GLOBAL CYBERSECURITY ALLIANCE

ISAGCA Whitepaper

Zero Trust Outcomes Using ISA/IEC 62443 Standards

www.isagca.org

Table of Contents

ISAGCA Whitepaper

Zero Trust Outcomes Using ISA/IEC 62443 Standards

Introduction

The concept of “zero trust,” a pivotal strategy in cybersecurity, was first introduced by Forrester analyst John Kindervag in 2010. Since then, it has evolved and been sustained within cybersecurity strategic planning and preparation. This “no one is trusted by default, always verify” premise has become a widely accepted strategy, with the idea that risk is internally and externally inherent. This evolution has led to the development of new architectures, models, concepts, paradigms and solutions in the implementation of zero trust, all of which are crucial for security practitioners and professionals in operational technology (OT) and industrial control systems (ICS).

At the heart of the zero trust model is the concept of trust, which can be conditional or absolute when designed for devices, systems, network components and users. Both types of trust require verification and authentication. This process ensures that a device, system, component or user knows something (*e.g.,* a password), has something (*e.g.,* a cryptographic key), or is something (*e.g.,* a registered authenticated user). The required level of verification and authentication depends largely upon the criticality of the device, system or component and the data it uses or stores. Therefore, mission-critical systems and sensitive data should come with the highest and most stringent forms of verification and authentication, a key principle in the zero trust model.

According to the U.S. National Institute of Standards and Technology (NIST), a globally recognized authority in cybersecurity, zero trust is a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least-privileged, per-request access decisions in information systems and services in the face of a network viewed as compromised. The basic premise of zero trust is that no implicit trust is granted to users, systems or system components based on their physical or network location because there is no trust in any network, user or device. This definition from NIST further solidifies the importance and validity of the zero trust concept in the cybersecurity field.

The zero trust strategy is becoming more relevant for industrial operations. In OT networks, it may not be feasible to prompt for authorization and verify access continuously. Instead, integrated controls can more finely manage access to resources, services and segmented network components and can involve alternative authentication methods. Hybrid approaches can incorporate zero trust principles where appropriate to enhance detection and response capabilities at scale.

Traditional security architectures are typically based on implicit trust, with hardened external perimeters around less protected internal operations often resulting in flat networks. According to Gartner, a zero trust architecture eliminates implicit trust (i.e., “This user is inside my security perimeter”) and replaces it with adaptive, explicit trust (*i.e.,* “This user is authenticated with multi-factor authentication (MFA) from a corporate laptop with a functioning security suite”). While some view zero trust as a rebranding of network segmentation and the principle of least privilege, successful implementation of zero trust requires studying how devices, systems, components and users interact, what is needed for interaction and how to minimize unnecessary interaction and access.

Implementing a control solution using components based on ISA/IEC 62443 principles can ensure that the security capabilities required for your zero trust architecture are already available.

The US Cybersecurity and Infrastructure Security Agency (CISA) has outlined a maturity scale for zero trust implementation across five pillars: identity, device, network/environment, application workload and data. However, the controls included do not perfectly align with OT/ICS networks. Additional controls that can be designed and implemented in the industrial space include:

- Network segmentation
- Software-defined networks
- Application layer gateways
- Continuous monitoring
- Deep packet inspection
- Secure remote access
- Secure protocols
- Endpoint protection
- Enhanced identity access management

OT Systems: Essential Functions

In OT security, priorities are structured differently than in IT, with safety being the utmost concern. The aim is to prevent the loss of life, endangerment of public health or damage to the environment, production or equipment. Therefore, any decision or security measure introduced must be technically understood for its impact on safety and availability. This underscores the importance of never overriding or interrupting these essential critical functions in zero trust architecture implementations, especially safety functions associated with fault-tolerant systems design.

OT systems typically employ a fail-to-a-known-state design (*i.e.,* fail-safe design) in the event of an unexpected situation or a component failure. The fail-safe design considers placing the equipment or process in a safe state that prevents injury to individuals or the destruction of property and avoids cascading events or secondary hazards. Cyber-related events, such as the loss of network communications, could trigger these fail-safe events. Organizations should define the thresholds at which OT components can operate with reduced or disrupted capabilities, such as lost network communications.

In the ISA/IEC 62443 series of standards, essential functions are defined as functions or capabilities required to maintain health, safety, the environment and availability of the equipment under control. Essential functions include:

1. The safety instrumented function (SIF)
2. The control function
3. The ability of the operator to view and
4. manipulate the equipment under control

ISA/IEC 62443-3-3, System security requirements and security levels, requires that security measures shall not adversely affect essential functions of systems that require high availability unless otherwise supported by a risk assessment. The controls detailed below from a zero trust perspective should not be introduced if they would prevent the operation of essential functions if their failure modes lead to loss of view, loss of control or loss of production, or if they circumvent backup and island mode capabilities for the process control systems and operators.

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

As cybersecurity can be another threat to the safety and reliability of industrial processes, NIST suggests including safety experts as part of the cybersecurity team to identify potential impact areas. Their insight into OT design and safety considerations will also help formulate cyber mitigations when considering whether additional cybersecurity requirements for safety systems are required. For example, safety considerations may require an organization to use physical separation instead of logical separation.

Remember to consider the following safety procedure: IEC 61511/ISA-84, *Standard for Instrumented Systems to Achieve Functional Safety in the Process Industries,* predicated upon a performance-based safety lifecycle (SLC) to help reduce risk and to provide a foundation for the development, operation and maintenance of safety instrumented systems (SIS). The SLC comprises three phases: analysis, design/implementation (realization) and operation and maintenance. Gap analysis and requirements for functional safety management plans incorporating the SLC for safety systems can be directed to OT vendors, original equipment manufacturers (OEMs) and third-party certification bodies.

Cost/Benefit Considerations for Zero Trust in OT

In the context of industrial control, zero trust brings additional considerations. In many industrial sectors, the application of concepts such as CIA — confidentiality, integrity and availability — are inverted and morphed into safety, availability, integrity and confidentiality (SAIC). Care is essential as a newly introduced interaction for authentication might be a minor difference in the IT space. Still, it can result in a negative performance difference or safety concern in the industrial world.

The scope of a zero-trust strategy and implementation is somewhat different for operational technology and industrial control systems in that mission-critical operations are more important to protect than access to sensitive data in most cases. While identity-central access management is more difficult within OT/ICS networks, zero trust can still evaluate the controls, tools and policies introduced within security programs and network architectures.

For instance, only a subset of zero trust principles is not applicable for field devices and instrumentation typically deployed in level 0 of the Purdue Model. At the supervisor level, or level 3 and above, many systems are capable of local access controls and network policy implementation of zero trust principles. While segmentation remains one of the most foundational security principles for OT/ICS, security controls introduced to implement zero trust strategies can bolster segmentation when adequately enforced.

Creating overly complex and burdensome controls leads to end-user fatigue, wasted resources and inefficiencies. When implementing zero trust, like any ICS solution, attention to the user experience will help ensure seamless adoption of these controls. Appropriate security automation, screen flow and efficient interactions will all reduce adverse reactions to zero trust controls. Segmentation ensures network and access boundaries between OT/ICS operations and enterprise resources and networks, dispersed operations and facilities, as well as secure remote access. Zero trust applied to OT/ICS bolsters network segmentation by following the five-step methodology applied to OT/ICS:

Five-Step Zero Trust Methodology Applied to Operational Technology

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

Implementing zero trust requires resources, buy-in from leadership and two technical foundations to build upon: asset inventory and an understanding of known threats and vulnerabilities. Cyber attacks affecting OT/ICS networks and operations can be intentional or accidental. They can be introduced by malicious threat actors or motivated/negligent insider threats. The resulting impacts can include potential safety incidents, cyber-physical damage or destruction, shutdowns, downtime and accidental cascading consequences. This is because availability is paramount. As a result, cybersecurity is a dynamic, continuous and iterative process.

When availability is paramount, applying ISA/IEC 62443 to OT networks requires dividing assets into zones and conduits. Zones are a grouping of logical or physical assets that share standard security requirements based on criticality and consequence, among other characteristics. Conduits are groupings of assets dedicated exclusively to communications that share the same security requirements. Conduits can also be used to describe tunnels communicating between zones. 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.

The Essential Message

By implementing a control solution using components implemented in accordance with 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 displayed below in figure 1 offers a more 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.

The zero trust strategy comprises an organization’s vision, approach, principles, goals and objectives and roadmap for migration. Its implementation involves deploying measurable, repeatable, supportable and extensible standards, tools and processes. When zero trust

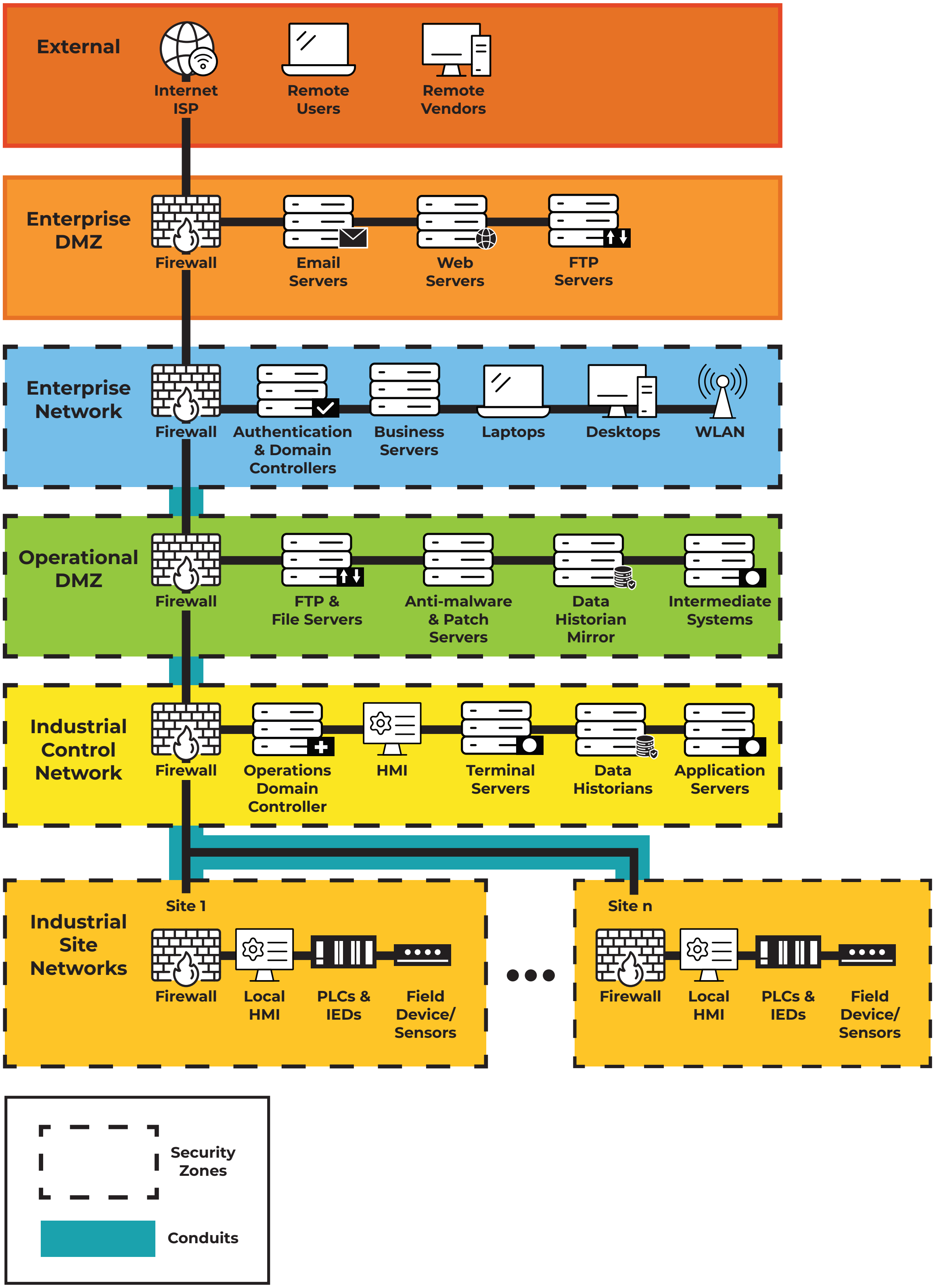

Figure 1: ISA/IEC 62443 Security Zones and Conduits

strategies are implemented alongside ISA/IEC 62443, they result in a more secure, coordinated and cost-effective architecture, ensuring the availability of mission-critical devices, systems and components. The five-step methodology mentioned, along with the zones and conduits from ISA/IEC 62443, supports an incremental migration approach to cybersecurity. This approach aims to achieve an interoperable, fully functioning, optimized cybersecurity architecture that secures critical assets and data from malicious threats and unintentional incidents.

Cost/Benefit Considerations for Security Practitioners

Access to today's OT systems is based on many layers of implicit trust by design for mission-critical functionality and availability. This trust may authorize that a device with a network path to the control system is authorized to connect and does not check that an attacker did not misappropriate the credentials. Further, we assume, or trust, that the device used to connect is secure. We implicitly trust the network, often using clear text protocols without sophisticated, modern integrity validation. OT systems take implicit trust to another level by rarely implementing robust network or device monitoring and threat detection. Zero trust principles offer a more secure path by improving these trust contexts with explicit trust policies instead.

OT System Zero Trust Scope

Zero trust is applied differently in different OT system contexts — remote access, edge to cloud, control equipment to an industrial demilitarized zone (iDMZ), control equipment peer communications and control equipment to I/O or field device communications. The system contexts are listed in ascending trust order, but trust should never be implicit. We will examine the five steps to zero trust and the system contexts using an ISA/IEC 62443 lens.

There is a tight crosswalk between zero trust and ISA/IEC 62443 controls/concepts:

Zero Trust	ISA/IEC 62443
Protect surface	Zone / 3-3 FR5 / 4-2 FR5
Network flow	Conduit / 3-3 FR5 / 4-2 FR5
Strong identity	3-3 FR1 / 3-3 FR2 / 4-2 FR1 / 4-2 FR2
Secure comms	3-3 FR3 / 3-3 FR4 / 4-2 FR3 / 4-2 FR4
Data flow policy	3-3 FR5 / 4-2 FR5
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

Remote Access

Zero trust is most commonly seen in remote access to control systems, typically with an external operator accessing an engineering workstation ("jump box") in the industrial DMZ. The perimeter of the iDMZ is the first zero trust protect surface and the basis of an ISA/IEC 62443 zone. The world beyond the iDMZ is not trusted — all actors must be authenticated, devices validated and network communications secured.

- Actor authentication is most typically performed via multifactor authentication. Connection authorization is granular; the actor is only allowed to see and connect to devices for which they are authorized.

- Device (the actor’s computer) authentication is performed via certificate validation, and often, the device is validated to meet system security policies (patch level, antivirus and such).
- The network is untrusted, data must be encrypted, and network integrity controls must be implemented. Industrial protocols are maturing, but many are still clear text with no integrity controls; if this traffic is required to leave the iDMZ boundary, it must be encapsulated in a secure tunnel.

A zero trust architecture often implements remote access via commercial secure service edge (SSE) providers. In this case, the SSE provided the controls described above and further augments security with traffic inspection, intrusion detection and auditing. These platforms also provide detailed security policy allow for time-of-day and geographic area connection granularity. The solutions can take security one step further by fully insulating the actor’s computer by instantiating a virtual in the cloud, implementing the connection over standard protocols (RDP/SSH) and feeding an HTML5 stream back to the actor’s computer. Similar controls are available via OT-specific remote access solutions from ICS vendors and third-party providers.

Edge to Cloud Communication

Today’s control systems often need to connect to the cloud in order to perform functions such as cloud-based analytics and reporting. It is recommended that control components do not directly connect to the cloud; instead, they should connect to a cloud “edge” component in the iDMZ, which will handle the cloud communications. Communication between the control components and the edge device should be appropriately secure for the specific environment and application. Depending on the criticality of the traffic, encryption should be considered to address confidentiality, and other network and component functions should be implemented to ensure availability. When communicating over public networks from the edge component to the cloud, it is important to use a secure encrypted protocol and integrity controls due to the untrustworthy nature of these networks.

As ISA/IEC 62443 requires, user, API key, and component authentication must be implemented. It is preferred that cloud communication be performed via a secure internet gateway, which will offer full traffic inspection and security monitoring.

Control Equipment to iDMZ Communication

Standard system components are often placed in the iDMZ or layers just below it, such as historian and other production-oriented databases, intermediary systems, patch servers and security information and event management (SIEM) systems. Control equipment is regularly connected to these services to store data or read production information. The iDMZ is more trusted than the zones that lay beyond, but zero trust controls such as authentication and authorization must still be implemented. Devices and users must be authenticated. Network communications will usually not be encrypted, but integrity controls are required. Network events and system telemetry must be continuously monitored and used to detect abnormal behavior. Traffic-based threat detection applies to these traffic flows.

iDMZ access networks are typically in physically secured facilities, and control equipment is on the manufacturing floor, where direct physical access is possible. To protect these vulnerable networks, network access controls via traditional IT-centric network access controls or software-defined networking (SDN) are often implemented.

Control Components Peer Communication

Control components like programmable logic controllers (PLCs), drives and drive controllers, and human-machine interfaces (HMIs) must communicate on the plant floor. These devices are sometimes all in one zone but most often segregated. Communication between these devices must be secured minimally with integrity controls. Risk assessment on traffic criticality will indicate if availability controls must be employed and if encryption should be employed to address confidentiality. Modern industrial protocols offer certificate-authenticated communications with full integrity controls. Encryption is an option, but care should be taken to address potential impacts on real-time deterministic network performance and to avoid hampering traffic-based threat detection. Data flow policy between devices must use an authorization policy to dictate which devices can communicate. Network events and device telemetry must be continuously monitored and used to detect abnormal activity.

Control Components to System I/O or Field Devices

Control component to I/O, or field device, communication is critical. Control components contain the "control" of the system, the logic dictating what action should be taken in the face of a given input or condition. The I/O or field devices are the actual inputs and outputs, the cyber/physical interface of the control system. If an attacker were to get access to one of the devices or control communication with it, they could take control of the control system by forcing the input and output conditions, leading to whatever outcome they desire.

Secure communications to these low-level devices are critical but often complex to achieve. Encrypted communications require device bandwidth, which takes away from the performance of the already performance-constrained device. A good meet-in-the-middle solution is for a protocol to implement secure communications but to communicate in clear text–transport level security (TLS) with a null cipher suite – yielding performant integrity-controlled communication.

Integrity-controlled communication prevents an attacker from indiscriminately communicating with a device or system component. All communication paths are preauthorized and authenticated. As previously mentioned, cleartext communication also enables passive traffic-based threat detection solutions.

Recommended Actions

While leveraging the capabilities of ISA/IEC 62443 and zero trust will require investment, the benefits more than justify the cost in terms of organizational resiliency, strength of financial controls and understanding of the capabilities of the current business model to adapt new technologies to realize future opportunities. Organizations with fully deployed zero-trust architectures have made significant strides along the maturity path for cybersecurity. Implementation requires leadership buy in, cooperation from multiple business units and departments and efficient maintenance, enhancement and change management procedures.

All organizations are encouraged to transition from a state of "unknown unknowns," which is a state of the implicit trust of third parties, to a state of "known unknowns," a state of zero trust. Implementing ISA/IEC 62443 controls is the most effective tool to achieve that goal. A zero-trust architecture requires the application of cybersecurity controls and associated zero-trust architecture principles at all levels of application architecture, including endpoints, services and data flows.

Cost and Benefit Considerations for Business Leaders

While zero trust operates in a way that assumes any user or connection to a network may be a threat and should not be implicitly trusted, it relies on a collection of techniques implemented via cyber practices and controls. Breaking down the business side of implementing a zero trust architecture, consider the following:

- Resources and personnel
- Enterprise security policy

- Communications and data flow
- Access and authentication
- OT security specifications

Resources and Personnel — ICS/OT components must support the intrinsic functions necessary for implementing zero trust. Role-based access control (RBAC), authentication mechanisms, device identity and so on will be included. ICS/OT systems designed and built to ISA/IEC 62443 standards will inherently have these functions and capabilities. Training the team to implement these cyber controls supported by the intrinsic functions will be a first step.

Enterprise Security Policy — Zero trust does not work if it is only partially deployed. Yes, there is a maturity approach that allows for a steadily improving implementation. Still, you cannot employ zero trust controls on one part of the system and ignore other parts. Attackers will quickly identify the missing controls. To be successful with zero trust, follow ISA/IEC 62443, which describes risk assessment steps, and use the five-step zero trust methodology. Borrowing from lean concepts — *"See the Whole,"* a system is not just the sum of its parts but the product of their interactions. Establish a security policy defining your zero trust mandates at the system level as an essential step towards zero trust strategy and implementation success.

Communications and Data Flow — To secure access to data and its components and devices (think *control point value* in a PLC), it is essential to understand where the data resides, where it will move to and who wishes to transform it. This communication and data flow will define where cyber controls (described above) must be implemented. It is as simple as that. But do not underestimate how complex it will be to get this "diagram" correct. Time invested in carefully mapping out data flow and communication paths will ensure a quality and predictable deployment of zero trust. Plus, documenting data flows is an essential step in creating threat models. Examine past risk assessment threat modeling exercises or use these data flow diagrams to support future threat modeling work.

Access and Authentication (A&A) — Given sufficient skill, capability (component and system), motivation and policy and an understanding of where cyber control points need to be deployed, the next step is to define "who" needs access ("why") to "what" and "when." Following zero trust principles, RBAC and A&A controls deployed across your architecture will complete this job.

OT Security Specification — This has been mentioned several times, but it is important to note that security for ICS/OT systems bears unique characteristics. Chief among them are safety and availability. Zero trust security controls cannot compromise the safety of a control scenario and cannot negatively alter dependent performance characteristics (like network throughput, response time, and control loop timing). As zero trust functions are implemented, remember what is unique about ICS/OT.

Conclusion

When implementing a control solution using components based on 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.

While it takes time to fully deploy, the cost-saving impact of zero trust becomes evident almost immediately and continues to grow as it becomes fully integrated into a cybersecurity strategy. 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 here, 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. However, deploying zero trust is not easy and often requires a shift in an organization's philosophy and culture regarding cybersecurity.

References

National Institute of Standards and Technology. (2022, May 6). Planning for a zero trust architecture. NIST Cybersecurity White Paper. Retrieved July 1, 2024, from https://csrc.nist.gov/publications/detail/white-paper/2022/05/06/planning-for-a-zero-trust-architecture/final

World Economic Forum. (2022). The zero trust model in cybersecurity. Retrieved July 1, 2024, from https://www3.weforum.org/docs/WEF_The_Zero_Trust_Model_in_Cybersecurity_2022.pdf

Cybersecurity and Infrastructure Security Agency. (2023, April). Zero trust maturity model (Version 2). Retrieved July 1, 2024, from https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf

National Institute of Standards and Technology. (2022, February). Zero Trust Architecture (NIST Special Publication 800-207). Retrieved July 1, 2024, from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

National Institute of Standards and Technology. (n.d.). Executive Order 14028: Improving the Nation's Cybersecurity. Retrieved July 1, 2024, from https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity

Nozomi Networks. (n.d.). OT network segmentation for cyber resiliency. Retrieved July 1, 2024, from https://www.nozominetworks.com/blog/ot-network-segmentation-for-cyber-resiliency

Authors/Titles:
*(Alphabetical by last name)**

Michael Chaney, former Program Manager at Idaho National Laboratory

Danielle Jablanski, OT Cybersecurity Strategist, Nozomi Networks

Andrew Kling, VP Cybersecurity, Schneider Electric

Robert Pingel, OT Cybersecurity Strategist, Rockwell Automation

*Special Note: In Memoriam of Michael Chaney (Idaho National Labs) who contributed to this paper. The 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.