Zero Trust Guidance for Critical Infrastructure

Applying Zero Trust to Operational Technology (OT) and Industrial Control System (ICS) Environments

cloud security alliance®

The permanent and official location for the CSA Zero Trust Working Group is https://cloudsecurityalliance.org/research/working-groups/zero-trust/

Acknowledgments

The scope of Zero Trust research and guidance necessarily includes cloud and on-premises environments along with mobile endpoints and applies to the Internet of Things (IoT) and operational technology (OT). The goals of the CSA Zero Trust (ZT) Working Group are to:

- Collaboratively develop and raise awareness of Zero Trust best practices as a modern, necessary, and cloud-appropriate approach to Information Security (InfoSec).
- Provide thought leadership and educate the industry about the strengths and weaknesses of different ZT approaches so organizations can make informed decisions based on their specific needs and priorities.
- Take a deliberately product- and vendor-neutral approach to architectures and implementation approaches for mature Zero Trust implementations.
- Take technically sound positions on Zero Trust and make defensible recommendations while remaining product- and vendor-neutral.
- The working group is composed of 9 different work streams that align with the Zero Trust Pillars.
- The lead workstream for this document is ZT4 - Devices, led by Jennifer "JJ" Minella and Joshua Woodruff.

Lead Authors

Jennifer Minella
Joshua Woodruff

Contributors

Dr. Ron Martin
Mark Fishburn
Michael Roza
Philip Griffiths
Roland Kissoon
Anna Pasupathy
Shamik Kacker
Rajesh Murthy
Samia Oukemeni
Gaurav Agarwaal
Shruti Kulkarni
Nathan Moser

Reviewers

Erik Johnson
Jason Garbis
John Kindervag
Chandra Rajagopalan
Will Schmitt
Alex Sharpe
Karen Uttecht
Annie Weathers
Will Schmitt
Mike Vo
Matthew Rogers
Vaibhav Malik
Mehmet Yilmaz
Venkatesh Gopal

CSA Global Staff

Erik Johnson
Stephen Smith

Additionally the CSA would like to thank the following valued collaboration partners for their interest in, contributions to and review of this document:

- US Department of Defense (DoD)
- US Cybersecurity and Infrastructure Security Agency (CISA)
- US National Security Agency (NSA)
- MIT Lincoln Labs
- Mitre Corporation
- Johns Hopkins University APL

Table of Contents

Abstract

This document delves into the critical and nuanced application of Zero Trust (ZT) principles within Operational Technology (OT) and Industrial Control Systems (ICS). It aims to bridge the gap between traditional information technology (IT) security methodologies and the unique demands of OT/ICS in Critical Infrastructure (CI) sectors. Recognizing the distinct challenges and architectures inherent in these environments, the paper not only clarifies the foundational concepts of ZT but also provides a tailored roadmap for implementing these principles effectively in OT/ICS settings. This roadmap employs a systematic approach from defining Protect Surfaces to continuous monitoring and maintenance based on the five-step process outlined in the NSTAC Report to the President on Zero Trust and Trusted Identity Management, ensuring resilience and security in CI amidst a rapidly evolving digital technology and threat landscape.

Target Audience

The primary audience is any security professional function, such as: Cybersecurity Architects, Security Engineers, SOC Analysts, ZT Practitioners, Operational Technology (OT) and Industrial Control Systems (ICS) Operators and Engineers, IT personnel, and Executive Stakeholders overseeing ZT strategy and/or Operational Technology.

The secondary audience is Chief Information Security Officers (CISOs), Threat Modelers, Incident Managers, Auditors, Business and Operational System Owners, Compliance Officers, Risk Managers, Network Administrators, IT Compliance Analysts, Data Privacy professionals, and vendors producing solutions and technologies in this space.

Introduction

Goal

The goal of this paper is to educate the target audience on considerations and application of ZT principles for Critical Infrastructure (such as energy, water, transportation, and healthcare), with a focus on Operational Technology (OT) and Industrial Control Systems (ICS). This guidance should serve as a tool for communication and collaboration between teams tasked with cybersecurity policies and controls and the system owners and operators of OT and ICS. Securing OT/ICS assets, especially in CI sectors, requires education and collaboration among cross-functional teams.

Document Scope

The scope of this document is centered on operationalizing Zero Trust security frameworks specifically within the Operational Technology (OT) and Industrial Control Systems (ICS) landscapes. It is dedicated to delineating practical strategies and specific methodologies tailored for CI environments. The document offers a detailed examination of the inherent differences between traditional IT and OT/ICS systems, focusing on aspects such as network design, device heterogeneity, and specific security requirements. It then progresses into a step-by-step implementation guide, presenting actionable insights for each stage of deploying a ZT model in these unique settings. This includes specific guidance on identifying critical assets, mapping data flows, constructing a tailored ZT Architecture (ZTA), policy formulation, and the nuances of continuous monitoring within an OT/ICS context. Targeted primarily at security architects, OT/ICS operators, and decision-makers in CI, this document serves as a comprehensive manual for adapting and applying ZT principles in sectors where security is paramount and yet distinctly challenging.

What Is Zero Trust?

"Zero Trust is a cybersecurity strategy premised on the idea that no user or asset is to be implicitly trusted. It assumes that a breach has already occurred or will occur, and therefore, a user should not be granted access to sensitive information by a single verification done at the enterprise perimeter. Instead, each user, device, application, and transaction must be continually verified.[1]"

Traditional, centralized, trust-based, "castle and moat," physical network perimeter security architectures are increasingly ineffective in today's decentralized computing landscape and remote workforce environments, where few organizational assets and users still reside inside the "castle."

Sophisticated threat actors are increasingly adept at exploiting any exposed technical or human vulnerability in modern, highly distributed enterprise networks that often leverage Internet connectivity

[1] NSTAC Report to the President on Zero Trust & Trusted Identity Management, pg. 1 & CSA definition of Zero Trust

heavily. Successful cyberattacks generally exploit implicit trust in some manner. This makes "trust" within digital systems a dangerous vulnerability that should be mitigated and managed. With ZT, all network assets and packets are implicitly untrusted and treated identically with every other packet flowing through the system. The trust level is defined as zero, hence the term Zero Trust.

ZT is an extensible, holistic enterprise security strategy that encompasses cloud/multi-cloud (all service models), on-premise/hybrid systems, internal and external partner/stakeholder user (organization-managed and Bring Your Own Device (BYOD)) endpoints, is inclusive of operational technology (OT), Industrial Control Systems (ICS) and Internet of Things (IoT), and even extends to physical security in some cases. Consequently, ZT has been compared to a mountain that should be climbed one step at a time[2]; that is, implemented incrementally and in a risk-based manner. These principles are a common theme in Cloud Security Alliance (CSA) Zero Trust (ZT) guidance.

Executive Summary

In most nations, the health of public services relies on secure and resilient Critical Infrastructure (CI). These infrastructures are deemed critical because their incapacitation or destruction would have a debilitating impact on the national security, economy, and social welfare of a nation. Operational Technology (OT) systems serve as the backbone of CI around the world.

"OT encompasses a broad range of programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems/devices detect or cause a direct change by monitoring and/or controlling devices, processes, and events. Examples include industrial control systems (ICS), building automation systems, transportation systems, physical access control systems, physical environment monitoring systems, and physical environment measurement systems."[3]

Critical Infrastructure Sectors

From energy and transportation to telecommunications, water supply, and healthcare, CI sectors collectively constitute the vital frameworks upon which modern civilizations rely.

Governments worldwide have become increasingly alert to the multifaceted threats facing CI. This heightened awareness stems not only from actual compromises but also from the discovery of sophisticated threat actors employing "living off the land" techniques. These adversaries exploit legitimate tools and processes within the infrastructure itself, making detection and mitigation particularly challenging. Such tactics underscore the need for comprehensive protection strategies that go beyond traditional security measures.

[2] CISA Zero Trust Maturity Model

[3] NIST Guide to Operational Technology (OT) Security: NIST SP 800-82r3

The United States President's Council of Advisors on Science and Technology (PCAST) issued a report outlining strategies to strengthen the nation's cyber-physical systems.[4] PCAST's recommendations offer a comprehensive approach to bolstering CI resilience. They advocate for setting clear performance goals, ramping up research into vulnerabilities, and establishing a national observatory to stay ahead of threats. The report also emphasizes breaking down organizational silos, strengthening government support, and holding industry leaders accountable. These suggestions aim to ensure our critical services can withstand adversity and keep running smoothly, even when faced with natural disasters, cyber attacks, or human errors.

Survey of Global Critical Infrastructure Sectors

CI sectors are recognized for their importance to national security, public health, safety, and economic stability, and encompass a diverse array of industries.

In the United States, the Cybersecurity and Infrastructure Security Agency (CISA) currently identifies 16 sectors as Critical Infrastructure[5]. Around the globe, governments and regional entities have defined CI sectors in ways that are most meaningful to them. Many of these can be viewed in a report by the International Critical Information Infrastructure Protection (CIIP)[6]. Published in 2008, the CIIP remains an unparalleled resource, meticulously detailing CI sectors across 25 countries and seven leading international organizations. Its comprehensive analysis offers invaluable insights on CI protection worldwide.

Common sectors widely viewed across the world as CI include (but are not limited to):

1. Energy (gas, petroleum fuels, refineries, pipelines, power generation and distribution/transmission)
2. Water (water supply, wastewater treatment)
3. Banking and finance (banks, financial organizations, trading exchanges)
4. Emergency services (law enforcement, fire, emergency response)
5. Healthcare (hospitals, clinics, labs)
6. Food supply (production, storage, distribution)
7. Communications (telecommunications, phone, fax, Internet, news media)
8. Public venues (sports arenas, stadiums, gathering places, places of worship)
9. Transportation and logistics (air, road, rail, sea and shipping/cargo/postal services)
10. Critical manufacturing (e.g., automotive, chemical, electronics, pharmaceuticals)
11. Government and public administration (e.g., departments, systems, facilities)
12. Education (schools, universities)

While these are the common sectors globally, in the United States, CISA also includes the following, many of which are applicable globally:

1. Chemical (basic, specialty, agricultural, and consumer)

[4] PCAST Releases Report on Strategy for Cyber-Physical Resilience
[5] Critical Infrastructure Sectors | CISA
[6] International CIIP Handbook 2008/2009

2. Commercial Facilities (entertainment and media, gaming, lodging, outdoor events, public assembly, real estate, retail, and sports leagues)
3. Dams (hydroelectric power, water supplies, irrigation, flood control, river navigation, industrial waste management, and recreation)
4. Military/defense departments and the Defense Industrial Base (a worldwide industrial supply chain that enables the military)
5. Information Technology (central to the nation's security, economy, and public health and safety due to increasing dependency on technology)
6. Nuclear Reactors, Materials, and Waste (power reactors, research and test reactors, active nuclear fuel cycle facilities, and licensed users of radioactive sources)

In April 2024, US President Biden issued a National Security Memorandum on Critical Infrastructure Security and Resilience, updating federal policies and responsibilities for protecting these vital sectors.

Nations worldwide are responsible for protecting their CI against both natural disasters and human-induced threats, including terrorist and cyber attacks. The ownership model of these vital assets varies globally, with a mix of public and private stakeholders. In many countries, a significant portion of CI is privately owned and operated, adding complexity to protection efforts.[7]

ZT in CI and OT/ICS Environments

CI is crucial for maintaining the well-being of communities and ensuring the resilience of nations in the face of various threats, both natural and man-made. And now, as societies become increasingly interconnected and dependent on technological advancements, the protection of CI has evolved into a global imperative, and the need for ZT along with it.

CI often consists of complex, interconnected networks that are increasingly internet-connected, making them susceptible to simple and sophisticated cyberattacks. A ZT approach authorizes access requested by users, devices, and applications, ensuring that every interaction and access request is thoroughly authenticated and contextually validated.

Unfortunately, it's widely acknowledged that many OT and ICS environments rely heavily on legacy systems, specialized protocols, and are often closed systems that cannot easily be patched or upgraded. Also, many organizations do not have an accurate inventory of their OT/ICS assets, and they are often poorly understood by those tasked with operating and securing them.

The following sections capture the main themes and trends applicable to implementing ZT within an OT/ICS environment.

[7] Critical Infrastructure Protection: CISA Should Improve Priority Setting

Unique Threat Vectors for Critical Infrastructure

The history of attacks on CI over the decades ranges from curious teenagers to hacktivism and even targeted nation-state attacks driven by political motives, highlighting the diverse and evolving nature of threats these sectors face. These unique threat vectors are compounded by the fact that traditional IT security practices often don't easily translate to OT environments, particularly in essential services; for instance, many OT devices lack IP addresses or standard operating systems, making conventional vulnerability patching strategies ineffective or inapplicable.

Regardless of the attacker's motivation, CI sectors are prime targets due to their vital roles in communities and economies. Below are key reasons why these environments attract malicious actors. While this list focuses on threat vectors, additional challenges of OT are provided further down in the Differences in Architecture & Technology of OT vs IT section.

- **Regulatory and Compliance Pressure:** The complex regulatory landscape governing CI can inadvertently create vulnerabilities. Compliance-focused security measures may not always align with the most effective cybersecurity practices, potentially leaving gaps that attackers can exploit.
- **Insider Threats:** Employees, contractors, or other individuals with insider knowledge and access to CI systems pose a unique risk. Whether acting maliciously or through negligence, insiders can bypass security measures and cause significant damage or disruption.
- **Supply Chain Vulnerabilities:** CI often relies on complex, global supply chains for both hardware and software components. Compromises in the supply chain can introduce vulnerabilities or malicious elements into systems, potentially affecting entire sectors without direct intrusion.
- **High Impact:** Disrupting or damaging CI can significantly affect public safety, national security, and the economy. Attackers aim to cause widespread chaos or interrupt essential services.
- **Interconnected and interdependent Systems:** CI sectors are highly interconnected and often interdependent. A breach in one area can cascade into others through lateral movement or interdependent connections, leading to a domino effect that amplifies the attack's impact.
- **Economic Motivations:** Some attacks on CI are financially motivated. Attackers may seek to extort money from organizations or nations by threatening to disrupt essential services unless a ransom is paid.
- **Cyber Espionage:** Nation-states and cybercriminals may target CI for the purpose of espionage. Gaining unauthorized access to industrial systems allows them to gather intelligence on a country's capabilities, vulnerabilities, and strategic assets.
- **Political Motivations:** Attacks on CI can be politically motivated, to destabilize a nation or exert pressure on governments to meet certain demands. This could be driven by geopolitical tensions, disputes, or ideological conflicts[8].

[8] DoD Zero Trust Symposium 2024 - DAY 2 - Defense Acquisition University

- **Easy Targets:** Many CI systems use legacy technologies that were not designed with modern cybersecurity considerations in mind. These systems may have vulnerabilities that can be exploited by attackers, with limited security measures and alerting.
- **Nation-State Cyber Warfare:** Nation-states may engage in cyber warfare and view CI as a strategic target. Disrupting an adversary's infrastructure can be a way to gain a strategic advantage in conflicts without resorting to traditional military means.
- **Physical Security:** OT/ICS attract malicious actors due to their exposed, often under-guarded nature, offering opportunities for direct tampering, espionage, and sabotage, exploiting physical vulnerabilities. An attack on physical infrastructure is oftentimes the easiest yet most impactful attack.[9]

Ransomware and data exfiltration have been prevalent attacks impacting CI in recent years. However, this trend may shift as new toolkits are deployed and threat actors' political motivations evolve to target Industrial Control System (ICS) with the intent to disable or disrupt them. These sectors are also commonly the victims of unsophisticated attacks, including social engineering, physical attacks, and attacks that leverage vulnerable ancillary service providers such as card readers and security camera systems.

Convergence of OT/IT with Digital Transformation

While recent technological advancements have increased our productivity and capabilities, the threat landscape has similarly evolved. When disparate systems at various security levels or maturities are interconnected, implementing relevant and reliable security controls across them becomes a big challenge.

In particular, the growth and ubiquity of the Internet, cloud, and industrial internet-of-things (IIoT) in the last two decades and their interconnectivity created numerous access points to critical systems, poking multiple holes in the previously less porous environment. The rush to embrace digital transformation interconnected these systems to increase productivity, efficiency, and agility, and exposed these systems further. In addition, inherent weaknesses in the traditional supply chain networks were exacerbated by increasingly connected systems that allow wider access once the attackers gain entry.

Historically, OT was “air gapped”, where it was completely disconnected physically from other networks. Presently, air gapped systems are rarely found in industry. Modern systems are often interconnected via embedded wireless access, cloud and other internet-connected services, and software-as-a-service (SaaS) applications. Even legacy systems interface with maintenance laptops or removable media for backups, maintenance upgrades and patches, or data transfers. This shift from air gapped systems to fully integrated networks, and the associated risk, must be accounted for when creating and applying security controls.

Here are a few key considerations for IT and security professionals tasked with securing OT/ICS environments.

[9] Third North Carolina Power Substation Targeted by Gunfire as BPS Physical Security Concerns Mount

Technological Advancements

Disruption in technology forces these systems to change. Once isolated, air-gapped systems are now increasingly interconnected within OT environments. The shift from serial to Ethernet connections, embedding wireless adapters in OT components, and interfacing with devices for maintenance have all contributed to a more connected, yet potentially vulnerable landscape. These once stable systems are now hooked up to dynamic, interconnected networks, forcing them to adapt to new risks and challenges.

Critical Infrastructure Interconnectivity

Collapsing boundaries and highly interconnected systems make CI sectors interdependent and tightly coupled. A disruption in one can trigger a chain reaction, causing a series of failures across others. For instance, power companies supply electricity to most other sectors, with even high-criticality entities having limited backup generation capabilities. Water is crucial for cooling servers, launching missiles, and producing steam for industrial processes. Refineries obtain crude oil from, and push products through, pipeline systems. Each of these cross-sector dependencies involves data flow between different entities, creating a complex web of interconnections where an attack on one sector could potentially trigger cascading disruptions across multiple industries or companies, amplifying the impact far beyond the initial target.

OT and IT Integration

The integration of OT and IT systems has accelerated, driven by the need for remote access, system monitoring and control, and data aggregation, analysis, and reporting. Integration and convergence, exemplified by Industry 4.0, extends beyond simple data collection to include bidirectional communication and control. For instance, outage notifications and responses now often require seamless OT/IT integration, with data from operational systems feeding into IT-managed communication channels.

Increasingly, OT data is being sent to cloud platforms for advanced monitoring and analytics. This trend is evolving towards more sophisticated, bidirectional data flows, allowing for real-time adjustments based on cloud-processed insights. A prime example is the tracking of goods from manufacturing through transportation to distribution, particularly crucial in food and pharmaceutical industries. Here, data continuously flows between OT systems (production lines, transportation sensors) and IT systems (inventory management, logistics planning), creating a digital thread that enhances efficiency and traceability.

While this integration offers significant benefits, including improved efficiency and data-driven decision-making, it also introduces new vulnerabilities due to increased connectivity and the blurring of traditional OT-IT boundaries. The challenge lies in harnessing these advantages while maintaining robust security across the converged infrastructure.
All in all, businesses are striving to enhance the efficiency of their OT/ICS systems and leverage these assets for broader business purposes, necessitating connections to both internal networks and external systems. In this context, ZT offers significant value-add to accelerate business growth securely. Adopting a ZT approach aids in securing systems, satisfying audit, legal, and compliance requirements, and

defending against cyberattacks. It enables organizations to pursue their goals rapidly in an ever-changing environment while maintaining robust security.

Importantly, ZT is not limited to new implementations. While successful implementation of a Zero Trust Architecture (ZTA) naturally leads to a 'secure-by-design' approach for new projects, it can also significantly strengthen existing systems. Through careful application of ZT principles, organizations can achieve 'secure-by-retrofit' for legacy systems, enhancing their security posture across both new and existing infrastructure. This dual applicability makes ZT a powerful strategy for comprehensive security improvement in OT/ICS environments.

Differences in Objectives of OT vs IT

To fully appreciate how and why OT/ICS environments operate as they do, it's essential to understand the primary business objectives and operational culture of these systems, which vary significantly from traditional enterprise IT environments.

CIs and the OT/ICS systems they rely on are, by definition, mission-critical. Unlike IT systems, which are often designed with the cybersecurity-focused CIA triad (confidentiality, integrity, and availability) in mind, OT/ICS systems were designed mainly for reliability and safety, where confidentiality and integrity receive less attention. This difference stems from the operational focus of OT/ICS environments, where maintaining continuous and safe operation is crucial, and downtime can have severe consequences. In these systems, safety is paramount, focusing on protecting human lives and preventing physical harm or damage to both people and the environment.

Here are a few related considerations for professionals securing OT/ICS environments.

Resilience, Uptime, and Safety Are Primary Objectives

Critical systems only allow for a narrow window of opportunity for maintenance and upkeep. Introducing newer tools and technologies into critical and legacy systems requires careful evaluation and testing to ensure implementation will not interfere with safety or operations. During a cybersecurity incident, preventing further damage and impact can mean slowing down or taking these essential services and systems offline, which will cause disruption to normalcy or even bring a nation to its heels.

Systems are Static, Complex, and Expensive

CI systems are characterized by high costs, extended lifespans, and intricate designs. These factors, combined with lengthy deployment processes, contribute to their static nature, making them less adaptable to evolving threats.

Assets often operate far beyond their intended lifespan, sometimes outliving the original equipment manufacturer (OEM) support cycle. Replacing or upgrading these systems is a complex, time-consuming process involving extensive design, engineering, procurement, and testing phases. This is particularly crucial for critical applications where errors could significantly impact safety, health, or the environment.

Consequently, older systems, despite potential security risks, are often maintained to extend infrastructure life while careful replacement processes are underway. This creates a unique challenge in balancing operational continuity with necessary security upgrades.

Further complicating matters, many OT systems use proprietary protocols, making regular updates difficult and creating vulnerabilities that attackers can exploit. This complexity adds another layer to the challenge of securing and modernizing OT/ICS environments.

Differences in Architecture & Technology of OT vs IT

In addition to the differences in the overall objectives for OT/ICS versus enterprise IT environments, there are also significant differences in the architecture and technologies used, at least within portions of OT/ICS systems. As mentioned in the Unique Threat Vectors for Critical Infrastructure section above, these differences provide further detail on additional challenges unique to OT/ICS.

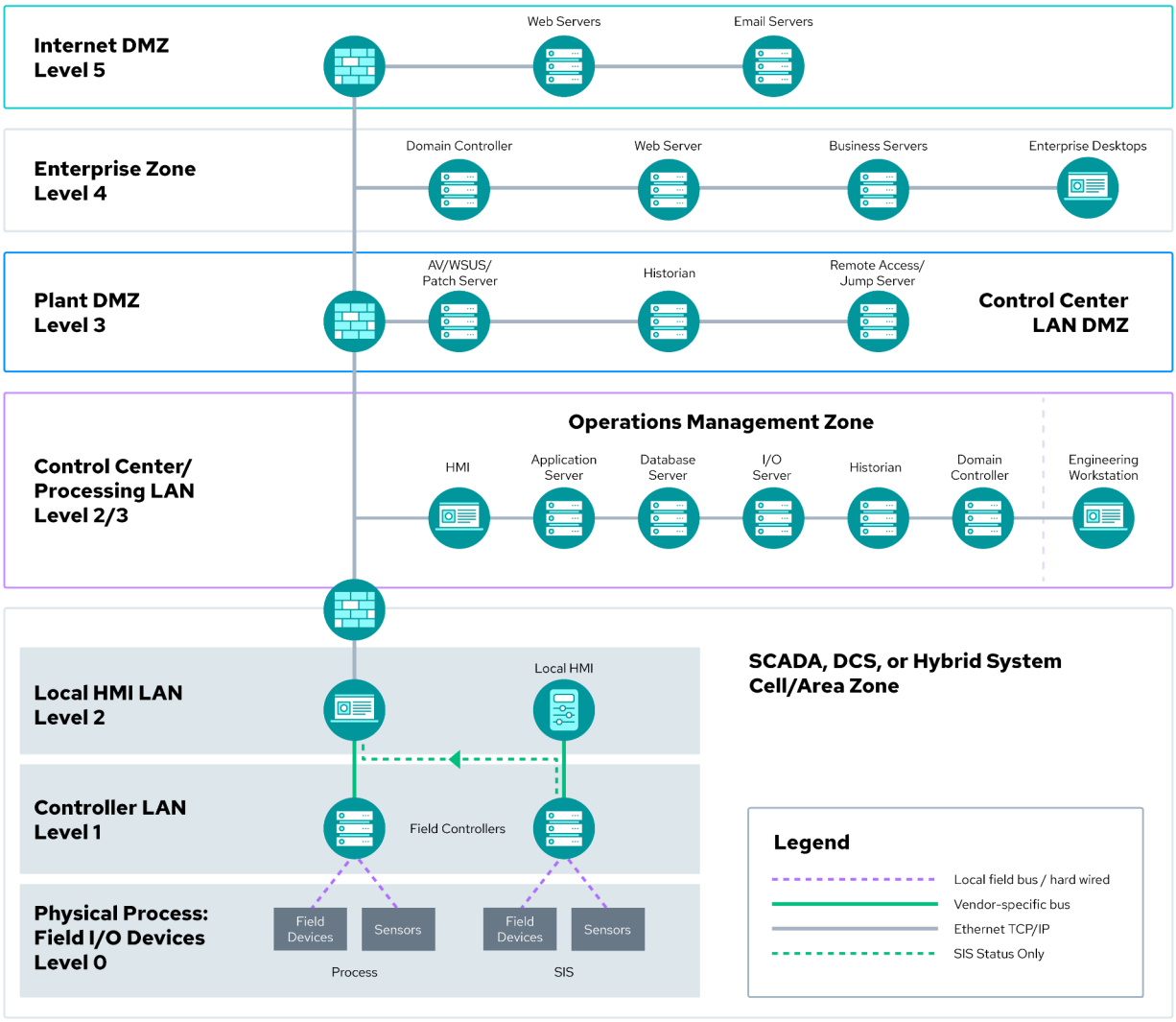
These differences are an important distinction to understand, because while overarching concepts like ZT can (and should) be applied to all segments, the details of the security policies and how the controls are applied and operationalized may vary.

For example, a standard enterprise IT cybersecurity policy may dictate a user lockout after three failed attempts. But, in an OT/ICS environment, the last thing you want to do is lock out the system operator from the HMI (Human-Machine Interface) they need to access in an emergency where human safety is at risk. Similarly, patching is a prominent and consistent part of vulnerability management on the enterprise IT side. In contrast, within OT/ICS networks, patching is the appropriate mitigation often less than 10% of the time, and by many reports, the number is much lower at 4%[10].

Here are considerations an IT or cybersecurity professional may face while securing an OT/ICS environment.

The Purdue Model[11] offers a common reference model to visualize the components and connections within an OT/ICS environment. Albeit insufficient for addressing modern cloud- and SaaS-connected infrastructures, this model serves well as a tool to communicate a few basic concepts covered throughout this paper.

[10] Dragos 2023 OT Cybersecurity Year in Review
[11] Cloud Industrial Internet of Things (IIoT) - Industrial Control Systems Security Glossary



Sample Purdue Model

Prevalence of Legacy Systems and Applications

Looking at the sample Purdue Model for context, the closer an asset is to the process execution level (Levels 0 and 1), the more proprietary the systems and protocols in use. However, the systems involved in process control, automation, and management (Levels 2 and 3) are most often comprised of Windows and Linux operating systems of varying types and ages. Many of these systems are running outdated and/or vendor-modified versions of operating systems that are rarely patched and are maintained by following processes and cycles different from traditional enterprise IT systems and endpoints.

The prevalence of legacy systems extends well beyond outdated operating systems and applications. For many of the world's CI environments, the OT/ICS systems running them are composed of cyber-physical assets with expected serviceable life spans measured in decades, not years.

From manufacturing automation systems to power generation to the pumps and flow sensors in wastewater treatment plants, components may be installed and serviced for 10, 20, and even 50 years.

Each year, many reports and surveys of OT/ICS networks prove the continued use of legacy systems within these environments. Most of these systems lack even basic protections. For example, one report[12] demonstrates:

- 71% have outdated operating systems.
- 66% have no automatic antivirus protection.
- 27% of industrial sites have at least one direct connection to the Internet.
- 54% have at least one remotely accessible device.
- 22% exhibited indicators of threats.
- 64% have plain-text passwords.

Unique Protocols and Proprietary Configurations

For IT and cybersecurity professionals, navigating the world of OT/ICS means understanding (at least conceptually) new protocols, learning a new vocabulary, understanding new risks, and developing new skill sets.

Industrial control protocols

The OT/ICS devices and networks, particularly in the lower levels of the Purdue Model, will be operating using a suite of protocols specific to the environment. For example, these may include combinations of Modbus, PROFIBUS, PROFINET, OPC, MQTT, EtherNet/IP, Fieldbus[13], and RS-485, among others.

And, while the protocols may use various well-documented industry standards, the exact configurations within the OT/ICS assets may vary from implementation to implementation, and may not be well-documented by the vendor or OT operator. For example, Modbus is a standard, but how the vendor or installer programmed the Modbus mapping for a particular PLC may be different.

Because of this, discovering and managing vulnerabilities and misconfigurations becomes more difficult. Unlike assets running standard operating systems, these devices can have custom operating systems, or no operating system at all, and rarely have patches available. Even if they did, downtime is often not an option due to uptime constraints, or the inability to install them.

Antiquity and aging of the system, as well as older technologies, allow less room for improvement. Often, the components were designed to do a specific function and have limited capabilities by design. Thus, limitations such as a lack of computational resources, limited function, and limited memory allow little to no room to update or add new security measures.

[12] Global IoT-ICS Risk Report (2020)
[13] What Is Fieldbus? Learn the Basics of a Fieldbus Network

Unencrypted communication

By design, many of these protocols (specifically those designed to run within the local control process zones) are unencrypted. The absence of encryption in OT systems leaves critical communication channels exposed to interception and manipulation. This vulnerability allows malicious actors to eavesdrop on sensitive operational data, inject false commands, or disrupt communication between control systems and field devices. Such actions can lead to unauthorized control over industrial processes, potentially causing operational disruptions, equipment damage, or even safety hazards.

However, many of these protocols were not designed to be encrypted, and overlaying encryption for these protocols can (and frequently does) introduce a latency that is intolerable or even hazardous in OT/ICS systems that depend on real-time communication.

For example, the use of encryption can add latency to communications, which may impact the real-time operations critical in ICS environments. These delays could affect the timely execution of commands or the synchronization of systems, leading to potential disruptions in control processes. In extreme cases, this could create a scenario where safety mechanisms are delayed or fail to operate as intended, especially in tightly coordinated systems like those found in power generation or chemical processing.

Knowledge and Skillset

Multi-generational hardware, architecture, and technologies in OT/ICS demand wider knowledge in multiple areas. Cross-training team members between OT and IT, along with setting up permanent cross-functional teams, is a strategy many organizations have found successful when building their OT/ICS cybersecurity practice. However, this integration of diverse skill sets presents a significant challenge, requiring careful planning, resources, and ongoing commitment to bridge the traditional divide between OT and IT domains.

Additional Physical Exposure

A significant and often underappreciated vulnerability in CI is the physical exposure of many assets. Unlike traditional IT systems housed in secure data centers, numerous OT/ICS components are deployed in open, accessible environments. Wind turbines, power transformers, pipeline pumping stations, and water treatment facilities are just a few examples of critical assets often situated in remote or publicly accessible locations.

This physical exposure presents multiple risks:

1. Direct tampering or sabotage by malicious actors
2. Vulnerability to natural disasters and extreme weather events
3. Potential for unintentional damage from accidents or human error
4. Opportunities for adversaries to gather intelligence through physical observation

Protecting these exposed assets requires a multi-layered approach that integrates physical security measures with technical controls. This may include perimeter security, surveillance systems, access

control mechanisms, hardened equipment housings, and regular physical security audits. Moreover, resilience planning must account for both physical and cyber threats, recognizing that a comprehensive security strategy addresses both domains in tandem.

While physical security in OT/ICS presents unique challenges, the guidance in this paper can help. As you'll soon learn, walking each of these components through the below five-step implementation process, including identifying what you have as DAAS elements, along with measuring and improving the security capabilities using the ZTMM pillars, provides for a progressive path of securing these components as part of your ZT journey.[14]

Monitoring Needs and Challenges

Monitoring in OT/ICS environments has a long and robust history, primarily focused on operational issues observed by console and field operators. However, the evolving threat landscape necessitates a shift in monitoring practices, particularly in detecting events potentially attributable to cyber-related incidents.

A significant challenge lies in the lack of comprehensive monitoring for malicious activity in OT systems. While operational data is closely watched, security-focused monitoring often lags behind. This gap can lead to cyber-related damages being misattributed to reliability issues or misconfigurations, potentially masking the true nature and extent of security incidents.

Implementing enhanced monitoring capabilities presents its own set of challenges. New connections required for network monitoring inherently increase the attack surface and risk of data exposure. However, the greater concern is that critical security data often isn't being collected, centralized, and correlated effectively by IT and security teams.

The path forward requires a delicate balance. OT environments need to adapt and integrate newer systems for continuous security monitoring while maintaining operational integrity. This evolution calls for increased interoperability between traditional OT monitoring systems and modern security information and event management (SIEM) tools.

Supply Chain Challenges

In OT/ICS environments, supply chain security poses significant challenges, some of which are shared with the IT world but often amplified in operational contexts. While IT faces its own supply chain security issues, OT suppliers typically prioritize business objectives and operational functionality over security to an even greater degree. This focus may result in a lack of built-in security measures throughout the OT supply chain, potentially leading to more severe vulnerabilities in OT/ICS systems. Vendors in this space may not have established processes for reporting, patching, and addressing security issues as robustly as their IT counterparts. Consequently, organizations must pay particularly close attention to the details of their OT/ICS supply chain, navigating a landscape where security information and practices may be less readily available or transparent than in the IT sector. This heightened scrutiny is crucial, as the potential

[14] Zero Trust in the Real World - Physical Security

impact of supply chain vulnerabilities in OT/ICS can have far-reaching consequences for CI and operational safety.[15]

While these challenges are significant, the industry is responding with evolving standards and best practices. For instance, standards related to supply chain security in OT/ICS are increasingly incorporating requirements for formal Validation and Verification (V&V) of cyber-critical devices, software, and upgrades. Standards such as those within ISA/IEC 62443 for Industrial Communication Networks Security exemplify this trend, stipulating V&V in several control objectives. These emerging standards represent an important step towards addressing supply chain vulnerabilities, though their implementation and effectiveness vary across different OT/ICS sectors and regions. Organizations looking to enhance their supply chain security should familiarize themselves with these standards as part of a comprehensive risk management strategy alongside a ZT journey.

Other Differences and Considerations

The list of every minute technical difference between enterprise IT and OT/ICS systems is too long to address, but a few additional considerations that may be novel for IT and security professionals managing cybersecurity for OT/ICS include:

- **Risk:** One of the biggest differences between IT and OT is risk. A failure of CI systems can lead to safety, health, and environmental consequences in addition to the impacts experienced by IT systems, such as financial loss or impact to national security.
- **Scale:** These systems (especially those in power, telecommunications and utility sectors) may be spread over large geographical areas spanning local, regional, national, and international boundaries. Aside from technical and operational differences, this may also introduce unique legal and regulatory considerations.
- **Complexity:** OT/ICS environments are effectively systems of systems due to their composition and the interconnected nature of their operation, typically made up of a variety of subsystems, each designed for specific tasks, such as cases where an OT/ICS system has an IT monitoring and control subsystem. Each subsystem could have its own hardware, software, and operational protocols that need to work in concert to function effectively. These subsystems are not standalone; they depend on one another to function. The failure or malfunctioning of one system can have cascading effects on others, which adds layers of complexity in terms of maintenance and troubleshooting.
- **Longevity:** OT/ICS infrastructures are often a mix of modern and legacy systems and components. These structures emerge and change over time. It's not unusual to see these systems lasting well over 50 years. The normal lifespan of components may be 10 to 15 years. These extended lifespans of systems have inherent risks and consequences to the business, as they must live with decisions made years or even decades ago.
- **Ownership:** There is rarely a single owner and authority for OT/ICS systems. There may be a mix of public and private ownership, both for-profit and nonprofit corporations operating these

[15] Pagers attack brings to life long-feared supply chain threat

systems. This is important to note because it introduces additional decision points and processes if and when the decision is made to optimize or update the systems.

Having explored the CI sectors, the distinctive challenges of OT/ICS, and the impact of digital transformation on the convergence of OT with IT, we now transition to applying ZT principles. The rest of this paper will detail how you can leverage the proven five-step process to effectively fortify your OT/ICS environments using a ZT strategy.

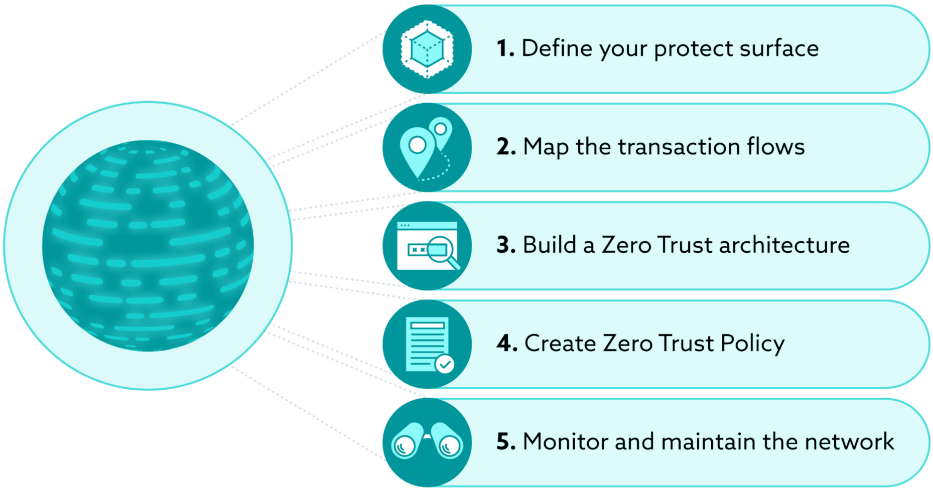
The Zero Trust Implementation Process

The Five-Step Implementation Process

The NSTAC Report to the President on Zero Trust and Trusted Identity Management[16] is a foundational reference document that CSA Zero Trust research leverages and aligns with. It provides an excellent background and overview and compares and contrasts different ZT references and approaches. It also introduces a repeatable, technology-agnostic five-step implementation process for ZT that is well suited to incremental and iterative execution.

1. Define the Protect Surface
2. Map the Transaction Flows
3. Build a Zero Trust Architecture
4. Create a Zero Trust Policy
5. Monitor and Maintain the Network

This document will describe this five-step journey in the context of the scoped CI technologies and sectors.



[16] NSTAC Report to the President on Zero Trust and Trusted Identity Management

Incremental and Iterative Execution

Let's explore how the five-step process enables immediate action and continuous improvement in your ZT journey.

Step 1: Define Protect Surface: Comprehensive Asset Discovery

Begin with a broad, organization-wide inventory and assessment of business and operational assets. This foundational step enables risk-based prioritization, setting the stage for targeted ZT implementation.

Steps 2-5: Focused, Iterative Refinement

For each identified Protect Surface, cycle through steps 2-5. This iterative approach allows for progressive elaboration, continually enhancing your ZT posture as you gain insights and refine your strategy.

This process empowers organizations to start immediately and improve continuously, adapting their ZT implementation to evolving discoveries. Later, we'll explore the "crawl, walk, run" approach, which enables organizations to begin with low-risk iterations and gradually tackle more complex systems.

Before delving into the detailed guidance for applying these steps to OT/ICS environments, let's examine an approach to identify and target ZT maturity levels.

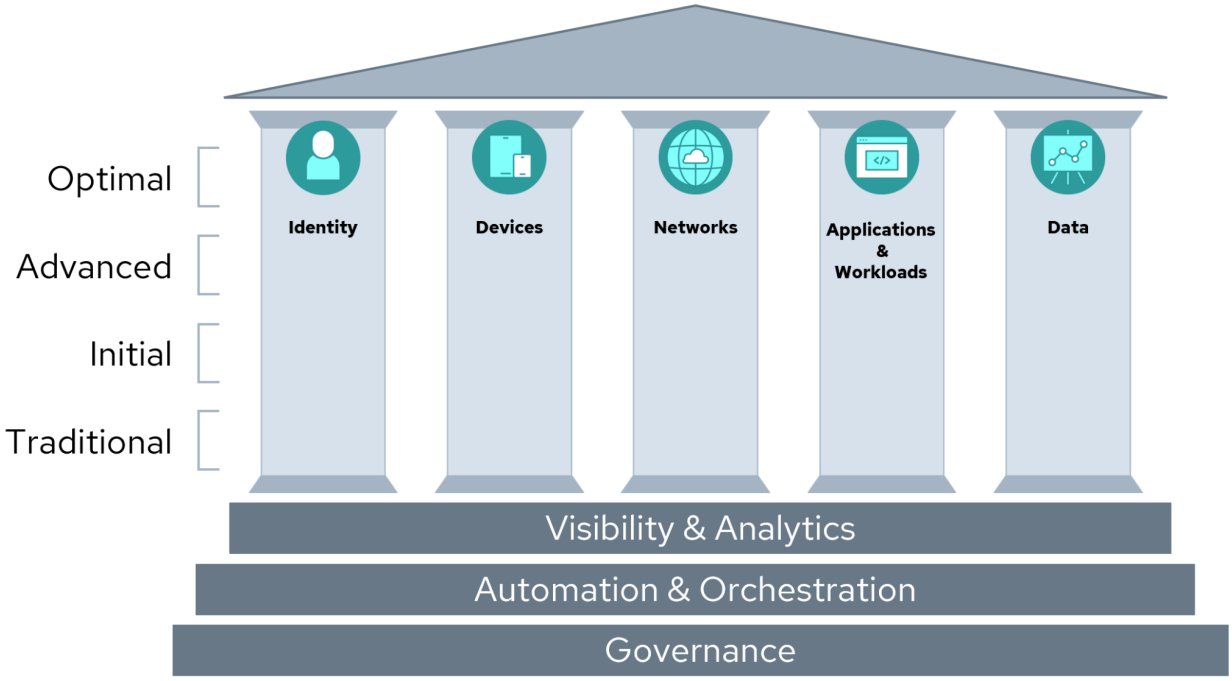
CISA Zero Trust Maturity Model (ZTMM)

The Cybersecurity and Infrastructure Security Agency (CISA) has published a Zero Trust Maturity Model (ZTMM)[17] which represents a gradient of implementation across five pillars in which advancements can be made over time toward optimization through four maturity stages.

CISA ZTMM Pillars

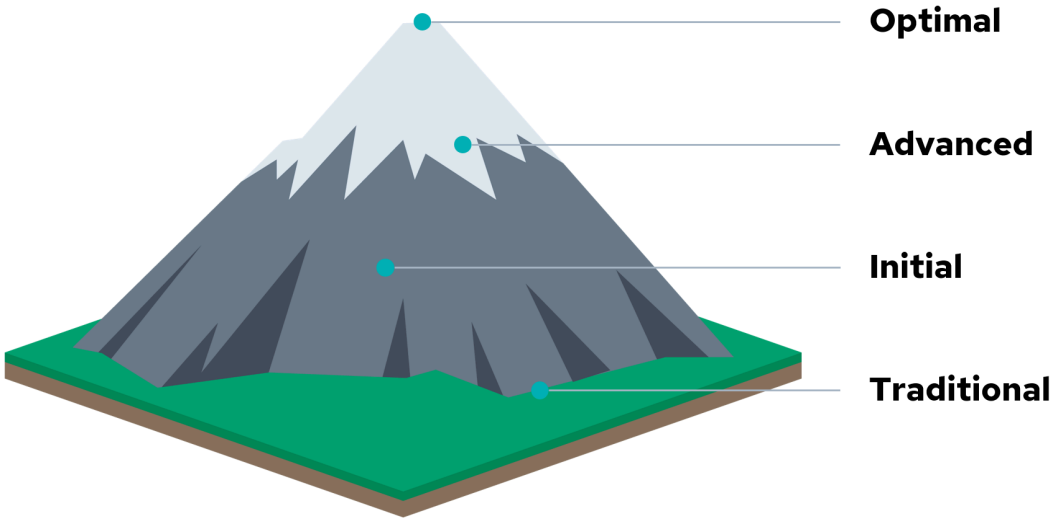
The five pillars, depicted below, include **Identity**, **Devices**, **Networks**, **Applications and Workloads**, and **Data**. Each pillar includes general details regarding the following cross-cutting capabilities: **Visibility and Analytics**, **Automation and Orchestration**, and **Governance**.

[17] Zero Trust Maturity Model Version 2.0



CISA ZTMM Maturity Levels

The stages of a Zero Trust Maturity Model (ZTMM) journey advance from a **Traditional** starting point to **Initial**, **Advanced**, and **Optimal** levels, as depicted below, are meant to facilitate a progressive ZT security journey. Each stage provides greater levels of protection, automation, detail, and complexity for adoption.



While originally published as guidance for US Federal Agencies, this model serves as a key industry reference across public and private industries. The CSA uses it as a key model against which to base a ZT journey in both IT as well as OT/ICS environments.

The U.S. Department of Defense (DoD) has developed its own Zero Trust Reference Architecture and Zero Trust Strategy, which include similar incremental security maturity levels. Notably, the DoD is reportedly enhancing these frameworks to incorporate activities specific to Operational Technology. For those interested in comparing the CISA and DoD approaches to Zero Trust maturity, the CSA offers an informative webinar Understanding the CISA Maturity Model and DoD's Zero Trust Strategy featuring ZT leads from both organizations, providing valuable insights into the similarities and differences between these two influential models.

ZT Implementation Process for OT/ICS

The five-step implementation process for ZT serves OT/ICS environments well. In fact, as shown in the following sections, each of the five steps map to established approaches for managing cybersecurity in OT/ICS and hybrid IT/OT environments, including NIST and the International Society of Automation (ISA) guidance.

Step 1: Defining the Protect Surface for OT/ICS

CSA has produced general Step 1 guidance in the publication Defining the Zero Trust Protect Surface. This section focuses on how this step can be applied to the unique nuances of OT/ICS environments and how it aligns with established OT/ICS guidance.

Defining the Zero Trust Protect Surface involves developing a robust and, ideally, dynamically maintained inventory of the organization's business system assets, classified by their associated risk and criticality to the organization, as well as their current level of security maturity. The organization's asset inventory is used to prioritize the order of ZT implementation, as recommended in the ZT learning curve, described next.

As previously discussed, Step 1 provides the foundation for the entire ZT journey, setting the stage for the iterative process of Steps 2-5. This comprehensive inventory enables organizations to strategically approach their ZT implementation, balancing criticality, risk, and existing security measures.

The Zero Trust Learning Curve: Crawl, Walk, Run

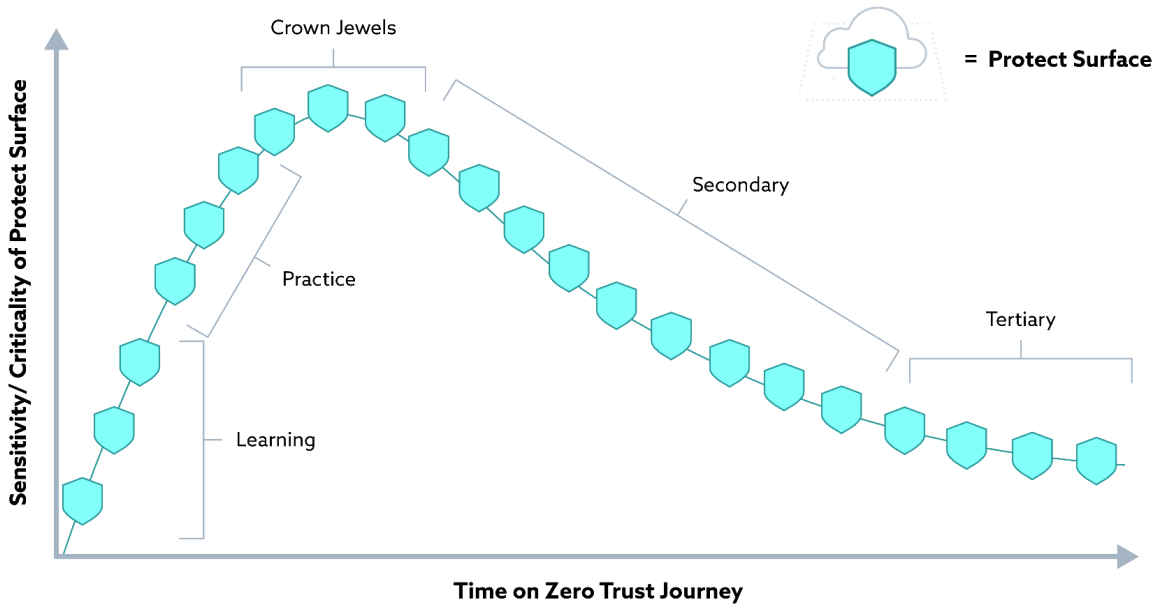
Implementing ZT, like any transformative strategy, benefits from a measured, incremental approach often described as "crawl, walk, run." This methodology is particularly valuable in OT/ICS environments where the stakes are high and disruptions can have severe consequences. It addresses the common pitfall of analysis paralysis—waiting for perfect conditions before taking action. Instead, this approach encourages immediate progress through low-risk initial iterations, setting organizations on a path toward enhanced security without overwhelming their resources or disrupting critical operations.

Organizations often begin by identifying a simple, low-risk "learning" Protect Surface for the first iteration through the five steps. This initial iteration - the "crawl" - allows teams to gain practical experience with

walking through all five steps of the ZT implementation process in a controlled, non-critical environment. As confidence and expertise grow, organizations can "walk" by iterating through practice Protect Surfaces. Finally, in the "run" phase, they tackle the most critical or intricate systems, often referred to as the *crown jewels*.

This strategic, phased approach facilitates a gradual mastery of the ZT implementation process. It builds competence and trust in the process, ensuring that when applied to mission-critical systems, the implementation is both effective and non-disruptive. As the organization progresses, it can extend ZT principles to secondary and tertiary systems, ultimately achieving a comprehensive, enterprise-wide ZTA.

The CSA advises organizations to iterate through several learning and practice Protect Surfaces leveraging existing tools and capabilities before investing in new ZT technologies. This approach yields invaluable insights that inform specific needs, architectural requirements, and integration points. We've observed instances where premature procurement, without this learning phase, resulted in solutions incompatible with core systems and the broader architecture. Such missteps can significantly complicate and slow down the ZT journey. By prioritizing learning over immediate acquisition, organizations can make more informed decisions, ensuring that future investments align seamlessly with their unique ZT requirements and existing infrastructure.



The Zero Trust Learning Curve: Deploying Zero Trust One Step at a Time

Protect Surfaces in OT/ICS

Along with creating the asset inventory, the first step of defining the Protect Surface is also the opportunity to identify the relationship of each asset to the business processes and value. For example, in critical industries like pharmaceuticals, even a single low-cost OT/ICS component can be crucial to meeting demand and sustaining profitability. A cyberattack on a $1,500 logic controller could impact millions of dollars in production and potentially affect access to life-saving drugs.

Identifying the organizational assets to be protected and understanding their business value and relationships enables organizations to define their ZT Protect Surfaces. What we are trying to protect is typically data, applications, assets, and services, commonly referred to as DAAS elements (covered in more detail In DAAS Elements Comprising the Protect Surface in this document). In OT/ICS environments, Protect Surfaces often encompass both digital and physical assets, reflecting their cyber-physical nature. Operational systems are frequently composed of multiple interconnected subsystems working in unison to achieve a specific output.

In some cases, a Protect Surface may encompass a cohesive assembly of critical system components, including machinery and their associated control systems, which necessitate collective safeguarding to ensure uninterrupted and secure operational integrity. Collectively, these DAAS elements and assemblies may simply be referred to as the "assets" when describing a ZT Protect Surface and policies.

When defining Protect Surfaces, it's beneficial to start broad and progressively refine. Begin by identifying business information systems or operational systems, then break these down into subsystems, and finally into individual DAAS elements. This hierarchical approach aligns well with the complex, interconnected nature of OT/ICS environments, which are effectively "systems of systems."

Each level of this hierarchy can potentially be a Protect Surface in its own right, depending on the organization's needs and the system's complexity. The goal is to identify the most granular Protect Surface that allows for implementing closely-aligned controls and least-privilege policies.

The ISA/IEC 62443 Zone and Conduit Model

Critical Infrastructure sectors each have their own guidance and regulations for cybersecurity, including data classification, segmentation, and risk management.

Cross-cutting all sectors, the International Society of Automation (ISA) maintains a set of standards for OT/ICS (defined by ISA more broadly as IACS). Among the list of standards is ISA/IEC 62443, a series of standards touted as “the world’s only consensus-based automation and control systems cybersecurity standards.”

The ISA/IEC 62443 series of standards contains both normative (required activities) and informative (helpful how-to) guidance for securing OT/ICS for system owners, system operators, risk professionals, and manufacturers. It also uses a reference architecture based on the Purdue Model and introduces the concepts of zones and conduits to be used for segmentation and access control.

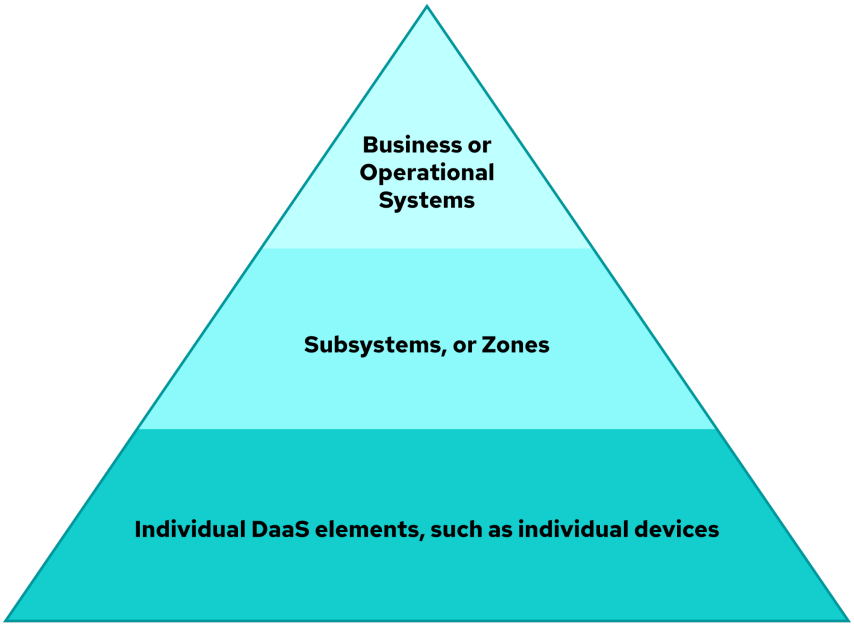
Zones, which group systems and components based on shared security requirements,[18] can be equated to subsystems in our hierarchy. Conduits, the communication paths between zones, will be explored further in Step 2: Mapping Operational Flows.

If you've already implemented the zone and conduit model, these zones can serve as a starting point for defining your Protect Surfaces. Each zone, or subsystem, can be further broken down into DAAS elements as needed.

[18] How to Define Zones and Conduits

Remember, defining Protect Surfaces is an iterative, progressively elaborated process. As you progress through the 5-step implementation, you may identify additional subsystems/zones, some of which may make sense to split out as separate Protect Surfaces. This refinement is a natural and intended outcome of the process, allowing for increasingly precise security controls.

One can think of defining an increasingly granular Protect Surface as a hierarchy, such as:



DAAS Elements Comprising the Protect Surface

Building upon the concept of Protect Surfaces, this section delves deeper into the specific components that make up these surfaces in OT/ICS environments. As previously mentioned, we often refer to the components that comprise a Protect Surface to be made up of DAAS elements: Data, Applications, Assets, and Services. In the context of OT/ICS, it's important to recognize that these elements often span both digital and physical domains. This comprehensive view ensures that all critical aspects of the operational environment are considered when implementing ZT principles. Let's explore each of these elements in detail, with specific examples relevant to OT/ICS settings:

Data

In OT and ICS environments, data encompasses not only traditional sensitive information but also critical operational data that directly impacts the safety, reliability, and efficiency of industrial processes. This includes:

- Control signals, system configurations, and process parameters
- Historian data, P&IDs, plot plans, equipment drawings, and spec sheets
- Production data (serialization data, materials sourcing data, production schedules)

- Intellectual property and patents
- Business data (shipping, billing, and other analysis)
- Configuration and design data, including OT program/logic configuration files
- Firmware files and software for patching and updates
- Data protected by industry-specific regulations (e.g., NERC CIP covered information)
- Other business, employee, payment, and vendor data

Applications

Applications are the collection of software, hardware, and infrastructure that fulfill important business, functional, or operational requirements. They provide direct or indirect interfaces to data. Examples include:

- Process and production applications (e.g., OPC applications, MES, SCADA, Historians)
- System management applications for hardware and software in the OT/ICS environment
- Identity and access management applications
- Human-Machine Interface (HMI) applications for operator interaction with machinery and processes
- Business process applications that may interface with OT/ICS operations
- Cloud and SaaS applications serving OT/ICS processes

Assets

Assets are resources that host data or perform critical functions within the organization. In OT/ICS environments, these can include both IT and OT components:

- Computer systems and devices used to access the OT/ICS environment
- Field controllers (PLCs, field logic devices)
- OT/ICS equipment core to providing services (e.g., manufacturing plant equipment, power generators)
- Devices executing physical processes (e.g., robotic arms, conveyors, chemical regulators)
- Sensors and transducers providing inputs to critical systems
- Network infrastructure within OT/ICS (switches, routers, firewalls, wireless access points)
- Physical building access devices
- Users (engineers, asset operators with specific knowledge/capabilities)
- APIs, device identities, and other non-person entities

Services

Services in OT/ICS environments apply business and technical expertise to create, manage, and optimize information and operational processes. These can include:

- Integral services - included as part of a Protect Surface
    - Network and communications services
    - Visibility and analytics services for OT vulnerability management and asset health monitoring
    - Automation and orchestration services
    - ICS and vendor-specific protocols
- Supporting external services - Protect Surfaces in their own right
    - Remote monitoring and control services (e.g., GE, Siemens, SE)
    - Domain name services (DNS)
    - Public Key Infrastructure and key management services
    - Identity services (e.g., IDaaS, FIDO/passkey services)
    - Cloud-based services like PaaS and SaaS that support OT/ICS operations

Defining the Protect Surface as DAAS elements helps to assess risk, manage vulnerabilities, and protect the most critical assets in OT/ICS environments. Regular assessment ensures alignment with evolving critical assets, helping CI owners and operators reduce the risk of successful attacks and maintain operational integrity.

Examples of Protect Surfaces within OT/ICS include:

Business Information System	Data	Applications	Assets	Services (Supporting)
Industrial Control System	Control, sensor, and process data used to manage chemical processes in a chemical plant	Production chemical process control application	Chemical plant sensors and PLCs	Heating, Ventilation, and Air Conditioning (HVAC)
Smart energy metering and billing system	Electrical consumption and customer data	Customer monitoring and billing system	A smart meter that consumes energy signals to support system monitoring and customer billing	Smart meter wireless network

While a given Protect Surface for an organization may remain constant, the DAAS elements composing it are constantly changing as new technologies are developed and old ones become obsolete. It is important for OT/ICS owners and operators to regularly assess their Protect Surfaces to ensure that they are still aligned with their critical assets.

Relationship between DAAS Elements and ZTMM Pillars

While DAAS elements and the CISA Zero Trust Maturity Model (ZTMM) pillars are both components of a ZT strategy, they serve different purposes in the implementation process:

1. DAAS Elements: These represent an inventory of assets that organizations seek to protect within their ZT strategy. DAAS elements help define Protect Surfaces, providing a comprehensive view of what needs to be secured.

2. CISA ZTMM Pillars: The five pillars (Identity, Devices, Networks, Applications and Workloads, and Data) provide a framework for implementing and maturing ZT capabilities across various aspects of an organization's infrastructure. They offer a structured approach to assess and enhance an organization's ZT maturity level.

Understanding DAAS elements and their classification by their CISA ZTMM pillars is helpful for effective ZT planning and implementation:

- DAAS elements answer the question "What are we protecting?" by inventorying critical assets.
- ZTMM pillars address "How mature are our protection mechanisms?" across different domains of the infrastructure and types of DAAS elements.

By leveraging both concepts, organizations can:

1. Effectively define their Protect Surfaces based on a comprehensive inventory of critical assets (DAAS elements), grouped into subsystems/zones as appropriate

2. Use the ZTMM framework to prioritize the implementation and maturation of ZT capabilities across all relevant aspects of their infrastructure

3. Prioritize efforts to gradually enhance their ZT posture comprehensively

4. Ensure adequate protection for all aspects of their infrastructure, both digital and physical

This integrated approach allows organizations to develop a robust ZT strategy that addresses both the specific assets to be protected and the maturity of the protection mechanisms across different domains of their infrastructure. It enables a more holistic view of security, ensuring that as the inventory of critical assets evolves, so too does the maturity of the ZT implementation across all relevant areas.

Tips for Defining the Protect Surface in OT/ICS Environments

As you embark on the ZT journey in OT/ICS, keep these tips in mind. Remember that the subsequent four steps of the ZT implementation process depend on the discovery and documentation completed during this first step.

Start with the Tools and Data Available

As with all ZT programs, organizations are encouraged to "start where they are". If you have access to tools such as configuration management database (CMDB) applications with robust features within your OT/ICS environment, that's fantastic. However, if your environment has no inventory management, partial inventory, outdated inventory, and/or is still running on paper or manual inventory processes, then that's what you have to start with. The first task is to aggregate that data for immediate use while considering ways to update the inventory processes and tools to sustain your ZT program moving forward.

Identify All Critical Assets that are Essential to the Operation of the Infrastructure

Organize the assets in a way that's meaningful for your organization. This may mean categorizing assets by DAAS elements (Data, Applications, Assets, and Services), using zones/subsystems, or a mix of both. You can further sub-group based on business processes, department/team, geography, regulation, or criticality.

Identify and Document the Assets' Roles in Business Criticality and Impact

Regardless of your grouping, defining the Protect Surface includes discovery and documentation to help identify the various assets' roles in business criticality and the impact that asset or system may have on business operations or safety. At this stage, the goal is not to perform a risk assessment but a business impact analysis (BIA). There are many standard frameworks and models for performing a BIA, including NIST[19], DHHS [20], and ISO, as well as industry or environment-specific models such as ISA/IEC 62443-3-2[21] for OT/ICS.

Identify and Document Dependencies of and by the Assets

The final part of this trifecta of tips is to include documentation detailing dependencies of and by the assets identified. This exercise ensures the organization properly assigns criticality to discrete assets based on the interdependencies that ultimately impact the BIA. This activity could be part of a broader resilience initiative (leveraging ORF), or an effort to produce disaster recovery and business continuity plans (DR/BCP).

Using the earlier example of a pharmaceutical manufacturing entity, it would be ill-advised to consider the criticality of a system (such as a manufacturing, assembly, and packaging process) without considering the constituent assets that comprise the Protect Surface. In the ideal ZT planning, the Protect Surfaces are defined individually (versus as a group or system of assets). This level of specificity can be more challenging in industrial environments but should be adhered to when possible.

[19] Business Impact Analysis (BIA) - Glossary | CSRC
[20] NIST Releases IR 8286D: Using Business Impact Analysis to Inform Risk Prioritization and Response
[21] Cybersecurity Risk Assessment According to ISA/IEC 62443-3-2

Where Possible, Keep Dynamic and Near Real-time Asset Inventory

As ZT matures, it relies increasingly on accurate, real-time data to inform policy decisions. The asset inventory is crucial in this regard. Organizations should aim to modernize their inventories with real-time or near-real-time data across all asset types.

This task has traditionally been a challenge not only within enterprise IT environments, but also (and especially) in industrial environments with OT/ICS assets. Applications that can connect through APIs to push, pull, and poll are desirable and organizations can address this through strategy or opportunistically as refresh and upgrade projects occur.

Or, more commonly and accessible, dynamic inventory solutions that update a system automatically and/or alert on changes. Some solutions watch traffic (directly through span/tap or via network devices); others interrogate the devices with appropriate OT-specific protocols. Semi-automated solutions can incorporate asset tracking into procurement and change management workflows.

Plan to Revisit and Update as an Ongoing Maintenance Task

Maintaining a ZTA necessitates continuous review. Ultimately, manual review and maintenance tasks should be automated as the ZT program matures. While mentioned here as relevant to maintaining an up to date inventory, additional information is provided in step 5, ongoing monitoring and maintenance.

Use an Approach Most Appropriate for the Systems or Environments in Scope

Keep in mind that the processes and tools within enterprise IT may not be translated directly to OT/ICS environments. Use tools, vendors, and processes tailored for OT/ICS to ensure the reliability and safety of those systems are preserved through discovery and analysis.

For example, considering the levels of the Purdue Model referenced earlier, running common tools such as NMAP may be harmless on the enterprise IT network, but could cause failures and faults in the lower levels of the Purdue Model, especially as you get closer to the cyber-physical assets and field devices.

Enterprise IT and cybersecurity professionals tasked with discovering OT/ICS assets will need and want to work closely with OT engineers and system operators. Novel tools and techniques should be tested in non-production systems and networks or in a digital twin.

Along the same lines, vendors and third parties involved in monitoring, maintaining, and performing incident response within OT/ICS networks should have specific expertise in those systems. This is covered further in step 2, mapping transaction flows, and step 5, ongoing monitoring and maintenance.

Gathering Metadata for each Protect Surface is Essential

The collection of **metadata** for each Protect Surface is a key concept. This information, which includes details such as data types, protocols, and system criticality, is crucial throughout the ZT implementation process. As you progress through each step—from mapping flows to designing architecture and creating policies—this metadata continuously evolves and expands. Each stage builds upon the metadata gathered from the previous one, providing increasingly detailed insights that allow for more precise, targeted security measures. Ultimately, this growing body of metadata drives the development of a uniquely tailored ZT policy, one that is finely tuned to the specific needs and characteristics of each Protect Surface.

While developing security measures specifically tailored for the Protect Surface is important, this task takes on even greater significance within OT/ICS environments. Unlike IT, which can rapidly implement solutions, the industrial sector presents a complex landscape. This complexity is not just due to OT infrastructure and varied communication protocols but also stems from the broad spectrum of stakeholders involved - from engineering and operations to Chief Risk Officers and control room staff to a host of third-party contractors and specialists. Each group brings its own unique perspectives and goals. This intricate web of considerations highlights the imperative for a customized ZT strategy, one meticulously designed to acknowledge and cater to the multifaceted needs and concerns inherent in CI settings.

Step 2: Mapping Operational Flows for OT/ICS

Mapping operational flows is the second of the five ZT implementation process steps. The objective of Step 2 is to understand how the system works by mapping the information flows to, from, and within the Protect Surface, including how various DAAS elements interact with each other and with other resources. Understanding these flows directly informs where to place proper controls.

While the CSA provides general guidance for this step in the Step 2 - Mapping Transaction Flows document, the OT/ICS context requires a slightly different perspective. In these environments, the concept of "transactions" is less relevant. Instead, we focus on mapping operational flows, process flows, and control flows. This shift in terminology better reflects the continuous and interconnected nature of OT/ICS systems, where the emphasis is on ongoing processes and control operations rather than discrete transactions.

This mapping information facilitates informed decisions about security controls, granular access policies, resource allocation, and strengthening the security posture.

Mapping Flows in OT/ICS Systems: A Strategic Imperative

Mapping operational flows in OT/ICS environments is essential for identifying how systems interact, pinpointing necessary controls, and establishing robust monitoring points to defend them. Unlike IT systems, OT systems demand a mapping approach that accounts for their physical and operational nuances.

As much as possible, each connection point should be treated as untrusted until verified, adhering to core ZT principles. This approach is fundamental for preventing the lateral movement of threats - an especially critical aspect in OT/ICS contexts, where the interconnectedness and specificity of systems present unique security challenges. As systems within OT are intricately linked and operate under different protocols than traditional IT environments, the risk of a threat moving undetected across the network is significantly heightened.

The discipline of OT/ICS cybersecurity involves an understanding of industrial operations. It benefits from familiarity with the languages of Programmable Logic Controllers (PLCs), the flow of Supervisory Control and Data Acquisition (SCADA) systems, and the architecture of Distributed Control Systems (DCS). This knowledge is helpful when implementing a ZT strategy tailored to the unique landscape of industrial environments.

Evolving Inventory: The Foundation of Operational Flow Mapping

The asset inventory developed in Step 1 serves as the critical foundation for operational flow mapping in OT/ICS environments. As you progress through step 2, you'll build upon and refine this inventory, creating a more comprehensive and dynamic understanding of your OT landscape.

A thorough asset inventory facilitates clear documentation of dependencies, interconnections, and access relationships between various assets. This clarity informs the development of operational flow maps, highlighting data movement within the system and potential vulnerabilities. The process of mapping flows often reveals previously overlooked assets or connections, allowing you to enrich the initial inventory with new elements, dependencies, and data flow information.

It's important to note that as you progress through each step of the ZT journey, you're likely to identify missed elements, though in decreasing amounts. This ongoing discovery process might even lead to changes in defined Protect Surfaces or their priorities.

While many organizations still manage inventories through manual methods, digitalizing this process should be part of your ZT roadmap. A digital, continuously updated inventory allows for real-time reassessment and realignment of operational flow mappings as your OT environment evolves.

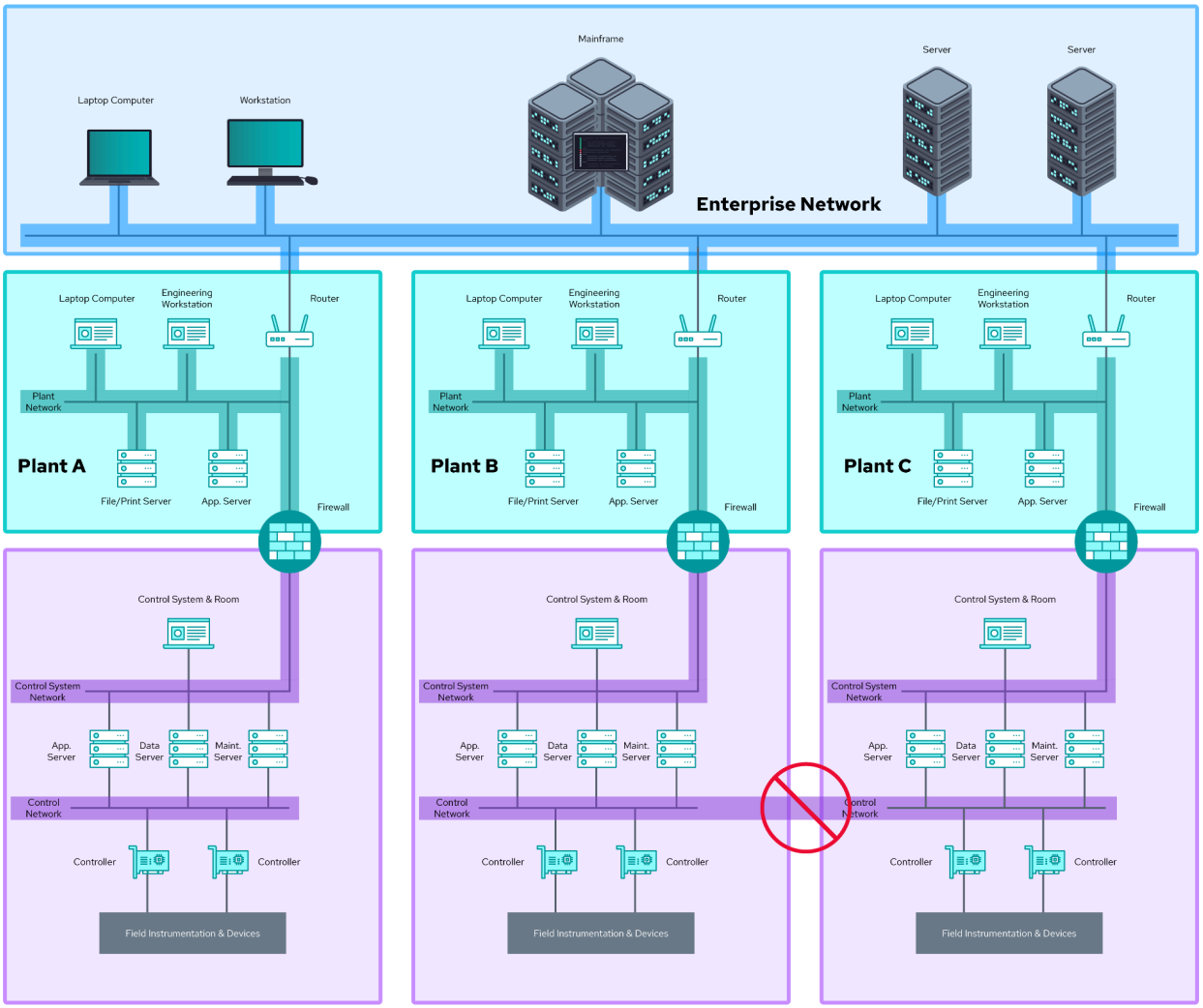
Mapping Flows using the ISA/IEC 62443 Zone and Conduit Model

Recall the ISA/IEC 62443 standards mentioned earlier. These standards provide a helpful reference model from which you can map operational flows in OT/ICS environments.

When modeling zones and conduits, there are a series of important rules that professionals must take into account.[22]

- A zone can have sub-zones.
- A zone can have more than one conduit. Cyber assets within a zone use one or more conduits to communicate.
- A conduit cannot traverse more than one zone.
- A conduit can be used for two or more zones to communicate with each other.

This diagram depicts examples of correct and incorrect zone and conduit architectures:



Source: How to Define Zones and Conduits

In the diagram above, the separate colored boxes represent zones, and the darker shaded areas within them represent conduits. Notice that a conduit can connect zones to each other (north/south traffic), but

[22] How to Define Zones and Conduits

a single conduit cannot traverse zones (east/west traffic). This is further described below in the Mapping operational flows with Conduits section.

Common Types of Conduits

Industrial systems utilize a diverse array of protocols and media, encompassing a wide spectrum of types, natures, and functions. The sheer multitude of these protocols reflects the complexity and specialization found in OT environments. Some common types of conduits include:

- Plant network based on Ethernet with various industrial protocols, including OPC
- Control network of the distributed control system (Example: Yokogawa Centum VNet/IP)
- Industrial field network (Example: Profibus DP, DNP3, HART7, and many others)
- Wireless network: ISA100, Wireless HART, and others
- A simple RS-232/422/485 serial cable to enable communication between two computers

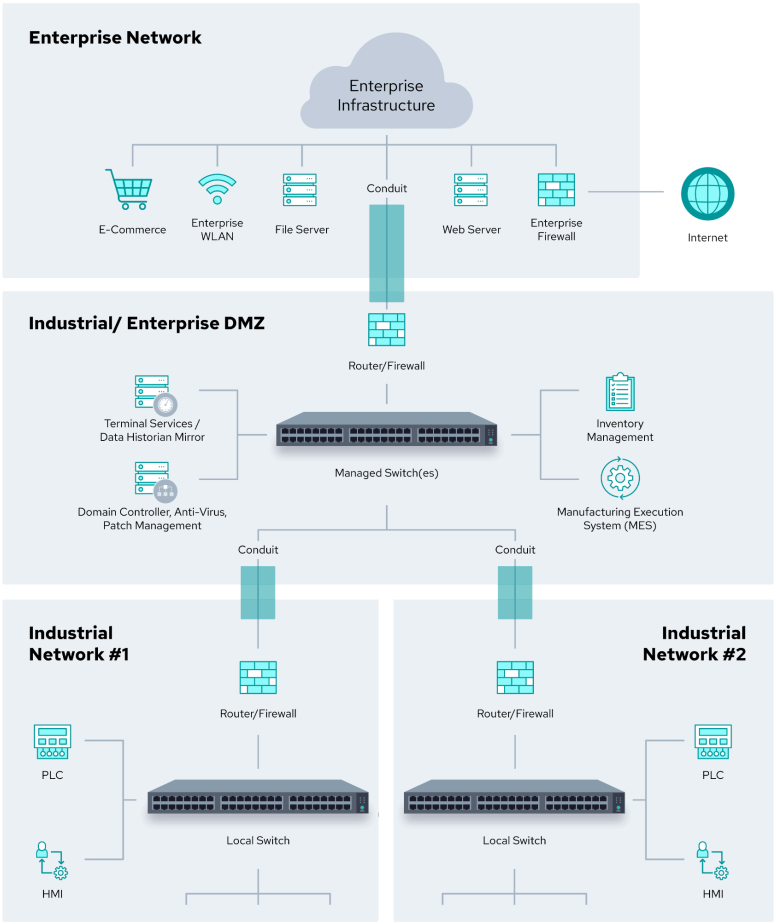
Mapping Operational Flows with Conduits

The conduit construct aligns very well with ZT flow mapping principles.

A conduit is a logical or physical grouping of communication channels that can connect two or more zones. The conduits connect the security zones, clearly defining the required communication paths within the OT/ICS network. This, in turn, feeds the requirements for segmentation and access control.

Where feasible, Asset Owners should try to keep their zones and conduits consistent with their network architecture to avoid extra unnecessary complexity.[23]

[23] Key Concepts of ISA/IEC 62443



Source: Key Concepts of ISA/IEC 62443: Zones & Security Levels | Dragos

Accurately mapping conduits is essential to understand the flow of data and interactions between different zones within the OT/ICS environment. When mapping operational flows, it is imperative to consider both legitimate and potentially unauthorized flows. This includes examining data exchanges between control systems, field devices, and other operational components, as well as interactions with external systems or networks. By thoroughly mapping these flows, organizations can gain visibility into potential attack vectors and identify areas where ZT principles should be applied.

Keep in mind that observed data flows provide valuable insight into which communication types are actively occurring and presumably allowed. However, ZT principles advocate for a default-deny model. Therefore, it's crucial to go beyond just observing active traffic. Evaluate conduit and intra-zone network configurations, as well as firewall rules, to identify all permitted traffic - even those flows that may not have been active during your observation period. Then, for each identified flow, decide whether it should be permitted or denied based on your ZT policy.

Furthermore, it is crucial to document the nature and purpose of each operational flow, including the types of data exchanged, the protocols used, and the criticality of the flow to operational processes. This information, or **metadata**, will inform the subsequent steps of architecting the ZT environment and creating appropriate policies to govern and secure these operational flows.

A key insight is to identify patterns or categories of flows during the mapping exercise. This surfaces enterprise security architecture building blocks which helps better inform the next step of designing a ZTA.

Beyond Zones and Conduits

Recall that a core concept of Zero Trust is to pinpoint the most granular Protect Surface to implement closely-tied controls, ensuring precisely targeted, least-privilege policies. While mapping operational flows with zones and conduits is extremely effective within OT/ICS environments, as you iterate and mature your ZT implementation, being able to define more granular components would further strengthen your security posture by preventing lateral movement of threats through isolation and provide further reduction of the blast radius.[24]

Segmentation Within OT/ICS Infrastructure

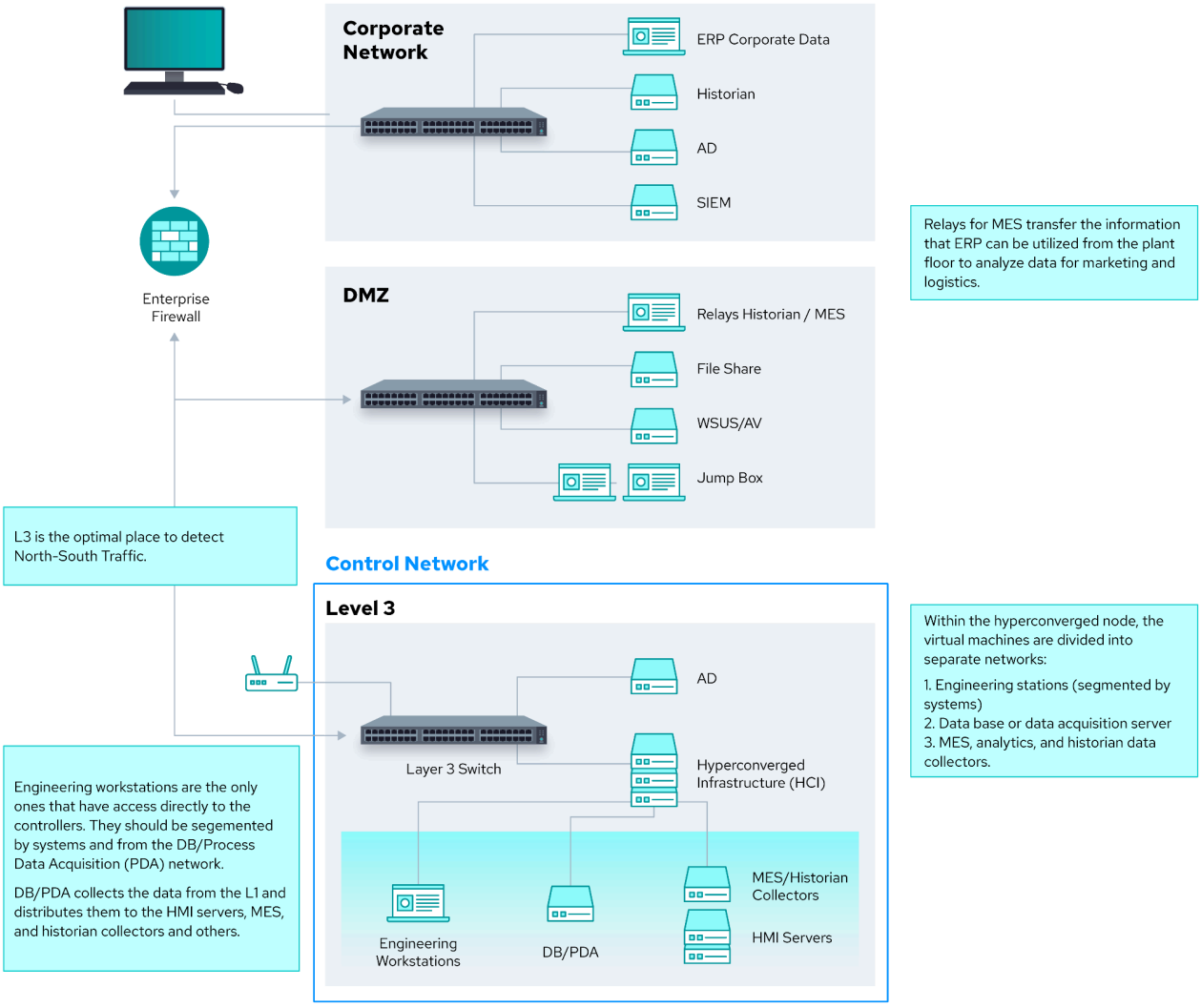
Using DMZs within OT/ICS infrastructure to segment IT and OT, typically at level 3 of the Purdue Model, is an effective strategy. While the next step in this paper, step 3, building a ZTA, will delve further into segmentation for ZT, some aspects are worth considering while mapping operational flows.

Frequently, the lower levels of the Purdue Model are left unmonitored because of flat architectures that lack sufficient managed switches. Flat networks lead to a lack of designated choke points. Without these choke points, plants may remain unaware of substantial amounts of network traffic from the plant floor. As a result, they may need to incorporate additional sensors and monitoring equipment. Another approach, as described in step 3 below, is to retrofit, or install, a software agent or layer 7 (L7) component to enforce additional security policies.

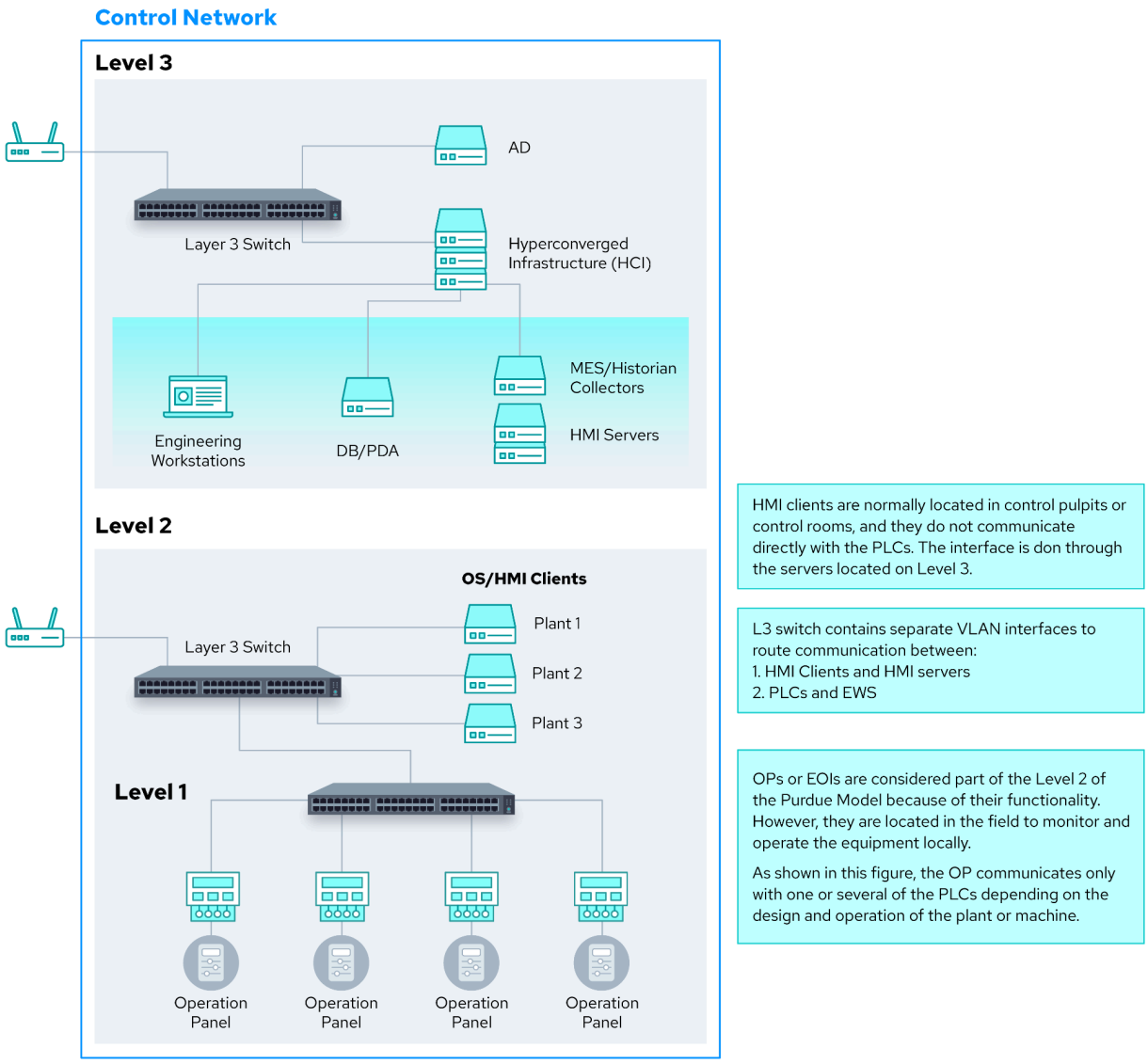
Implementing managed switches, sensors, and agents could significantly enhance your ability to map operational flows accurately. While these components may not be part of your initial ZT implementation cycles (such as your learning or practice Protect Surface iterations), they're valuable considerations for future iterations. As you progress through the five-step process, keep these potential enhancements in mind. They can serve as bookmarks for design elements to revisit, ultimately leading to more comprehensive and precise operational flow mapping in your OT/ICS environment.

[24] For OT/ICS, it's not CIA, but AAA | OT Cybersecurity

To help visualize this, below are diagrams from Dragos' whitepaper "Network Segmentation Challenges and Solutions".[25] These diagrams mention ERP (Enterprise Resource Planning) and MES (Manufacturing Execution Systems), which you can read more about in Dragos' whitepaper; the purpose of including these diagrams here is to help stimulate your thinking about operational flow mapping, as well as provide a primer for the next step, building a ZTA.



[25] Whitepaper: Network Segmentation Challenges and Solutions



Convergence of OT/IT and Mapping Operational Flows

As previously mentioned, the rapid pace of digital transformation, notably accelerated by the pandemic, has intensified the convergence of OT and IT systems. This shift makes operational flow mapping even more critical as it requires the integration of both traditional and contemporary connections, underscoring the need to manage a mixed ecosystem of protocols and technologies. As vendors drive this convergence with integrated products, it is essential that mapping strategies accurately reflect these novel interconnections.

The rapid pace of business and technological advancements often outstrips traditional security measures. A ZT strategy is ideally suited to address this gap, offering a responsive and adaptive security solution. The success of this strategy depends on the comprehensive mapping of operational flows, which is vital for both understanding and securing data pathways, especially as they expand or are modified in response to digital transformation.

What happened to the air-gap?

The traditional air-gap separating OT and IT systems is diminishing. Why? In a lot of cases, because it makes good business sense.

- Fast-moving markets require agile responses to customers, requiring connecting business systems with OT systems powering daily operations.
- A food manufacturer might want to let web applications and consumer choice directly drive the manufacturing of specific ingredients on a factory floor. When business processes drive demand, orders can be sent directly to OT for completion.
- Optimize energy usage by linking IT systems with OT systems that monitor and control energy consumption, enabling real-time energy management and cost savings through automated adjustments based on demand, usage patterns, and utility rates.
- In industries like oil and gas or utilities, integrating IT with OT allows for remote monitoring and control of field operations. This integration facilitates decision-making based on real-time data, enhancing safety and operational efficiency.

When there is no physical air gap, OT environments have connectivity to IT networks. Consequently, internet-borne attacks can reach OT devices, making Zero Trust imperative.

While IT and OT convergence drives innovation, it also tends to make it harder to see and understand the specific roles and interactions of systems within OT networks. Therefore, mapping operational flows becomes increasingly vital. This process must accurately outline how data travels between assets and the existing network connections, ensuring enhanced visibility and, subsequently, strengthened security. Note that, in some cases, retrofitting ICS components may have happened without being made widely aware, which can invalidate an air-gap once assumed to be effective. Pay close attention to these potential "hidden" retrofits as you work through the mapping process.

Tips for Mapping Operational Flows in OT/ICS

Tools and Technology To Help

Many vendors provide effective solutions for inventory discovery and operational flow mapping, including passive and active polling techniques. Tools like Dragos Platform[26], Claroty[27], Nozomi Networks[28], and Armis Centrix[29] offer dynamic asset discovery and some include dynamic operational flow mapping, potentially accelerating the first two critical steps of the ZT implementation process. Additionally, many

[26] Asset Visibility for ICS environments | Dragos Platform
[27] Asset Inventory - Platform | Claroty
[28] OT Asset Inventory Management
[29] Full Asset Inventory and CMDB Enrichment | Armis

OT-protocol aware firewall vendors offer similar visibility capabilities, with some able to auto-flag labels (metadata) or integrate third-party metadata for dynamic policy creation.

However, it's important to note that deploying such software isn't always feasible or permissible. Some critical industries, such as Marine and Shipping, may face regulatory restrictions on deploying certain tools. Additionally, disconnected or serially connected networks require alternative approaches.

Where automated tools can be used, continuous network monitoring enhances confidence that network changes are quickly recognized, documented, and validated. In environments where software deployment is limited, consider alternative 'systems-based' approaches to security and risk management. One such approach is Consequence-driven Cyber-informed Engineering (CCE), a framework highly regarded in OT environments. CCE, developed by Idaho National Laboratory, offers valuable insights for scenarios where traditional software solutions aren't applicable.

Ultimately, the choice of tools and methodologies should align with your specific operational constraints, regulatory requirements, and security objectives. A combination of automated tools, OT-aware firewalls, manual processes, and innovative frameworks like CCE[30] can provide a robust approach to inventory and flow mapping in diverse OT/ICS environments.

Culture and Collaboration

As mentioned earlier, the OT/ICS discipline is vastly different from IT and includes a wide range of other functional constituents. Often, OT and IT personnel don't communicate on a regular basis. Engage a collaborative effort between cybersecurity, IT, OT, and ICS experts to ensure that the mapping of operational flows accurately reflects the complex interactions and dependencies inherent in these environments. This collaborative approach ensures that all potential pathways for data - and, by extension, potential attack vectors - are accounted for and secured.

Documenting Your Flows

Documenting every aspect of the discovery, design/architecture, and implementation processes is essential. Documentation requirements should be embedded into change management processes. These documentation requirements should include updates to the asset inventory, network drawings, and backups, as well as verification of updated transaction flows.

This ensures that the operational flow mapping is well-recorded and can be easily updated or referenced. You should view and document operational flows as systems, recognizing their interdependencies. This comprehensive understanding is critical for developing controls and environments that are custom-built for each Protect Surface.

[30] Consequence-driven Cyber-informed Engineering

Closing Out Step 2

Let's close out step 2: mapping operational flows with a quote from John Kindervag, the creator of Zero Trust:[31] "Protect the data like oil. Just as oil increases in value as it is refined, so does data. Therefore, transaction flow mapping in OT/ICS must include rigorous measures to safeguard data at every stage of its transformation and transport, treating it with the same level of protection as any valuable resource."

Mapping operational flows transcends a mere procedural task; it evolves into a strategic cornerstone of OT/ICS security. This process not only fortifies your systems against evolving threats but also deepens organizational understanding of critical operations and remote access. By meticulously charting these flows, you create a foundation for resilient security that adapts to emerging risks while ensuring uninterrupted industrial processes. Ultimately, this exercise strengthens your entire security posture, aligning protective measures with the intricate realities of your OT/ICS environment.

Step 3: Building a Zero Trust Architecture in OT/ICS

The CSA has general guidance for the five-step implementation process found in the Zero Trust Advancement Center (ZTAC) Resource Hub. This section provides guidance specific for OT/ICS environments.

After step 1, defining the Protect Surface and step 2, mapping operational flows, the next step is step 3, build (design) a Zero Trust architecture (ZTA). This is a planning and documentation design stage where the information gathered in the first two steps is used to identify where in the architecture ZT policies can be enforced.

Purdue Model and OSI Model

Note that this section references both *levels* of the Purdue Model (levels 0-5) and *layers* of the OSI model (layers 1-7), which are distinctly different. The Purdue Model is referenced in this document as a reference architecture for describing the groupings of assets common in OT/ICS networks and is meant to be a tool for discussion between IT and OT engineers. The OSI model is a conceptual framework used to describe the functions of a networking system. While the Purdue Model helps in understanding the hierarchical structure of industrial control systems, the OSI model is used to describe how data is transferred between components within that structure, regardless of their level in the Purdue hierarchy.

Policy Enforcement Points

CI necessitates a well-thought-out architecture design that accounts for the unique nature of the systems and assets involved. This involves conducting a thorough assessment of the infrastructure's critical components (step 1), identifying potential entry points for threats (step 2), and determining the appropriate segmentation (step 3). By understanding the critical assets' dependencies and their interactions, a resilient and secure architecture can be crafted.

[31] Things Run Amok. Leveraging Zero Trust to protect IoT and OT assets.

These are referred to as ZT policy enforcement points (PEPs), and planning enforcement points is a much simpler task when the assets can be protected with software (such as agents) that can be easily deployed and granularly tuned for layer 7 policy control. In environments with headless devices (such as IoT) and the prevalence of cyber-physical assets and legacy devices, such as those in OT/ICS, this step can be a bit more complex, explored further in the upcoming section Planning Policy Enforcement Points.

Once planned, the ZTA design will ensure uniform and robust security measures across the protected OT/ICS environment.

Diagramming the OT/ICS Architecture

Diagramming the environment offers a visual representation that facilitates more intuitive and thorough planning at this stage. If one doesn't exist already, the most practical next step is to create a diagram of the OT/ICS environment(s) in scope.

The diagram may be created and updated manually based on several inputs or data sources. Ultimately, the ideal ZT environment will have the integrations and modernization to automate this task, but that's not where most organizations are starting.

Common options at this stage may include some or all of these inputs and methods:

- Manually creating network diagram(s) (e.g., in Microsoft Visio or similar tool)
- Using third-party discovery and inventory tools (ideally ones that can automate discovery and/or offer visualization natively or API connections to a visualization tool)
- Contracting a managed service partner for discovery and inventory management (e.g., Claroty, Dragos, Nazomi, Armis, Zscaler, and others as an example)
- Leveraging manufacturer vendor-specific tools (e.g., Siemens, Rockwell Automation, Emerson, Honeywell, Schneider Electric, Yokogawa, etc.)

Elements to consider for inclusion in this diagram are:

- Each asset identified in step 1 define the Protect Surface
- Logical connections and topology (specifically each operational flow identified in step 2 mapping operational flows)
- Physical connections and topology (OSI layer 1 network connections)
- Network connections and topology (OSI layer 2 and layer 3 network connections)
- Classification of data stored on or accessed within the system
- Business impact of protected assets
- Protocols in use for logical connections and network routing
- Relevant notes detailing other dependencies, user population, and access parameters where applicable

The ISA/IEC 62443 zone and conduit model described earlier in this document maps beautifully to a ZTA, as Siemens describes further in this whitepaper. If your organization is already following ISA/IEC 62443

guidance and/or has documentation or assessments based on ISA/IEC 62443, there are many elements that can be directly transferred into your ZTA planning.

Security Zones and the Zero Trust Protect Surface

The ISA/IEC 62443 security zones correlate to the ZT task of defining the Protect Surface.

Recall from step 1, a security zone is a grouping of systems and components based on their functional, logical, and physical relationships that share common security requirements. After steps 1 and 2 of defining the Protect Surface and mapping the operational flows, the assets can be grouped into security zones if they haven't already as part of mapping operational flows.

In an ideal ZTA, each asset is its own Protect Surface and therefore its own security zone. However, as a starting point, it is acceptable or frequently inevitable to use groups of assets, or business operations systems, classified into security zones. This can be later refined for the policy creation in the next step, at which point additional granularity will be applied if possible.

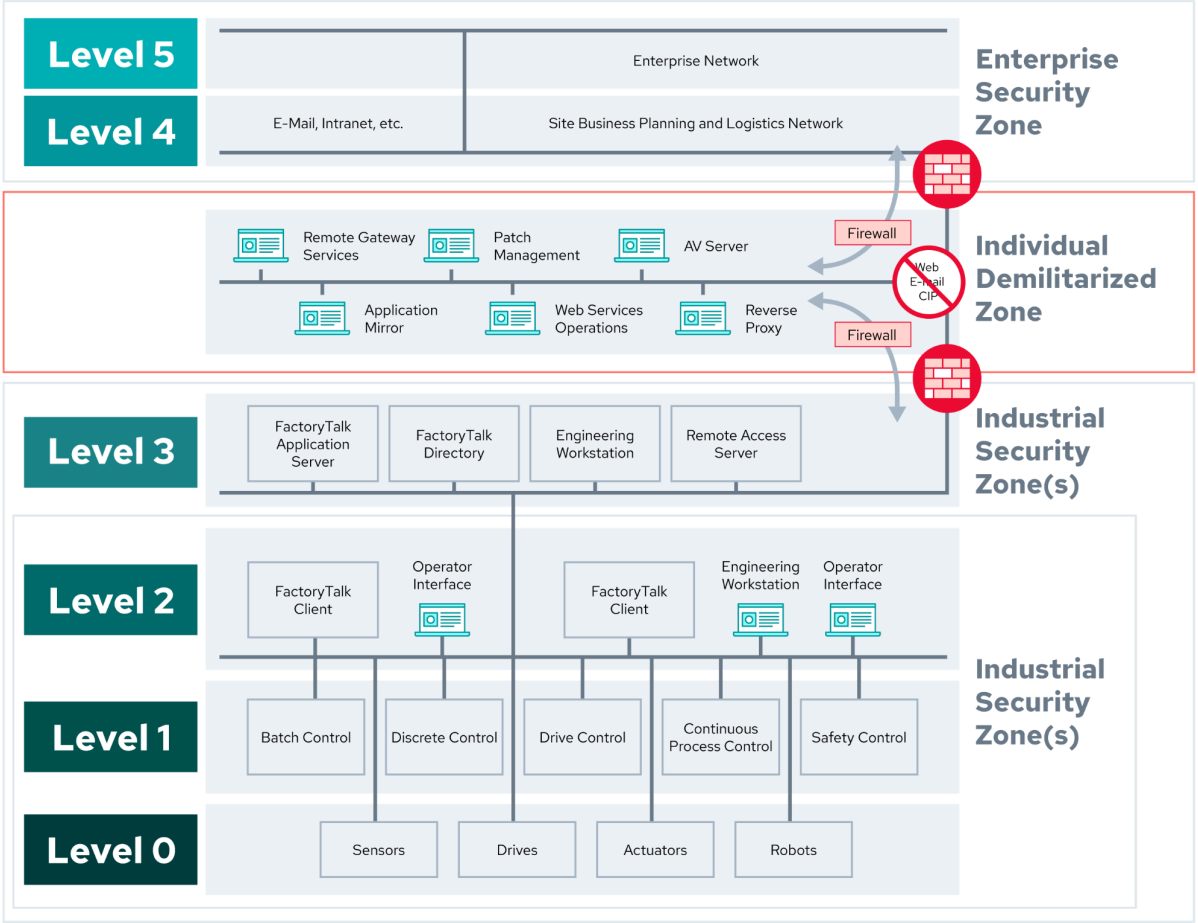
Segmentation and Zero Trust Enforcement Points

Segmentation models within the ISA/IEC 62443 correlate to the placement and type of ZT policy enforcement points (PEPs).

Segmentation requirements become apparent with the zone and conduit view. Here, it's clear which assets need to communicate with one another. Additional conduits would also define any remote access or access paths traversing between the enterprise IT network and the OT network.

Operationally, segmentation between the IT and OT networks, and segmentation within the OT network, looks different than enterprise IT segmentation both in architecture and implementation. More specifically, in the IT networks, we may have a central set of firewalls and rules to allow access to or through different networks and devices.

In an OT network, ideally, there should not be a single path that traverses more than one hop within the Purdue Model levels. For example, you would not design a VPN or access path from the enterprise IT network or Internet (Purdue Model level 5) directly into an HMI (Purdue Model level 2 or 3). Instead, there would be one hop (or conduit) from the enterprise IT network (Purdue Model level 4) to the IT/OT DMZ (Purdue Model level 3.5) and then a separate hop (conduit) into the OT/ICS management (Purdue Model level 2 or 3).



Multiple hops of the Purdue Model (Source: The Purdue model for Industrial Control Systems)

That said, there are a few notable exceptions:

- Unidirectional data going *out* from the OT environment to (e.g.) monitoring or data collection/analytics for processes.
- Purpose-built applications for interacting with the OT assets which may cross several boundaries at once, such as connected SaaS applications.
- Bringing in cloud technologies to production processes, e.g., AI/ML, or bringing in cellular capabilities.

Additionally, the concept of Unified Namespace facilitating seamless data exchange and integration between different OT systems, IT systems, and cloud platforms is gaining traction due to its event-driven architecture for complex solutions processing.

While the ISA/IEC 62443 standards and the zone and conduit model are not the only options for a reference model, it does offer a vendor-neutral international standard that has been widely used, adopted, and referenced across most, if not all, CI sectors. The model fits well into ZT planning, and many resources are available to assist with planning.

Planning Policy Enforcement Points (PEPs) in OT/ICS

While designing a ZTA, consider the importance of ease of operation and maintenance, as well as the flexibility to adapt to evolving network and business requirements. Equally crucial is ensuring redundancy across both control and data planes, encompassing Policy Enforcement Points (PEPs) and Policy Decision Points (PDPs), as described in the Zero Trust Architecture (NIST SP 800-207).[32] This redundancy eliminates single points of failure, thereby safeguarding the availability and safety of critical systems. Such a comprehensive approach guarantees a resilient and adaptable ZT framework, protecting CI with efficiency, agility, and uninterrupted operation.

CI and particularly an OT/ICS environment demands granular access controls to regulate the flow of information and interaction between users, devices, and protected assets.

Policy Enforcement Point (PEP) Placement

Foundational to a ZTA, the goal is to place the enforcement point as close to the protected asset as possible. For modern applications and workloads, adding a software-based ZT agent in or immediately in front of the asset is usually straightforward. This is the preferred implementation for the enterprise IT network (Purdue Model level 4 and higher), parts of the DMZ between IT and OT networks (around Purdue Model level 3.5), and into the control and processing network where the OT/ICS application servers, databases, data historians, engineering workstations, and HMIs reside (Purdue Model levels 2 and 3).

Lower in the Purdue Model (levels 0 and 1), closer to the field devices, the environment often comprises legacy or stripped-down operating systems, PLCs, and other assets that cannot support a software client. In such scenarios, it may be necessary to retrofit the infrastructure to enable policy enforcement at layer 7 (application layer), or to implement network-based enforcement at layer 2 (data link layer) or layer 3 (network layer) of the OSI model. This retrofitting might involve adding capabilities such as installing a network router that supports L7 policies to enforce security measures where traditional software clients are infeasible.

Note: L7 policies require deep inspection of application-level traffic, often involving a Policy Enforcement Point (PEP) that proxies this data. Given the specialized protocols and diverse technologies in OT systems, implementing L3 policies – focusing on routing layer rules – is often more practical. This approach aligns better with the realities of OT systems, where simpler, less intrusive security measures are preferable.

Considerations for planning enforcement points in OT/ICS include:

- Use any existing work such as ISA/IEC 62443 diagrams, documentation, risk assessment, or zone and conduit planning and/or documentation/evidence from compliance reporting or audits.

[32] PDP is the policy engine in the control plane, a key concept of ZTA; see NIST SP 800-207 for more detail

- If the asset supports a software agent/client, consider that as a policy enforcement point (e.g., Zero Trust Network Access solutions, privileged access management).
- If the asset cannot natively support a software agent/client, consider augmenting or upgrading it to do so (e.g., updating the asset and installing software or adding a software or hardware-based enforcement gateway in front of the protected asset).
- If the asset cannot support a software agent/client, plan a network-based enforcement point, such as:
    - Layer 3-7 segmentation with OT/ICS appropriate firewalls
    - Layer 3-7 segmentation with virtualized network solutions such as SDN or VRF
    - Layer 2-4 segmentation with OT/ICS appropriate routers or routing switches
    - Layer 2-3 segmentation with purpose-built LAN microsegmentation gateways
    - Layer 1-2 segmentation with unidirectional gateways or data diodes
- Take this opportunity to identify what will need to be monitored in step 5, ongoing monitoring and maintenance, and how to achieve the monitoring.

The landscape in OT/ICS environments is rapidly evolving, with innovative solutions emerging to address the challenges of legacy and headless devices. For instance, Siemens has introduced the concept of "ID cards for machines" and developed SCALANCE-LPE equipment, while Zscaler is working on "Zero Trust enabled SIM cards" that will connect to a zero trust cellular edge. These advancements are paving the way for applying ZT principles to devices that traditionally couldn't accommodate a direct PEP. Such innovations are bridging the gap between modern security paradigms and legacy infrastructure, enabling a more comprehensive ZTA across diverse OT/ICS environments.

The combination of information discovered throughout steps 1 and 2 should offer a great starting point for planning an overall architecture and then prioritizing the ZT implementation, which will often be executed incrementally.

Shrewd planning at this stage will ensure you can enforce the intended policy during the next step (step 4, creating ZT policy) and will allow the flexibility to start with broader policy statements and then fine-tune for granularity as the program matures.

Step 4: Creating Zero Trust Policy in OT/ICS

The CSA has general guidance for the five-step implementation process found in the ZTAC Resource Hub. This section provides guidance specific for OT/ICS environments.

Creating the ZT policy is the first major “doing” step after the initial three planning steps. At this stage, you’ll execute the planned access control designed in step 3, building a Zero Trust architecture.

Fine-tuning access permissions and regularly reviewing access rights ensure that users can access only the critical assets and functions required for their tasks. Employing the principle of least privilege, access is restricted to the bare minimum required for designated tasks. This approach effectively minimizes potential attack vectors and unauthorized access.

Zero Trust policy in OT/ICS environments centers on granular allow rules, akin to conduits in ISA 62443, permitting only authorized users to access specific resources through designated applications. While in traditional IT environments, ZT typically mandates immediate termination of access if a dynamic policy element changes during an active session, OT/ICS requires a more nuanced approach. At zone boundaries, a deny-by-default stance remains crucial. However, within zones, an allow-by-default approach may be necessary due to safety considerations. This adaptation acknowledges the potential dangers of abruptly terminating sessions or blocking access to critical systems in industrial settings, which could jeopardize human safety. The application of ZT in OT/ICS thus requires a delicate balance, weighing stringent security measures against the imperative of maintaining safe, uninterrupted operations. This approach ensures robust protection while recognizing the unique operational demands and safety requirements of industrial environments, marking a key difference from IT-centric ZT implementations.

Goals of the Zero Trust Policy

Creating ZT policy allows:

1. **Simplified Application Management:** By focusing on allowing applications essential to support CI operations, it becomes more manageable than attempting the continuous task of identifying and blocking all undesired applications.
2. **Targeted Security Focus:** Recognizing that most breaches and malicious activities occur on allow rules, this policy concentrates security efforts on the traffic that is authorized, allowing only what is strictly required for legitimate business purposes.

Actions for Creating a Zero Trust Policy

Based on the Protect Surface and assets (identified in step 1), the operational flows mapped (step 2), and the ZTA (designed/planned in step 3), the following actions are taken during the 4th step to create ZT policy.

User and Device Identity Authentication

Implement authentication and authorization of users and devices at key transaction points. In OT/ICS environments:

- Balance rigorous identity verification with the need for timely access to critical systems.
- Consider the potential impact of authentication failures on operational continuity and safety.
- Strategically place enforcement points to minimize operational risks while maximizing security benefits.
- Implement constant monitoring of device posture, user behavior, and application behavior to enable rapid identification of security events, including unauthorized access attempts.

Security Policy Rules

Comprehensive security policy rules are formulated, keeping in mind CI requirements. These rules involve:

- **Network Segmentation:** The architecture is designed to segment the network, limiting access privileges and preventing lateral movement of threats.
- **Principle of Least Privilege:** Access rights are strictly governed by the principle of least privilege, ensuring users only have access to resources necessary for their specific tasks.
- **Traffic Inspection and Logging:** Ongoing traffic inspection is conducted to identify and address potential security threats. Detailed logging of traffic aids in the investigation of any security incidents.

Adherence to Security Standards

The security policy rules strictly adhere to the established security standards specific to CI.

Universal User Follow-Up

In CI, user monitoring varies based on system capabilities. For systems supporting individual accountability (e.g., Windows machines), users are continuously monitored and tracked, ensuring consistent security enforcement. However, many OT systems lack support for traditional user management technologies like LDAP. In these cases, alternative monitoring strategies should be employed:

- Use configuration management tools to detect system changes, even if not attributable to individuals.
- Implement group accounts where individual accounts aren't possible, always changing default passwords.
- Utilize physical access controls to limit and monitor system access.
- Install cameras in areas where other monitoring forms are unfeasible.

This approach balances the need for accountability with the technical limitations of OT environments, maintaining security vigilance across diverse systems.

Decryption Policy Rules

Where appropriate, decryption policy rules are used to gain visibility into application traffic, enabling the security policy rules to effectively inspect and identify potential threats within the traffic.

Asset-Specific Security Boundaries in Zero Trust Policy

In ZTA for OT/ICS, 'asset-specific security boundaries' complement the concept of 'microsegmentation'. While microsegmentation effectively controls network traffic through granular subdivisions, asset-specific security boundaries focus on placing security controls directly adjacent to critical assets within the Critical Infrastructure. These boundaries extend the ZT principle by physically or logically enclosing each Protect Surface with precise, tailored controls. This method ensures that security measures are as close as possible to the assets they protect, minimizing the internal attack surface and aligning with the principle of least privilege by enforcing strict access controls.

ZT policy rules define these asset-specific security boundaries to ensure precise control over who or what can interact with each asset, under what conditions, and when. This level of specificity is essential in OT/ICS environments, where operational continuity and safety are paramount. By implementing both microsegmentation and asset-specific security boundaries, organizations can achieve a robust defense-in-depth strategy that secures network traffic while also fortifying the immediate surroundings of physical assets.

The integration of asset-specific security boundaries into the ZT model allows for a more comprehensive security framework that adapts to the unique challenges of OT/ICS. Such security architectures are particularly beneficial in environments with diverse operational technologies and varying access requirements. Implementing asset-specific security boundaries strengthens the overall security posture by bringing protective measures closer to the operational elements they safeguard, enhancing the responsiveness and resilience of CI operations.

The Kipling Method for Policy Creation

ZT policies can be created using the Kipling Method, which addresses the "who, what, when, where, why, and how" aspects of the network and its policies. Leveraging the Kipling Method for policy creation empowers granular enforcement, ensuring that only known, authorized traffic and legitimate application communication are allowed within the CI network. This strategic process substantially reduces the attack surface while minimizing the reliance on traditional port-based firewall rules.

By employing the Kipling Method, precise policies can be defined for access control and communication within the OT/ICS networks. It can easily formulate policies by addressing the following key points.

Who (Asserted Identity)

Identify and define the authorized users, devices, and entities that should have access to CI resources. Establish clear roles and privileges for different personnel based on their responsibilities and tasks within the infrastructure.

- *Key question*: Who should access this resource?
- *Considerations*:
    - Identify authorized users, roles, and entities.

    - Establish access privileges based on responsibilities and regularly review the justification for such access.
    - Implement phishing resistant multi-factor authentication for improved security.
    - Regularly review and update user access rights.
    - Maintain a central user identity repository for streamlined management.

What (Application)

Determine which approved applications and services authorized identities can use to access critical resources. Ensure that only secure and sanctioned applications interact with the infrastructure.

- *Key question*: What applications are allowed?
- *Considerations*:
    - Define approved and secure applications.
    - Implement application allowlisting and denylisting.
    - Monitor application usage to detect unauthorized software.

When (Timing)

Specify the conditions under which access to critical resources is granted. Define access rules that control when and under what specific circumstances certain identities can interact with assets or systems. Importantly, ensure that in emergency situations, operators are not locked out of critical systems.

- *Key question*: When can access occur?
- *Considerations*:
    - Set specific access schedules and timing rules (while allowing for emergencies).
    - Implement time-based access controls for critical resources.
    - Configure access expiration for temporary privileges.

Where (Destination)

Identify the specific servers, databases, network segments, and other assets within the CI with which authorized identities are permitted to communicate.

- *Key question*: Where can access take place?
- *Considerations*:
    - Identify the allowed destinations or endpoints.
    - Define network segments and subnets for controlled communication.
    - Implement geographic restrictions if required.

Why (Purpose)

Identify the reasons and purposes behind each access request to critical resources. Apply data classification and contextual information to ensure that access is granted based on the legitimate needs of the request.

- *Key question*: Why is access necessary?
- *Considerations*:
    - Document the reasons and purposes for each access request.
    - Apply data classification to differentiate sensitive information.
    - Use contextual information to determine access legitimacy.

How (Method of Access)

Describe the methods and protocols used by authorized identities to access critical resources. This involves specifying the allowed communication channels, authentication mechanisms, and encryption standards.

- *Key question*: How is access granted?
- *Considerations*:
    - Specify authentication methods (e.g., username/password, tokens).
    - Implement encryption for data transmission.
    - Define allowed communication protocols (e.g., HTTPS, SSH).
    - Utilize virtual private networks (VPNs) or other secure channels for remote access, and layer MFA where appropriate.

Step 5: Ongoing Monitoring and Maintenance Activities in OT/ICS

The CSA has general guidance for the five-step implementation process found in the ZTAC Resource Hub. This section provides guidance specific for OT/ICS environments.

For CI, continuous monitoring and analysis are crucial to detect and respond swiftly to any potential threats. Real-time analysis of network traffic, user behaviors, and device activities allows security teams to promptly identify anomalies and potential security breaches. Regular security assessments and penetration testing are also conducted to identify and address vulnerabilities proactively.

Activities for Ongoing Support of Zero Trust in OT/ICS

At a minimum, your ZT program in an OT/ICS environment should include the following elements.

Incident Response Planning for OT/ICS

If your team has been tasked with incident response (IR) for OT/ICS assets, it's suggested that you bring in specialists for this activity and incorporate and integrate the OT/ICS portion of the IR plan with the enterprise IT IR plan for a holistic approach.

Enterprise IT service providers and IR teams that don't specialize in OT/ICS environments are not equipped for this task. Work with a specialized partner, and identify and secure that partner early, not during or after a cybersecurity incident. That partner may also be instrumental in assisting with the other activities in your ZT planning, starting with step 1 and continuing through step 5.

The OT/ICS assets may be targeted, but in recent years, notable CI attacks have originated on the enterprise IT side. This is another case for tackling the OT and IT IR planning holistically. Your ZTA will inform the relationship of the protected assets, the operational flows, and dependencies including those to and from the IT network.

Visibility and Monitoring of OT/ICS

Visibility into the OT/ICS networks is a key piece of any cybersecurity plan and certainly a required element for a ZTA. Ensure you have identified the assets and data paths that need to be monitored and have a plan for collecting the appropriate data and sending it to the appropriate repository. This may include centralized logging, OT/ICS SOC tools, and/or tools from a manufacturer or third-party partner responsible for monitoring the network.

Also, keep in mind that these environments will be communicating with protocols specific to the OT/ICS environment, and traditional enterprise IT tools may not be suited to or even aware of this traffic. Work with your manufacturers, installers/integrators, or monitoring partners to ensure OT/ICS-aware tools are in place. This will likely include OT/ICS-aware firewalls, among other tools.

One noticeable benefit of an OT/ICS network (versus an IT network) is the opportunity for much more granular visibility and high-fidelity alerting. These networks don't have the continuous chatter and volume of data and flows that plague IT networks, meaning monitoring and identifying baselines and anomalies can be markedly easier.

Vulnerability Management in OT/ICS

You may recall from earlier in Differences in Architecture of OT/IT that patching is the appropriate action in OT/ICS networks only around 4%-10% of the time. This means your OT/ICS network vulnerability management program should not center around patch management. Instead, it should include contextual vulnerability assessment and rely heavily on visibility/monitoring and other mitigating controls. The ZT policies, if properly implemented, serve as a perfect mitigating control in an OT/ICS vulnerability management program.

On the networking side, mitigating controls could include making equipment invisible to unauthenticated/unvalidated entities using techniques such as software-defined perimeter (SDP) and single-packet authorization (SPA)[33], and/or the emerging network hiding protocol (NHP)[34], which builds on the principles of network obfuscation introduced by SPA but is extending these to the broader network architecture level rather than focusing solely on endpoint or service hiding.

Detailed Ongoing Zero Trust Architecture Efforts

Sustaining a ZTA that continues to protect your environment as it grows and evolves requires ongoing efforts. These efforts should align with (and not duplicate) existing efforts to mature a cybersecurity program and/or maintain compliance with laws and industry regulations.

Ideally, a ZTA will meet a maturity level that allows for automation of these ongoing activities, and limited manual documentation and reporting. Whether manual or automated, the ZT lifecycle and activities need to be continued throughout the life of the system(s) in scope.

The cadence of these updates will depend on how manual or automated the data collection is along with any prevailing guidance, regulatory requirements, or laws dictating your activities for cybersecurity efforts in your geography or sector. At a bare minimum, it is suggested that these activities be repeated annually. If systems and automation allow for it, every 90 days or continuous analysis is preferred. For industries with potential impact to safety, health, or the environment, documentation will need to be reviewed and updated as part of change management.

Activities will include the following.

Revisiting Step 1, Defining the Protect Surface as Assets Change

This can be addressed by piggybacking ZTA tasks with any internal ticketing and approvals for acquisitions and/or moves, adds, or changes in the OT/ICS network(s).

Revisiting Step 2, Mapping Operational Flows as Access Requirements Change

Even if the assets remain static for a period of time, the access requirements and therefore operational flow mappings may need to be updated. Examples include pandemic scenarios, such as shelter-in-place orders, that demanded additional remote access to OT/ICS networks.

[33] Software-Defined Perimeter (SDP) Specification v2.0 | CSA
[34] OpenNHP Documentation

Revisiting Steps 3 and 4, Building a Zero Trust Architecture and Creating Policies

As technology advances, assets are replaced or upgraded, and access scenarios change, the ZTA and policies will also be updated. These activities include maintaining documentation and diagrams of the architecture and updating controls and products or integrations that serve the ZT policy enforcement points.

As part of this activity, it's also advisable to periodically reassess your security vendors and tools, requesting updates on roadmaps to understand new features and integrations available to you.

Revisiting Step 5, Incident Response, Monitoring, and Vulnerability Management Processes

The entire ZT roadmap is a rinse-and-repeat workflow, and step 5, detailing the ongoing care and maintenance of the environment, is no exception. Incident response plans, monitoring tools, analysis, and vulnerability management should be part of the continuous evaluation and improvement activities.

SANS Top 5 Critical Controls in OT/ICS

Often, cybersecurity professionals are inundated with conflicting and overlapping cybersecurity guidance. The goal of the guidance here is to continue offering ZT planning for OT/ICS, relating it to the existing guidance and activities as much as possible.

The SysAdmin, Audit, Network, and Security (SANS) Institute outlines five essential OT/ICS systems controls to guide organizations in investing appropriately based on threat-informed activities[35]. Having gone through all five implementation steps, we can now reflect on how the ZT strategy fortifies the SANS critical controls. These align well with many of the ZT roadmap activities suggested here.

1. ICS Incident Response
2. Defensible Architecture
3. Visibility Monitoring
4. Secure Remote Access
5. Risk-Based Vulnerability Management

[35] The Five ICS Cybersecurity Critical Controls

Zero Trust and the Five Critical Controls for OT/ICS

The five critical controls and their relationship to a ZTA in OT/ICS are:

ICS Incident Response

The OT/ICS-specific incident response plan is part of ZT roadmap step 5, ongoing monitoring and maintenance. It's also required for most CI sectors worldwide.

As discussed earlier in Convergence of OT and IT with Digital Transformation and Incident Response Planning for OT/ICS, Incident Response emerges as a critical area requiring specialized attention. With ICS Incident Response identified as the first critical control, it is essential to understand that response plans for OT environments are fundamentally different from those in IT settings.

While adopting a ZT strategy is crucial, it must be distinctly tailored for OT sectors. Despite the core principles of ZT remaining consistent, their application needs specific adjustments to address the unique challenges and operational nuances of each sector. This ensures that security measures are both effective and pertinent, keeping pace with the converging landscapes of IT and OT.

Defensible Architecture

SANS states architectures that support visibility, log collection, asset identification, and segmentation are defensible, as in they can be defended if attacked. The Zero Trust Five-step implementation detailed in this document offers a prescriptive process for creating a defensible architecture. From identifying assets to monitoring, the ZTA addresses each feature of a defensible architecture.

In OT environments, where systems may not support modern patches, the principle of "mitigation over patching" takes precedence. This approach emphasizes mitigation strategies rather than frequent updates. During operational flow mapping, prioritize compensating for inherent vulnerabilities of legacy systems through segmentation, access control, and continuous monitoring. Recall additional techniques mentioned in the Vulnerability Management section.

ICS Network Visibility Monitoring

This critical control recommends continuous network security monitoring of the OT/ICS environment with protocol-aware tool sets, which aligns with step 5, ongoing monitoring and maintenance. This approach ensures comprehensive visibility into the operational state and security posture of OT/ICS systems.

In OT/ICS environments, visibility monitoring focuses primarily on internal changes. ZT principles emphasize the importance of monitoring configuration file changes within the environment, as these can indicate potential security breaches or unauthorized alterations to critical systems. This perspective

should be integral to step 2, mapping operational flows, with a vigilant eye on internal system modifications.

Secure Remote Access

Secure remote access entails an inventory of remote connections, paths, and access methods. These items are defined throughout the ZT implementation process, starting with step 1, defining the Protect Surface, continuing through step 2, mapping the operational flows, and through steps 3 and 4 of building a ZTA and creating the policies. In addition, the ongoing monitoring in step 5 activities ensures remote access remains centrally managed, controlled, and is not being abused.

Emphasizing the point made in Closing Out Step 2 on the criticality of mapping operational flows, diligently working through step 2 will help identify remote access communication paths and external connections which are a priority to secure, recognizing that many OT security incidents have originated from internet-facing services.

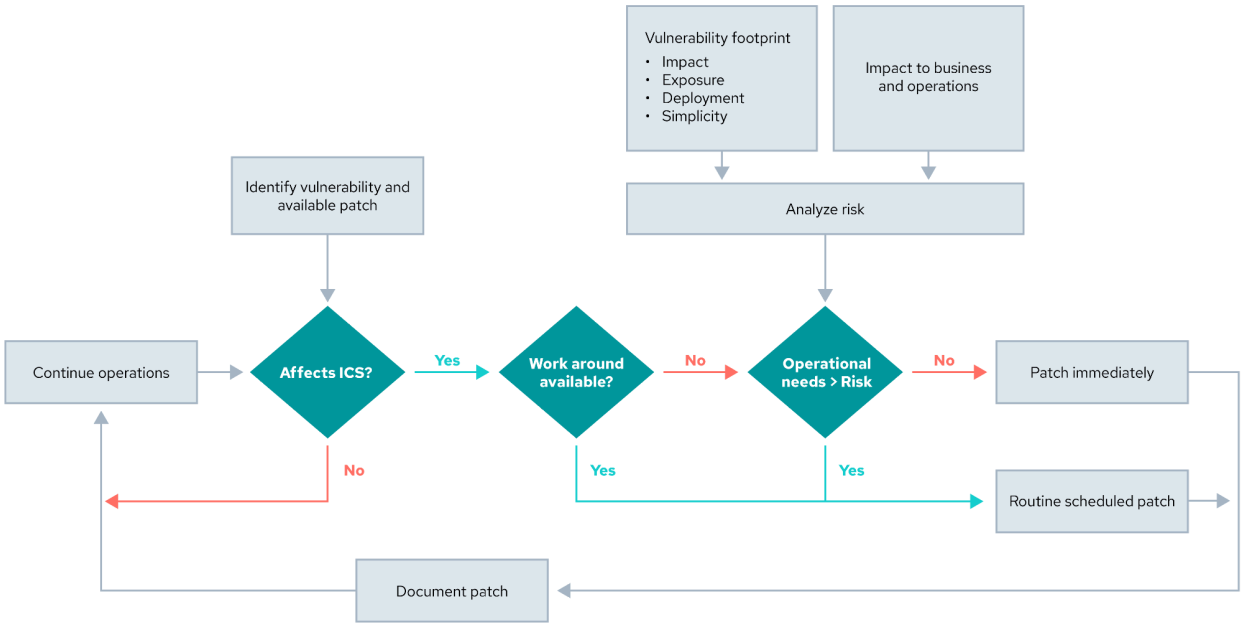
Risk-Based Vulnerability Management

Risk-based vulnerability management in OT/ICS environments considers cyber-physical assets, controls, and expected operating conditions. The ZT implementation process enhances this approach by providing a comprehensive understanding of critical data pathways through operational flow mapping. This insight informs segmentation strategies and simplifies system complexity, crucial for effective risk management.

ZT principles support this critical control by facilitating appropriate patching practices, implementing mitigating controls where patching isn't feasible, and enabling continuous monitoring. This SANS control aligns with the NIST Cybersecurity Framework (CSF)[36] and Zero Trust Architecture (ZTA)[37], which complement each other in improving cybersecurity of devices, assets, applications, and services.

Importantly, vulnerability management in OT/ICS deviates from traditional IT practices, particularly in scanning, identification, and patching processes. CISA recommends a specific patching workflow for control systems, reflecting the unique challenges in these environments:[38]

[36] NIST Cybersecurity Framework 2.0
[37] NIST Zero Trust Architecture
[38] Recommended Practice for Patch Management of Control Systems



Guidance For New OT & ICS Systems

This document generally focuses on providing guidance for applying ZT principles within existing Operational Technology (OT) and Industrial Control System (ICS) environments. The strategies and methodologies outlined here are designed to help organizations retrofit ZT security measures into their current infrastructure. This includes a detailed examination of OT/ICS systems' unique characteristics, challenges, and specific recommendations for implementing ZT capabilities, despite such constraints.

While this guidance generally targets existing environments, it's important to recognize both the evolving threat landscape and cybersecurity technology marketplace, which includes increasing customer and regulatory agency requirements for technology to be "secure by design" - particularly for CI installations. Consequently, Vendors and Original Equipment Manufacturers (OEMs) are increasingly incorporating general cybersecurity and ZT capabilities into new technology and enhancements to existing products. This proactive integration of general cybersecurity and ZT capabilities specifically is particularly important for greenfield deployments, where new infrastructure can be procured and implemented securely by design.

Accelerating Zero Trust with Modern Solutions

As the industry advances, many vendors/OEMs are embedding ZT features and capabilities into their solutions, offering capabilities such as hardware-based security modules, machine identity, ZT networking overlays, continuous authentication, microsegmentation, and enhanced monitoring as built-in functions. Some of these capabilities are developed by the vendors while others are enabled by partnering - either white-labeled or explicit partnerships.

A few examples include Siemens, GE Vernova, Rockwell Automation, and Schneider Electric. Some of these examples are direct product capabilities, some are recommendations for ZT in industrial control systems. These innovations can significantly expedite the adoption of a ZT posture, especially in greenfield scenarios where the absence of legacy systems allows for more straightforward implementation of modern security frameworks. It should also be noted that some of these capabilities can also be applied to brownfield scenarios when the vendor OEM is delivering a software based capability which can be over-the-air (OTA) updated to existing products and installation bases - e.g. applying a firmware update to an industrial firewall to enable ZT overlay connectivity.

As ZT relies on integrating the various pillars into a cohesive and automated approach, OEM vendors who build comprehensive portfolios, partnerships, and 3rd party integrations (via open APIs) will be best placed to help CI (OT/ICS) organizations to reach a high maturity of ZT (see the CISA Zero Trust Maturity Model referenced earlier in this document). This integration is crucial because it allows for real-time enforcement of security policies and continuous verification of security posture across the entire IT environment. By automating these processes, organizations can quickly and efficiently detect and respond to threats, minimize human error, and ensure that security measures are consistently applied.

Leveraging these cutting-edge technologies can help organizations achieve a robust ZTA more efficiently. This approach not only enhances security but also ensures compliance with evolving regulatory requirements and adapts more readily to the dynamic threat landscape.

By integrating ZT principles into new and existing deployments, organizations can avoid the complexities and constraints associated with retrofitting legacy systems. This document serves as a foundational guide for securing existing OT/ICS environments, while also acknowledging the forward-looking trend towards inherently secure-by-design technologies.[39]

Conclusion

In today's interconnected world, CI sectors face an ever-evolving landscape of cyber and physical threats. As these sectors embrace digital transformation and the convergence of operational technology (OT) and information technology (IT), the need for robust, adaptable security strategies has never been more pressing. ZT offers a powerful strategy for fortifying these critical systems against increasingly sophisticated adversaries that can keep pace with rapid technological advancements and the evolving threat landscape.

This paper provides a comprehensive roadmap for applying ZT principles to OT/ICS environments. By executing the repeatable five-step process organizations can effectively mitigate risks and enhance the resilience of their CI.

1. Define the Protect Surface
2. Map Operational Flows
3. Build a Zero Trust Architecture

[39] CISA Secure By Design

4. Create Zero Trust Policies
5. Monitoring and Maintenance

The guidance presented here is not a one-size-fits-all solution, but rather a flexible, scalable approach that can be tailored to the unique requirements of each sector and for both new and existing systems. By leveraging existing standards, such as ISA/IEC 62443, and aligning with the five critical controls outlined by SANS, along with secure-by-design principles for new systems, this ZT strategy integrates with current best practices while providing a forward-looking path for continuous improvement.

Organizational Collaboration and Commitment

Ultimately, the successful implementation of ZT for CI demands a collaborative, cross-functional effort along with a strong organizational commitment to risk mitigation. It requires executive commitment along with the expertise of cybersecurity professionals, the insights of OT engineers and system operators, and OT solution providers' innovation. By fostering open communication, shared understanding, and a commitment to security and safety at every level, CI sectors worldwide can harness the power of ZT to safeguard the systems that underpin our modern way of life. In doing so, they not only protect their own operations but also contribute to the collective resilience of our global community in the face of an ever-changing threat landscape, enhancing the safety, reliability, and resilience of services that are essential for physical and economic well-being.

Useful Resources

References

1. Existing CI & OT Guidance and Regulations
    a. Critical Infrastructure resources by sector at NIST CSF 1.1 Critical Infrastructure Resources | NIST
    b. SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security | CSRC
    c. ISA/IEC 62443 Series of Standards
    d. The Five ICS Cybersecurity Critical Controls
    e. PCAST Releases Report on Strategy for Cyber-Physical Resilience
    f. US OMB Memo M-24-14: Administration Cybersecurity Priorities for the FY 2026 Budget
    g. National Security Memorandum on Critical Infrastructure Security and Resilience | The White House
    h. PCAST Strategy for Cyber-Physical Resilience Feb 2024
    i. DHS Offers WMD, Critical Infrastructure AI Guidance – MeriTalk
    j. Mitigating AI Risk: Safety and Security Guidelines for Critical Infrastructure Owners and Operators
    k. MITRE ATT&CK ICS Matrix
    l. Top 20 Secure PLC Coding Practices
    m. OT Zero Trust Alliance
    n. Simplifying Adoption of ISA/IEC-62443 Using the Zero Trust Model for Operational Technology - Palo Alto Networks
    o. ISAGCA Whitepaper: Zero Trust Outcomes Using ISA/IEC 62443 Standards
    p. Zero Trust Whitepaper - Siemens Global
    q. CRITICAL INFRASTRUCTURE - CYBYR
    r. CISA Identifying and Mitigating Living Off the Land Techniques
    s. CISA Alert: Threat Actors Continue to Exploit OT/ICS through Unsophisticated Means
    t. Principles of Operational Technology Cyber Security
2. Critical Infrastructure sectors by region
    a. UK: Critical National Infrastructure | NPSA
    b. EU: erncip
    c. US: Critical Infrastructure Sectors | CISA
    d. Singapore: Cybersecurity Act
    e. India: National Critical Information Infrastructure Protection Centre
3. CSA Resources
    a. CSA Zero Trust Resource Hub
    b. CSA Cloud Security Glossary
    c. CSA Defining the Zero Trust Protect Surface | CSA
    d. CSA Map the Transaction Flows for Zero Trust | CSA
    e. CSA Zero Trust for Critical Infrastructure Presentation Recording of Dr. Ron Martin
    f. CSA Zero Trust for OT & IoT - Zscaler CSA ZT WG Presentation Recording
    g. CSA Agentless Network Microsegmentation - BYOS

h. CSA ZT Networking for difficult use cases - CI/OT/IoT, air gapped networks and more - NetFoundry

4. Other References
   a. NSTAC Report to the President on Zero Trust and Trusted Identity Management
   b. International CIIP Handbook 2008/2009
   c. CISA Zero Trust Maturity Model Version 2.0
   d. DoD Zero Trust Reference Architecture
   e. DoD Zero Trust Capability Execution Roadmap
   f. DoD Zero Trust Strategy
   g. DoD Zero Trust Symposium 2024 recordings - day 1, day 2
   h. CISA/NSA/FBI/ASD ACSC Guidance: Best Practices for Event Logging and Threat Detection
   i. Consequence-driven Cyber-informed Engineering (CCE) - Idaho National Laboratory
5. Service Provider References
   a. Dragos
      i. Robert M. Lee on LinkedIn: The Evolution of Industrial Cyberthreats: Year in Review Report
      ii. Asset Visibility for ICS environments | Dragos Platform
      iii. Key Concepts of ISA/IEC 62443: Zones & Security Levels | Dragos
      iv. Whitepaper: Network Segmentation Challenges and Solutions
   b. Claroty Asset Inventory - Platform
   c. Nozomi Networks
      i. OT Asset Inventory Management
      ii. ISA/IEC 62443 Compliance Mapping Guide
   d. Armis Full Asset Inventory and CMDB Enrichment
   e. ICS Village
   f. SCYTHE
   g. Zscaler
      i. Building a resilient manufacturing environment through zero trust OT cybersecurity controls
      ii. Complete OT Security | Zscaler
      iii. Zero Trust for OT & IoT - Zscaler
   h. Zero Trust Security – Massive Scale Consulting

Definitions of Acronyms Used in This Paper

This paper uses the following acronyms as defined within the CSA Glossary[40]:

1. Critical Infrastructure (CI)
2. Cybersecurity and Infrastructure Security Agency (CISA)
3. Cyber Physical Systems (CPS)
4. Data, Applications, Assets, and Services (DAAS)

[40] Cloud Security Glossary

5. Distributed Control System (DCS)
6. Human-Machine Interface (HMI)
7. Industrial Control System (ICS)
8. Industrial Internet of Things (IIoT)
9. Operational Technology (OT)
10. Programmable Logic Controller (PLC)
11. Policy Enforcement Points (PEPs)
12. Policy Decisions Points (PDPs)
13. SysAdmin, Audit, Network, and Security (SANS)
14. Safety Instrumented System (SIS)
15. Hardware Security Module (HSM)
16. Zero Trust (ZT)
17. Zero Trust Architecture (ZTA)
18. Zero Trust Advancement Center (ZTAC)
19. Zero Trust Maturity Model (ZTMM)

Glossary

Zero Trust Glossary References:

- CSA Glossary (main/primary)
- On2IT ZT Glossary - Zero Trust Dictionary (John Kindervag)
- CSA SDP Glossary (Software Defined Perimeter)