Adapting Zero Trust Principles to Operational Technology

Publication: April 29, 2026

Cybersecurity and Infrastructure Security Agency
Department of War
Department of Energy
Federal Bureau of Investigation
Department of State

Executive Summary

Authoring Agencies: The Zero Trust Operational Technologies Security Working Group developed this document. The Working Group is a joint initiative led by the Cybersecurity and Infrastructure Security Agency (CISA), Department of War (DoW), and Department of Energy (DOE)—with the aim of supporting organizations in applying zero trust (ZT) principles to operational technology (OT). The Zero Trust Operational Technologies Security Working Group gratefully acknowledges the contributions of the following participating agencies: Department of State (DOS), Federal Bureau of Investigation (FBI), and the National Institute of Standards and Technology (NIST).

Purpose of Document: This paper provides considerations for applying ZT principles to OT systems and environments to system owners, operators, and security personnel. It addresses the unique challenges of transitioning to a ZT architecture within OT, considering technology gaps from legacy infrastructure, operational constraints, and the safety requirements that come from the critical link between cybersecurity and physical processes.

Intended Audience: ZT practitioners and OT owners and operators who are responsible for implementing ZT in OT but may have limited understanding of OT environments and their unique constraints. While this document has specific references for applying ZT to federal OT systems, any organization with OT systems can apply the information provided.

Summary of Important Topics: Key focus areas include establishing comprehensive asset visibility, proactively addressing supply chain risks, and implementing robust identity and access management. The document emphasizes layered security controls—encompassing network segmentation, secure communication protocols and vulnerability management—alongside a fundamental shift in security philosophy that assumes a breach occurred and prioritizes uninterrupted operations, safety, and reliability. The document aligns with the National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF) 2.0 functions of Govern, Identify, Protect, Detect, Respond, and Recover.

Summary of Document's Conclusion: Successful implementation requires a holistic approach, adaptation of ZT principles to the specific characteristics of each OT environment, and strong collaboration between IT, OT, and cybersecurity teams. By applying ZT to OT, organizations can significantly enhance the security and resilience of their OT environments, from industrial control systems to facility automation, helping ensure a more secure and reliable future for both critical infrastructure and mission operations.

Table of Contents

Introduction

Zero trust (ZT) offers a modern, adaptive approach to cybersecurity by eliminating implicit trust and continuously validating access based on identity, context, and risk. ZT principles assume a breach has already occurred and are designed to limit threat actor movement and potential damage. For operational technology (OT), applying ZT requires careful consideration because OT systems interact with the physical environment and are constrained by availability and safety requirements, as well as legacy technology with long lifespans.

The blanket application of traditional information technology (IT)-focused ZT capabilities to OT is neither reasonable nor feasible and requires continuous collaboration between OT engineers, IT architects, and cybersecurity professionals. This collaboration should include clear communication channels, joint development of policies and controls, and a shared understanding of both mission objectives and technical limitations.

This document provides recommendations for ZT practitioners and OT owners and operators to implement ZT principles while considering the unique constraints and challenges of OT environments. This document is authored by:[1]

- Cybersecurity and Infrastructure Security Agency (CISA)
- Department of War (DoW)
- Department of Energy (DOE)
- Federal Bureau of Investigation (FBI)
- Department of State (DOS)

The authoring agencies encourage network architects, security personnel, and procurement staff—especially those unfamiliar with OT systems—to review and use this document with the goals of understanding OT's unique constraints and tailoring a collaborative, risk-informed approach when adapting ZT to OT.

Audience and Scope

This document is written with the aim of supporting U.S. government organizations in securing critical infrastructure and OT, though any organization with OT can apply the recommendations provided. It is intended for ZT practitioners and OT owners and operators who are responsible for implementing ZT in OT but may have a limited understanding of OT environments and their unique constraints. Organizations looking for more detail on ZT principles should reference CISA's Zero Trust webpage.

[1] Hereafter referred to as the authoring agencies.

For the purposes of this document, OT is defined as:

> A broad range of programmable systems and devices that interact with the physical environment or manage devices that interact with the physical environment. These systems and devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include industrial control systems, building automation systems, transportation systems, physical access control systems, physical environment monitoring systems, and physical environment measurement systems.[2]

Structured into Govern, Identify, Protect, Detect, Respond, and Recover sections, this document aligns with CISA's Cross-Sector Cybersecurity Performance Goals 2.0 and the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) version 2.0 to simplify reader adoption. The document also aligns with existing high-level guidance and best practices across the U.S. federal government and industry, including the CISA Zero Trust Maturity Model (ZTMM), NIST SP 800–82 Rev.3, DoD Zero Trust Reference Architecture v2.0, DOE's Cybersecurity Strategy, and international standards (such as ISA/IEC 62443), providing consistency with widely accepted ZT and OT cybersecurity principles. This document intends to bridge the gap between ZT concepts and OT within a single document.

Evolving Threat Landscape and the Need for Zero Trust

With advancements in technology and networking, OT systems that were traditionally isolated or manually controlled are becoming increasingly interconnected, digitally monitored, and remotely operated. This growing convergence between IT and OT expands the attack surface, introduces new attack vectors and magnifies cybersecurity risks.

Improperly secured pathways create opportunities for threat actors to gain access to IT and OT networks. Once inside the IT network, threat actors, such as those conducting activity tracked publicly as Volt Typhoon, can escalate and maintain access by exfiltrating Active Directory credentials. Once compromised, shared domains or credentials between IT and OT environments are one way for threat actors to move laterally into the OT network. Other threat actors have compromised trusted third-party vendor software updates, exploited supply chain weaknesses, and taken advantage of insecure and unrestricted remote access granted to vendors and operators to gain network access. Threat actors have also adopted living off the land (LOTL) techniques in IT networks while prepositioning to move to OT networks. If on the OT network, threat actors could then use OT-specific capabilities (see PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure for more information).

Threat actors increasingly demonstrate offensive capabilities against OT systems, using cyber-enabled means with the aim of compromising, manipulating, degrading, and disrupting the critical physical processes these systems control. Historical examples of this capability include malware packages designed and tailored for use in targeting OT and critical infrastructure systems, such as CrashOverride, Havex, BlackEnergy 2 and 3, Trisis, and Incontroller.

---

[2] Keith Stouffer et al., "Guide to Operational Technology (OT) Security," *NIST Special Publication*, NIST SP 800-82r3. https://doi.org/10.6028/NIST.SP.800-82r3.

LOTL techniques—the abuse of native tools and processes on systems—obscure malicious behavior, making detection by traditional security tools more difficult. Security is further complicated by the decades-long lifecycle of OT equipment, with older components potentially lacking any security support.

Cyber incidents in OT environments can cause operators to lose visibility or control of critical systems, potentially leading to catastrophic outcomes. This is because OT systems directly control physical processes—unlike IT systems, where impacts are often limited to data or service availability. As these environments evolve, traditional perimeter-based defenses and implicit trust models are no longer sufficient. Applying ZT principles can help close those gaps but only when adapted to fit OT's operational realities.

Unique Constraints for Zero Trust in OT

Successfully applying ZT principles to OT requires careful consideration because OT systems interact with the physical environment, and there are inherent differences in system design, architecture, and unique mission-critical priorities. These differences typically emerge via constraints on availability, legacy systems, and different team structures.

Availability Requirements. Unlike IT systems, OT systems involve layers of sensors, actuators, logic solvers, and user interfaces that operate in real time to deliver physical products, services, or resources—often running continuously. These systems are engineered for high availability, reliability, and safety, making them less tolerant of disruptions or reconfiguration. Maintaining these availability requirements alongside decades-long lifecycles can be challenging while supporting more agile security approaches.

Legacy Insecure Systems. The historical lack of security on legacy OT devices alongside their long lifecycle has resulted in inherent vulnerabilities, which threat actors increasingly exploit. Many legacy OT systems rely on proprietary, insecure protocols that can neither be actively scanned nor undergo routine penetration testing without risking critical uptime. Near-constant availability requirements limit opportunities for routine patching, security testing, system upgrades, and maintenance. While these environments often include built-in redundancies and failover capabilities, their design for continuous operation poses significant challenges to traditional cybersecurity practices.

Limited Logging. Logging and forensics capabilities are often minimal, limiting the effectiveness of traditional threat detection and response methods. Capturing OT-specific data sources (e.g., discrete event logs, engineering files, database queries, network, and process data) is essential for identifying threat actor activity and detecting anomalies before damage occurs.

OT/IT Collaboration. Implementing ZT in OT environments requires cross-functional teams that can thoughtfully navigate the tradeoffs between security, availability, and operational constraints. Tailoring successful ZT solutions to the unique characteristics of OT environments requires continuous collaboration between OT engineers, IT architects, and cybersecurity professionals. This collaboration should include clear communication channels, joint development of policies and controls, and a shared understanding of mission objectives and technical limitations.

The following considerations are meant to assist organizations trying to safely overcome the constraints of OT while applying ZT for each NIST CSF category.

Govern

Improving and maintaining security processes requires proper governance. This section raises considerations for adjusting governance structures with the goals of maintaining safety, navigating out of legacy constraints with procurement, and capturing supply chain information.

Governance Structures

In OT environments, effective governance should clearly define roles and responsibilities of operational stakeholders and cybersecurity personnel, recognizing the specialized expertise each brings to the table. OT stakeholders may include asset owners (e.g., plant managers, energy managers), operators, engineers, system integrators, vendor support or managed service contracts, and OT-specific security teams. Personnel with cross-disciplinary fluency (such as IT personnel understanding OT architectures and safety constraints or OT personnel understanding cybersecurity principles and threat modeling) can be useful to avoid accidental disruptions when implementing ZT. Remote access and emergency override (break-glass) scenarios tend to be high-risk areas for disruption and should be prioritized for this cross-disciplinary understanding.

Organizations should set acceptable risk tolerances, establishing clear escalation procedures for instances when ZT security controls could impact system availability or safety. In many cases, risk-informed exception handling and compensating controls—such as out-of-band anomaly detection or network segmentation—are necessary where traditional ZT mechanisms are impractical or disruptive to OT processes.

Ultimately, success hinges on embedding shared accountability into the operational approach, shifting from siloed decision-making to a unified, mission-aligned approach. This helps ensure ZT strengthens both cyber resilience and continuity of critical operational functions.

Overcoming Zero Trust for OT Constraints Through Procurement

Security practitioners commonly face operational constraints and legacy limitations when applying ZT methodologies to OT. Although no single tool or silver-bullet technology resolves these operational challenges, strategic procurement for transitioning off of insecure legacy infrastructure enables long-term alignment with ZT principles without extensive mitigating controls.

Procurement can facilitate the gradual transition away from legacy infrastructure and lay the groundwork for ZT-aligned operations. Newer OT components can support essential capabilities that are absent in many legacy components, such as security logging, secure communication protocols, and identity and access management. These capabilities enable better monitoring, segmentation, and enforcement without disrupting operational processes.

Closely coordinating procurement decisions with OT operators helps ensure seamless integration, minimizes operational disruptions, and supports the development of secure, sustainable workflows. For procurement considerations that promote security by design, see CISA and partners' joint guide, Secure by

Demand: Priority Considerations for Operational Technology Owners and Operators when Selecting Digital Products.

Supply Chain and Third-Party Risk Management

Several supply chain risk management practices support the adoption of ZT principles. While these initiatives are distinct, they are intentionally integrated within the CISA ZTMM and the DoD Zero Trust Strategy and Reference Architecture to create cohesive security outcomes.

For OT environments, these practices generally apply but are often not comprehensive. For example, while some suppliers provide Software Bill of Materials (SBOM) for newer control systems, legacy OT products rarely have such documentation. As a mitigating measure, organizations can assess the maturity of the vendor's supply chain by reviewing existing SBOMs, evaluating vulnerability management practices, confirming if they are a Common Vulnerabilities and Exposures (CVE) Numbering Authority, and if the security capabilities of their components align with the risk posed by typical connectivity scenarios.

OT asset owners also need a broader understanding of their components, including supply chain restrictions on safely operating hardware, vendor-supplied or controlled infrastructure and software features. Some organizations may choose to select products based on design, manufacturing, or assembly location to enhance quality and reduce risk. Approved product lists and product certifications can further reduce supply chain vulnerabilities.

Most asset owners interact with third parties for code development, integration, or technical support. ZT mandates that agencies only grant third-party access to OT equipment with proper authorization and oversight. This can be achieved by securing remote access channels, blocking ports via policy, physical controls, or procedural enforcement. While technical controls are preferred over manual ones, at minimum, a method must be in place that limits and monitors third-party access.

Supply chain risk data should inform trust decisions, helping reduce the potential for adversarial manipulation through indirect vectors such as compromised vendor access or firmware.

Identify

To enable proper prioritization during the ZT implementation process, an organization should identify their assets, changes to those assets, and the potential consequences of a cyber incident. This section highlights OT-specific considerations for identifying and changing assets and how physical consequences can shape risk decisions.

Comprehensive Asset Inventory and Asset Discovery

To understand risk and design an effective ZT architecture, organizations should begin by creating a comprehensive asset inventory—an organized, regularly updated list of an organization's systems, hardware, and software. This list enables understanding of the systems, devices, and communications that compose the OT environment.

The key difference between typical IT and OT asset inventories lies in the tooling and communication protocols. The tooling generally relies on passive monitoring, which avoids the risk of disruption, particularly to older components. Organizations can conduct active scanning using built-in OT protocols or with newer components.

Note: Typical active scanning should not be attempted without a deep awareness of your system, as this may knock a legacy device offline.

OT communications protocols are increasingly embedded in standard NetFlow analysis tools, but some vendors may use proprietary protocols that are not easily parsed. Understanding these protocols is key to mapping what function a device performs and identifying which components are executing core control system processes.

Practitioners should understand OT network topologies, recognize that automated tools may only produce partial results—particularly in highly segmented or air-gapped networks—and analyze if the cost of deploying an OT-specific asset inventory and management tool across all segments and subnets might prove cost prohibitive. Organizations can manage costs through network understanding, careful planning, and thoughtful sensor/agent placement within the OT network, providing visibility into the largest or key network segments and devices. Ultimately, a comprehensive asset inventory is foundational to securing OT environments, serving as a critical enabler of ZT capabilities.

For a longer discussion on conducting an OT asset inventory, see CISA and partners' joint guidance Foundations for OT Cybersecurity: Asset Inventory Guidance for Owners and Operators.

Configuration and Change Management

Once an asset inventory is in place, organizations should develop a process for configuration and change management, as needed. As changes can directly impact physical processes, safety and system reliability, OT change management must follow structured, rigorously governed procedures rooted in safety and engineering checks. Two foundational elements define effective OT change management—risk mitigation and comprehensive documentation.

All changes should follow a formalized Management of Change (MOC) process, including updates to ZT policies. MOC processes help ensure changes are thoroughly reviewed and approved before implementation, minimizing potential disruptions and hazards. A robust MOC process typically includes a multi-disciplinary review board that assesses proposed changes from several critical perspectives, including:

- **Engineering Peer Review.** Validates the technical feasibility and benefits of the proposed change.
- **Safety Review.** Critically assesses how the change might affect safety systems or increase risk, paramount in OT.
- **Size, Weight, Power, and Material Review.** Confirms that changes do not exceed physical limitations of the equipment or environment, which is particularly important for legacy systems.
- **Operational Review.** Evaluates potential operational disruptions and impacts on production processes, often including an outage request to make the change.

- **Maintenance Review.** Considers long-term impact on operating expenses and maintenance demands.

Once all reviews are complete, appropriate management personnel should provide formal authorization. Every decision, technical specification, and configuration detail must be meticulously documented. Crucially, a full system backup should be taken immediately before and after any configuration change. This documentation is essential and serves as a critical record for troubleshooting, incident response (IR) and auditing. Notably this process is almost always a slower rate of change than IT patch cadences. Escalation policies need to be in place to understand where a known exploited vulnerability needs to be patched more quickly. Proactively maintaining documentation and backups and can help safely speed up this process.

Risk Management, Threat Modeling, and Cyber-Physical Consequences

ZT architectures fundamentally rely on continuous monitoring, validation, and context-aware decision-making, all requiring real-time insight into threats and risk posture. As outlined in NIST SP 800-207, the DoD Zero Trust Strategy and CISA's Zero Trust Maturity Model (reinforced by Executive Order 14028), risk assessment and threat modeling fall squarely within the traditional scope of ZT. However, for OT environments, these practices must extend beyond typical IT considerations to encompass potential cyber-physical consequences. A misconfigured or compromised system can lead to safety or operational failures, impacting not just a single component but the entire environment.

Building upon the previously identified assets and associated access controls, this section details a process for conducting thorough risk assessments and threat modeling specifically tailored to OT environments. By integrating threat modeling with mission impact assessments, organizations can align security decisions with the physical consequences unique to OT environments, so that ZT works alongside—not in place of—safety protocols to reduce exposure and enforce trust decisions based on relevant threat information.

Risk Assessment Methodology: A Practical Approach

When addressing OT risk tolerances, organizations should prioritize safety and operational continuity above all else. Risk evaluations in OT environments must be practical and mission-aware, recognizing unique constraints and priorities of OT, namely maintaining availability, and ensuring safety. Organizations should begin by identifying critical processes and associated assets, including legacy systems and control system components. Risk assessments should integrate asset inventories, vulnerability scanning results, and system interdependencies to surface potential exposures. A semi-quantitative approach-combining automated data with expert elicitation is recommended to balance analytical rigor with operational insight. This method enables organizations to assess the likelihood and impact of cyber-physical threats, prioritize mitigations, and make informed ZT decisions without compromising essential functions.

Threat Modeling for OT: Mapping the Attack Surface

OT systems often lack robust logging, monitoring, and detection capabilities commonly found in IT environments. This makes threat modeling essential for effectively prioritizing security resources. Develop

threat models that accurately reflect the interconnected and complex nature of OT environments, recognizing the potential for cascading failures across critical processes.

Identify relevant threat actors (e.g., nation-state adversaries, criminal groups, insider threats) and analyze potential attack vectors (e.g., compromised engineering workstations, vulnerable remote access points, supply chain compromises). Map potential attack paths to understand how adversaries could move laterally across systems, elevate privileges, and disrupt critical processes. This analysis should explicitly consider how IT-OT convergence might expand the attack surface.

Importantly, avoid procuring components or systems that assume security through air-gapping or segmented architecture alone, as modern threats can exploit the false sense of isolation these models provide. A realistic and comprehensive threat model provides the foundation for prioritizing defense measures, validating ZT assumptions, and aligning security efforts with mission-critical risks.

Cyber-Physical Consequences: Real-World Impact

The consequences of an OT cyber incident are often physical and can have immediate and severe impacts. These include disruptions to essential services (e.g., power, water, transportation, etc.), physical damage to industrial equipment, environmental harm, and serious safety incidents affecting personnel and the public. Organizations should account for these cascading effects when designing and prioritizing ZT security controls, ensuring they align with mission-critical functions and safety protocols.

Integrating Risk Assessments With Zero Trust Principles: A Proactive Approach

Risk assessments and threat modeling should directly guide the implementation of ZT principles in OT environments. Assets and communication paths identified as high-risk require stricter access controls, more robust monitoring, and strategic network segmentation, where appropriate. This proactive stance enables organizations to prioritize resources effectively, reduce attack surfaces, and mitigate potential impacts before adversaries can exploit vulnerabilities.

Prioritization and Mitigation: Focused Security Efforts

Identified risks should be prioritized by evaluating both their likelihood and potential impact, with mitigation strategies aligned closely with security controls and IR plans outlined in subsequent sections. By focusing resources on the most probable and highest-impact risks, organizations can account for operational constraints while strategically allocating limited resources where they matter most.

Protect

A robust ZTA protects OT components from unauthorized access. This section details considerations for segmentation, identity, credential, and access management (ICAM), and remote access.

Network and Microsegmentation

Network segmentation remains one of the most foundational and effective security controls in OT environments, often serving as the primary line of defense. Unlike traditional IT networks that historically relied on perimeter-based security, OT networks have long embraced segmentation to enhance safety,

availability, and reliability. This concept has been a core tenet of OT architecture for decades, reflecting the need to isolate critical functions. Isolation enables ZT principles and prevents cascading failures across interconnected systems.

In OT, segmentation limits the blast radius of a cyber or operational incident, minimizing the potential of a single compromise to negatively impact broader system functions. Importantly, legacy OT systems already possess many of these foundational segmentation techniques, including physical air gaps, dedicated virtual local area networks (VLANs), and carefully controlled access to sensitive zones, providing a useful baseline for ZT implementation.

However, segmentation alone is not foolproof. Air gaps can be bridged, VLANs can be misconfigured, and overly permissive access rules can undermine intended isolation. Well-segmented environments remain vulnerable without continuous validation, strong access control policies, and proper network monitoring.

For the advancement of ZT in OT, organizations should treat segmentation as a dynamic, enforceable security policy instead of a one-time architectural decision. The management of network segmentation may need to be done out of band of the operational network due to latency concerns, or simply to make it easier to detect adversary activity. Microsegmentation adds another layer of defense, encompassing specific assets, protocols, and users by enabling more granular trust boundaries while preserving operational integrity.

IT Segmentation Vs. OT Segmentation

While both IT and OT employ segmentation, the underlying philosophies and implementations differ significantly (see **Table 1**).

Table 1. IT vs OT Segmentation

Feature	IT Segmentation	OT Segmentation
Primary Goal	▪ Contain breaches ▪ Enforce compliance ▪ Manage access	▪ Protect physical processes ▪ Provide safety and reliability ▪ Prevent disruption
Focus	▪ Data confidentiality ▪ Data Integrity	▪ System availability ▪ System safety
Complexity	▪ Often based on logical groupings (e.g., departments, applications)	▪ Driven by functional boundaries and process control requirements (e.g., cell control, safety systems)
Disruption Tolerance	▪ Higher–some downtime is often acceptable	▪ Extremely low–disruptions can have physical consequences
Tools	▪ Primarily software-defined networking (SDN) ▪ Virtual firewalls	▪ Firewalls, jump hosts, secure gateways, data diodes ▪ Often relies heavily on physical network separation

Feature	IT Segmentation	OT Segmentation
Directionality	▪ More bidirectional communication allowed	▪ Primarily unidirectional–OT systems push data out, minimizing inbound connections

Implementing OT Segmentation

Effective OT segmentation begins by identifying functional boundaries within the OT environment and designing the network with restrictive communication across those boundaries. This is typically achieved through a combination of the following:

- **Firewalls.** Enforce access control policies between segments.
- **Jump Hosts.** Provide secure, controlled access points for remote administration. See the **Jump Hosts (Bastion Hosts)** section.
- **Secure Gateways.** Act as controlled interfaces for transferring data between networks.
- **Data Diodes.** Enforce unidirectional communications via hardware controls.

Concentrate activity monitoring within each segmented boundary, allowing for early detection of anomalous behavior. Design segmentation boundaries for operational self-sufficiency, minimizing reliance on external networks to sustain critical functions. The guiding principle is to build autonomy into each zone, enhancing resilience.

Enforcing strong media protection policies and procedures forms another cornerstone of OT segmentation. Due to the air-gapped or isolated nature of many OT systems, removable media represents a significant adversarial attack vector. The method for moving data into and out of OT systems must be conducted securely and follow these core practices:

- **Data Encryption.** Enforce encryption on all data transferred to and from removable media. Verify the authenticity of cryptographic signatures before granting access.
- **Access Controls.** Apply strict access controls and authorization procedures for the use of removable media devices.
- **Auditing and Monitoring Removable Media.** Regularly audit and monitor removable media device usage to detect and respond to unauthorized activities.
  Note: Sandboxing is effective, where feasible.
- **Employee Training.** Educate employees on the cybersecurity risks associated with removable media and safe handling procedures.

Microsegmentation for Enhanced Security

ZTA principles eliminate implicit trust and minimize lateral movement within networks. In OT environments, these goals are supported by microsegmentation, an extension of traditional network segmentation that introduces more granular policy-driven controls.

Microsegmentation enables targeted security rules in OT environments, often leveraging existing technologies that isolate and protect critical components within the OT environment, such as:

- **Business Units.** Separating distinct operational functions or areas to contain risk.
- **Control Systems From Safety Systems.** Preventing adversaries from compromising critical safety mechanisms like safety instrumented systems.
- **Data Tag Access.** Enforcing specific read/write permissions for individual data points within programmable logic controllers (PLCs) and other control devices.

A layered segmentation strategy allows OT defenders to significantly reduce the attack surface, strengthen containment and enhance resilience against internal misuse and external threats. The segmentation strategy may start with broad network boundaries and extend down to granular microsegmented zones. This approach upholds the operational imperatives of safety and reliability.

Identity, Credential, and Access Management for OT

ICAM is essential for implementing ZT in OT, but its deployment must carefully balance traditional security principles with OT's critical priorities of safety, performance, and reliability. Many OT systems predate modern ICAM capabilities and often require compensating controls above the device level. ICAM solutions can succeed in OT environments if they are suitably tailored to operator workflows and supported by clear procedures that manage potential disruptions or safety risks.

While general best practices like least privilege remain foundational, the following OT-specific challenges necessitate thoughtful adaptation:

Segregation is Paramount. Do not directly connect IT and OT ICAM systems. Avoid direct IT-OT trust relationships as they increase the attack surface. Active Directory should be entirely segmented if used in OT—ideally as a separate forest or domain—to maintain network isolation and reduce cross-domain risk.

Emergency Access is Non-negotiable. Implement robust emergency access mechanisms to OT applications and assets. Safety, performance, and reliability cannot be jeopardized by overly restrictive access controls. This requires pre-defined, documented procedures and, potentially, break-glass accounts with limited lifespans and stringent auditing.

Compensating Controls Are Essential. Limitations in OT technology (e.g., legacy systems, proprietary protocols, etc.) or operational needs may prevent implementing ideal access controls or direct ICAM support. Layered compensating controls (e.g., coarse-grained role-based access control [RBAC], network segmentation, out-of-band monitoring, or physical safeguards) fill these gaps by securing the environment around vulnerable assets, without interfering with critical operations. Implement multifactor authentication (MFA), where feasible, even if only at the jump host level.

Consider OT-Specific Protocols. OT-specific protocols—such as Modbus, DNP3, ENIP/CIP and their secure equivalents (Modbus Security, DNP SAv5, CIP Security)—are often incompatible with standard IT security tools. Solutions must be designed to understand and interact with these protocols without compromising safety or availability in OT environments.

Secure Remote Access: Jump Hosts and Privileged Access In OT

Remote access is a major weakness in OT as it represents an initial access vector into an insecure legacy network, but remote access may be necessary for operating distributed infrastructure. This section provides considerations for how to secure remote access through segmentation, access management, and detection strategies.

Jump Hosts (Bastion Hosts)

Jump hosts are dedicated, hardened jump boxes within the OT demilitarized zone (DMZ) acting as the sole entry point for remote access. The authoring agencies strongly recommend a jump host for adding user authentication to legacy networks and enforcing segmentation. These hosts should require MFA, be regularly patched, hardened according to organization-approved hardening recommendations, and monitored continuously. Consider using a jump host solution specifically designed for OT environments, offering features like session recording, anomaly detection, enhanced auditing, and time-based access constraints.

Privileged Access Management

Privileged access management (PAM) is a security practice designed to limit changes to an environment without privileged access. PAM is particularly important for remote access, as it is often intended for read-only monitoring or emergency changes—which cannot be enforced without PAM. Security teams should review accounts capable of performing tasks that compromise the safety and integrity of the OT environment and consider those accounts privileged.

Given the nature of some OT environments, privileged accounts may be shared accounts used by operators, with well-monitored break-glass accounts for emergency access. For existing systems, a combination of physical controls, knowledge management, and provisions for departing employees can mitigate remote access management risks. As asset owners transition to newer equipment, the following technologies can be used to support ZT access management approaches alongside break-glass safety mechanisms:

Vaulting Credentials. Vaults enable secure storage and rotation of privileged credentials. This method can allow for easier rotation of shared accounts and help transition off a shared account if the OT component supports multiple accounts.

Session Recording and Monitoring. Log all privileged sessions for audit and forensic purposes. Log storage should be pushed out of the OT network, without bi-directional control—this prevents access to the network.

Just-In-Time (JIT) Access. Where possible without compromising the safety and integrity of the environment, grant privileged access only when needed and for a limited duration to minimize the risk of abuse and lateral movement. Confirm JIT access continues to be timely to prevent shadow IT or any safety impacts. Operators frequently use JIT access to restrict remote vendor connections to narrowly specified maintenance and support windows.

Multifactor Authentication. Use MFA to restrict firmware or logic changes for critical systems. All privileged access coming from a remote or external environment into OT should enforce MFA. Physical access is a common second factor in existing OT implementations.

Agent-Based vs. Agentless

Remote access monitoring can be done via agents on endpoints (i.e., endpoint detection and response [EDR]), or agentless using technologies like passive network monitoring (i.e., intrusion detection systems). Agents require extensive compatibility testing and may impact system warranties; however, internal network monitors do not typically observe abuses in remote access until the victim begins sending malicious commands. These trade-offs are discussed further in the Detect section.

Secure Communication, Data Integrity, and Encryption

Most OT networks operate without authentication or encryption. While adding confidentiality through encryption can enhance security, it is often a secondary concern in OT environments. Integrity and authentication—achieved through signing—are typically more critical, particularly when encryption could introduce latency or complexity in safety-critical systems.

Because many OT applications are time-sensitive, adding encryption without consideration of systems constraints could disrupt operations. Key management processes must also align with operational workflows. For example, authentication using digital signatures is generally safer than full encryption—expired certificates will not halt operations if communications remain in the clear.

Encryption efforts, where needed, should focus on protecting the semantic structure of communications, such as addresses (e.g., registers, coils, function codes) that reveal operational intent. Frequent updates to real-time process values are often less sensitive and computationally not worth encrypting in resource-constrained environments.

The path to enabling secure communication will vary based on existing system architecture. Some modern OT protocols offer secure extensions (e.g., BACnet/SC, Modbus over Transport Layer Security [TLS], CIP Secure, DNP SAv5); though, these features are often disabled to allow for simpler integration or backwards compatibility. If secure protocol support is unavailable or cannot be enabled due to vendor limitations (e.g., the environment is not interoperable), the next best solution is to wrap legacy protocols in secure tunnels (e.g., via TLS-enabled gateways), so that encryption and authentication occur outside the control devices themselves.

Require encryption for data flows into and out of the control network, especially when traversing untrusted or third-party networks such as telecom connections between facilities or remote vendor access. By prioritizing authentication and integrity and applying encryption judiciously, OT environments can strengthen communications security without compromising operational continuity.

Vulnerability and Patch Management in OT Environments

Effective patch management in OT environments requires strong coordination with operational staff. Unlike IT systems, OT systems or components often require downtime, scheduled maintenance, or authorized

service interruption windows to safely deploy patches and minimize operational impact. Patching outside these windows is discouraged unless there is an outsized risk of exploitation and impact. Structured decision frameworks, such as the Stakeholder-Specific Vulnerability Categorization (SSVC) decision trees, can help evaluate tradeoffs between downtime and exploitation risk for a specific vulnerability.

Edge devices and remote access systems should follow a more frequent patching cadence. These systems often serve as enforcement points for OT segmentation and are critical to overall security posture.

Use redundant system architectures or hot patching techniques, where possible, to apply updates with minimal disruption and increase patch rates for some systems and configurations. Testing patches in a non-operational environment is ideal; however, this is not always feasible and may be cost prohibitive. In such cases, request information from vendors on their testing practices to reduce deployment risk.

The focus should shift to isolating vulnerable systems and applying compensating controls when patching cannot be promptly performed. This may include increasing monitoring, restricting communication pathways, or deploying virtual patches through network defenses. The goal is to reduce the system's exposure to known threats while maintaining operational safety and continuity.

Detect

This section focuses on network and host detection capabilities. The need for OT-specific technology increases as the focus shifts from IT components and application software to control systems and sensors.

Continuous Monitoring Across IT and OT Boundaries

Monitoring is a key element of ZT, providing critical visibility and increasing opportunities for detection of threat actor activity. In OT environments, prioritize monitoring at network boundaries, particularly where OT connects to IT or external systems. These junctions often present the greatest risk.

CISA maintains an open source security information and event management (SIEM) tool, Malcolm, which includes Zeek parsers for common OT protocols and supports deep traffic analysis. Excessive traffic into the OT network, particularly external commands, may signal poor segmentation practices.

Passive OT network monitoring typically relies on Switched Port Analyzer (SPAN) ports or unidirectional data taps for observation and traffic monitoring. Network Terminal Access Points (TAPs) provide passive, load-free visibility into traffic without requiring reconfiguration of switch infrastructure. Most networking equipment and many OT products allow the use of syslog for data aggregation and analysis.

Design a monitoring architecture with resilience in mind. Ideally, build a solution within the OT environment that securely monitors networks and devices without adding failure points or expanding the protect surface. This may require establishing an out-of-band network that prevents traffic from commingling.

Monitoring below the IT/OT boundary, closer to the physical process, requires knowledge of the operational system. In OT, the relatively static nature of OT environments is an advantage. Two primary approaches to implementing behavioral analytics in OT environments are baseline-based detection and specification-based detection.

Baseline-based Detection

This method uses statistical models to identify deviations from normal behavior.

- Highly effective in OT environments; however, it requires carefully defined learning windows to capture all operational modes.
- Alternatively, employing static rules informed by domain expertise may address edge cases and failure scenarios, such as protocol commands that disable components or switch the primary controller.

Specification-based Detection

- This approach defines the range of valid behaviors, akin to the design of simple safety systems.
- This robustly captures known failure states and operationally viable conditions within the broader control system state machine.

Operator collaboration is essential for reducing false positives and provides clear utility to both the cybersecurity and engineering teams. Add behavioral detections for timing interval metadata (i.e., one system speaking too frequently) if secure communication is not in place. This allows for spoofing detection without extensive documentation for proprietary data fields.

More advanced continuous monitoring, such as interpreting specific instructions or predicting process impact, requires a sophisticated understanding of the OT systems and their behavior under various operating conditions.

Endpoint Detection and Response Considerations for Embedded Systems

OT environments require unique considerations when implementing EDR that differ significantly from traditional IT contexts. Four key barriers include: legacy challenges, restrictive products, a shift toward cloud connected EDR solutions, and LOTL techniques.

Legacy Challenges. Legacy architectures and low-power legacy components may make applying EDR difficult to anything below the human machine interface (HMI) or engineering workstation without impacting system performance. Even there, standard EDR products may not support a particularly old operating system. A lightweight approach for embedded systems EDR is monitoring telemetry (CPU and memory usage, new processes, and configuration changes) with the expectation that embedded OT systems are unlikely to be modified frequently.

Restrictive Products. Often embedded OT systems closely tie the application and operating system. This prevents users from deploying an agent or running software on the component. Warranty policies also often restrict these changes unless considered during procurement.

Cloud Increasing Connectivity. The shift to cloud makes procurement of on-premises only EDR solutions more difficult. Most EDR products rely on a connection back to the vendor's servers, which is often prohibited or impractical in isolated or air-gapped OT networks. If possible, the recommended approach is

using a staging server in the DMZ that downloads and pushes EDR updates rather than any bi-directional communication from EDR agents.

Living off the Land. LOTL refers to the technique of using legitimate tools, protocols, and behaviors already present in the environment (e.g., PowerShell, Windows Management Instrumentation, HMI software, vendor programming tools, etc.); threat actors can carry out malicious activity while evading detection with this technique. In OT networks, the prevalence of legacy and unauthenticated protocols makes this approach especially effective, where attackers can mimic normal operations without deploying custom OT-specific malware. For information on LOTL, see CISA and partners' joint guidance Identifying and Mitigating Living Off the Land Techniques.

EDR solutions in OT environments must go beyond simple network access controls. They require behavioral and heuristic-based detection methods that can identify subtle deviations in expected patterns. However, precision is called for when implementing these controls. Carefully scope blocking capabilities; otherwise, they may interfere with established operator workflows or compromise safety-critical processes.

Respond

ZT assumes that a breach has already occurred, meaning adversaries have bypassed initial defenses described in the **Protect** section. Given this premise, response and recovery are critical to minimizing the impact of cyber incidents and quickly returning to full operational capacity.

Incident Response Planning for OT-Specific Scenarios

Asset owners should build upon existing emergency response procedures, risk assessments, and business continuity plans (BCPs) for the development of robust IR strategies tailored to OT environments. For cyber-specific incidents, the IR plan should include:

- **Isolation Procedures.** Clearly define when and where the disconnection of systems should occur, along with pre-authorized personnel responsible for executing these actions.
- **Decision Matrices, Flow Charts, and Playbooks.** Develop tools that address common cyber threats in the OT environments, leveraging frameworks like MITRE ATT&CK®.
- **Contact Information.** Maintain up-to-date details for in-house and external IR personnel, including IR retainers.
- **Communication Plans.** Establish protocols for internal and external communication during incidents.

Ensure existing IR plans delineate clear roles and responsibilities for operations, engineering, and OT/IT teams. Regular reviews, testing, and approval by an appropriate authorizing official responsible for risk and cost management are essential. Review plans at least quarterly to maintain accuracy, with at least annual testing that confirms IR plans are understood, actionable, and effective. Immediately review and test IR plans after events—such as geo-political tensions, increased criminal activity, or natural disasters—occur that heighten risk.

Customize IR tools like decision matrices, flow charts, and playbooks to the organization's specific needs. For example, asset owners must determine when isolation of OT systems from IT environments or shut down operations should occur. In the event of a detected compromise on a safety network, proactively shutting down operations can mitigate safety risks, helping to limit the impact to financial loss rather than safety consequences. Conversely, an asset owner may choose to continue operations if a compromise is detected on a disconnected engineering workstation as the impact on the organization would be minimal.

Threat Containment Strategies

Containing cyber incidents in OT environments requires a multi-layered approach distinct from traditional IT responses. While physical, logical, network, and procedural controls remain vital, OT systems prioritize uptime, safety, and process integrity—necessitating nuanced strategies.

- **Physical Security.** Enforce strict access controls using badging, biometric authentication, and security checkpoints, to help ensure only authorized personnel interact with affected systems.
- **Logical Access Control.** Rigorously apply the principle of least privilege by reviewing and limiting account permissions to the minimum necessary for specific job duties. Implement "just enough access" and "just-in-time" principles to effectively reduce threat vectors.
- **Network Isolation.** Air-gapping or aggressively segmenting OT systems can disrupt critical processes, potentially leading to safety incidents or production shutdowns. Security teams must collaborate with operators when determining which business functions can continue under heightened segmentation or isolation and for how long. Risk assessments should weigh the impact of operational disruption against the risk of continued compromise. In some cases, "soft segmentation"—a carefully defined demarcation point within the network—may be a more appropriate initial step.

OT systems are often designed for reliability not security, making rapid changes is potentially risky. Clearly defining system ownership (who is responsible for risk assessment decisions and system disposition) and establishing the IR team's operating posture are essential considerations that go beyond technical controls. OT incident response, unlike IT, often requires balancing aggressive containment measures with maintaining safe and reliable operations. Coordination with process engineers and operations staff is critical to understanding the implications of any actions taken.

Implementing these strategies effectively contains threats, minimizes disruption to critical infrastructure, and accounts for the unique operational constraints of OT environments. Thorough documentation of all actions taken and a clear understanding of potential consequences are vital for successful incident resolution and post-incident recovery.

Coordinate Incident Response for Critical Infrastructure

Effective cybersecurity for OT environments demands seamless coordination between government agencies (e.g., DoW, the intelligence community, and Sector Risk Management Agencies) and critical infrastructure sectors. This requires:

- **Clear Communication Channels.** Establish protocols for secure information sharing, including threat intelligence and mitigation strategies.
- **Joint Incident Response Plans.** Confirm roles and responsibilities are well-defined, enabling faster and more effective responses.
- **Sector-specific Expertise.** Leverage specialized knowledge and foster strong public-private partnerships for unified defense.

A coordinated approach minimizes incident impact, accelerates recovery, and enhances the resilience of critical infrastructure. Regular exercises and ongoing collaboration are key to maintaining readiness and strengthening collective security.

Recover

Recovery is a necessary element of resilient critical infrastructure. Proactively including the considerations below in ZT programs can help detect threats and protect infrastructure. OT-specific data sources and continuity processes are stressed to prioritize contingency plans are created and tested.

Data, Configuration, and System State Backups

Effective recovery in OT environments hinges on comprehensive system backups tailored to the unique needs of OT systems. These backups should prioritize the following elements:

- **Operating System (OS) Configurations.** Restore OS settings that maintain system functionality.
- **Application Software.** Maintain access, along with recovery or reinstallation capabilities, to application software, including associated licenses.
- **Application Configurations and Engineering Logic.** Back up and deploy configurations and engineering logic critical to system operations.
- **Application Data.** Safeguard essential data, ensuring continuity of operations.

Backup capabilities across OT devices can vary significantly. Some devices support only offline backups, require manual downloads, or provide incomplete backup options. Others lack backup functionality altogether. Adhering strictly to vendor manuals and best practices is essential for carrying out proper backup procedures. Organizations should also consider maintaining up-to-date standby systems that can be quickly deployed as hot swaps during outages.

While backups for engineering workstations and certain networking equipment can often follow standard IT processes, OT-specific devices (e.g., controllers) require specialized attention. Regular backups should include logic, In/Out (I/O) lists, startup values, and other configuration details as specified in device documentation. In some cases, historians may track engineering data, but this should not replace dedicated backups.

Given the interoperability challenges inherent in OT environments, retaining detailed engineering documentation is critical. This includes cause-and-effect matrices, control narratives, I/O lists, logic printouts, and specification sheets. These resources are invaluable for restoring systems and troubleshooting disruptions effectively.

System Restoration and Integrity Validation

The restoration of OT systems often requires licensed engineering software specific to the equipment. Keeping engineering software for all critical OT equipment licensed and readily available onsite allows for rapid restoration.

Regularly test backup files on development systems, verifying file integrity is maintained and restoration capabilities are functional. Employ alternative verification methods—such as file hashing, checksum validation, or engineering software capable of comparing backup files with running code—if development systems are unavailable.

Business Continuity and Cyber Resilience in Industrial Systems

Organizations operating industrial control systems likely have a BCP in place. Regularly review and update BCPs for effectiveness. Minimally, a BCP should:

- Identify critical processes and define recovery time objectives.
- Establish clear procedures that continue essential services during disruption events.

Integrating cybersecurity considerations into the BCP is vital for ascertaining that recovery efforts account for potential cyber incidents. This integration enhances the organization's ability to successfully maintain operations and swiftly recover in the face of cyber threats.

By focusing on comprehensive backups, rigorous restoration testing, and a well-integrated BCP, organizations can strengthen their cyber resilience and help ensure the continuity of critical industrial operations.

Summary

Implementing ZT security principles in OT environments is a complex but essential endeavor. It goes beyond a mere technological upgrade, representing a fundamental shift in security philosophy, one that assumes adversaries may already be present in the network. Unlike traditional IT security models, ZT in OT must balance the imperatives of safety, reliability, and continuous operation.

Successfully navigating this journey requires a holistic approach that includes comprehensive asset visibility, robust identity and access management, and proactive supply chain risk management. Layered security controls—such as network segmentation, secure communication protocols, and rigorous vulnerability management—serve as foundational building blocks. However, tools and technologies alone are insufficient to achieve ZT.

Strong collaboration between IT, OT, and cybersecurity teams is critical to achieving effective and sustainable implementation of technology and processes. This collaboration requires breaking down organizational silos, fostering mutual understanding, and tailoring ZT principles to the unique characteristics and operational requirements of each OT environment. Ultimately, ZT in OT is not about achieving perfection or zero risk, but about making informed, deliberate decisions that reduce exposure and improve resilience without compromising mission-critical operations.

Feedback

Government and critical infrastructure entities should direct any feedback and questions to the relevant office:

- DoW Zero Trust Portfolio Management Office: osd.pentagon.dod-cio.mbx.zt-pfmo@mail.mil
- CISA: zerotrust@cisa.dhs.gov

Resources

- CISA: Zero Trust Maturity Model
- DoW: Zero Trust Strategy: DoD Zero Trust Strategy
- DoW: Zero Trust Reference Architecture
- DOE: Office of Cybersecurity, Energy Security, and Emergency Response (CESER)
- CISA: Secure by Demand: Priority Considerations for Operational Technology Owners and Operators when Selecting Digital Products
- NIST: Cybersecurity Framework 2.0
- NIST: Special Publication 800-207: Zero Trust Architecture
- NIST: Special Publication 800-63B-4: Digital Identity Guidelines: Authentication and Authenticator Management
- NIST: Special Publication 800-82r3: Guide to Operational Technology (OT) Security
- CISA: Guide to Securing Remote Access Software
- ISA/IEC: 62443 Series of Standards (a comprehensive set of standards for industrial automation and control systems [IACS] security)
- MITRE ATT&CK®: Matrix for ICS
- SANS Institute: ICS Security Resources
- Forrester: Zero Trust In Practice
- CISA: ICS Advisories

Disclaimer

CISA and the authoring agencies do not endorse any commercial entity, product, company, or service, including any entities, products, or services linked within this document. Any reference to specific commercial entities, products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring by CISA and the authoring agencies.

Acknowledgements

The DoW Zero Trust Portfolio Management Office, CISA Zero Trust Office, DOE Office of the Chief Information Officer, and DOE's owners and operators for providing and coordinating zero trust and OT expertise across the U.S. interagency.

Version History

April 29, 2026: Initial version.

Appendix: Acronyms

Table 2 lists all the acronyms used in this document and their definitions.

Table 2. Acronyms

Acronym	Definition
BCP	Business continuity plan
CISA	Cybersecurity and Infrastructure Security Agency
CSF	Cybersecurity Framework
DMZ	Demilitarized Zone
DoW	Department of War
DOE	Department of Energy
DOS	Department of State
EDR	Endpoint detection and response
FBI	Federal Bureau of Investigation
HMI	Human machine interface
IR	Incident response
I/O	In/Out
ICAM	Identity, credential, and access management
ICS	Industrial Control Systems
IT	Information technology
JIT	Just-in-time
LOTL	Living off the land
MOC	Management of Change
MFA	Multifactor authentication
NIST	National Institute of Standards and Technology

Acronym	Definition
OS	Operating system
OT	Operational technology
PLC	Programmable logic controller
RBAC	Role-based access control
SBOM	Software bill of materials
SDN	Software-defined networking
SIEM	Security information and event management
SPAN	Switched port analyzer
SSVC	Stakeholder-Specific Vulnerability Categorization
TAP	Terminal Access Point
ZT	Zero trust
ZTA	Zero trust architecture
ZTMM	Zero Trust Maturity Model

References

Stouffer, Keith et al. “Guide to Operational Technology (OT) Security.” NIST Special Publication. NIST SP 800-82r3 (2023). https://doi.org/10.6028/NIST.SP.800-82r3.