SOLUTION BRIEF

Zero Trust for OT Security

A Practical Path to Cyber Resilience in Critical Infrastructure with CoIP® Platform

zentera™

Executive Summary

Power generation, manufacturing, oil and gas, healthcare, and other critical infrastructure operators face a powerful but perilous convergence of IT and operational technology (OT). Digital transformation and industrial IoT initiatives drive real-time data exchange, remote monitoring, and analytics – yet these same connections introduce unprecedented cyber risk. Traditional air-gapped strategies can't keep pace with modern threats, and simple firewall segmentation often isn't enough.

This white paper explores:

- Why industrial networks are vulnerable as IT and OT merge
- The limits of perimeter-based security and why adding more firewalls isn't the answer
- How Zero Trust—specifically a "Zero Trust DMZ"—can protect critical assets without disrupting operations
- Zentera's unique, software-defined approach to implementing Zero Trust across legacy-rich industrial environments

Our goal is to arm you with **actionable insights** and a **practical roadmap** to safeguard mission-critical operations, leveraging NIST-aligned Zero Trust strategies tailored for OT.

Potential Risks of OT Attacks

- Financial losses from production downtime and lost work in progress
- Costs to remediate and recover
- Loss of customer confidence and brand image
- Safety and environmental hazards
- Fines, lawsuits, and liability
- Bad publicity with shareholders and stakeholders
- Non-renewal of insurance coverage

The IT-OT Convergence Challenge

A New Era of Risk

For decades, OT environments were physically air-gapped from external networks. Today, demands for efficiency, remote access, and data analytics are eroding these boundaries, creating a convergence of IT and OT that greatly expands the attack surface. Even a single compromised credential on the corporate side can become a pivot point for attackers to access industrial control systems.

Key Drivers of OT Connectivity

Real-Time Data Analytics: Operations teams rely on up-to-the-minute production data to optimize processes.
Remote Vendor Access: OEMs and support teams routinely connect into ICS for monitoring, diagnostics, and maintenance.
Digital Transformation: Cloud-based applications, edge computing, and IoT sensors create constant data flows between corporate IT and factory floors.

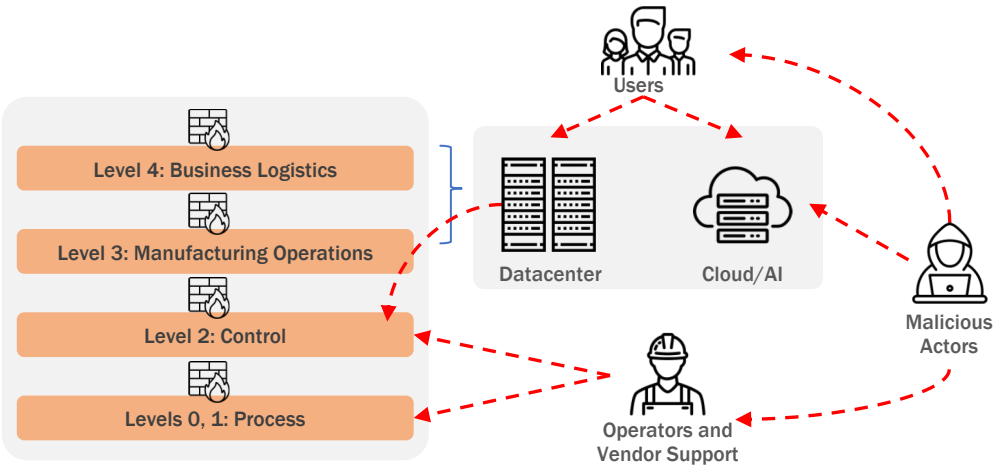
ICS Devices: Critical and Vulnerable

Industrial control systems (ICS) often run on specialized or legacy platforms that cannot be easily patched or upgraded. They were designed for reliability and safety, not security. Introducing modern security controls – like frequent patches, endpoint agents, or encryption—poses operational and compatibility challenges.

Perimeter Defenses Under Pressure

Firewalls and network segmentation still have value, but the intricate connectivity required by converged IT-OT networks can quickly undermine a perimeter-centric model. A single misconfiguration, rogue device, or malicious insider can bypass traditional defenses, opening the door for lateral movement and sabotage.

Reality Check: Achieving secure IT-OT connectivity is no longer optional. It must be done **in a way that doesn't compromise availability or safety** – and that's where Zero Trust can excel.



IT/OT with Purdue Reference Model Segmentation

Increasing connectivity to remote operators and business applications exposes OT environments to risks posed by determined actors

Zero Trust for Industrial Security

Breaking the "Air Gap" Illusion

Many organizations rely on partial or notional "air gaps," believing ICS networks remain insulated. However, any data flow or remote access channel essentially bridges that gap. Attackers exploit these connection points, leveraging vulnerabilities in IT or supplier systems to move laterally into OT environments.

Core Zero Trust Principles

Zero Trust assumes nothing on the network is safe by default. Every user, device, and process must be continuously authenticated, authorized, and encrypted based on identity, context, and policy. In OT environments, the key outcomes are:

Least Privilege Access

Operators, vendors, and applications only interact with the specific ICS resources they need.

Micro-Segmentation

If a breach occurs in one segment, it cannot automatically spread to the rest.

Continuous Validation

Ongoing checks of identity and device posture ensure that if something changes – like a suspicious action – access can be immediately revoked.

The Payoff for OT

Zero Trust places security closer to the device, user, or application, dramatically shrinking the attack surface and limiting lateral movement.

Importantly, modern overlay-based solutions, like Zentera's, make adoption feasible without wholesale network re-designs.

This makes it possible to harden existing, legacy OT infrastructure against cyber-physical threats, making the operations resilient in the fact of threats.

Even when the network is compromised, Zero Trust keeps assets and resources cloaked, protecting operations

Why More Firewalls Can't Solve ICS Challenges

Complexity and Scalability

Simply layering additional firewalls around every ICS device or subnet sounds logical but quickly becomes unmanageable. Each firewall requires configuration ("punching holes" for specific ports, protocols, and addresses), and each newly connected device and service requires more rules. It's not unusual to see networks with thousands – sometimes tens of thousands – of firewall rules, making them virtually impossible to maintain or audit. Often a ping becomes the best way to know if connectivity exists.

Lateral Traffic Overload

Modern ICS environments don't just communicate vertically (to external networks) but also laterally between equipment on the factory floor, across different production lines, or between control systems and data historians. When you deploy firewalls internally, each pair of communicating systems may need dedicated rules. This can cause the number of rules – and the effort to maintain them – to explode exponentially, resulting in massive and costly operations.

Limited Visibility into Identity

Firewalls primarily make decisions based on packet headers (e.g., IP addresses and ports). They can't inherently recognize the user, device, or specific software process generating traffic. If an unauthorized user obtains legitimate network credentials or spoofs an approved IP address, the firewall alone cannot discern the difference. That leaves your systems vulnerable to lateral movement by adversaries who appear to be "trusted" or "inside."

Conclusion: Firewalls Are Necessary But Not Sufficient

While perimeter firewalls remain a key line of defense, they cannot deliver the fine-grained, identity-driven controls that modern OT security demands. Zero Trust overcomes these shortfalls by enforcing policy at a higher level—around individual assets, user identities, and applications, rather than just network addresses.

Zentera's Distinctive Approach

Bridging IT and OT Without Ripping Out Networks

Zentera's CoIP® (Cyber over IP) Platform implements Zero Trust as a secure overlay, abstracting security from the underlying network infrastructure. This approach provides microsegmentation and identity-based access controls without forcing you to re-plumb networks, rewrite IP addresses, or install software to sensitive ICS devices.

Core Components

Microsegmentation Gatekeepers (MSG): Dedicated appliances that deploy inline to enforce Zero Trust policies, creating isolated *Virtual Chambers* for assets, lines, or entire subnets.

zLink Agents: Lightweight agents that enforce Zero Trust policies from within the operating system of a VM, bare metal server, or cloud instance – as close as possible to the applications and data being protected.

zCenter Orchestrator: A centralized policy engine that maps user and device identities to allowed resources.

The CoIP Overlay Network: End-to-end encryption with continuous identity verification across IT-OT boundaries to defeat snooping and spoofing.

What Sets Zentera Apart

Agent + Agentless Flexibility

Attach a small agent if possible – or protect unpatchable, legacy PLCs via a MSG that enforces Zero Trust right on the device perimeter.

On Demand "Zero Trust DMZ"

Instantly create a DMZ-like boundary around a critical asset or subnet. Only explicitly authorized users and applications can reach inside.

NIST Alignment

Built to mirror NIST SP 800-207 guidelines for continuous monitoring and adaptive access control.

No Forklift Upgrades

Maintain production uptime without redesigning IP schemes or physically relocating devices.

Support for Legacy ICS Devices and Networks

Even outdated devices that can't be patched or run agents remain protected behind a Zentera gateway.

Why a "Zero Trust DMZ" Matters for OT – and How to Build One

Evolving the Traditional Perimeter DMZ

Legacy IT architectures use a DMZ to separate external-facing services from internal networks. Zentera's "Zero Trust DMZ" applies that concept at a finer-grained level for critical OT environments:

Localized Security Perimeters

Place a Microsegmentation Gatekeeper in front of a cluster of machines, or even a single system, to create a virtual DMZ that enforces security policies for traffic crossing the boundary.

Minimal Disruption

No need to reinvent network topology; the gateway enforces identity-based access for every traffic flow.

Scalable, Adaptive Coverage

Deploy as many Zero Trust DMZs as needed. Each environment can expand, contract, or shift without major operational hurdles.

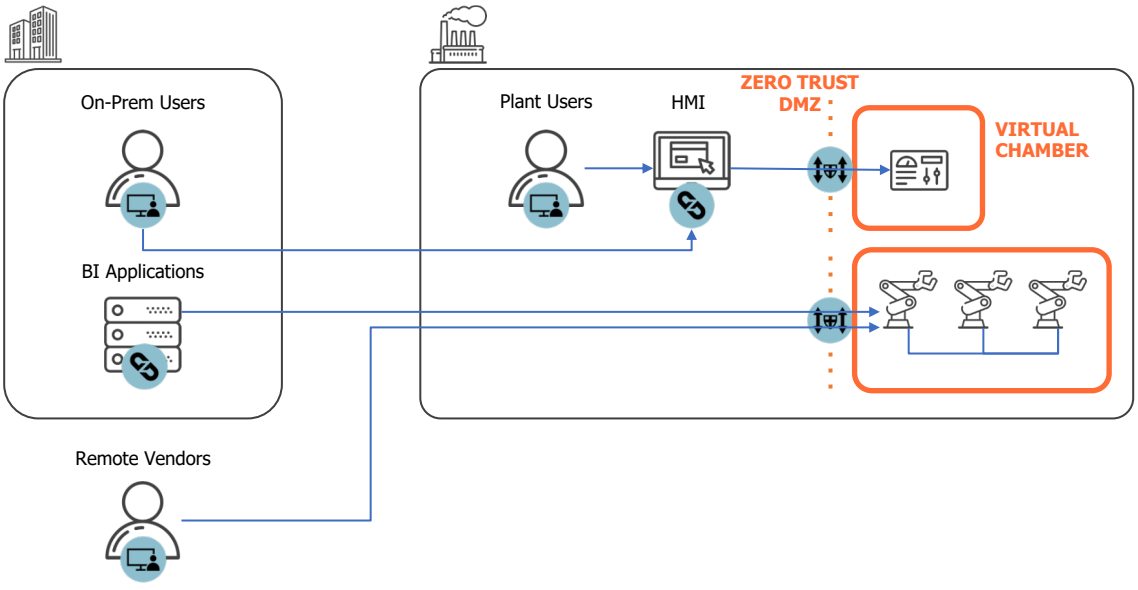
Real-World Use Cases

SCADA Systems: Cloak SCADA servers behind an MSG, ensuring only authenticated engineers or applications can reach them.

Vendor Access: Provide third-party technicians strictly limited paths to specific controllers, sparing the rest of the ICS from unnecessary exposure.

Brownfield Devices: Shield obsolete line equipment behind a gatekeeper that allows only the legitimate ICS traffic they need to function.

By replicating this Zero Trust DMZ concept wherever necessary, you avoid the pitfalls of large, monolithic firewall configurations and maintain precise, identity-driven control over who (or what) accesses your most sensitive assets.



Implementation Framework and Best Practices

Identify Crown Jewels and High-Risk Zones
Start by mapping out key ICS systems that pose the greatest risk if compromised—these become the first candidates for Zero Trust protection.

Establish Identity and Access Requirements
Define user roles, device types, and required services. Use role-based policies that align with operational workflows to avoid over-restriction or confusion.

Start with a Pilot
Select a limited-scope ICS environment (e.g., a single production line or SCADA server). Deploy Zentera's CoIP Platform, and then install agents or deploy Microsegmentation Gatekeepers to cloak target systems and continuously enforce user, device, and application authentication.

Scale Incrementally
After success with the pilot, replicate the approach for broader coverage (additional lines, substations, or vendor access points). Zentera's overlay model accelerates each subsequent deployment.

Integrate with Existing Security Tools
Leverage the CoIP Overlay to start reducing firewall complexity and improve maintainability. Feed logs from Zentera into your SIEM for unified alerting and incident response.

Refine Continuously
Collect telemetry from gateways, watch for anomalies, and adjust policies to evolving operational and threat landscapes.

- Install CoIP Platform
- Onboard servers with zLink agents and devices with Micro-Segmentation Gatekeeper

- Create Zero Trust DMZ
- Learn existing traffic and define Zero Trust policies
- Turn on policies in Detection mode

- Enforce policies in Prevention mode
- Monitor logs
- Refine policies as needed

Conclusion and Next Steps

Securing IT-OT convergence is challenging yet inescapable. The old "air gap" assumptions and perimeter-centric approaches are no match for modern threats, and simply stacking more firewalls around ICS assets leads to complexity and blind spots. Zero Trust, built on identity-driven access and micro-segmentation, offers a robust, scalable alternative—one that can align seamlessly with demanding industrial requirements for reliability and uptime.

Zentera's CoIP Platform delivers:

- Rapid microsegmentation using overlays
- Agentless Protection for unpatchable or legacy ICS devices
- On-Demand Zero Trust DMZ capabilities that minimize complexity
- NIST 800-207 Alignment for continuous monitoring and adaptive access

Next Steps

- Assess your ICS environment for high-risk assets and connectivity paths.
- Pilot a Zero Trust DMZ deployment around a critical ICS system.
- Expand across additional lines, facilities, or operational zones once proven.
- Optimize over time by refining policies, layering with existing defenses, and scaling coverage as your digital transformation advances.

Ready to protect your industrial operations?

Contact Zentera to start your Zero Trust journey. We'll help you implement fast, effective security for both IT and OT—without re-plumbing networks or disrupting production.

About Zentera

Zentera Systems is the leader in Zero Trust Security solutions for the digitally-transformed enterprise. Founded by experts in networking, security, and remote access, we offer award winning Zero Trust networking, security, and multi-cloud connectivity that overlays any fragmented infrastructure and deploys rapidly on premises or as a service.

Our global enterprise customers and network of partners use our products to secure employee and third-party access, protect against data leaks, and instantly defend applications in complex hybrid and IT/OT environments. Based in Silicon Valley, we have received numerous recognitions, including Cool Vendor for Cloud Security by Gartner.

www.zentera.net
sales@zentera.net
+1 (408) 436-4811

zentera™

Copyright© 2025 Zentera Systems, Inc. All rights reserved. Zentera®, Zentera CoIP®, CoIP®, and certain other marks are registered trademarks of Zentera Systems, Inc., in the U.S. and other jurisdictions, and other Zentera names herein may also be registered and/or common law trademarks of Zentera. All other product or company names may be trademarks of their respective owners.