ISAGCA Webinar Series

Zero Trust Outcomes Using ISA/IEC 62443 Standards

Link to Whitepaper

Authors/Presenters:

Andrew Kling , VP Cybersecurity, Schneider Electric
Bob Pingel, OT Cybersecurity Strategist, Rockwell Automation
Danielle Jablanski, ICS cybersecurity strategist CISA

ISA GLOBAL CYBERSECURITY ALLIANCE

Andrew Kling, VP Cybersecurity, Schneider Electric

Andy has over four decades of software development experience while working in multiple industries. He has worked at Schneider Electric since 2001. At Schneider Electric, Andy has managed many process control engineering teams. As a result of this experience, Andy has ushered the Schneider Electric Development organization to comply with ISA 62443 cybersecurity standards at the process, product, and system levels, achieving several security-related world firsts along the way. Andy is a leader in the Schneider Electric technical cybersecurity community, sits multiple industry committees, is a technical board member for First Watch - a cybersecurity start-up based in NZ, and regularly guest-lectures university courses on cybersecurity.

His expansive knowledge has attracted audiences with multiple high-level government security agencies worldwide. He has provided security briefings to members of the White House National Security Council and the State Department. Holder of multiple patents, the Schneider Electric 2021 global innovation challenge winner, and a sought-after speaker on Cybersecurity, Andy has remained at the forefront of his field, with the level of expertise to see and impact big picture challenges in both world-class corporate and government sectors.

Bob Pingel, OT Cybersecurity Strategist

- Bob is in his fourth decade with Rockwell Automation.
- He has held technical and managerial roles with increasing responsibilities in product development and enterprise IT security governance.
- He is currently an OT Cybersecurity Strategist, collaborating with product development teams to ensure Rockwell Automation delivers secure solutions, compliant with the increasing worldwide regulations, to allow their customers to meet stringent resilience goals.

Rockwell Automation

Danielle Jablanski, ICS cybersecurity strategist CISA

Danielle Jablanski is an ICS cybersecurity strategist at the US Cybersecurity and Information Security Agency (CISA), serving in the Office of the Technical Director. As the lead for ICS strategy, she is responsible for expanding the utility and reach of ICS products and services, coordinating internal and external stakeholder efforts, and maximizing public-private efforts for the OT and ICS cybersecurity industry and critical infrastructure owners and operators. She is also a nonresident fellow at the Cyber Statecraft Initiative of the Atlantic Council's Scowcroft Center for Strategy and Security. Jablanski is also an advisor at Kutoa Technologies, and an Adjunct Professor teaching Intro to ICS Cybersecurity at Dallas College. Jablanski has been responsible for conducting technical, academic, and market research on emerging technologies throughout her career. She has independently consulted for the US government and industry on novel technology applications. She began her career with the Stanley Center for Peace and Security evaluating cyber impacts to nuclear weapons policy. Previously, Jablanski contributed to the creation and development of the Stanford Cyber Policy Center at Stanford University and spent time as a senior research analyst and industry strategist before joining CISA.

Agenda

- Zero Trust Strategy
- Why does Zero Trust matter today?
- 5 Steps to Applying Zero Trust
- Essential Functions & Zero Trust
- Cost/Benefit Considerations for Zero Trust in OT
- Cost/Benefit Considerations for Security Practitioners
- Cost/Benefit Considerations for Business Leaders
- High-Level Implementation Strategy

Zero Trust as a Strategy

IS	IS NOT
A conceptual framework for strategically building defensible architectures	A silver bullet for cybersecurity
A mechanism for setting required level of verification and authentication for devices, systems, components, and users	A single system policy that can be pushed to multiple machines or zones automatically
A way to enforce accurate, least-privileged, per-request access decisions in information systems	An out of the box solution
Applicable to OT/ICS	Applicable to every single type of field device and instrumentation setup

Why does Zero Trust matter today?

Evolution of Connectivity	• Network connectivity on prem → Connectivity between sites → SCADA Cloud Adoption
Diverse Attack Patterns	• Tailored for a single target – intent: prolonged access and loss of view and/or control scenarios • Opportunistic based on credential harvesting and exchanges on the dark web • Insider threat scenarios (compromised, malicious, negligent)
Access Points	• Virtual Private Networks (VPNs) and Remote Desktop Protocol (RDP)
Security	• Spoofing/phishing for credentials & credential directory grabs • Man in the middle – on insecure systems or from open/internet ports • Beginning to automate required mechanisms to capture data and communications once statically logged and reviewed (maybe)
	• Personal devices (esp. government and commercial smart buildings)

5 Steps to Applying Zero Trust

1. Identify mission-critical devices, systems and components
2. Map flows of data and access to mission-critical devices, systems and components
3. Architect your network to secure mission-critical devices, systems and components from malicious threats and unintentional incidents
4. Create automated rules (where possible) for the flow of traffic, data and access only where intended and not off-network or to unknown services, devices or components
5. Continuously monitor OT/ICS networks to log and inspect all traffic, assets, users and access requests

Essential Functions & Zero Trust

Essential Functions according to the ISA/IEC 62443 standard are “functions or capabilities required to maintain health, safety, the environment and availability of the equipment under control.”

Examples include:

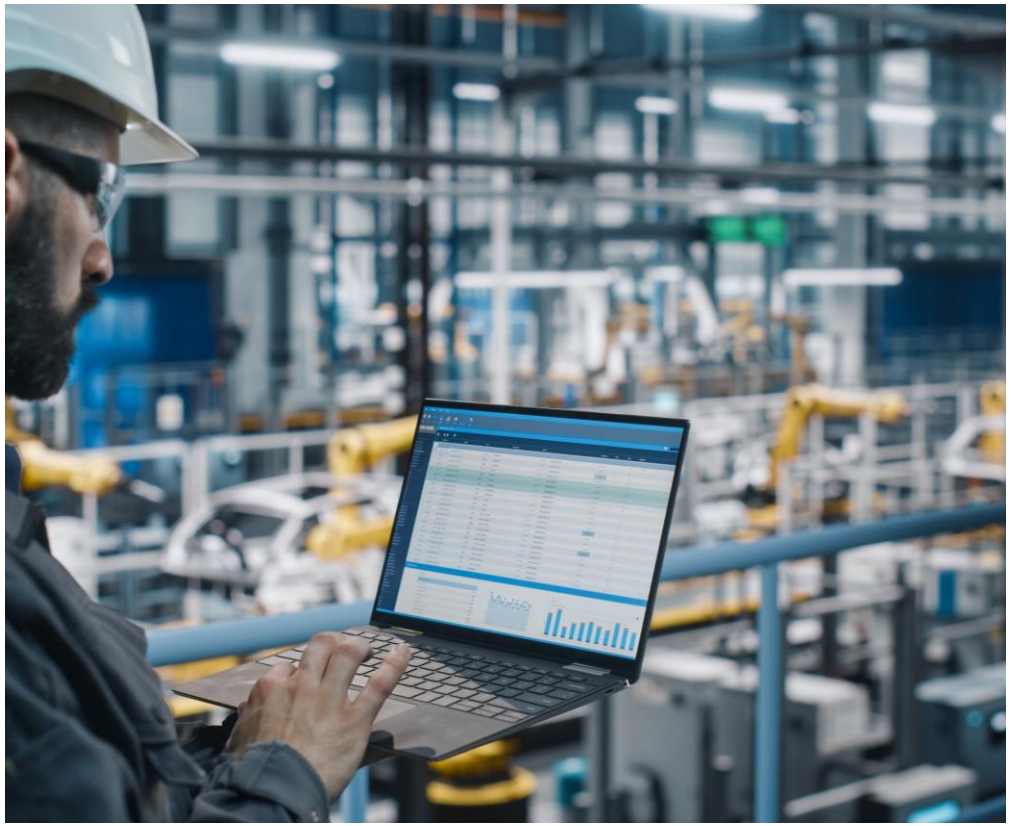
- **Safety instrumented functions (SIF)**
- **Control function**
- **Ability of the operator to view and manipulate the equipment under control**

ISA/IEC 62443 Standard Part	Essential Functions Review Sections
2-1: Security program requirements for IACS asset owners	NET 1.3 / 1.4 / 1.5 / DATA 1.3
2-4: Security program requirements for IACS service providers	SP.05.01-SP.05.09
3-2: Security risk assessment for system design	ZCR 3.3
3-3: System security requirements and security levels	Section 4.2
4-2: Technical security requirements for IACS components	Section 4.2
Least privilege	2-4 SP.03.08 3-3 SR 2.1 4-2 Section 4.4
Continuous monitoring	3-3 FR2 / 3-3 FR6 / 4-2 FR2 / 4-2 FR6

Cost & Benefit Considerations for Zero Trust in OT

- Establishing context for ZT in the ICS and OT world
- Cautions concerning operator fatigue
- Implementing zero trust requires resources, buy-in from leadership and two technical foundations to build upon:
  - Asset inventory
  - An understanding of known threats and vulnerabilities

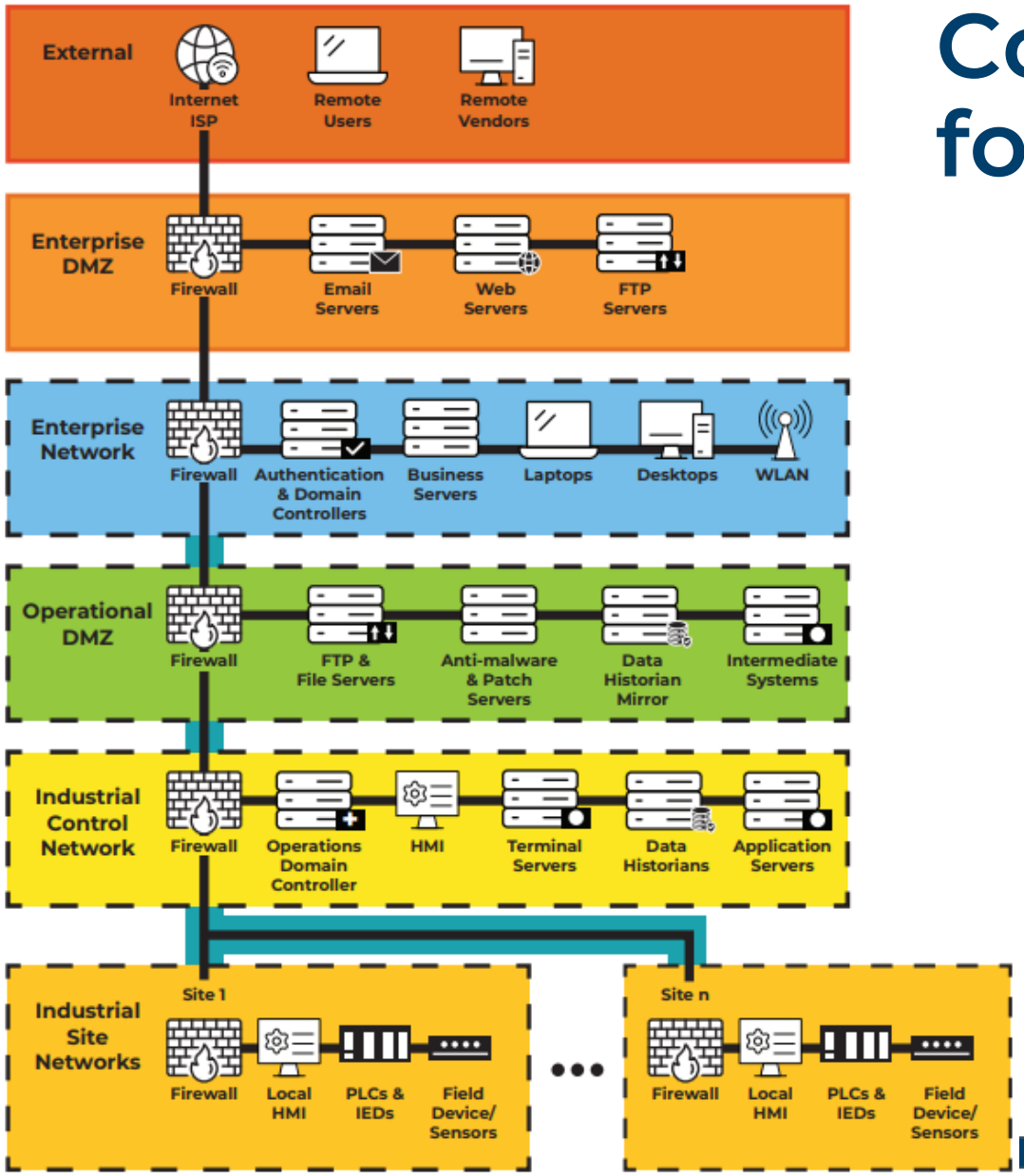
Cost & Benefit Considerations for Zero Trust in OT



When availability is paramount, applying ISA/IEC 62443 to OT networks requires dividing assets into zones and conduits.

- Zones - A grouping of logical or physical assets that share standard security requirements based on criticality and consequence, among other characteristics.
- Conduits - Groupings of assets dedicated exclusively to communications that share security requirements.
- ISA/IEC 62443, used as a tool, helps organizations strategically look at how zones operate and how our networks communicate, access is managed, devices discovered and identified, and protocols used to understand their behaviors better and inform the controls chosen.

ISA GLOBAL CYBERSECURITY ALLIANCE



Cost & Benefit Considerations for Zero Trust in OT

Using ISA/IEC 62443 principles, you are assured that the intrinsic security capabilities necessary to achieve your zero trust architecture are already available

The ISA/IEC 62443 model of security zones and conduits offers a granular approach for evaluating devices and systems capable of incorporating zero trust principles and assigning appropriate controls that can be implemented within an ICS/OT environment.

ISA GLOBAL CYBERSECURITY ALLIANCE

Implementation Strategy: Zero Trust Application Contexts

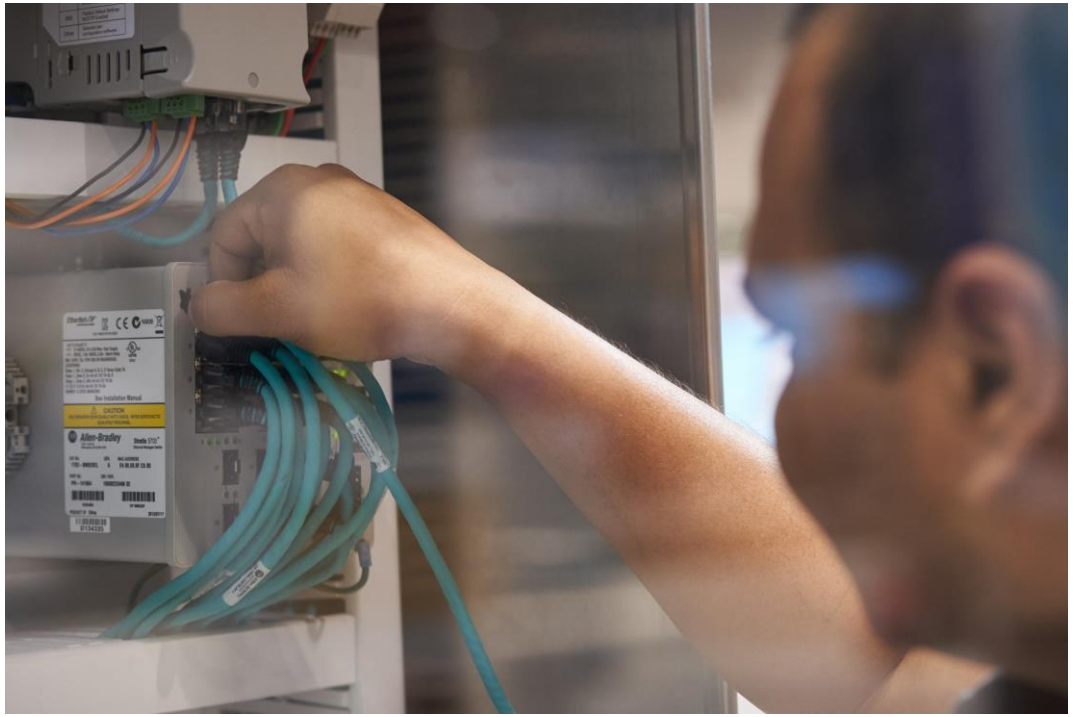
Zero Trust can be applied in many areas within a typical automation application, but some more easily than others

- Secure Remote Access
- Zone / Perimeter Control
- Intra Zone / Controller-to-FieldDevice

Implementation Strategy: Perimeter Building Blocks

I understand my trust zones, how do I build perimeters?

- Secure Remote Access
  - Bespoke Secure Remote Access solutions
  - Secure Service Edge
  - VPN
- Zone / Perimeter Control
  - Firewall
  - Zone Perimeter Device
  - Secure Industrial Protocol
- Intra Zone / Controller-to-FieldDevice
  - Secure Industrial Protocol



Conclusion

- Using ISA/IEC 62443 principles, you can be assured that the necessary security capabilities for achieving a zero-trust architecture are available
- The implementation of zero trust involves additional upfront and maintenance costs as it elevates security dimensions and magnitude, but it also offers significant benefits in terms of understanding and organizing a security strategy.
- In a cybersecurity landscape crowded with different opinions, zero trust can bring order and coherence to a policy enforcement approach, leading to short-term gains and long-term improvements in cyber posture.
- ISA/IEC 62443 and zero trust go hand in hand for success. Every organization should prioritize visibility of all mission-critical and business-critical processes and implement appropriate cybersecurity controls.
- As discussed today, zero trust maturity covers a wide range of cyber-defense topics, ensuring that a balanced and proven set of cyber controls addresses ICS/OT defensive needs.

In Memoriam of Michael Chaney (Idaho National Labs), who contributed to Zero Trust Outcomes Using ISA/IEC 62443 Standards whitepaper.

ISAGCA and authors were saddened to hear that co-author Michael Chaney passed away in early 2024. We want to acknowledge his efforts as a ISAGCA member and founding member of the ICS4ICS team. We encourage leaders to continue to learn from his strategic support and impacts on our industry.

Questions/Answers

Be Part of the Movement to Prioritize OT Cybersecurity

Change the Culture

Recognize cybersecurity as a fundamental workplace tenet alongside functionality, efficiency, and safety

Learn more | www.isagca.org

ISA GLOBAL CYBERSECURITY ALLIANCE

ISA Cybersecurity Resources

Free guidance, training, and more:

ISA Global Cybersecurity Alliance - www.isagca.org

A collaborative forum to advance OT cybersecurity and understanding of ISA/IEC 62443

ISASecure www.isasecure.org

The world's leading conformance certification program for ISA/IEC 62443

ICS4ICS www.ics4ics.org

Improve how cybersecurity incidents are managed with training, processes, and exercises

Get involved:

- ISA/IEC 62443 standards available from ISA (free access with ISA professional membership!)
- Cybersecurity training and certificate program
- Help develop the standard – open to all at no charge – www.isa.org/ISA99