EXECUTIVE WHITE PAPER

Zero Trust in OT

From “Air Gaps” to
“Always Verify”.

howest
university of applied sciences

UNIVERSITEIT GENT
CAMPUS KORTRIJK

ICIL4.0 WP2.4

TABLE OF CONTENTS

ZERO TRUST IN OT

INTRODUCTION

FROM “AIR GAPS” TO “ALWAYS VERIFY”

Not long ago, industrial systems lived in their own safe bubble. PLCs and SCADA servers were “air-gapped” – disconnected from the internet. Trust was implicit. But digital transformation, remote work, and IT/OT convergence have punched holes in that bubble. Suddenly, the same threats hitting corporate laptops are knocking on factory doors.

This is where **Zero Trust** comes in: *“Never trust, always verify.”*

THE OLD WORLD VS. THE NEW WORLD

Let's imagine a medieval castle (perimeter defense). Now replace it with an airport (Zero Trust) where every passenger, staff member, and bag is checked continuously – even after entering the terminal.

Old World (Implied Trust):

- Engineers assumed the OT network was safe if it was inside the perimeter.
- Legacy PLCs or HMIs could run for 20+ years without updates.
- Remote access was bolted on via VPNs or jump servers.

New World (Zero Trust):

- Every connection –user, vendor, or machine – must continuously prove it belongs.
- Access is granted based on identity, context, and least privilege.
- Monitoring, segmentation, and policy enforcement become *living processes*, not one-off projects.

DEMONSTRATION

A COMMON REMOTE ACCESS SCENARIO

Let's model this with a realistic OT remote access use case:

1. **Traditional Model**
    - Vendor connects via VPN → jump server → industrial workstation.
    - Weak point: if the VPN or corporate domain is breached, attackers can move laterally into OT.
2. **Zero Trust Model**
    - Remote vendor request → ZTNA broker (USRV/HERA for critical OT)
    - Broker checks identity, device health, time, location.
    - Only the *specific engineering workstation* is exposed, not the entire OT network.

This reduces the attack surface dramatically.

THE SEVEN PILLARS OF ZERO TRUST IN OT

- **Users**: Continuous identity verification and MFA.
- **Devices**: Automated inventory, patching, and monitoring.
- **Applications & Workloads**: Securing on-prem, mobile, and cloud.
- **Data**: Encryption in transit and at rest.
- **Network & Environment**: Segmentation, isolation, granular policy.
- **Visibility & Analytics**: Threat intel, AI/ML-driven detection.
- **Automation & Orchestration**: Fast, automated responses.

GOVERNANCE & CERTIFICATION VIEW

Executives often frame Zero Trust adoption in terms of **certification and governance**.

Here's the process mindset they expect:

1. Management commitment
2. Define scope (NIS2, ISO 27001, IEC 62443)
3. Risk assessment & GAP analysis
4. Implement Zero Trust measures:
    - **People**: Awareness and training
    - **Process**: Policies based on continuous verification
    - **Technology**: IAM, 2FA, JITA, ZTNA, PAM, VLANS
5. Internal audits → external audits → certification

CHALLENGES

Executives should know Zero Trust is powerful, but not magic:

- Legacy OT systems may not support modern identity protocols.
- Safety-critical systems (SIS, triconex) require uninterrupted access.
- Vendor remote access can introduce hidden risks.

That's why many companies start with *quick wins* like network segmentation, local firewalls, PAM (Privileges Access Management), IDS (Intrusion Detection Systems), and OT domain, then expand into ZTNA and SOC (Security Operations Center) monitoring.

CASE STUDY

THE FICTILE TILE FACTORY LAB

A fictitious tile factory lab (FICTILE) demonstrates Zero Trust implementation in OT. The lab features PLCs (Beckhoff, Siemens, Phoenix Contact), HMIs, IIoT devices, and Windows endpoints.

Initial State: Flat network, default credentials, all traffic allowed.

Zero Trust Implementation:

- **Identify**: Asset inventory with an ICS Network Monitoring Tool.
- **Manage**: Centralized identity, MFA.
- **Control**: VLANs, IT/OT segmentation.
- **Protect**: Encryption, least privilege.
- **Detect**: IDS for anomalous traffic.
- **Analyze**: Threat intel risk scoring.
- **Automate & Orchestrate**: Alerts and partial automated response.

Result: Legacy OT can transition from implied trust to a Zero Trust baseline.

ROADMAP

FROM NOW TO 3 YEARS

- **Quick Wins (20–30 days):** Inventory assets, enforce MFA, deploy VLANs.
- **Medium Term (6–12 months):** Implement PAM, IDS/Claroty, segment OT/IT.
- **3-Year Vision:** Zero Trust embedded in audits, SOC operations, and supply chain partnerships.

TAKEAWAY

Zero Trust in OT isn't just a buzzword – it's the mindset shift from "air-gapped and safe" to "always suspect, always verify."

It's not about ripping and replacing legacy systems overnight. It's about **incremental, risk-based steps** that executives can align with NIS2 and ISO 27001 compliance while protecting the business from the very real threats knocking on their factory doors.

By implementing a comprehensive set of zero-trust capabilities in your industrial environment, you will significantly enhance your overall security:

- A full user inventory ensures accurate identity management, while multi-factor authentication strengthens password security.
- Self-managed and hosted identity stores provide better access control and protection.
- Rule-based dynamic access enables fine-grained control, and periodic authentication ensures ongoing verification.
- With full and automated device inventory, you gain visibility and control over your assets.
- Device-based access control prevents unauthorized or untrusted devices from accessing critical resources, reducing the attack surface and minimizing the potential for security breaches.
- A full application inventory allows better management and monitoring.
- Integrated email anti-phishing measures fortify your defenses against social engineering attacks.
- Application access is restricted to authorized users even on public networks.
- Data encryption in transit safeguards sensitive information.
- Macro-segmentation enhances network isolation, and severely impairs malicious actor activities, reducing risk and impact.
- Extended traffic monitoring enables detection of suspicious activities.
- Increased traffic encryption further protects confidentiality and data privacy.
- Extended log collection and analysis using threat intelligence enhance threat detection capabilities.
- Automated threat alerts enable prompt response to potential threats.
- Although partially automated, incident response processes become more efficient.

REFERENCES

THE FOLLOWING SOURCES PROVIDED INSIGHTS OR ARE CITED IN THIS DOCUMENT.

- https://attack.mitre.org/tactics/ics/
- https://vapt.eu/offensive-security/penetration-testing/ics-scada-penetration-testing/
- https://cyberzoni.com/standards/iso-27001/operational-capabilities
- https://waterfall-security.com/ot-insights-center/ot-cybersecurity-insights-center/rethinking-secure-remote-access-to-industrial-and-ot-networks/
- https://www.cci-es.org/en/activities/pocket-guide-cybersecurity-in-the-industrial-automation-pyramid/
- https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-ZTStrategy.pdf
- https://dodcio.defense.gov/Portals/0/Documents/Library/CS-Ref-Architecture.pdf