White Paper
May 2025

Defining Industrial Zero Trust Vision

DeltaV™

EMERSON™

www.emerson.com/deltav

Table of Contents

Defining Industrial Zero Trust Vision

Executive Summary 3
1. Introduction 4
1.1 Purpose 4
1.2 Relevant Documentation 4
1.3 Cybersecurity Threat Mitigation Landscape 5
1.4 The Need for Zero Trust 8
1.5 Defining Zero Trust 8
2. Zero Trust in OT 10
2.1 OT-specific Concerns 10
2.2 Assessing Risk to OT Systems 11
2.3 Emerson's On-ramp to the Zero Trust Journey 12
3. The Zero Trust Journey 13
3.1 Zero Trust Maturity Journey 13
3.2 Zero Trust Architecture Components 17
3.3 Potential Threats Associated with Zero Trust Architecture 19
3.4 Partnership Ecosystem 21
3.5 Optimal Maturity Level Objectives for OT 23
4. Final Considerations 25

Executive Summary

Problem Statement

New cybersecurity technologies continually emerge in the marketplace but are always outpaced by evolving cyber threats. A need for improvement and digital transformation of the current operational technology (OT) space necessitates a paradigm shift in how plants secure their operations. OT systems must be connected to the internet and cloud to drive performance, but that connection must be secured in a way that prioritizes availability.

Key Proposition

The increasing frequency of high-profile cyberattacks on OT systems underscores the urgent need for a holistic zero trust cybersecurity approach to safeguard critical infrastructure against current and emerging threats. Moreover, in Executive Order 14028, the federal government mandates a move toward zero trust architecture.

What is Zero Trust?

Zero trust is a security framework that operates on the concept of "never trust, always verify." No user or device, whether inside or outside the network, is trusted by default. Instead, every access request must be authenticated, authorized, and continuously validated before granting access to applications and data. Zero trust is not a product to be purchased, but rather a strategy and company culture to be followed long-term.

Key Features of Emerson's Zero Trust Approach

Zero trust principles, while not a single solution for all cybersecurity issues, offer a robust defense against evolving cyber threats. Emerson recommends that organizations define long-term cybersecurity goals for DeltaV systems and begin the zero trust journey, gradually adopting and enhancing security measures as personnel and solutions mature.

Key Considerations

- Zero trust is a concept and journey, hence no list of architecture components available today is all-inclusive. New components will evolve over time and others will become less useful.
- Zero trust for OT does not conflict with other concepts such as defense-in-depth.
- Zero trust requires a partnership ecosystem where technology and automation providers work in tandem to develop and deploy seamlessly interconnected solutions.
- OT teams should rely on vetted solutions for developing zero trust architecture to work with DeltaV systems.
- Emerson continues to evaluate options for incorporating zero trust conceptual applications into DeltaV systems, especially with concepts that support the secure-by-design approach, and there are some steps in the zero trust maturity journey that can be implemented on DeltaV systems today.

1. Introduction

1.1 Purpose

As industrial operational technology (OT) environments become increasingly interconnected and digitized, the need for robust cybersecurity measures has never been greater. 21st-century industry faces a unique set of security challenges, and traditional approaches are no longer sufficient to protect critical infrastructure. An evolving threat landscape, transformation of the compute paradigm, and heterogeneity of industrial systems has triggered regulatory pressures focused on protecting public safety and national security.

Accordingly, modern OT cybersecurity requires a holistic and systematic approach based on an industry-accepted zero trust principles-based framework. This white paper explores the vision of zero trust principles—applied to industrial OT environments generally as well as the DeltaV Distributed Control System (DCS) specifically—and emphasizes a holistic approach to cybersecurity that is adaptable to various deployments (on-prem, hybrid, cloud) and can be scaled across the layers of the technology stack (networks, applications, endpoints, and data), with the goal of attaining comprehensive protection of the OT environment via interoperable solutions.

1.2 Relevant Documentation

Understanding modern standards and frameworks is an essential baseline in translating zero trust principles to conformant deployments. The National Institute of Standards and Technology's (NIST's) publication SP 800-207[1] is a primary guideline that outlines the key concepts and essential elements of zero trust architecture across industry segments. In addition, the NIST Cybersecurity Framework[2] and SP 800-53[3] provide risk-focused strategies and security measures that are in harmony with zero trust principles.

Given the amplified convergence of information technology (IT) with OT in the industrial sector, it is important to consider global ISO/IEC norms that were developed for IT segments to comprehend the impact on OT. ISO/IEC 27001[4] Information Security Management and ISO/IEC 27002[5] Code of Practice for Information Security Controls are fundamental standards widely adopted by IT organizations. Although these standards don't explicitly define zero trust, they provide a framework for managing information security risks that are implicitly based on zero trust principles and thus highlight the importance of information security management and optimal practices necessary for zero trust.

The ISA/IEC 62443[6] series of standards focuses on security for industrial automation and control systems, incorporating zero trust principles, especially in critical infrastructure areas.

ISA/IEC 62443 explicitly calls for risk assessments, network segmentation, access controls, modelling for zones and conduits, and continuous monitoring. This series of standards provides practical steps for implementation that consider the heterogeneous nature of industrial compute environments comprised of legacy systems with limited upgradability. Therefore, ISA/IEC 62443 recommends compensating controls for legacy OT systems to address zero trust framework requirements.

[1]https://csrc.nist.gov
[2]https://www.nist.gov/cyberframework
[3]https://csrc.nist.gov
[4]https://www.iso.org/standard/27001
[5]https://www.iso.org/standard/75652
[6]https://www.isa.org/standards-and-publications

The Cybersecurity and Infrastructure Security Agency (CISA)[7] complements zero trust standards via its Zero Trust Maturity Model (ZTMM). This model offers a structured approach for developing strategies that enable organizations to transition towards a zero trust architecture. ZTMM outlines the gradient based implementation across five distinct pillars, where advancement can be made gradually to maintain continuity.

In addition to standardization, zero trust has been extensively discussed in industry publications by leading companies like Microsoft , Emerson, Intel[8] and others, emphasizing the critical role of zero trust for strengthening security postures.

1.3 Cybersecurity Threat Mitigation Landscape

Although new cybersecurity measures and technologies are continually coming to market, they always seem to be outpaced by evolving threats. 83% of company boards say they have improved their understanding of cyber-risks, and yet many struggle to keep pace with changing cyber-threats.

According to a report by ABI Research[9], the OT cybersecurity market is projected to grow from $12.75 billion in 2023 to approximately $21.6 billion by 2028, with 9.2% CAGR. This growth is driven by increased digitalization and smart manufacturing trends across various industrial sectors, leading to a heightened demand for robust cybersecurity measures.

The SANS Institute 2024 industrial control system (ICS)/OT cybersecurity survey[10] highlights progress in critical infrastructure security, with improvements in detection capabilities and cloud adoption.

In the survey, only 33% of respondents utilized OT-specific monitoring in 2019. This increased to 52% in 2024, as a reflection to the growing concerns on CS/OT cybersecurity. However, the survey also highlighted significant gaps in readiness and workforce preparation. Only 34% of respondents use ICS/OT-specific tools to prepare for cyber incidents. This indicates that despite increased maturity, many organizations are still lacking adequate cybersecurity measures for OT environments, creating additional risks as interconnectedness grows. This report supports the 2025 U.S. Homeland Threat Assessment by the Department of Homeland Security[11] that warns of escalating threats to critical infrastructure from domestic and foreign adversaries.

[7]https://www.cisa.gov/zero-trust-maturity-model
[8]https://www.intel.com
[9]https://www.abiresearch.com
[10]https://sansorg.egnyte.com
[11]https://www.dhs.gov

In 2024, the Cybersecurity and Infrastructure Security Agency (CISA) released numerous ICS advisories to address various security issues, vulnerabilities, and exploits affecting industrial control systems. These advisories highlight the ongoing efforts by CISA to address security concerns in industrial control systems across various sectors and vendors. ICS Advisory Project[12] , an open-source project that provides dashboard of CISA ICS advisories reports that throughout 2022-2024, manufacturing continues to remain the top affected segment (Figure 1-3).

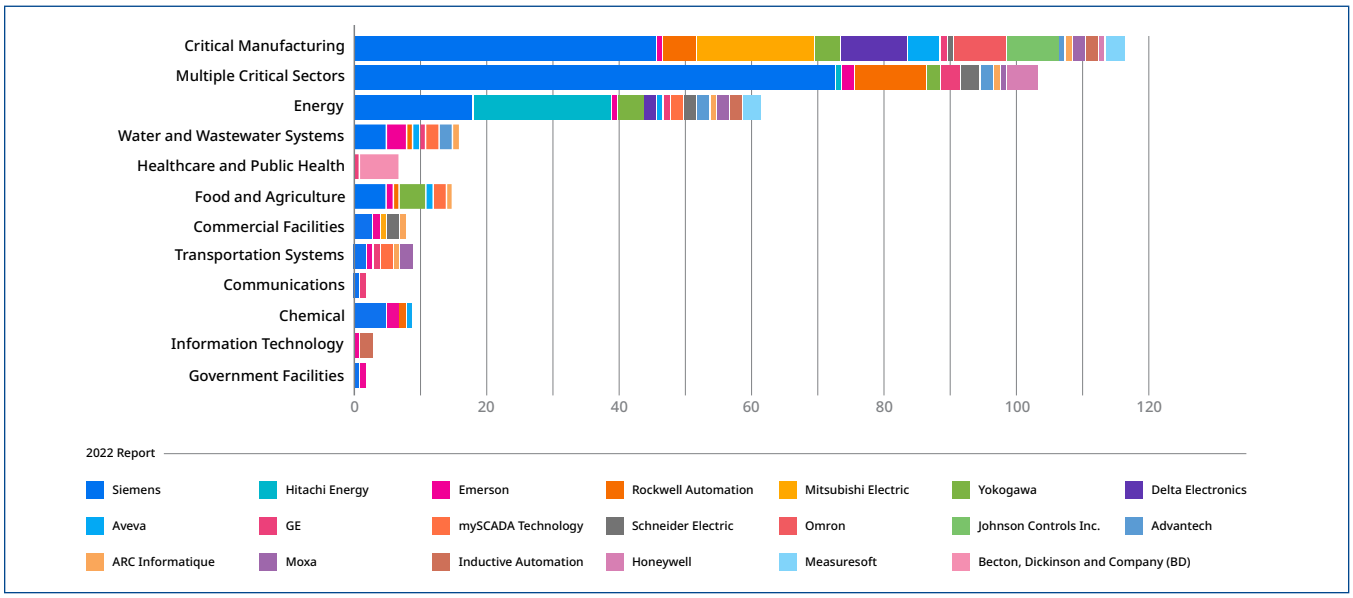

Figure 1: *ICS-Cert Advisory Count in 2022.*

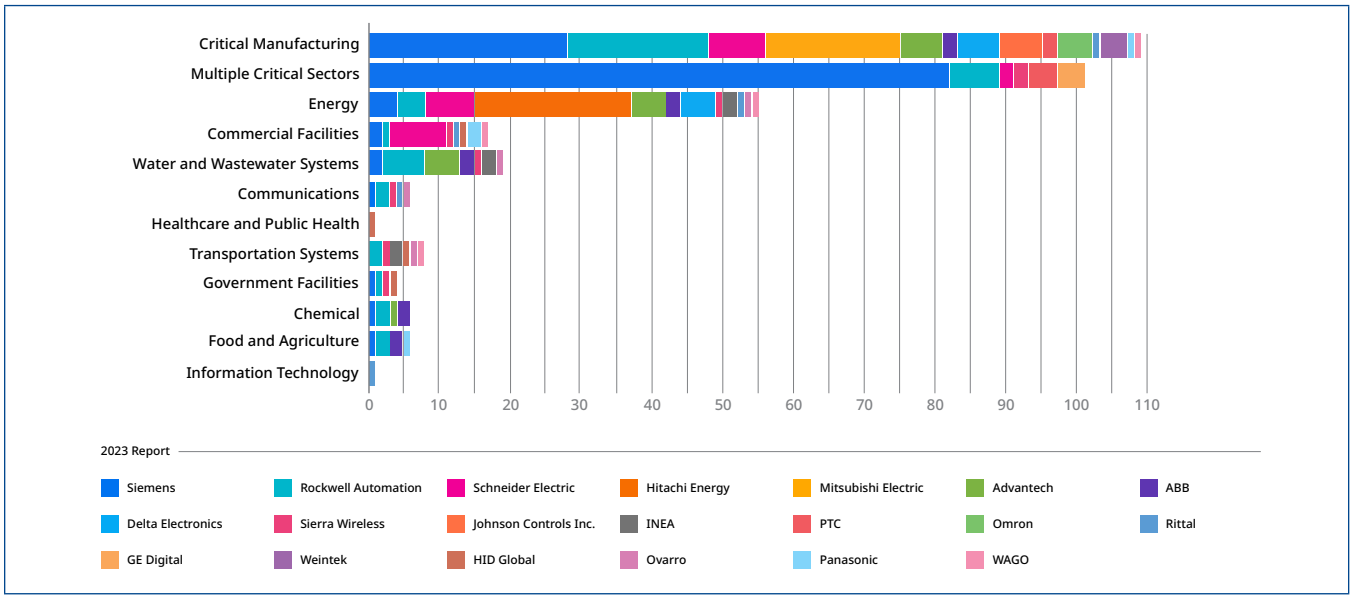

Figure 2: *ICS-Cert Advisory Count in 2023.*

[12]https://www.icsadvisoryproject.com/home

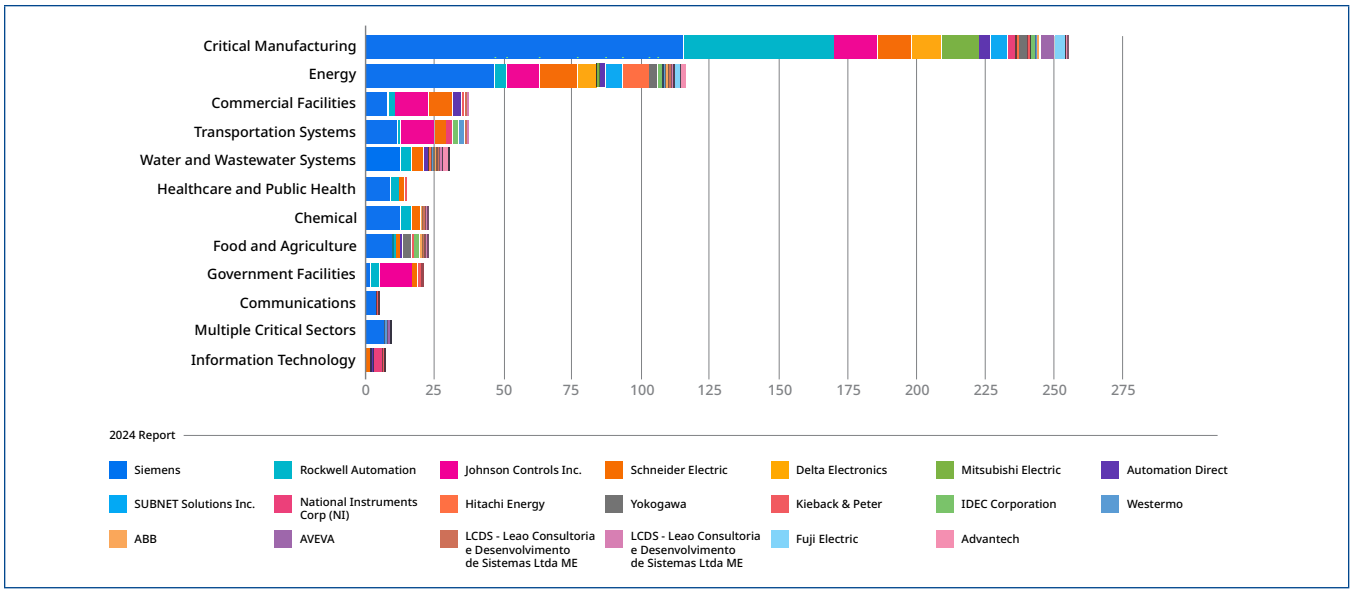

Figure 3: *ICS-Cert Advisory Count in 2024.*

1.3.1 Critical Perspectives

New requirements continue to be imposed over the global supply chain, revolving around verifications that will guarantee data security, recovery models, compliance and governance, vulnerability management, and security assurance plans. Requirements and regulation do not follow a cookie-cutter model, thus the complexity of operating in this new environment can vary based on critical elements such as having a standardized checklist, as well as having strategies in place to add a new provider in the ecosystem or ensuring chain of trust during regular validations.

The inclusion of new steps implies a need for more resources, more time and, accordingly, more cost associated to supply chain verifications that were not required before cybersecurity became so relevant. Years ago, OT teams would not spend extensive time with cybersecurity as asset owners in these industries were not hearing about real life scenarios at their level, only at the IT network levels. Today, there are many examples of OT systems hit by ransomware and other cyber-threats, so what used to be a hypothetical case ("IF I'm hit, then I'll take some actions") is now a matter of assumed risk ("WHEN I'm hit, then I better be prepared.")

1.3.2 The IT/OT Convergence

Cybersecurity for IT and OT have the same objectives, though the priorities are slightly different. In the confidentiality, integrity, and availability (CIA) triad, in general IT will prioritize confidentiality over integrity and availability, with availability at the last position. This is not to say that availability does not matter for IT. Availability is critical, but not as critical as confidentiality. Conversely, OT will prioritize availability over integrity and confidentiality, with confidentiality the least critical. Again, this is not to say that confidentiality is not important for OT, but it is not as important as availability. Despite the different priorities, the main objective for IT or OT cybersecurity is to protect systems against cyber-threats.

Identity management is the starting point for zero trust on both IT and OT, but each technology has its own nuances that need to be addressed separately. In IT, flexibility of endpoints is a given, but they all receive the same policies and security controls depending on which part of the network they are connected to, and which user is authenticating on those devices. Also, the segmentation of systems and networks in IT is not dependent on brands or specific vendors' choices, as in IT the design, implementation and support for the infrastructure is self-provided—IT teams typically specify what their personnel can manage and support. This means that pursuing a zero trust journey is easier than in OT where design, implementation and support is likely provided by others, neither IT nor OT.

1.4 The Need for Zero Trust

Adoption of trailblazing technologies such as Artificial Intelligence (AI), 5G, Internet-of-Things (IoT), and edge computing have revolutionized industrial computing, significantly shifting the paradigm. Historically, OT systems were built on implicit trust—specifically security based on air-gapping as a primary method of protection via isolated internal zones of connectivity. With the rise of digital transformation, that model is no longer viable. OT systems are increasingly connected and interconnected, and IT networks and cloud services protrude the boundaries of OT, making traditional air-gapping insufficient and unsustainable.

In addition to a rising new paradigm of industrial computing, it is also essential to recognize the increased number of high-profile cyberattacks that have targeted industrial and OT systems. Examples such as the denial-of-service attack on Ukraine's power grid (2015), NotPetya ransomware attack (2017), and Oldsmar Water Treatment Facility hack (2021) have demonstrated that traditional security practices are insufficient in the modern era. Additionally, there was a rise in state sponsored attacks on critical infrastructure in 2023-2024. The SektorCERT[13] report from Denmark in 2023 demonstrated the capabilities of state-level adversaries. A recent communication[14] from the White House warns that essential infrastructure—such as water and wastewater systems—is a key focus for threat actors sponsored by foreign states. In fact, the IBM Security X-Force Threat Intelligence Index found that manufacturing is the most attacked industry – mainly driven by attackers taking advantage of existing OT/IT vulnerabilities.

This confluence of increasing connectivity and growing recognition of the value of OT targets demonstrates the urgency in developing a holistic zero trust approach to cybersecurity that can embrace novel technologies and apply proactive and dynamic security controls to ensure that industrial systems are prepared to address current and emerging threats effectively. This forward-thinking approach is crucial for protecting critical infrastructure and maintaining the integrity and availability of essential services in an increasingly connected world.

1.5 Defining Zero Trust

Zero trust is a security framework that operates on the concept of "never trust, always verify." This means that no user or device, whether inside or outside the network, is trusted by default. Instead, every access request must be authenticated, authorized, and continuously validated before granting access to applications and data. NIST SP 800-207 provides the following definition:

> *Zero trust provides a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised. Zero trust architecture is an enterprise's cybersecurity plan that utilizes zero trust concepts and encompasses component relationships, workflow planning, and access policies.*

Contrary to what the name says, zero trust does not mean that there is no trust to anything or anyone. Instead, zero trust requires a complete chain of trust based on constant verifications to ensure the right access and privilege is only given to the assigned resources in the ecosystem.

Zero trust is not a product, software, or single solution. It is a concept with several principles that enable asset owners to set a long-term journey striving to achieve a higher level of security for their systems. In the context of this document, zero trust is specifically applied to OT systems, where several cybersecurity challenges exist due to lack of a proper cyber posture.

[13]https://sektorcert.dk

[14]https://www.epa.gov

Ultimately, a zero trust framework is built around five core concepts:

- **Continuous Verification:** Always verify access to all resources, regardless of the user's location or device.
- **Least Privilege Access:** Grant users the minimum level of access necessary to perform their tasks, reducing the attack surface.
- **Micro-Segmentation:** Divide the network into smaller segments, each with its own security policies, to prevent lateral movement by attackers.
- **Strong Authentication:** Implement multi-factor authentication (MFA) and other robust identity verification methods.
- **Continuous Monitoring:** Monitor all network traffic and activities for suspicious behavior to detect and respond to threats quickly.

A zero trust strategy inherently rejects a common misconception of securing industrial control systems (ICS) that becomes less accurate with each passing year: that internal systems can be trusted implicitly. This is outdated and dangerous, evident in the trajectory of the cyber-attacks over the past decade. Threats change daily, but the security status of the ICS often does not, as applying patches and security updates can conflict with strict OT uptime requirements. Moreover, an increased reliance on third-party services has opened wide avenues for ICS attacks. These factors demonstrate that every part of the supply chain can be potentially compromised, which could lead to a cascading effect.

The principle of least privilege, a fundamental principle of zero trust, minimizes the attack surface by granting only the necessary access levels required for specific tasks to every internal system. In parallel, continuous monitoring with detection and response to anomalies in real-time enhance the resilience of ICS against cyber threats.

1.5.1 Current Limitations for Zero Trust Deployment on the Deltav DCS

Because achieving zero trust is a journey, not all concepts explained in this white paper are currently provided by Emerson. Some aspects of the zero trust maturity journey require changes to the DeltaV system (e.g., secure communications which is planned to be available with future versions of DeltaV software), and may require adding new layered solutions to the DeltaV system (e.g., policy engine, policy administrator, policy enforcement point, etc.). Despite being a thought-leadership piece, this document also lists some solutions and best practices that can be followed today to improve a DeltaV system cybersecurity posture which can be paired with the zero trust maturity journey.

Asset owners should not feel discouraged if they cannot fully implement zero trust as a bill-of-material today. The focus should be on defending critical DeltaV systems with currently available Emerson-vetted solutions. In the future, additional layers of protection will be made available and by then, Emerson will be able to provide such solutions for users to deploy on their DeltaV systems. Conversely, when the future solutions become the bill-of-material for DeltaV systems, there will be new considerations for the future as the threat landscape is always evolving.

2. Zero Trust in OT

2.1 OT-specific Concerns

As previously mentioned, the most important CIA triad indicator for OT is availability of systems. A system outage means limited or no production, which means revenue impact, and huge pressure to get issues resolved urgently. Integrity and confidentiality continue to be important, but not as prominent as availability in OT systems.

OT systems are more segregated than IT systems, and this may be the case because of lack of coordination during project design, compatibility between policies used at the IT network layers and the OT systems, or because some OT systems are not updated as regularly and must be kept "off-the-grid" to prevent exploitations. For example, one organization may use a certain brand of antivirus for the endpoints connected to the corporate networks, but at the same time have three other brands of antivirus as well as allow-listing technologies running on three different control systems that were provisioned by different OT vendors. This situation is very common and represents a risk and challenge to asset owners who cannot get support for all systems from a single vendor or their own IT department.

In addition, over a decade ago it was acceptable for asset owners to keep OT systems "air-gapped" from any other networks. As a result, it was common to see standalone OT systems performing their control functions without any type of monitoring or automatic patching. Today, this is no longer possible. Direct or indirect connectivity to external systems (or even to the internet or cloud) is needed at all layers. In a digitally transformed manufacturing world, "air-gapped" systems truly do not exist – all systems are always connected to other networks somehow.

However, OT systems are rarely integrated to a common management infrastructure serving different brands and types of control systems because each control system is designed, implemented and supported independently by its manufacturer. Availability and performance are guaranteed by the vendor of choice. While this support can be extremely beneficial, many OT teams seeking more flexibility and increased operational excellence are pursuing a manufacturing layer domain or root automation domain at level 3 of the Purdue Model to provide identity management services to various OT systems. Ultimately, this should not be a problem as long as there is still enough separation between the Level 3 and higher networks (Enterprise/Corporate IT). However, this increased connectivity will drive a need for increased cybersecurity, which will likely require a zero trust journey.

Besides identity management and the dependency to externally provided warranties and support, OT systems are harder to patch due to the availability requirements limiting the opportunity for service outages. Moreover, OT systems are set with a lifecycle of 10-20 years which is significantly longer than IT systems which are commonly expected to be replaced or updated within 3-5 years. This disparity creates further complexity for managing and maintaining cybersecurity across the IT/OT convergence.

Another point to consider is the cybersecurity maturity of OT personnel if compared to IT. Cybersecurity is a common function of corporate IT departments, whereas for OT, cybersecurity is a burden, and very much a foreign language that requires OT personnel to spend precious time and resources pursuing training.

2.2 Assessing Risk to OT Systems

Historically, governmental entities and standards committees used to categorize key industries (e.g. power, water, healthcare, and similar) as critical infrastructure when considering regulation and response for cyber preparedness. More recently, however, the definition of critical infrastructure has broadened as a company does not need to be critical infrastructure to experience a cyber-attack that has broad national consequences. The challenge of categorizing companies or certain industries as potential targets is that the remaining sub-set of firms – not included in the so called "danger zone" – can themselves impact critical infrastructure. For example, a manufacturer outside of the oil and gas industry may think that they do not need a robust cybersecurity defense strategy because they believe they will not be a tempting cyber-attack target. However, botnet army attacks have proven that even non-critical assets can be used to then target other critical assets for financial or geopolitical reasons.

Another issue is that different industries may have different approaches to cybersecurity, and that leads into potential threat scenarios. As an example, the life sciences industry has always considered the integration of identity stores to enable single sign on, but without proper implementation the required trust across multiple Active Directory deployments can cause a cascade failure eventually reaching industrial control systems as a side effect.

OT teams should always have defenses in place that match the risk profile assessed by the asset owner. Ultimately, that means teams must take steps to identify the risk level. Risk assessments should be performed in collaboration with industry experts and the defenses should be designed to lower the initially identified risk during the assessment to an acceptable level based on the asset owner's business strategy. Such assessments are critical for OT assets, regardless of the industry, geographic location, systems used, partnerships in place, etc.

While the list of cybersecurity risks to OT systems grows with each passing day, there are many common concerns teams can reference when assessing risk profile. Some of them are as follows:

- **Malware Infection:** A common attack which relies on malicious code installation into the target nodes or malicious code injection on running applications. Although industrial control system workstations and servers should not be directly connected to the internet, malware infection is still a possible attack since the viruses can be transmitted on internal networks or through other means such as removable media.
- **Social Engineering:** This is an indirect attack that is targeted to obtain user credentials which then become an entry point to the control systems. The attacker convinces a user to divulge their username/password or open a file containing malware that compromises their workstation – allowing the attacker to gain a foothold on the network. Education of possible social engineering attacks can reduce the threat.
- **The Trusted Insider:** Misuse is a critical (and critically underrated) threat to control systems. Personnel that have been dismissed might still have access to the control system and could use this access to change settings on a live system. Processes and guidelines to immediately and thoroughly revoke access should be in place.
- **Intrusion via Remote Access:** This attack occurs when an intruder has obtained control system user credentials and gains access to the control system using available remote access mechanisms. Strong remote access defenses including two-factor authentication and "jump servers" can mitigate this threat.
- **Denial-of-Service (DoS) Attacks:** There are multiple types of DoS attacks, but the consequence of such attacks is to prevent legitimate users, nodes and services from performing their functions within a control system by reducing their access to any of the available control interfaces. This attack can affect network communications, embedded nodes or even user access to the system. A well-defended system with a reduced attack surface can lower the possible avenues of DoS attacks.
- **Man-in-the-Middle Attacks:** An intruder inserts himself in between a legitimate client and the resources that client is attempting to access. The specific exploit used will change over time if new protocol weaknesses are discovered and left unpatched. A strong patching regimen and utilization of secure protocols can reduce or even eliminate the possibility of this type of attack.

- **ARP Spoofing:** This is a specific type of attack that relies on a first compromise of a system workstation, and then uses the compromised workstation to poison the network ARP table to implement a man in the middle attack. When successfully deployed, ARP spoofing allows the compromised workstation to receive communication packets which were supposed to be delivered to another node in the system.
- **Network Reconnaissance and Cracking Tools:** Active and passive reconnaissance tools give both administrators and attackers information on network configuration and topology. "Cracking" tools take that reconnaissance a step further and decipher network traffic, either on-the-fly or offline.
- **Remote Code Execution:** Remote code execution is when the attacker can arbitrarily run code on a target system without having physical access to the system under attack. The attackers can take advantage of a flaw in a network protocol to cause the program to execute instructions sent through the network protocol. There are several mitigations to this type of attack including but not limited to data execution prevention and application whitelisting.
- **Impersonation Attempts and Elevation of Privileges:** This attack happens when the attacker can already run code on a target, and using an exploit, the attacker can get the code to run at a higher level of privilege.

2.3 Emerson's On-ramp to the Zero Trust Journey

Zero trust is not meant to be the ultimate, single solution for all cybersecurity issues, but the zero trust principles – if followed correctly – can provide a strong defense against ever-evolving cyber-threats. Emerson continues to evaluate options for zero trust conceptual applications into DeltaV systems, especially with concepts that support the secure-by-design approach.

There are some steps in the zero trust maturity journey that can be implemented on DeltaV systems today. Emerson does not encourage users to deploy unvetted technologies on DeltaV systems, but this recommendation does not mean that asset owners are locked into doing nothing. Instead, Emerson highly recommends organizations define a long-term goal for DeltaV system cybersecurity so they can start the zero trust journey today. Even if the first steps towards the optimal goal are small and simple, as personnel's maturity increases, new solutions from Emerson will become available in parallel.

Throughout the path for zero trust, do not forget these important concepts:

- **Continuous Monitoring and Validation:** Emphasize the importance of continuous monitoring and validation of user identities, device health, and data flows. This ensures that trust is never assumed and is always verified.
- **Least Privilege Approach:** Highlight the necessity of implementing the least privilege principle. Users and devices should only have the minimum access necessary to perform their functions.
- **User Experience:** Consider the end-user experience. While security is paramount, it should not overly hinder productivity. Strive for a balance between robust security measures and a seamless user experience. However, keep in mind that usually security and convenience do not go together.
- **Scalability and Flexibility:** Discuss the need for a scalable and flexible architecture that can adapt to evolving threats and organizational changes. Zero trust should be able to grow and change with the organization.
- **Stakeholder Engagement:** Stress the importance of engaging various stakeholders within the organization. A successful application of zero trust principles requires input and cooperation from all stakeholders such as IT, OT, security teams, business units, etc.
- **Compliance and Regulatory Considerations:** Address how zero trust can help meet compliance and regulatory requirements. This can be a significant driver for adoption in industries with stringent data protection laws.
- **Education and Training:** Highlight the need for ongoing education and training for employees. A well-informed workforce is crucial for the effective implementation of zero trust principles.

- **Future Proofing:** Consider future proofing a zero trust architecture by staying informed about emerging technologies and threats. This proactive approach ensures that security measures remain effective over time.

3. The Zero Trust Journey

3.1 Zero Trust Maturity Journey

US CISA's Zero Trust Maturity Model publication (April 2023) entertains the concept of a zero trust maturity journey which is comprised of four steps: traditional, initial, advanced and optimal.

- **Traditional:** Asset owners should assess their current cybersecurity posture to help determine the next steps towards a zero trust concept adoption. Traditional is the starting point of the journey.
- **Initial:** Zero trust is a journey, and asset owners will not be successful if they all aim for perfection overnight. The initial step is to start moving towards the zero trust concept adoption goal while celebrating early wins. Once achieved, the lessons learned to get to this step may not clearly indicate how far one is from completing the full journey, but it should help set the direction for the upcoming steps that are yet to be completed, while making sure the organization is not deviating from the initial plan.
- **Advanced:** This step may be considered the half-way point through the zero trust adoption journey, and more importantly it serves as another opportunity to celebrate additional successes, certify the direction is still aligned with long-term goals, and update plans accordingly. A complete zero trust journey achievement might not be realistic as the threat landscape is an ever-evolving problem, so the advanced step may eventually become the standing zone with several increments into it. It should be just fine to stay in the advanced step as long as there is noticeable progress being made throughout the journey.
- **Optimal:** This is the step few (if any) asset owners may get to as most will remain in the continuous improvement phases of the advanced step. This is not to say that this step is useless, and to the contrary, the optimal step should serve as the guiding principle for the whole journey. It is possible the optimal step may evolve/change over time, and it may be always far-reaching, but it cannot be dismissed.

3.1.1 Maturity Model Pillars

Per US CISA's zero trust maturity model there are five pillars of reference to be considered as part of the zero trust concept: identity, device, network / environment, application & workloads, and data (Figure 4).

- **Identity:** Refers to an attribute or set of attributes that uniquely describe a system user including non-person entities within the system.
- **Device:** Refers to any asset (including its hardware, software, firmware, etc.) that can connect to a network, including servers, workstations, embedded devices, network devices, and more.
- **Network / Environment:** Refers to an open communications medium including typical channels such as system networks as well as other potential channels such as application-level channels used to transport messages.
- **Applications & Workloads:** Includes systems, computer programs, and services that execute on-premises, on mobile devices, and in cloud environments.
- **Data:** includes all structured and unstructured files and fragments that reside or have resided in specific systems, devices, networks, applications, databases, infrastructure, and backups (including on-premises and virtual environments) as well as the associated metadata.

The base of the five pillars is comprised of three key concepts which are considered part of the actions that help with the zero trust maturity journey: visibility and analytics, automation and orchestration, and governance.

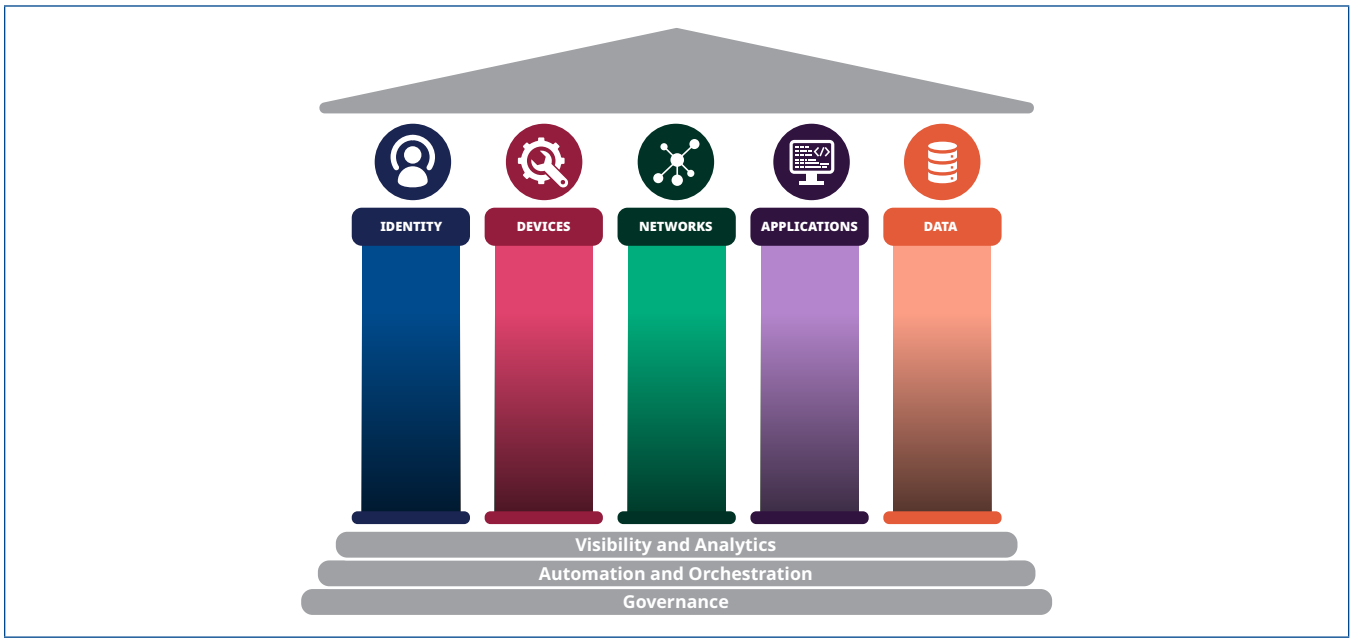

Figure 4: *CISA's Zero Trust Maturity Model Pillars.*

3.1.2 Maturity Model Pillars Reflecting The OT Reality

The steps within the zero trust maturity journey apply to all five maturity model pillars, with unique features to be realized as asset owners navigate the journey. The US CISA publication provides an overview of zero trust application more focused on IT systems than on OT. Below is an adaptation of the steps (by maturity model pillar) focused on an OT environment.

For the OT asset owner and OT system vendor responsibilities, please consider: (R) responsible, (A) accountable, (C) consulted and (I) informed.

	Traditional	Initial	Advanced	Optimal	OT Asset Owner	OT System Vendor
IDENTITY	Credentials	Credentials and proper privilege management	Multi-Factor Authentication (MFA)	Fully enforced Multi-Factor Authentication (MFA)	R, A	C, I
	Identity stores per OT system	Identity stores managed per OT system	Centrally managed identity stores for OT systems	Integrated OT identity stores (no integration to Enterprise)	R, A	C, I
	No risk assessments	Limited identity risk assessment	OT-wide risk assessment	Continuous validation and risk analysis	R, A	C, I
	Permanent access with periodic reviews	Access expires with periodic reviews	Access expires with policy enforcement and periodic reviews	Session-based access	R, A	C, I

	Traditional	Initial	Advanced	Optimal	OT Asset Owner	OT System Vendor
DEVICES	Manually track OT asset inventory	Manually track OT asset inventory (on-prem database)	Automated OT asset inventory (on-prem database)	Automated OT asset inventory (offsite central database)	R, A	I
	Limited compliance visibility	Limited compliance visibility	Enforced compliance	Supply chain risk management	R, A	I
	No threat monitoring	Periodic assessments to manually detect threats	Automatic threat detection (passive monitoring)	Integrated threat detection including host agents	R, A	C, I
	No device criteria for resource access	Limited device-based access control	Initial resource access depends on device posture	Device authentication with real-time device risk analysis	I	R, A

	Traditional	Initial	Advanced	Optimal	OT Asset Owner	OT System Vendor
NETWORK / ENVIRONMENT	Large perimeter Macro-segmentation	Initial segmentation based on system functions	Expanded segmentation with well-defined security mechanisms	Expanded segmentation with well-defined and fully enforced security mechanisms	R, A	C, I
	Limited resiliency	Initial plans for resiliency with manual periodic reviews	Improved resiliency with manual periodic reviews	Adaptable resiliency with automatic enforcement	R, A	C, I
	No network configuration	Static network configuration	Dynamic network configuration	Adaptable network configuration	R	A, C, I
	Minimal traffic encryption with ad-hoc key management	Choice of secure protocols that allow for digital signing and optional encryption and formalized key management policies	Enforced communication digital signing (encryption for cross-boundary links) with key management	Enforced communication digital signing (encryption for cross-boundary links) with key management and integrated threat prevention	C, I	R, A

	Traditional	Initial	Advanced	Optimal	OT Asset Owner	OT System Vendor
APPLICATIONS AND WORKLOADS	Permit non-critical application access via private networks	Permit non-critical application access via private networks using credential with local authentication	Permit non-critical application access via private networks using Multi-Factor Authentication (MFA) with local trust store	Permit non-critical application access via private networks using fully enforced Multi-Factor Authentication (MFA) with local trust store	R, A	C, I
	Minimal workflow integration into protection	Formal code deployment mechanisms through CI/CD pipelines	Protections integrated in all application workflows with context-based access controls	Protection against sophisticated attacks in all workflows	I	R, A
	Ad-hoc development, testing, and production environments	Static and dynamic security testing prior to deployment	Coordinated teams for development, security and operations	Immutable workloads with security testing integrated throughout lifecycle	I	R, A

	Traditional	Initial	Advanced	Optimal	OT Asset Owner	OT System Vendor
DATA	Manual inventory of data	Limited automation to inventory data	Automate data inventory with tracking	Continuous data inventory	R, A	C, I
	Manual categorization of data	Preliminary/ Basic strategy for data categorization	Consistent, tiered, targeted data categorization and labeling	Automated data categorization and labeling	C, I	R, A
	On-prem data stores	Some highly available data stores	Redundant, highly available data stores	Optimized data availability	R, A	C, I
	No Data Loss Prevention (DLP)	No Data Loss Prevention (DLP)	Static Data Loss Prevention (DLP)	Data Loss Prevention (DLP) exfil blocking	I	R, A
	Static access controls	Limited automation to access controls	Automated context-based access	Dynamic access controls	I	R, A
	Minimal encryption of data at rest and in-transit with ad-hoc key management	Encrypt data in-transit Initial centralized key management policy for users to manage	Encrypt data at-rest	Encrypt data in-use	A, C, I	R

3.2 Zero Trust Architecture Components

The list of components presented in this section is not to be considered all-inclusive but rather an effort to cover what is presented in the NIST SP 800-207 zero trust architecture and Microsoft Evolving Zero Trust publications. Since zero trust is a concept and journey, new components may be added to the list later, while others may be depreciated and/or removed over time.

- **Policy Engine:** This component is responsible for the decision to grant access to a resource within the infrastructure. The decision will rely on several of the other components listed below and may also require manual authorization if that is an option system administrators want to implement.
- **Policy Administrator:** This component (not a person, but rather an application/service) is responsible for enforcing the access permissions granted by the Policy Engine. Zero trust starts with the approach of never trusting anything until authorization and permissions are granted based on the authentication of the given resource within the infrastructure.
- **Policy Enforcement Point:** This component is responsible for enabling, monitoring, and eventually terminating connections granted by the Policy Engine. This logical component can be broken into two components, the client (agent running on endpoints), and a gateway or proxy that would manage the interaction between resources when the endpoints are not able to run agents on them.
- **Continuous Diagnostic and Mitigation System:** This component is responsible for the cybersecurity status of all assets within the zero trust environment. It can check for software updates, validates the integrity of the software running on assets (based on the policy engine), performs vulnerability checks on the assets, and checks for any non-approved component(s) within the environment.
- **Industry Compliance System:** In case the asset owner has to abide by an industry-specific regulatory control, this component will serve as the repository for specific policies so it can ensure compliance within the zero trust environment.
- **Threat Intelligence Feed:** This is an important aspect of modern security protections. Threat intelligence provides a common ground for determining what is a known threat that must be blocked within the environment. The threat intelligence concept considers several data sources to determine threat vectors. Ideally, any asset can serve as a feed for threat intelligence as long as it is set to share its information (logs, events, etc.).
- **Network and System Activity Logs:** This component collects logs from various data sources so they can be correlated by the security information and event management (SIEM) solution. Often, this component is a part of a SIEM, or it may be a dedicated component for gathering specific asset information (e.g., a syslog server can be deployed to gather data from network switches and forward the information to a SIEM).
- **Data Access Policies:** These are the rules used by the Policy Engine to grant access to assets and resources within the environment. Policies can be configured/created using the management interface, or they can be dynamically generated by the Policy Engine based on specific guidelines set for the environment.
- **Public Key Infrastructure (PKI):** This is the component responsible for the generation, storage and revocation of digital certificates used by assets, resources, and communications within the zero trust environment. It may include certificates generated externally by a trusted certificate authority or even a segregated PKI that is not using X.509 certificates.
- **Identity Management System:** This is the component responsible for account management for users as well as endpoints. It will integrate with existing directories to authenticate identities and refer to role-based access control for authorization. This component will interface with PKI, for example, and any other resource that provides artifacts related to system accounts.

- **Security Information and Event Management (SIEM) System:** This component is responsible for gathering events and logs from various data sources within the environment. It will correlate the events and logs, store data in raw format, and present processed information in a dashboard with previously configured indicators to facilitate cybersecurity investigation. This component will either perform the function of the network and system activity Log collection, or it will interface with that specific component. It may also receive data feeds from threat monitoring solutions co-deployed in the environment. There may exist a daisy-chain of SIEMs, depending on the segmentation applied to the infrastructure, with the ultimate goal of forming a security operations center.
- **Threat Monitoring Solution:** This component is responsible for generating an online asset inventory with dynamic maps of the communications among all identified assets. From the gathered data, techniques are used to determine patterns for potential anomaly detections, and the threat monitoring solution will interface with other components (such as threat intelligence feeds, the industry compliance system, continuous diagnostic and mitigation system, etc.) to provide advanced reporting, incident response playbooks, and vulnerability management for the assets within the environment.

3.2.1 Zero Trust Architecture for OT

Figure 3 is an adaptation of NIST's Core Zero Trust Logical Components to incorporate the zero trust architecture components listed above with connections between some of them, illustrating how they interact with each other. The core principle is that users and systems are not trusted until they are authenticated, authorized, and have defined policies enforced for how they interact with resources. Resources can be anything, including trusted users and systems. Resources will not be trusted until they are provisioned, authenticated and authorized, and have defined, enforced policies allocated to them.

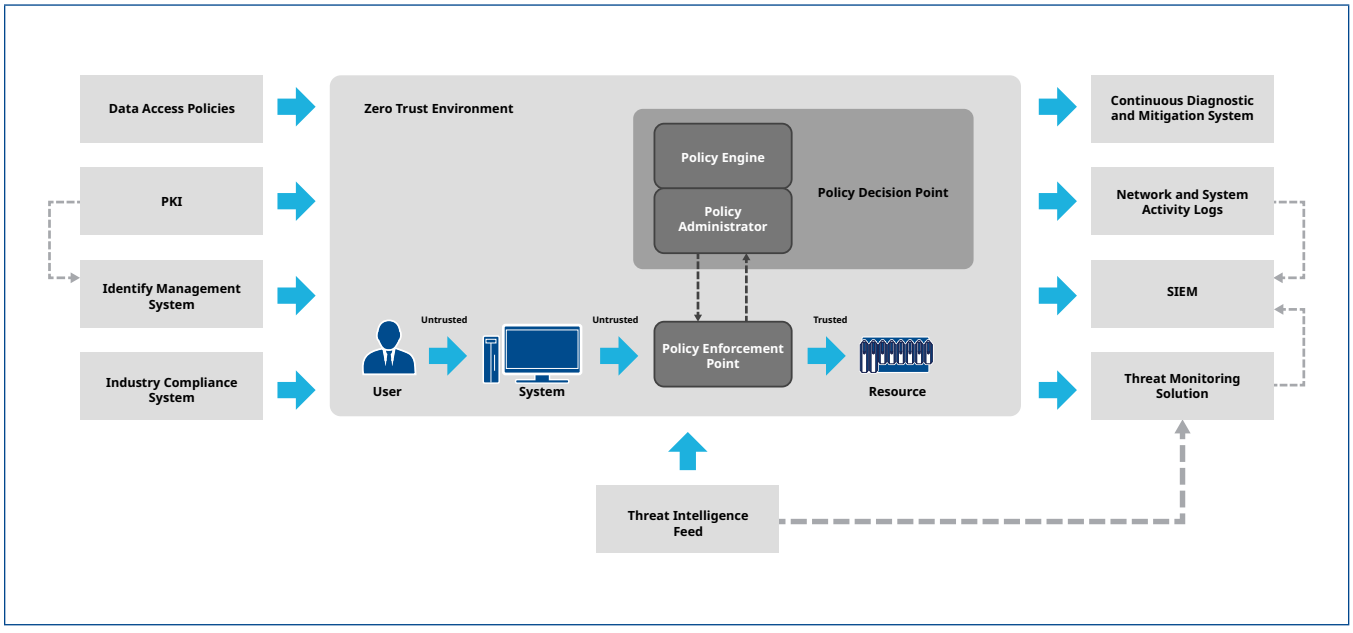

Figure 5: *Adapted NIST's Core Zero Trust Logical Components.*

An important aspect of the zero trust principle is that it does not conflict with other concepts such as defense-in-depth. In fact, the two concepts can be complementary to each other and coexist in the same environment. The key principle is that users, systems and resources must go through provisioning, authentication, authorization, and policy enforcement before they can gain access to anything when applying the zero trust principle to a given environment—even if they are already part of a defense-in-depth strategy.

Figure 6 illustrates what a merger between a DeltaV distributed control system following the defense-in-depth strategy plus the zero trust principle and components might look like, without prescribing what specific software components (part numbers, etc.) would be required. In this abstraction, the Identity Management System and PKI are part of the component listed as independent DeltaV domain controllers which form the local Microsoft Windows Active Directory to allow authentication within the DeltaV environment. Role-based authorization is matched by the DeltaV User Manager application.

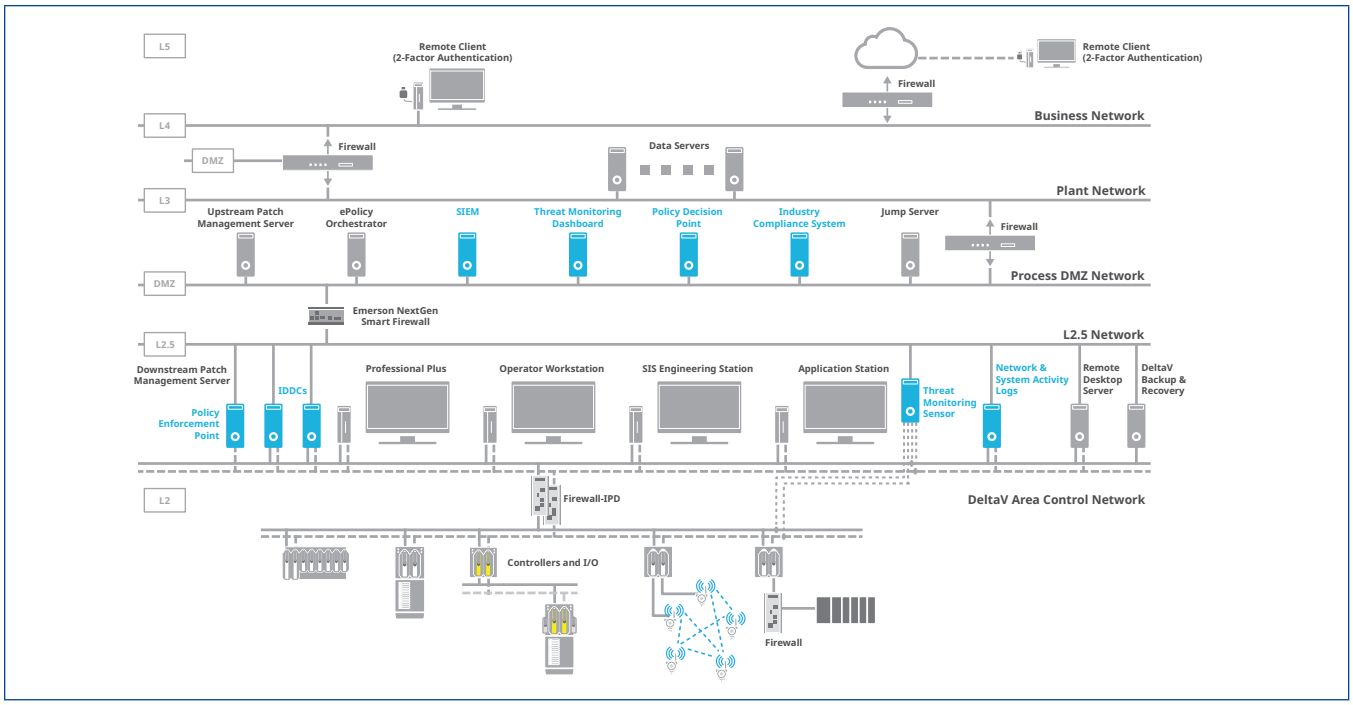

Figure 6: *DeltaV system reference architecture abstraction with defense-in-depth and zero trust components.*

3.3 Potential Threats Associated with Zero Trust Architecture

There is no single solution to address all potential cyber-threats. The threat landscape does not stop to wait for cybersecurity solutions to expand and be augmented, therefore even with an optimum implementation of zero trust today, there may still be some weak links that will need to be addressed and threats will continue to expand. However, in the NIST SP 800-207 publication, there is a section dedicated to threats associated with zero trust architecture which have been ported over to this document with minor adjustments to support the OT context.

- **Subversion of Zero Trust Process:** The zero trust process relies on a properly configured policy engine and administrator. Any administrator (person) with permissions to alter the policy engine or police administrator can intentionally or unintentionally create a threat by allowing untrusted access to resources or weakening the policies. If the policy administrator is compromised, then the protection may grant improper access to resources which otherwise would have been blocked by a properly configured system.
- **Denial-of-Service or Network Disruption:** Zero trust relies on the policy administrator, which grants the permissions to access resources in the environment. If an attack targets the policy enforcement point, the policy engine or the policy administrator with denial-of-service techniques, then the zero trust concept will fail and no access will be granted (zero trust will rely on deny-by-default). With no access to resources, the whole system will be unavailable until the denial-of-service issue is resolved. An option to mitigate this risk is to co-locate the key zero trust components in different network locations (e.g., on-premises and in-the-cloud) or use multiple on-premises options, or even multiple cloud options. Although doable, the mitigation is not a guarantee of success.

- **Stolen Credentials / Insider Threat:** The zero trust principle relies on trust granted upon authentication and authorization. Network location and predicted behavior also play a function in zero trust, so in case a man-in-the-middle attack happens, by exception the connection would still not be authorized based on abnormal behavior. However, social engineering and phishing attacks can still be successful in retrieving credentials, or disgruntled personnel might choose the path of sharing confidential information which may allow attackers to take control of the policy engine and policy administrator to alter or bypass protections altogether.
- **Visibility on the Network:** The combination of network and system activity logs, threat monitoring solutions, SIEM and threat intelligence will provide a comprehensive view of all assets, resources, and communications within the zero trust environment. However, there are always hard-to-reach networks, encrypted communications, or proprietary devices or protocols which require a deeper level of inspection, potentially reducing the broader visibility of the environment. Lower visibility creates blind spots which are vulnerabilities that can be exploited to defeat or downgrade the protection offered by zero trust principles.
- **Storage of System and Network Information:** The same data used for monitoring the environment can be used by the attacker to compromise the protections in place. Usually, the data gathered and transmitted to the SIEM will be stored in a secure vault, inaccessible to users; however, the correlated data displayed by the SIEM is accessible to system administrators which in turn can be compromised if access and/or permissions are hacked. The management tools used to configure the policies within a zero trust environment, if compromised, can serve as a source for reconnaissance.
- **Reliance on Proprietary Data Formats or Solutions:** This threat vector is especially relevant for OT, as industrial control systems are based on proprietary technologies often supported by a single vendor. Relying on a single vendor can be detrimental to zero trust in case a specific vendor has a security issue or disruption. Changing technologies, again especially in OT, tends to be costly so it is rare and often takes decades to happen. Mitigating this risk requires asset owners to assess vendors and technologies used on their environments so that both user and vendor are working in lockstep from a security perspective.
- **Use of Non-Person Entities (NPE) in Zero Trust Administration:** Automation of processes used to manage policies and rules within zero trust environments (which may also include artificial intelligence) can become a threat vector if false positives – or false negatives – trigger wrong actions. Mitigating this risk requires regular tuning of the protective systems. Machine-based administration may also receive a lower rating for access based on implicit protective measures (e.g., users may be required to use two-factor authentication, but AI-powered automation may use credentials only) and attackers may take advantage of that to gain access to the policy engine, or even trick the system to grant elevate access to the wrong components to enable a compromise.
- **AI vs Zero Trust:** The era of generative AI brings many opportunities to organizations, from boosting productivity to new AI-driven applications and more. But along with tremendous value, AI also brings new data risks. Data security is the foundation for secure AI adoption; hence, zero trust data challenges and data security are core competencies of implementing generative AI for ICS and OT. Some of today's top data challenges are:
  - **Data Oversharing:** Users may gain access to sensitive data via AI apps that they are not authorized to view or edit due to lack of labeling policies or access controls.
  - **Data Leakage:** Users may inadvertently leak sensitive data to unsanctioned AI apps, or by using sanctioned AI apps if the organization hasn't ensured the AI-generated responses inherit the data protection controls of the files referenced.
  - **Noncompliant Usage:** Users may generate high-risk content or content that doesn't abide by ethics standards with AI apps, such as documents created to hide insider trading, money laundering, or other illegal activities.

3.4 Partnership Ecosystem

As described in the DeltaV Security Manual, Emerson follows the defense-in-depth strategy to defend DeltaV systems. Figure 5 illustrates currently available solutions and providers that work with Emerson to offer solutions to DeltaV systems users. Solutions highlighted in blue are either self-developed by Emerson or have a strong partnership between the solution provider and Emerson, with OEM agreements in place to manage the lifecycle of the offerings. Solutions highlighted in green are solutions delivered by solution providers where there are not necessarily partnership agreements in place. Both solution sets, blue or green, are offered by Emerson for DeltaV systems as a standard solution offering or as an engineered solution. The list of partners that currently form this cybersecurity ecosystem for DeltaV systems is presented below for reference:

- **Trellix:** Formerly McAfee Enterprise, Trellix has been a partner of Emerson for DeltaV systems since 2015 and the current DeltaV-tailored solutions powered by Trellix are DeltaV Endpoint Security, DeltaV Application Allow-Listing, DeltaV SIEM and DeltaV Network Security Monitor.
- **Belden:** Over 15 years of solid relationship Emerson and Belden (initially Hirschmann) have been working together to release Belden products as Emerson brand-labeled solutions for DeltaV systems. These products include Emerson NextGen Smart Firewall, DeltaV Firewall-IPD, and DeltaV NextGen Smart Switches. The Tofino firewall is offered as a buy-out to be used as an industrial networks firewall.
- **Acronis:** Another long-term relationship, Acronis and Emerson offer the DeltaV Backup & Recovery product for DeltaV systems. Currently, this is the only fully vetted backup solution for DeltaV systems from Emerson.
- **OPSWAT:** Emerson and OPSWAT have been working together for at least 6 years, and the relationship started based on the need for removable media scanning. OPSWAT is currently an Emerson Alliance Member, and additional products were added to the list for DeltaV use cases such as OPSWAT's data diode technology for DeltaV Edge.
- **Thales:** DeltaV systems can be implemented with two-factor authentication using smart cards. The underlying solution to make this happen (card readers, smart cards, and drivers) in most cases has been provided by Thales (formerly Gemalto or SafeNet).
- **Safran & Microchip:** Time synchronization is an important part of many electronic systems including cybersecurity, therefore DeltaV systems can be connected to GPS time servers from many manufacturers. The two providers Emerson has worked with over the years are Safran (formerly Orolia / Spectracom) and Microchip (formerly Microsemi / Symmetricon).
- **Dragos & Nozomi Networks:** The relationship with Dragos and Nozomi Networks to address the threat monitoring solutions for DeltaV systems started in November 2021. Threat Monitoring Solutions for DeltaV systems was officially released in July 2022. A lot of work has been done by Dragos, Nozomi and Emerson, to make these partnerships very successful. Although categorized as buy-outs, Threat Monitoring Solutions are supported by Emerson's Cybersecurity Group if designed, implemented and operationalized by Emerson.
- **ConsoleWorks, BeyondTrust & CyberArk:** In 2023/2024, Emerson's Cybersecurity Group investigated layered and non-intrusive solutions to enhance the secure remote access options for DeltaV systems. ConsoleWorks, BeyondTrust and CyberArk have all been investigated so Emerson can provide them as engineered solutions for DeltaV systems upon request.

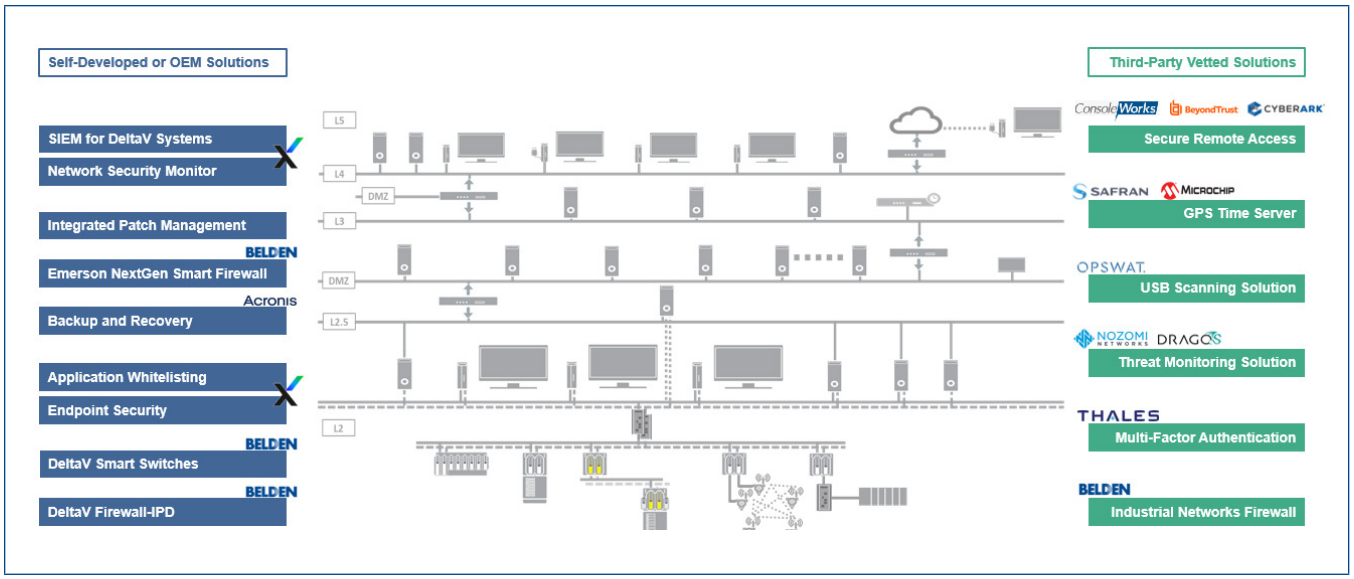

Figure 7: *Bolt-on cybersecurity solutions for DeltaV systems.*

Existing partnerships allow Emerson to continue expanding on the protections offered for DeltaV systems, and it is clear that additional partners and solutions will need to be added to the DeltaV ecosystem so the zero trust principle can be followed to its full extent. There are system features (such as secure communications) which will be provided by Emerson as future versions of DeltaV software are released, but layered capabilities that are needed to meet zero trust requirements are not yet clearly defined for DeltaV systems.

This document has been created in collaboration between Emerson and solution providers who are either providing solutions to address specific zero trust techniques, or that are leading the way by following zero trust principles within their organizations or supporting the ones who are doing the same, including:

- **Microsoft:** DeltaV software runs on top of Windows operating systems and some security features available for Windows are already embedded (or can be enabled) within DeltaV workstations and servers. Zero trust is a key initiative for Microsoft, and several components are already available for teams to use while investigating options to pursue their zero trust maturity journey.
- **Intel:** As an enabler of secure architectures, Intel provides microprocessors that run on several devices. DeltaV workstations and servers are powered by Dell and run Intel CPUs.

3.5 Optimal Maturity Level Objectives for OT

By considering what cybersecurity solutions are currently available for DeltaV systems and evaluating concepts under investigation for future releases of DeltaV software, it is possible to abstract an optimal state for zero trust maturity pillars in DeltaV systems at a high level.

- **Identity:** DeltaV system users shall authenticate using a fully enforced multi-factor authentication system that currently would rely on smart cards, but in the future could use other technologies such as electronic wristbands, biometrics, and more. DeltaV system identity stores will be integrated to a manufacturing layer consolidated identity store for OT, but not tied to the enterprise – automation and enterprise trust stores will interface with each other without integration. DeltaV systems will be assessed for vulnerabilities and risks continuously, taking advantage of automated processes. Access to any resource within a DeltaV system will be session-based with embedded policy enforcement continuously monitored.
- **Device:** Currently DeltaV system assets can be retrieved from Guardian Support Portal via asynchronous updates of the DeltaV System Registration. Following zero trust principles, DeltaV system assets will be gathered automatically, and records will be saved in an offsite central database for easier and more resilient access. With a complete asset inventory and software bill of material, the asset owner can run constant supply chain risk assessments to prevent unintentional issues from impacting the overall protection structure. DeltaV systems will be monitored for anomalies and threats with integrated threat detection including host agents for complete visibility of processes, services, and software running in each device. DeltaV system devices (not only stations) will be authenticated before they can access resources within the DeltaV Area Control Network, and there will be a real-time device risk analysis.
- **Network / Environment:** The DeltaV Area Control Network and surrounding networks will need to go through an in-depth review to allow for expanded segmentation with well-defined and fully enforced security mechanisms. Solutions may include the use of logical segmentation provided the implementation has embedded monitoring to identify compromises before they get escalated. Redundant networks will continue to be relevant, but the resiliency model will likely need to be adaptable with automatic enforcement. Adaptability of the networks will also apply to how the network components, logical connections, and resource access interact with one another. DeltaV system communications between any asset, resource or component will be digitally signed for proper authentication, and optionally encrypted according to user needs. Encryption will apply for cross-boundary links, and digital certificates will be managed from a PKI dedicated to OT.
- **Applications & Workloads:** Non-critical application access is permitted within the DeltaV Area Control Network if users authenticate using multi-factor authentication validated against local trust stores. Threat Intelligence comes into play to determine malicious activities continuously, and therefore protection against sophisticated attacks can be applied to all DeltaV system workflows. Development of DeltaV software relies on immutable workloads with security testing integrated throughout the DeltaV software lifecycle to add peace-of-mind for asset owners.
- **Data:** Data available within the DeltaV system boundaries, incoming or generated by the system, will be continuously monitored and stored for forensics. Data is categorized and labelled automatically by the system, so it is easier to measure the criticality of a compromise. Data is more easily accessible—provided the user requesting access has permissions—and any data traversing the DeltaV system boundaries (inside-out) will go through data loss prevention techniques for proper sanitization. Access to data is dynamically controlled and encryption is applied for data in-use (more relevant than in-transit or at-rest).

Expanding on the secure communications applicability to DeltaV systems, which is paramount to allow Emerson to evolve DeltaV systems in the zero trust maturity journey, it is necessary to explain that currently (up to version 15 of DeltaV software) DeltaV nodes are not authenticated, proprietary DeltaV communications are not signed nor encrypted, a trust store is mainly used for DeltaV user authentication, and PKI is primarily serving two-factor authentication needs. In future releases of DeltaV software, the idea is to expand on these security protections by:

1. Enabling node authentication and performing firmware validation at the endpoint level.
2. Implementing DeltaV Area Control Network communications digital signing.
3. Allowing for optional communication encryption.

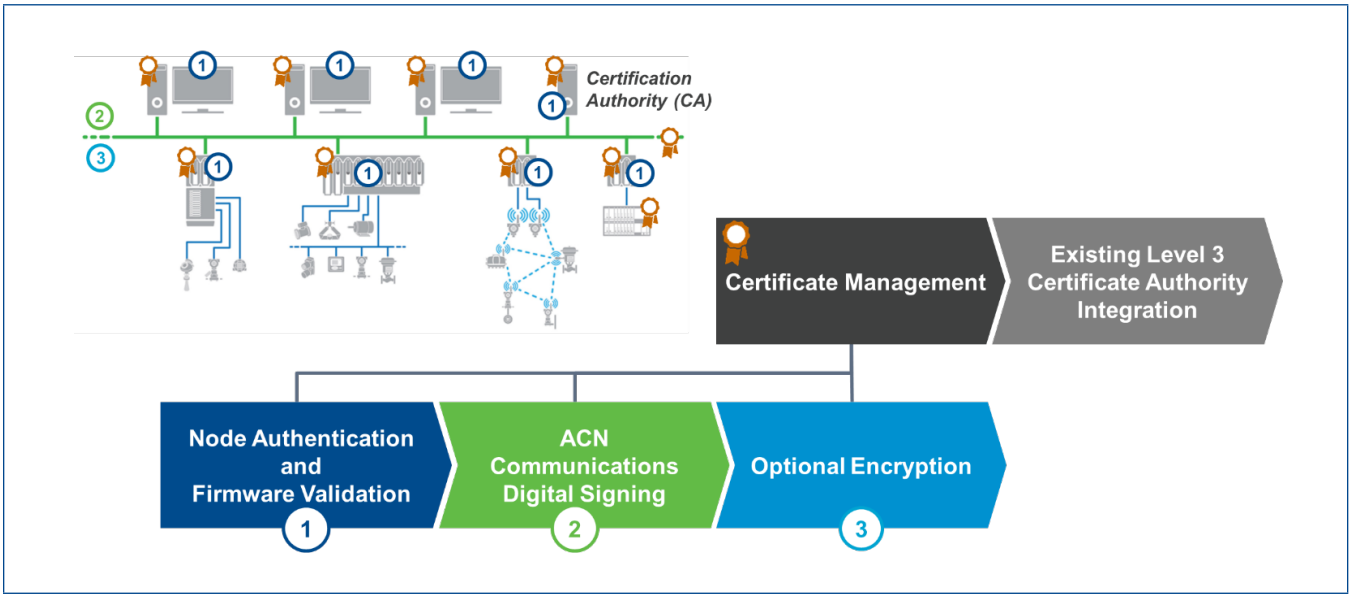

Figure 8: *Certificate management ensures ease of use.*

Emerson's support policy for DeltaV systems is based on a closed ecosystem formed by Emerson technology and approved vendor solutions which are either embedded or layered on top of DeltaV systems. Organizations have the option to acquire the approved layered solutions that they choose, while knowing that only the specific options made available by Emerson for DeltaV systems can be supported by Emerson.

There are two types of cybersecurity solutions offered by Emerson for DeltaV systems:

- Self-Developed or OEM solutions
- Third-Party solutions

Self-Developed or OEM solutions are sold, provisioned, maintained and supported by Emerson as the single point of contact. Independent of the root cause of an issue, anything impacting Emerson homegrown or OEM solutions will be addressed by Emerson. Documentation is included with support, and updates, patches, and hotfixes are all part of the support structure as well as lifecycle management for these components.

Third-party solutions are vetted by Emerson for use with DeltaV systems, and, in this case, there is a strong collaboration between the selected third-party vendors and Emerson through an official partnership. Emerson may generate documentation pertaining to DeltaV component changes or configuration options, while the support for third-party components continues to be the vendor's responsibility.

If teams choose to use unvetted technologies on DeltaV systems, support limitations apply. Emerson is not required to support unvetted technologies on DeltaV systems. This includes solutions that may seem benign, but that have not been validated by Emerson, and could potentially cause harm to the essential functions of a control system—in this case a DeltaV system.

Even without support or guarantees that unvetted solutions will work with DeltaV systems, some teams may choose to use them based on their own corporate policies. Emerson may agree to perform solution validation as an engineered solution option, which offers no guarantee for a successful implementation. In these cases, Emerson cannot commit to make DeltaV product changes in case of incompatibility issues with the unvetted technologies, any test results are of confidential knowledge to the engaged organization, and the test validity applies to the specific architecture considered for the test—including the software versions tested—and therefore might need to be repeated every time there is a significant variance of the environment considered for testing.

4. Final Considerations

Zero trust is a broad concept and not a specific application or software. While it is not a single solution to every cybersecurity scenario, the zero trust principles – if followed correctly – can provide a strong defense against the ever-evolving cyber-threats. Emerson continues to evaluate options for incorporating zero trust conceptual applications into DeltaV systems, especially with concepts that support the secure-by-design approach, and there are some steps in the zero trust maturity journey that can be implemented on DeltaV systems today.

Emerson does not encourage users to deploy unvetted technologies on DeltaV systems, but this recommendation should not mean that asset owners are unable to proceed on their zero trust maturity journey. Instead, Emerson highly recommends organizations define a long-term goal for DeltaV system cybersecurity so they can start this journey today. Even if the first steps towards the optimal goal are small and simple, as personnel's maturity increases, new solutions from Emerson will become available in parallel. Throughout the path for zero trust, do not forget these important concepts:

- **Continuous Monitoring and Validation:** Emphasize the importance of continuous monitoring and validation of user identities, device health, and data flows. This ensures that trust is never assumed and is always verified.
- **Least Privilege Principle:** Highlight the necessity of implementing the least privilege principle. Users and devices should only have the minimum access necessary to perform their functions.
- **User Experience:** Consider the end-user experience. While security is paramount, it should not overly hinder productivity. Strive for a balance between robust security measures and a seamless user experience. Just keep in mind that usually security and convenience do not go together.
- **Scalability and Flexibility:** Discuss the need for a scalable and flexible architecture that can adapt to evolving threats and organizational changes. Zero trust should be able to grow and change with the organization.
- **Stakeholder Engagement:** Stress the importance of engaging various stakeholders within the organization. A successful application of zero trust principles requires input and cooperation from all stakeholders such as IT, OT, security teams, business units, etc.
- **Compliance and Regulatory Considerations:** Address how zero trust can help meet compliance and regulatory requirements. This can be a significant driver for adoption in industries with stringent data protection laws.
- **Education and Training:** Highlight the need for ongoing education and training for employees. A well-informed workforce is crucial for the effective implementation of zero trust principles.
- **Future Proofing:** Consider future proofing your zero trust architecture by staying informed about emerging technologies and threats. This proactive approach ensures that security measures remain effective over time.

Contact Us
www.emerson.com/contactus