semaphore
CONSULTING PARTNERS

Designing secure OT environment based on PERA model

Rostyslav Yevdiukhin

Date: 16.04.2026

Identity Day Norway

About a speaker

Ross is Senior Advisor in Semaphore Consulting Partners.

Worked for 4 of Fortune 100 companies.

Main interest - AD, IAM, PAM, remote access and overall digital infrastructure.

Ross (Rostyslav) is Ukrainian living in Norway for 15 years. Main hobby - work. Secondary hobby - non-paid position in the Board of the Ukrainian Association in Norway. Other hobbies on pause waiting for the war to end.

Leading daily demonstrations near Parliament in Oslo (Mon, Thu, Fri 17:00, Sun 12:00)

Defending against Information Warfare vs Information Technology Warfare

Translation: April 9th. "Never again" is not just a memory, but a commitment. War and aggression do not play out through armed force alone. We are attacked daily in the information domain.

In Norway, we have so far shown resilience against malicious influence, but there is no guarantee that this will continue. Trust is a cornerstone of our democracy—worth more than the Sovereign Wealth Fund. It must be defended. Polarization and extremism must be fought. The responsibility rests on us all. We must continue to stand up for democracy—that which unites us.

IT and OT - TL;DR

- OT = IT - 20 years
- No Antivirus (and surely no XDR)
- Limited use of the firewall
- Classic perimeter defense thinking vs Zero Trust / layered defenses

IT Remote Access

- PAM system for secure RDP and SSH
- Session recording
- Manual approval step for credential checkout in the Vault
- Browser sandboxing for HTTPS
- Data Leak Prevention
- XDR on the endpoint (maybe integrated with Identity with auto-actions)
- Direct Access from third-parties' endpoints to database or servers - is a big no-no

OT Remote Access

Vendors demand VPN access from the central location that is used for all customers.

Often they want line of sight to PLC from the management server with all necessary tools.

"Let's put a router, that you will plug into Internet when you need us to connect".

Router producer:

"Built-in automated cybersecurity:

- Our automated networking eliminates human error in cybersecurity configuration. Every device includes:

  Automated Linux iptables-based firewall at the edge, rendering HUB LAN-connected devices invisible to the internet"

OT Vendors (im)maturity

Vendors demand the use of shared accounts with fake multi-factor authentication.

Typical excuse - we provide services to this big chain and they don’t complain.

We require a code delivered with SMS after the password, what can go wrong!?

No SOC 2 type 2 even for large worldwide vendors.

ISO 27001 audits with findings and most important parts missing from the statement of applicability.

What is OT?

Operational technology (OT) is the hardware and software that monitors and controls devices, processes, and infrastructure, and is used in industrial settings. IT combines technologies for networking, information processing, enterprise data centers, and cloud systems. OT devices control the physical world, while IT systems manage data and applications. (Cisco)

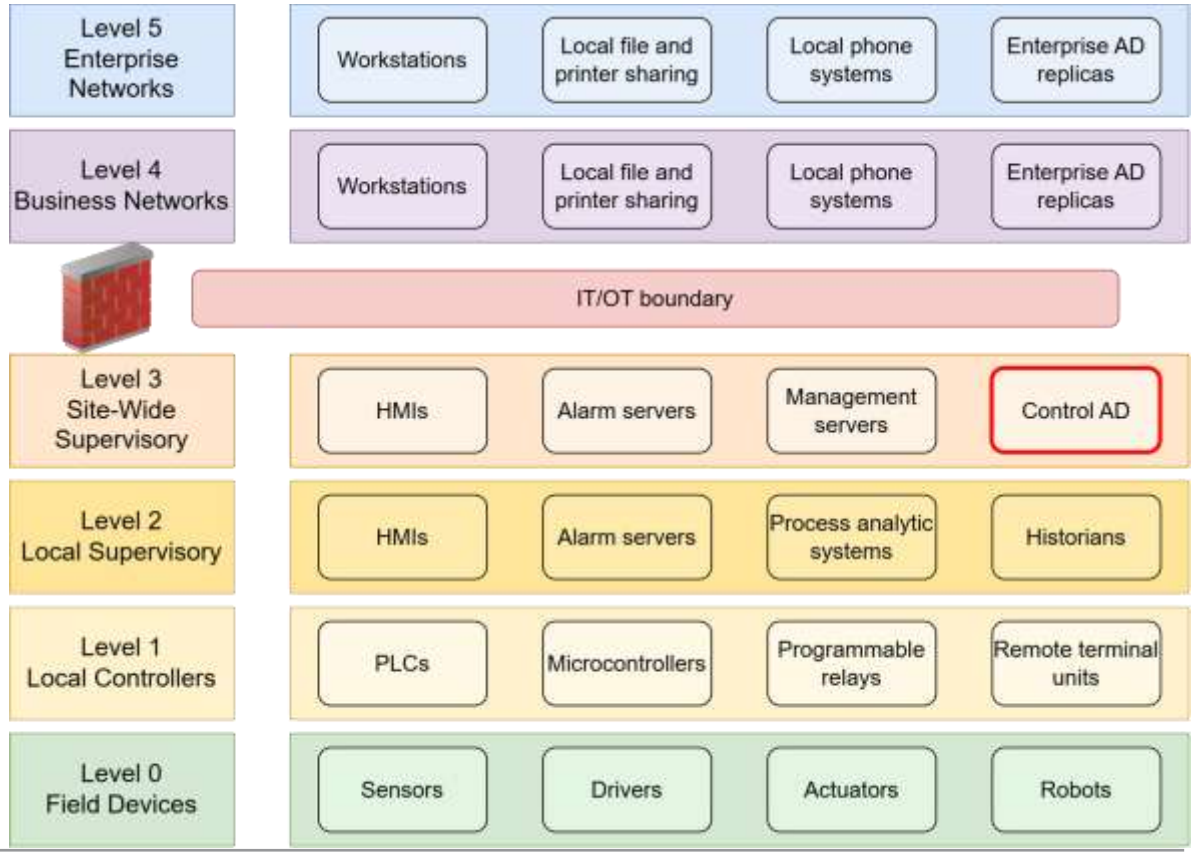
SANS Purdue / PERA model

Reference architecture for systems separation

Key requirement:

Active Directory (AD) can be implemented to help manage control networks, but any such AD deployment should be completely independent of the business AD. Domain Controllers and other AD servers should be placed in Level 3.

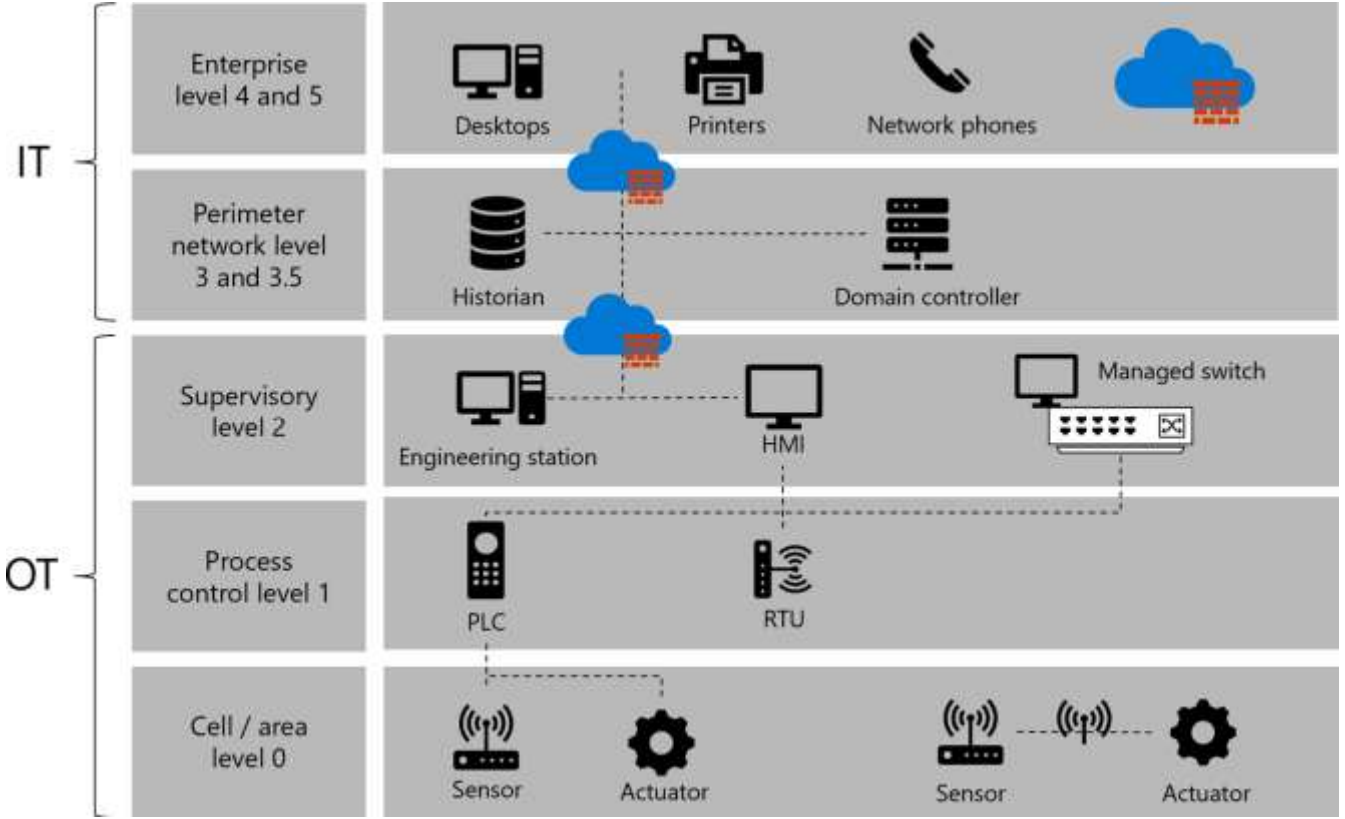
Levels 0-2 are often not TCP/IP, but BACnet, Modbus and other families of protocols.



IT vs OT

Hard to draw the line.

This example from Microsoft is not according to Purdue model.



https://learn.microsoft.com/en-us/azure/defender-for-iot/organizations/best-practices/understand-network-architecture

SANS Purdue / PERA model

Real-life dangerous scenarios:

Direct connections from third-party networks directly to PLC allowing to change the code.

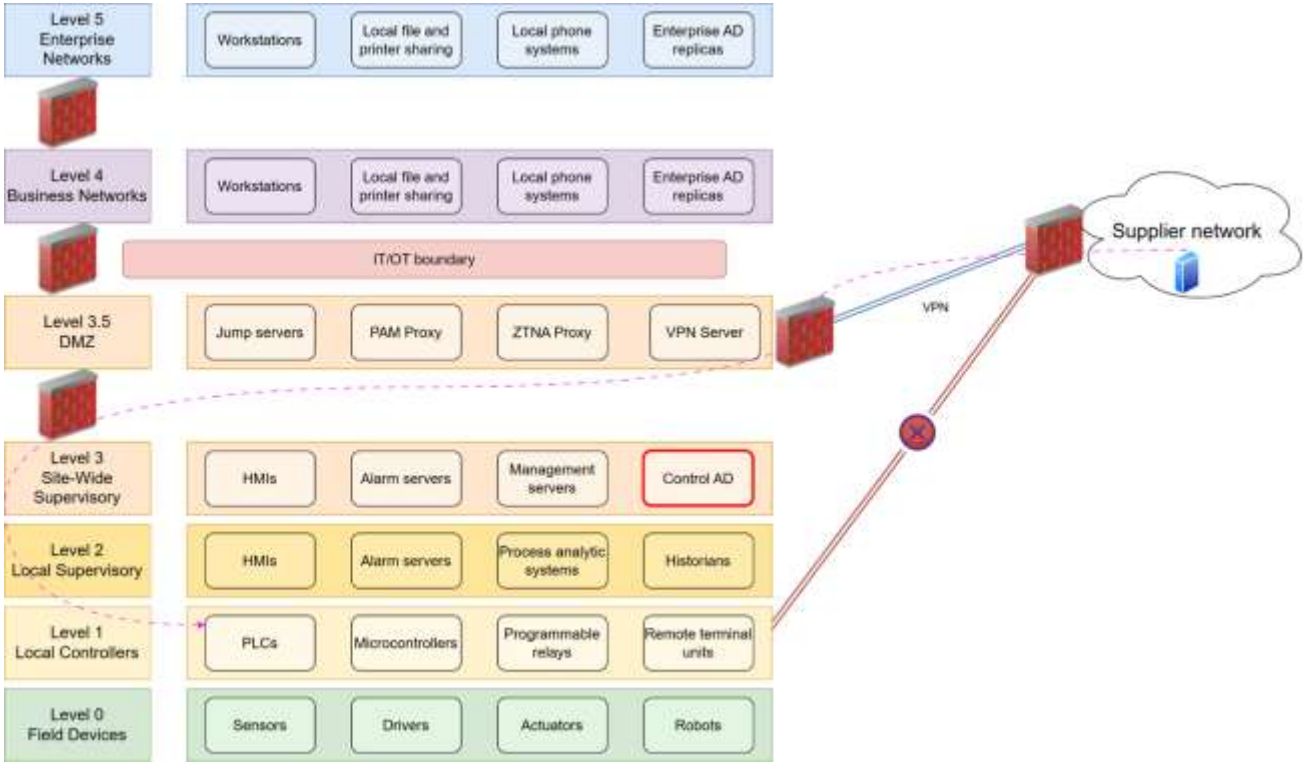
Direct connections to servers with remote desktop / teamviewer over Internet.

5g routers or special reverse proxy appliances plugged into network.

Must be replaced with:

PAM / VDI / Session isolation

Management servers for local programming of PLCs



Big organisations => big challenges

In addition to Enterprise ADs, you now need another AD for OT.

Can you have one OT AD shared across all facilities?

Enterprise ADs

Facility A

Facility B

Facility C

OT AD

OT AD

OT AD

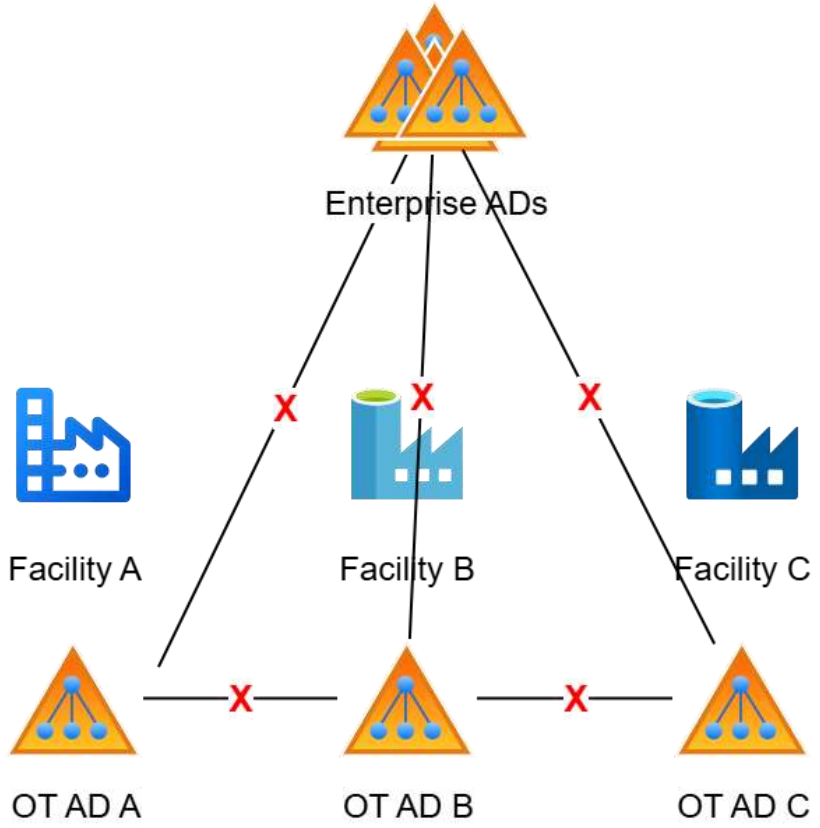
Organisation perspective

In addition to Enterprise AD(s), you now need another AD for OT.

- Can you have one OT AD shared across all facilities?
- Big and well respected consultancy company says - yes.

For a proper isolation, these ADs should be isolated and independent.

- Challenge with operation and maintenance, IAM lifecycle management etc.
- Supplier access to the environment.



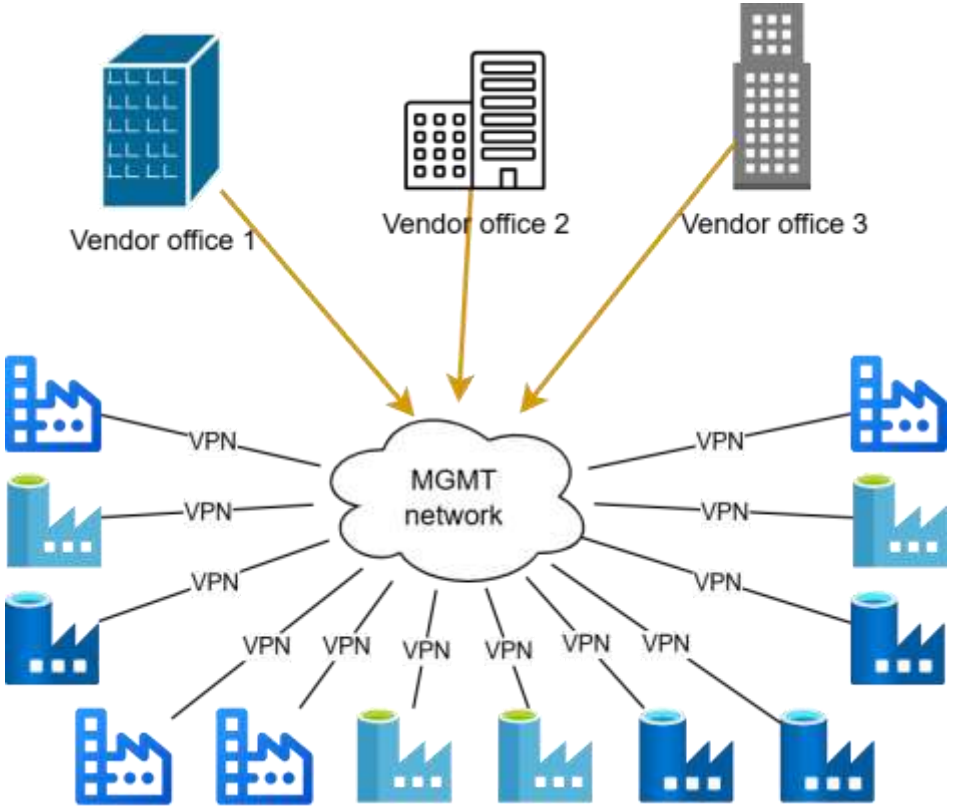
Vendors and PERA model

- OT Control applications are lacking OIDC/OAuth 2.0 for users, but often they support OAuth 2.0 for APIs.

- Authentication is a mystery to OT developers.
  - IIS with custom authentication, because Windows Integrated Authentication sometimes fails with trust. Users have to type corporate password on some strange login window…
  - LDAP authentication for Enterprise users will mean connection from OT server to Enterprise Domain Controllers.
  - Local users/passwords is the likely authentication method. Bad practices: no salting, weak hashing.

OT Supplier / Vendor perspective

Centralized management and monitoring.

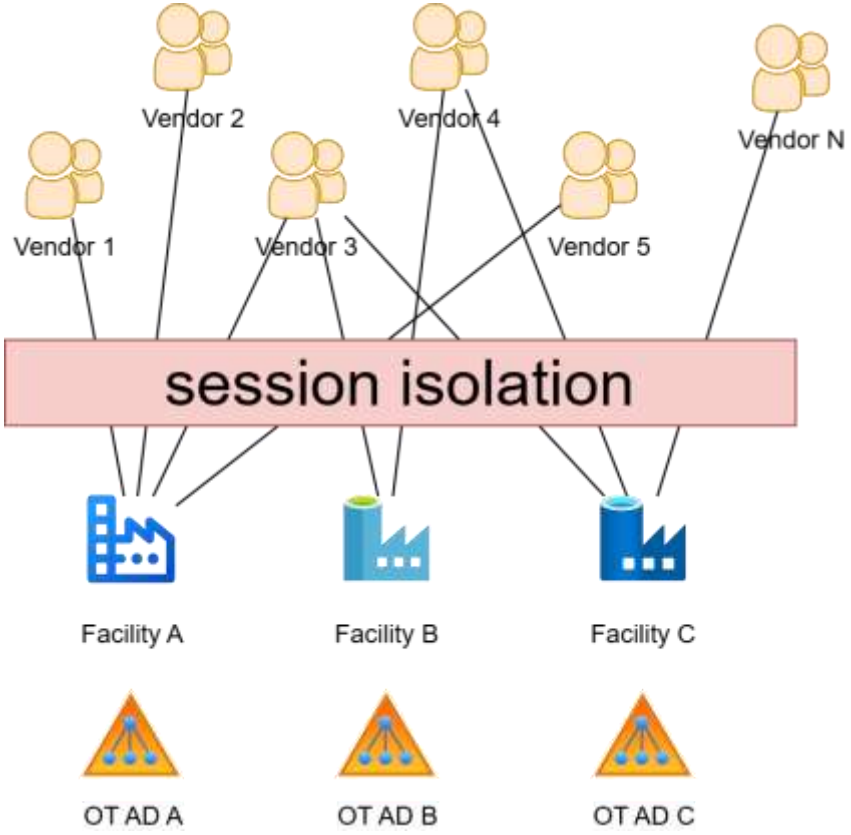


Enterprise perspective

Large amount of vendors, not always shared across facilities.

In order to control access - authentication should be owned by Enterprise.

Access only through the session isolation - no direct access from external addresses into OT infrastructure.



Legal governance - NIS / NIS2

Example from Norway:

A provider of an essential service shall ensure that suppliers and others who perform work that may affect the security of network and information systems, and who perform work for or on behalf of the business, carry out the work in a manner that ensures that the requirements for adequate security are met.

A provider of an essential service shall, through an agreement or by another suitable means, make the security measures applicable to suppliers as mentioned in the first paragraph, to the extent necessary to maintain an adequate level of security.

<...>

A provider of an essential service shall prepare written instructions, routines, and procedures for digital security. …

…

The governing documents and action plans according to the first and second paragraphs shall be made known to personnel who perform tasks for or on behalf of the business and who may gain access to the business's network and information systems.

Key takeaways

Enterprises:

- Set stricter requirements for suppliers of OT services
- Invest in Secure Architecture
- Implement solutions for secure remote access for the OT Supplier use case

OT Suppliers:

- Develop remote access solutions where customers have control over access and information
- Use modern authentication/authorisation (OIDC / Oauth 2.0), do not rely on Enterprise AD connection
- Use standalone servers as a secure architecture, avoid Active Directory dependency

Q&A

Thank you for attention.

Contacts:

Linkedin: linkedin.com/in/ross-ua

Signal: RossUA.40

Facebook: rostyslav.yevdyukhin

E-mail: rostyslav@ukrainsk.no

Den ukrainske forening i Norge x **Slava Ukraini Norge**

A **special project** for a **special team**

THE MISSION

2 boat motors: 40hp and 100hp
for active Black Sea operations

HOW TO SUPPORT

Bankkonto 1645.16.24397
Vipps #12602

Tax deduction available
(skattefradrag)
for donations 500-25 000 NOK

ukrainsk.no/motors