **CISA Zero Trust Maturity Model** – Implementation guidance
  https://www.cisa.gov/zero-trust-maturity-model

Resources

- **NIST SP 800-82** – Guide to ICS Security
  https://csrc.nist.gov/pubs/sp/800/82/r3/final
- **IEC 62443** – Industrial automation security standards
  https://webstore.iec.ch/publication/7029

Books

- Kindervag – *Build a Zero Trust Network* (O'Reilly)
- Knapp & Langill – *Industrial Network Security* (Syngress)

Part of the OT Security Learning Series