

INDUSTRIAL SECURITY

CONFERENCE COPENHAGEN

2025

Name: Mischa Diehm, Martin Scheu
Design & Defense OT-Networks

Plan

Workshop

- Big Picture
- Lab Intro
- Defend
- Monitoring
- Zones & Conduits
- Network Automation

And in between, Labs, Labs, Labs.
.. ok, we try ..

Who we are



Mischa Diehm



Martin Scheu

Big Picture



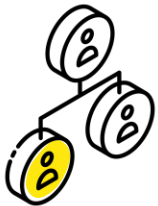
OT Networks are Business-critical

- Network disruptions lead to significant financial losses (e.g., production downtime).
- Regulatory pressure is increasing.



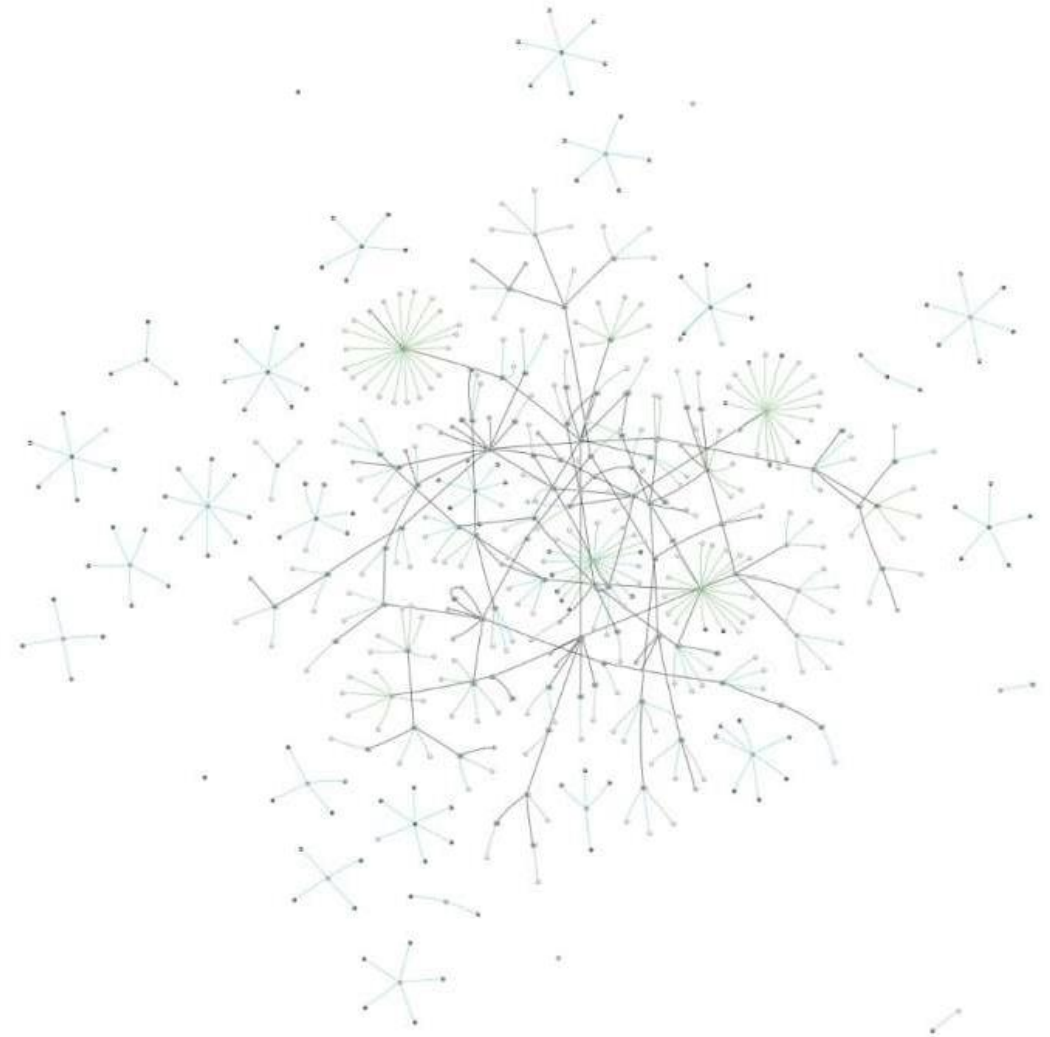
Growth and Complexity of OT Networks

- Historically grown structures
- Increasing interconnectivity (Smart Grid, Industry 4.0, etc.)
- IT, OT, and IoT are converging



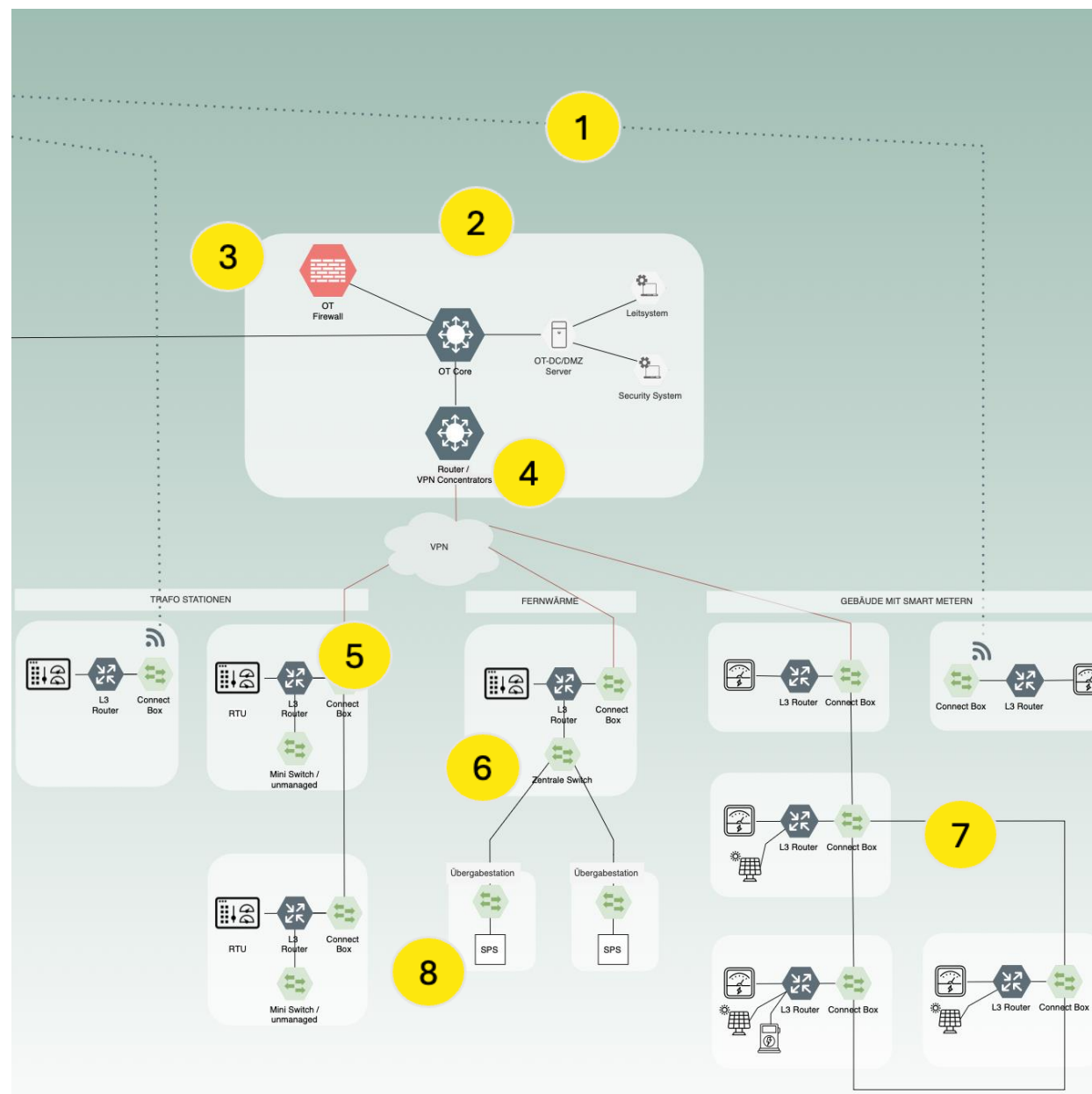
Shortage of Expertise and Time

- Few people are familiar with networks
- Low level of (network) automation



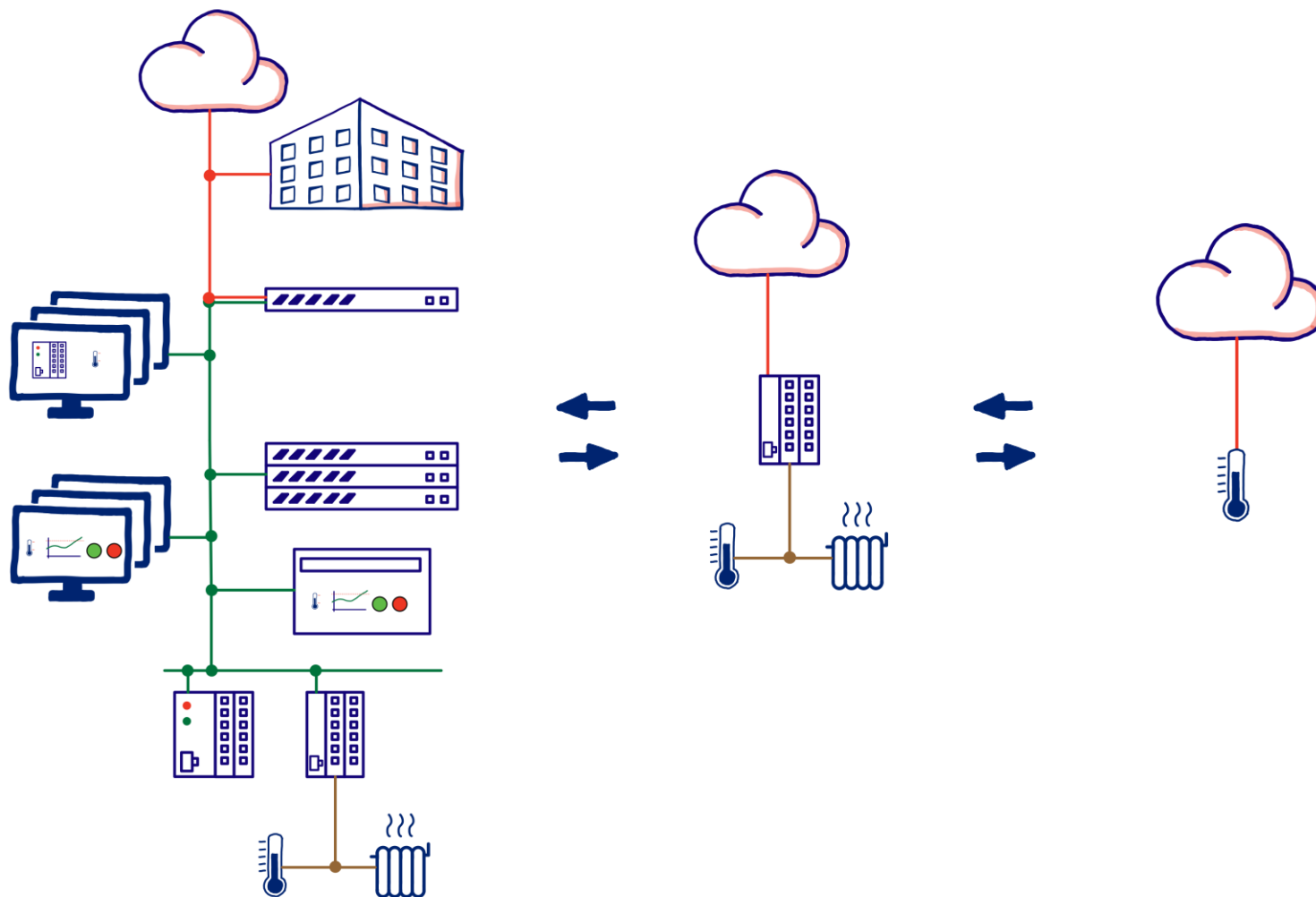
Endless questions..

1. How can we ensure secure remote access?
 2. Do we need a dedicated OT core?
 3. How are these networks routed?
 4. Do we need a firewall that “understands” OT protocols?
 5. Do I need decentralized firewalls?
 6. How can I standardize the setup for different use cases?
 7. How do I minimize the blast radius at Layer 2?
 8. How do I microsegment critical systems?
- ... etc.



Purdue Model

- Wasn't meant to be a network architecture blueprint
- Today layers are blended and integrated within one device
- But it helps with orientation - understanding what type of device we're dealing with

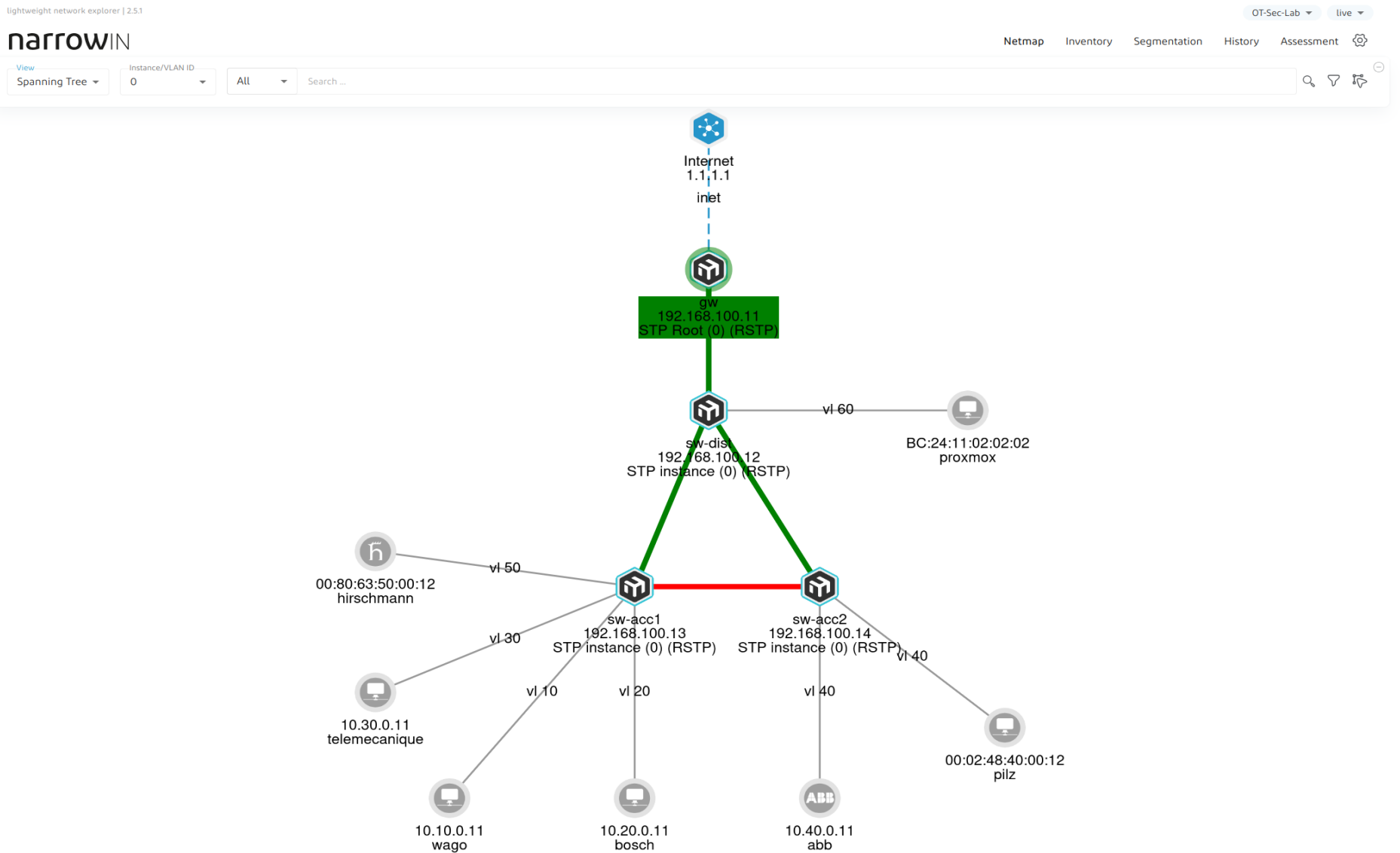


Lab Intro

INDUSTRIAL SECURITY CONFERENCE COPENHAGEN

[illegible]

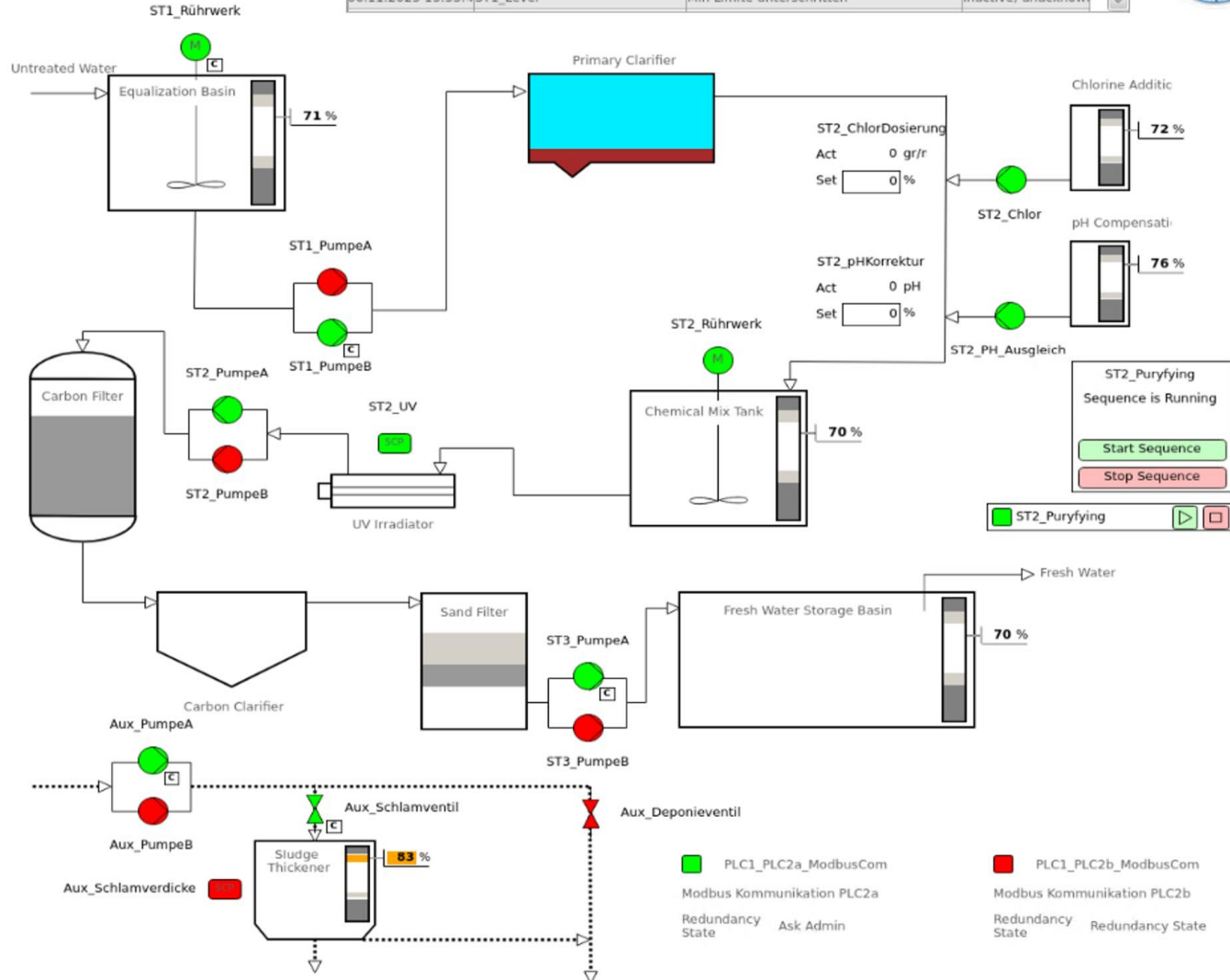
INDUSTRIAL SECURITY
CONFERENCE COPENHAGEN



Water Treatment

Control Center	VisuTest	Alarm / Event
----------------	----------	---------------

Timestamp	Object	Message	State
06.11.2025 13:33:52	ST2_ChlorLevel	Min Limite unterschritten	inactive, unacknow
06.11.2025 13:33:55	ST1_PrimaryClearing	Min Limite unterschritten	inactive, unacknow
06.11.2025 13:33:44	ST2_SalzLevel	Min Limite unterschritten	inactive, unacknow
06.11.2025 13:33:40	ST1_Level	Min Limite unterschritten	inactive, unacknow



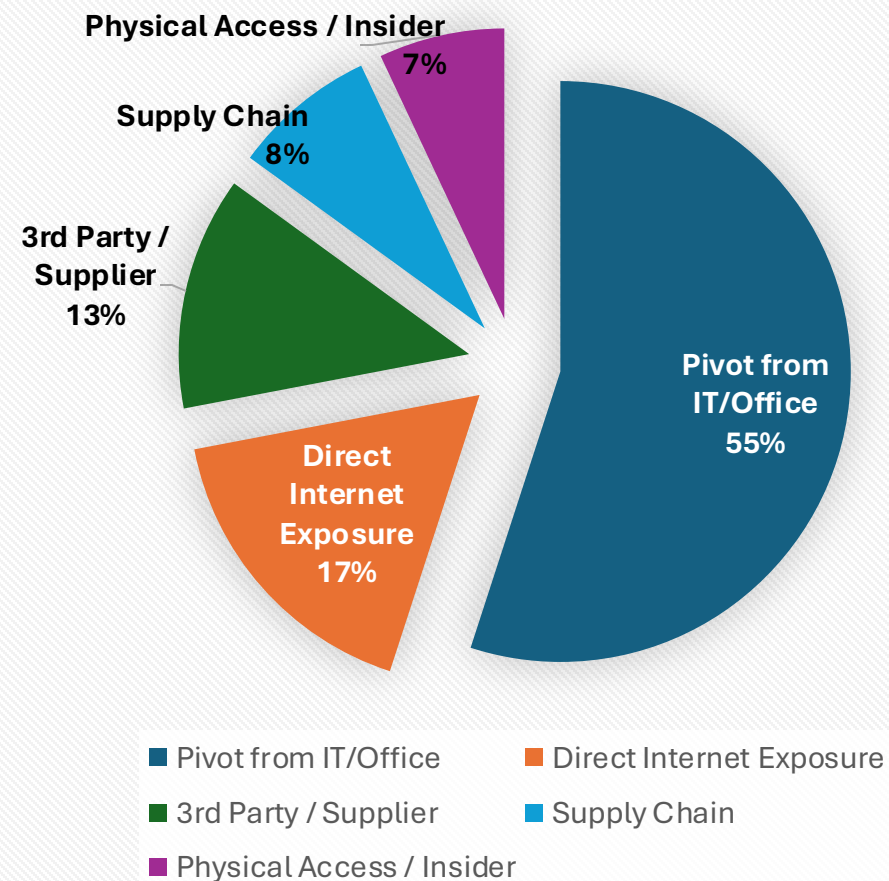
Defend

OT Attacks

Mostly:

- Weak or absent network segmentation
- Default or weak credentials
- Direct Internet exposure of OT devices

Approx Distribution of OT Attack Paths



Its not about fancy technology;
But the human behaviour, discipline, and organisational culture

Defending OT Networks

Principle	Underlying human element
Know your network	Someone must own asset management and actually maintain it with documentation, change control, patch schedules.
Segmentation / least privilege	Humans decide convenience vs. security, push back on “complex network designs,” or forget to revoke access.
Credential hygiene	People choose passwords, reuse credentials, grant rights, skip MFA enrolment, share accounts.
Supply-chain security	Humans vet vendors (or don’t), sign code, manage trust relationships, and approve updates.
Resilience	Teams plan, test backups, and rehearse responses or neglect to.
Persistent adversaries	Humans monitor logs, correlate signals, escalate incidents or miss them through fatigue or culture.

Attackers exploit human behaviour - not code

Even nation-state actors with zero-days prefer to:

- Phish someone for credentials
- Wait for a misconfiguration
- Abuse over-privileged accounts
- Abuse legacy remote-access paths
- Use stolen admin tools (LotL)

These are not technical breakthroughs;

They're exploitation of predictable human patterns: haste, habit, and hierarchy

Technology can enforce policy - but only we create, follow, and adapt the policy

Monitoring

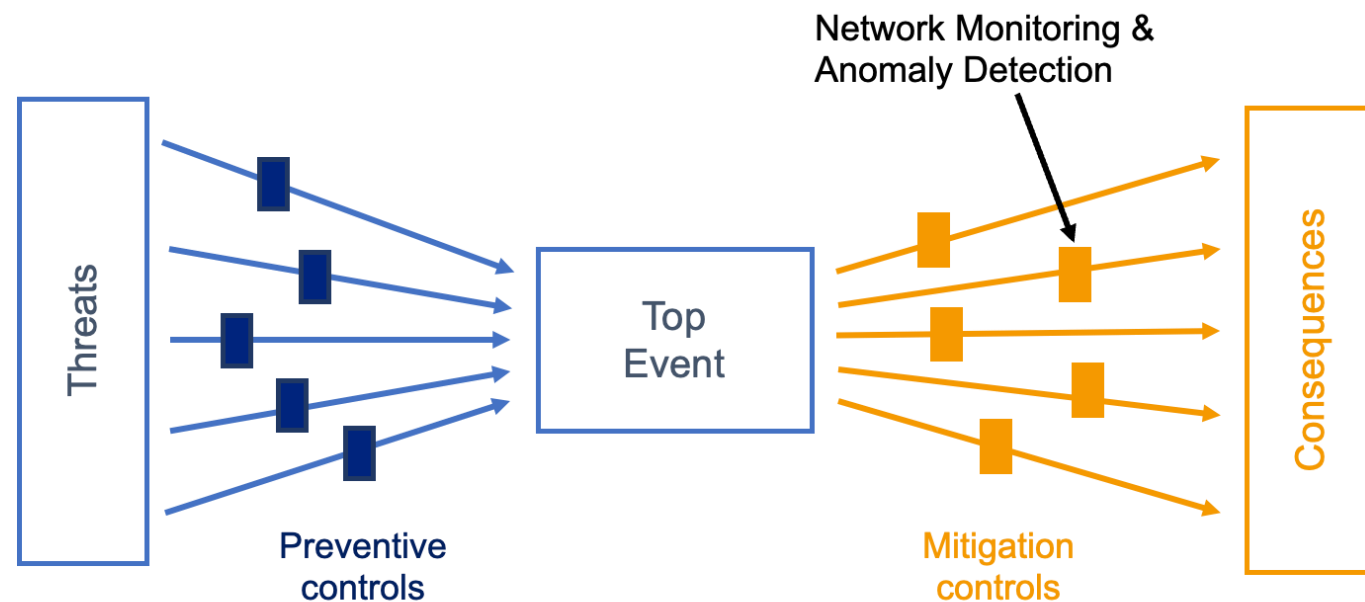
OT Network Security Monitoring

Mandatory - but overhyped

- Would you isolate a OT host?
- Would you dynamically block OT communication?

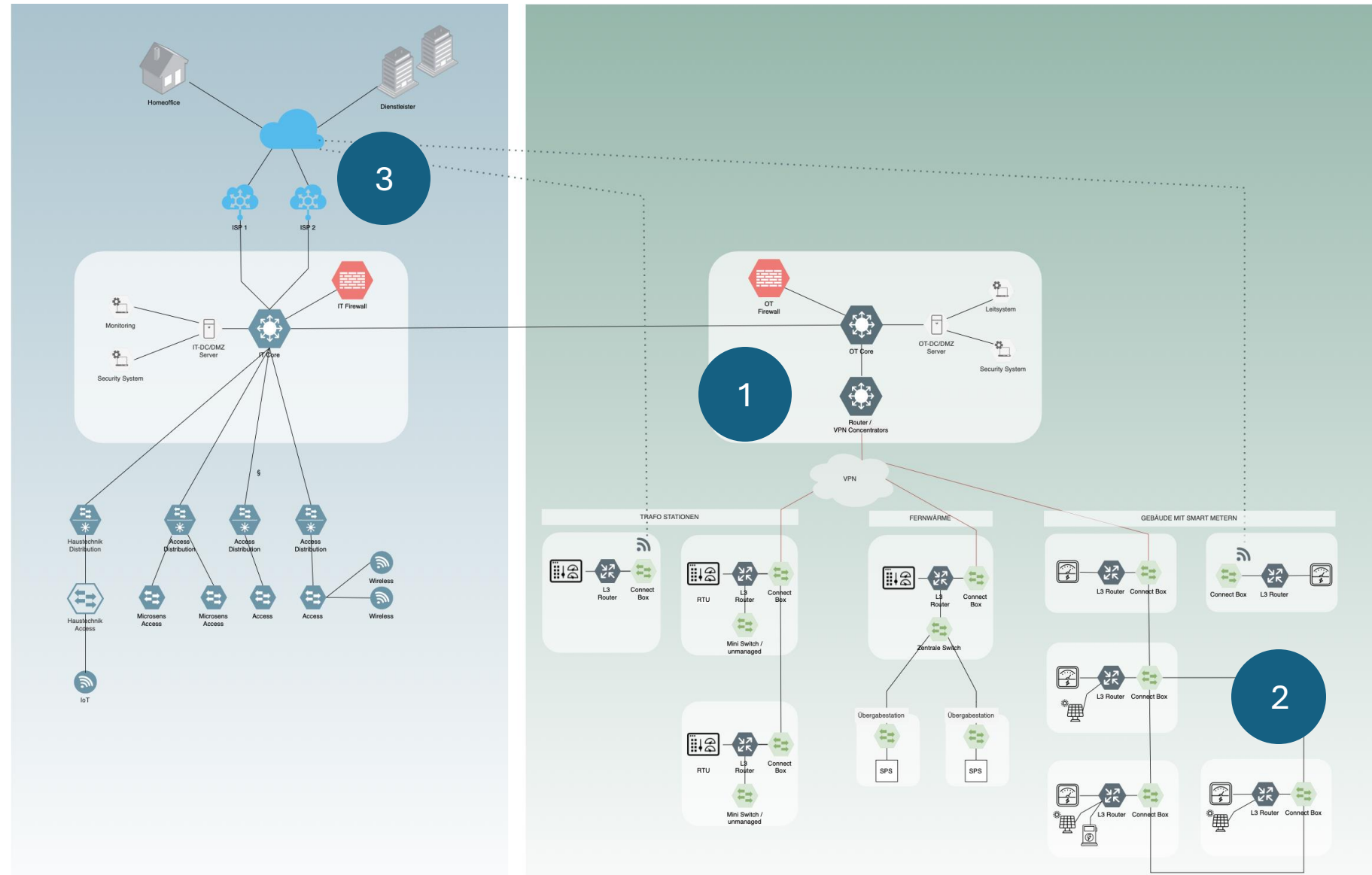
What it really is:

- Monitoring only - no active intervention
- Real value lies in **visibility**, not **control**



OT attack detection systems are only as good as
the response process behind them

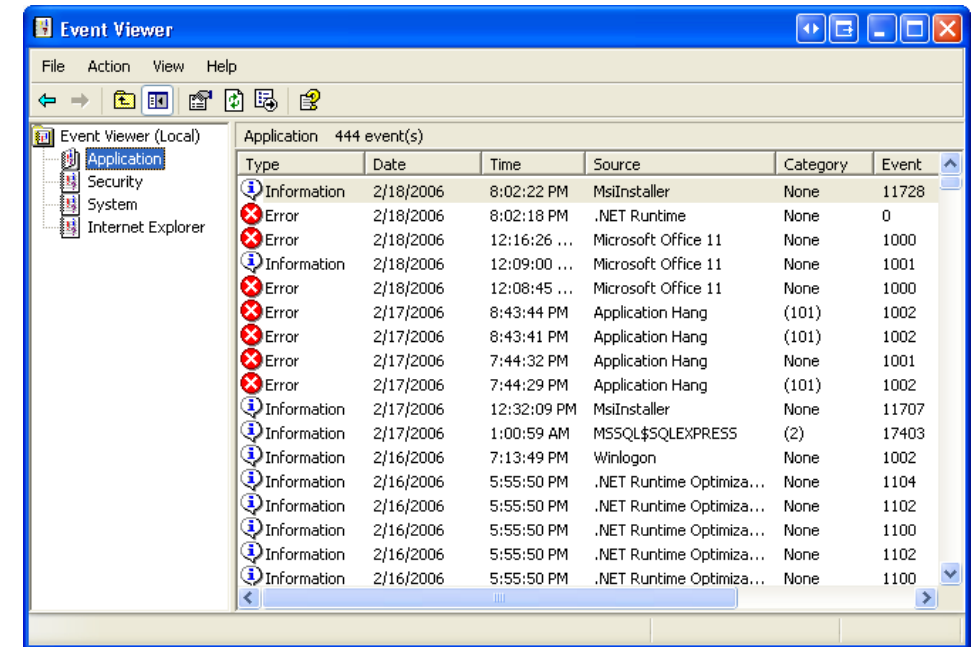
Sensor Placement



Logs

Tales from Incident Response (IR):

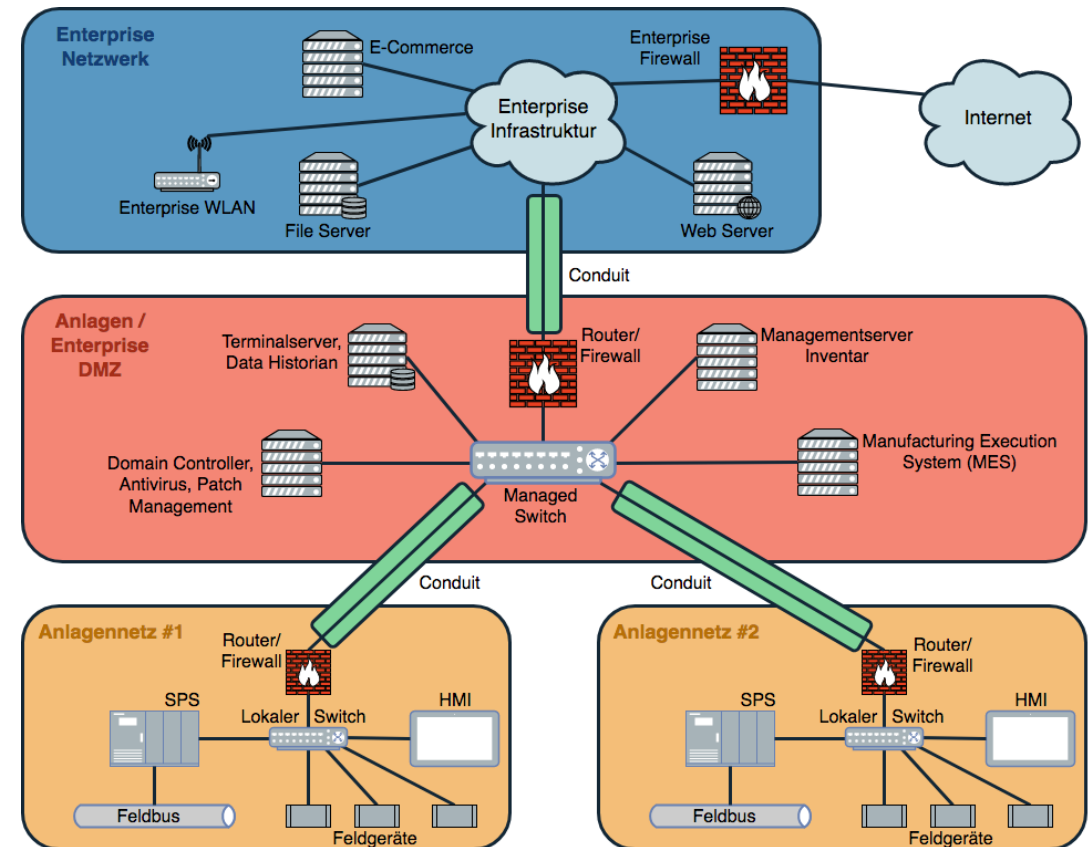
- First question: **“Where are the logs?”**
- Second question: **“That’s all you have?”**
- IR often starts with chasing visibility
- No logs, no timeline, no indicators, no story
- Everything should talk to your log server.
- Even old OT devices produce some logs!



Zones & Conduits

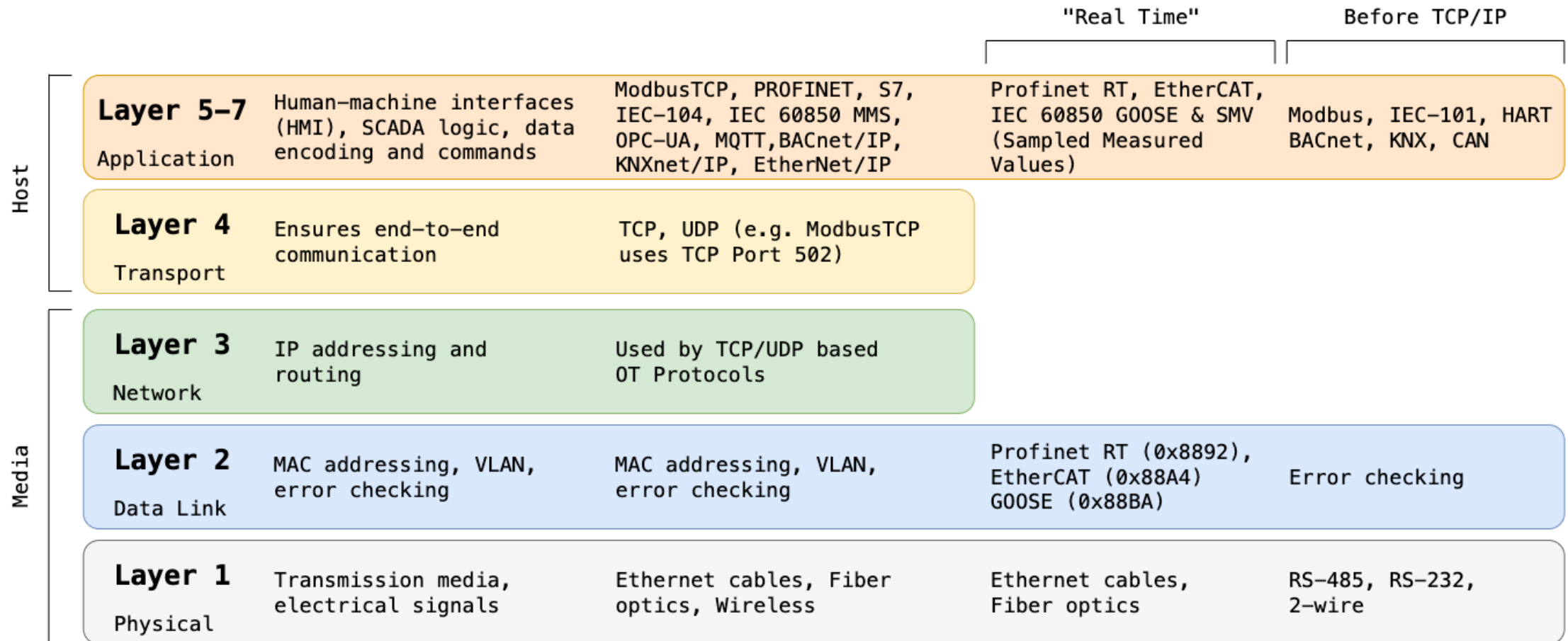
Segmentation and Zones

- The **division** of a large network into smaller, isolated subnetworks (segments or zones).
- **Damage containment ("Blast Radius")**: A security incident (malware, attack) in one zone does not automatically spread to other zones.
- **Containment of network issues** (e.g., broadcast storms, malfunctions) within the affected segment.
- **Protection of production** from failures in other network areas.



Source: <https://www.sichere-industrie.de/zones-conduits/>

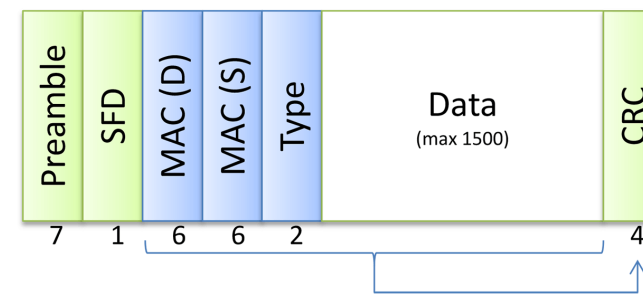
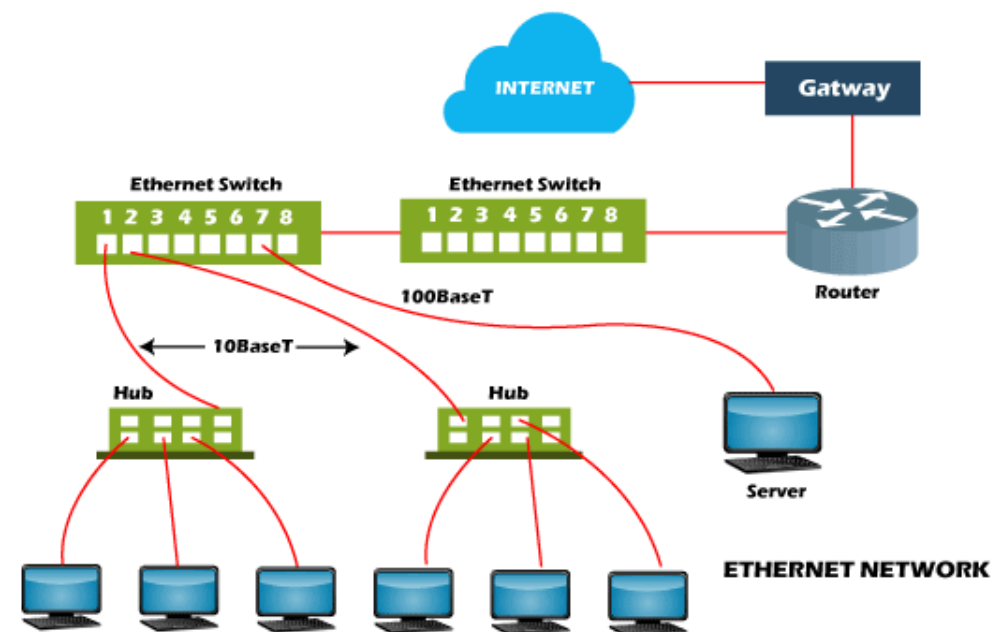
Simplified OT OSI Layer Model



Layer 2 - Ethernet

The dominant technology for connecting devices in local networks

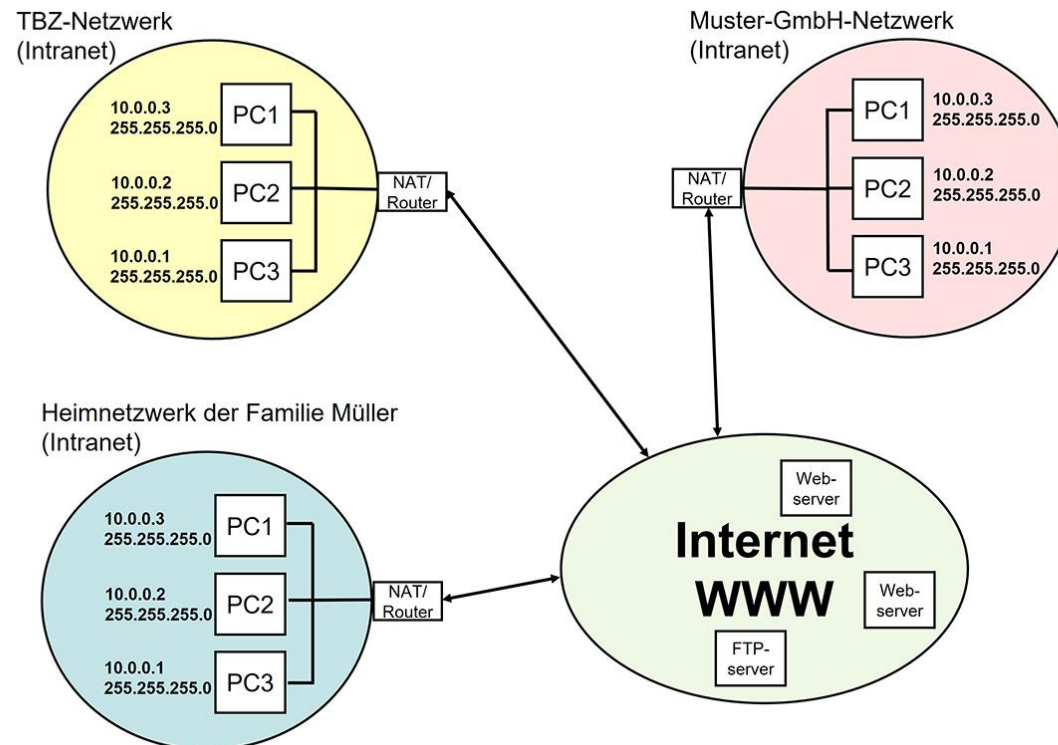
- Data transmission in packets (frames)
 - Data is broken down into small units
- Addressing via MAC addresses
 - Media Access Control
 - Globally unique
 - 48-bit addresses



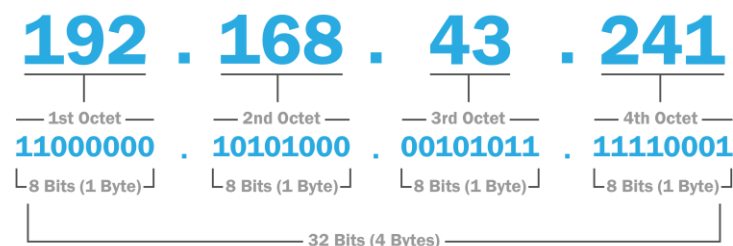
Layer 3 - IPv4

Fundamental Protocol of the Internet

- 32-bit address format
- Public IPs
- Private IPs:
 - 10.x.x.x
 - 172.16.x.x to 172.31.x.x
 - 192.168.x.x
- NAT (Network Address Translation)
- Subnet mask & network/host portion:
 - 255.255.255.0 (or /24)



IPv4 Address Format





A simple Zone Concept

			To										
			OT DMZ			OT - Operations				OT - Engineering			
						Default	Service	...	Hygiene	Waste Treatment	Main Process	Central Control Room	Management
From	OT DMZ	Default											
		Service											
		..											
	OT - Operations	Hygiene											
		Waste Treatment											
		Main Process											
		Central Control Room											
	OT - Engineering	Management											
		Configuration											
		...											

Network Automation

Manual processes leave holes
Gaps are inevitable
And they accumulate over time

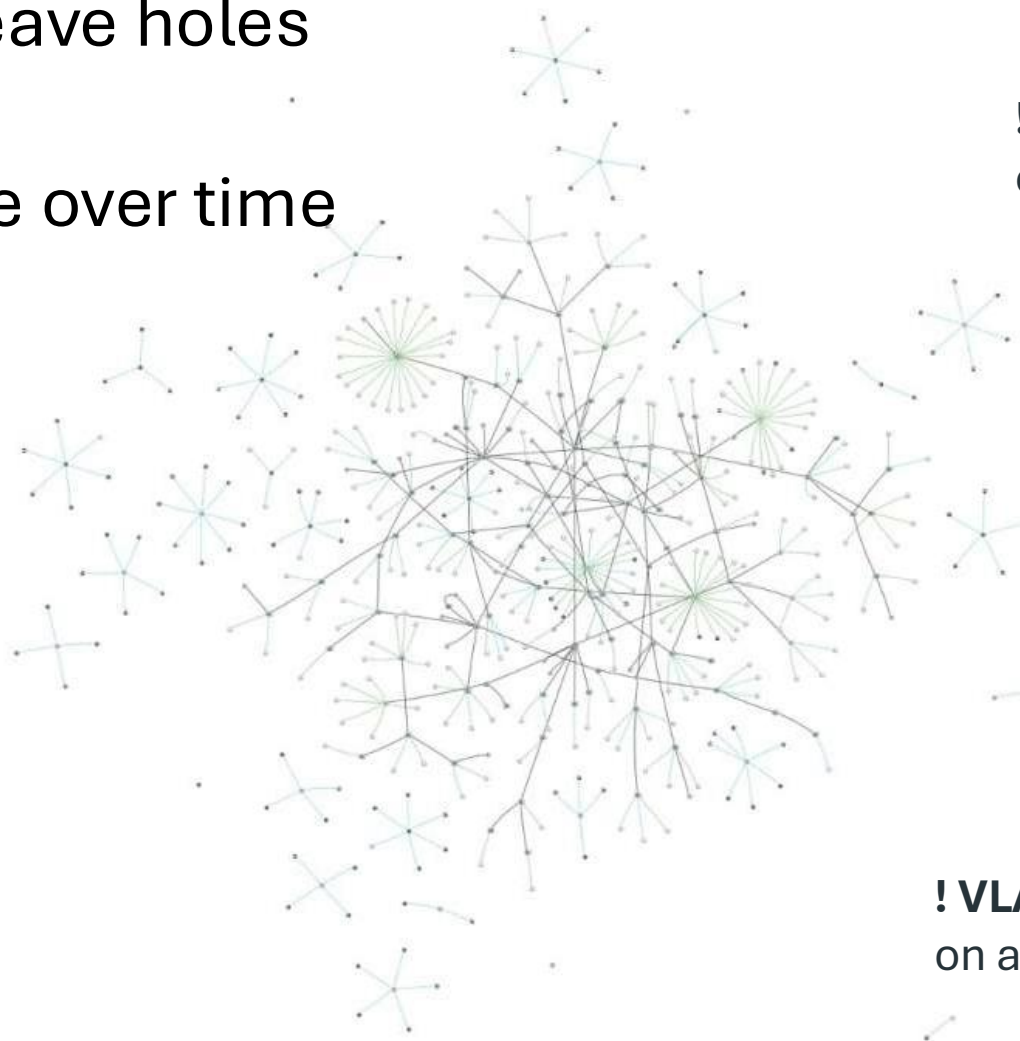
**! Reversible
password encryption**
on 16 devices

! Missing Port security
on 20% of the devices

! NTP not configured
on 5% of the devices

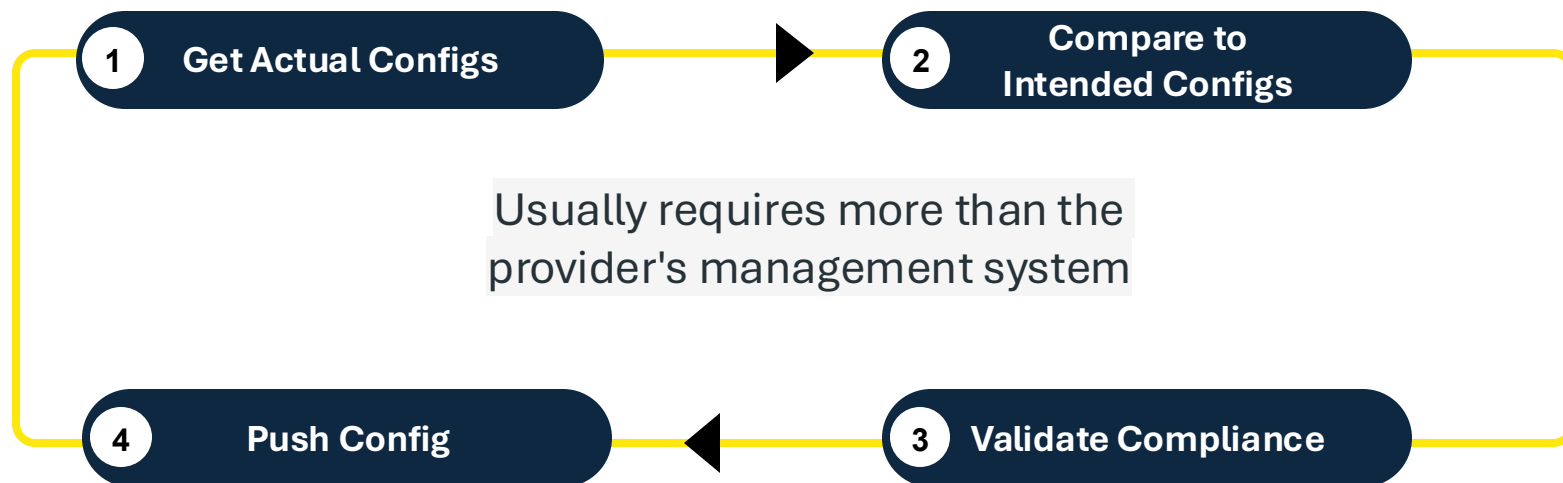
! STP misconfiguration
on 4 devices

! VLAN 1 not disabled
on all devices



Let's automate it!

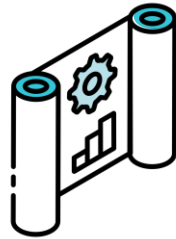
Through automation, these blind spots can be identified and resolved, preventing configuration drift.



Conclusion: OT network labs allow us to



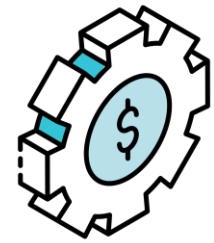
Train on context-specific networks



Test-before-deploy
approach in critical
OT networks



Analyse Security in
realistic OT
Environments



Full-cycle
Automation: design-
test-deploy-observe

Stay in touch

mischa.diehm@narrowin.ch



martin.scheu@switch.ch

<https://www.linkedin.com/in/martin-scheu/>

