Zero Trust in OT: Challenges and Opportunities in a High-Stakes Environment

Introduction

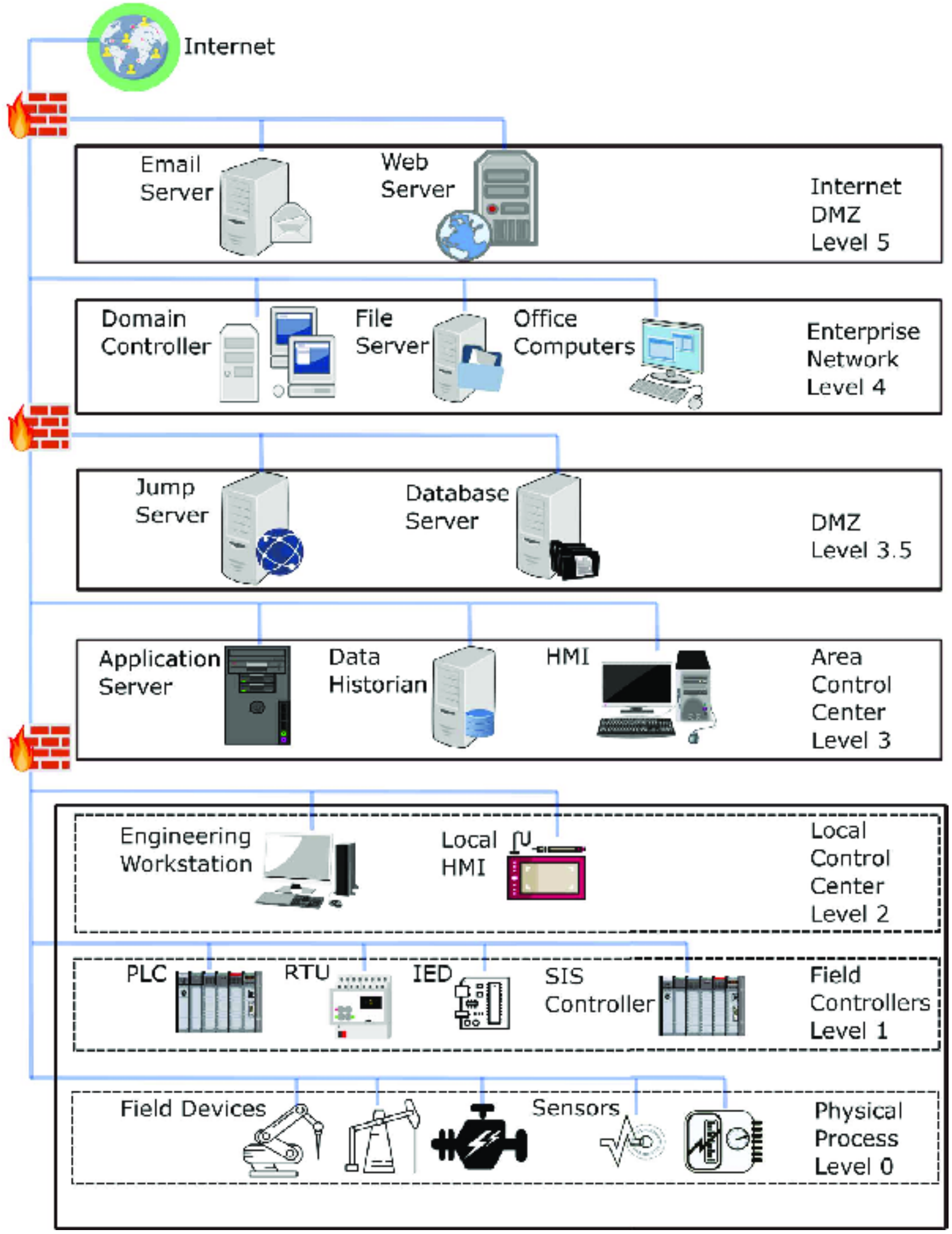
The convergence of Operational Technology (OT) and Information Technology (IT) has blurred traditional network boundaries, exposing critical infrastructure to a wider range of cyber threats. Nation-state actors, such as those attributed to China in the recent Volt Typhoon campaign, and criminal syndicates are increasingly targeting OT/IoT systems to disrupt essential services, steal sensitive data, and even cause physical damage. Examples of such attacks include:

- **Volt Typhoon:** This campaign, attributed to a Chinese state-sponsored actor, targeted critical infrastructure in the US, particularly in Guam, with the apparent goal of disrupting communication networks and critical infrastructure in the event of a future crisis.
- **Attacks on Ukraine:** The ongoing conflict in Ukraine has seen a surge in cyberattacks against critical infrastructure, including the power grid and communication networks, highlighting the vulnerability of OT systems in geopolitical conflicts.
- **US Water Treatment Facilities:** Multiple incidents targeting water treatment plants in the US, such as the 2021 attack on a Florida facility, demonstrate the potential for cyberattacks to disrupt essential services and endanger public safety.
- **Colonial Pipeline:** The 2021 ransomware attack on Colonial Pipeline crippled fuel distribution across the US East Coast, underscoring the economic and societal impact of OT breaches.

These attacks demonstrate the urgent need for robust cybersecurity measures in OT environments. Zero Trust, a security framework that assumes no user or device can be trusted by default, offers a promising approach to mitigating these threats. However, implementing Zero Trust in OT presents unique challenges that differ significantly from IT environments.

Purdue Model for ICS Network Security

The Purdue Model is a structured framework for segmenting Industrial Control Systems (ICS) networks to enhance security. It divides the network into hierarchical levels, each with specific functions and security requirements.



Purdue Level	Description
Connectivity to Enterprise Network:	A secure connection is established between Level 5 and the enterprise network, typically through a demilitarized zone (DMZ) with additional security measures like firewalls and intrusion detection systems.
Level 5: Enterprise Network	*Devices*: Corporate IT systems, Email servers, Internet access *Connectivity*: Connected to Level 4 business planning systems and external networks
Level 4: Business Planning and Logistics	*Devices*: Enterprise Resource Planning (ERP) systems, Supply chain management systems *Connectivity*: Connected to Level 3 manufacturing operations systems and Level 5 enterprise systems
Level 3: Manufacturing Operations and Control	*Devices*: Manufacturing Execution Systems (MES), Production scheduling systems, Data historians *Connectivity*: Connected to Level 2 supervisory systems and Level 4 business planning systems
Level 2: Supervisory Control	*Devices*: Supervisory control and data acquisition (SCADA) systems, Historians, Engineering workstations *Connectivity*: Connected to Level 1 controllers and Level 3 manufacturing operations systems
Level 1: Basic Control	*Devices*: Programmable Logic Controllers (PLCs), Remote Terminal Units (RTUs), Human-Machine Interfaces (HMIs) *Connectivity*: Connected to Level 0 devices and Level 2 supervisory systems
Level 0: Physical Processes	*Devices*: Sensors, actuators, drives, motors, robots *Connectivity*: Direct connection to Level 1 controllers

Security Measures:

- Firewalls: Deployed between levels to restrict traffic flow and prevent unauthorized access.
- Intrusion Detection/Prevention Systems (IDPS): Monitor network traffic for malicious activity and block or alert on suspicious events.
- Data Diodes: Allow one-way data flow from lower to higher levels, preventing data manipulation or exfiltration from higher levels.

Challenges of Implementing Zero Trust in OT

1. **Legacy Systems and Long Lifespans:** OT environments often rely on legacy devices with long lifespans, limited processing power, and outdated operating systems. These devices may not support modern security protocols or be compatible with Zero Trust solutions.

2. **Specialized Protocols and Equipment:** OT networks utilize specialized protocols, such as Modbus and DNP3, which may not have built-in security features. Additionally, specialized equipment may lack the ability to implement essential Zero Trust components like encryption and multi-factor authentication.

3. **Physical Impacts:** Unlike IT systems, attacks on OT can have direct physical consequences. Compromising a control system in a power plant or manufacturing facility can lead to equipment malfunction, production disruptions, and even physical damage. In these environments, the risk of operational impact commonly outweighs the risk from security concerns.

4. **Limited Vendor Support:** The OT security landscape is characterized by a limited number of vendors offering security solutions tailored to specific protocols and equipment. This can make it challenging to find compatible Zero Trust solutions.

5. **Limited Capabilities to Support Zero Trust Frameworks:** While Zero Trust frameworks exist for IT environments, they are just beginning to be developed for OT environments, and the guidance and standards specifically designed for OT implementations are challenged by limited device support for many advanced zero trust tenants.

6. **Engineering Workstations and Remote Access:** Engineering workstations and remote access points are often critical for managing OT systems. These can become entry points for attackers if not adequately secured within a Zero Trust framework.

Benefits of Zero Trust in OT

Despite the challenges, implementing Zero Trust in OT offers significant benefits:

1. **Reduced Attack Surface:** By applying the principle of least privilege and micro-segmentation, Zero Trust limits the lateral movement of attackers, minimizing the impact of a breach.

2. **Enhanced Resilience:** Zero Trust architectures can be designed to be more resilient to failures, as they do not rely on a single point of failure.

3. **Improved Visibility and Control:** Zero Trust provides greater visibility into network activity and allows for granular control over access to critical systems.

4. **Alignment with Manual Processes:** OT environments often have well-established manual processes and procedures that can serve as a backup in case of cyberattacks. Zero Trust can complement these existing practices.

5. **Network Segmentation:** OT equipment is often inherently segmented by its function and location, making it well-suited for the micro-segmentation principles of Zero Trust.

ATARC Zero Trust OT Lab

As participants engage in the ATARC Zero Trust OT Lab (Lab) it is paramount they understand the lab's intent: demonstrating the fully integrated Zero Trust principles within an OT environment. The lab is not a platform for demonstrating niche solutions and then linking those solutions to isolated areas of Zero Trust. This lab is meant to support proofs of concept for integrated solution sets, possibly incorporating multiple vendors' products, implementing Zero Trust solutions in a simulated production environment.

Participants should look to DoD's Zero Trust Reference Architecture and CISA's Zero Trust Maturity Model as the key references for their integrated solutions. Participants should not be constrained by the IT-focus of these documents but are challenged to modify and implement solutions that meet the spirit of these guides within the OT context. Similarly, participants need not look to demonstrate the highest level of Zero Trust maturity but show how their solution set can evolve to support full maturity.

Use cases provide additional reference points. Again, the lab is not a platform for demonstrating how a single product fits within the context of the provided use cases but how an integrated solution set addresses the use cases in toto. Participants' must submit the following:

- How their integrated solution addresses the Zero Trust pillars and capabilities,
- The maturity level their integrated solution achieves as defined in Reference 2; and
- At a high level, how the integrated solution addresses the provided use cases.

These submissions will be screened in advance to ensure Lab resources are not expended inappropriately and to avoid wasting possible participants' time. Integrated solutions should address the full scope of the provided scenarios, perhaps not at the highest maturity level but touch all aspects of the scenarios. If vendors have solutions that address only limited aspects of the scenarios, they should seek to partner with other vendors or an integrator so a total solution will be proven in the Lab.

Use Case Scenarios

The intended outcome of presentations is to validate innovative, efficient, and effective zero trust activities to reduce risk in OT network, system, devices. Many in government have stated Zero Trust cannot or is too burdensome to be applied to OT. Industry will prove otherwise in scenarios representative of common OT, i.e., security, facility, manufacturing, logistics, medical, etc. environments.

Notes

- The Purdue model is useful to describe the challenges and classify issues that exist in Operational Technology environments and is broadly although not universally recognized.

- Use of the Purdue model is intended to challenge and focus the use cases on the OT environments. Feel free to suggest and apply other frameworks that achieve the underlying cybersecurity goals of the scenario. Please cross-reference your chosen model to the Purdue as applicable.
- While ATARC has intentionally focused on key areas of risk and chosen to not make specific reference to NIST IOT/OT-related standards or Zero Trust models. However, these documents were part of the development process and did inform the specific use cases. If specific standards or models inform your approach to these use cases, please make them explicit in your presentations and demonstrate how you used them in your design to achieve the tenants of Zero Trust.

Assumptions

- Demonstrated solutions will focus on protecting the operational environment (Purdue levels 3.5 and below) as this the current gap from the earlier phases that focused exclusively on protecting IT solutions. **Solutions that only cover the IP protocol and will not be sufficient.**
- The primary method for controlling OT environments will focus on user authentication and authorization and network segmentation, both between IT and OT networks, but also within the OT environment.
- 100% "air-gapping" of OT environments is rare, making comprehensive asset discovery and boundary definition critical.
- There may be a very limited ability within OT devices to handle different user roles, but this is typically handled through compensating controls and continuous monitoring.
- Modern security techniques such as encryption and multi-factor authentication are not supported by many OT devices and protocols.
- Vendors often support devices and configurations remotely and these connections need to be managed and secured.
- A "deny-all, permit by exception" approach is critical to securing OT environments.
- Employ the concept of least privilege to restrict access and required software to the minimum required for task execution.

Capability 1: Protecting Network and Purdue-level Segmentation

Scenario 1a: Discover and Classify Assets

[1a.1] Demonstrate the capability to discover and identify devices across IT and OT environments, regardless of protocol or physical connection (e.g. IP, MODBUS, or serial connection). [1a.2] Include the ability to identify known, wn, and transient devices. [1a.3]Ensure data / decision displays include logical and geospatial information.

Scenario 1b: Boundary Definition

[1b.1] Demonstrate the capability to classify and organize the asset inventory by network connectivity, Purdue level and role. [1b.2] Show how this inventory organization comprehensively identifies the boundaries of OT and IT networks so network-level policies and enforcements can be planned, implemented, and audited. [1b.3] Map and classify networks by showing physical and logical connections. [1b.4] Clearly identify important devices and communication paths that represent the greatest risk. [1b.5]Ensure data / decision displays include logical and geospatial information.

Scenario 1c: Network Segmentation/Separation

[1c.1] Demonstrate the capability to consume, design and implement policies to enforce the secure segmentation[1] of OT environments. [1c.2] Demonstrate how the solution monitors and restricts protocols based on OT security guidance from CISA: discover and identify insecure protocols, encryption, etc. [1c.3] Demonstrate how connections across Purdue levels are monitored and automatically enforced in real-time (e.g. Ensure that specific management stations only have access to specific devices at specific times). [1c.4] Highlight where controls cannot be enforced and require human processes and/or compensating controls. [1c.5]Ensure data / decision displays include logical and geospatial information.

Scenario 1d: Network Response

[1d.1] Demonstrate the capability to log, alert and automatically respond to network communications that breach policies. Include examples at the OT/IT boundary and deeper within the Purdue levels. [1d.2] At various Purdue levels, highlight examples of deny-by-default approach while maintaining operational ability. [1d.3] Highlight where controls cannot be enforced and require human processes and/or compensating controls. [1d.4]Ensure data / decision displays include logical and geospatial information.

Capability 2: Enabling Identity-aware Controls in Real-time

Scenario 2a: Identify User and Non-person Entity Accounts

[2a.1] Demonstrate a solution that can comprehensively track accounts across use cases and roles. The solution should identify both human and machine-level accounts and include those managed with IT / IT-like assets in the upper Purdue levels as well as accounts within level-0, level-1 systems. [2a.2]Ensure data / decision displays include logical and geospatial information.

Scenario 2b: Manage Accounts and Enforce Access

[2b.1] Demonstrate the capability to consume, design and implement policies to enforce separation and management of roles. Showcase how the solution allows RBAC by a combination of device features or processes (e.g. manufacturer, physical location, activity).

[1] Segmentation here is used descriptively and is not intended to imply a specific technology. Use any method that achieves Zero Trust isolation (e.g. micro-segmentation, cloaking, etc).

[2b.2] Show how user and entity access and change requests are enforced and logged. [2b.3] Highlight where controls cannot be enforced and require human processes and/or compensating controls. [2b.4]Ensure data / decision displays include logical and geospatial information.

Scenario 2c: Implement MFA

[2c.1] Implement a secure access method that enforces MFA, integrates with the user & network solutions above and supports on-prem, remote, staff, & contractor roles. [2c.2] Demonstrate how the solution might handle both user and NPE accounts. [2c.3] Highlight where controls cannot be enforced and require human processes and/or compensating controls. [2c.4]Ensure data / decision displays include logical and geospatial information.

Scenario 2d: Vendor Access

[2d.1] Demonstrate the discovery and control of vendor initiated external access. [2d.2] Show the ability to automatically enforce controls for providing access to specific vendors. Include examples that allow admin to restrict access to specific devices and at specific times. [2d.3] Demonstrate how all requests and changes are logged. [2d.4]Ensure data / decision displays include logical and geospatial information.

Scenario 2e: Support Emergency Requests and Temporary Access

[2e.1] Demonstrate a secure access process where additional rights are granted for a specific time to an existing user. Maybe an individual is going on vacation and needs to authorize a backup resource for a week. [2e.2] One scenario should have an engineer request elevated access as part of a critical response that an administrator approves. [2c.3]Ensure data / decision displays include logical and geospatial information.

Capability 3: Stateful Monitoring & Recovery

Scenario 3a: Discover and collect configuration information

[3a.1] Demonstrate a capability that discovers and collects configuration information across the key components of the OT environment, including IT-like, OT systems, and infrastructure devices. [3a.2] Show how the approved baselines for the expected state are identified and protected. [3a.3]Ensure data / decision displays include logical and geospatial information.

Scenario 3b: Monitor environment for changes

[3b.1] Demonstrate the ability to detect state change on OT equipment and compare that to the expected baseline state and highlight changes. [3b.2]Ensure data / decision displays include logical and geospatial information.

Scenario 3c: Restore configuration to known good baseline

[3c.1] Demonstrate the ability to restore device configurations to a known good state if an unauthorized or unintended change is detected. Include scenarios for monitoring approved changes and alerting and/or blocking changes that are against policy, e.g. wrong user pushing a change, a change being pushed out of normal processes, wrong device requesting changes. [3c.2]Ensure data / decision displays include logical and geospatial information.

Scenario 3d: Device Composition & Supply Chain Risk

[3d.1] Decompose OT device inventory with additional content on hardware, software and firmware makeup including both open source and commercial modules and demonstrate the ability to highlight devices affected with a specific vulnerability. [3d.2] Demonstrate the ability to identify and alert on the issue, as well as show the ability to remediate and/or mitigate risk. [3d.3]Ensure data / decision displays include logical and geospatial information.