Carnegie Mellon University
Software Engineering Institute

KEY TAKEAWAYS FROM ZERO TRUST INDUSTRY DAY 2024

Patsy Bulisco

April 2025

DOI: 10.1184/R1/27234240

Introduction/Overview

In May 2024, Zero Trust Industry Day 2024 brought together vendors and partners to create a dialogue, propose solutions, and brainstorm ideas for implementing zero trust practices in an environment composed of information technology (IT) and operational technology (OT) systems [SEI 2024a]. The concept of *zero trust* is a cybersecurity framework that operates on the principle of "never trust, always verify." As organizations face growing threats from cyberattacks, this cybersecurity approach is increasingly relevant in both IT and OT environments.

Successfully implementing zero trust in IT and OT environments requires careful planning, collaboration among stakeholders, and a focus on aligning security measures with operational needs. Organizations must navigate these challenges while ensuring the integrity and availability of critical systems. Effective communication, continuous training, and a phased approach can help facilitate this transition.

The SEI zero trust event focused on the challenges of implementing zero trust in the context of a chip manufacturing company with IT, OT, Internet of Things (IoT) systems, and a 24/7/365 operation. The scenario's company, Secluded Semiconductors Inc., comprising a mainland headquarters and remote island manufacturing facility, set the stage for myriad discussions at the event.[1]

This paper describes the following key takeaways from Zero Trust Industry Day 2024:

- differences between IT and OT environments
- importance of stakeholder collaboration
- roadmap for implementing zero trust
- measuring success
- key challenges

[1] Rhonda Brown, Senior Solutions Engineer at the Software Engineering Institute, described the event's scenario in a white paper [Brown 2024]. To spark discussion, multiple experts presented at the event. To see their presentations, refer to the SEI Zero Trust Industry Days 2024 collection [SEI 2024d].

Differences Between IT and OT Environments

While both IT and OT environments share the overarching goal of protecting the organization's assets, their priorities differ significantly, which leads to potential conflicts in their security strategies. Effectively implementing zero trust in these environments requires understanding their different goals and the importance of stakeholder collaboration.

In IT, security teams tend to focus on traditional cybersecurity measures, protecting sensitive data from unauthorized access, and adhering to regulations and standards. These regulations and standards include, but are not limited to, the General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA), and Payment Card Industry Data Security Standard (PCI DSS). Conversely, OT security teams largely focus on the safety and reliability of industrial systems, often using different tools and practices.

In a traditional OT environment, operational safety is extremely critical. Organizations must conform to guidance and standards set by the Occupational Safety and Health Administration (OSHA). Many organizations use the *CIA triad* to develop security systems or evaluate organizational security. The letters in the triad refer to confidentiality, integrity, and availability and are often thought of in reverse order, AIC, since availability (i.e., system uptime) is the most important focus in an OT environment. This focus is different from IT environments, where the confidentiality and integrity of data usually take precedence over availability. It's important to understand these differences, especially when planning to connect OT to an IT infrastructure.

Systems must be designed so that OT hardware can be quickly and safely disconnected when an outage or compromise might affect the security and/or uptime of the OT environment. When designing a security strategy that covers both IT and OT environments, a plan acknowledging their differences and establishing communication between the IT and OT security teams is vital to success.

Importance of Stakeholder Collaboration

Implementing zero trust in an integrated IT and OT environment requires collaboration among various stakeholders. Effective communication and collaboration among management, IT/OT security teams, and operational staff are essential for developing a cohesive zero trust strategy that addresses the unique needs of both IT and OT environments. Management must ensure that security initiatives align with business objectives, while security teams must collaborate to ensure that solutions meet the needs of IT and OT. The operational staff can also provide insight into the daily operational realities and requirements of OT systems.

Establishing a cross-functional team can make it easier to share insights, foster a common understanding, and reconcile differing priorities between IT and OT. This team can identify the specific needs of the IT and OT organizations and build a roadmap for a security ecosystem that

addresses the seven tenets of zero trust without burdening operational users or the security teams tasked to deploy and monitor the ecosystem [Rose 2020].

Roadmap for Implementing Zero Trust

Currently, there is no security vendor that can provide a comprehensive zero trust solution for IT and OT environments. Effective collaboration is critical to building a clear roadmap for zero trust implementation with solutions that are targeted, feasible, and cost effective.

A zero trust architecture should be designed and deployed with zero trust tenets that address users, devices, applications and workloads, data, and networks. It can be designed and deployed using visibility and analytics, automation and orchestration, and governance. Organizations that want to build a zero trust architecture will find it easier to manage their implementation plan and progress by using the steps below to create a roadmap that describes what zero trust looks like for their specific needs:

1. **Understand your organization** by completing an asset inventory and comprehensive security assessment of both IT and OT environments. Identify assets as well as potential vulnerabilities, threats, and gaps in current policies and technologies. This involves engaging stakeholders including managers, IT/OT security teams, and operational staff to understand their priorities, concerns, and expectations.

2. **Establish clear and concise security policies** that encompass both IT and OT systems. These policies should not only outline access controls, authentication requirements, and monitoring protocols but should also reflect the operational realities and risks associated with OT systems.

3. **Implement robust identity and access management (IAM) solutions** that ensure granular access controls and reply on continuous verification of users and devices. Use role-based access to limit user permissions based on users' specific functions; this access should incorporate multi-factor authentication (MFA) to enhance security.

4. **Establish continuous monitoring systems** that can detect anomalous behavior in both IT and OT environments. Use security information and event management (SIEM) tools that aggregate and analyze data from various sources to detect threats in real time. A security orchestration, automation, and response (SOAR) platform can also be combined with a SIEM tool; this approach helps integrate and automate security operations by reducing the effort required to detect, prioritize, and remediate threats.

5. **Utilize network segmentation** to create isolated environments for different systems and applications. Microsegmentation can further enhance security by limiting lateral movement within the network, making it harder for attackers to move between network segments. This can be a critical aspect of protecting an environment.

6. **Develop an incident response plan** tailored for both IT and OT systems. This plan should outline procedures for responding to breaches, including communication protocols, roles and responsibilities, and recovery processes.

7. **Implement employee training programs** across the organization to raise awareness about zero trust principles and security best practices. These training programs should require the organization to regularly update employees about emerging threats and provide ongoing education about the importance of cybersecurity.

8. **Regularly review and update security measures** following a defined process that adapts these measures to evolving threats and changes in technology. Involve stakeholders in the update process to inform these adaptations, ensuring continuous improvement.

Measuring Success

It can be challenging to measure the effectiveness of a zero trust architecture. One of the primary challenges is identifying observable factors that can be tracked, quantified, and analyzed. As organizations transition to a zero trust model, it's essential to

- establish baseline metrics that reflect the organization' current security posture
- continuously measure improvements over time

These metrics include tracking the implementation rate of zero trust capabilities and assessing how these changes influence the organization's overall risk posture. It's necessary for the organization to regularly reassess and adjust these metrics since success may look different as the threat landscape and organization's needs evolve. By maintaining a dynamic approach to measurement, organizations can effectively gauge their path toward a zero trust environment.

Zero trust emphasizes continuous verification and context-based access, which can make it difficult to pinpoint specific metrics. Organizations must look beyond standard indicators (e.g., the number of detected threats or breaches) and focus instead on observable behaviors (e.g., user experience, frequency of MFA prompts for resources, and the context in which access requests occur). Organizations can also create playbooks that model attacker behavior and test that behavior against the organization's environments before and after implementing controls; this approach helps identify whether there have been any improvements.

When measuring zero trust, another significant challenge is the lack of comparable metrics across different vendors. The market is saturated with a variety of zero trust solutions, and each vendor may define and measure key performance indicators (KPIs) differently. This inconsistency can make it difficult to benchmark progress, and organizations may find themselves comparing apples to oranges when evaluating the effectiveness of various solutions. To address this challenge, organizations should establish a set of standardized metrics tailored to their unique environment and objectives, thereby facilitating a more comprehensible assessment of progress.

Key Challenges

Implementing zero trust presents challenges, including the following, especially in environments that encompass both IT and OT:

- Bridging the gap in the mindsets of IT and OT staff helps the organization create a cultural shift and alignment toward common goals.
- Legacy technology, which often lacks modern security features, creates complexity and raises the cost of interconnecting devices and systems.
- Implementing comprehensive monitoring can generate vast amounts of data, which can overwhelm security teams.
- Budget constraints may limit the organization's ability to fully invest in necessary technologies, appropriate personnel, and needed training.

Panel Discussion

During the 2024 Zero Trust Industry Day event, Kris Rush, Technical Director of the Monitoring and Response Directorate at the Software Engineering Institute, led a panel discussion where participants discussed zero trust challenges, including implementation, metrics, mandates and guidance, and OT environments [SEI 2024b]. This section contains the questions that event organizers and attendees submitted and a summary of the discussions the questions generated.

What are some of the greatest challenges that you have faced when helping clients and partners implement zero trust?

This question explores several themes, which we describe below:

- overlooking the cultural dynamic
- focusing on technology before the need
- lack of understanding about zero trust
- having a compliance mindset

Overlooking the Cultural Dynamic. The biggest risks were organizational, not technical, and the first listed challenge was culture. As with any new technology, there are challenges with people, politics, and culture in the organization. The challenge with people involves resistance to change; for example, traditional network and firewall professionals can feel threatened when the organization introduces new network deperimeterization. Political and cultural challenges arise when the organization doesn't acquire the proper institutional buy-in that a change requires. Often, certain key groups or individuals in the organization aren't fully aware of what is transpiring in the organization. Therefore, it's important to involve relevant stakeholders from the start, including executives, supporting functions, operations, DevOps, and compliance functions.

Focusing on Technology Before the Need. For many organizations, *zero trust* is an ambiguous term that has been pushed as a cure-all. The market offers a variety of solutions and promises designed to

help organizations implement zero trust. It's important to focus on education, value, and benefits instead of focusing on zero trust implementations or tools.

Lacking Understanding About Zero Trust. It's important to have the skills and knowledge to recognize how zero trust technology differs from traditional (implicit trust) network security. In many cases, the term *zero trust* is used without defining what it actually means. Vendors at conferences claim to be "zero trust," and they are willing to sell solutions as "zero trust." For this reason, it's important to make the concept of zero trust simple and clear to help users and consumers understand it, including how one solution can differ from another. When examining zero trust solutions, be sure to understand how those solutions address the principles of zero trust and how the solutions benefit your organization.

Having a Compliance Mindset. After breaches or incidents, some organizations become discouraged and frustrated. They expect their compliance department to tell them what to do. Some current regulations, edicts, and mandates are not accompanied by sufficient guidance to demonstrate what good security looks like. As a result, compliance drives the solution set instead of the organization's security mission. When security is the mission, compliance is the outcome.

It's difficult to understand that zero trust may not be applicable in OT environments since OT intersects with IT in most cases. Even if there is an infrastructure that we characterize as OT (e.g., manufacturing, critical infrastructure, healthcare). Is it possible to take advantage of the protections and benefits of zero trust in environments or components of our network that don't at first appear to be a ready fit for zero trust?

The OT environment poses several different challenges when it comes to networking, infrastructure, and the types of traffic and technologies it uses. Some zero trust principles absolutely apply. When segmenting into trust zones, the *Purdue Model for ICS Security* can map to the language of the different zero trust maturity models [PERA 2024]. Trust zones can be organized to minimize potential breaches. There are new challenges that may not have existed 20 years ago, and those challenges can be addressed with the new ideas raised in zero trust initiatives.

There isn't enough pressure on organizations to invest in increasing security for OT systems. Many organizations have been unable to justify the cost of securing these systems effectively. It's easy to justify the costs when traditional system users aren't protected; someone will become upset when a bad event happens. We're seeing a major uptick in those events, including an increase in ransomware attacks against IoT and OT devices. The threat actors are becoming more aware.

It's important to recognize that IT and OT environments operate differently and that some of the initial zero trust guidance comes from an IT perspective rather than an OT perspective. Keeping those differences in mind, the initial guidance still provides massive benefits regarding what zero trust can deliver. As we look to further innovate in industry, it's crucial to enable the convergence between traditional OT technology and the types of capabilities that can be delivered in it and from the cloud.

However, these capabilities should be delivered in a way that doesn't expose increasing risks. There are nuances and differences between IT and OT environments, but those differences do not extend to IT and OT being at odds.

How do we, in a vendor- or solution-agnostic way, agree on some sort of common taxonomy to represent the principles of zero trust and identify areas where we can observe, evaluate, and measure using hard metrics that are comparable across solutions, between vendors, and between networks? How do we use those metrics to determine our progress along the zero trust journey and evaluate the efficiency and effectiveness of the chosen implementation?

It's difficult to apply the same metrics to everyone, because success looks different from each customer base. Metrics that matter to an organization depend on what industry it's in. How much of the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) framework do we successfully use [MITRE 2024]? How much harder is it or longer does it take to execute or disrupt the cyber kill chain or flow?

Developing common metrics requires forums with organizations that represent different industries coming together and articulating the KPIs and metrics that matter most to them. Then, this contributed information must be consolidated across many different industry types to build a set of generic or industry-specific metrics. Ultimately, if a solution does not deliver business value or positively impact operational resilience, then its value to the organization will be questioned.

It's useful to understand what organizations see as success; solution providers can leverage that information to incorporate a measurable and testable view of zero trust deployment at a mature, advanced level.

Metrics should encompass what is important for an organization to understand, present, and update periodically, including answering questions like the following:

- What is my level of protection?
- How much of and what parts of my network(s) have I specifically secured?
- Are my users using these tools?

Future Zero Trust Industry Days

At the 2024 Zero Trust Industry Day event, attendees, presenters, and panel members discussed many important topics related to successfully implementing zero trust in organizations. SEI researchers are exploring new ways to challenge the community and are committed to continuing to build a zero trust body of knowledge to help organizations implement the "never trust, always verify" principle of zero

trust. We invite you to follow our progress on zero trust and look for announcements of upcoming zero trust events by checking out the SEI's Zero Trust Blog series on the SEI website [SEI 2024c].

Bibliography

[Brown 2024]
Brown, Rhonda. *Zero Trust Industry Days 2024 Scenario: Secluded Semiconductors, Inc.* Software Engineering Institute, Carnegie Mellon University. February 2024. https://insights.sei.cmu.edu/library/zero-trust-industry-day-2024-scenario-secluded-semiconductors-inc/

[MITRE 2024]
The MITRE Corporation. ATT&CK. *The MITRE ATT&K Website*. October 23, 2024 [accessed]. https://attack.mitre.org/

[PERA 2024]
Purdue Enterprise Reference Architecture (PERA). *Purdue Model for ICS Security*. November 4, 2024 [accessed]. https://www.pera.net/

[Rose 2020]
Rose, S. & Borchert, O. *Zero Trust Architecture*. NIST SP 800-207. National Institute of Standards and Technology (NIST). 2020. https://doi.org/10.6028/NIST.SP.800-207

[SEI 2024b]
Software Engineering Institute. *Zero Trust Industry Days 2024: Panel Discussion*. May 2024. https://insights.sei.cmu.edu/library/zero-trust-industry-day-2024-panel-discussion/

[SEI 2024c]
Software Engineering Institute. Zero Trust. *SEI Blog.* October 23, 2024 [accessed]. https://insights.sei.cmu.edu/blog/tags/zero-trust/

[SEI 2024a]
Software Engineering Institute. SEI Zero Trust Industry Days 2024. *SEI Website*. March 2024. https://insights.sei.cmu.edu/library/sei-zero-trust-industry-days-2024/

[SEI 2024d]
Software Engineering Institute. SEI Zero Trust Industry Days 2024 [collection]. *SEI Website*. October 23, 2024 [accessed]. https://insights.sei.cmu.edu/library/sei-zero-trust-industry-days-2024-collection/

Legal Markings

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM24-1424

Contact Us

Software Engineering Institute
4500 Fifth Avenue, Pittsburgh, PA 15213-2612

Phone: 412/268.5800 | 888.201.4479
Web: www.sei.cmu.edu
Email: info@sei.cmu.edu