

Industrial Control Systems: how to secure them in practice!

DEFCON 32

August 2024

WAVESTONE

AGENDA

- 01 Introduction to ICS cybersecurity**
- 02 Securing ICS – ICS inventory**
- 03 Securing ICS – Backups**
- 04 Securing ICS – Network security**
- 05 Securing ICS – System hardening**
- 06 Securing ICS – Detection on the cheap**



1. Introduction to ICS cybersecurity

- Introduction to ICS: standard design and components
- What's wrong with ICS cybersecurity: Wavestone ICS audit benchmark
- Focus on PLC and ICS protocols
- How to secure ICS: a typical action plan

Where do we find Industrial Control Systems?



Transport



Utilities



Oil & Gas



Pharmaceutical



Nuclear



Military /
defense

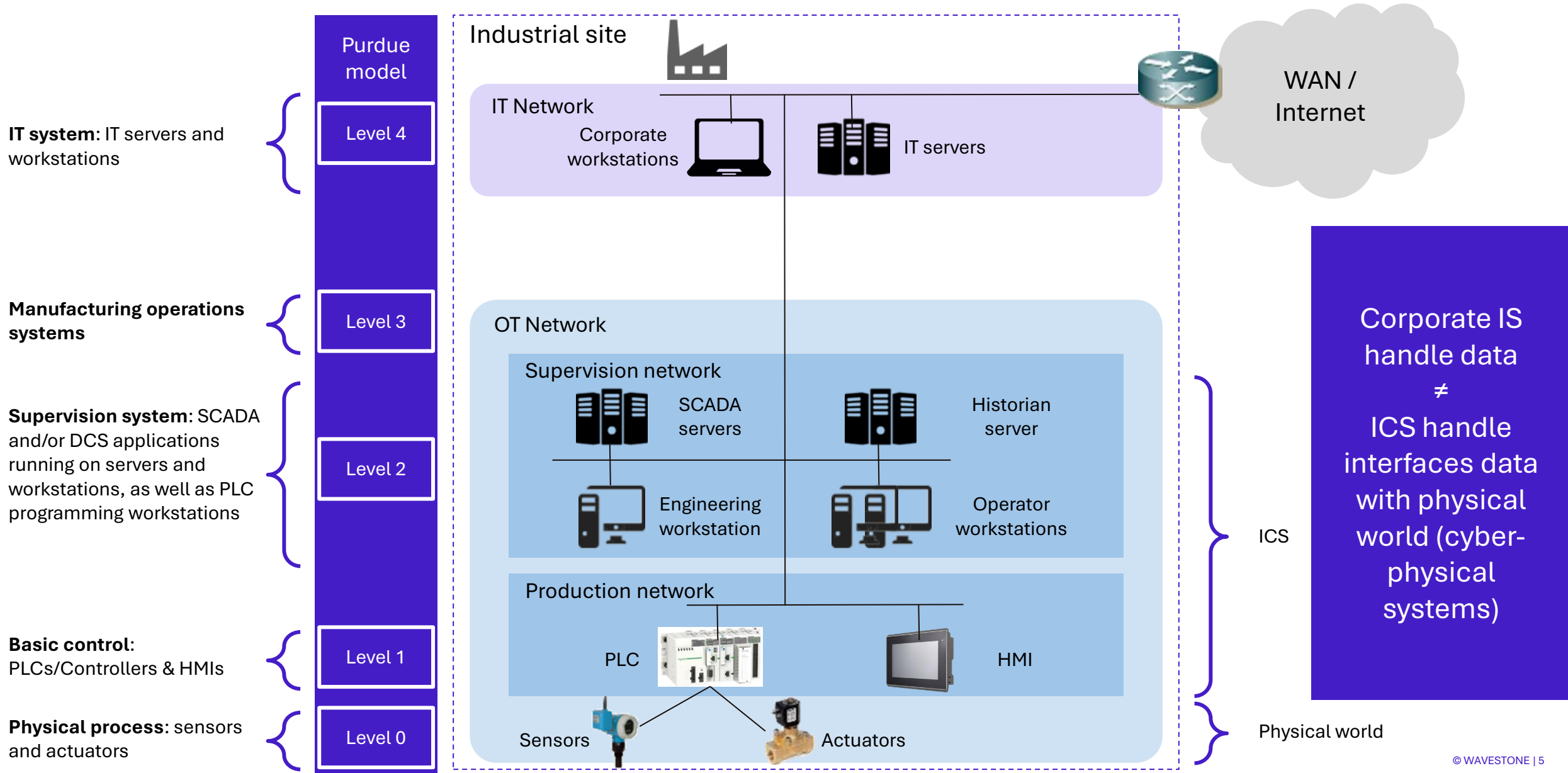


Automobile



Agribusiness

What is an Industrial Control System (ICS)?



A bit of vocabulary

ICS (Industrial Control System)

=

OT (Operational Technology)

≈

SCADA (Supervisory Control And Data Acquisition)

≈

DCS (Distributed Control System)

Nowadays, people tend to say “SCADA” for anything related to ICS

ICS components

Sensors and actuators: Allow interaction with the physical world (pressure sensor, valves, motors, ...)

Local HMI: Human-Machine Interface, permits the supervision and control of a subprocess

PLC (Programmable Logic Controller): Manages the sensors and actuators

Supervision screen: Remote supervision of the industrial process

Data historian: Records all the data from the production and Scada networks

MES: Manufacturing execution system (production status, scheduling, etc.)

RTU: Remote Terminal Unit (standalone PLC)

Other low-level devices: Intelligent electronic devices, wireless devices, variator frequency drives, remote I/O, etc



ICS vendors



The traditional vision: Why is OT security 20 years behind?



Very long-life components (+20 years), frequent obsolescence



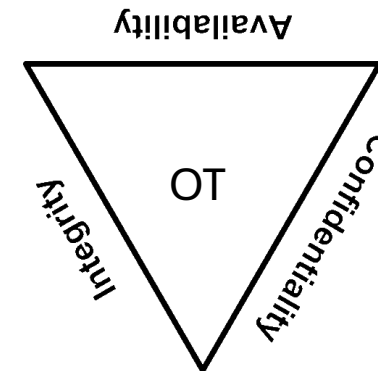
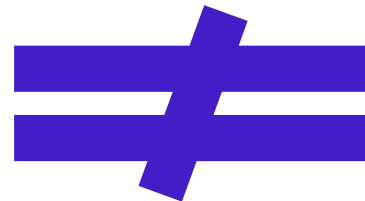
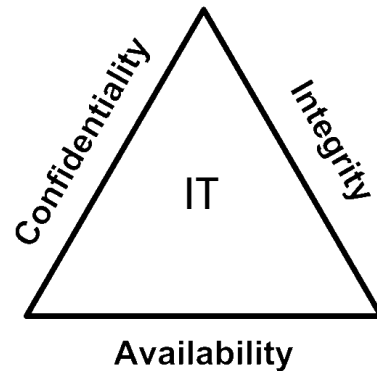
The main criterion is availability, not confidentiality



Recent use of standard components & protocols



Systems designed to be isolated but now connected



The new vision: Leveraging the strengths of OT



Few changes once
the system is
secured



No data encryption
issues



Quality culture &
good change
management



Dedicated safety
systems to prevent
a major incident

ICS operations = Safety + Availability + Quality

Some cases of attacks on ICS

2010 – Stuxnet, Iran

- **Malware attack** on the industrial IS of nuclear complexes in Iran
- ~ **1000** uranium enrichment **centrifuges** destroyed
- Delay and loss of credibility of Iran's nuclear program

SIEMENS



2015 – Industroyer, Ukraine

- **Simultaneous hacking** of 3 electrical distribution centers in Ukraine
- ~ **50 electrical substations** and **250,000 households** out of power for 3 to 6 hours



2017 – Wannacry, World

- **Ransomware attack** targeting computers using the Microsoft Windows OS
- Use of the « **Eternal Blue** » vulnerability to spread
- Despite having a patch available, a majority of industrial systems were not patched at the time of the attack



2017 – Triton, Petro Rabigh

- **Malware** designed to attack safety systems, targeting Schneider Electric systems
- Would cause physical safety systems to **cease operating** or to **operate in an unsafe manner**
- Cyberattack prevented from reaching its full capabilities

Schneider
Electric

2021 – Water treatment plant, Florida

- Use of **TeamViewer** to access computer
- Sodium hydroxide levels were increased in the water, and would have resulted in mass sickness



2021 – Colonial Pipeline, United States

- **Ransomware attack** on computers managing the pipelines
- **\$4,4 million** demanded as ransom in bitcoins
- 5-day service interruption

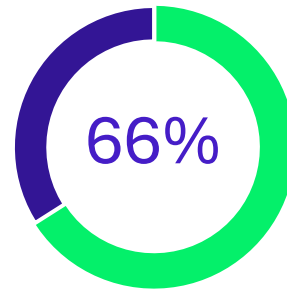


Most attacks on ICS are either **complex targeted attacks**, or **ransomware** attacks spreading to ICS due to lack of network segmentation

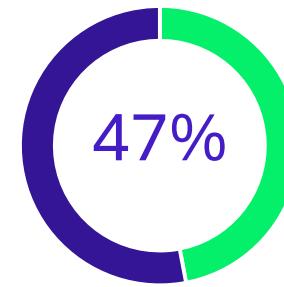
Governance

Who's in charge of ICS Cybersecurity?

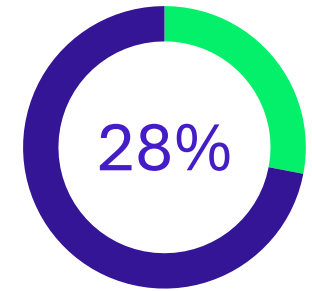
A specific ICS policy exists



An on-site cybersecurity manager is identified



Cyber requirements for 3rd parties are defined



Governance is a key issue, which tends to be overlooked in cybersecurity projects.



It is necessary to create mixed IT/OT teams, and the support of IT cybersecurity teams is generally necessary for the upskilling of OT teams.

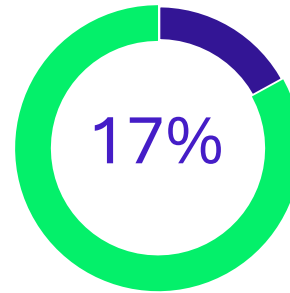


Although dedicated cybersecurity tools can help in improving the level of security, no tool will replace qualified personnel.

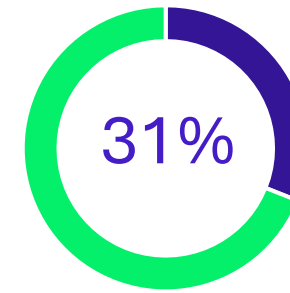
Network segmentation

No ICS is 100% isolated.

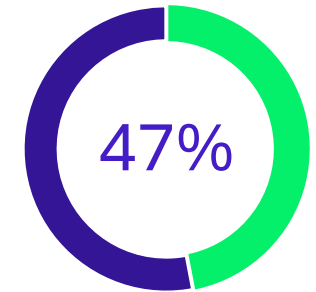
PLCs on the office network



PLCs accessible from the office network



Presence of a DMZ between IT & OT



Network segmentation is often a good starting point for ICS security projects.



Safety Instrumented Systems are the most sensitive assets to protect and should be segmented first.

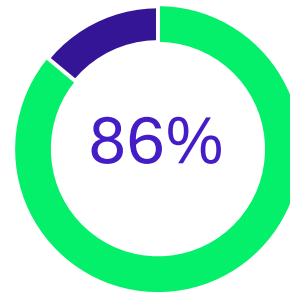


A network segmentation project usually involves other technical (Active Directory) and organizational (RACI for system administration) segmentation projects.

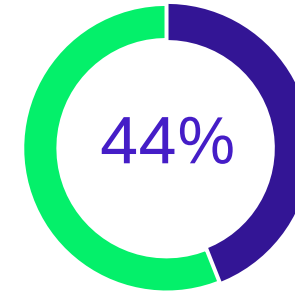
Remote access

Remote access is a business need.

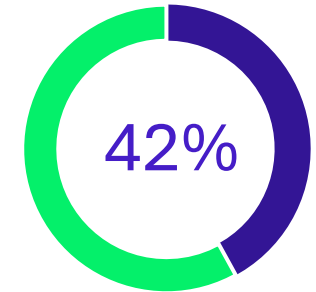
Remote access to ICS exists



There is a site-to-site connection between the ICS and a third party



Use of unofficial solutions for remote access



It is very common for part of the industrial perimeter to be under the responsibility of third parties, often requiring remote access for maintenance or even supervision.



It is recommended to provide a vetted solution to avoid insecure local initiatives.

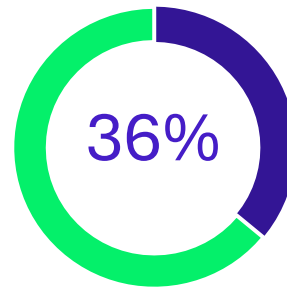


It is important to take into account the specific needs of the sites (real-time monitoring of third-party actions by a local actor, non-permanent and limited access to certain machines) when defining the proposed solution.

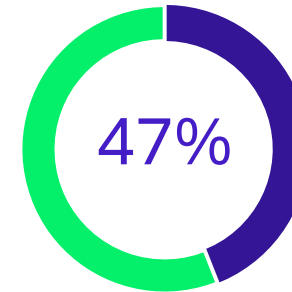
System administration

Segmentation is not just a network issue

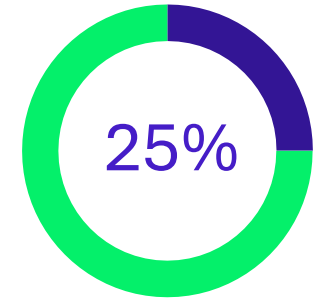
No security patches applied



No AV/EDR solution



Windows OT machines are part of the corporate AD



The system administration of standard equipment (Windows type) requires specific skills and appropriate training, both of which are rarely present on the OT side.



The application of security patches is necessary, but should be done in a pragmatic way, based on the exposure of the equipment. Over-investment in the subject should be avoided.

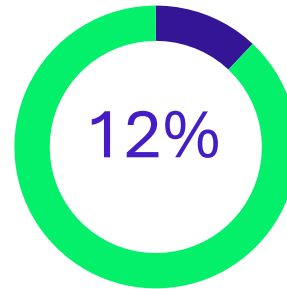


As long as OT equipment is part of the corporate Active Directory, an attacker or ransomware can propagate to the ICS, regardless of the network filtering rules.

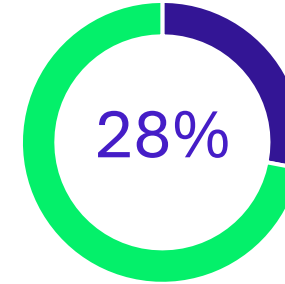
Resilience

Think resilience
globally

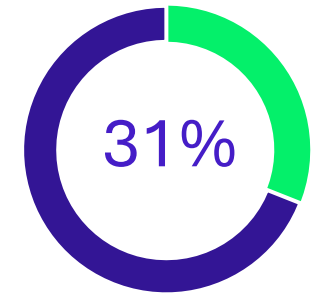
Suffered a
production-
impacting incident
within 12 months



Use of obsolete
components without
sufficient/controlled
spare part



The site has an up-
to-date inventory



Although backups are usually present, it is rare that they cover all the machines needed for production, especially machines provided and managed by a third-party.



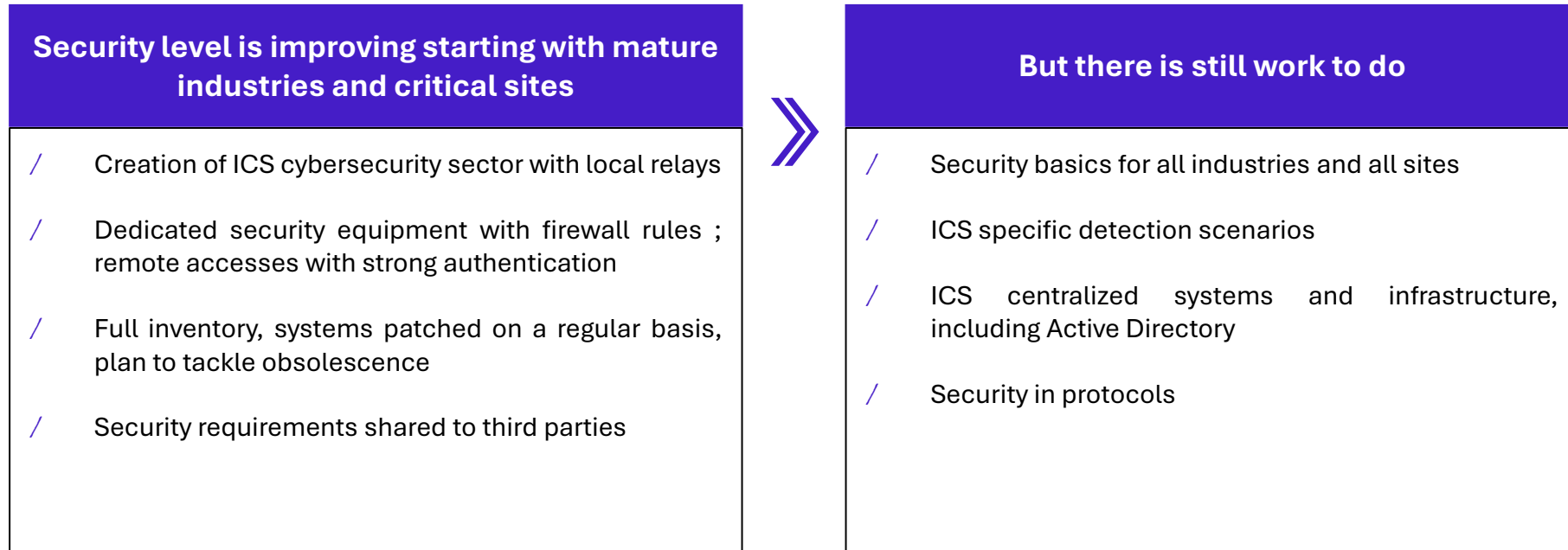
It is essential to have a detailed and up to date view of your equipment, and to integrate elements supplied by & under the responsibility of third parties (packaged PLCs / blackbox)



For many industries, especially manufacturing, the availability of production lines is not sufficient for resilience, other systems need to be integrated into the overall thinking (MES, ERP)

OT benchmark – ICS security is slowly evolving

Regulations and recent attacks have made several companies work on securing ICS



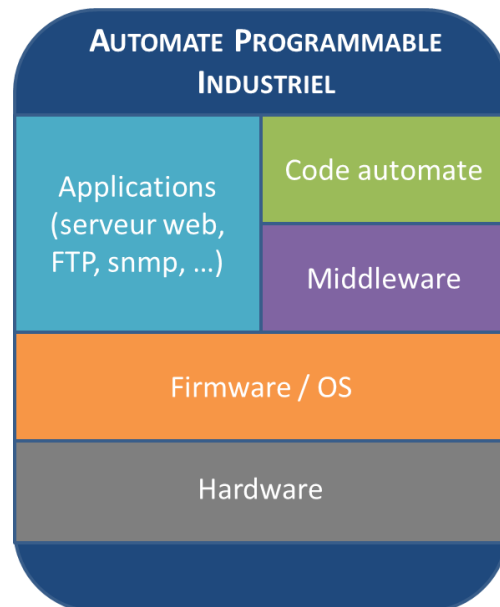
OT specificities can be leveraged to improve cybersecurity

ICS operations = Safety + Availability + Quality

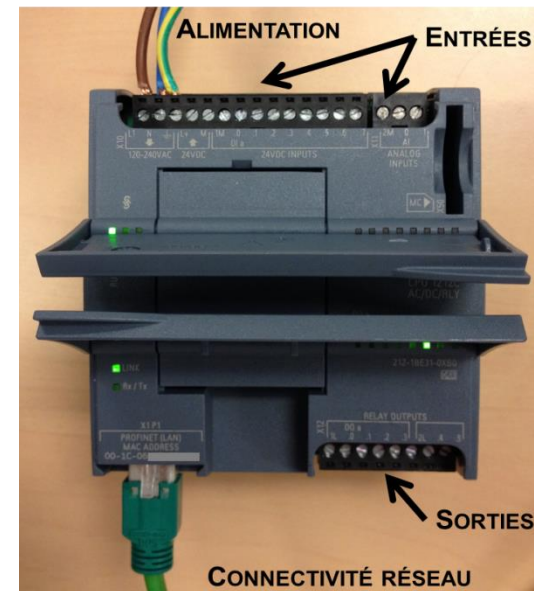
What is a PLC?

- / Real-time digital computer used for automation
- / Replaces electrical relays
- / Lots of analogue or digital inputs & outputs
- / Rugged devices (immune to vibration, electrical noise, temperature, dust, ...)

What's inside?



Siemens S7-1200



Security in protocols

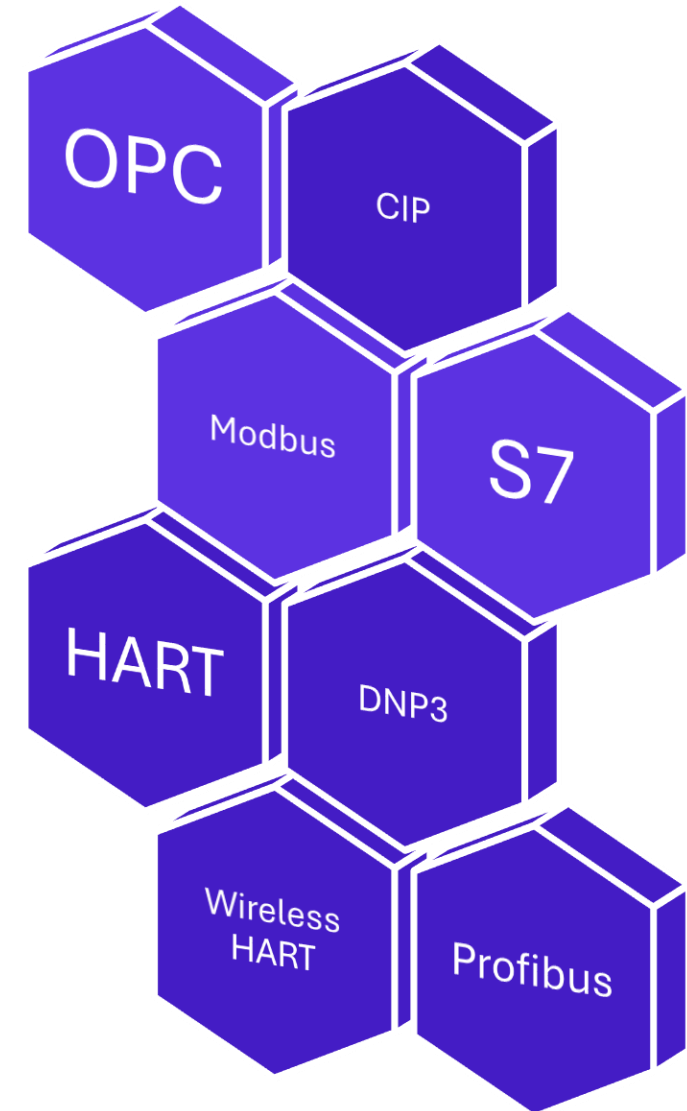
At the beginning, specific protocols on specific **physical layer**

(RS232, RS485, 4-20 current loop)

Some protocols were **adapted to TCP/IP**, like Modbus, and other were developed to allow interoperability.

ICS devices often use **specific protocols**, some of them are **proprietary**, and some of them are **common standards**

Most of these protocols are **unauthenticated and unencrypted**



Focus on 2 main OT protocols



Modbus


- Serial communication protocol invented in 1979 by Schneider Electric, now Royalty-free
- Controller / Worker protocol with no object description
- Security: unauthenticated & unencrypted
- TCP port 502
- The most common Modbus functions allow to read and write data from/to a PLC
- Undocumented Modbus function codes can also be used to perform specific actions (administration)



OPC-UA


- OPC-UA : Unified Architecture, defined in IEC 62541 in 2015
- Service oriented architecture (client/server) with a node hierarchy
- Security
 - Several security levels: none, signature, signature and encryption
 - Compatible with X.509 certificates and Kerberos, Login/password connection
 - Fine grained access rights for each node
- TCP port 12403 in our setup
- Current implementations are weak and ease the comprehension of the industrial process for an attacker

#Foreverdays



#foreverdays is a term coined by @reverseics
Very important concept when talking about ICS
The highest vulnerabilities are not patched.

So it is really worth considering the effort of patch
management of ICS equipment when you know



Securing ICS – Many topics to address



How to start an industrial site cybersecurity project?

STEP 1



Knowing your ICS & industrial processes

- Start by going on-site! Do a site tour, meet the people, understand the context. Each industry has its own very specific constraints
- Identify & map the ICS resources (servers, PLCs, other low-level devices)

STEP 2



Limiting network exposure

- Separate IT & OT networks (logically at least)
- Limit exchanges with the IT to what's absolutely necessary
- Ensure no direct access to low-level devices from IT / Internet

STEP 3



Pragmatic view of security patches

- Is it really worth the effort patching PLC vulnerabilities when you have foreverdays?
- Being able to quickly patch a vulnerability exploited in the wild is probably more important than installing all patches every month
- Everything that can be reached by the corporate IT or an external network must be patched regularly

STEP 4



Ensuring end-to-end resilience

- Beware of ransomwares! Have offline backups, and try to perform a restore at least once a year
- Discuss business continuity with people on-site, and ensure they took OT into consideration

Put the human at the center of the cybersecurity approach

Start small & grow

Lab introduction

<https://tinyurl.com/DEFCON-32-OT>

In this workshop, we will **secure** a very simple Industrial Control System!

Each participant has its **own virtual lab** and will perform hands-on exercises

We will focus on **5 key topics** for ICS cybersecurity

You will see that securing ICS is **not very complicated** and also **not that different from IT**





2. Securing ICS – ICS inventory

- Inventory strategies
- [Hands on] Build your asset inventory
- Focus on network probes / passive network monitoring solutions

Asset inventory: Introduction

Creating an asset inventory is a **foundational step in securing your ICS**. While the initial creation of an asset inventory can be relatively straightforward, **maintaining it regularly presents significant challenges**, even for mature organizations.



Do not wait for a perfect asset inventory before starting other OT cybersecurity activities

Getting Started with Asset Inventory



/ Baseline Inventory

/ Incremental Updates

/ Continuous Monitoring

Asset inventory: What does it contain?

An OT asset inventory is a **comprehensive list of all the assets within the OT network that have an IP address** (*Servers, workstations, firewalls, switches, PLCs, HMIs and any other OT devices*), detailing **key information** to help **manage** and **secure** these assets effectively.

What can be included in an asset inventory?

01

Minimal Information

- ✓ Name
- ✓ IP Address
- ✓ Type of Asset

02

Additional Information

- ✓ Manufacturer
- ✓ Model
- ✓ OS/Firmware Version
- ✓ Physical Location
- ✓ Software Installed and Their Versions

03

Extended Relevant Information

- ✓ Asset Obsolescence / end of date support
- ✓ Warranty Information
- ✓ Asset Criticality
- ✓ Backup Information
- ✓ Asset Exposure on the Network
- ✓ User Accounts
- ✓ Maintenance Schedule

Having outlined the key information, let's now explore the tools that will streamline the inventory process

Asset inventory: Methodology to create it

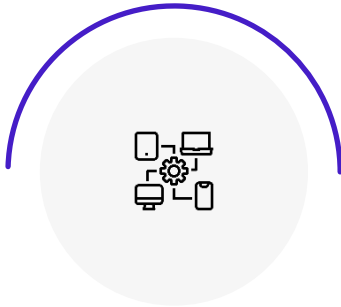
A **comprehensive asset inventory** is achieved through a **dual approach**, combining a **manual on-site survey and visit** with **tool-based methods** to ensure both visible and hidden assets are thoroughly captured and accurately documented.

Manual approach: go on site and list every asset you see in the plant

Tools & Techniques:

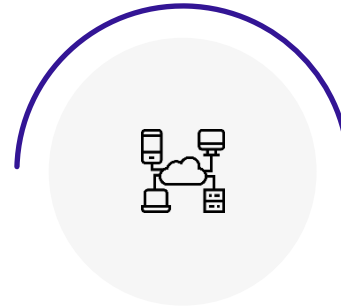
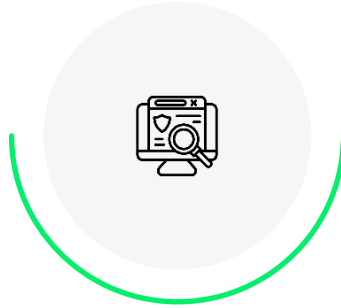
ARP Scan

Connect to key assets & Use **Address Resolution Protocol (ARP)** scans to identify and map devices on the network, helping to **reveal assets that might not be immediately visible**



Direct Connection

Connect directly to each asset to gather **configuration information**, such as **IP addresses** and **network settings** (e.g., using commands like **ipconfig**)



Network Scans

Perform comprehensive network scans like **ping scans** to detect active devices and **nmap** to some extent to gain deeper insights into the **devices' services and characteristics**

Network Capture

Capture and analyze network traffic using **PCAP files** to identify devices, **communication patterns**, and potential **hidden assets** within the network



Bear in mind there is no magic tool if you start from scratch!

Asset inventory: How to maintain it?

Maintaining an **accurate** and **up-to-date** asset inventory is **crucial for effective network management** and **security**. There are two main strategies, which can be combined for mature organizations to ensure thoroughness and reliability.

Organizational process

Main Owner of the Asset Inventory

Designate a **primary person** or team responsible for maintaining the asset inventory. This **ensures accountability** and **consistency** in the updating process

Manual Updates

Update the inventory each time there is a change in the network. This could include **adding new devices**, **decommissioning old ones**, or making **significant configuration changes**

Annual Global Review

Conduct a **comprehensive review** of the entire asset inventory at least once a year. This helps to verify **the accuracy** of the records and **catch any discrepancies or omissions**.

Automated process

Using tools like network probes

Deploy network probes to **continuously monitor** the network for changes. These tools can automatically **detect new devices**, **changes in configurations**, and any **other relevant network activity**

Integration with other network systems

Integration with other NMS (Network Management Systems) like SolarWinds → Performance, configurations Data

Integration with EDR tools → Provide detailed information about endpoints, including real-time status, installed software, and security posture

Asset inventory: [Hands on] Create your asset inventory

1. How many assets do you find on the network?
2. What are they used for in the industrial process?
3. What are their IP addresses?
4. What kind of assets do you find?
5. What are their OS/firmware version?

Asset inventory: Introduction on network probes / passive network monitoring solutions

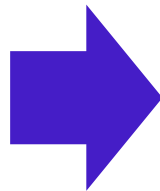
OT network probes are network Intrusion Detection System (IDS) dedicated to OT networks

It is a very powerful tool with multiple functionalities. The main functionality is network **detection** but the tool offers additional very useful features.

Main functionality: Detection

As network IDS, probe listens to the OT network, create a baseline of known and legitimate communications and then detect everything that deviates from the baseline

Probe can perform Deep Packet Inspection (DPI) on most OT protocols



Asset Inventory

Probe can keep a list of all assets identified on the network

Network Cartography

Probe can create a map of the network

Vulnerability & Obsolescence management

Probe can identify the version of assets and compare them with list of known vulnerabilities

Threat Detection

Probe has an updated database of known threats, like an antivirus

Asset inventory: Network probes: tool to help build your asset inventory?

Network probes are not a magic tool that can help you build your cartography and asset inventory

Probes only see what you let them see

What you need to do first

- 1 Build a **manual asset inventory**, using a simple Excel template for example
- 2 Formalize a complete **network diagram** of the OT network, manually as well
- 3 Reach a first level of maturity by implementing at least **priority projects**, such as network segmentation and secure remote access



Prerequisites

Having a good understanding of the network is essential before deploying network probe

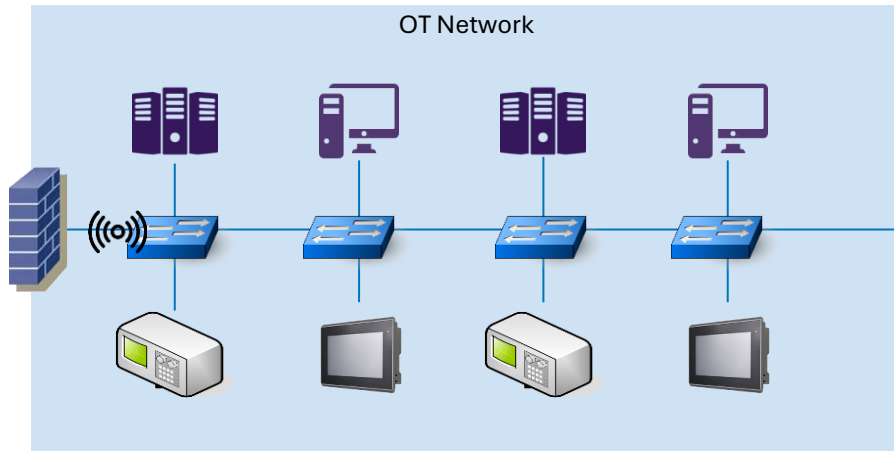
- You need to know the **list of your sub networks**
- Launching a **redesign of the OT network** might be necessary to make the most of the tool and reduce the number of collectors required
- A LAN refresh for the network switches might also be necessary to implement **port mirroring** instead of installing taps



Often seen as a **great tool for asset inventory** (e.g., to install quite early in the roadmap), a network probe is **more useful for detection** and is **aimed at more mature sites** and organizations

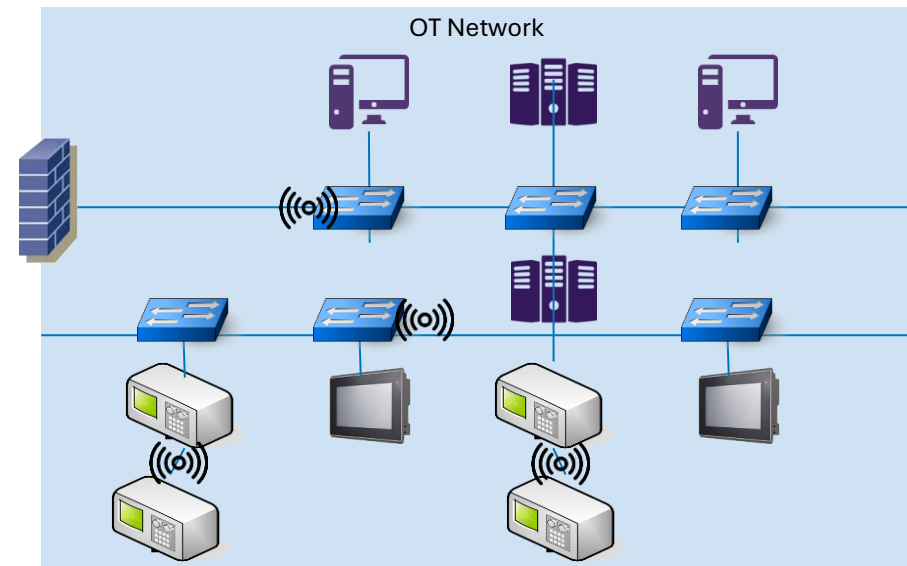
Asset inventory: Network probes: use case depending on network topology

Flat network



One collector is enough to capture all the network

Multiple layer network



Multiple collectors are needed to capture all traffic, a good understanding of the network is needed to know where to install the collectors



3. Securing ICS – Backups

- Backup strategies
- [Hands on] Backup your OT systems

Backups: Typical backup requirements for OT

Typical backup requirements for OT

1. Define and formalize a backup plan for all systems in the OT scope
2. Perform backups following the backup plan
3. Always have an offline copy of your backup
4. Document operational procedure for backup & restore
5. Regularly test the restore procedure on samples from the OT to verify the integrity of the backups

Backups: What is a backup plan?

Backup plan: document listing your OT backup strategy

In terms of format, it can be an Excel spreadsheet

What does it contain?

The list of assets/systems that need to be backed-up

- SCADA/DCS systems: configuration + data
- PLC programs
- Firewalls and switches configuration
- Important software and licenses (supervision and programming)

The backup requirements for each family assets

- Owner and responsibilities
- Data type to be backed up
- Methodology: manual vs. automated, full copy vs. only relevant data, etc.
- Storage: online + offline
- Frequency and retention period

Backups: OT backups: different than in IT?

Well not really!

Most backups in OT can be standard Windows and network devices backups

So everything can be automated with standard IT tools

Even for PLCs if you do not want to invest in dedicated OT solutions that are often quite expensive

How and when to backup a PLC?

- Every time there is a PLC program change
- PLC program change happen manually with an automation engineer using his engineering workstation (a Windows laptop)
- The program needs to be saved locally on the machine by the automation engineer
- Then there can be an automated process to save the program files or the entire Windows machine through IT tools

Backups: Is it sufficient?

Cyber resilience needs to be taken into account in OT

Backup is only the first step

Restore is required

And most importantly Disaster Recovery Plan (DRP) in case of cyber attacks

- Prioritization of systems is essential
- Minimum viable system to restart operation

Testing restoration of systems through reconstruction exercise at scale is necessary to be prepared in case of loss of information system

➔ These considerations can be included from the design of the systems

Backups: [Hands on] Backup your OT systems

1. Backup the PLC program using Schneider Electric SoMachine Basic software
2. Backup the SCADA project using Schneider Electric IGSS software



4. Securing ICS – Network Security

- [Hands on] Build network diagrams of a secure network with draw.io
- Improve network security step by step: from a flat network to fully segmented OT network
- [Hands on] Implement firewall rules on the ICS setup

Network security: [Hands on] Build network diagrams of a secure network with draw.io

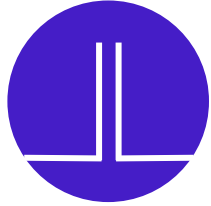
The network of your ICS setup is completely flat today

How do you want to segment it step by step to make it more secure?

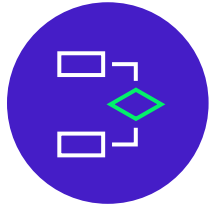
Draw several network diagrams of your setup to represent the different steps

1. IT/OT segmentation
2. Focus on remote access
3. Segmentation within the OT network

How to build a secure OT network architecture?



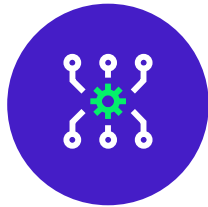
Step 1: IT and OT networks segmentation



Step 2: IT/OT segmentation with DMZ



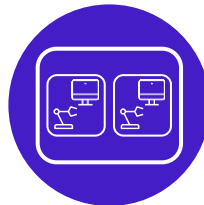
Step 3: Secure remote access to OT



Step 4: Dedicated OT infrastructure services



Step 5: Dedicated OT workstations for administration



Step 6: Segmentation within the OT

Standard industrial site without network segmentation

Purdue model

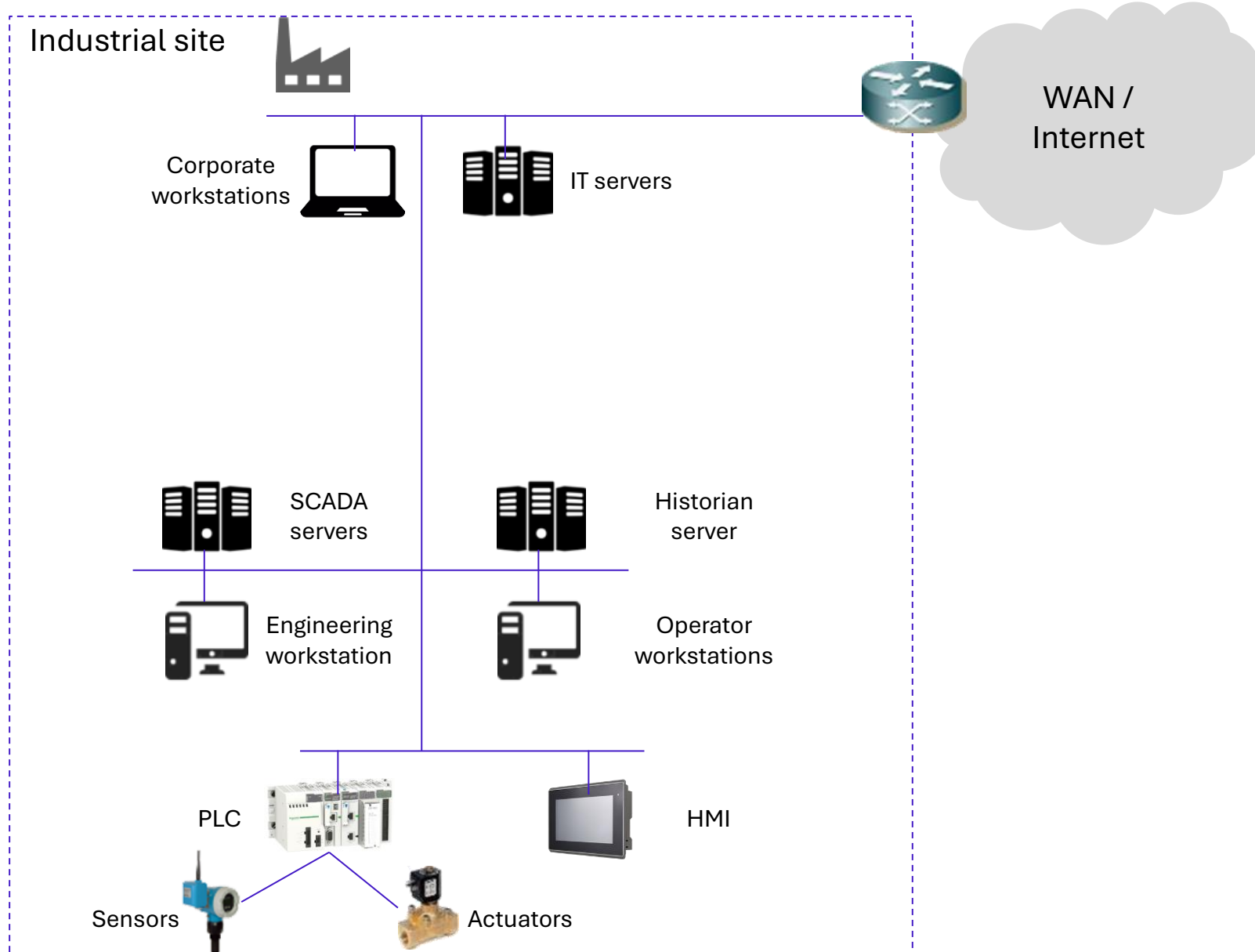
Level 4

Level 3

Level 2

Level 1

Level 0



Step 1: IT and OT networks segmentation

Purdue model

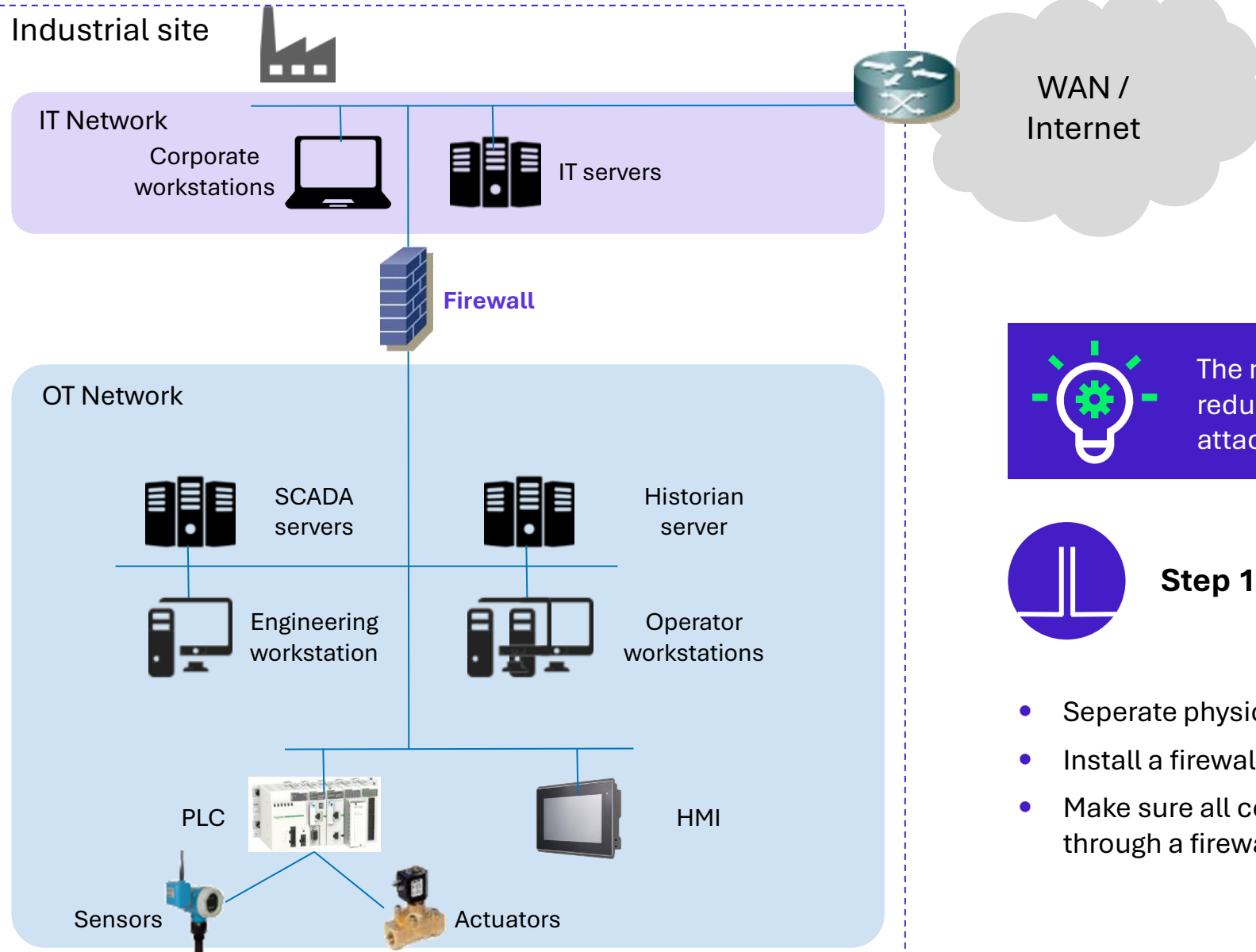
Level 4

Level 3

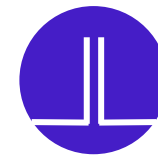
Level 2

Level 1

Level 0



The number of interconnections should be reduced to a minimum, to reduce the attack surface and facilitate maintenance



Step 1: IT and OT networks segmentation

- Separate physical IT components from OT components
- Install a firewall to segment IT and OT networks
- Make sure all communications between OT and IT go through a firewall

The Demilitarized Zone

Purdue model

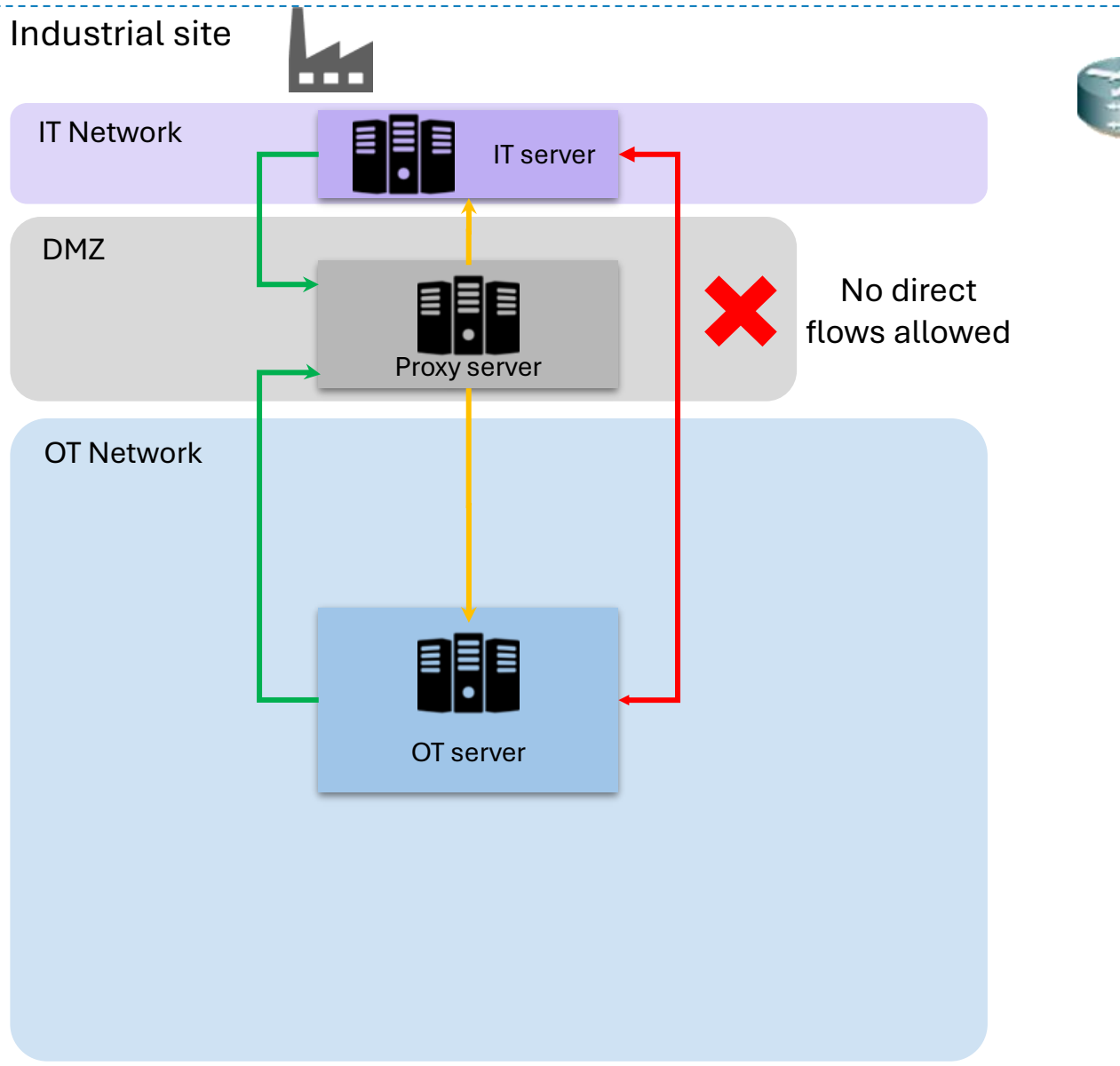
Level 4

Level 3

Level 2

Level 1

Level 0



WAN /
Internet

- Authorized connection
- Forbidden connection
- Restricted connection

In theory, DMZ best practices must be implemented:

- No direct communication between IT and OT
- Incoming communications to the DMZ preferred by default
- Tolerated outgoing communications from the DMZ when technically not feasible to do otherwise



Authorized connection for incoming communications does not mean that every connection is allowed! You still need to **restrict connections only to the necessary services**

Step 2: IT/OT segmentation with DMZ

Purdue model

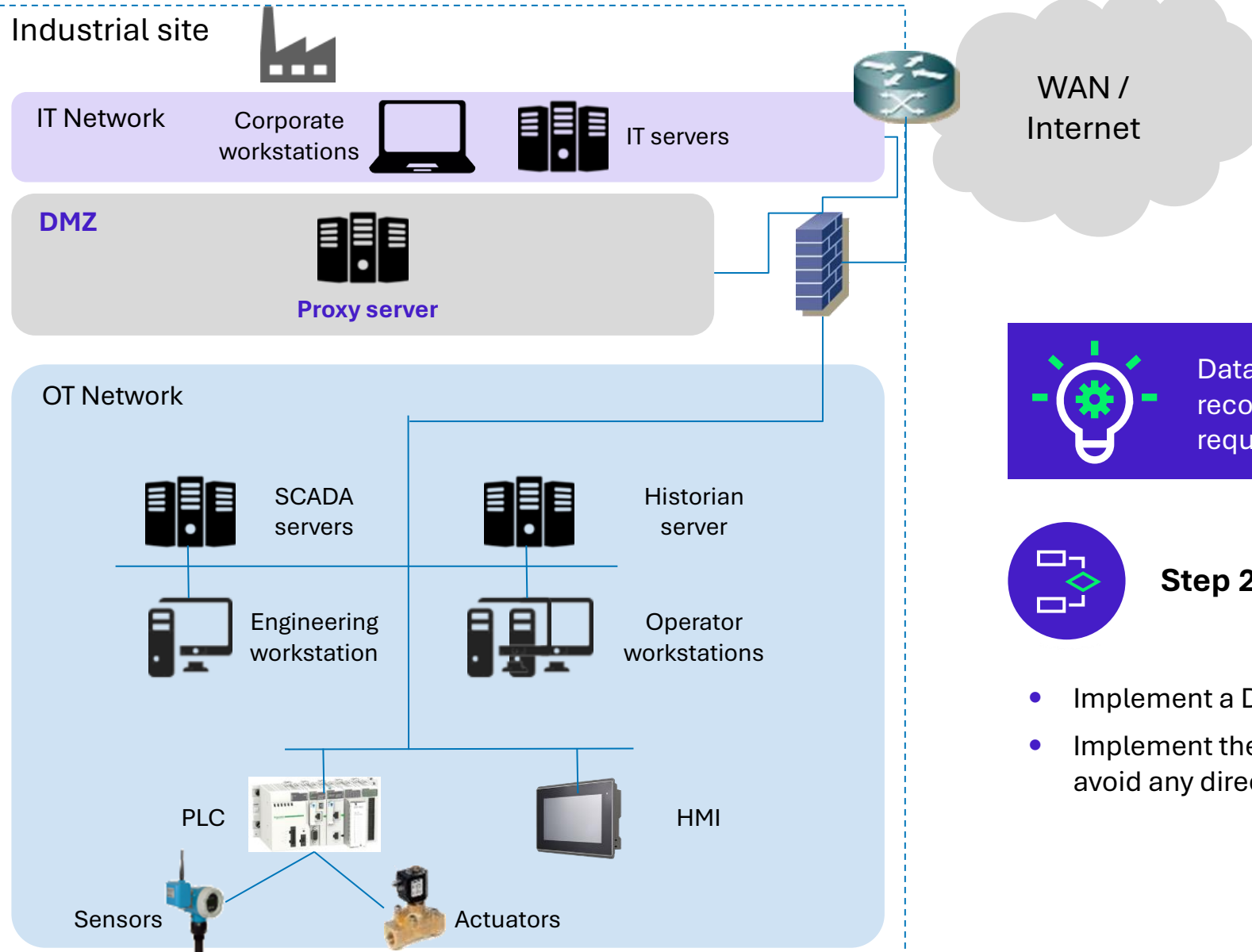
Level 4

Level 3

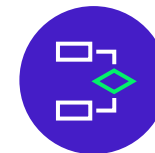
Level 2

Level 1

Level 0



Data should always be sent to the DMZ and recovered from it, rather than it being requested by the DMZ directly.



Step 2: IT/OT segmentation with DMZ

- Implement a DMZ between IT and OT
- Implement the necessary proxy server and services to avoid any direct communication

Step 3: Secure remote access to OT

Purdue model

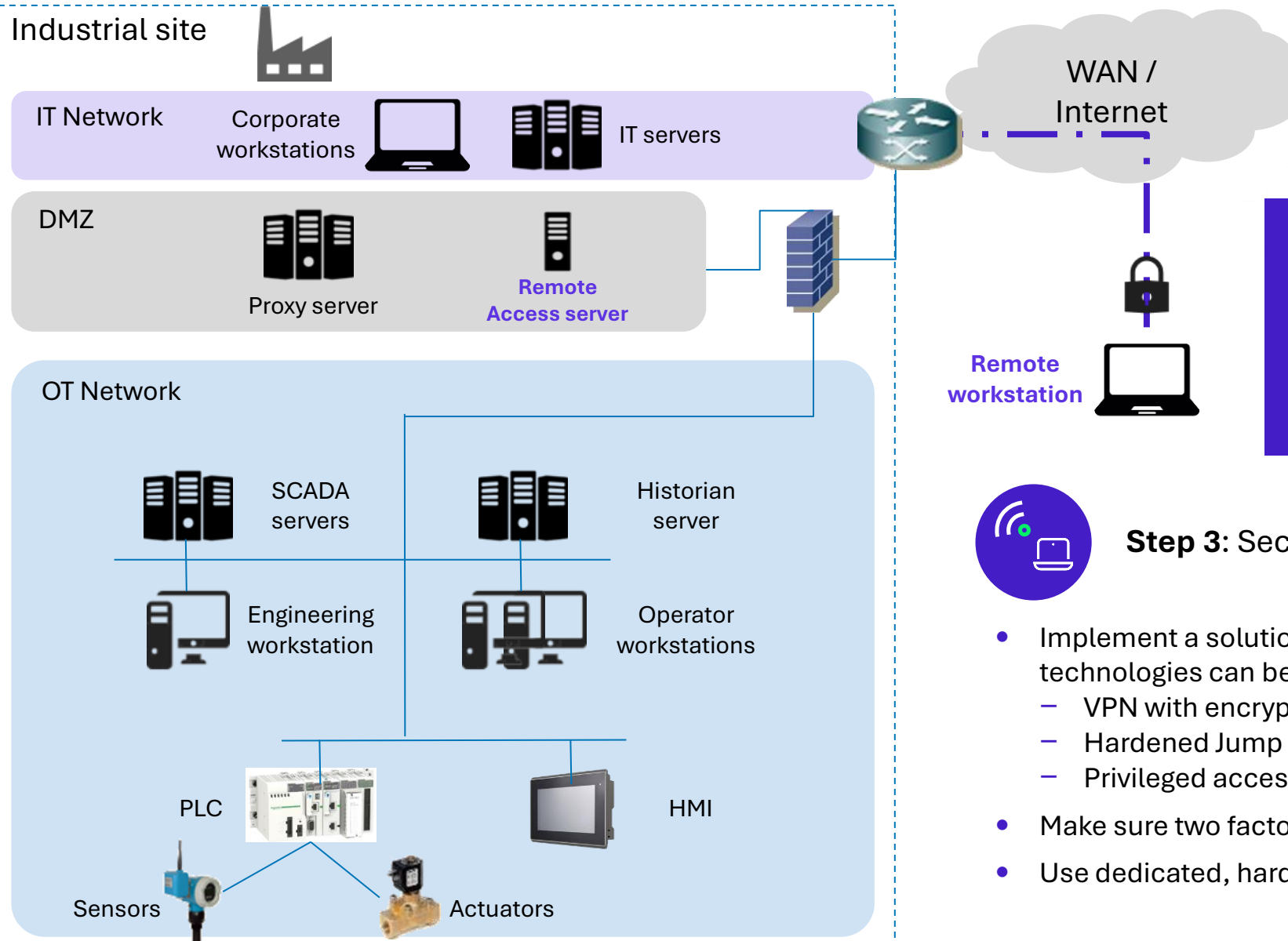
Level 4

Level 3

Level 2

Level 1

Level 0



A secure remote access solution, validated by the company must be implemented.



Step 3: Secure remote access to OT

- Implement a solution validated by the company - several technologies can be used:
 - VPN with encrypted tunnel
 - Hardened Jump Host
 - Privileged access management system
- Make sure two factor authentication is enabled
- Use dedicated, hardened workstations when possible

Step 4: Dedicated OT infrastructure services

Purdue model

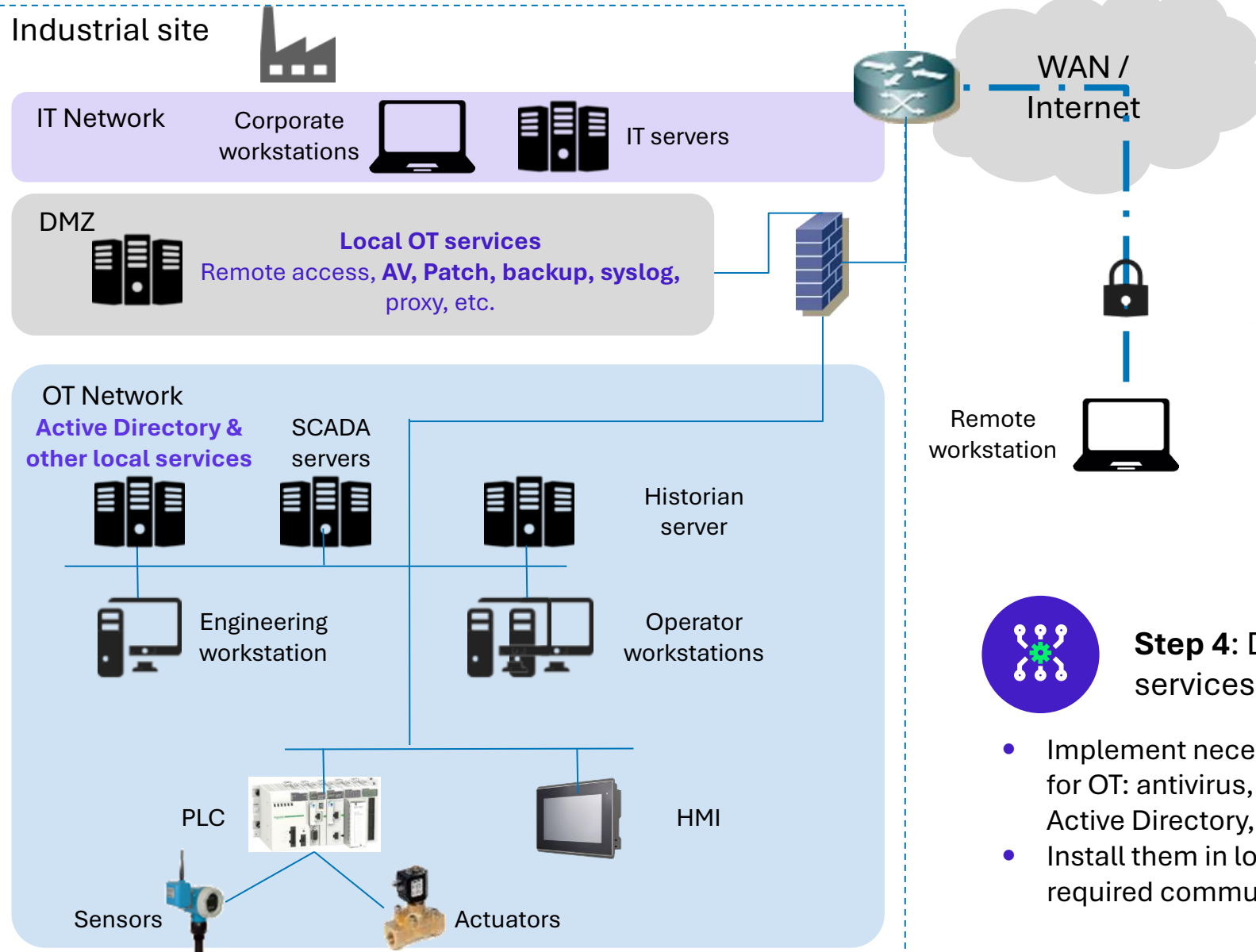
Level 4

Level 3

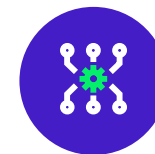
Level 2

Level 1

Level 0



Infrastructure services can be situated in either the DMZ or the OT network. As a general rule, if a server communicates with resources outside the OT, it must reside in the DMZ.



Step 4: Dedicated OT infrastructure services

- Implement necessary infrastructure and security services for OT: antivirus, patch management, backup, syslog, Active Directory, etc.
- Install them in local DMZ or core OT network depending on required communications

Step 5: Dedicated OT workstations for administration

Purdue model

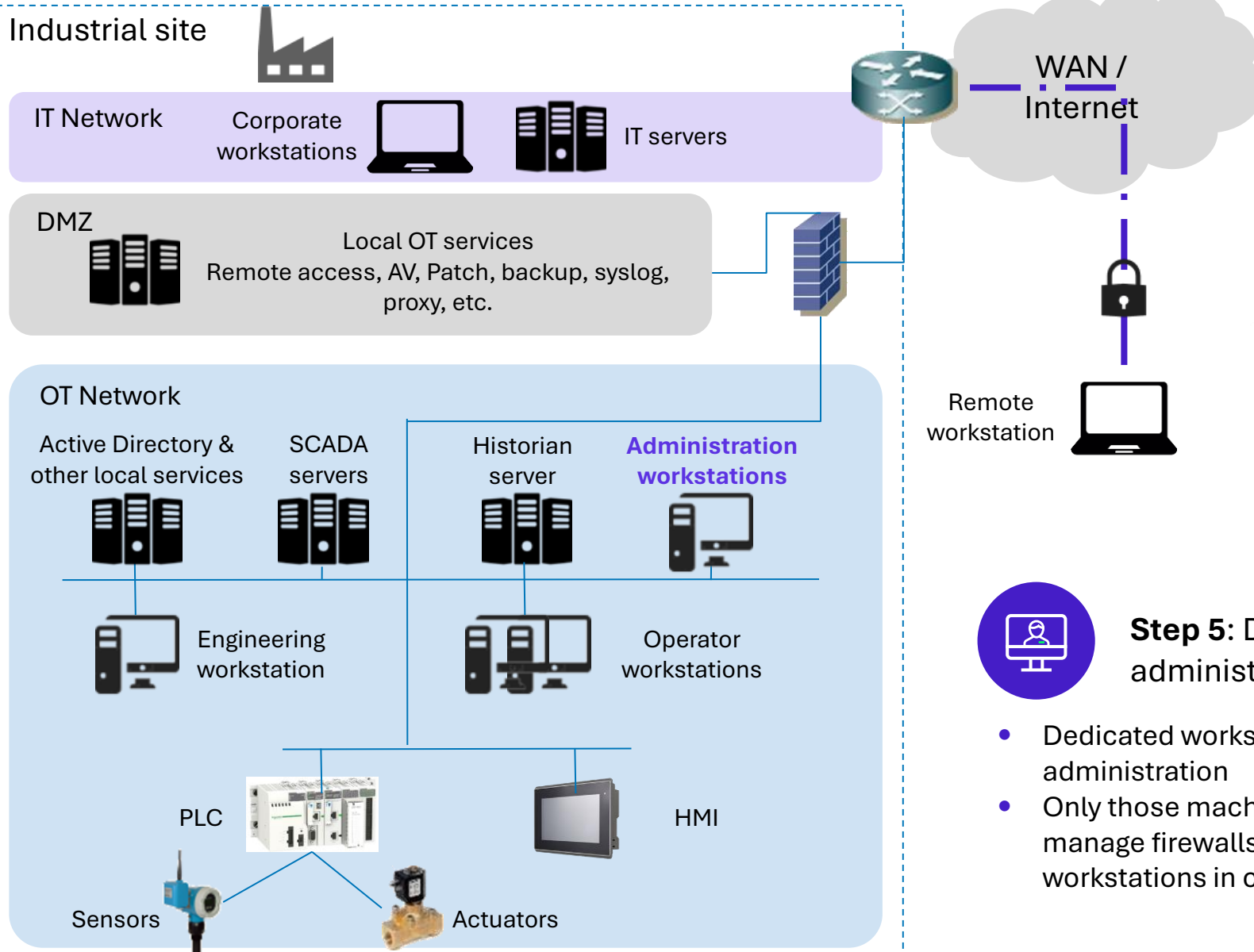
Level 4

Level 3

Level 2

Level 1

Level 0



Administration might be a tricky word in OT. In that case, administration means network and system administration i.e. managing firewalls, switches, servers and workstations.



Step 5: Dedicated OT workstations for administration

- Dedicated workstations must be implemented for OT administration
- Only those machines must be allowed to connect to and manage firewalls, switches, as well as servers and workstations in case of administration through RDP

Step 6: Segmentation within the OT

You can introduce OT segmentation by several means that can be combined together, depending on your network's current complexity and structure:

Dual homed machines

By having two network interfaces, each connected to a different network, you can limit the exposure of critical systems to potential threats from less secure networks while allowing selective data exchanges. The device with 2 network cards will thus act as router.

Segmentation by systems

By creating separate networks for different systems, you can tailor security measures to each system's specific needs, reducing the overall attack surface and containing potential breaches within individual segments, especially if they are managed by different teams or suppliers.

Segmentation following Purdue model

By dividing the network into layers (at least supervision and PLCs), you enhance security and control by isolating different levels of devices with various criticality levels with firewalls and monitoring traffic, thereby reducing the risk of cross-segment threats.

Step 6: Segmentation within the OT – Dual homed machines

Purdue model

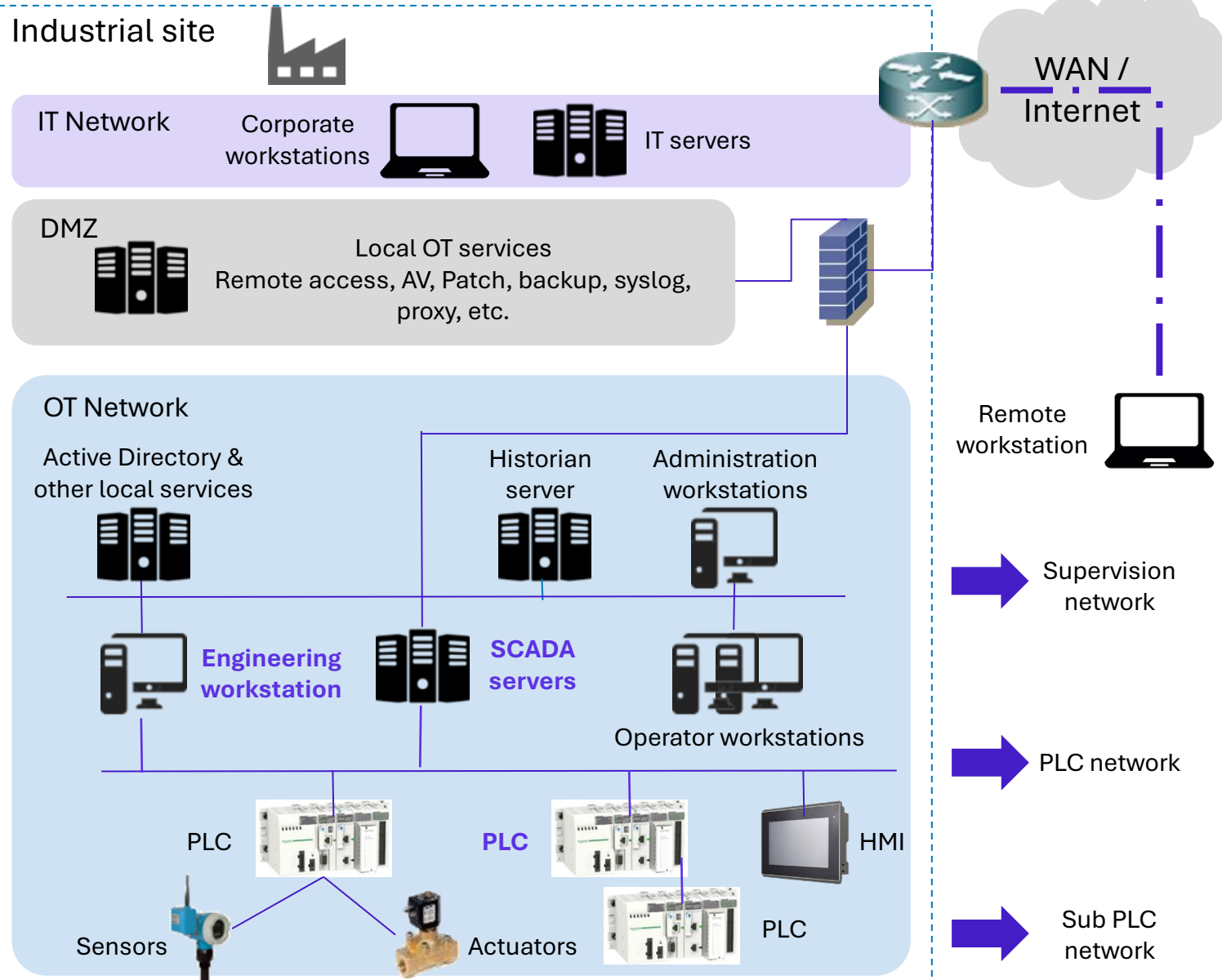
Level 4

Level 3

Level 2

Level 1

Level 0



OT network segmentation design with dual homed machines are often offered by OT vendors:

- One network for the supervision
- One network for the PLCs and process network

The SCADA server acts as pivot for the networks

This method can allow you to implement basic segmentation without extensive infrastructure changes. It is adapted to networks where SCADA servers need to communicate without filtering to PLCs

However, be careful not to bypass this design with another system needing to access a PLC directly!

PLCs also often act as dual homed machines to allow network segmentation across the different parts of the industrial process

Step 6: Segmentation within the OT – By systems

Purdue model

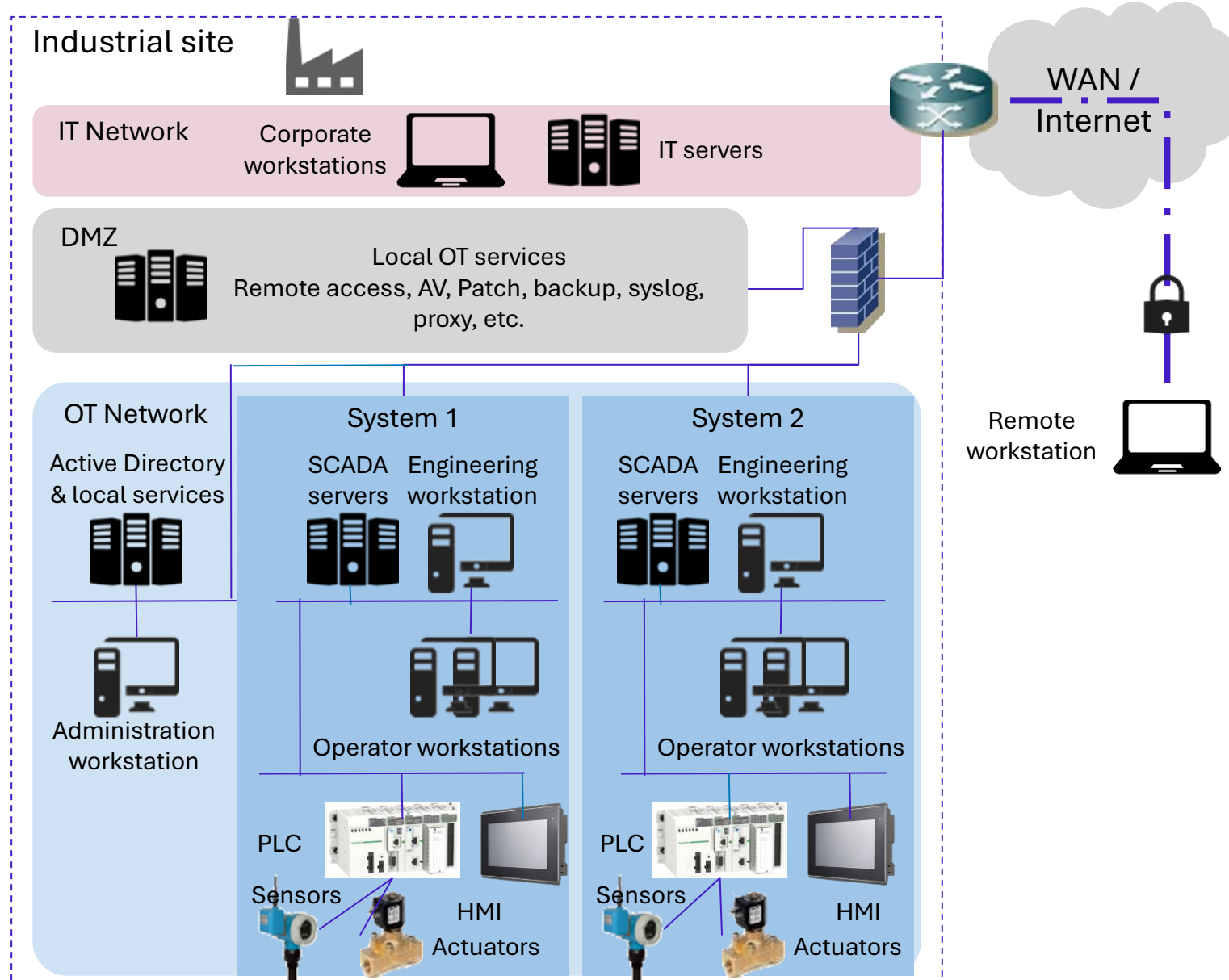
Level 4

Level 3

Level 2

Level 1

Level 0



Segmentation within the OT can be done by systems or applications.

If you have multiple systems, having one dedicated network for each system is recommended in the following cases:

- Systems are running independently with limited exchanges between each other
- Different teams, or suppliers are managing the systems

However, if different systems are fully integrated together and rely on common OT devices, network segmentation might not be necessary.

Segmenting by systems allows the tailoring of segmentation to specific operational needs. It is adapted to networks that have distinct systems with varying security requirements.

Step 6: Segmentation within the OT – Purdue Model

Purdue model

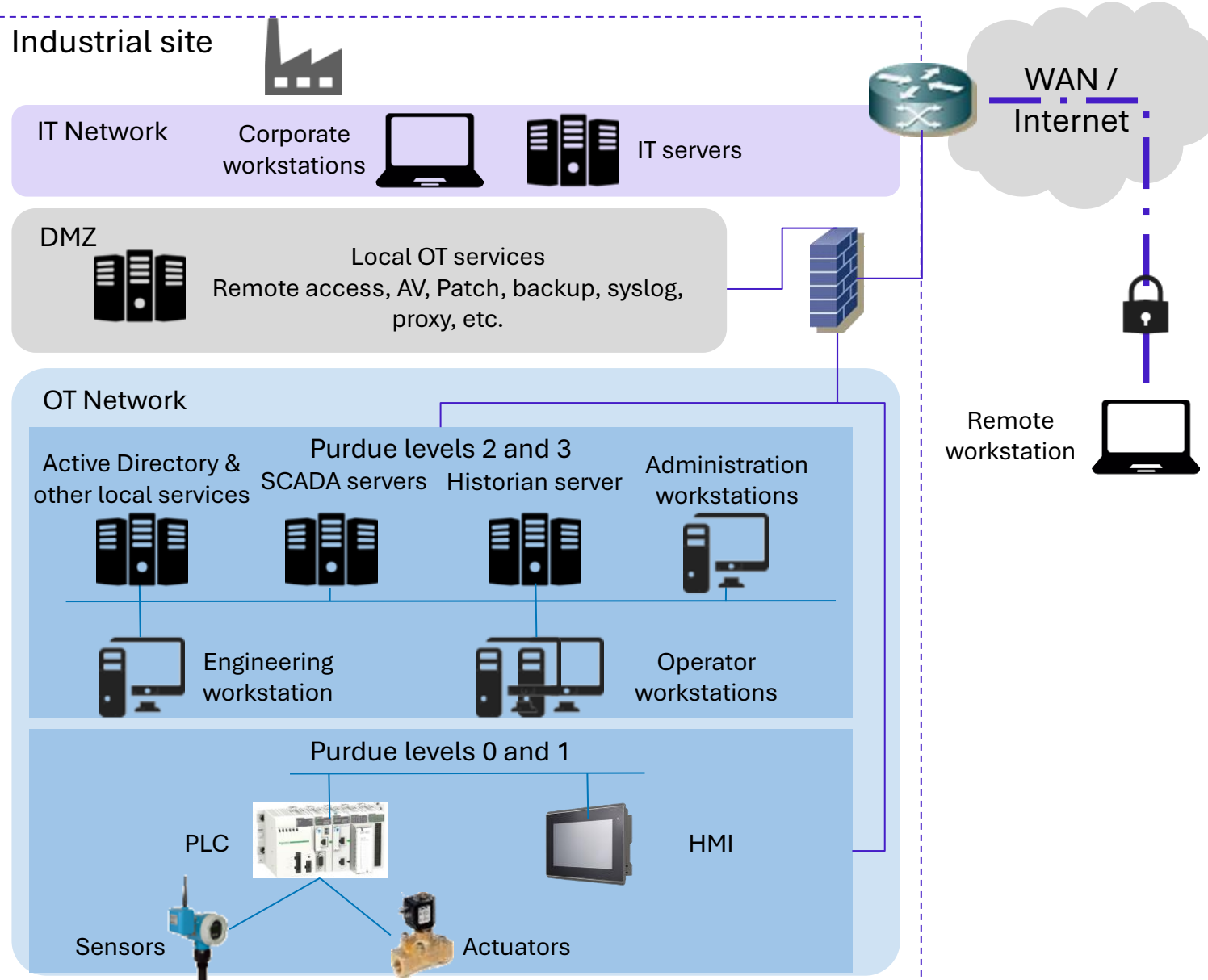
Level 4

Level 3

Level 2

Level 1

Level 0



The Purdue model is a structural model for industrial control system that splits OT devices into multiple layers, each having its own characteristics and needs.

This model is usually used as a reference architecture for network segmentation.

Theoretically, one dedicated network could be implemented for each level of the Purdue model:

- 0 for sensors and actuators
- 1 for PLCs
- 2 for supervision
- 3 for Manufacturing operations systems

In practice, splitting into two networks is sufficient:

- Levels 0 and 1 for low level OT devices
- Level 2 and 3 for the more standard Windows world with servers and workstations

Step 6: Segmentation within the OT - Recommendations

To summary, here are the main recommendations to segment the OT network internally:

1

**Dedicated OT
firewall**

A dedicated OT firewall should be implemented, in addition to the IT/OT firewall to manage specifically the segmentation and filtering between the different OT sub networks.

2

**Segment OT
into multiple
sub networks**

**At least one
network / VLAN
should be
implemented for
the following
devices.**

Administration

Infrastructure services

Wireless devices

OT servers

OT workstations

PLCs and other OT devices

**Do not forget to
segment as well
for each system!**

Reference network architecture

Purdue model

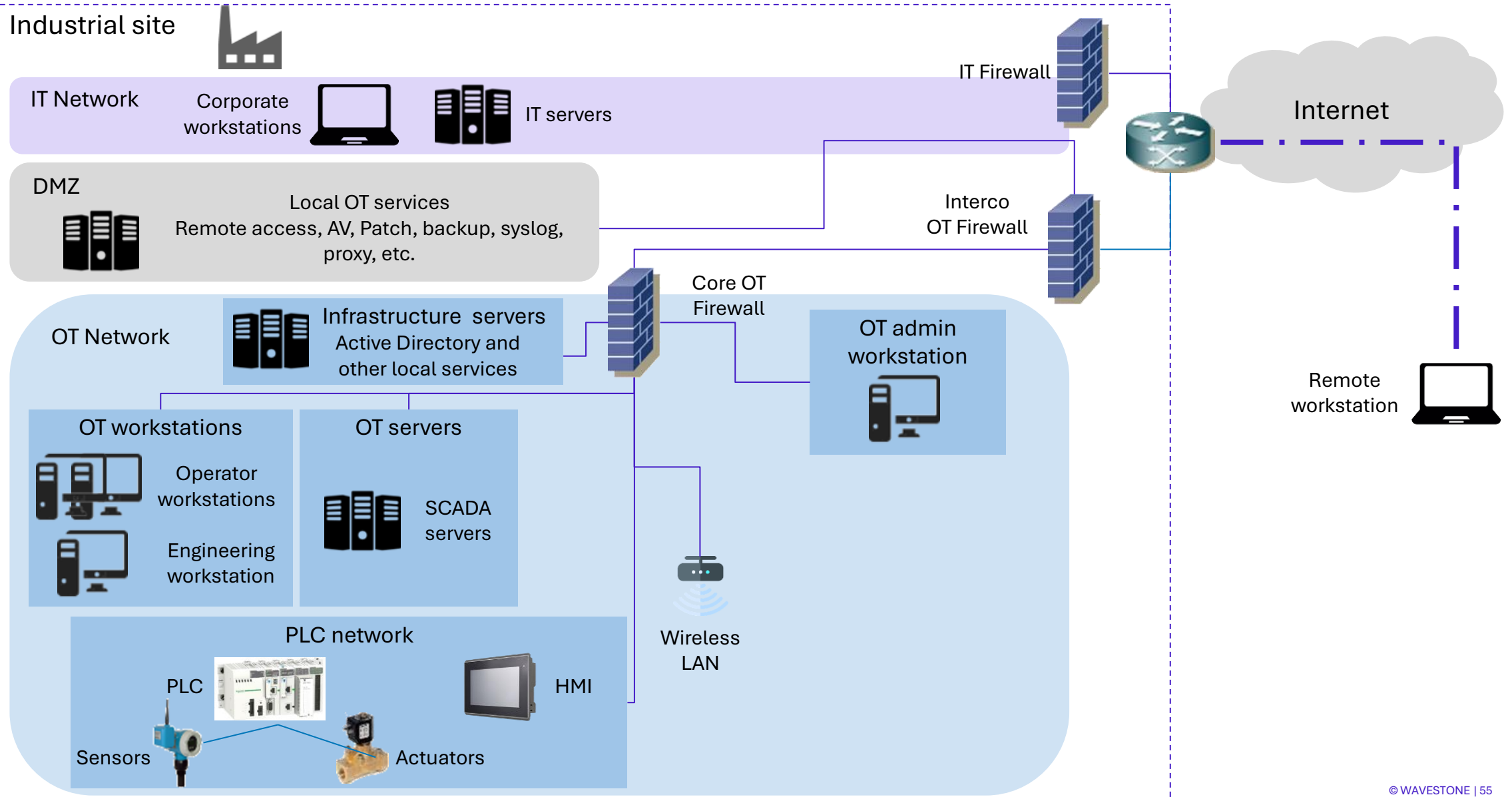
Level 4

Level 3

Level 2

Level 1

Level 0



How to scale? Central OT DMZ

Purdue model

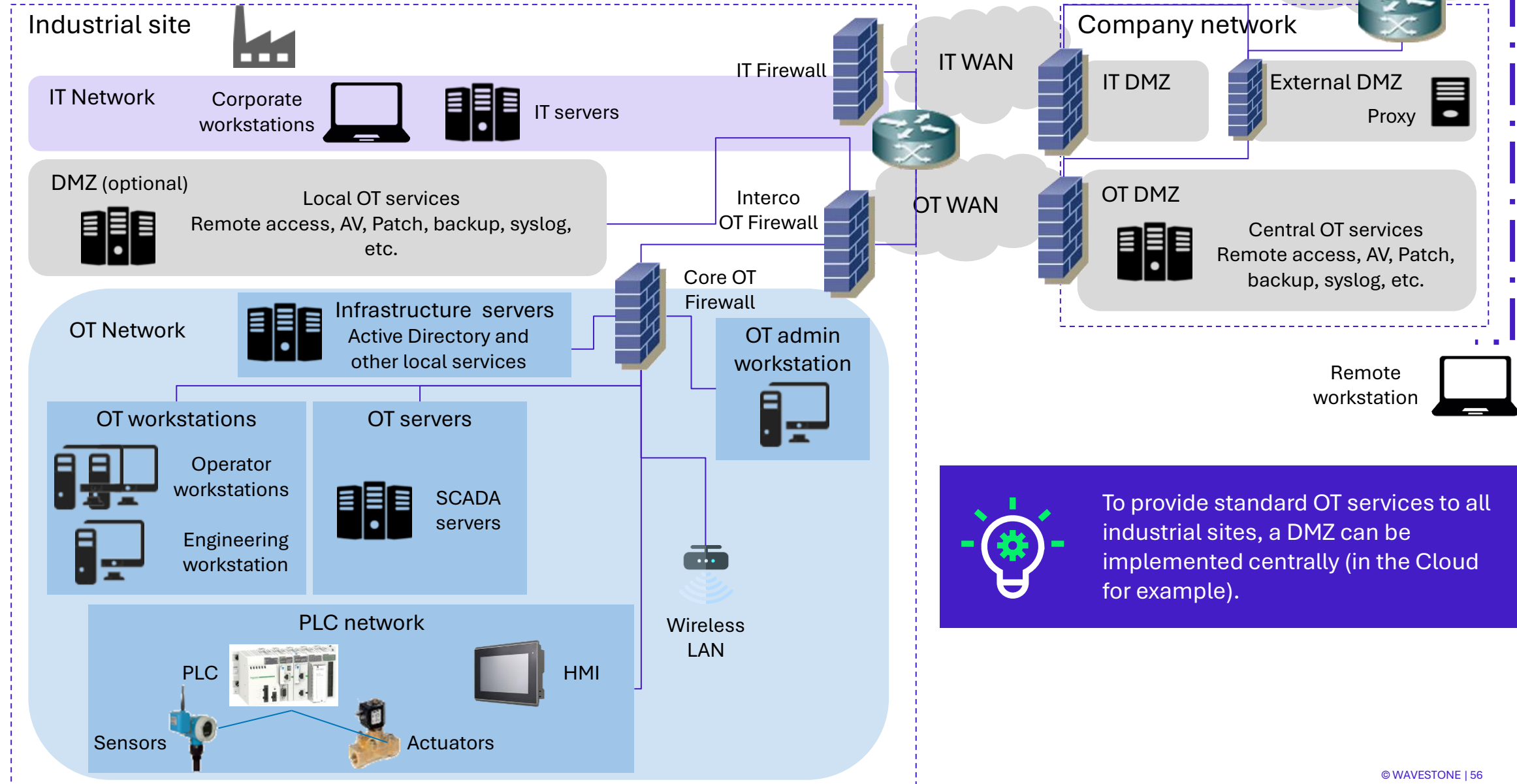
Level 4

Level 3

Level 2

Level 1

Level 0



How to scale? Central OT DMZ

Purdue model

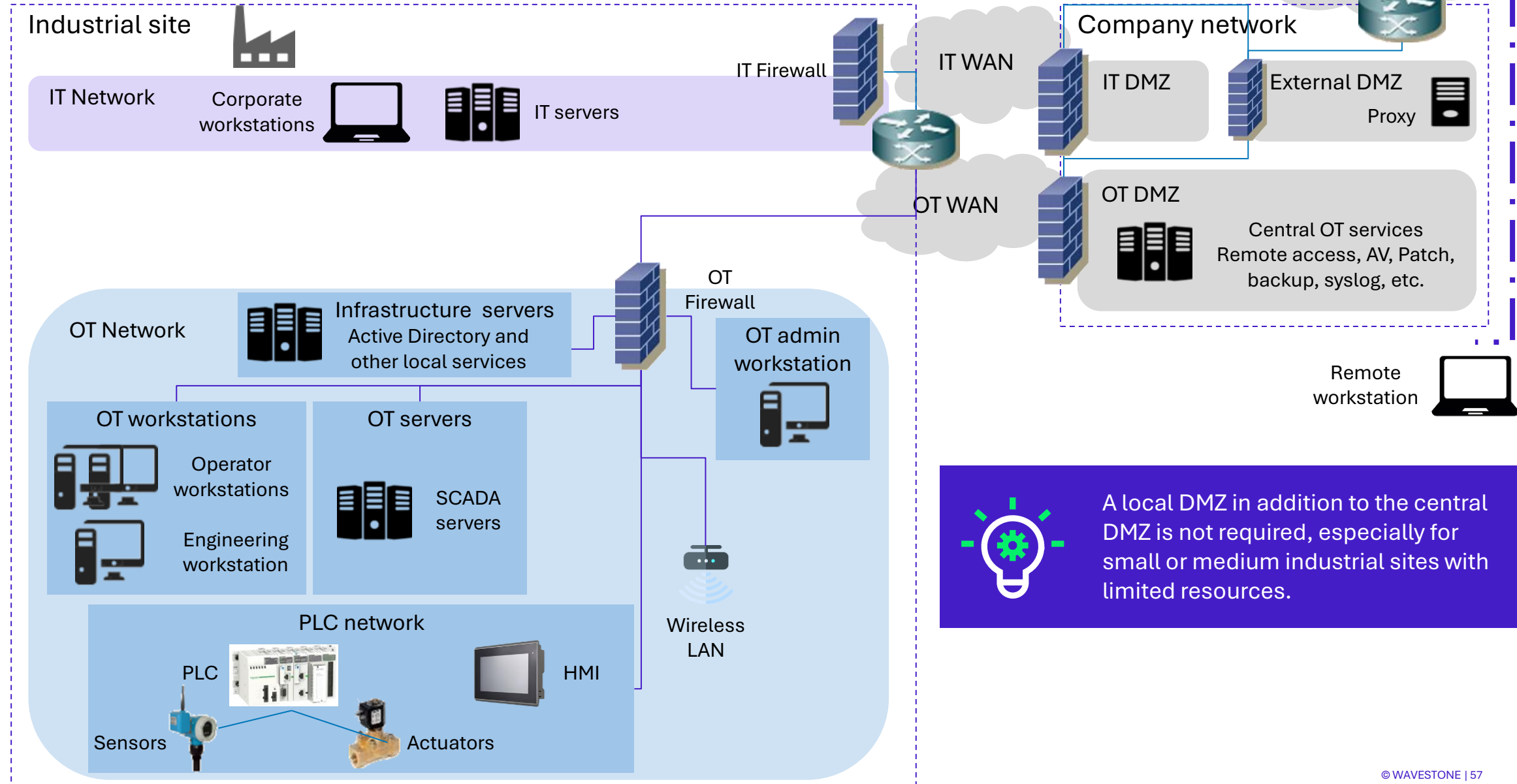
Level 4

Level 3

Level 2

Level 1

Level 0



A local DMZ in addition to the central DMZ is not required, especially for small or medium industrial sites with limited resources.

Network security: [Hands on] Implement firewall rules on the ICS setup

Connect to the pfSense web interface and implement the necessary filtering rules



5. Securing ICS – System hardening

- Guidelines on Windows hardening in OT environment
- [Hands on] Harden the SCADA machine using provided Windows scripts
- Guidelines on network devices hardening
- [Demos with TM221 PLC] A few words on PLC hardening

System hardening

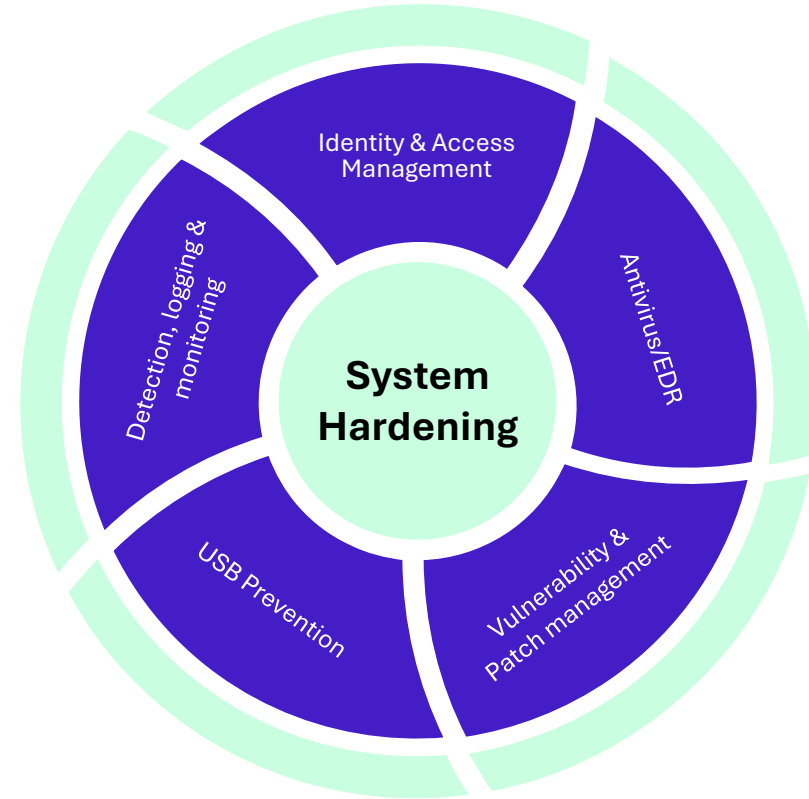
Guidelines on hardening in OT environment

In cybersecurity, the **hardening** process consists of **applying specific configurations** to reduce the attack surface of assets in order to protect against the risks of exploiting a vulnerability.

Key system hardening measures consist of the following:

- Disable / Uninstall everything that is not necessary
- Use secure versions of protocols/services
- Configure specific system parameters to enhance security

But **other cybersecurity topics** can be addressed when considering system hardening



System hardening

Windows hardening – Cybersecurity topics



Accounts

Only legitimate people must be able to access machines



Antivirus

A dedicated software must be installed to protect from malware



Programs & Configurations

System settings must be configured to only allow the programs necessary for operations and harden necessary services



Updates

Mechanisms must be put in place to keep systems and programs up to date



USB Protection

Mechanisms must be put in place to ensure that physical access to the machine does not allow the security mechanisms to be circumvented.



Audit/Logging

Machines must log events to trace user and system actions

System hardening

Windows hardening guidelines



Accounts

1. Rename and disable default accounts (Administrator and Guest)
2. Remove or disable unused accounts
3. Create nominative accounts for standard users & administration
4. Make sure only legitimate accounts are part of the local administrators group
5. Enable a strong Password Policy and Account Lockout Policy
6. Protect screen saver with a password



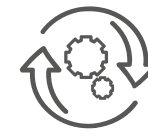
Antivirus

1. Install an antivirus and make sure signature databases are updated daily



USB Protection

1. Disable USB storage on machines where USB devices are not used
2. Disable Autorun
3. Configure a green list of USB thumb drives



Updates

1. Install Microsoft security patches at least annually



Programs & Configurations

1. Uninstall unnecessary programs
2. Harden the User Account Control (UAC) parameters
3. Configure the Windows Firewall
4. Make sure internet access is prohibited
5. Disable or harden RDP (Remote Desktop Protocol)
6. Disable or harden SMB (Server Message Block)
7. Check and delete unnecessary startup programs and services
8. Display file extension
9. Install Bitlocker on laptops



Audit/Logging

1. Configure the advanced audit policy
2. Define a maximal size for event log (20 M bytes)
3. Configure logs archiving once log file is full
4. Configure NTP client to synchronize clock with same NTP server in the plant for all devices

System hardening

Windows hardening prerequisites



Some hardening actions may impact the operation of certain applications, user experience, or desktop performance. These actions must therefore be carried out with caution, following the following principles:

1. Perform hardening actions preferably during a **maintenance period**
2. Perform a **backup** of the targeted machine before implementing hardening measures
3. Ensure that it is possible to **restore the machine** from the previous backup
4. Perform **non-regression tests** throughout the implementation of the hardening protocol, to ensure that industrial production runs smoothly.

System hardening: [Hands on] Harden the SCADA machine using provided Windows scripts

1. Uninstall all unnecessary software or program
2. Implement a robust password policy
3. Implement a robust account lockout policy
4. Harden the User Account Control (UAC) parameters
5. Configure the Windows Firewall
6. Disable SMB or harden it
7. Disable RDP or harden it
8. Restrict the use of removable media
9. Configure the audit policy
10. Configure the Event log

System hardening: Guidelines on network devices hardening

Similar principles apply to network devices hardening:

1. Create nominative accounts for administration
2. Configure robust passwords and password policy
3. Disable default accounts
4. Update the firmware
5. Disable unused interfaces, protocols or physical ports
6. Use secure versions of protocols
7. Harden SNMP parameters
8. Activate logging
9. Configure NTP

System hardening: A few words on PLC hardening

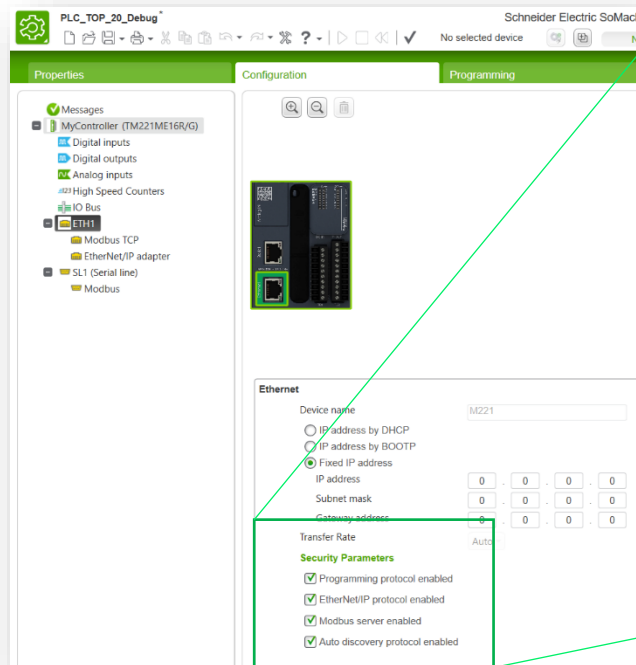
- PLC hardening is **not a priority**
 - A lot of things cannot be done on old devices
- **However, it is important to reduce the attack surface and there are some basics to follow:**
 - **Protect PLC program** with a password
 - Disable unused interfaces and protocols: HTTP, Telnet, FTP etc.
 - Or use secure version of protocols: **HTTPS, SSH, SFTP** etc.
 - Change default passwords on used interfaces (HTTP, FTP, SNMP etc.)
 - Configure ACL (Access Control List) wherever you can
 - Disable remote programming (when relevant, especially for PLCs safety)
- Other helpful things:
 - Firmware update
 - Logging configuration (when possible)

Best way to protect PLCs is through **network filtering**: firewall implementation with restricted firewall rules

System hardening

[Demos with TM221 PLC]

The Schneider TM221 is an entry-level PLC, with very limited configuration possibilities



Security Parameters

- ☒ Programming protocol enabled
- ☒ EtherNet/IP protocol enabled
- ☒ Modbus server enabled
- ☒ Auto discovery protocol enabled

Allows the PLC to be configured and programmed over the network. If disabled, you need to connect using USB

Allows the PLC to respond to specific network scans by soMachineBasic to identify PLCs on the network



6. Securing ICS – Detection on the cheap

- Basic cybersecurity monitoring
- [Hands on] Implement OT detection scenarios on the SCADA following TOP 20 PLC secure coding practices

Detection on the cheap: Basic cybersecurity monitoring

Detection in OT is not that different than in IT

Indeed, many assets in OT are just like in IT (servers, workstations, firewalls, switches, etc.)

Moreover, many attacks in OT will come from IT, so it is a good thing to start with standard IT detection scenarios



First configure logs locally

- **Windows machines**
- **Network switches**
- **Firewalls**
- Bonus: **application logs + PLCs** (but PLCs do not usually generate logs, especially old assets)



Then centralize logs

- Start by sending **firewall logs** first to your SIEM
- Use an intermediary **syslog server** to centralize other logs (Windows logs and network switches logs)
- Consider adding **other log sources**: AV/EDR, network probes, Active Directory, etc.



SOC

- Working on **detection scenarios is important**
- Start by **standard IT** detection scenarios
- Include **log sources step by step**
- Add **OT detection** scenarios when mature enough

Detection on the cheap

TOP 20 PLC secure coding practices – Introduction

1 / 2

Secure PLC Coding Practices: Top 20 List

Version 1.0 (15 June 2021)



1. Modularize PLC Code

Split PLC code into modules, using different function blocks (sub-routines). Test modules independently.

2. Track operating modes

Keep the PLC in RUN mode. If PLCs are not in RUN mode, there should be an alarm to the operators.

3. Leave operational logic in the PLC wherever feasible

Leave as much operational logic e.g., totalizing or integrating, as possible directly in the PLC. The HMI does not get enough updates to do this well.

4. Use PLC flags as integrity checks

Put counters on PLC error flags to capture any math problems.

5. Use cryptographic and / or checksum integrity checks for PLC code

Use cryptographic hashes, or checksums if cryptographic hashes are unavailable, to check PLC code integrity and raise an alarm when they change.

Download the full document on www.plc-security.com

Detection on the cheap


Content of the TOP20

Title

25 / 42

Secure PLC Coding Practices: Details

Version 1.0 (15 June 2021)



PLC Security
TOP 20 LIST

Short description

Security objective

- Integrity of
 - PLC logic
 - I/O values
 - PLC variables
- Hardening
- Resilience
- Monitoring

12. Validate inputs based on physical plausibility

Ensure operators can only input what's practical or physically feasible in the process. Set a timer for an operation to the duration it should physically take. Consider alerting when there are deviations. Also alert when there is unexpected inactivity.

Security Objective	Target Group
Integrity of I/O values	Integration / Maintenance Service Provider

Target group:

- Product supplier
- Integration / Maintenance Service Provider
- Asset Owner

Guidance

a) Monitor expected physical durations

If the operation takes longer than expected to go from one extreme to the other, that is worthy of an alarm. Alternatively, if it does it too quickly, that is worthy of an alarm too.

Example

a) Monitor expected physical durations

- The gates on a dam takes a certain time to go from fully closed to fully open
- In a wastewater utility, a wet well takes a certain time to fill

Guidance:

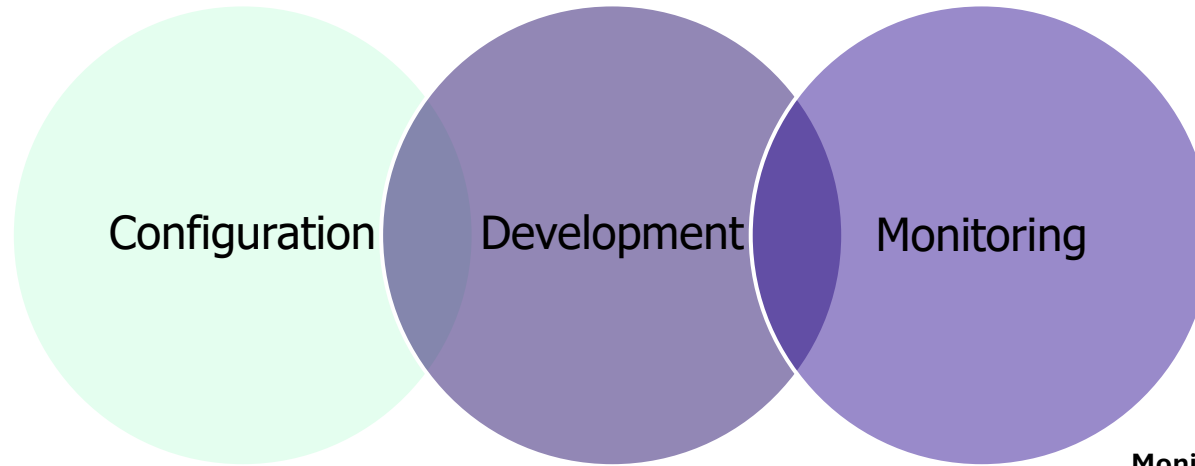
Everything that helps implementing the practice

Example:

Implementation or scenario examples for certain industries, products, ...

Detection on the cheap

Our understanding of the TOP 20



Configuration

- 3. Leave operational logic in the PLC wherever feasible
- 10. Assign designated register blocks by function (read/write/validate)
- 13. Disable unneeded / unused communication ports and protocols
- 14. Restrict third-party data interfaces
- 15. Define a safe process state in case of a PLC restart

Development

- 1. Modularize PLC Code
- 6. Validate timers and counters
- 7. Validate and alert for paired inputs / outputs
- 8. Validate HMI input variables at the PLC level, not only at HMI
- 9. Validate indirections
- 11. Instrument for plausibility checks
- 12. Validate inputs based on physical plausibility

Monitoring

- 2. Track operating modes
- 4. Use PLC flags as integrity checks
- 5. Use cryptographic and / or checksum integrity checks for PLC code
- 16. Summarize PLC cycle times and trend them on the HMI
- 17. Log PLC uptime and trend it on the HMI
- 18. Log PLC hard stops and trend them on the HMI
- 19. Monitor PLC memory usage and trend it on the HMI
- 20. Trap false negatives and false positives for critical alerts

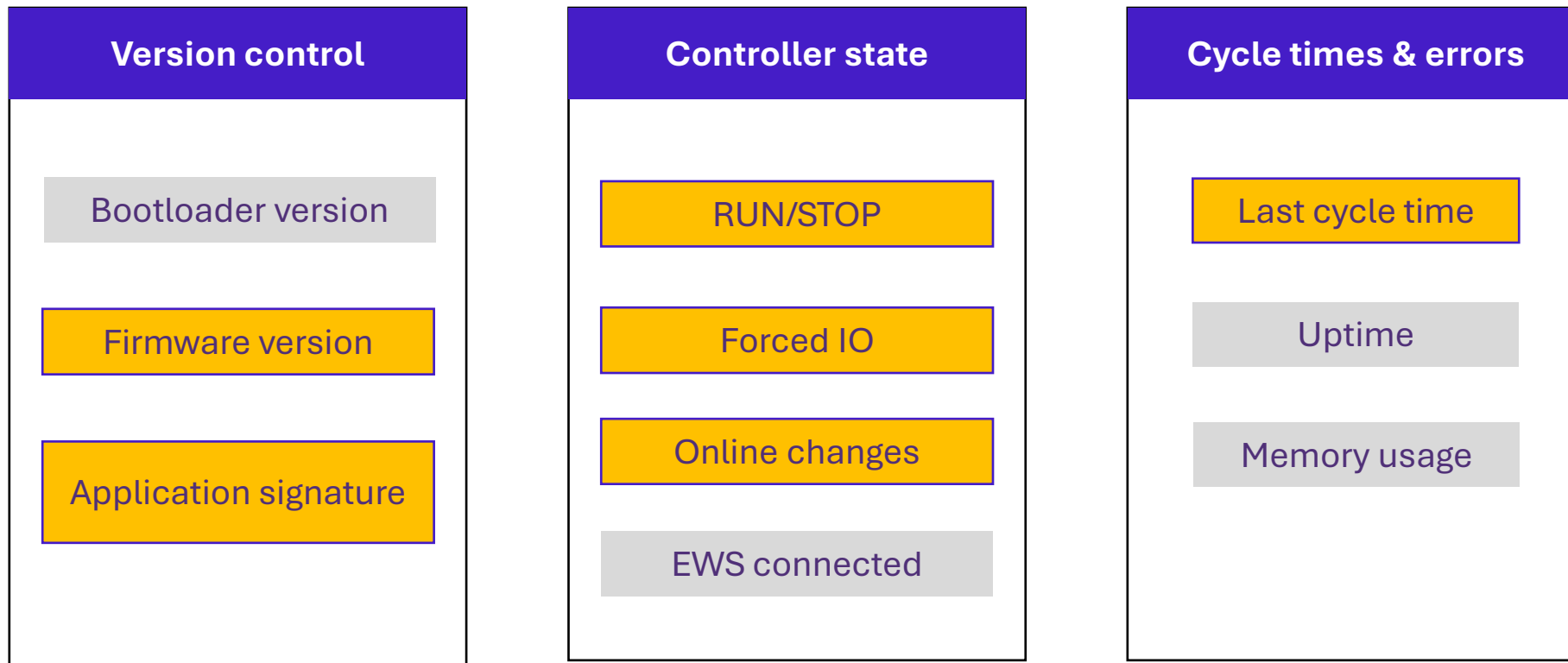
Detection on the cheap

[Hands on] PLC monitoring for cybersecurity

XXX

Implemented in the demo environment

Leverage operational data to identify potential cyber-related events





Conclusion

**Securing ICS is not that hard in itself
But how can we make it work at scale?**

Industrial Control Systems: how to secure them at scale!



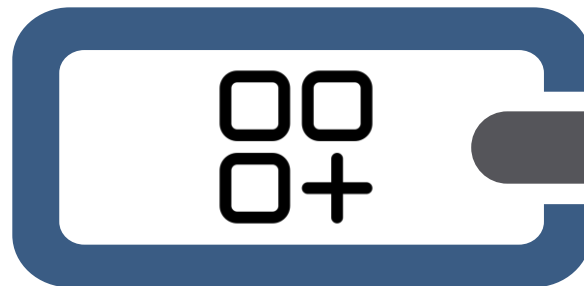
Key streams to launch at organization level for an OT cybersecurity program

1
OT governance: build
your organization of
OT correspondents

2
Industrial Critical
Sites protection:
focus first on your
critical sites
security

3
OT cybersecurity at
scale: projects at BU
level to secure all
sites

Key success factors



**Go on site & Know your
OT environment**



**Start small & grow
Be pragmatic**



**Put the human at the
center of the approach**

