

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



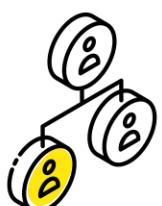
OT Networks are Business-critical

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



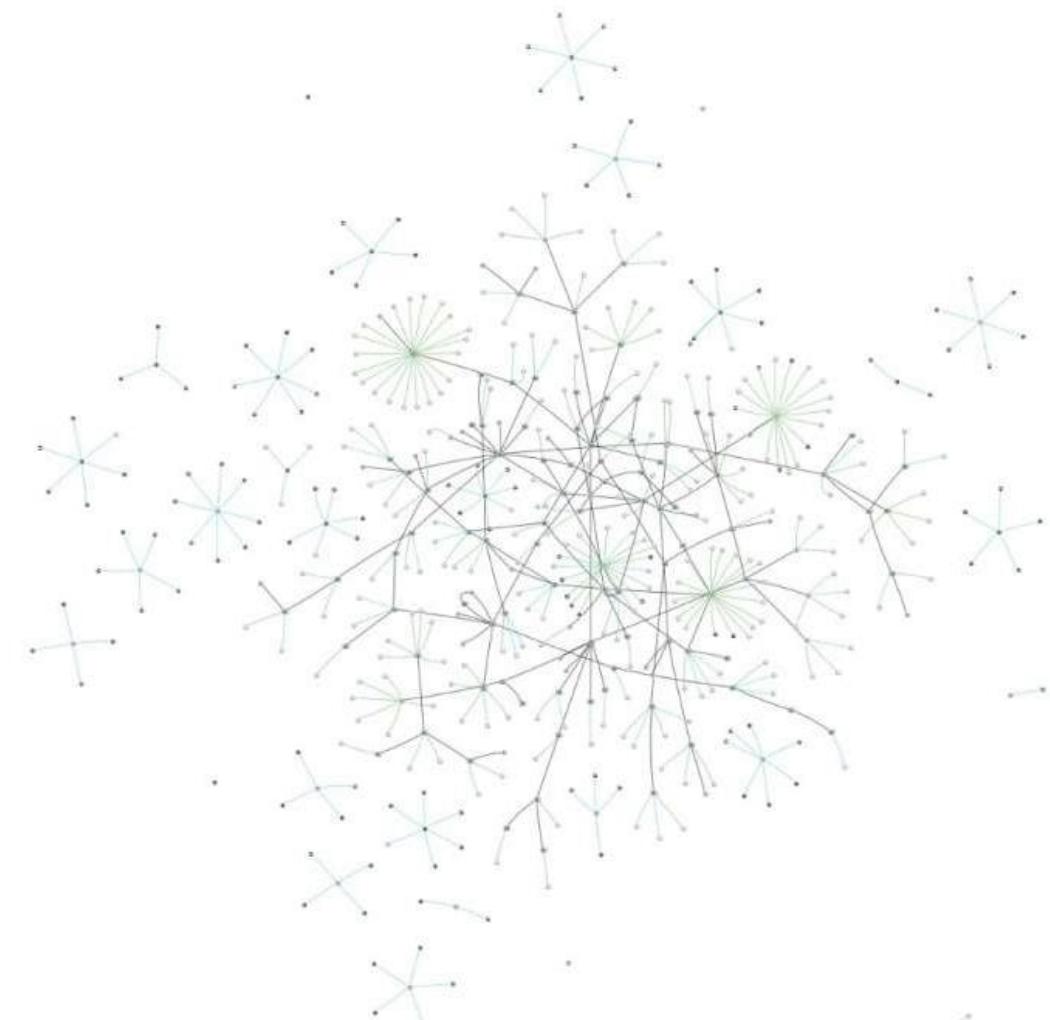
Growth and Complexity of OT Networks

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



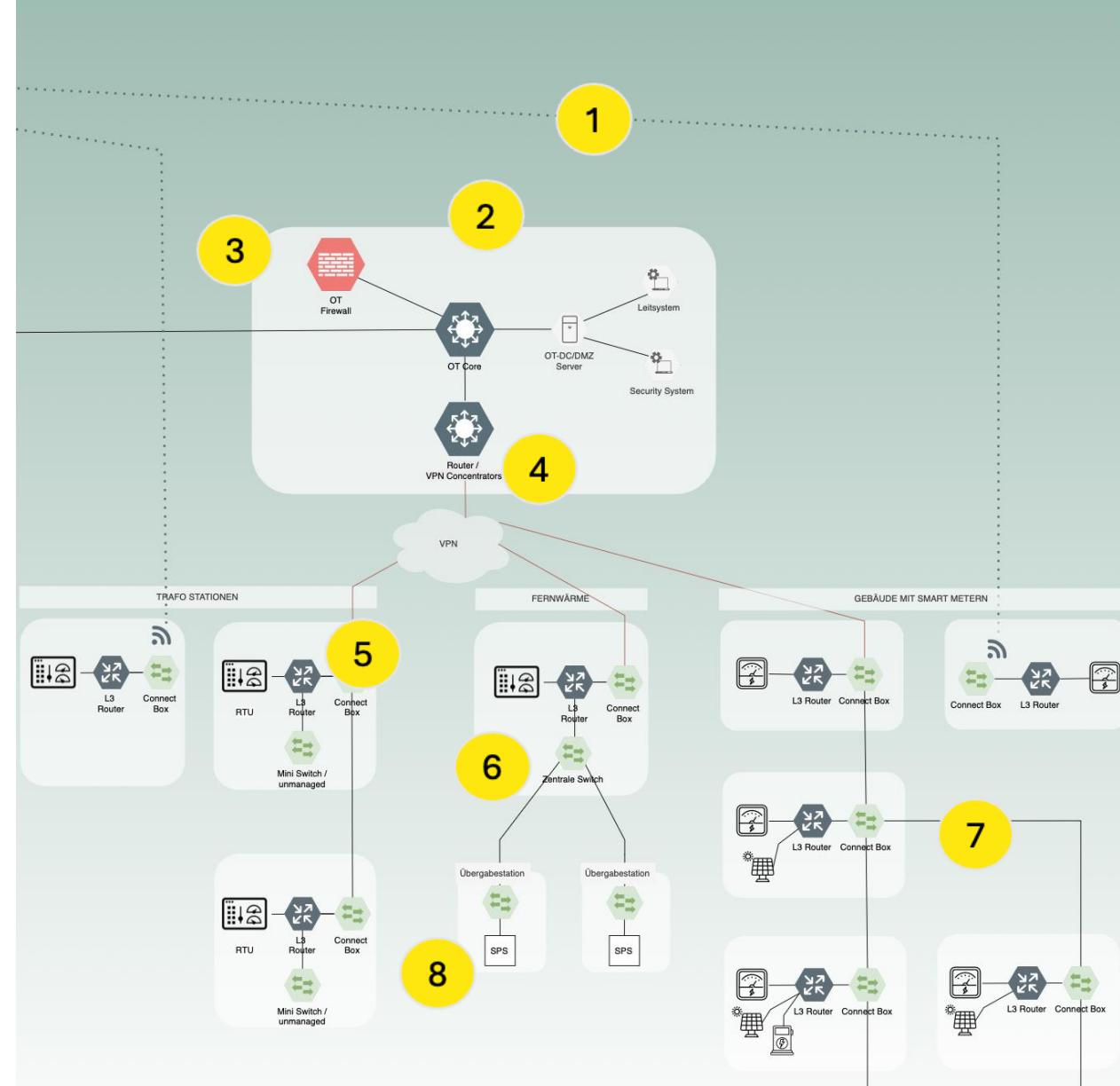
Shortage of Expertise and Time

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



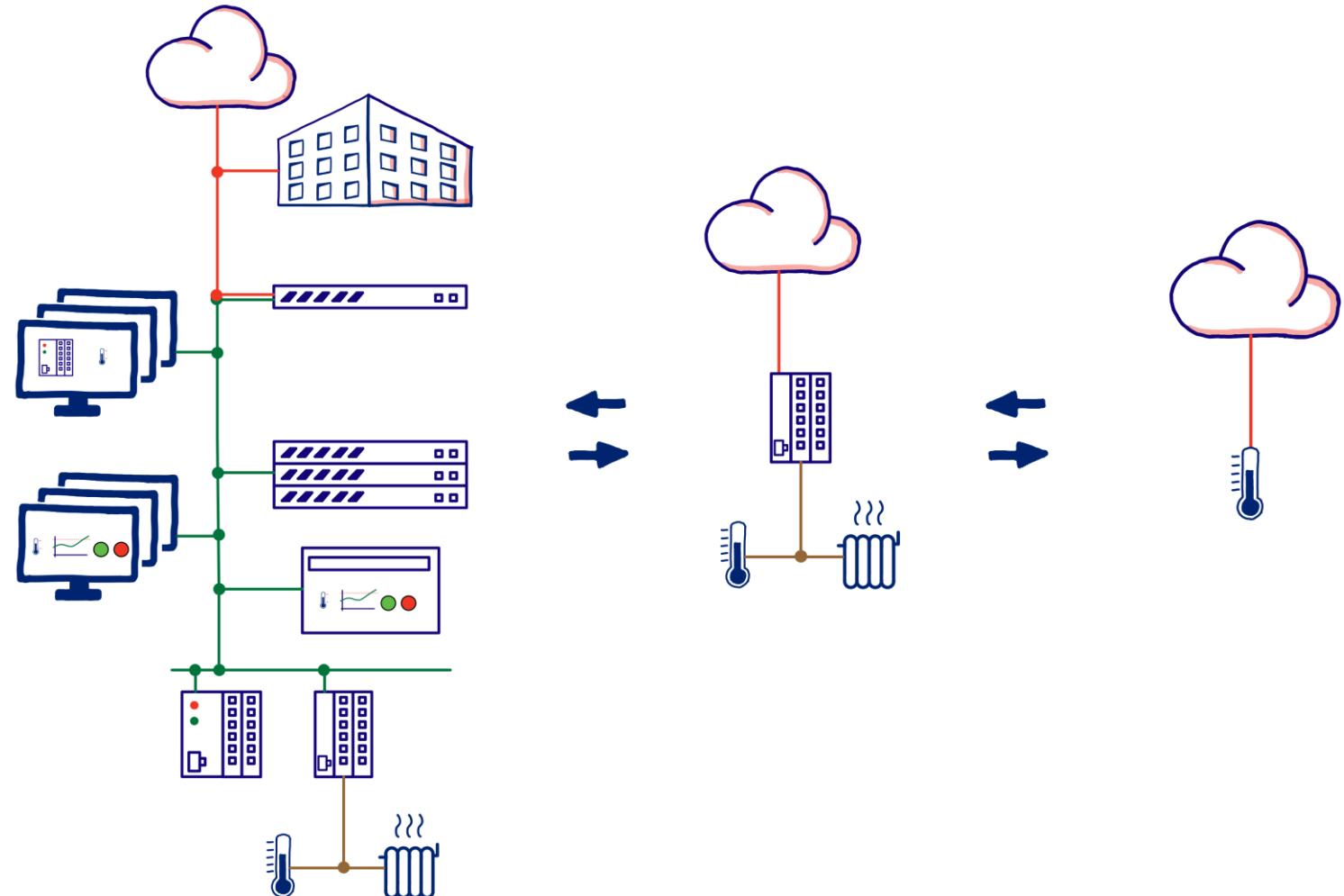
Endless questions..

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.



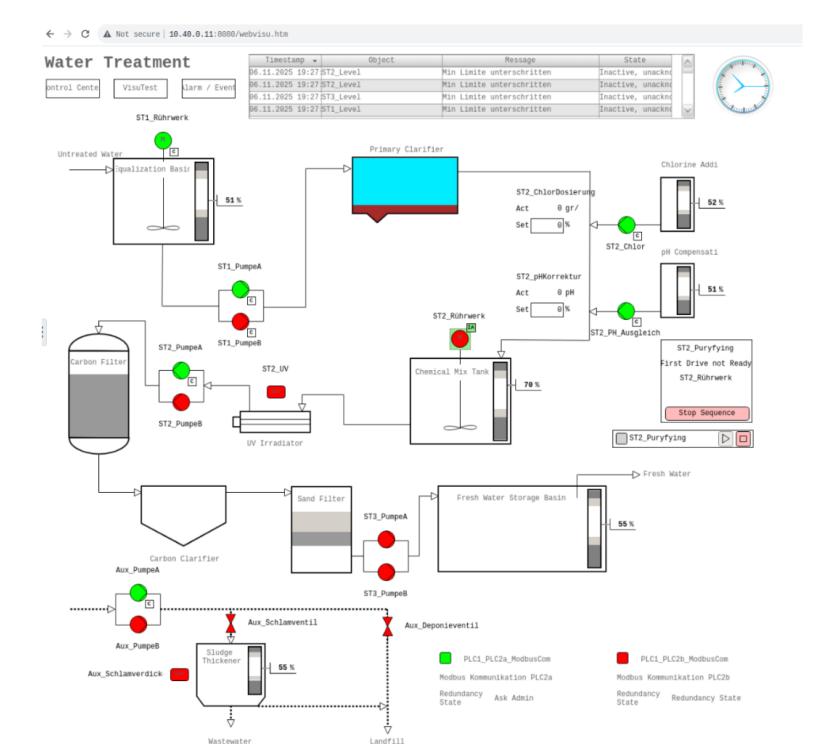
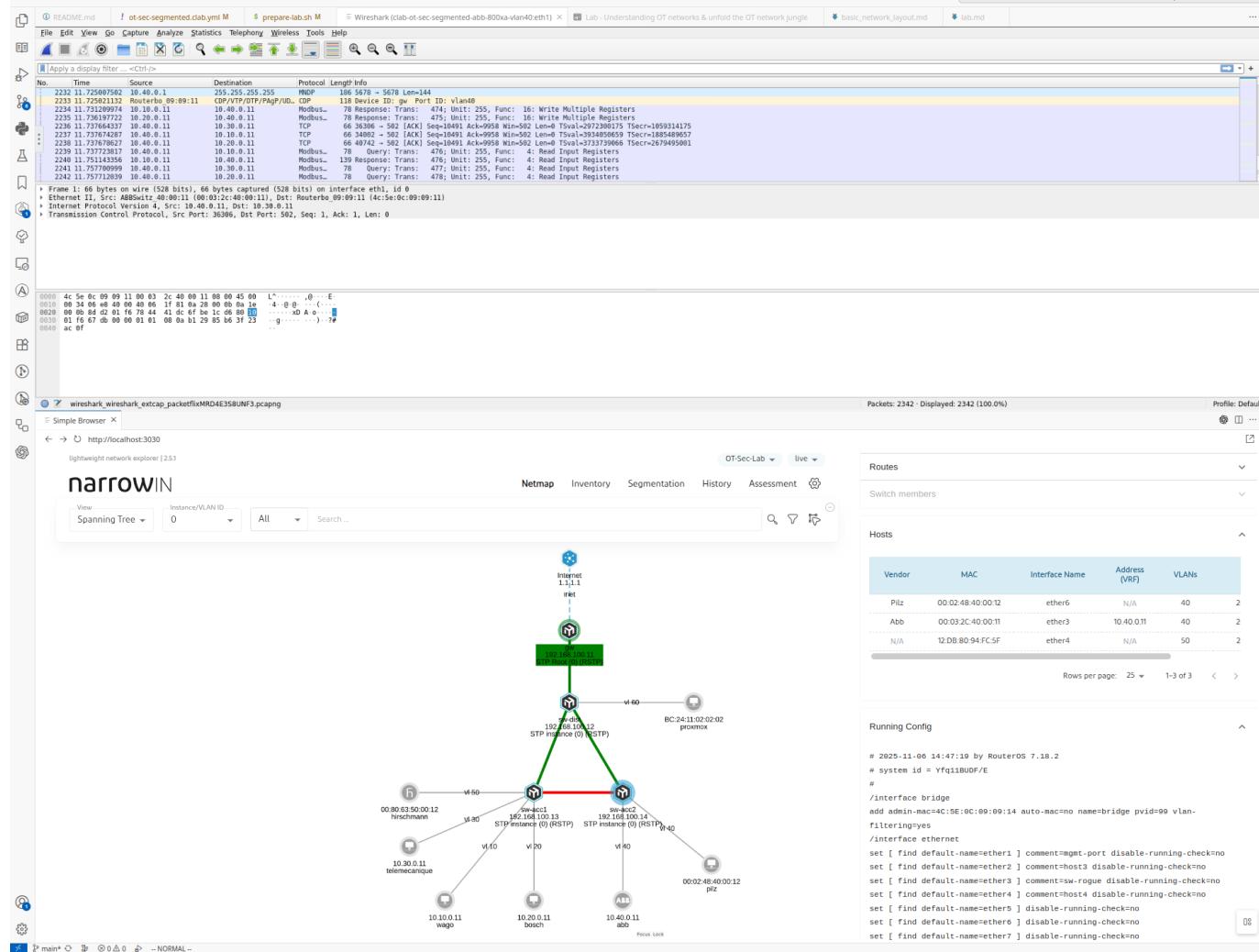
Purdue Model

- 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



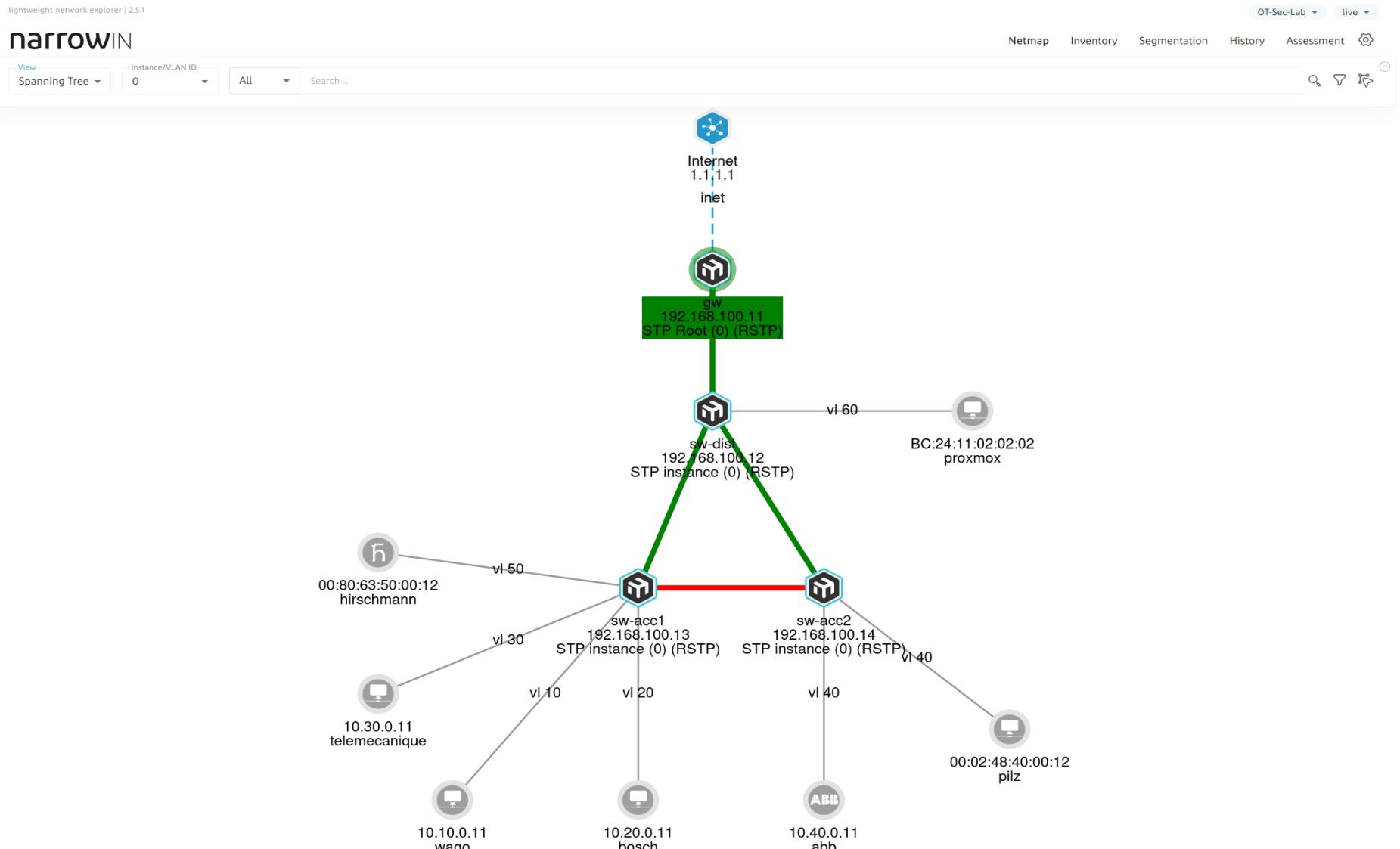
Lab Intro

INDUSTRIAL SECURITY CONFERENCE COPENHAGEN



> Big Picture > **Lab Intro** > Defend > Monitoring > Zones & Conduits > Network Automation

INDUSTRIAL SECURITY CONFERENCE COPENHAGEN

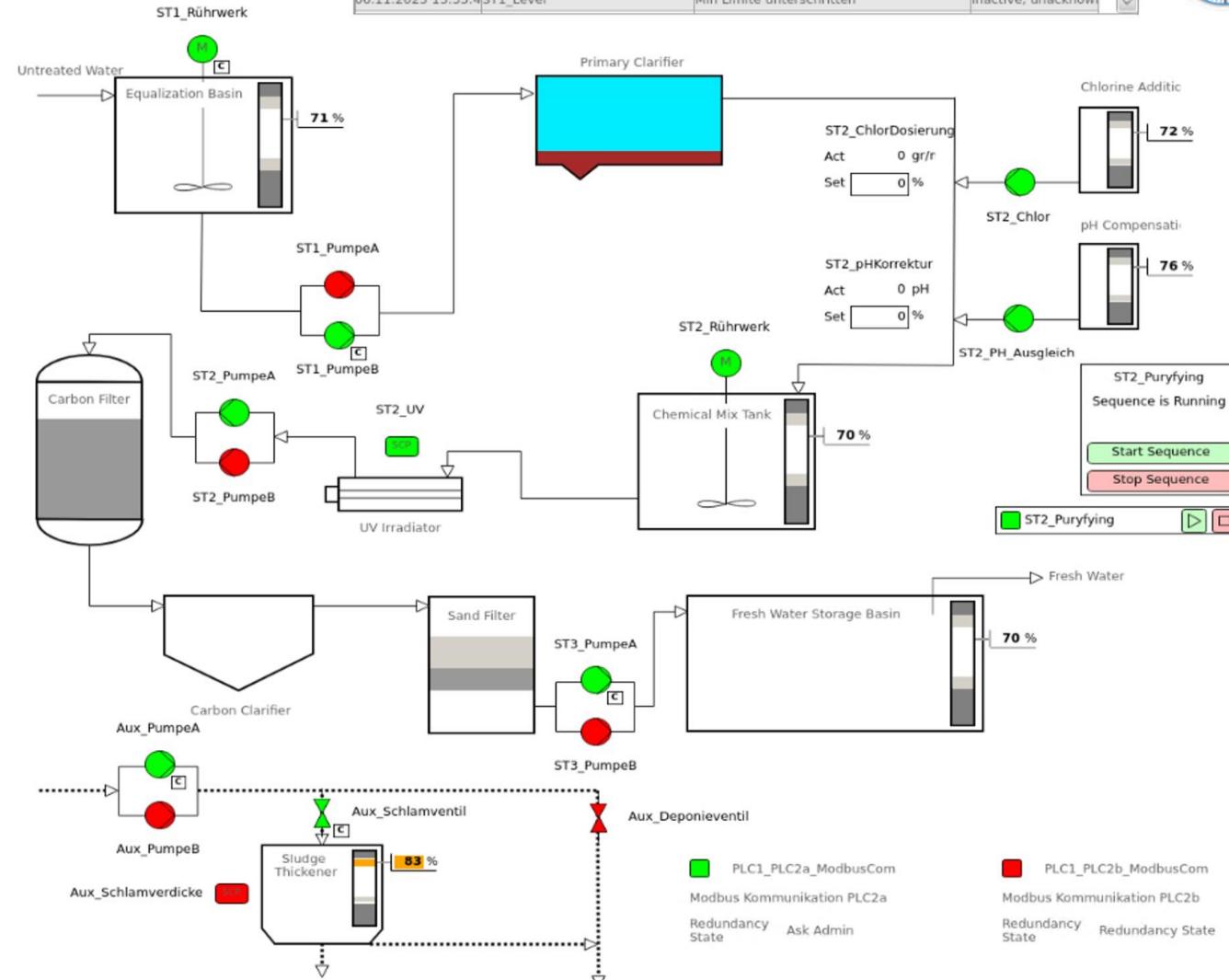


INDUSTRIAL SECURITY CONFERENCE COPENHAGEN

Water Treatment

Control Center VisuTest Alarm / Event

Timestamp	Object	Message	State
06.11.2025 13:33:5	ST2_ChlorLevel	Min Limite unterschritten	Inactive, unacknowl.
06.11.2025 13:33:5	ST1_PrimaryClearing	Min Limite unterschritten	Inactive, unacknowl.
06.11.2025 13:33:4	ST2_SalzLevel	Min Limite unterschritten	Inactive, unacknowl.
06.11.2025 13:33:4	ST1_Level	Min Limite unterschritten	Inactive, unacknowl.

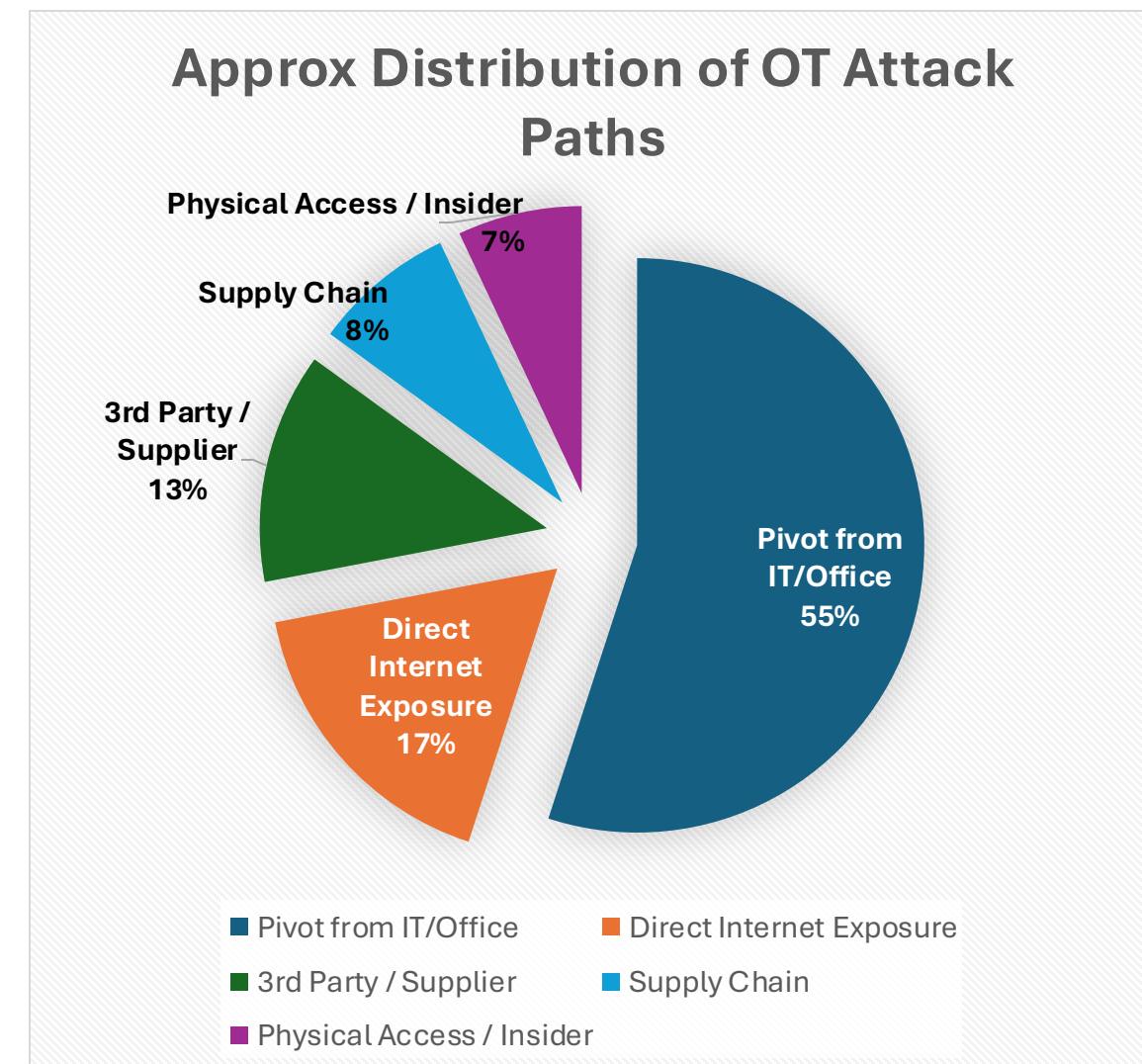


Defend

OT Attacks

Mostly:

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



Defending OT Networks

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

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

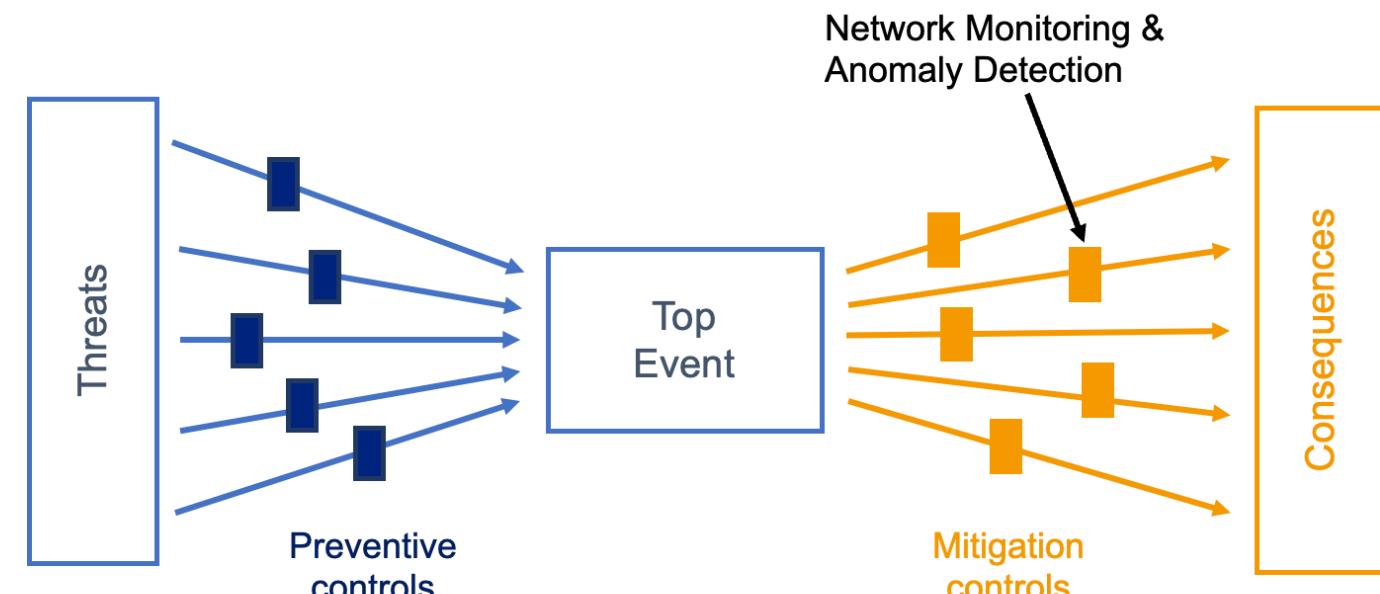
OT Network Security Monitoring

Mandatory - but overhyped

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

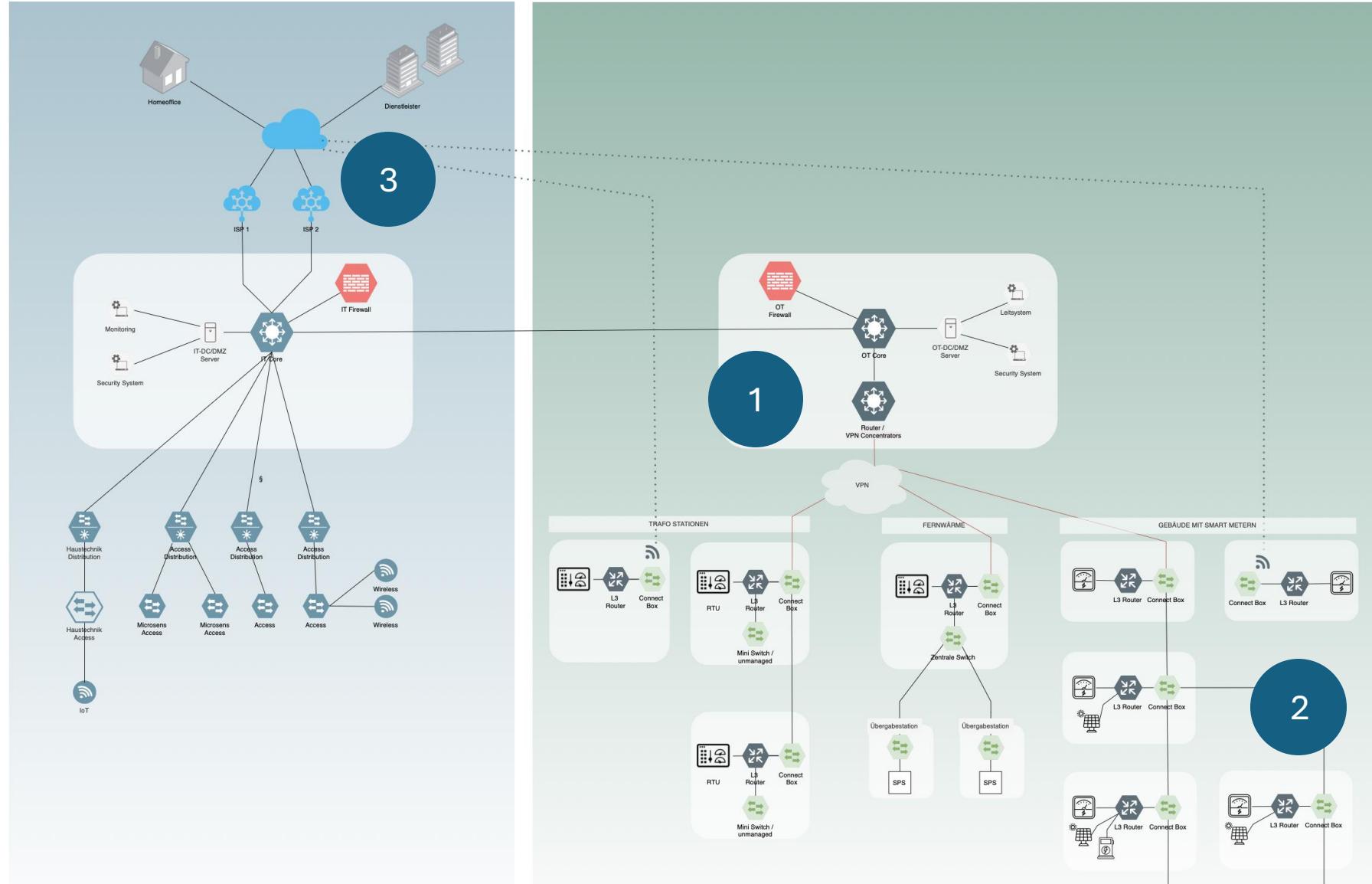
What it really is:

- 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

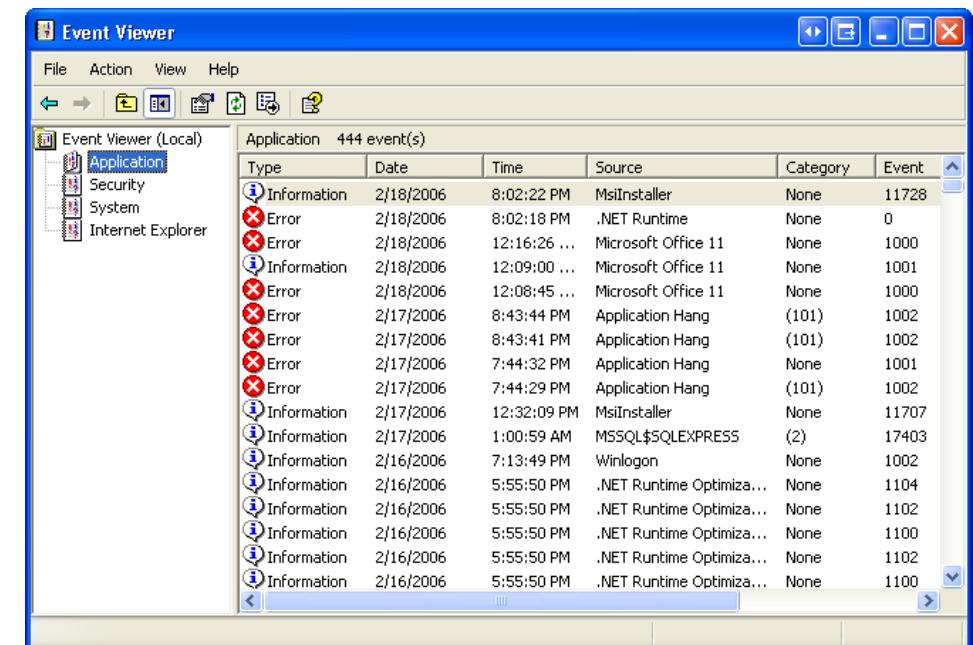
Sensor Placement



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!



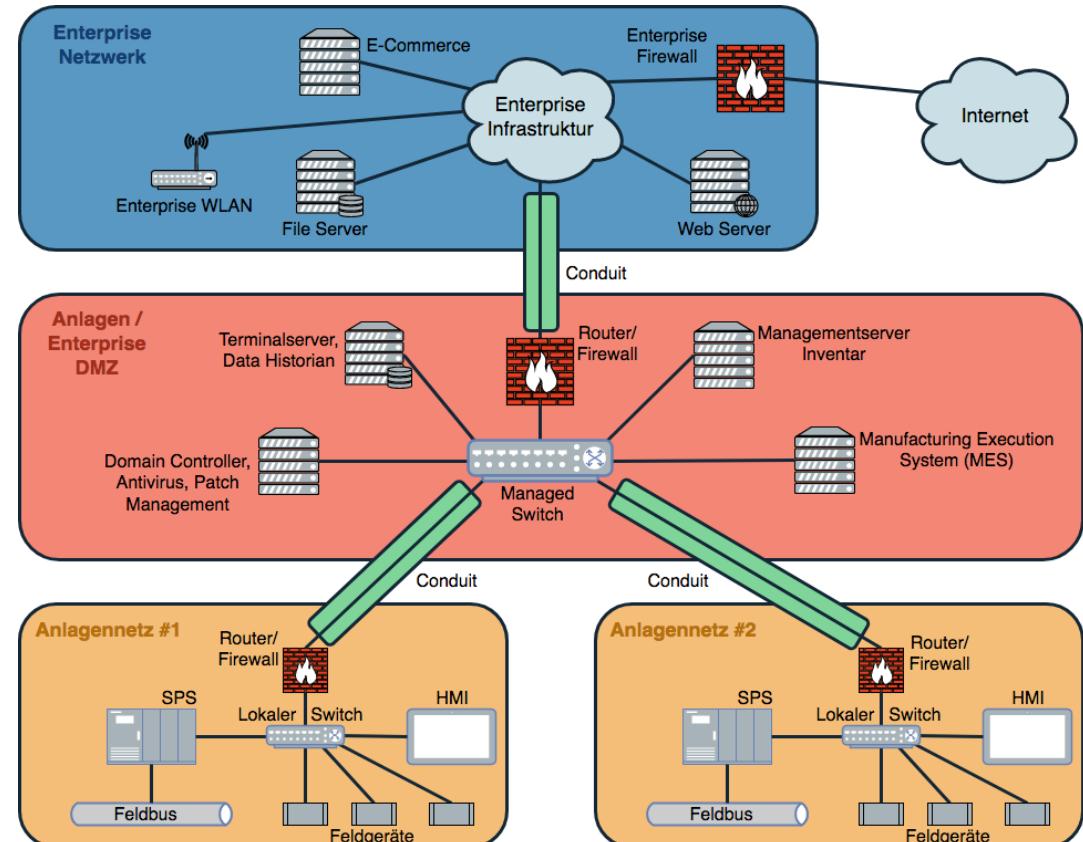
The screenshot shows the Windows Event Viewer application window. The title bar reads "Event Viewer". The menu bar includes "File", "Action", "View", and "Help". The toolbar contains icons for navigating between log files, opening files, and performing search operations. On the left, a navigation pane displays four categories: Application (selected), Security, System, and Internet Explorer. The main pane is titled "Application 444 event(s)" and lists log entries in a table format. The columns are "Type", "Date", "Time", "Source", "Category", and "Event". The table contains numerous rows of log entries, primarily errors and information messages from various sources like .NET Runtime, Microsoft Office 11, and MSSQL\$SQLEXPRESS, spanning dates from February 16 to 18, 2006.

Type	Date	Time	Source	Category	Event
Information	2/18/2006	8:02:22 PM	MsiInstaller	None	11728
Error	2/18/2006	8:02:18 PM	.NET Runtime	None	0
Error	2/18/2006	12:16:26 ...	Microsoft Office 11	None	1000
Information	2/18/2006	12:09:00 ...	Microsoft Office 11	None	1001
Error	2/18/2006	12:08:45 ...	Microsoft Office 11	None	1000
Error	2/17/2006	8:43:44 PM	Application Hang	(101)	1002
Error	2/17/2006	8:43:41 PM	Application Hang	(101)	1002
Error	2/17/2006	7:44:32 PM	Application Hang	None	1001
Error	2/17/2006	7:44:29 PM	Application Hang	(101)	1002
Information	2/17/2006	12:32:09 PM	MsiInstaller	None	11707
Information	2/17/2006	1:00:59 AM	MSSQL\$SQLEXPRESS	(2)	17403
Information	2/16/2006	7:13:49 PM	Winlogon	None	1002
Information	2/16/2006	5:55:50 PM	.NET Runtime Optimiza...	None	1104
Information	2/16/2006	5:55:50 PM	.NET Runtime Optimiza...	None	1102
Information	2/16/2006	5:55:50 PM	.NET Runtime Optimiza...	None	1100
Information	2/16/2006	5:55:50 PM	.NET Runtime Optimiza...	None	1102
Information	2/16/2006	5:55:50 PM	.NET Runtime Optimiza...	None	1100

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/>

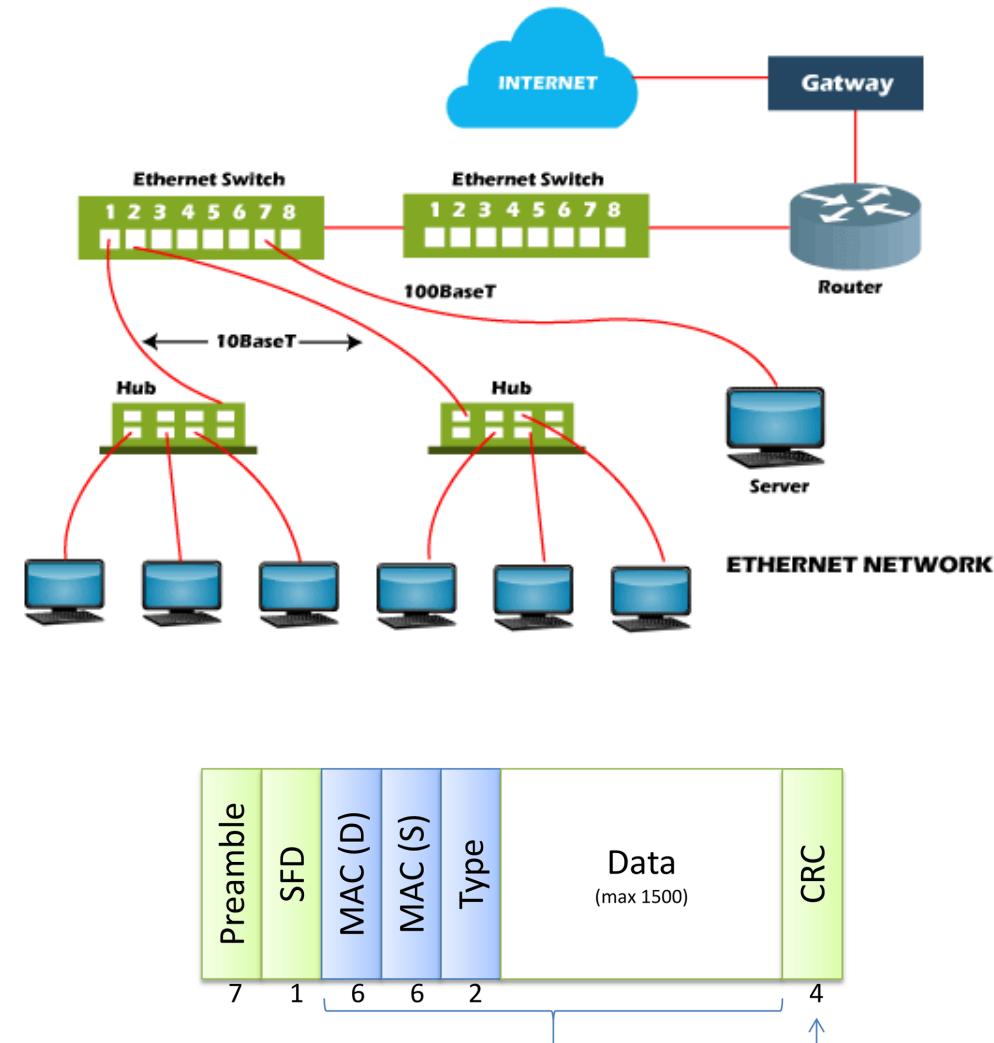
Simplified OT OSI Layer Model

		"Real Time"	Before TCP/IP
Host	Layer 5-7 Application	Human-machine interfaces (HMI), SCADA logic, data encoding and commands	ModbusTCP, PROFINET, S7, IEC-104, IEC 60850 MMS, OPC-UA, MQTT, BACnet/IP, KNXnet/IP, EtherNet/IP
	Layer 4 Transport	Ensures end-to-end communication	TCP, UDP (e.g. ModbusTCP uses TCP Port 502)
	Layer 3 Network	IP addressing and routing	Used by TCP/UDP based OT Protocols
	Layer 2 Data Link	MAC addressing, VLAN, error checking	Profinet RT (0x8892), EtherCAT (0x88A4) GOOSE (0x88BA)
	Layer 1 Physical	Transmission media, electrical signals	RS-485, RS-232, 2-wire

Layer 2 - Ethernet

The dominant technology for connecting devices in local networks

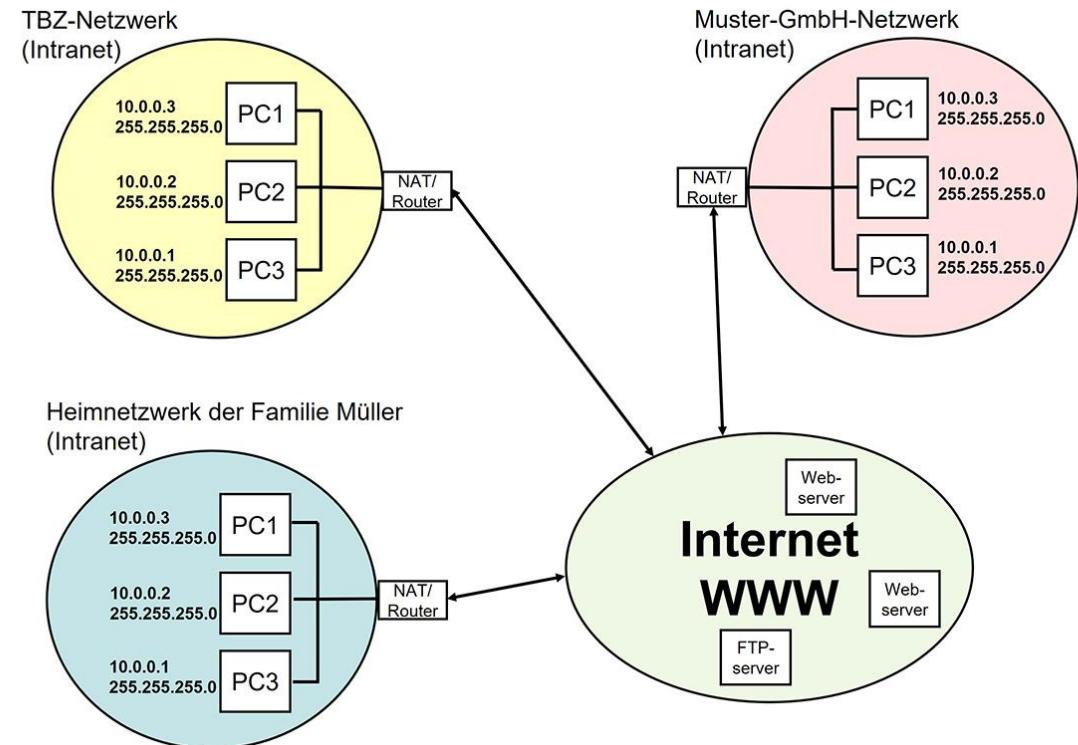
- Data transmission in packets (frames)
 - Data is broken down into small units
- Addressing via MAC addresses
 - Media Access Control
 - Globally unique
 - 48-bit addresses



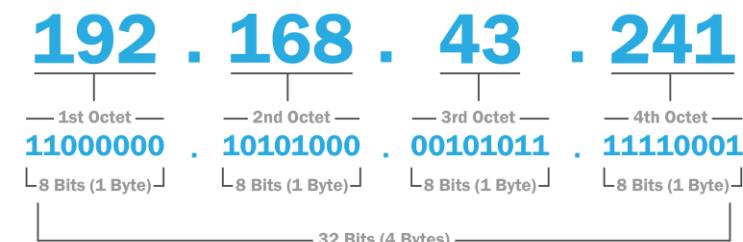
Layer 3 - IPv4

Fundamental Protocol of the Internet

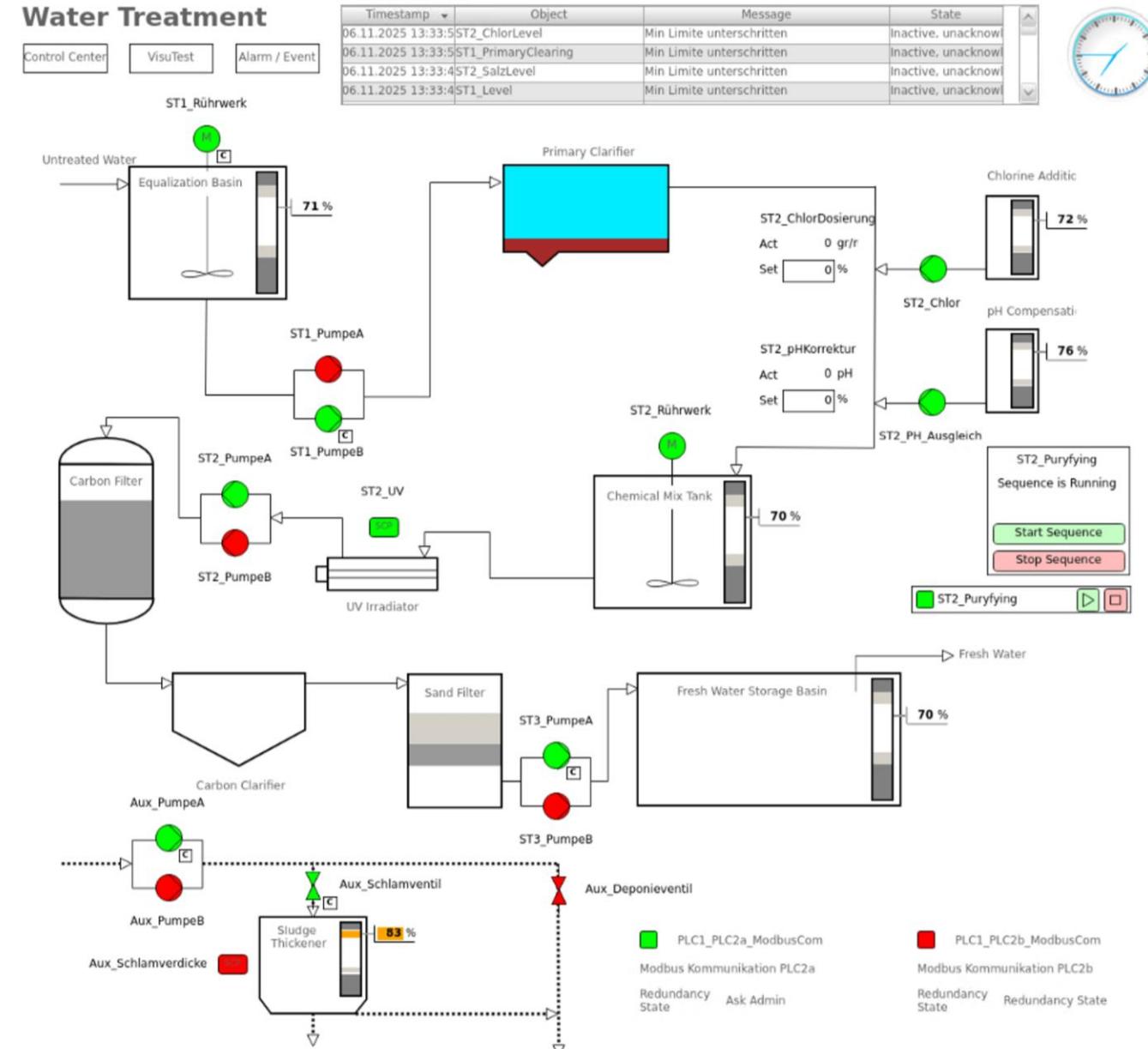
- 32-bit address format
- Public IPs
- Private IPs:
 - 10.x.x.x
 - 172.16.x.x to 172.31.x.x
 - 192.168.x.x
- NAT (Network Address Translation)
- Subnet mask & network/host portion:
 - 255.255.255.0 (or /24)



IPv4 Address Format



Exercise: define Zones and Conduits

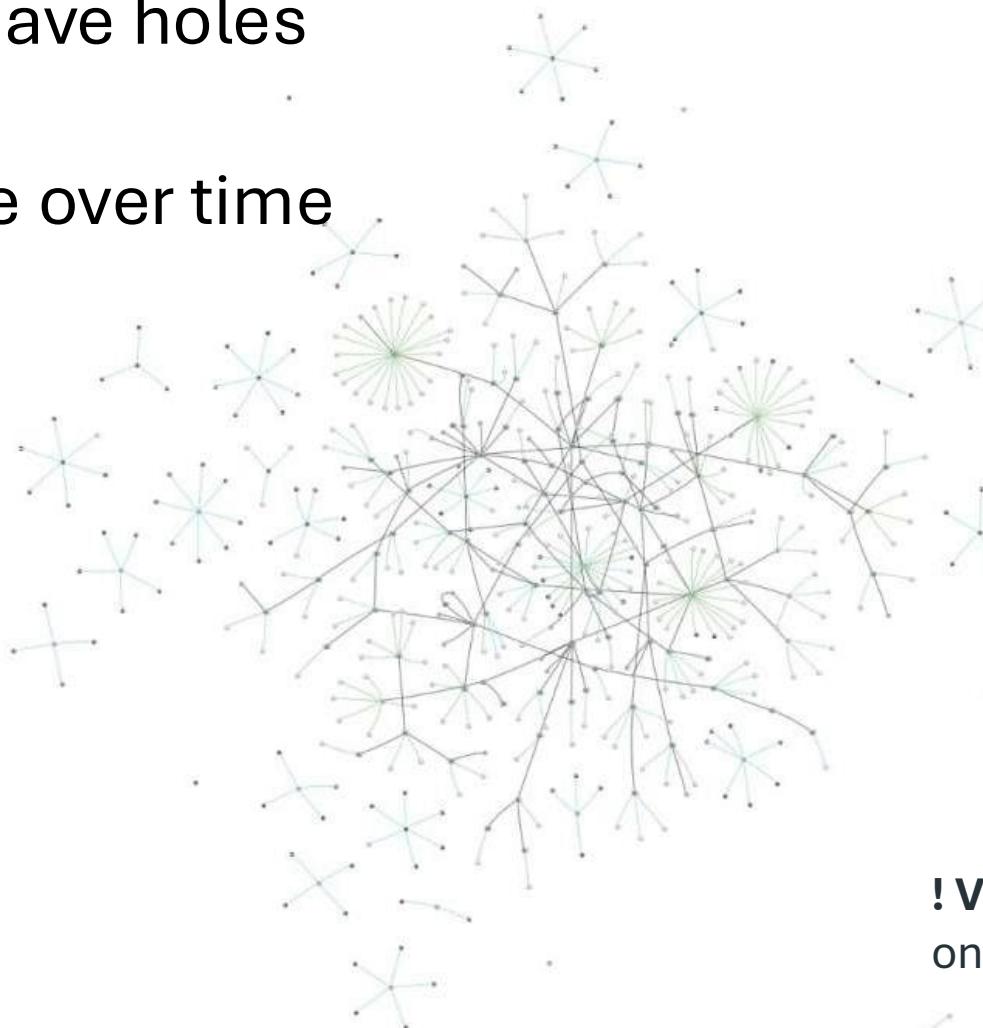


A simple Zone Concept

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

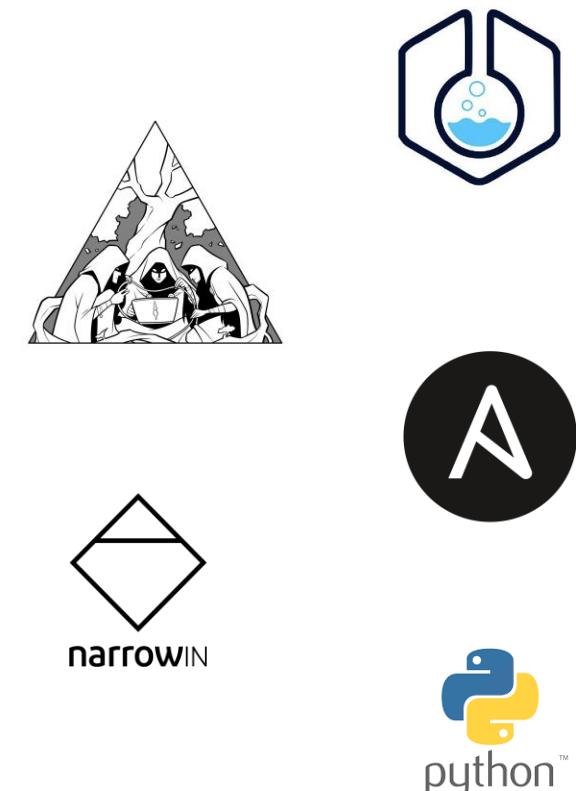
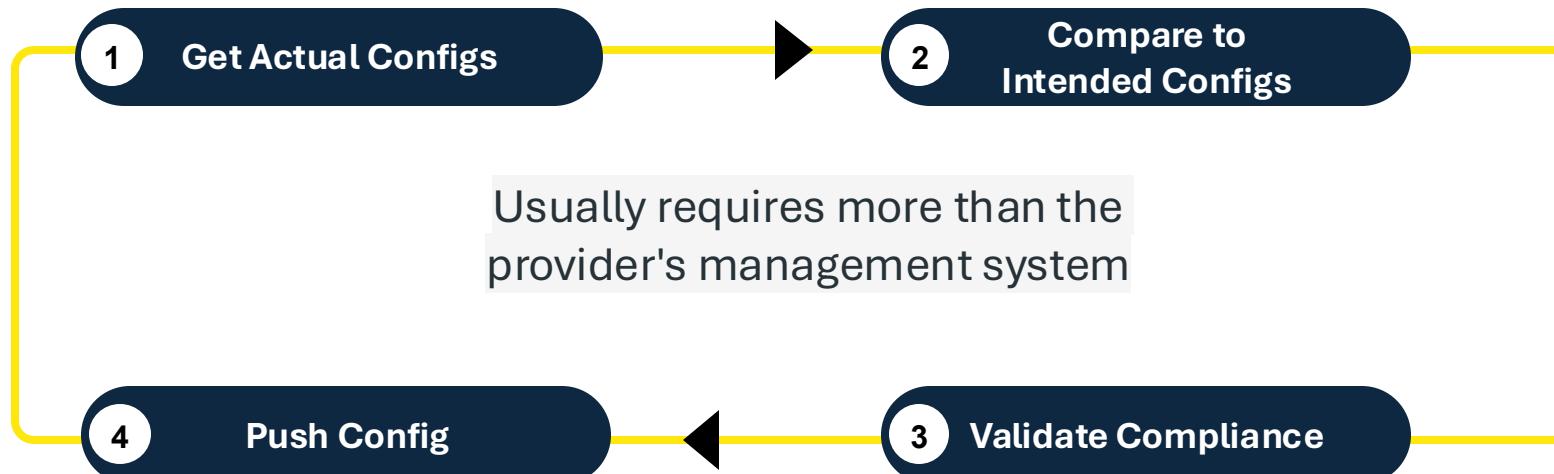
! NTP not configured
on 5% of the devices

! STP misconfiguration
on 4 devices

! VLAN 1 not disabled
on all devices

Let's automate it!

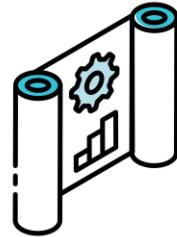
Through automation, these blind spots can be identified and resolved, preventing configuration drift.



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/>

