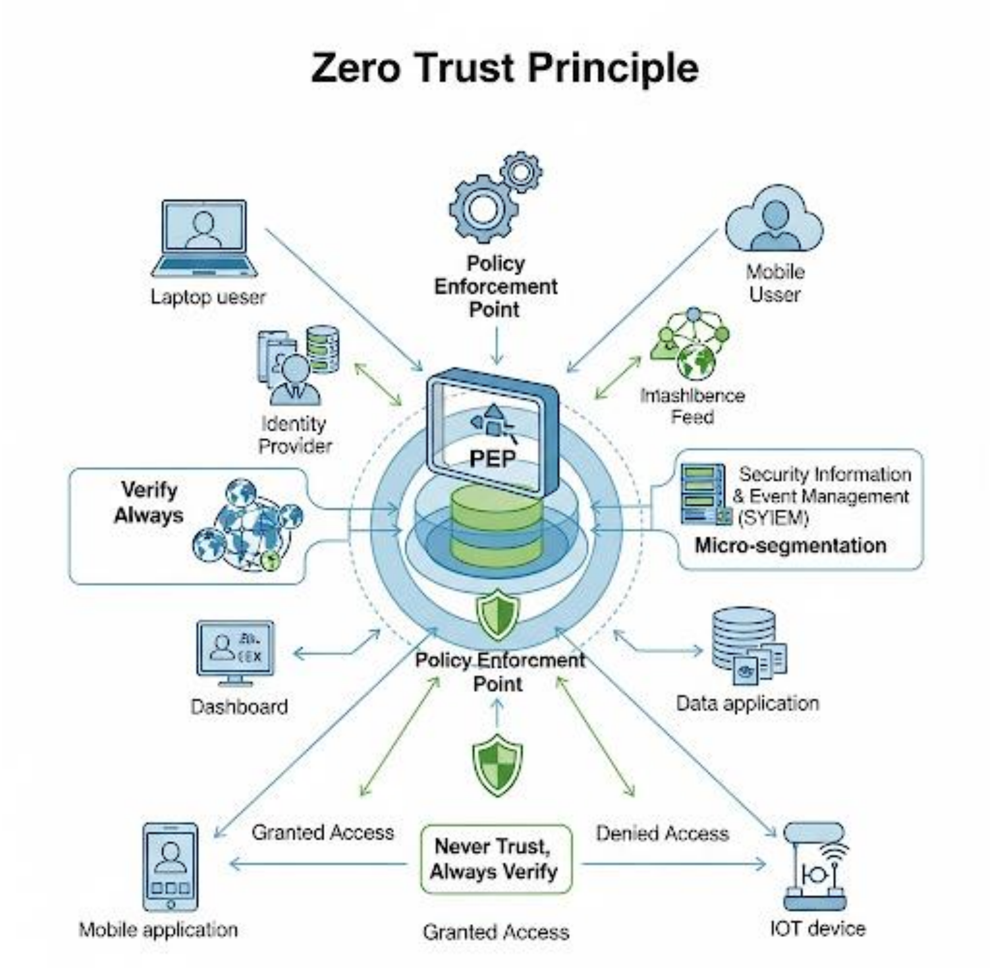
August 2025

Yosi Shavit MBA, CISO, CISM, CDPSE , CC– Information Security & ICS Cyber Expert

The Zero Trust Principle – How It Is Applied in the OT Domain and Industrial Control Systems



Introduction

In this article, I will briefly describe the general concept of the **Zero Trust** principle then, I will delve into how this model applies specifically to **Industrial Control Systems (ICS)** and **Operational Technology (OT)** environments. Later in the article, I will also connect the topic to the **hazardous materials domain**, where such materials are managed or controlled through industrial control systems.

What is the Zero Trust Principle in the Cybersecurity Domain?

Zero Trust Principle is the idea that no user, device, or system should be trusted by default, even if it is inside the organization's network.
Instead of assuming trust based on network location, Zero Trust enforces continuous verification, strict access controls, and least-privilege access at all times. Its goal is to reduce the attack surface, prevent lateral movement, and detect threats early by assuming that threats may already exist within the network.

The Main Challenge: Why Is Zero Trust needed in ICS?

The traditional OT model relied on an "air gap" or physical perimeter protection, which has become less effective in the age of connected networks and insider threats.

The assumption that "anyone inside the network is trusted" is no longer valid: a breach into the network can enable uncontrolled lateral movement, especially within SCADA and DCS systems that control physical processes.

Zero Trust Principles in OT / ICS Environments

Here are several principles of the Zero Trust approach in industrial control environments**:**

- **Never trust – always verify**: Every access request is continuously validated, even if it originates from inside the network.
- **Least Privilege Access**: Users and devices are granted access only to the specific resources necessary for their function.
- **Micro-Segmentation**: Networks are divided into smaller zones and subnets to limit lateral movement by attackers.
- **Context-Aware Access**: Access decisions are based on contextual factors such as device type, geographic location, working hours, etc.
- **Centralized Policy and Consistent Enforcement**: A unified and comprehensive policy framework is applied consistently across the network and systems.
- **Continuous Monitoring and Shared SIEM for IT and OT**: Event analysis and full activity logging should be integrated across both IT and OT environments.

Guidelines for Implementing Zero Trust in ICS

Here are some guidelines**:**

- **Avoid assumptions of a trusted network**: ICS identities and assets may not be current or fully reported.
- **Initiate segmentation**: If physical separation isn't possible, establish smaller logical segments.
- **Identify and block resources with unknown access**, such as cellular modems or unsecured remote access solutions.
- **Use controlled jump servers**, enforce **Multi-Factor Authentication (MFA)**, and implement access management systems for ICS connectivity.
- **Deploy unidirectional gateways** to enable outbound-only data flows and prevent inbound disruptions.

- **Integrate organizational processes**: Foster collaboration and a unified language between IT and OT teams, with clearly defined responsibilities.

Challenges in Implementing Zero Trust in ICS

- **Legacy operational systems** that do not support authentication or encryption.
- **Implementing encryption or access control** may introduce delays and impact real-time reliability - a critical concern in industrial control.
- **Heterogeneous infrastructures** with components from multiple vendors and undocumented legacy maintenance practices.
- **Cultural gaps between OT and IT teams** hinder a common language and effective collaboration.

Why Zero Trust Is Critical in OT Networks Handling Hazardous Materials?

- **Tangible Physical Threats**

Control systems in industries such as petrochemicals, energy, wastewater treatment, hazardous transportation, or regulated food production directly manage **toxic, flammable, explosive, or polluting substances**.

Any breach or deviation in control data (temperature, pressure, flow, PH values) can lead to:

- **Explosions or fires** (due to gas ignition or leaks),
- **Widespread environmental contamination**,
- **Harm to nearby populations** (residential areas, public roads),
- And even **loss of life**.

- **Use of Outdated and Insecure OT Technologies**

Protocols like **Modbus, OPC-DA, and DNP3** are widely used to control industrial systems, but were designed **without encryption, authentication, or access control mechanisms**.

Controllers such as **PLCs, RTUs,** and **HMIs** stations as well, are often deployed without support for standard security updates.

Zero Trust provides protection even when hardware upgrades are not feasible.

How Zero Trust Protects OT Environments Handling Hazardous Materials (HazMat)

Micro-Segmentation Based on "Protect Surfaces"

- Logical segmentation of critical zones:
  - A zone managing **tank temperature**
  - A zone monitoring **flammable material pipelines**
  - A zone with access to **emergency operation components** (safety relays, ESDs).
- Each zone is protected by **independent policies**: only **authenticated users** with **specific functions** can issue commands.

Strict Authentication for Devices, Workstations, and Users

- Users attempting to modify industrial parameters (e.g changing a pressure threshold) must undergo **two-factor authentication** and **context analysis**:
  - Is this a trusted station?
  - Is the access happening at a normal time?
  - Does the user have proper privileges?

Access Rules Based on Risk and Profile

- Example: Even a control engineer may only access critical systems if:
  - They are not connected via a public VPN
  - Logged in from a secured workstation
  - No anomalous activity is detected via SIEM
  - No **ongoing cyber incident** is active in the plant.

Practical Example:

A chemical fertilizer manufacturing plant

- Substances such as **ammonia, nitric acid, or chlorine** are stored in tanks, flow through pipelines, and are managed by SCADA systems.
- If an attacker breaches the network and changes the **tank temperature above 70°C**, this could trigger an **explosion risk**.
- With Zero Trust implemented:
  - The **temperature control system** will filter out commands not coming from a **signed and authorized user**.
  - **Communications are encrypted** – commands cannot be injected.
  - **Real-time monitoring** through SIEM/OT-SOC detects anomalies and **automatically blocks suspicious activity**.

Summary and Recommendations

1. Zero Trust is not just a security framework, it is a critical infrastructure for the survival of industrial systems.
2. Especially in HazMat facilities, it is unacceptable to assume that "nothing will happen" - the potential for disaster demands continuous monitoring and controlled access at all times.
3. Key considerations include:
   - Segmentation based on attack surfaces
   - Real-time protection of data flows
   - Physical and logical separation of control stations
   - Use of MFA, jump servers, and NDR (Network Detection & Response).

Yosi