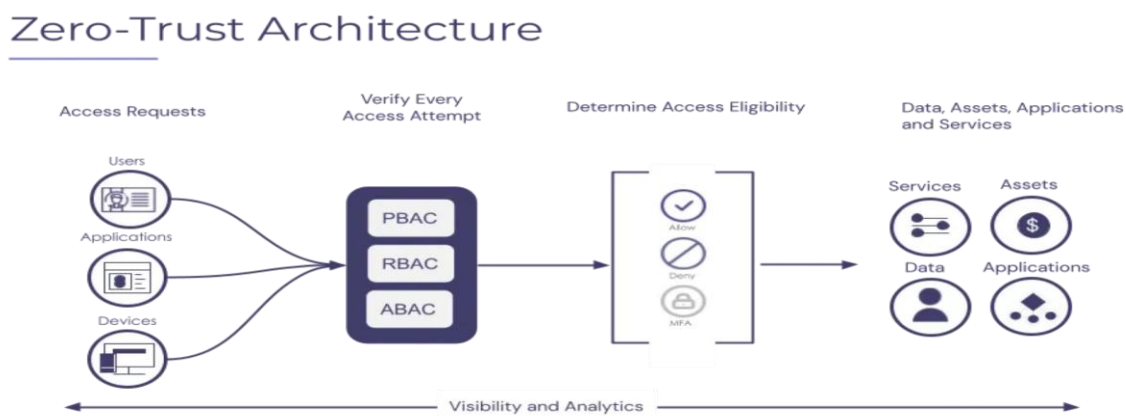
Zero Trust Architecture for Securing Industrial Networks in the Era of IIoT and Industry 4.0



Student Name: Kamal Al-Rawafi
Supervisor: Dr.Khaled Taher Al-Hussaini
Department: of Mechatronics
University: Dhamar University
Date: September 20, 2025

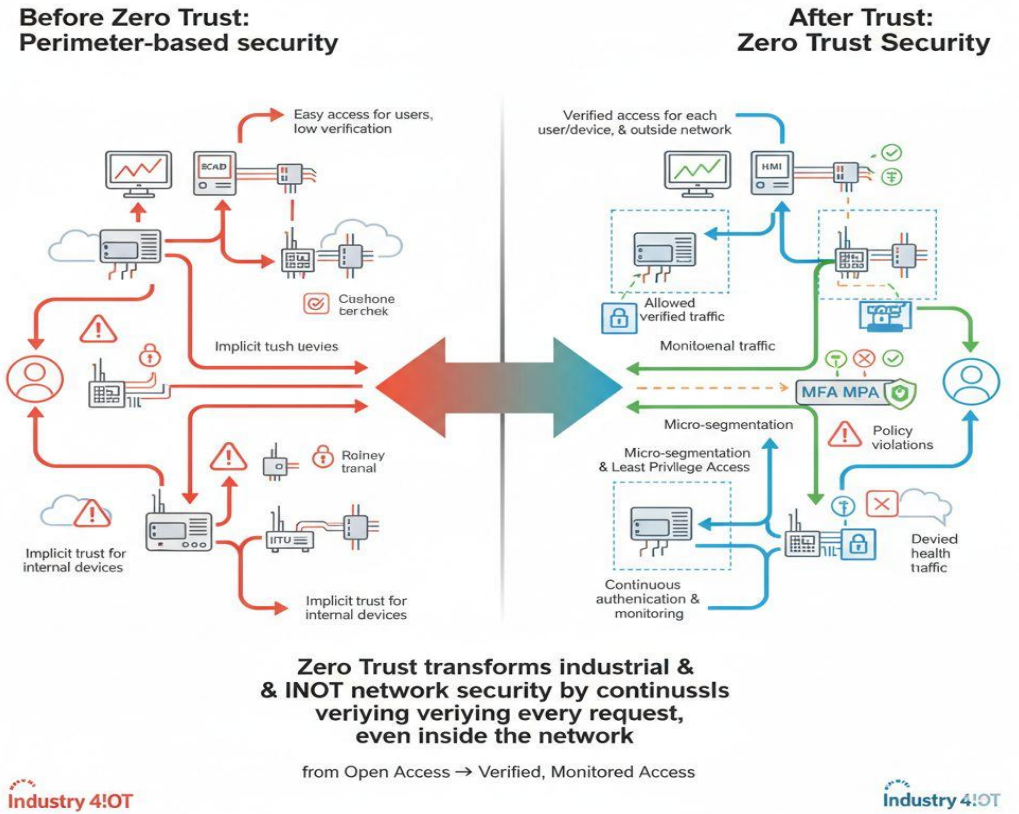
Introduction

◇ With Industry 4.0 and IIoT networks have become more interconnected and more vulnerable to attacks.

◇ Traditional security such as firewalls is no longer enough to protect industrial networks.

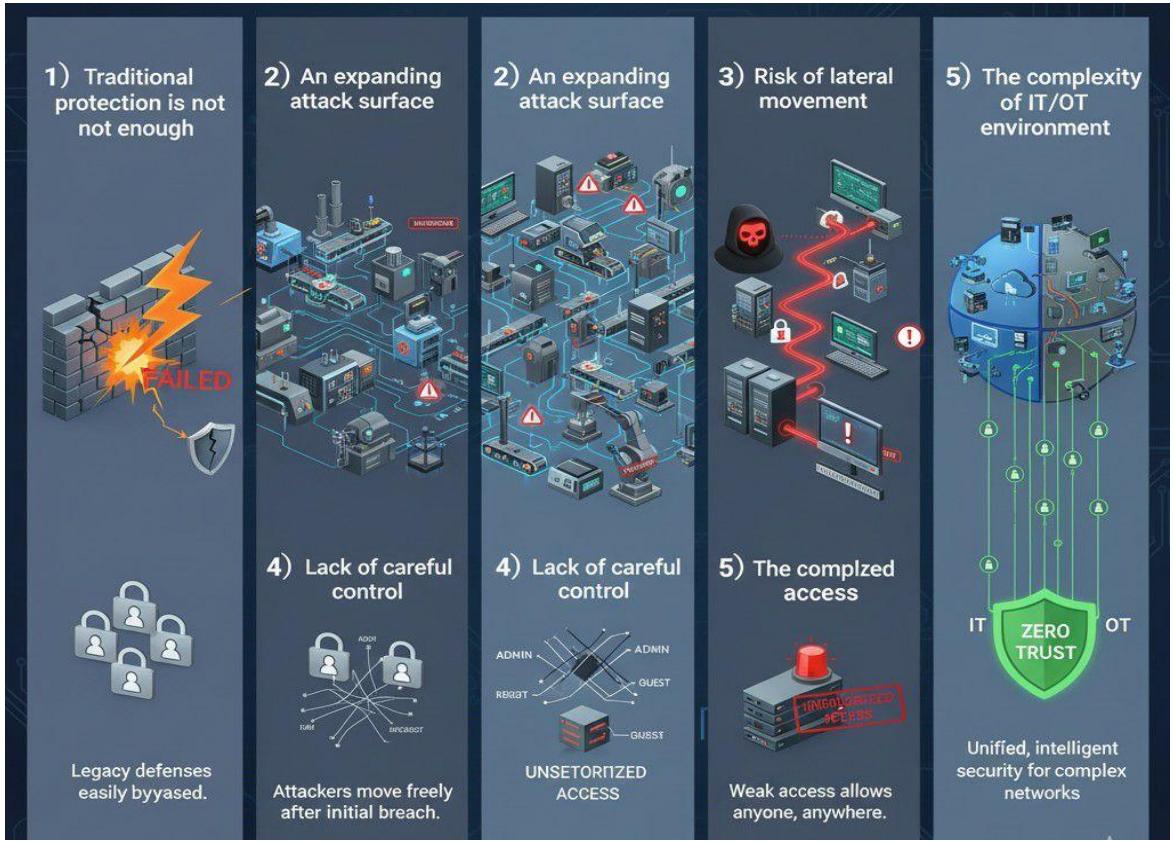
◇ Zero Trust Architecture: no prior trust, permanent verification, and limited powers.

◇ In this presentation we will discuss: the problem, objectives, significance, scope, theoretical basis, challenges, and solutions.



Research Problem

- Traditional protection is no longer effective for industrial networks.
- Outdated devices expand the attack surface.
- Attackers move laterally once inside the network.
- Weak authentication and control increase risks.
- Complex IT/OT environments require a smarter model like Zero Trust.



Strategic Objectives

1. Analysis of cyber threats.

2. Evaluation of the ZTA application.

3. Identify implementation challenges.

4. Custom ZTA framework proposal.

5. Study of benefits and impact.

6. Make practical recommendations.

Importance of Research & Zero Trust Security for Industrial Networks:

- Protect critical infrastructure and essential services.
- Defend against evolving cyber threats with continuous verification.
- Secure identities & access to prevent unauthorized entry.
- Ensure business continuity and support safe digital transformation.

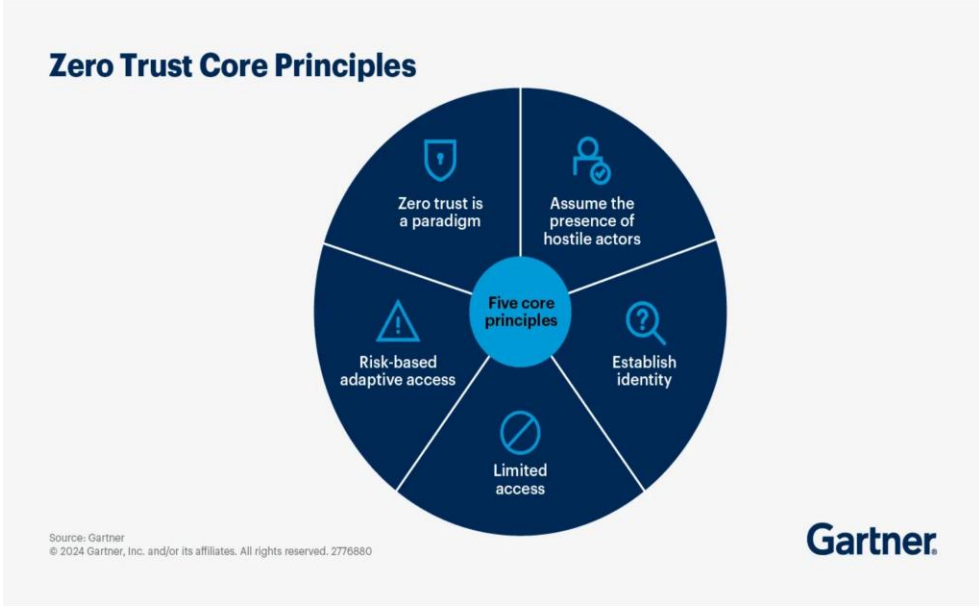
The Principle of Zero Trust

"Never trust, always verify"

The core principle that challenges traditional security models

Key Principles:

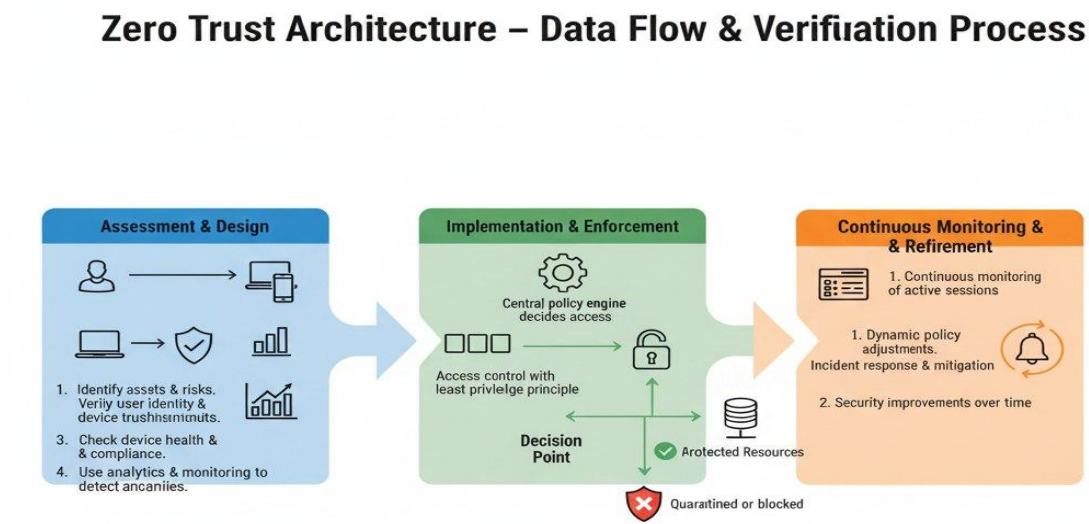
- No trust... Always check.
- Declare and record each access.
- Constant verification during the session.
- The lowest possible validity.
- Network section (Microsegmentation).
- Access is by context.
- Every traffic is suspicious



Zero Trust Architecture

Principle: Never Trust, Always Verify.

- Assessment & Design: Identify risks, verify users/devices, check compliance.
- Implementation & Enforcement: Policy engine controls access, least privilege, allow or deny.
- Monitoring & Refinement: Continuous monitoring, adjust policies, incident response, improve security.



Zero Trust Features and Disadvantages :

Features / Advantages:

- Strict policy-based access.
- Strong user/device authentication.
- Continuous device health checks.
- Network microsegmentation.
- Fine-grained, context-aware access control.

Disadvantages / Challenges:

- Complex implementation.
- High resource and expertise demand.
- Potential user frustration.
- Difficult integration with legacy systems.

Uses of Zero Trust

Securing Remote Access

Ensuring secure access to industrial resources from any location without traditional VPN vulnerabilities

Protecting Cloud Environments

Securing access to cloud-based industrial applications, data, and services

Industrial IoT Security

Granular access control for countless interconnected devices and machine-to-machine communications

OT/IT Convergence

Bridging security gaps between IT and OT networks to protect critical infrastructure

Why Zero Trust Works

Elimination of Implicit Trust

Removes the biggest vulnerability of traditional security: the assumption that internal network traffic is safe.

Reduced Attack Surface

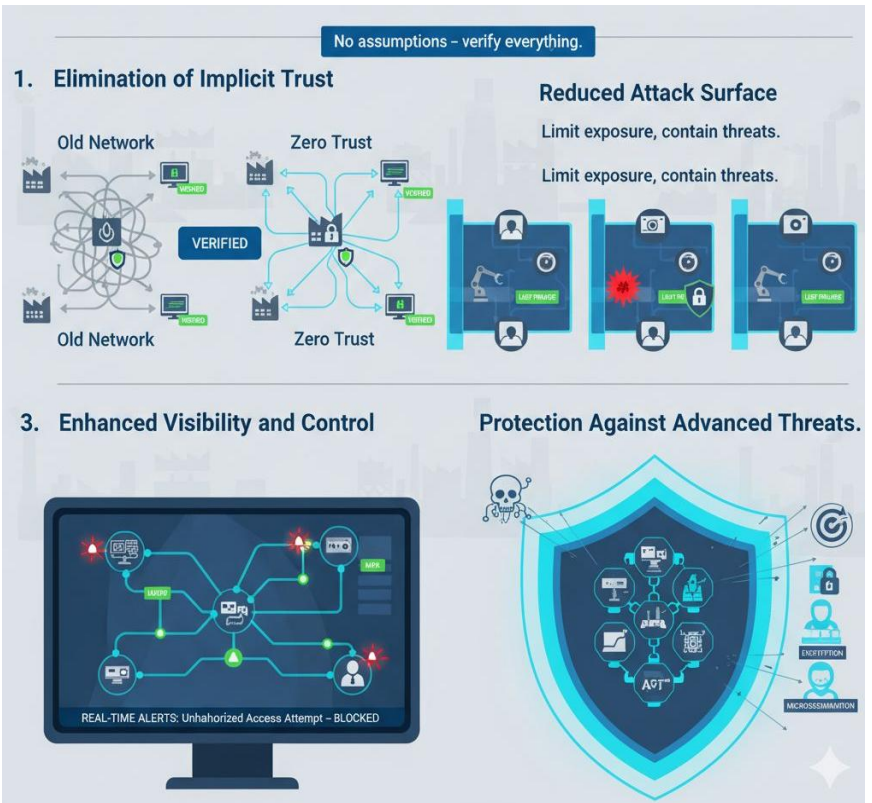
Microsegmentation and least privilege access limit lateral movement, containing breaches effectively.

Enhanced Visibility and Control

Continuous monitoring provides deep insights into all network activities, enabling faster threat detection.

Protection Against Advanced Threats

Layered security approach makes it more resilient against sophisticated attacks, including APTs and ransomware.



Challenges Facing Zero Trust

Hybrid-Network Complexity

Integrating disparate legacy OT systems, modern cloud services, and IIoT devices with different protocols and security mechanisms

Legacy System Integration

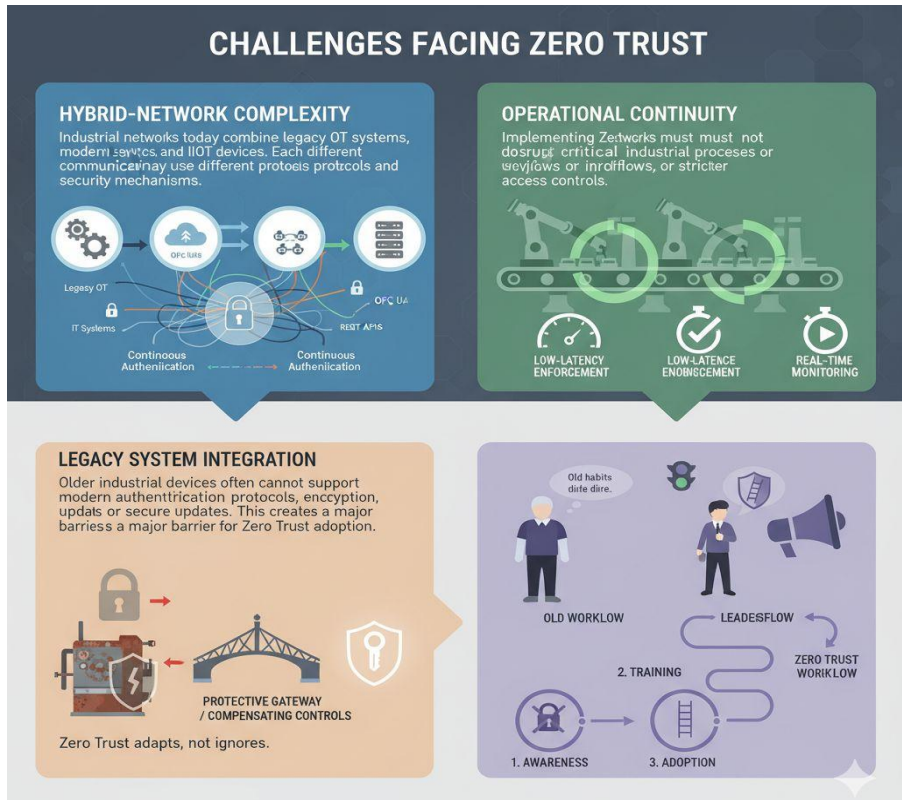
Adapting older devices that cannot support modern authentication protocols or encryption

Operational Continuity

Implementing security without disrupting critical processes or introducing unacceptable latency

Cultural Resistance

Overcoming organizational resistance to new security paradigms and workflows



Summary:

With the transformation of IIoT and Industry 4.0, industrial networks are becoming more interconnected and vulnerable to attacks, and traditional models are no longer enough. The Zero Trust Architecture is based on the principle of "Never trust, always check", with precise access control, multi-factor authentication, and constant monitoring, which reduces the attack surface and enhances flexibility, despite the challenges of integration with legacy systems.