EXECUTIVE WHITE PAPER

Securely Connect IT and OT Networks

howest
university of applied sciences

UNIVERSITEIT GENT
CAMPUS KORTRIJK

ICIL4.0 WP2.2

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This paper explores the accelerating convergence of Information Technology (IT) and Operational Technology (OT) networks.
The analysis identifies key attack vectors that exploit this interconnectedness, including weaknesses in VPNs, pivoting and lateral movement techniques, session hijacking of web-based tools, and direct compromise of remote client devices. To counter these threats, the paper reviews architectural frameworks and software and hardware solutions.

For corporate and lower-risk environments, it advocates for modern, cloud-based approaches like Secure Service Edge (SSE) and Secure Access Service Edge (SASE), which are built on a Zero Trust philosophy.

For high-consequence OT environments where a breach could have severe physical consequences, it details robust hardware-enforced solutions such as unidirectional gateways, hardware-enforced remote access (HERA), and time-limited physical switches.

The paper concludes that securing the modern industrial enterprise demands a risk-based decision-making process, by classifying assets according to their criticality and the potential consequences of a compromise.

Best practices

- **Reduce broad access**: Replace legacy full network access VPNs with limited access that only connects approved users to specific zones and nothing else. This minimizes blast radius if an account or device is compromised.
- **Segment with purpose**: Enforce “deny by default” between IT and OT, and apply unidirectional hardware boundaries for the most critical systems so attack data cannot flow into the plant, even if software tools fail.
- **Favor hardware-enforced** remote access for high-consequence sites: Options such as one-way screen sharing, time-limited physical switches, or hardware-filtered keyboard/mouse channels materially raise the bar for attackers compared with software-only tools.
- **Treat browsers with caution in OT**: Where browser-based access is necessary, shorten sessions, add strong reauthentication, and monitor for cookie theft and unusual re-use patterns.
- **Assume the endpoint can be hostile**: Continuously check device health, limit privileges, and record/inspect remote actions. If risk is high, require solutions that remain safe even when the helper’s device is compromised.

IT-OT NETWORK INTEGRATION

As industrial organizations embrace digital transformation, the historic divide between information technology (IT) and operational technology (OT) networks is rapidly narrowing.

While cybersecurity traditionally treats IT and OT as separate domains each with its own protocols, tools, and risk priorities their growing interdependence is eroding. As IT systems increasingly support the management, monitoring, and control of OT processes, IT disruptions can have immediate operational consequences. Even cyberattacks confined to IT infrastructure without directly targeting industrial control systems (ICS) can interrupt production if critical OT operations rely on compromised servers, networks, or applications.

This transformation is driven by three key priorities:

1. **Operational Efficiency:** Unifying OT data (e.g., sensor metrics, machine health, production KPIs) with IT analytics enables predictive maintenance, real-time optimization, and faster decisions—minimizing unplanned downtime.

2. **Remote Access:** Secure remote connectivity for vendors, integrators, and IT support eliminates costly site visits, shortens repair times, and maintains 24/7 operations.

3. **Scalability & Flexibility:** Cloud services and SD-WAN simplify new site deployments with minimal hardware, while virtualization and containerization require seamless OT-IT integration for dynamic provisioning and management.

Think of your IT network as the front office and your OT network as the factory floor. In the past, these two areas were almost completely separate. Now, by connecting them, a security problem in the office can spill over and shut down the entire factory. Even if an attack only hits the IT systems, it can halt production if the factory relies on that IT infrastructure to operate.

This integration introduces risks from:

1. **Third-party vendors:** Technicians and partners who need remote access can accidentally introduce threats.

2. **Unsecure devices:** Laptops or other devices connecting to the network might not have the same level of security, creating weak points.

3. **Software flaws:** Vulnerabilities in the software used for remote access can be exploited by attackers to move from the business network into the control systems.

THREAT SCENARIOS

WEAKNESSES IN DIGITAL TUNNELS (VPNS)

A “classic” VPN connection provides broad network access through a single authentication point. When malware infects a remote endpoint connected via VPN, it can immediately traverse the encrypted tunnel to reach internal OT networks, which lack adequate monitoring and feature legacy systems that cannot be easily patched or secured.

A simple malware can rapidly spread across IT to OT.

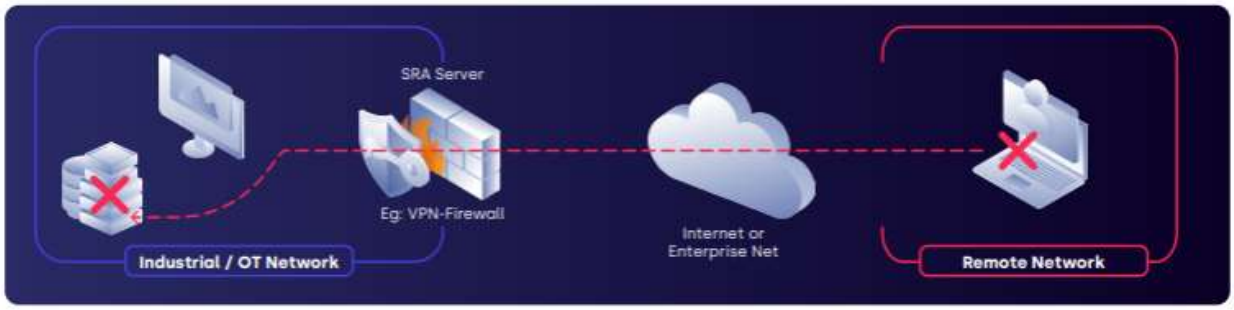

Figure 1 VPN connection to OT network source [2]

PIVOTING ATTACKS

SILENT SPREAD INSIDE THE NETWORK

Modern attackers rarely target systems directly; instead, they employ sophisticated pivoting techniques to move laterally through networks after gaining initial access.

Attackers target central access points like jump servers or cloud remote-access broker so they can move deeper while looking like normal users. They employ built-in Windows utilities, PowerShell scripts, and standard network protocols to conduct reconnaissance and escalate privileges, making their activities difficult to distinguish from normal system administration tasks.

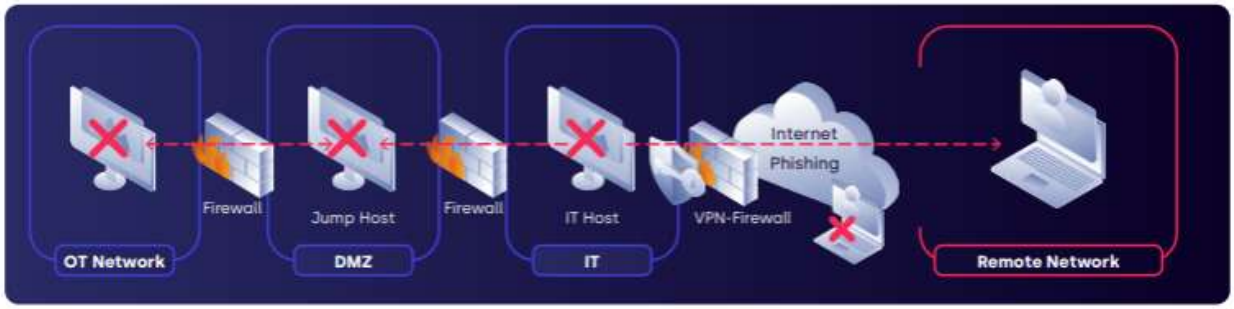

Figure 2 Pivoting attack source [2]

SESSION HIJACKING

TAKING OVER WEB SESSIONS

Browser-based remote access solutions, increasingly popular for their ease of deployment, introduce unique vulnerabilities through session hijacking attacks. Attackers steal temporary login tokens (cookies) and reuse them to impersonate staff.

Attackers can steal these session identifiers through various means, including malicious attachments, cross-site scripting attacks, or by intercepting network traffic on unsecured connections. Once obtained, these cookies allow attackers to impersonate legitimate users, effectively bypassing both password requirements and multi-factor authentication measures. The attack is particularly insidious because the compromised session appears legitimate.

The “Citrix Bleed” flaw is a recent example that enabled ransomware crews like LockBit to hijack sessions, harvest credentials, and spread across networks before launching disruptive attacks [1].

CLIENT-SIDE COMPROMISE

COMPROMISING THE REMOTE LAPTOP ITSELF

The most sophisticated attacks target the remote access clients themselves, employing advanced malware that operates directly on users' laptops or workstations.

These attacks can bypass traditional VPN security measures through techniques such as virtual display manipulation, where malware creates invisible screens to conduct malicious activities while presenting fake error messages to distract legitimate users.

Malware can monitor for active remote access sessions, then hijack control of the connection to perform unauthorized actions in OT environments. These attacks can

bypass VPN split-tunneling protections and other security measures designed to isolate remote access traffic [2].

DEFENSIVE STRATEGIES

Establishing secure IT-OT connectivity requires a fundamental understanding of network architecture principles. This section examines the established frameworks and strategies for secure industrial network design. Like designing a building, they serve as a blueprint.

THE PURDUE MODEL

THE "LAYER CAKE" OF SECURITY

The Purdue Model, developed in the 1990s, remains the cornerstone framework for industrial control system security. This hierarchical model organizes complex ICS environments into distinct levels, creating clear boundaries between enterprise and operational functions.

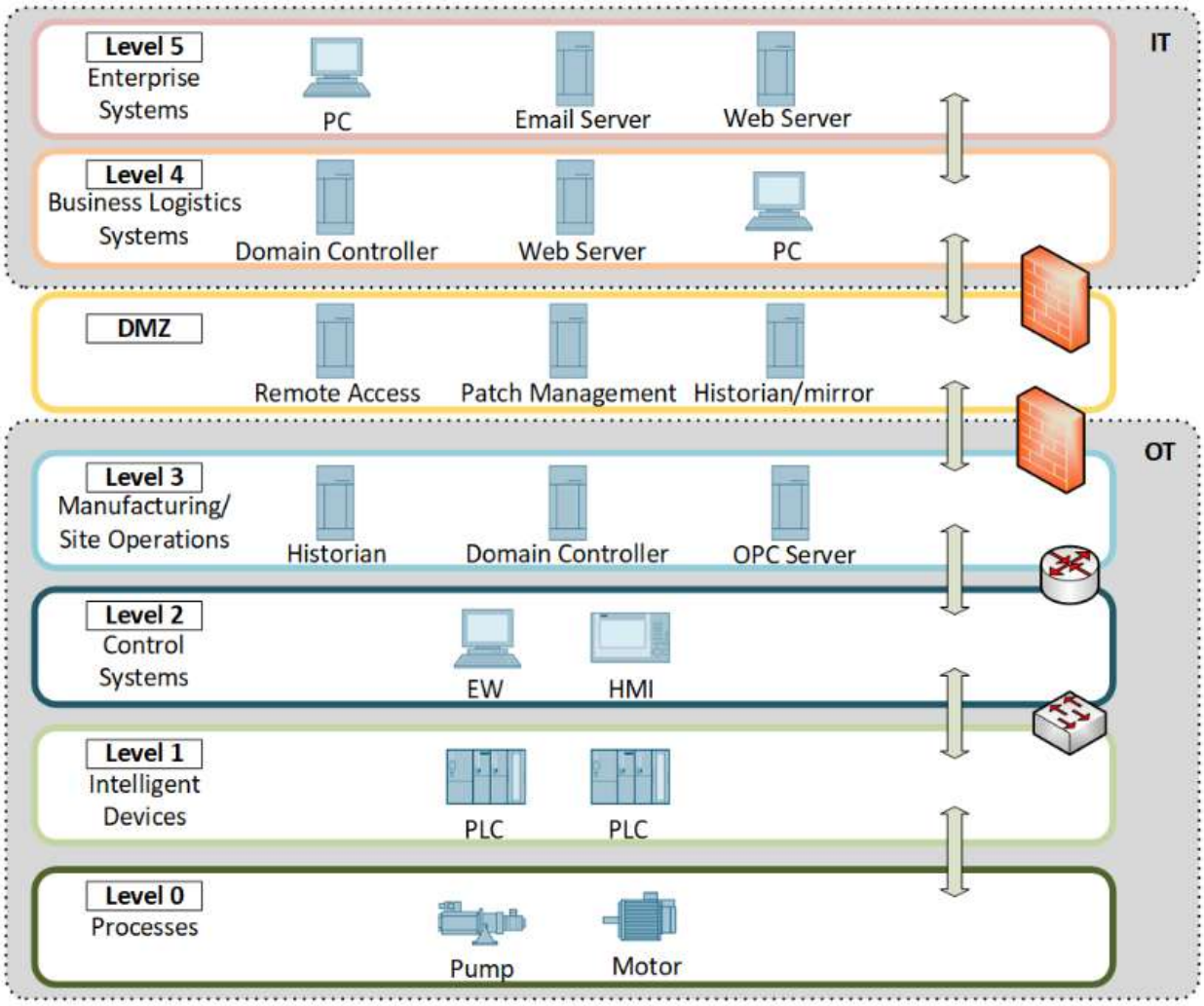

Figure 3 Perdue Model adaptation source [4]

- **Top Layers (The Office):** *Levels 4, 5 in* Figure 4 Perdue Model adaptation source [4]. This is your business network (IT), where you have email, finance systems, and internet access. It's the most public-facing part of your company.

- **Bottom Layers (The Factory Floor):** *Levels 0-3 in* Figure 5 Perdue Model adaptation source [4]. This is your industrial network (OT), which includes the machines, sensors, and controllers that run your physical processes.

- **The "Buffer Zone" (DMZ):** *Level 3.5 in* Figure 6 Perdue Model adaptation source [4]. The most important rule of the Purdue Model is to create a secure buffer zone, known as a Demilitarized Zone (DMZ), between the office and the factory. It's a neutral space where data can be safely exchanged without creating a direct, open pathway. For example, production data can be sent to the DMZ, and business systems can pick it up from there without ever touching the factory network directly.

*The Purdue Model provides a simple, powerful rule: **keep your office and factory networks separate**, using a controlled buffer zone for all communication. This layered approach is the first step in preventing a problem on the business network from shutting down production.*

IEC 62443

SECURE BUBBLES AND GUARDED PATHWAYS

IEC 62443 is a modern, more flexible blueprint that adapts to today's complex environments. Instead of rigid layers, it focuses on risk. Think of it as creating secure **zones** and "guarded pathways" called **conduits**:

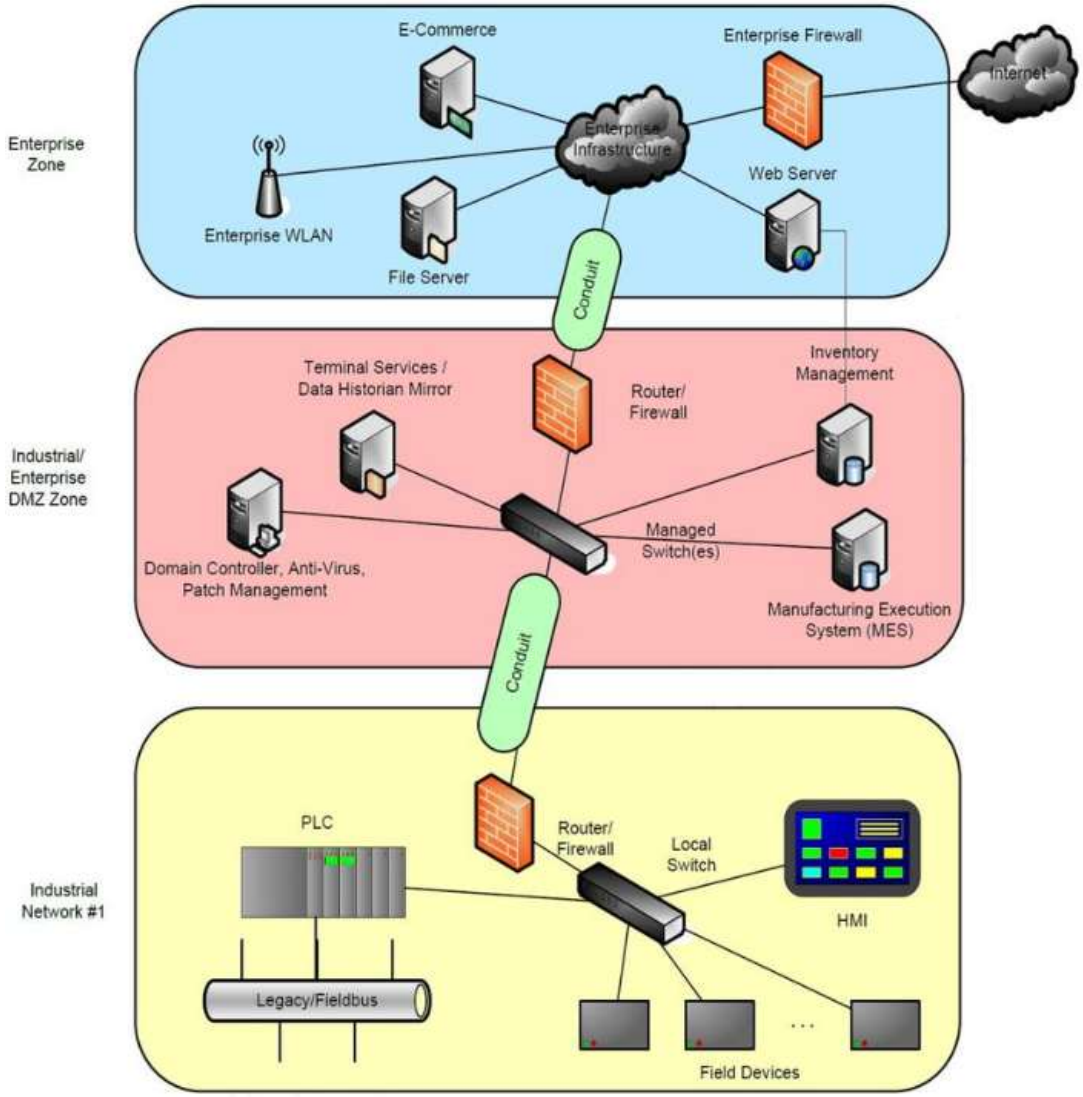

Figure 7 Zone model of Industrial Control Systems source: ISA/IEC 62443

- **Zones (Secure Bubbles):** The framework groups similar equipment into a protected bubble. All the controllers for a specific production line would be in one zone, while the safety systems would be in their own, separate, high-security bubble. Each zone gets a security level based on how critical it is.

- **Conduits (Guarded Pathways):** Any communication between these bubbles must travel through a pre-defined, guarded pathway. Controlling what kind of information can pass through, in which direction, and who is allowed to use it. Highly sensitive areas, can use a "one-way only conduit".

NAMUR OPEN ARCHITECTURE (NOA)

THE "DATA SUPERHIGHWAY"

NAMUR Open Architecture is a cutting-edge blueprint designed for the "smart factory" (Industry 4.0). It addresses how to get valuable data from your factory machines for analysis and optimization without disrupting the core operations.

It works by creating a **second, parallel highway just for data**.

- **The Main Road:** The existing, reliable control network that runs the factory, untouched and secure. It's the safe lane.
- **The Data Superhighway:** *In red in Figure 8 Proposed New IIOT Perdue Model source [5].* A new, separate channel is created to pull data and metrics out of the machines and send it securely to cloud-based monitoring platforms.

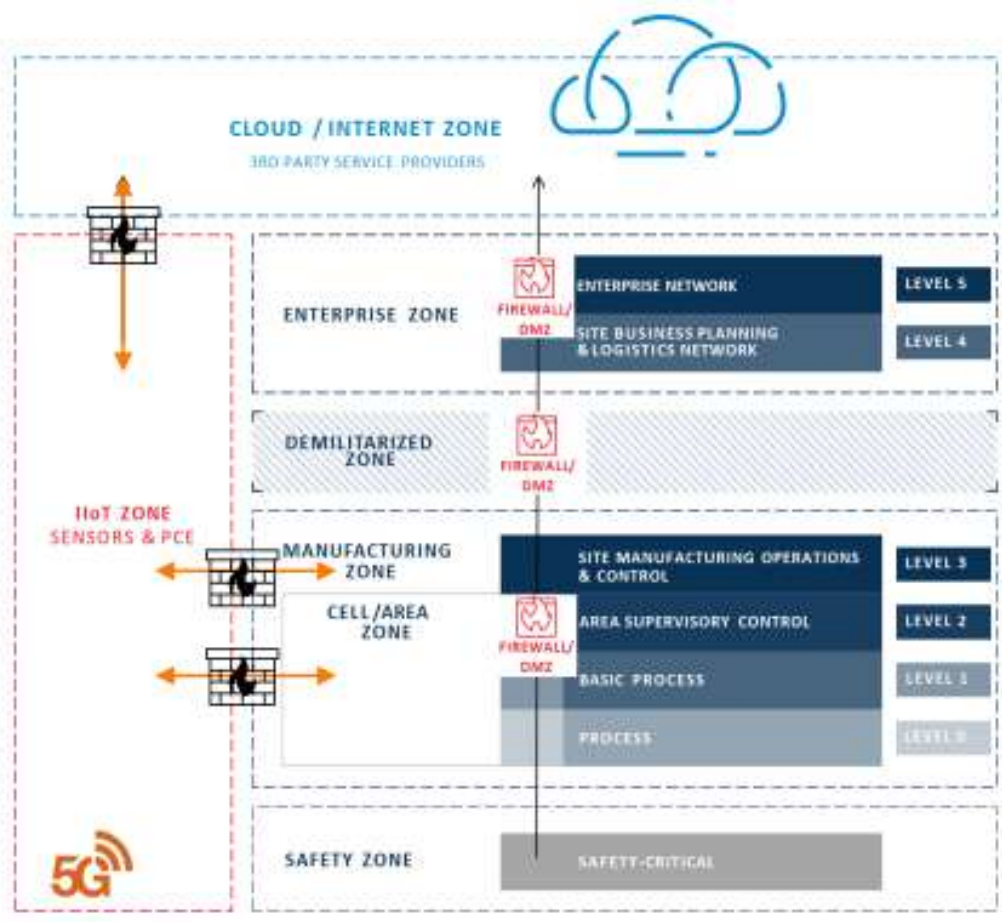

Figure 9 Proposed New IIOT Perdue Model source [5]

*NOA allows you to embrace Industry 4.0 and data analytics without a risky "rip and replace" of your proven factory systems. It provides a **secure and separate path** for your operational data, keeping your core production safe.*

EXPLORE SOLUTIONS

KEY STRATEGIES TO REDUCE RISK

- **Grant "Keys, Not Master Keys"**: We give employees access only to the specific applications they need to do their jobs (least-privilege access), drastically reducing our attack surface.

- **Continuous Verification**: We don't just check IDs at the door. User and device trust is continuously re-validated in real-time for every action, allowing us to adapt instantly to any sign of trouble.

CLOUD-BASED APPROACHES

Secure Service Edge (SSE)

SSE consolidates multiple security services into a single, cloud-based platform. Think of it as an integrated security hub that protects users and data everywhere.

Key components:

- **Zero Trust Network Access (ZTNA)**
  Acts as a "digital bouncer" for our applications. Instead of giving users broad network access like a traditional VPN, ZTNA grants access to specific applications only after verifying the user's identity and the security of their device [1].

- **Cloud Secure Web Gateway (SWG)**
  Is a smart filter that protects our employees from web-based threats by blocking access to malicious websites and inspecting traffic for hidden dangers [1].

- **Cloud Access Security Broker (CASB)**
  Provides visibility and policy enforcement for sanctioned and unsanctioned cloud applications, preventing data exfiltration and ensuring compliance in SaaS environments [1].

- **Firewall-As-A-Service (FWaaS)**
  Is a powerful, cloud-based firewall that protects our entire organization without the need for physical hardware at every location. It provides centralized control and consistent protection for all traffic [1].

Secure Access Service Edge (SASE)

SASE extends SSE security hub and combines it with our network into a single, unified service. Like a global, intelligent network that has security built-in. It ensures that our security policies are enforced consistently across every office, factory, and remote user.

Key components:

- **Software-Defined Wide Area Networking (SD-WAN)**
  Is a technology that simplifies the management of wide area networks (WANs). Unlike traditional networks where management is tied to physical hardware like routers and switches, SD-WAN allows organizations to control their network infrastructure through software [1].

- **Zero Trust Network Access (ZTNA)**

- **Cloud Secure Web Gateway (SWG)**

- **Cloud Access Security Broker (CASB)**

- **Firewall-As-A-Service (FWaaS)**

HARDWARE-ENFORCED SOLUTIONS

PROTECTING MISSION-CRITICAL OT NETWORKS

Hardware-enforced technologies provide the strongest guarantee that no attack information can penetrate protected networks.

- **Physical impossibility of attack:** Unlike software firewalls, which can have flaws, these hardware solutions make it physically impossible for malicious commands to travel back into our protected network.

- **Protection for critical assets:** For our most essential infrastructure, these technologies offer a level of assurance that software-only solutions like VPNs or firewalls simply cannot match.

Unidirectional Gateways

Fully NIST SP 800-82 compliant, these appliances physically permit data flow in only one direction from OT to IT while blocking any reverse traffic. Their optical isolation and embedded protocol replication ensure that even a zero-day exploit on the gateway cannot relay attack commands back into the protected network [2].

Unidirectional Remote Screen View

Attended remote access transmits only screen images out of the OT environment. Remote experts view real-time video but cannot send keystrokes or control signals back. An on-site operator performs all actions, eliminating any risk of automated or unauthorized commands reaching OT assets [2].

Hardware-Enforced Remote Access

HERA uses two separate, one-way hardware channels: one for sending screen images out and another for receiving encrypted keyboard and mouse commands. This hardware is designed to reject anything that isn't a simple keystroke or mouse movement, blocking sophisticated attacks. It's the digital equivalent of having separate, guarded tunnels for incoming and outgoing traffic [2].

Time-Limited Hardware Switches

This is a physical "on/off" switch for remote access. By default, the connection is physically broken. To enable it, an authorized person on-site must turn a physical key, typically after a verification phone call. Access is granted for a short, pre-set time (e.g., 60 minutes) before the switch automatically disconnects again. This dramatically shrinks the window of opportunity for any potential attack [2].

RISK-BASED DECISION

Effective IT-OT convergence begins with a risk-based assessment that classifies each environment and workload. Once assets are classified, select technologies that align protection intensity with risk:

- **Low-Medium Consequence**
  Adopt modern cloud-native SSE/SASE offerings for cost-effective, scalable protection of corporate and non-critical plant networks. These deliver ZTNA, SWG, CASB, FWaaS, and SD-WAN integration without the complexity of custom hardware deployments [1].

- **High Consequence**
  Deploy hardware-enforced solutions—unidirectional gateways, URSV, HERA—to safeguard control and safety systems. Their physical one-way data flow and time-limited switches ensure no adversary-originated traffic can enter OT networks [2].

- **Critical Infrastructure**
  Layer attended unidirectional remote screen view (URSV) for forensic-grade monitoring of safety-critical assets, complemented by stringent on-site human oversight. This “air-gapped” model guarantees that only vetted, manual interventions occur in the most sensitive zones [2].

REFERENCES

[1] U.S. Cybersecurity and Infrastructure Security Agency, U.S. Federal Bureau of Investigation, New Zealand's Government Communications Security Bureau, New Zealand's Computer Emergency Response Team, Canadian Centre for Cyber Security, June 2024. [Online]. Available: https://www.cisa.gov/sites/default/files/2024-06/joint-guide-modern-approaches-to-secure-network-access-security-508c.pdf. [Accessed September 2025].

[2] Waterfall, Rethinking secure remote access to industrial and OT networks, 2025.

[3] W. Toll, "Preventing Lateral Movement is a Key Strategy for 2025," January 2025. [Online]. Available: https://www.elisity.com/blog/the-top-11-cyberattacks-using-lateral-movement-a-2023-2024-analysis-for-enterprise-security-leaders#:~:text=over%2070%25%20of%20successful%20breaches%20leveraging%20lateral%20movement. [Accessed September 2025].

[4] C. K. G. K. C. R. J. B. GEORGIOS MICHAIL MAKRAKIS, "Industrial and Critical Infrastructure Security: Technical Analysis of Real-Life Security Incidents," *IEEE TRANSACTIONS and JOURNALS,* 2021.

[5] T. V. d. Wouwer, "Securing the digital factory," Orange CyberDefense, October 2021. [Online]. Available:

https://www.orangecyberdefense.com/fileadmin/be/Resources/OCD_live_2022/OCD_Live_Atlas_Copco.pdf. [Accessed September 2025].