Simplifying Adoption of ISA/IEC 62443 Using the Zero Trust Model for Operational Technology

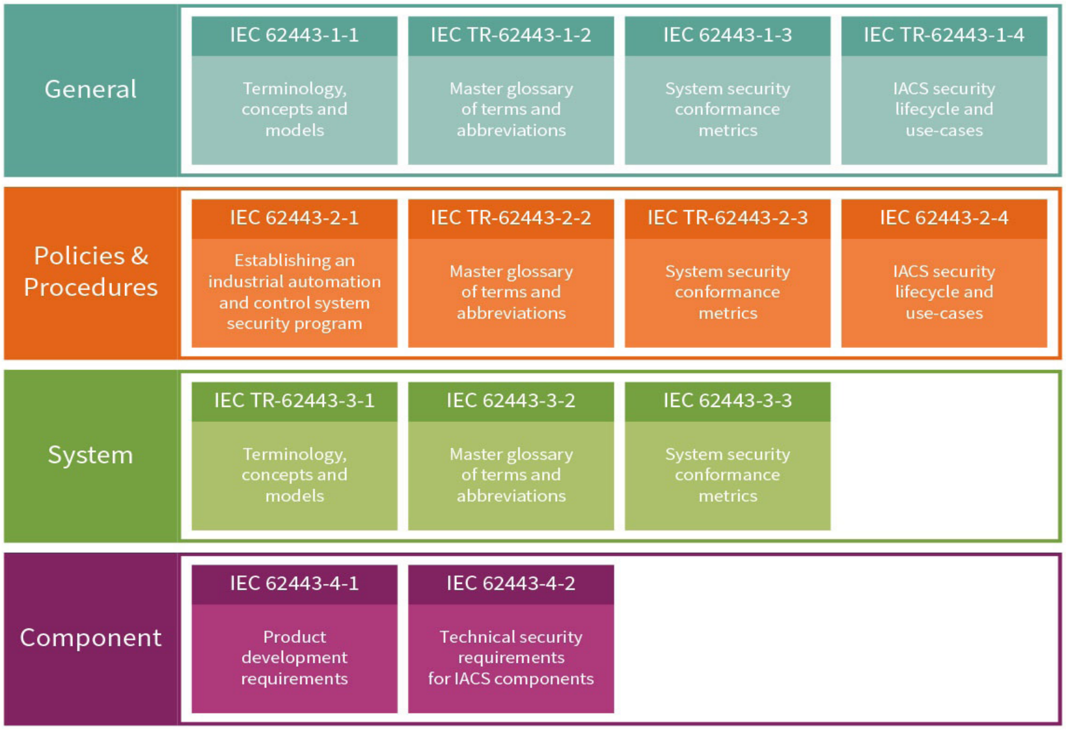
Introduction

According to a study by Ponemon Institute, half of all organizations and companies that depend on operational technology (OT) and industrial control systems (ICS) have suffered a disruption of or impact on OT operations due to a cyber incident, resulting in downtime to plant or operational equipment.[1] Depending on the industry, a cyber event in OT systems that results in disruption or misuse could mean significant damage—physical, financial, environmental, and/or health and safety.

As more IT and OT systems are converged, the opportunity for cyber events to impact production operations grows. Likewise, the expanding attack surface of industrial internet of things (IIoT) devices provides additional opportunities for cyber incidents. However, a shocking number of companies and organizations continue to ignore or vastly underestimate the cybersecurity risk and subsequent business risk. Whether it's manufacturing, oil and gas, electricity, healthcare, or a different OT-dependent industry, more companies should be thinking twice about how to adopt innovative technologies and devices and leverage a security approach as an enabler of safe and secure operations.

To improve secure operations and protect their OT environments, organizations need to adopt a cybersecurity framework designed for OT, such as the ISA/IEC 62443 series of standards (see figure 1). The series provides a flexible framework to address and mitigate current and future security vulnerabilities in industrial automation and control systems (IACSs). Because they can apply to all key industry sectors and critical infrastructure, the ISA/IEC 62443 standards are integral components of the US Cybersecurity Framework.

While the ISA/IEC 62443 standards are more than a thousand pages long, the core cybersecurity principles set forth are straightforward and proven in both IT and OT environments to effectively address cybersecurity risks. This paper focuses on the portion of the ISA/IEC 62443 standards that outlines technical standards for the components used in industrial control systems, including embedded devices, network assets, and software.



General	IEC 62443-1-1 Terminology, concepts and models	IEC TR-62443-1-2 Master glossary of terms and abbreviations	IEC 62443-1-3 System security conformance metrics	IEC TR-62443-1-4 IACS security lifecycle and use-cases
Policies & Procedures	IEC 62443-2-1 Establishing an industrial automation and control system security program	IEC TR-62443-2-2 Master glossary of terms and abbreviations	IEC TR-62443-2-3 System security conformance metrics	IEC 62443-2-4 IACS security lifecycle and use-cases
System	IEC TR-62443-3-1 Terminology, concepts and models	IEC 62443-3-2 Master glossary of terms and abbreviations	IEC 62443-3-3 System security conformance metrics	
Component	IEC 62443-4-1 Product development requirements	IEC 62443-4-2 Technical security requirements for IACS components		

Figure 1: The components of IEC 62443

[1] "Cybersecurity in Operational Technology: 7 Insights You Need to Know," Ponemon Institute, March 2019, https://lookbook.tenable.com/ponemonotreport/ponemon-OT-report.

At the same time, the Zero Trust model has gained mainstream status for securing IT networks. Similar to the concept of the principle of least route within OT, the Zero Trust model is a widely accepted approach to cybersecurity that can be readily applied to OT environments to help meet the technical and architectural requirements of ISA/IEC 62443. The two frameworks align in many technical aspects, with only context and terminology differing somewhat.

Better yet, using the Zero Trust five-step methodology (which fulfills the principle of least route) will simplify the implementation of the IEC 62443 series of standards for OT environments, enabling organizations to improve security of their critical OT systems using an iterative approach.

Simplifying ISA/IEC 62443 Using the Zero Trust Five-Step Methodology

Zero Trust is a strategic initiative that helps prevent successful cyberattacks by eliminating the concept of trust from an organization's network architecture. Rooted in the principle of "never trust, always verify," Zero Trust is designed to protect modern digital environments by using network segmentation, preventing lateral movement, providing Layer 7 threat prevention, and simplifying granular access control.

Traditional security models operate on the outdated assumption that everything inside an organization's network should be trusted. Under this broken trust model, it's assumed that user and device identities are not compromised. It further assumes that all users and devices act and operate responsibly and can be trusted. In comparison, the Zero Trust model recognizes that blind, unverified trust is a vulnerability.

When the Zero Trust model was first published, some organizations were reluctant to adopt it because they erroneously believed that it would be too difficult, costly, or disruptive to implement. In truth, designing Zero Trust environments is even simpler than building traditional hierarchical networks. In addition, it's not necessary to rip and replace existing networks to deploy Zero Trust. Instead, companies can move from legacy environments to Zero Trust over time using an iterative approach.

As companies begin to realize this, acceptance and adoption of the Zero Trust approach is growing, with a survey of IT security leaders reporting 275% year-on-year growth in the number of North American organizations that have or plan to have a defined Zero Trust initiative in the next 12 to 18 months. The study also found that 60% of organizations in North America, and 40% globally, are currently working on Zero Trust projects.

Creating a Zero Trust IT environment is a relatively simple process that can be iterated upon to protect one asset at a time until the entire environment is protected. This pragmatic approach and five-step methodology (see figure 2) can also be valuable for securing OT environments using Zero Trust principles.

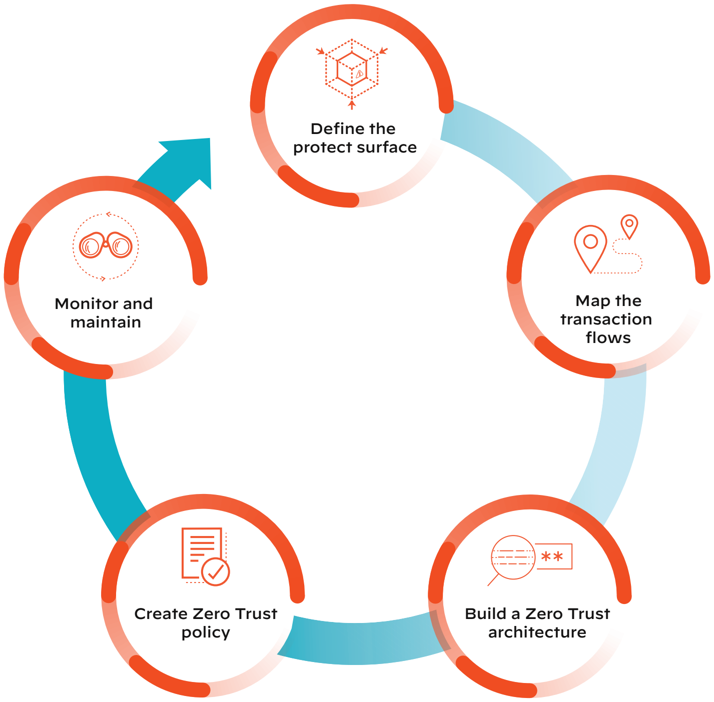

Define the protect surface
Map the transaction flows
Build a Zero Trust architecture
Create Zero Trust policy
Monitor and maintain

Figure 2: Five steps to a Zero Trust environment

Step 1: Define the Protect Surface

In an industrial context, the protect surface encompasses all connected devices relevant to the industrial process. This starts with the industrial process; its digital enablers, including I/O devices, programmable logic controllers (PLCs), and more; and Ethernet and IP infrastructure devices, such as routers, switches, and common IT gear. You should consider the actual protect point to be the physical device (robot, valve, or other connected physical asset) and any network equipment required to power, control, or report the status of that device. In this process, identify the critical digital assets and paths, making note of the one-to-one relationships of digital assets to the physical process.

Security in OT safeguards the very lifeblood of the company. That said, you can never protect everything with the highest security. You have to decide what's the most important and most critical, and what will have the largest impact on production and safety.

Step 2: Map the Transaction Flows

Unlike IT systems, the most important thing to protect in OT is the industrial process itself. To properly design the Zero Trust environment, you need to understand the flow of data and its alignment to processes inside the OT network.

Make sure you understand all the components involved in a process and their relationships with other components and processes. How do the different components you identified in the first step interact with each other?

[2] "The State of Zero Trust in Global Organizations," Okta, May 2020, https://www.okta.com/resources/reports-state-of-zero-trust-security-in-global-organizations.

Once you have identified the assets and processes that are critical to safety and operations, you must begin to understand the network and data dependencies (critical digital assets) required to maintain the operations. This flow includes both the required production data (relative to industrial process) and the supporting network processes that make IP-based communications possible. For example, what would happen if the Domain Name System (DNS) were disrupted and domain controllers became unavailable? With a full understanding of the risk points and failure points in a system design, you can truly understand the flows and their dependencies.

Step 3: Architect a Zero Trust/Zone and Conduit Network

With your protect surface defined and flows mapped, the Zero Trust/Zone and Conduit architecture should become more apparent. You should now understand the physical relationship between data processes and real-world actions, giving you the ability to engineer a deterministic network architecture where the production process as well as its supporting critical digital processes and gear are protected.

Knowing what to protect and why, coupled with an understanding of how production is impacted if those services are compromised, you can design a production-centric, cyber-protected process around data flows appropriate to your production process.

Step 4: Create the Zero Trust Policy

Once you've engineered your Zero Trust architecture, you need to create the supporting Zero Trust policies, following the so-called Kipling Method to answer the who, what, when, where, why, and how of your network and policies.

For one resource to talk to another, a specific rule must allow that traffic. The Kipling Method of creating policy enables granular enforcement so that only known allowed traffic or legitimate system communication is permitted in your network. This process significantly reduces the addressable attack surface.

Create policy that links steps 1 and 2, and implements step 3 into policy and design, in an engineered format.

Step 5: Monitor and Maintain the Network

To make sure the previous steps are performing as required, monitor what those assets and flows (steps 1 and 2) are, and should be, doing. This becomes your baseline for normal behavior. Create alerts and respond to aberrant or anomalous behavior.

Inspecting and logging all traffic on your network are essential components of Zero Trust and ISA/IEC 62443.

Inbound industrial data should be contextualized into security value (e.g., understanding a set-point in a PLC), and then security infrastructure that programmatically understands the industrial process will block or allow certain commands or command values within the industrial process.

Conclusion

As briefly demonstrated here, the key to industrial security is the production process. Zero Trust can be implemented and leveraged to enhance or deliver an IEC 62443 Zone and Conduit architecture as long as you make the protect surface the entire production process (along with its critical digital assets).

To learn more about identification of cyber assets, determination of critical digital assets, and the application of Zero Trust as a mechanism for safely and effectively satisfying the technical aspects of IEC 62443, see the Reference List included in this document or reach out to **accenture@paloaltonetworks.com**.

Reference List

ISA/IEC 62443: The ISA/IEC 62443 series of standards, developed by the ISA99 committee and adopted by the International Electrotechnical Commission (IEC), provides a flexible framework to address and mitigate current and future security vulnerabilities in IACS.

Zero Trust: Zero Trust is a strategic initiative that helps prevent successful data breaches by eliminating the concept of trust from an organization's network architecture.

Kipling Method: Rudyard Kipling put forth the concept of "who, what, when, where, why, and how" in his poem "Six Serving Men." The Kipling method is used in Zero Trust to understand how to define granular security policies.

Principle of Least Route: Coined by Rockwell Automation and stemming from the IT principle of least privilege, this concept limits the paths into a system, making it harder to penetrate, by giving network access only to fulfill a specific function.

NIST: The National Institute of Standards and Technology (NIST) is a unique federal agency. Its mission is to promote US innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

About the Authors

This white paper was jointly developed by Palo Alto Networks and Accenture Security.

Working through a strategic partnership, Palo Alto Networks and Accenture Security offer multiple solutions, including cybersecurity, managed security services, network optimization and transformation services, security operations and optimization services, compliance strategy/risk management, endpoint security, and network transformation.

Accenture

Accenture is a leading global professional services company, providing a broad range of services in strategy and consulting, interactive, technology and operations, with digital capabilities across all of these services. We combine unmatched experience and specialized capabilities across more than 40 industries — powered by the world's largest network of Advanced Technology and Intelligent Operations centers. With 513,000 people serving clients in more than 120 countries, Accenture brings continuous innovation to help clients improve their performance and create lasting value across their enterprises. Visit us at www.accenture.com.

Palo Alto Networks

Palo Alto Networks, the global cybersecurity leader, is shaping the cloud-centric future with technology that is transforming the way people and organizations operate. Our mission is to be the cybersecurity partner of choice, protecting our digital way of life. We help address the world's greatest security challenges with continuous innovation that seizes the latest breakthroughs in artificial intelligence, analytics, automation, and orchestration. By delivering an integrated platform and empowering a growing ecosystem of partners, we are at the forefront of protecting tens of thousands of organizations across clouds, networks, and mobile devices. Our vision is a world where each day is safer and more secure than the one before. For more information, visit www.paloaltonetworks.com.

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com