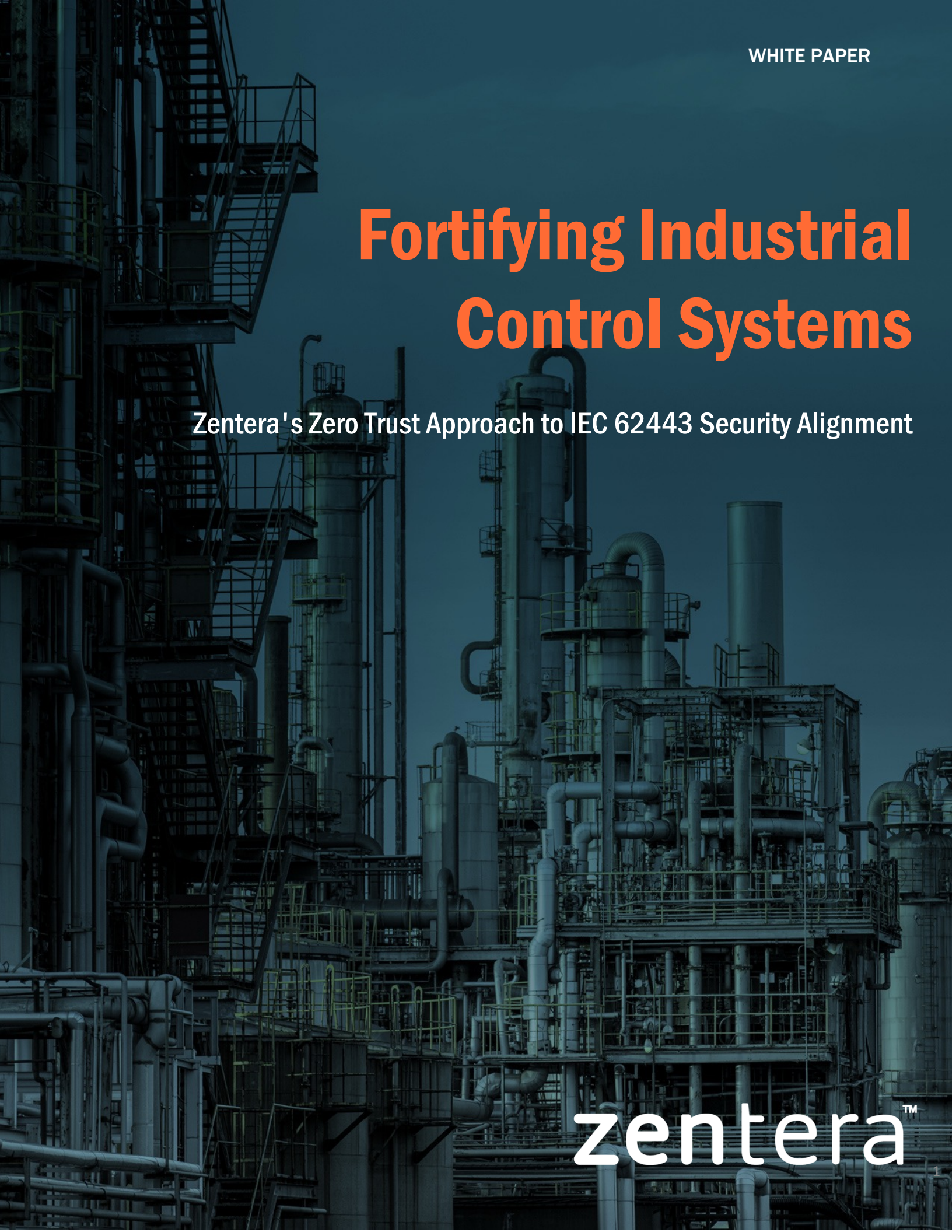


WHITE PAPER

Fortifying Industrial Control Systems

Zentera's Zero Trust Approach to IEC 62443 Security Alignment

zentera™

Executive Summary

Industrial enterprises today face unprecedented cybersecurity risks as state-sponsored threat groups and ransomware gangs increasingly target operational technology (OT) environments. Recent campaigns like **Volt Typhoon** – a Chinese state-backed group – have pre-positioned in IT networks with the goal of pivoting into OT systems and disrupting critical infrastructure. Meanwhile, ransomware attacks on manufacturers and utilities have surged by nearly **87% year-over-year**, with over **80 distinct threat groups** now actively targeting industrial control systems (ICS). The consequences are dire: weeks of production downtime, multi-million dollar losses, and even safety and environmental incidents when attackers compromise ICS processes.

To address this evolving threat landscape, organizations are turning to the **ISA/IEC 62443** standards – the global benchmark for industrial cybersecurity – which provide a comprehensive, risk-based framework for securing Industrial Automation and Control Systems (IACS).

However, achieving alignment is challenging in practice. Surveys indicate many manufacturers believe they have not fully addressed IEC 62443 requirements, largely due to legacy equipment constraints, flat networks, and minimal downtime tolerance. Traditional security approaches like perimeter firewalls and air-gaps are insufficient against modern threats and often conflict with operational continuity.

Zero Trust architecture has emerged as a revolutionary approach to fortify industrial control systems without disrupting operations. By enforcing "never trust, always verify" at every connection – using identity-based authentication, microsegmentation of networks, and continuous monitoring – Zero Trust directly aligns with IEC 62443's core principles of defense-in-depth and zone-based security. Importantly for OT environments, a well-implemented Zero Trust solution can be overlaid on existing networks agentlessly, extending protection to unmodifiable legacy PLCs and SCADA devices.

Zentera's Zero Trust platform exemplifies this modern approach. It overlays advanced security controls on brownfield industrial networks (no ripping-and-replacing of infrastructure) and maps logically onto IEC 62443's zones and conduits model. Key capabilities include:

- Application-Level Microsegmentation: Creating virtual "chambers" around ICS assets to contain attacks and enforce least privilege access
- Identity-Based Access Control: Requiring strong authentication for every user and device connection – even legacy OT endpoints – via integration with corporate identity systems and multi-factor authentication
- Agentless Protection: Using inline enforcement devices (Gatekeepers) that don't require installing software on legacy controllers, thus securing decades-old equipment that cannot be modified
- End-to-End Encryption: Automatically encrypting and integrity-checking all ICS traffic over the overlay, protecting protocols like Modbus and OPC UA that lack native security

- Unified Monitoring & Response: Logging every session and policy decision for full visibility and compliance audit trails, and enabling rapid isolation of anomalies in real time

This white paper critically evaluates the current state of ICS security and Zentera's Zero Trust architecture through the lens of a CISO or OT security director.

It highlights how Zero Trust can directly satisfy the seven IEC 62443 Foundational Requirements (FR1–FR7) without costly downtime, and how it provides compelling business benefits – from preventing catastrophic production outages to ensuring regulatory compliance and protecting corporate reputation.

We compare Zentera's approach with traditional Purdue-model security, identify areas to sharpen the messaging for high-level stakeholders, and offer guidance on making the implementation actionable and risk-driven.

By adopting a Zero Trust architecture aligned with IEC 62443 and NIST SP 800-207, industrial enterprises can drastically improve their cyber resilience.

They can reduce the risk of costly breaches by 75% or more, avoid downtime that can cost millions per day, and safely embrace digital transformation (Industrial IoT, remote operations) on a secure foundation. With regulators and threats escalating, the time to fortify ICS with Zero Trust is now.

1. The Industrial Cybersecurity Imperative

Evolving Threat Landscape for OT

Unlike typical IT breaches, attacks on industrial systems carry **physical and financial consequences** that can be devastating. CISOs and OT security leaders must contend with threats that directly impact **safety, production, and compliance**:

- **State-Sponsored Intrusions**: Advanced Persistent Threat (APT) groups are regularly targeting manufacturing, energy, and critical infrastructure. The XENOTIME group, known for attacks on oil & gas, has expanded into manufacturing. Malware like INDUSTROYER and TRISIS demonstrate the capability to disrupt grid operations or sabotage safety systems. Most recently, Volt Typhoon was found deeply embedded in U.S. critical infrastructure IT networks (communications, energy, transport) with the aim to pivot into OT and cause disruption during a geopolitical crisis. These stealthy intrusions often use "living off the land" tactics and valid credentials, evading detection for months or years.

- **Ransomware and Cybercrime**: Criminal groups have increasingly moved from data theft to "lock-and-impact" ransomware in industrial sectors. Recent attacks caused multi-week shutdowns in automotive and chemical plants. Dragos reported an 87% spike in ransomware attacks on industrial orgs in 2024, with at least 80 groups now pursuing OT targets. The average cost of an OT ransomware incident exceeds $5 million, and recovery often takes 3–5× longer than for IT-only incidents due to proprietary control systems. In one case, a major building automation firm spent $27 million in cleanup costs after a ransomware breach.

- **Supply Chain Vulnerabilities**: Third-party vendors and contractors are a frequent weak link. Compromised VPN credentials or remote access tools used by maintenance providers have led to breaches where attackers bypass perimeter defenses. For example, insecure remote connections contributed to the Colonial Pipeline incident and other ICS intrusions. TSA's cybersecurity directives now mandate measures like network segmentation and multi-factor authentication (MFA) for pipeline operators to curb this risk.

Operational Impact of OT Breaches

The fallout from an ICS security incident goes far beyond data loss. Consider a large manufacturing CISO's perspective: a cyber attack can result in physical equipment damage, safety incidents harming personnel, environmental releases violating regulations, loss of product quality control, and intellectual property theft (e.g., stolen formulas or production recipes). Business leaders also fear the financial hit from unplanned downtime, which can be on the order of $1–2 million per day in lost output for a big plant, not including contract penalties and recovery costs. Moreover, breaches can incur regulatory fines, lawsuits, and even affect insurance coverage renewal.

In critical infrastructure, national security concerns come into play, as underscored by joint government advisories treating OT cyber risks as "core business risks essential to national security".

2. IEC 62443 – The OT Security Standard

To counter these threats, industrial organizations look to the ISA/IEC 62443 series of standards, which provide a comprehensive blueprint for securing IACS. IEC 62443 is a risk-based framework with guidelines spanning from corporate risk management to technical controls. Key aspects include:

- **Holistic Security Lifecycle**: IEC 62443 defines processes for risk assessment (62443-3-2), security management systems (62443-2-1), and ongoing maintenance. It's not just about one-time fixes, but continual improvement.
- **Security Levels (SL1–SL4)**: The standards recognize different required rigor depending on threat scenarios – from basic malware protection (SL1) up to highly critical systems needing advanced APT defense (SL4).
- **Foundational Requirements (FR1–FR7)**: Seven categories of controls all IACS should implement: Identification & Authentication, Use Control (Least Privilege), System Integrity, Data Confidentiality, Restricted Data Flow (Segmentation), Timely Response, and Resource Availability. These map closely to classic IT security principles but are tailored for OT nuances.
- **Zones and Conduits Model**: A core IEC 62443 concept is dividing the system into security zones (grouping assets by criticality and trust level) with controlled conduits managing communications between zones. This is essentially the principle of network segmentation applied methodically to OT. A higher security zone (say, Safety Instrumented Systems) should only talk to a lower zone (site operations network) through restricted, well-monitored conduits.

The Alignment Gap

Despite its clear guidance, implementing IEC 62443 in brownfield environments is hard.

Common challenges include legacy devices with no built-in security, flat networks that lack any internal segmentation, very limited maintenance windows to install updates, and siloed IT/OT teams. We detail these obstacles next.

3. Brownfield Challenges in Achieving IEC 62443

Most industrial sites have evolved over decades, with processes running on legacy PLCs, distributed control systems (DCS), and older operating systems. Bringing such environments up to modern security standards can feel like changing the engines on a plane mid-flight. Key hurdles include:

- **Legacy Equipment Constraints**: Industrial equipment often has 15–25 year lifecycles and runs on proprietary OS or firmware. Many PLCs and controllers cannot support modern authentication or encryption, and patching them can require halting production (unacceptable in many cases). Shared passwords or even no authentication is common on these devices (violating FR1), yet upgrading them might mean multi-million dollar system replacements.

- **Flat, Unsegmented Networks**: Historically, OT networks were designed flat for easy data flow and high availability. Security zones didn't exist – all devices could often talk openly. Introducing VLANs or additional firewalls now means untangling poorly documented connections and interdependencies. Mis-segmentation could accidentally block needed communication, causing outages. As a result, many sites remain one big zone, making attack containment (FR5) nearly impossible with traditional means.

- **Operational & Cultural Realities**: In industrial settings, downtime is deadly to KPIs. Plants may only have a few hours of scheduled downtime per year, meaning security retrofits must be incremental and fail-safe. There is often resistance from operations teams who fear new security controls might disrupt the sensitive processes they manage. Additionally, finding staff who deeply understand both OT protocols and cybersecurity is difficult – many organizations lack a "translator" between IT security and OT engineering. This can lead to inertia or mistakes in applying IT-centric tools to OT.

- **Financial Justification**: Upgrading OT security can carry hefty costs with unclear ROI. Re-architecting networks or replacing legacy gear for security alone is hard to justify against production investments. Security budgets in OT are often a fraction of IT's, and every dollar competes with operations needs. CISOs need to frame these investments in terms of risk reduction and business continuity (e.g., avoiding a $50M incident) to get buy-in.

These constraints explain why a different approach is needed – one that meets security objectives without requiring massive infrastructure changes or downtime. This is where a Zero Trust overlay becomes compelling.

4. Zero Trust for ICS: A New Approach Aligned with IEC 62443

Zero Trust is a security model grounded in the idea that no user or device should be inherently trusted, even if inside the network perimeter. Every access request must be authenticated, authorized, and verified continuously. While Zero Trust originated in IT, it is increasingly seen as essential for OT as well, especially with IT/OT convergence eroding any true network air-gap.

Core Principles of Zero Trust in the OT Context

In practice, implementing Zero Trust in industrial networks involves:

- **Microsegmentation**: Breaking the network into small, isolated zones down to the level of individual critical devices or applications. This contains any attacker movement. In IEC 62443 terms, it operationalizes the zone & conduit model with fine granularity. Each "conduit" is governed by strict policy – nothing talks to anything unless explicitly allowed.
- **Strong Identity and Authentication Everywhere**: Requiring every human operator, engineer, or remote vendor, as well as every machine or software process, to prove its identity before any communication. For humans, this means integration with Active Directory/LDAP, multi-factor authentication, and role-based access tied to job function. For devices, it may involve certificates or unique credentials per device (to avoid shared passwords in PLCs, satisfying FR1). Zero Trust assumes an attacker might already have a foothold, so it shuts down lateral movement by preventing credential reuse and enforcing least privilege.
- **Continuous Monitoring and Verification**: Unlike the "set and forget" of legacy firewalls, Zero Trust requires ongoing analysis of traffic patterns and user behavior. Anomalies trigger alerts - and potentially, automated containment. In OT, this means keeping detailed logs of every access to critical PLCs, with context like who, when, and from where. Solutions must integrate with SIEMs and OT security monitoring tools for correlation (addressing FR6 for timely response).
- **Assume Breach and Minimize Impact**: Design the network and controls under the assumption that some malware or adversary will get in. Therefore, put in place measures so that a compromise of one node does not compromise the whole system. This leads to concepts like "Virtual Chambers" around crown jewel assets (we cover this shortly) and hardened jump hosts. Essentially, any path an attacker might use is restricted, watched, and can be shut down if misused.
- **Design for Resilience**: In OT, Zero Trust must be implemented in a way that does not break operations (aligning to FR7 on availability). This means fail-safe or fail-open mechanisms on security devices (so if they fail, they don't stop the plant), non-intrusive deployment (no changes to legacy device configuration), and performance transparent encryption that doesn't add unacceptable latency to control traffic. As NIST SP 800-207 notes, a Zero Trust architecture for OT may need hybrid approaches – applying strict controls where feasible, but accommodating essential functions that can't be interrupted.

5. Zentera's Zero Trust Architecture Overview

Zentera's Zero Trust platform was built with these OT requirements in mind, offering a software-defined overlay (the CoIP® Platform) that can be deploys organically on top of existing networks.

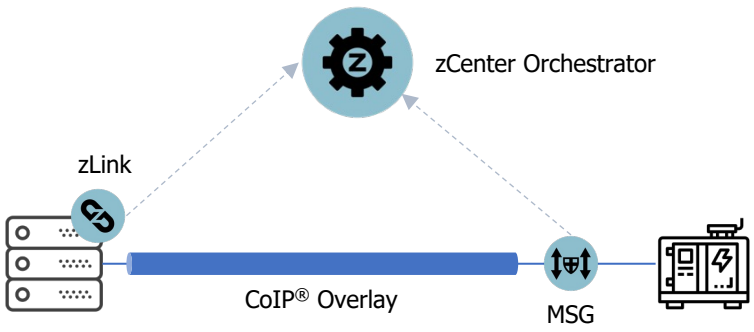
Below we break down its key components and how they map to the needs discussed:

zCenter Orchestrator: The brains of the system, this centralized controller defines security policies (who can access what, under what conditions) and enforces identity integration. It ties into existing enterprise IAM (e.g., Active Directory, SAML SSO) to leverage current user accounts and roles, so OT security aligns with corporate identity governance. zCenter also logs all access attempts, providing an audit trail for compliance.

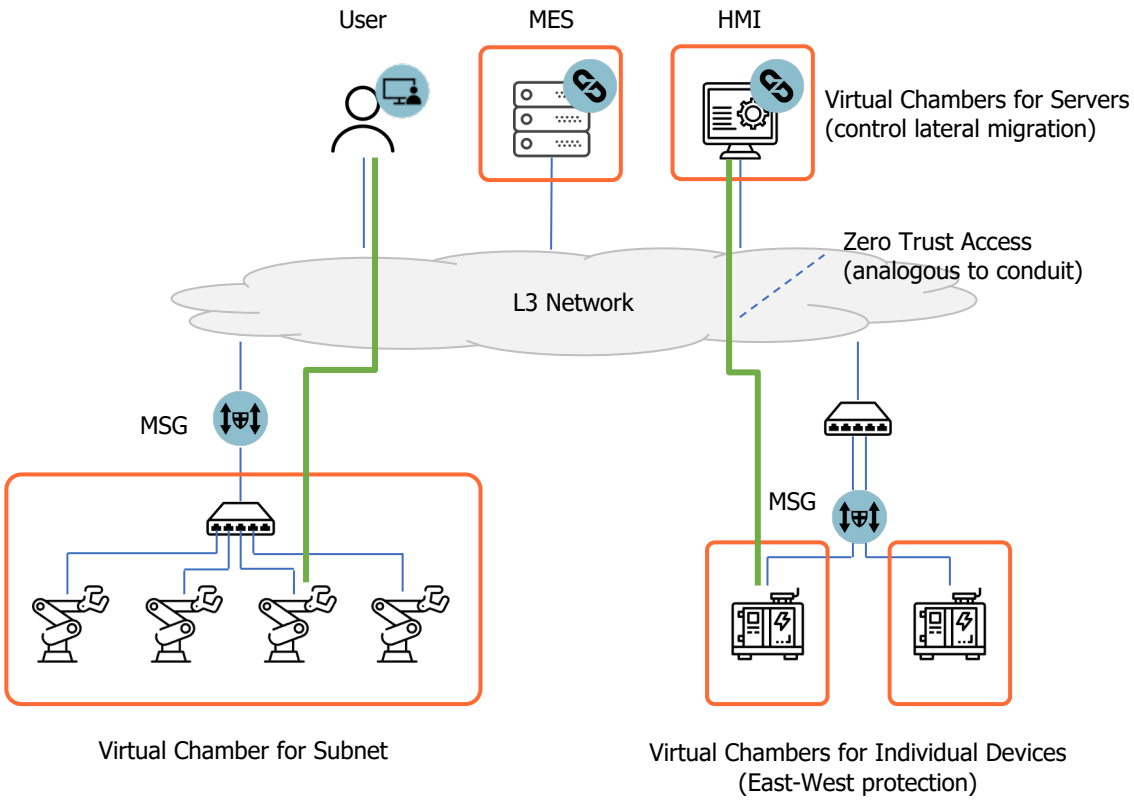
CoIP® Overlay: This is a virtual network fabric that encrypts all traffic and brokers connections between authenticated entities. Think of it as a secure tunnel that wraps around each session, ensuring communication integrity (FR3) and confidentiality (FR4) even if the underlying network is insecure. The overlay routes connections through an "intermediate system" as per NERC CIP guidance (an architecture akin to an air-gap in effect). Importantly, it's transparent to existing infrastructure – no need to re-address devices or rewire networks; the overlay can use the same IPs and simply control the flows on top.

- **Microsegmentation Gatekeeper (MSG)**: A hardware or virtual appliance that sits inline with critical assets (like a PLC network segment or a cluster of servers). It enforces per-workload access control at a very granular level. For example, an MSG can be placed in front of an unpatchable Windows NT-based HMI system; it will cloak that HMI so nothing can talk to it except what policy allows (e.g., only trusted RDP sessions from an authorized user on a trusted engineering workstation). Because the Gatekeeper operates at line speed and has a fail-open hardware bypass, it can be introduced without affecting uptime – if it loses power, it simply lets traffic through to avoid downtime (while alerting the NOC). Agentless Protection: This design means even if a device can't run an agent, it is protected by the gatekeeper's policing of traffic.

- **zLink Software Agent**: For systems where software can be installed (modern Windows/Linux servers, VMs, or cloud workloads that interface with OT), zLink serves as a host-based enforcement point. It provides similar microsegmentation and encryption at the source, ideal for securing OT data centers or new IIoT devices that run standard OS. zLink and the Gatekeeper both enforce the same policies orchestrated by zCenter, giving unified control across both legacy and modern assets.



The combination of these elements allows creating "virtual chambers" around assets (like an MES server or a DCS controller) and strictly governed "conduits" between them via the overlay. Essentially, Zentera operationalizes the IEC 62443 zones and conduits concept: Virtual Chambers = zones; Zero Trust policies = conduits controlling data flows. This is achieved without physically rearchitecting the network, a huge benefit for brownfield deployment.



6. Key Advantages in Industrial Settings

Zentera's approach yields several advantages summarized below:

- **Non-Disruptive Implementation**: Because it's an overlay, you don't need to change IP addresses, routing, or switch configurations to deploy Zero Trust. For a 24/7 plant, this is crucial – new security measures can be introduced gradually and with minimal disruption to normal operations. Compare this to traditional segmentation which might require re-addressing subnets or inserting new firewall chokepoints (often involving downtime).

- **Agentless Legacy Protection**: Many OT systems simply cannot run security agents or even support modern protocols. Zentera's MSG provides a way to enforce authentication and traffic rules on those devices without touching them. For example, a legacy PLC with no user authentication can effectively be "wrapped" by the overlay which requires the user to authenticate at the gateway before any packets reach the PLC. This closes a critical gap and helps achieve FR1 (Identification & Authentication) on legacy equipment.

- **Protocol-Agnostic Security**: Traditional deep packet inspection might struggle with proprietary or timing-sensitive OT protocols (and could introduce latency). Zentera instead secures at the session layer, meaning it doesn't rely on protocol-specific parsing – any IP-based protocol (Modbus/TCP, OPC UA, Ethernet/IP, etc.) is automatically encrypted and controlled. This avoids breaking protocol operations while still ensuring confidentiality and integrity (fulfilling FR3 and FR4 for traffic that wasn't built with security).

- **Incremental, Risk-Based Rollout**: Zero Trust can be deployed incrementally. A recommended strategy is to start with the most critical or vulnerable assets (e.g., a safety system network or a high-value production line). Zentera supports this because you can begin with a couple of Gatekeepers and a small policy set, then expand zone by zone. This aligns with maintenance windows – secure one segment during a scheduled downtime, learn and adjust, then tackle the next, etc. It also aligns with risk-based prioritization that CISOs favor (focus on crown jewels first).

- **Built-in Defense-in-Depth**: Instead of one firewall at the perimeter, Zero Trust introduces multiple checkpoints: user must authenticate, device posture can be checked, connection must be explicitly authorized by policy, traffic is encrypted, and anomalies are watched. This layered security is exactly the "defense in depth" philosophy of IEC 62443. If an attacker somehow slips past one control (say they steal a credential), they still face other hurdles (can't reach unauthorized zones, can't eavesdrop or tamper with data, will be detected by unusual access patterns, etc.).

In summary, Zentera's Zero Trust architecture was engineered to satisfy IEC 62443 requirements in real-world OT environments where traditional methods often fail. In the next section, we explicitly map Zentera's approach to each foundational requirement (FR1–FR7).

7. Alignment with IEC 62443 Foundational Requirements

Foundational Requirement	What We Do	Compliance Benefit
FR1: Identification & Authentication Control (IAC) "Establishing identity trust for all users and devices."	Zentera enforces authentication for every session, integrating with enterprise IAM so that *no user is anonymous* on the OT network. Even headless devices are identified by their cryptographic credentials on the overlay, preventing spoofing of PLCs or engineering workstations.	Meets IEC 62443 requirements for unique IDs (SR 1.1) and device identification (SR 1.2). On the business side, this reduces insider risk and shared-password issues that plague audits. In plain terms: You can always answer "Who accessed what, and were they authorized?" – critical for both security and regulatory peace of mind.
FR2: Use Control (Least Privilege) "Restrict each person or component to the minimum necessary access."	Through microsegmentation and role-based policies, Zentera allows granular control such that an *operator's workstation is only allowed to interact with its specific production line systems*, while say an OT engineer role might have broader access, and third-party vendors only see their assigned equipment. This enforces least privilege in an otherwise flat network.	Fulfills access authorization requirements (SR 2.1) by eliminating implicit trust. For CISOs, this directly addresses one of the biggest risk questions: *are we over-exposing our critical systems?* With Zentera, you can confidently say that each connection is vetted and limited.
FR3: System Integrity "Ensure the ICS performs its functions free from unauthorized manipulation."	Zentera's overlay provides *end-to-end encryption and integrity checks* for all communications, so attackers cannot hijack or alter commands in transit (addresses SR 3.1 for communication integrity) Additionally, the strict segmentation helps prevent malware spread; even if a Trojan gets into one machine, it's boxed in and cannot scan or move laterally to others (a compensating control given many OT nodes can't run anti-virus).	Supports malicious code protection (SR 3.2) and session integrity (SR 3.8) by design. For operations, this means a virus on an HMI won't easily propagate to controllers and cause widespread outages – containing incidents to minimize impact.

Foundational Requirement	What We Do	Compliance Benefit
FR4: Data Confidentiality "Safeguard sensitive data from unauthorized disclosure."	All traffic within Zentera's virtual overlay may be encrypted with *strong cryptography* (TLS 1.3). This is crucial because native OT protocols often send proprietary process data in cleartext (recipes, setpoints, etc.). Zentera protects those without needing to wait for vendors to implement protocol encryption.	Satisfies confidentiality requirements (SR 4.1, SR 4.3) out-of-the-box. It also handles information persistence controls (SR 4.2) by terminating sessions cleanly so no stray data remains accessible. Business-wise, this can prevent IP theft (e.g., a formula being sniffed on the network) and helps meet data protection regulations.
FR5: Restricted Data Flow "Segment networks to control communications."	Using the Virtual Chamber concept, we create *logical isolation* between all assets (fulfilling SR 5.1 Network Segmentation). Policies then serve as virtual conduits controlling what traffic may pass between zones (SR 5.2 Zone Boundary Protection). For example, you might create separate zones for your packaging line vs. your formulation tanks in a pharmaceutical plant, ensuring a malware outbreak in one cannot jump to the other.	Achieves the zone-conduit model without needing to re-wire networks. It also covers person-to-person communication restrictions (SR 5.3) by locking down channels like remote desktop or SMB only to authorized use. For the CISO, this directly translates to *risk reduction*: reduced downtime due to resilience, shorter incident recoveries, and avoided ransom payments.

Foundational Requirement	What We Do	Compliance Benefit
FR6: Timely Response to Events "Monitor and respond to security events promptly."	Zentera provides a detailed audit log of all connection attempts and policy enforcements. Unusual or blocked attempts are just as important as successful connections, giving early warning of lateral movement attempts (e.g., why is this workstation trying to ping a PLC it never contacted before?). The platform can integrate with SOC monitoring tools and SIEMs, correlating OT events with IT alerts (SR 6.3/6.4). In case of detected compromise, security can remotely isolate a device by updating policies in real time, containing the threat to one zone (SR 6.5 Incident Response).	Meets logging and continuous monitoring requirements (SR 6.1, 6.2) and provides a mechanism for prompt incident response (SR 6.7) without physically pulling cables. This kind of rapid containment is key – if a rogue process is detected, the CISO can ensure it's cut off in seconds, not hours, and without sending technicians on-site immediately.
FR7: Resource Availability "Ensure necessary resources (equipment, network, controls) are available when needed, even under attack."	Our solution is built to respect the high-availability needs of OT: • The overlay adds minimal latency and is designed to be lightweight so as not to impede control traffic (SR 7.2) • MSGs have fail-open modes to avoid downtime, and support HSR and PRP redundancy • By limiting the blast radius of attacks (like DoS or ransomware), it helps keep most of the system operational even if one part is hit – for example, microsegmentation can isolate a DoS attack to a single cell and prevent cascading failure (SR 7.1). • It also secures backup links and out-of-band recovery channels (SR 7.4) so that in a worst-case, systems can be restored safely.	Aligns with availability protection mandates while actually improving uptime by containing incidents. From a business viewpoint, this means the security solution itself is low-risk to deploy (it won't be the cause of stoppages), and in fact it preserves production continuity by preventing one infected machine from taking down a whole assembly line.

8. Comparing Zero Trust to Traditional ICS Security Approaches

Traditional Purdue-model security relies on perimeter firewalls, VLANs, jump hosts, and—in some plants—air-gaps. These controls delivered value when OT networks were largely static, but they struggle against today's living-off-the-land attackers and converged IT/OT environments.

Dimension	Legacy Approach	Zentera Virtual Chamber Approach
Segmentation	VLANs or physical firewalls at level-3/4 boundaries; difficult to introduce mid-life; changes require downtime.	Software-defined virtual chambers microsegment assets without touching the switch fabric; zones can be added or removed in minutes.
Access Control	IP/port rules at the perimeter; once inside, lateral movement is often unrestricted.	Identity-based policies are enforced at every connection—user, device, and application must be authenticated and authorized before traffic flows.
Legacy-device Coverage	No practical way to add MFA or encryption to decades-old PLCs; compensating controls usually stop at the firewall.	Agentless Gatekeepers cloak unmodifiable PLCs, enforce MFA at the boundary, and encrypt traffic end-to-end.
Remote/vendor Access	Broad VPN access exposes large network segments; credentials frequently reused.	Just-in-time, scoped conduits grant vendors access only to the assets they maintain and only for the duration approved.
Visibility and Monitoring	East-west traffic inside the plant is largely invisible; logs concentrate at perimeter devices.	Every session—permitted or denied—is logged centrally, giving full visibility for incident response and compliance.
Deployment Impact	IP re-addressing, switch upgrades, and outage windows often required.	Drop-in overlay with fail-open hardware; can be introduced during routine maintenance with no IP changes.

9. Application to Complex Industrial Environments

Addressing Diverse Industrial Challenges

Zentera's Zero Trust architecture applies to a wide range of industrial sectors, each with unique security challenges:

Manufacturing
- Protection of intellectual property in product designs and manufacturing processes
- Segmentation of production lines to prevent cross-contamination of security incidents
- Secure vendor remote access for equipment maintenance and troubleshooting
- Protection of quality control systems and production data

Pharmaceuticals / Life Sciences
- Validation-friendly security implementation for GMP environments
- Protection of intellectual property in formulations and manufacturing processes
- Segmentation to maintain data integrity for regulatory compliance
- Secure integration of manufacturing execution systems (MES) with ERP

Oil & Gas / Chemical
- Isolation of safety instrumented systems (SIS) from potential compromise
- Secure connections between field operations and corporate networks
- Protection of sensitive process control systems in hazardous environments
- Compliance with both IEC 62443 and industry-specific regulations

Utilities / Critical Infrastructure
- Protection of SCADA systems controlling distributed infrastructure
- Secure remote access to unmanned facilities
- Microsegmentation of operational networks with minimal disruption
- Integration with existing compliance frameworks (NERC CIP, etc.)

Real-World Success Patterns

Organizations that successfully implement Zero Trust in industrial environments typically demonstrate these common patterns:

- **Start with Critical Assets**: Focus initial implementation on the most sensitive or vulnerable industrial systems.
- **Leverage Maintenance Windows**: Align security implementation with planned maintenance to minimize operational impact.
- **Incremental Improvement**: Accept that perfect security is not achievable immediately; prioritize continuous improvement.
- **Operations Collaboration**: Involve operations teams from the beginning to ensure security measures respect operational requirements.
- **Compensating Controls**: Use Zentera to provide compensating controls for legacy systems that cannot be directly hardened.
- **Document Everything**: Maintain comprehensive documentation of security zones, policies, and compliance alignment.

10. Implementation Roadmap: From Assessment to Zero Trust

Zentera's solutions are developed to encourage OT cybersecurity practitioners to take forward steps, even in the face of imperfect information.

For example, even if you do not have an existing asset inventory, you can use Zentera to help build one. Once installed, zCenter logs and makes all traffic flows visible, and built-in Learn functions help accelerate policy definition. The telemetry provided by the platform provides valuable input to guide and inform the buildout of IEC 62443 zones and conduits.

Phase	Objectives	Typical Timebox
Assess & Plan	Build an OT asset inventory; map data flows; rank zones by business risk; draft a target zone-and-conduit model.	**Weeks 1-4**
Proof of Concept	Deploy zCenter plus one Gatekeeper or zLink group in a non-critical cell; validate expected data flows against observed traffic; develop policies and validate latency, and fail-open behavior.	**Weeks 5-8**
Protect Crown Jewels	Roll out to the highest-risk zones (e.g., safety systems, high-value lines); implement MFA for all human access; integrate logs with SOC.	**Months 3-4**
Plant-Wide Expansion	Extend microsegmentation to remaining lines, remote sites, and clouds; refine policies from "learning" to "enforce".	**Months 5-9**
Continuous Improvement	Quarterly risk reviews, policy tuning, and onboarding of new IIoT or cloud workloads; maintain IEC 62443 evidence package.	**Ongoing**

11. Actionable Recommendations for Industrial Cybersecurity Leaders

Prioritize by risk. Start with assets whose compromise would halt production or threaten safety.

Define zones early. Use the IEC 62443 model, grouping devices with similar function and criticality; everything else is a conduit. But don't worry if you get it wrong, as zone definitions are simple to change.

Require strong identity everywhere. Integrate the overlay with corporate IAM and enforce phishing-resistant MFA for every human session.

Wrap, don't rip-and-replace. Use zLink agents wherever you can to enforce policy. Use Gatekeepers to secure devices that cannot run agents.

Encrypt OT traffic by default. Protect clear-text protocols without waiting for vendor upgrades.

Shrink vendor exposure. Replace persistent VPNs with time-bound, role-scoped access paths that are logged and recorded.

Feed OT logs to the SOC. Treat plant telemetry the same as IT, and correlate events to spot cross-domain campaigns like Volt Typhoon.

Test fail-open scenarios. Confirm that security hardware will not stop the line if power or links are lost.

Measure success. Track dwell-time, incident containment radius, unplanned downtime, and audit findings to show ROI.

Iterate quarterly. Update the zone map and policies as processes, regulations, and threats evolve; keep the IEC 62443 evidence dossier current.

12. Conclusion: The Path Forward for Industrial Cybersecurity

Industrial enterprises cannot afford the consequences of a modern OT breach: multi-million-dollar downtime, safety incidents, and reputational damage. Recent joint CISA-NSA advisories warn that Volt Typhoon has **already compromised IT networks in U.S. communications, energy, and water utilities**, pre-positioning for lateral movement into OT systems.

Momentum for IEC 62443 adoption is growing, and a Zero Trust overlay helps implement IEC 62443 security for the most critical assets, quickly and without costly rebuilds:

Security: Every connection is authenticated, authorized, encrypted, and monitored.
Compliance: Controls align one-for-one with IEC 62443 FR 1-7, providing a ready audit trail.
Operational resilience: Fail-open design and microsegmentation contain attacks without disrupting production.
Business value: Plants gain freedom to adopt cloud analytics, IIoT, and remote expertise safely, turning security into a competitive advantage.

The Bottom Line: Adopting a Zero Trust architecture now shields critical operations against the next Volt Typhoon-style campaign, dramatically reduces compliance effort, and preserves uptime that directly protects revenue.

References

IEC 62443 Standards Series – International Society of Automation
IEC 62443-1-1: Concepts and Models
IEC 62443-2-1: Requirements for an IACS Security Management System
IEC 62443-3-2: Security Risk Assessment and System Design
IEC 62443-3-3: System Security Requirements and Security Levels
CISA Advisories on Industrial Control System Security
NIST Special Publication 800-82: Guide to Industrial Control Systems Security
Zentera Industrial Security Solution Brief

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.

zentera™

www.zentera.net

sales@zentera.net

+1 (408) 436-4811