INDUSTRIAL SECURITY CONFERENCE COPENHAGEN 2025

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

Plan

Workshop

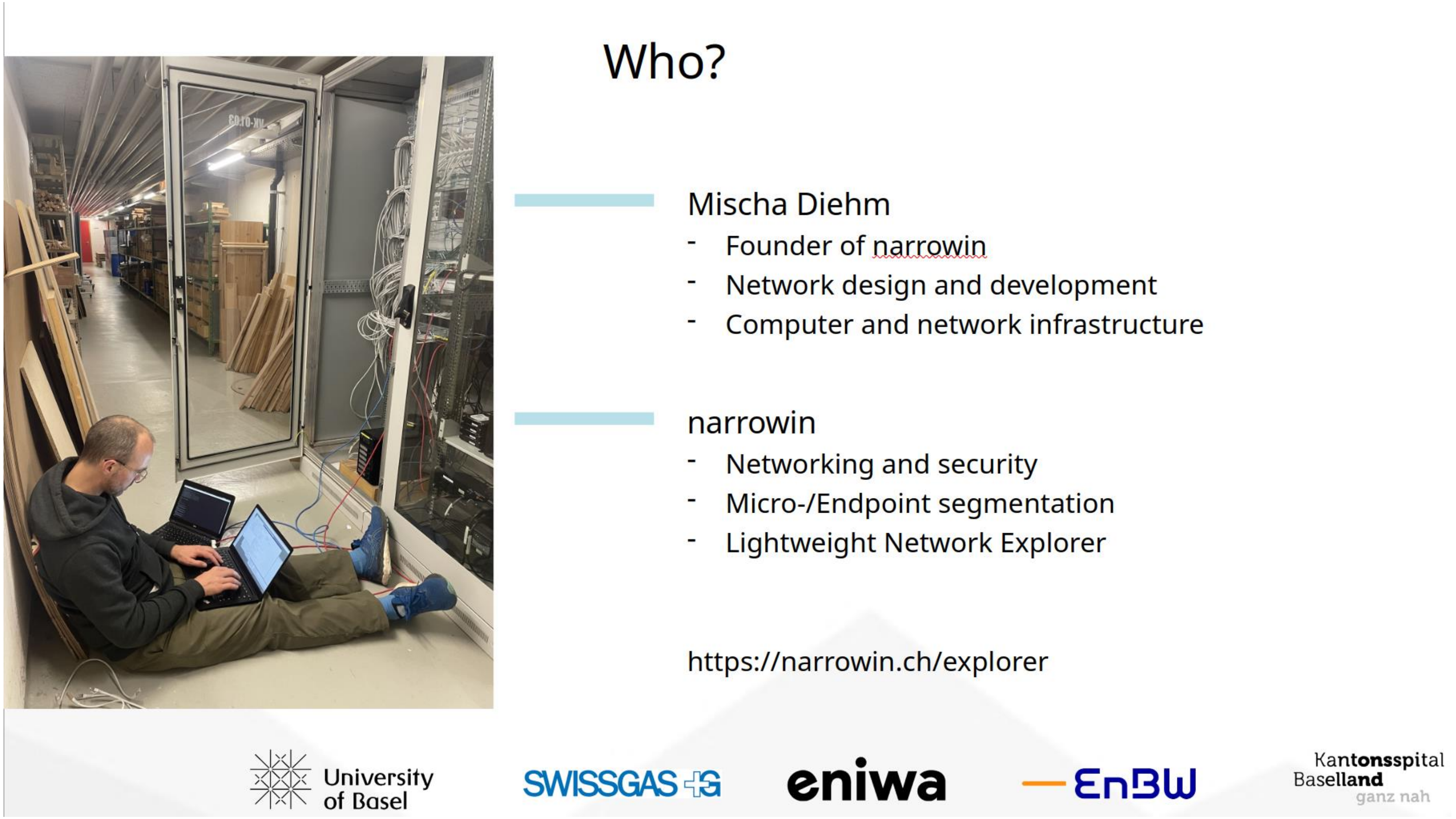
- Big Picture
- Lab Intro
- Defend
- Monitoring
- Zones & Conduits
- Network Automation

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

Who we are

Mischa Diehm

Martin Scheu



Who?

Mischa Diehm

- Founder of narrowin
- Network design and development
- Computer and network infrastructure

narrowin

- Networking and security
- Micro-/Endpoint segmentation
- Lightweight Network Explorer

https://narrowin.ch/explorer

University of Basel

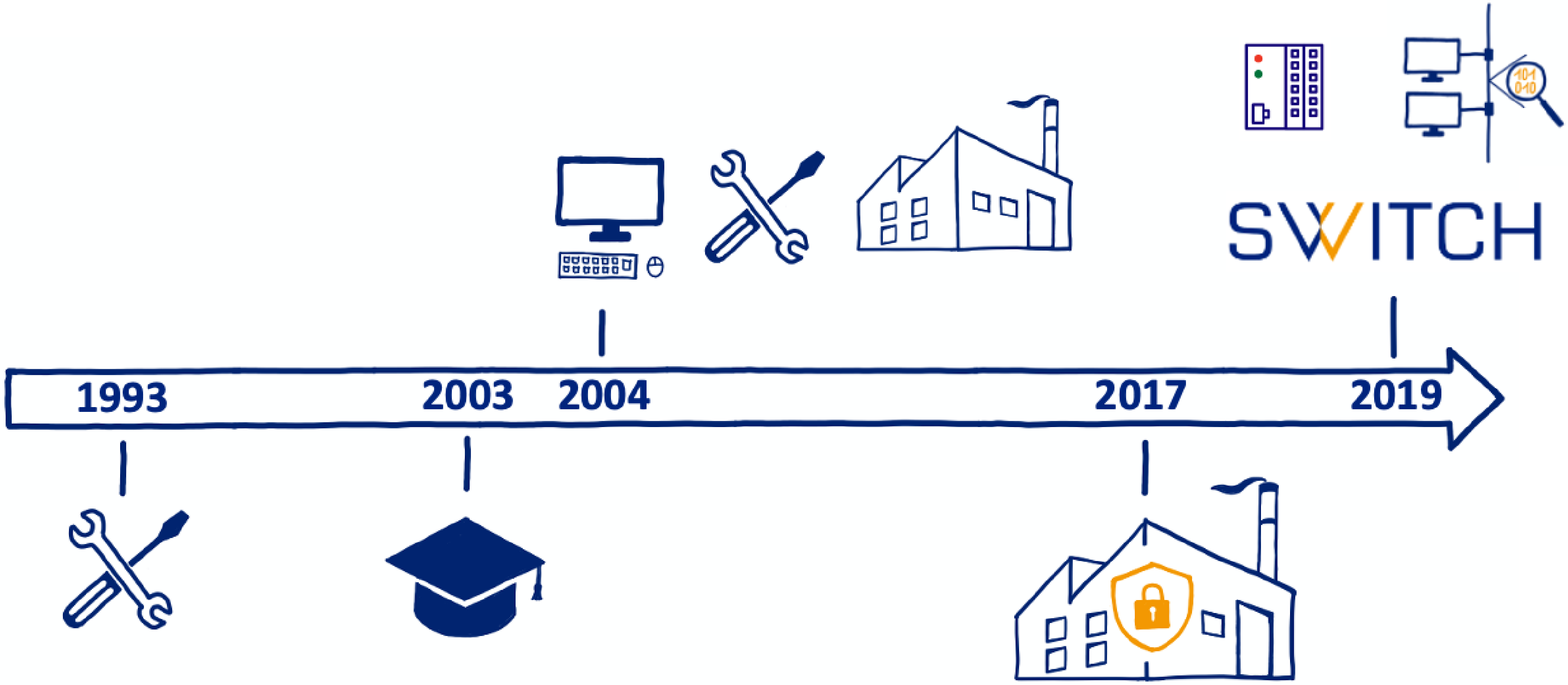
SWISSGAS

eniwa

EnBW

Kantonsspital Baselland
ganz nah

Martin Scheu



Big Picture

OT Networks are Business-critical

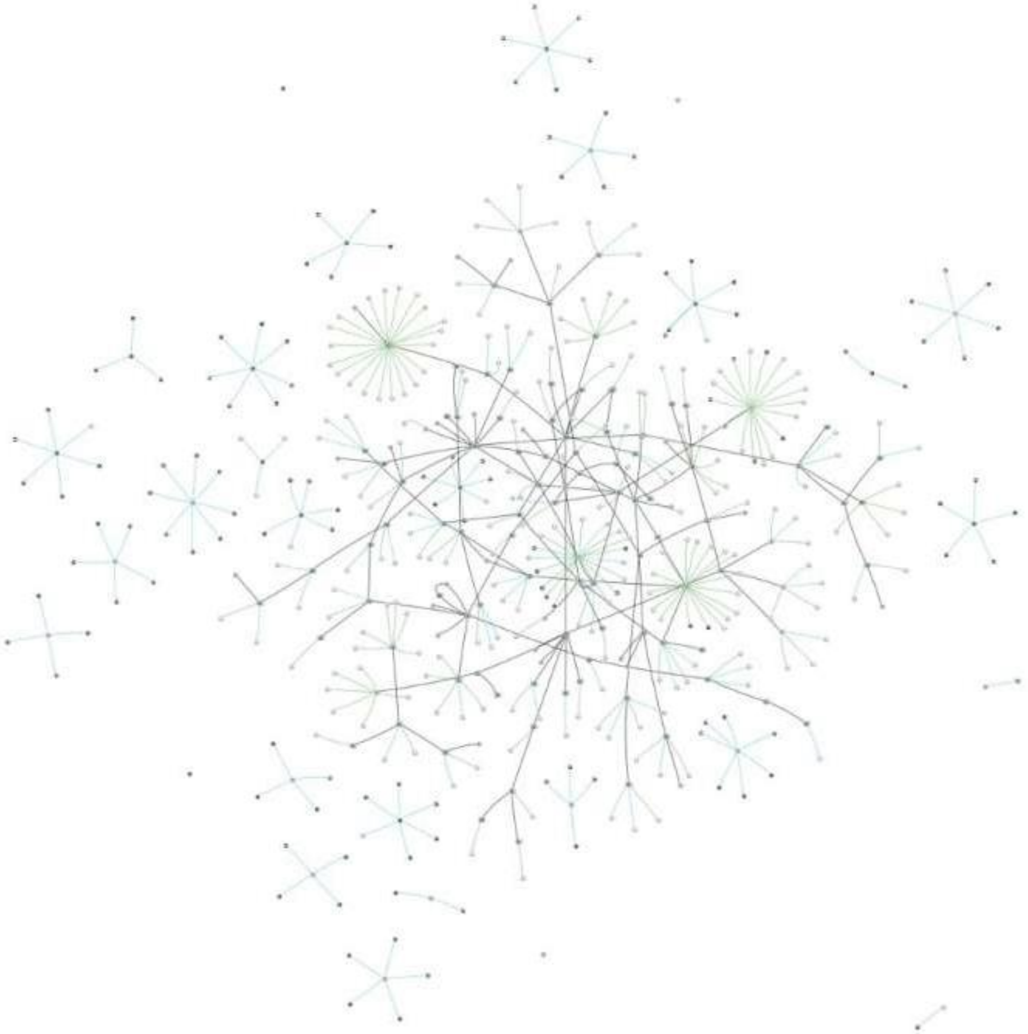
- Network disruptions lead to significant financial losses (e.g., production downtime).
- Regulatory pressure is increasing.

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

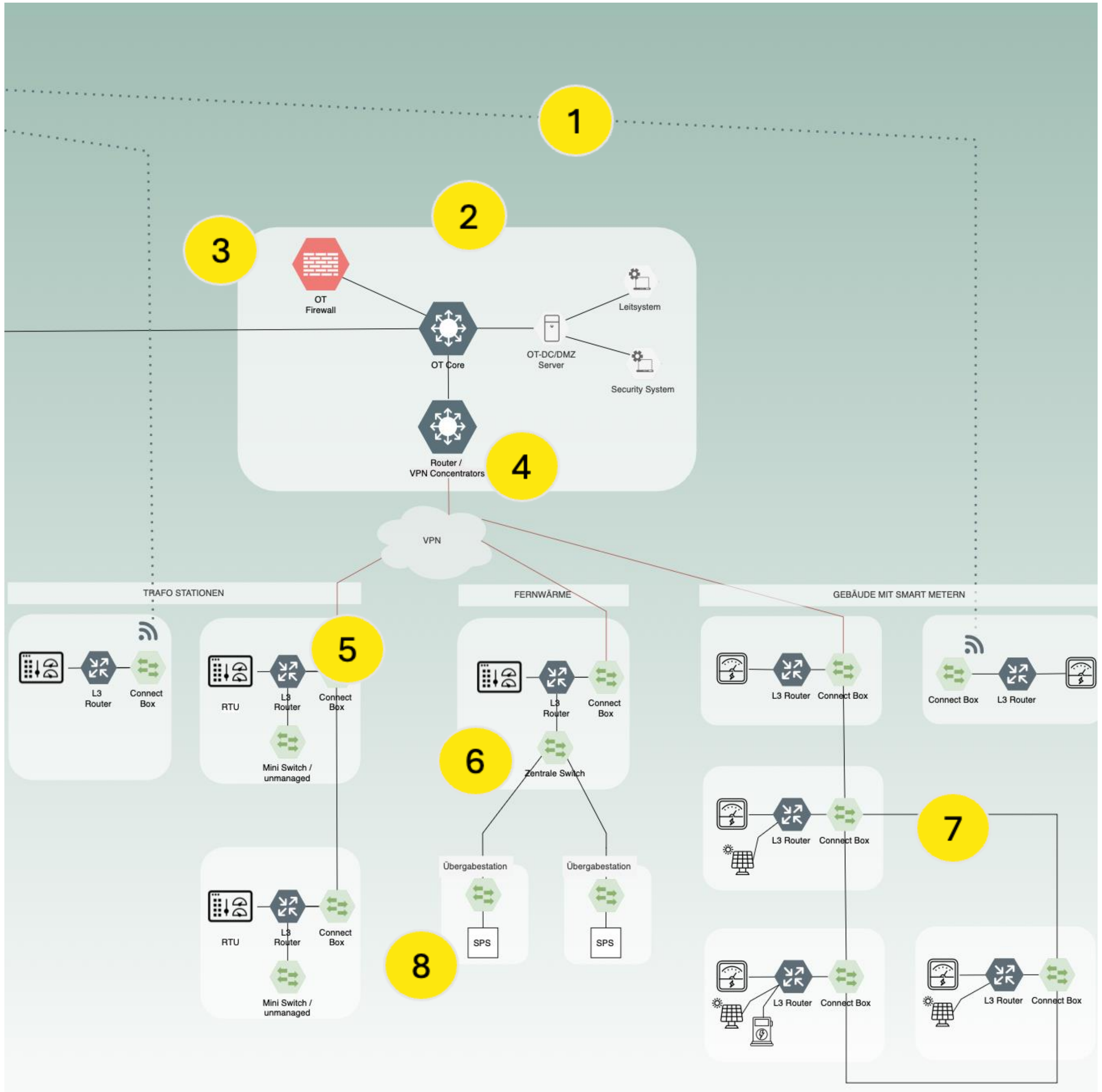
- Few people are familiar with networks
- Low level of (network) automation



Endless questions..

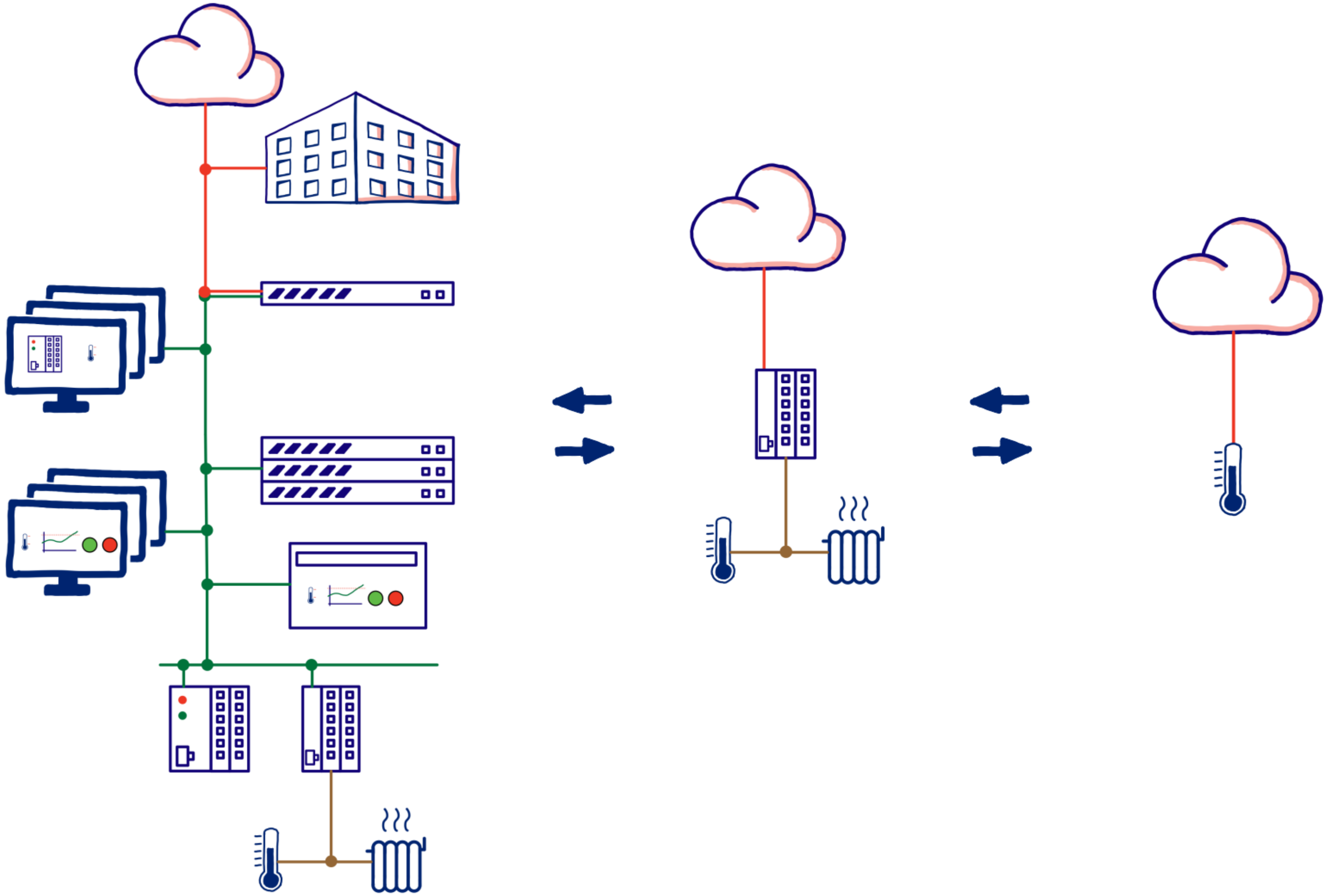
1. How can we ensure secure remote access?
2. Do we need a dedicated OT core?
3. How are these networks routed?
4. Do we need a firewall that “understands” OT protocols?
5. Do I need decentralized firewalls?
6. How can I standardize the setup for different use cases?
7. How do I minimize the blast radius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

… etc.

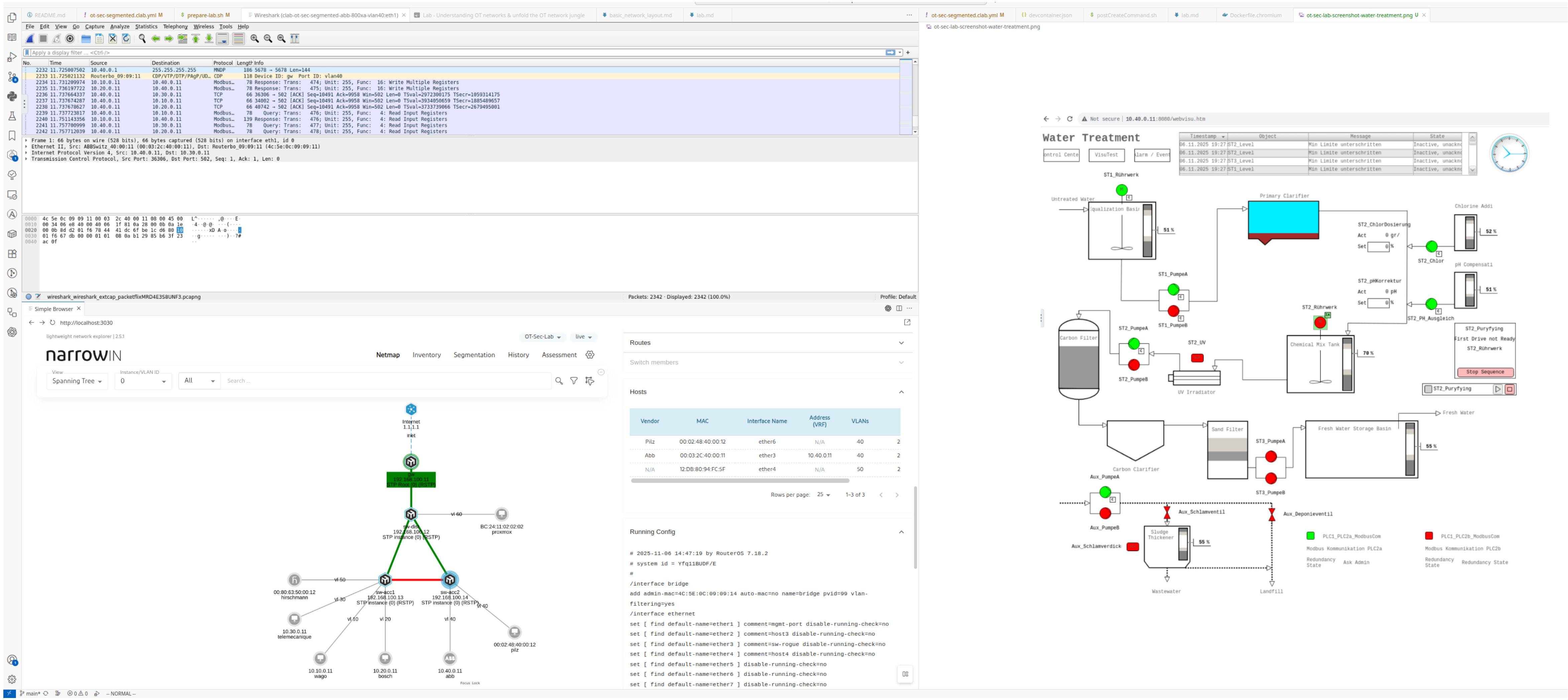


Purdue Model

- 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



```
No.  Time         Source            Destination           Protocol  Length Info
2232 11.725007502 10.40.0.1         255.255.255.255       MNDP      186 5678 → 5678 Len=144
2233 11.725021132 Routerbo_09:09:11 CDP/VTP/DTP/PAgP/UD…  CDP       118 Device ID: gw  Port ID: vlan40
2234 11.731209974 10.10.0.11        10.40.0.11            Modbus…    78 Response: Trans:   474; Unit: 255, Func:  16: Write Multiple Registers
2235 11.736197722 10.20.0.11        10.40.0.11            Modbus…    78 Response: Trans:   475; Unit: 255, Func:  16: Write Multiple Registers
2236 11.737664337 10.40.0.11        10.30.0.11            TCP        66 36306 → 502 [ACK] Seq=10491 Ack=9958 Win=502 Len=0 TSval=2972300175 TSecr=1059314175
2237 11.737674287 10.40.0.11        10.10.0.11            TCP        66 34002 → 502 [ACK] Seq=10491 Ack=9958 Win=502 Len=0 TSval=3934050659 TSecr=1885489657
2238 11.737678627 10.40.0.11        10.20.0.11            TCP        66 40742 → 502 [ACK] Seq=10491 Ack=9958 Win=502 Len=0 TSval=3733739066 TSecr=2679495001
2239 11.737723817 10.40.0.11        10.10.0.11            Modbus…    78    Query: Trans:   476; Unit: 255, Func:   4: Read Input Registers
2240 11.751143356 10.10.0.11        10.40.0.11            Modbus…   139 Response: Trans:   476; Unit: 255, Func:   4: Read Input Registers
2241 11.757700999 10.40.0.11        10.30.0.11            Modbus…    78    Query: Trans:   477; Unit: 255, Func:   4: Read Input Registers
2242 11.757712039 10.40.0.11        10.20.0.11            Modbus…    78    Query: Trans:   478; Unit: 255, Func:   4: Read Input Registers

▸ Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface eth1, id 0
▸ Ethernet II, Src: ABBSwitz_40:00:11 (00:03:2c:40:00:11), Dst: Routerbo_09:09:11 (4c:5e:0c:09:09:11)
▸ Internet Protocol Version 4, Src: 10.40.0.11, Dst: 10.30.0.11
▸ Transmission Control Protocol, Src Port: 36306, Dst Port: 502, Seq: 1, Ack: 1, Len: 0

0000  4c 5e 0c 09 09 11 00 03  2c 40 00 11 08 00 45 00   L^······ ,@····E·
0010  00 34 06 e8 40 00 40 06  1f 81 0a 28 00 0b 0a 1e   ·4··@·@· ···(····
0020  00 0b 8d d2 01 f6 78 44  41 dc 6f be 1c d6 80 10   ······xD A·o·····
0030  01 f6 67 db 00 00 01 01  08 0a b1 29 85 b6 3f 23   ··g····· ···)··?#
0040  ac 0f                                              ··

wireshark_wireshark_extcap_packetflixMRD4E3S8UNF3.pcapng    Packets: 2342 · Displayed: 2342 (100.0%)    Profile: Default
```

http://localhost:3030

lightweight network explorer | 2.5.1

narrowIN

View: Spanning Tree · Instance/VLAN ID: 0

Hosts

Vendor	MAC	Interface Name	Address (VRF)	VLANs
Pilz	00:02:48:40:00:12	ether6	N/A	40
Abb	00:03:2C:40:00:11	ether3	10.40.0.11	40
N/A	12:DB:80:94:FC:5F	ether4	N/A	50

Rows per page: 25 · 1–3 of 3

Running Config

```
# 2025-11-06 14:47:19 by RouterOS 7.18.2
# system id = Yfq11BUDF/E
#
/interface bridge
add admin-mac=4C:5E:0C:09:09:14 auto-mac=no name=bridge pvid=99 vlan-
filtering=yes
/interface ethernet
set [ find default-name=ether1 ] comment=mgmt-port disable-running-check=no
set [ find default-name=ether2 ] comment=host3 disable-running-check=no
set [ find default-name=ether3 ] comment=sw-rogue disable-running-check=no
set [ find default-name=ether4 ] comment=host4 disable-running-check=no
set [ find default-name=ether5 ] disable-running-check=no
set [ find default-name=ether6 ] disable-running-check=no
set [ find default-name=ether7 ] disable-running-check=no
```

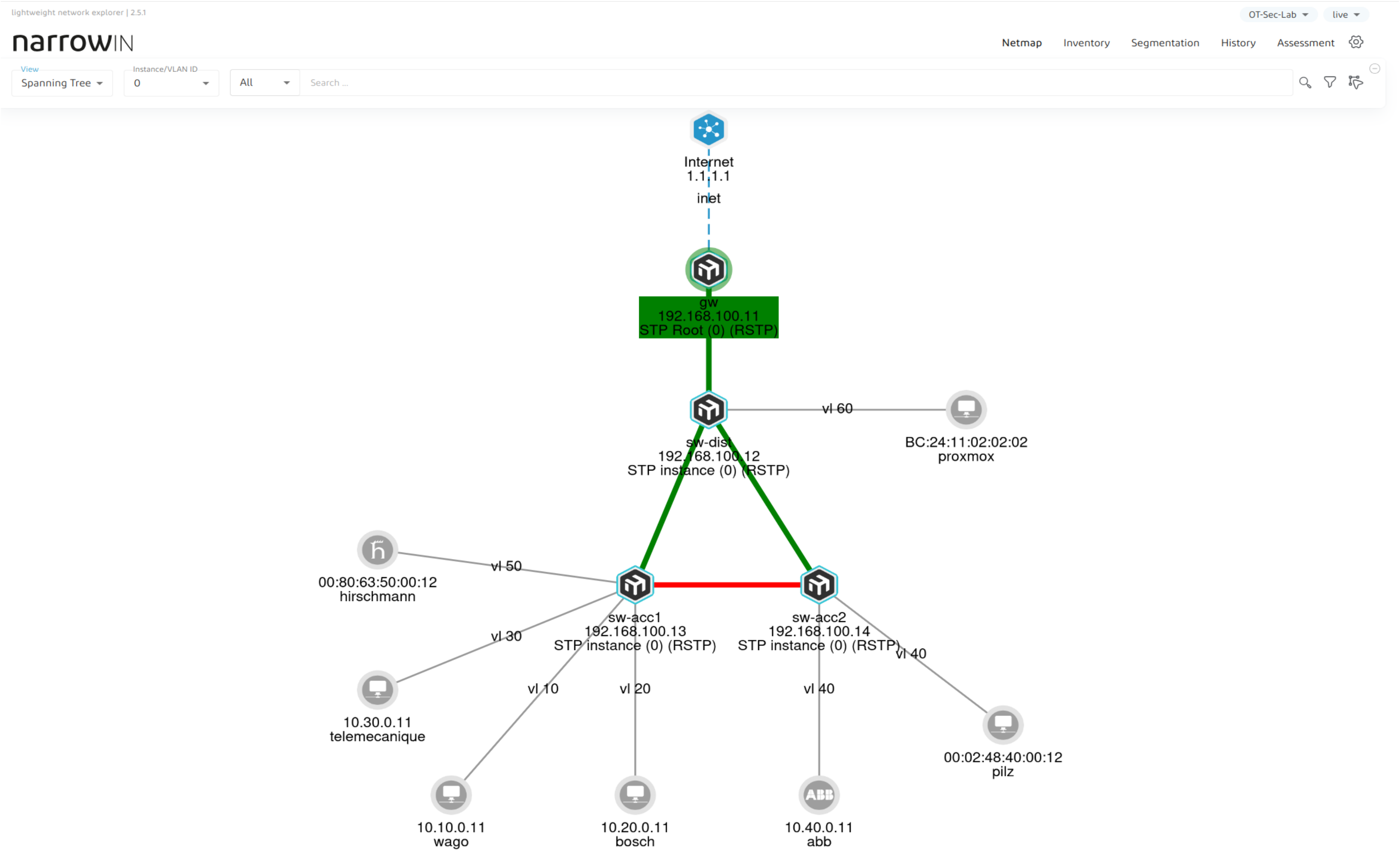
ot-sec-lab-screenshot-water-treatment.png

Not secure | 10.40.0.11:8080/webvisu.htm

Water Treatment

ontrol Cente · VisuTest · Alarm / Event

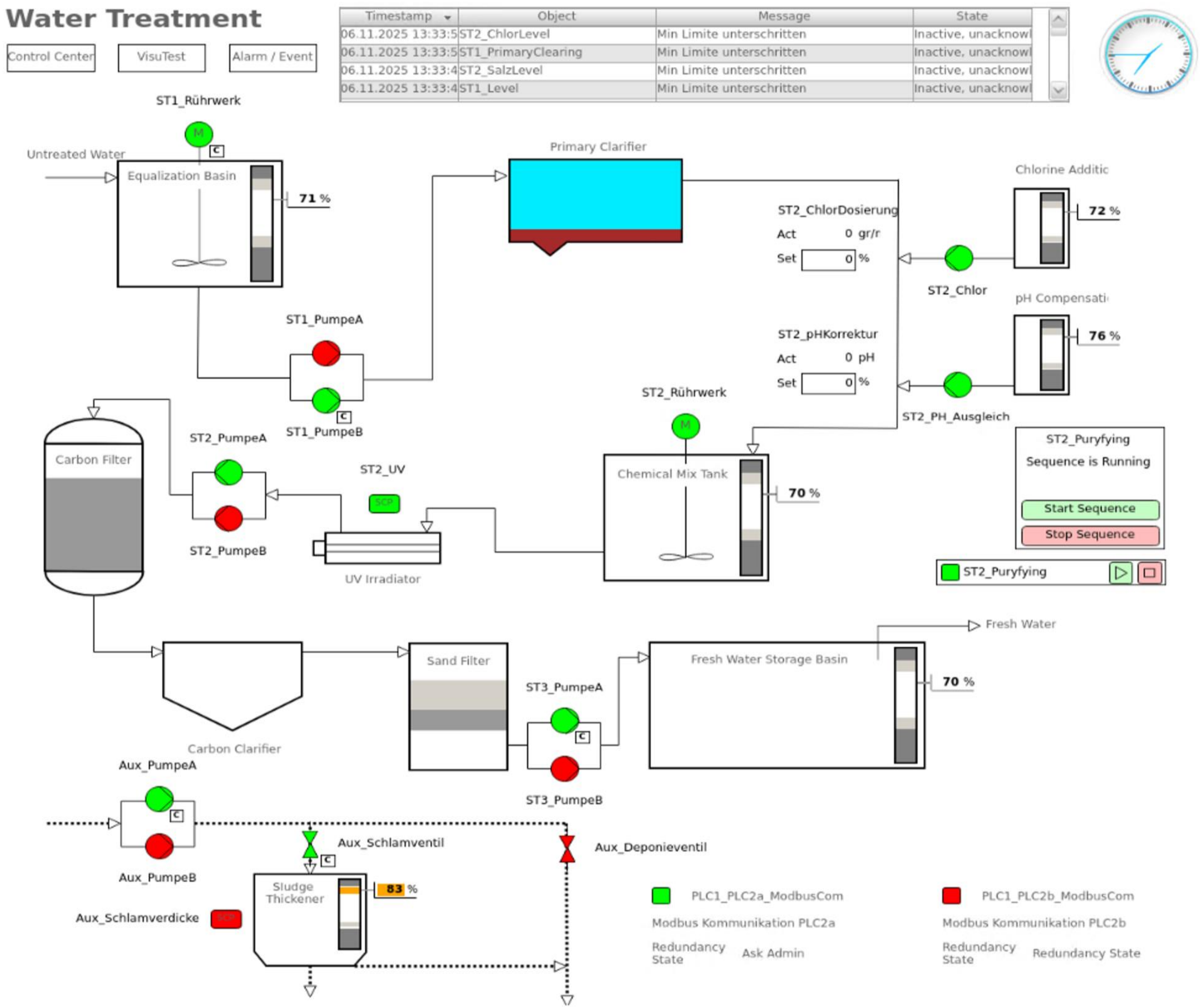
Timestamp	Object	Message	State
06.11.2025 19:27	ST2_Level	Min Limite unterschritten	Inactive, unackno
06.11.2025 19:27	ST2_Level	Min Limite unterschritten	Inactive, unackno
06.11.2025 19:27	ST3_Level	Min Limite unterschritten	Inactive, unackno
06.11.2025 19:27	ST1_Level	Min Limite unterschritten	Inactive, unackno



View: Spanning Tree

Instance/VLAN ID: 0

All



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

ST2_ChlorDosierung
Act 0 gr/r
Set 0 %

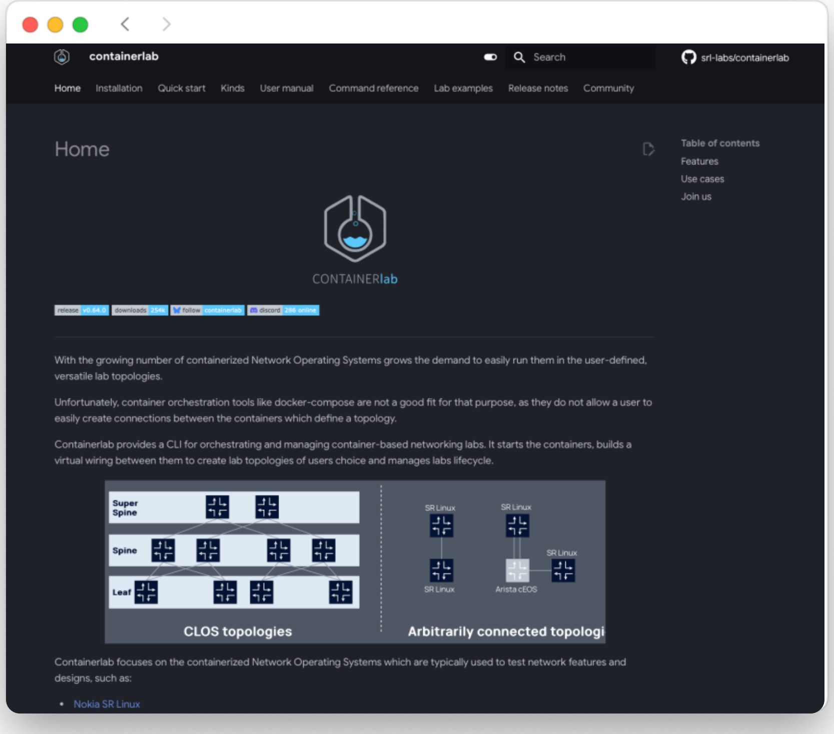
ST2_pHKorrektur
Act 0 pH
Set 0 %

ST2_Puryfying
Sequence is Running

Introducing Containerlab

https://containerlab.dev

- Containerized network operating systems (NOS, major vendors available)
- Can also launch traditional virtual machine-based routers
- Can interconnect arbitrary Linux containers
- Runs network operating systems in containers (Docker/Podman)
- Linux network namespaces
- Ideal solution for test environments
- Easy topology definition (text based - scriptable).



Home

With the growing number of containerized Network Operating Systems grows the demand to easily run them in the user-defined, versatile lab topologies.

Unfortunately, container orchestration tools like docker-compose are not a good fit for that purpose, as they do not allow a user to easily create connections between the containers which define a topology.

Containerlab provides a CLI for orchestrating and managing container-based networking labs. It starts the containers, builds a virtual wiring between them to create lab topologies of users choice and manages labs lifecycle.

Containerlab focuses on the containerized Network Operating Systems which are typically used to test network features and designs, such as:

- Nokia SR Linux

«Containerlab provides a CLI for orchestrating and managing container-based networking labs. It starts the containers, builds a virtual wiring between them to create lab topologies of users' choice and manages labs lifecycle.»

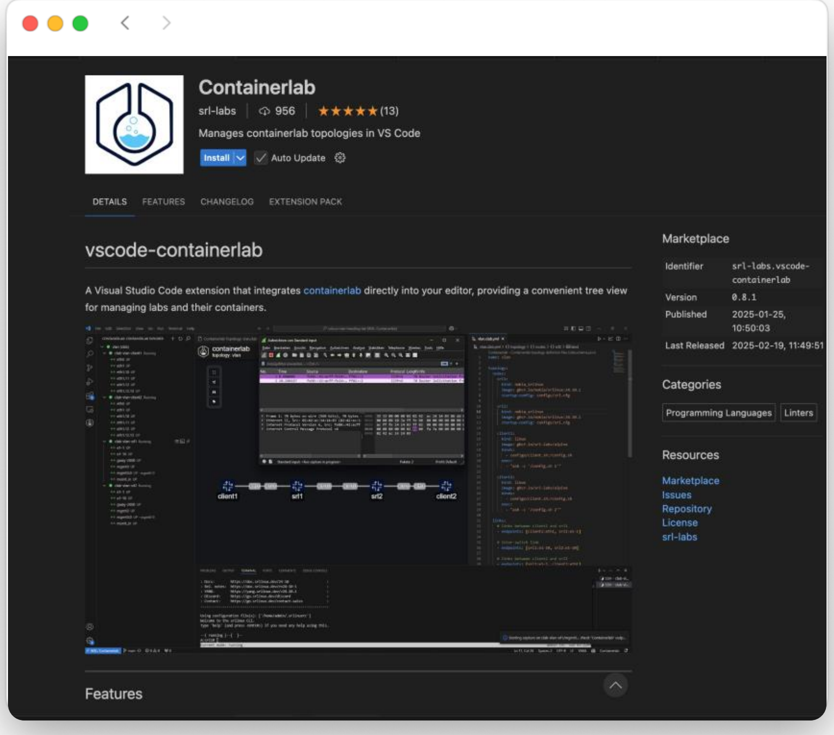
… and there‘s a helpful VSCode extension

Simplified workflow for almost everything from the command line. Useful even for network engineers – like me – who are more accustomed to working in a CLI-driven environment ;-)

Features:

- Lab explorer: Real-time monitoring of lab status, including nodes and links.
- Lab Editor: topology modifications within VS Code environment.
- TopoViewer: visual representation of the lab setup.

- Packet Capture: Wireshark integration, capture traffic on a selected link.
- Direct CLI Access: connect to node consoles.
- Link Impairment Tuning: simulation of network delays, packet loss, etc.



Containerlab

srl-labs | 956 | ★★★★★ (13)

Manages containerlab topologies in VS Code

vscode-containerlab

A Visual Studio Code extension that integrates containerlab directly into your editor, providing a convenient tree view for managing labs and their containers.

Features

Marketplace

Identifier	srl-labs.vscode-containerlab
Version	0.8.1
Published	2025-01-25, 10:50:03
Last Released	2025-02-19, 11:49:51

Categories

Programming Languages | Linters

Resources

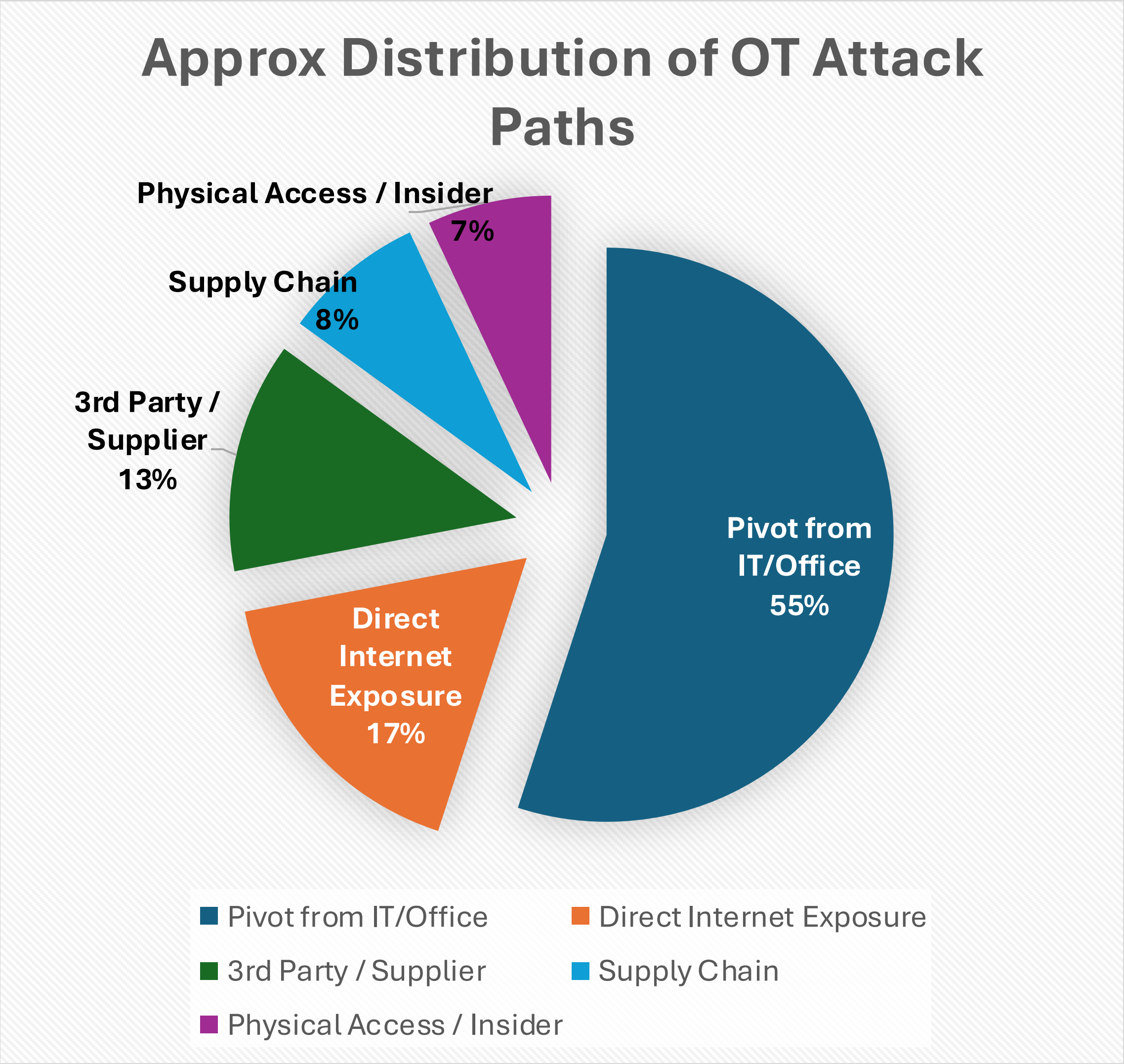
Marketplace
Issues
Repository
License
srl-labs

Defend

OT Attacks

Mostly:

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



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

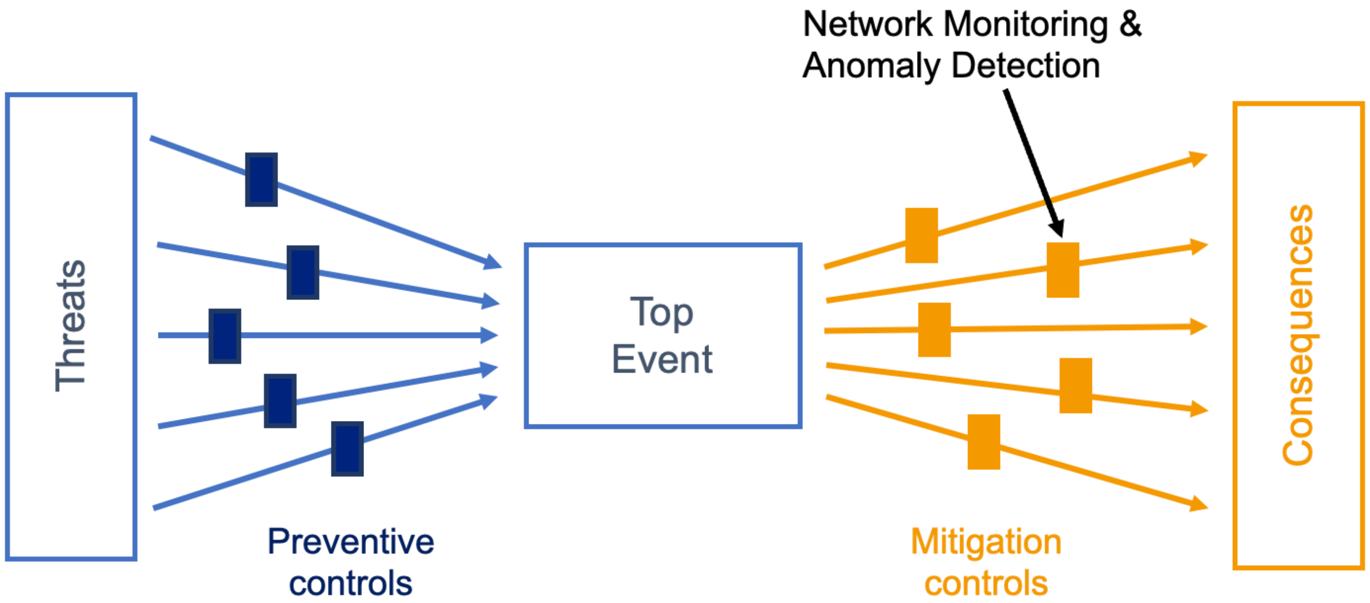
OT Network Security Monitoring

Mandatory - but overhyped

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

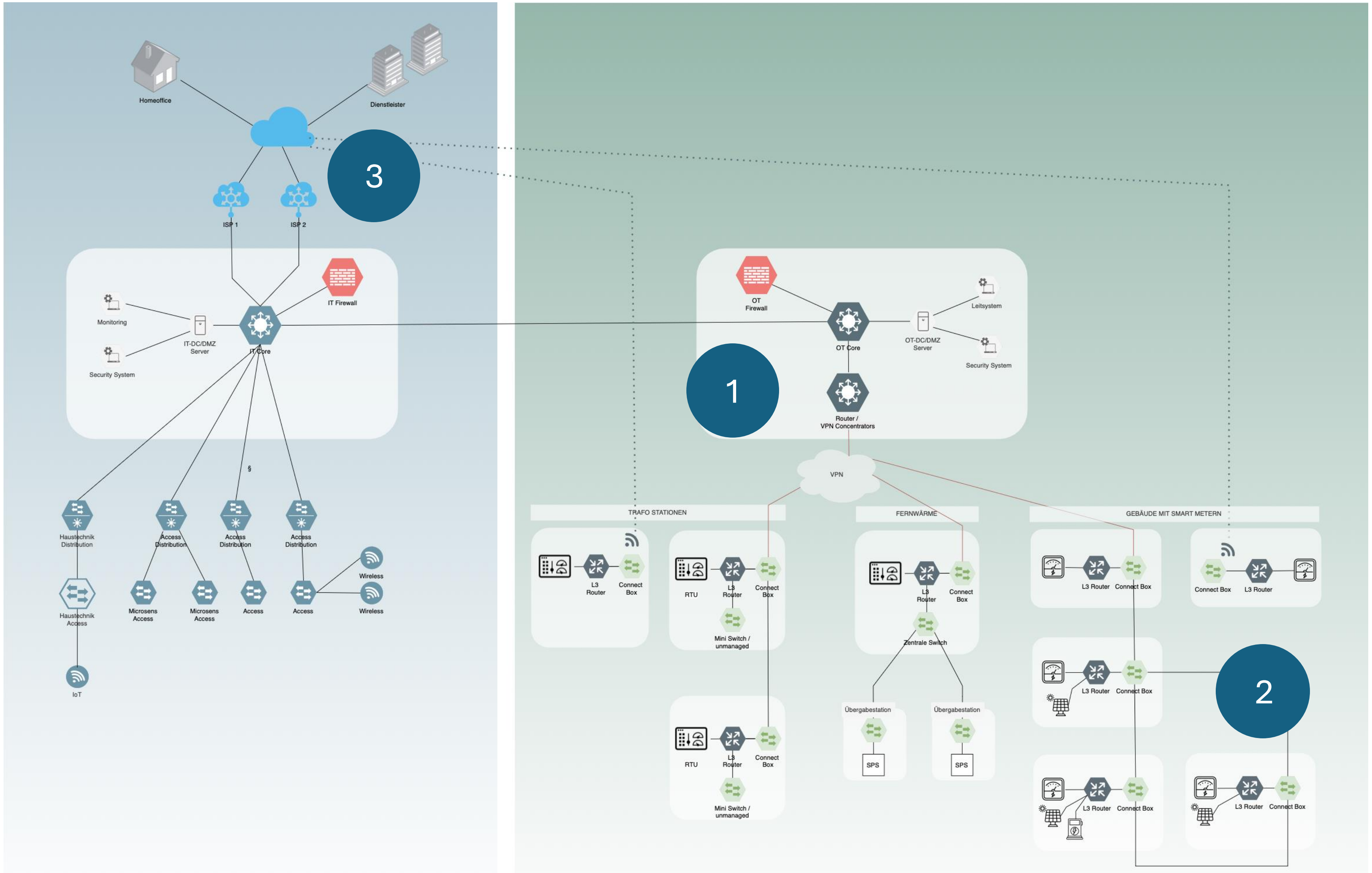
What it really is:

- 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



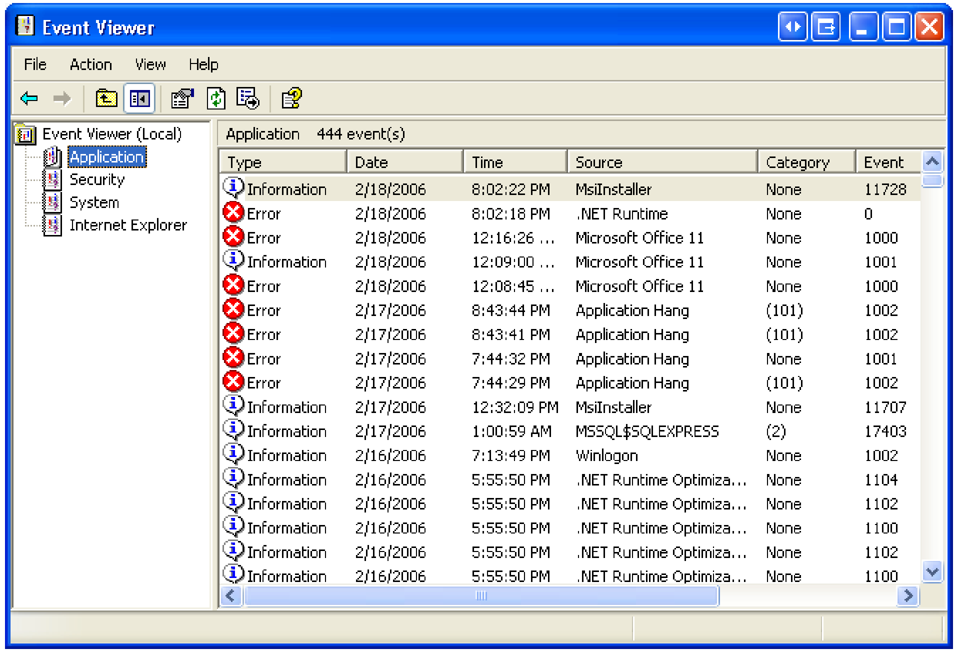
Logs

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!



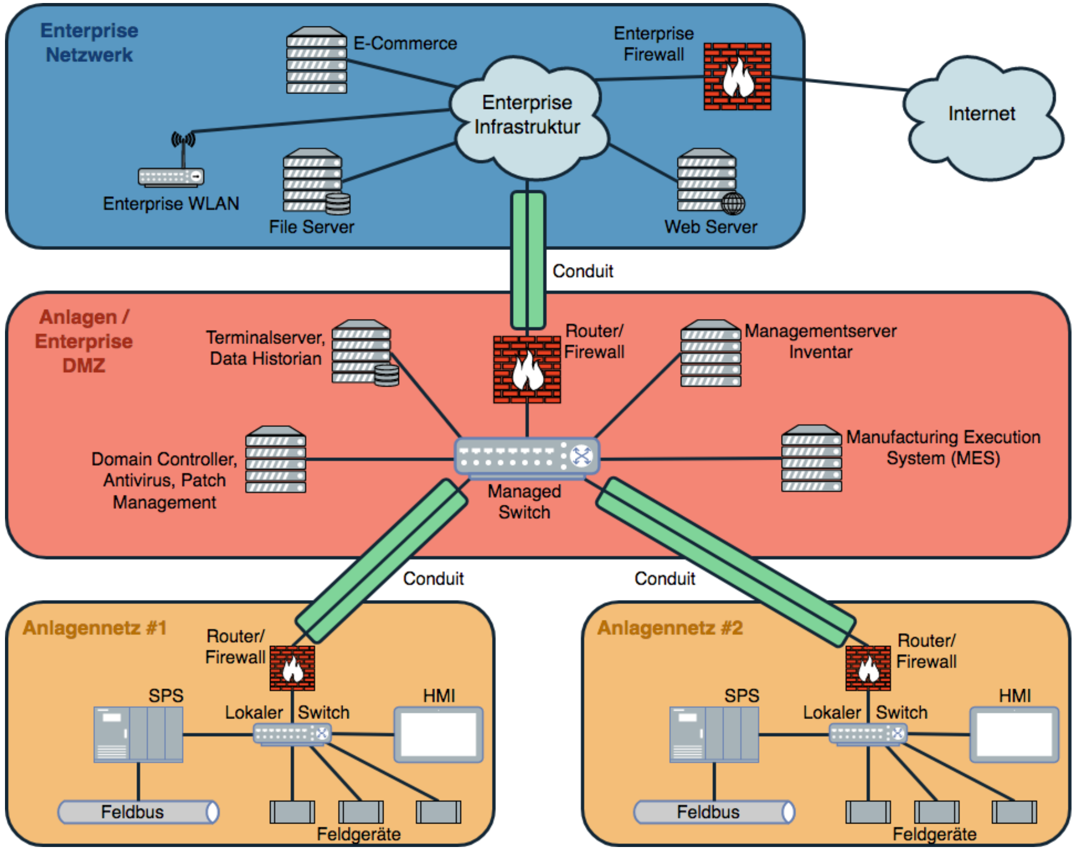
Application 444 event(s)

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/

-> Comon ground for OT & network Engineers

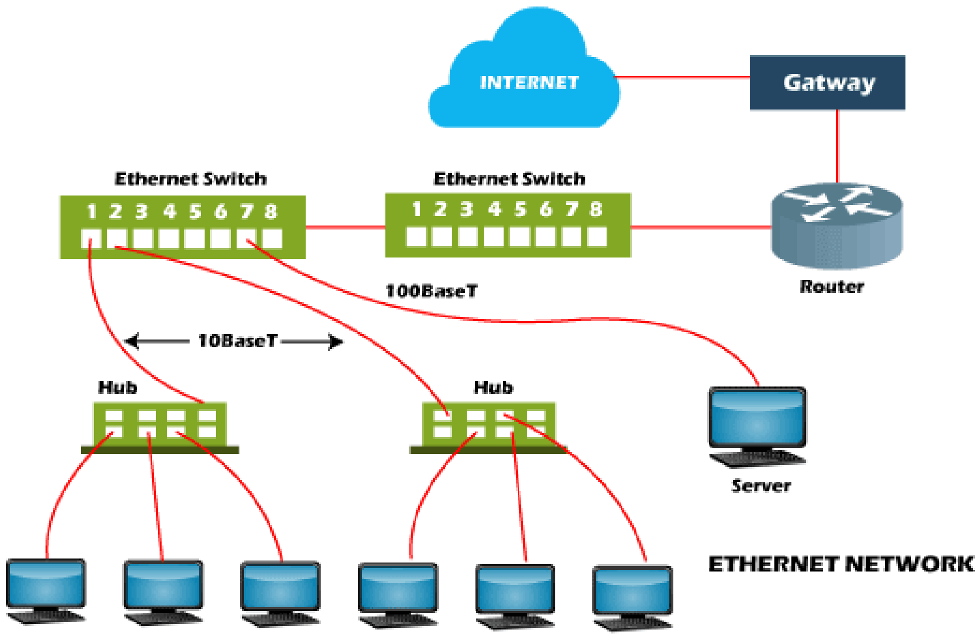
Simplified OT OSI Layer Model

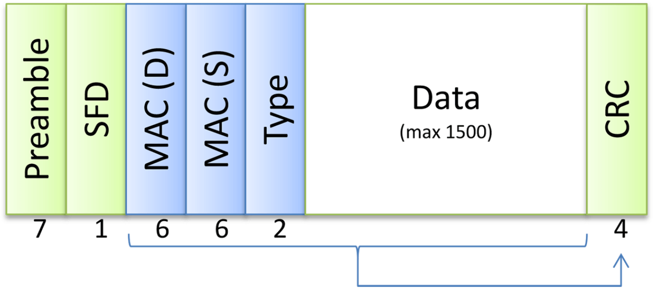
				"Real Time"	Before TCP/IP
Host	**Layer 5-7** Application	Human-machine interfaces (HMI), SCADA logic, data encoding and commands	ModbusTCP, PROFINET, S7, IEC-104, IEC 60850 MMS, OPC-UA, MQTT,BACnet/IP, KNXnet/IP, EtherNet/IP	Profinet RT, EtherCAT, IEC 60850 GOOSE & SMV (Sampled Measured Values)	Modbus, IEC-101, HART BACnet, KNX, CAN
	Layer 4 Transport	Ensures end-to-end communication	TCP, UDP (e.g. ModbusTCP uses TCP Port 502)		
Media	**Layer 3** Network	IP addressing and routing	Used by TCP/UDP based OT Protocols		
	Layer 2 Data Link	MAC addressing, VLAN, error checking	MAC addressing, VLAN, error checking	Profinet RT (0x8892), EtherCAT (0x88A4) GOOSE (0x88BA)	Error checking
	Layer 1 Physical	Transmission media, electrical signals	Ethernet cables, Fiber optics, Wireless	Ethernet cables, Fiber optics	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





Preamble	SFD	MAC (D)	MAC (S)	Type	Data (max 1500)	CRC
7	1	6	6	2		4

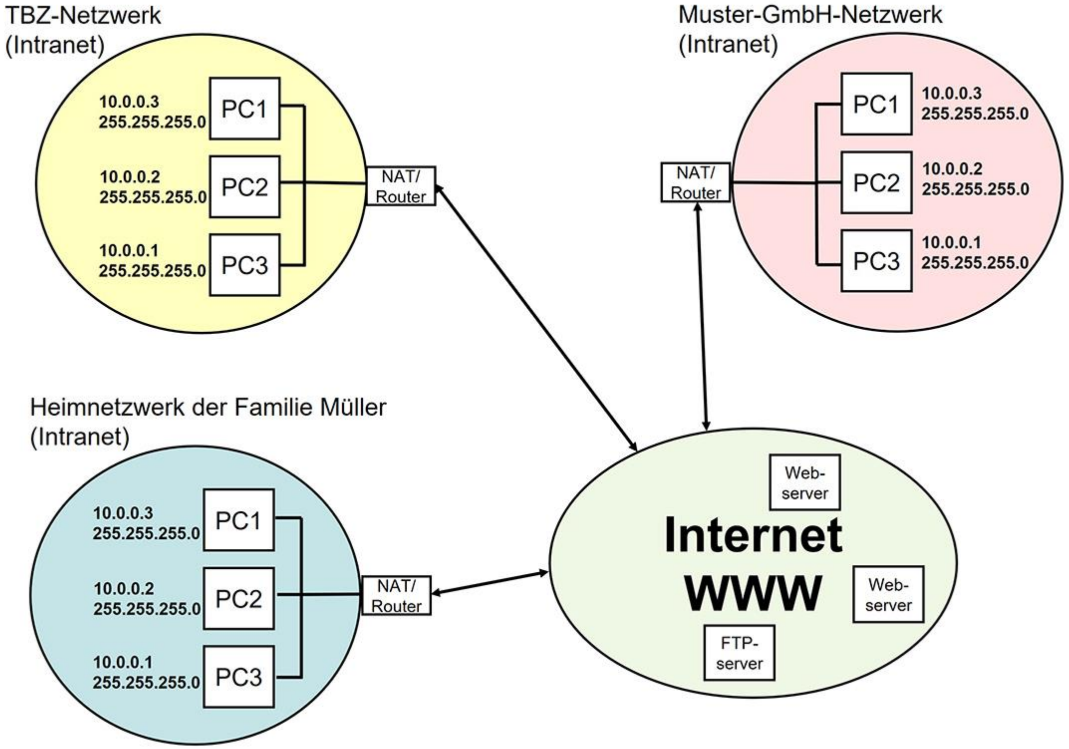
Layer 3 - IPv4

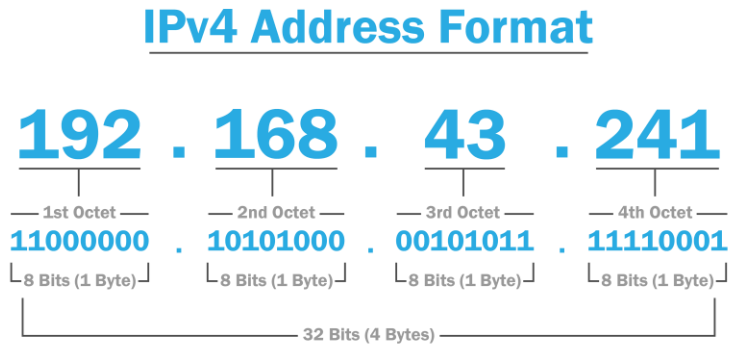
Fundamental Protocol of the Internet

- 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

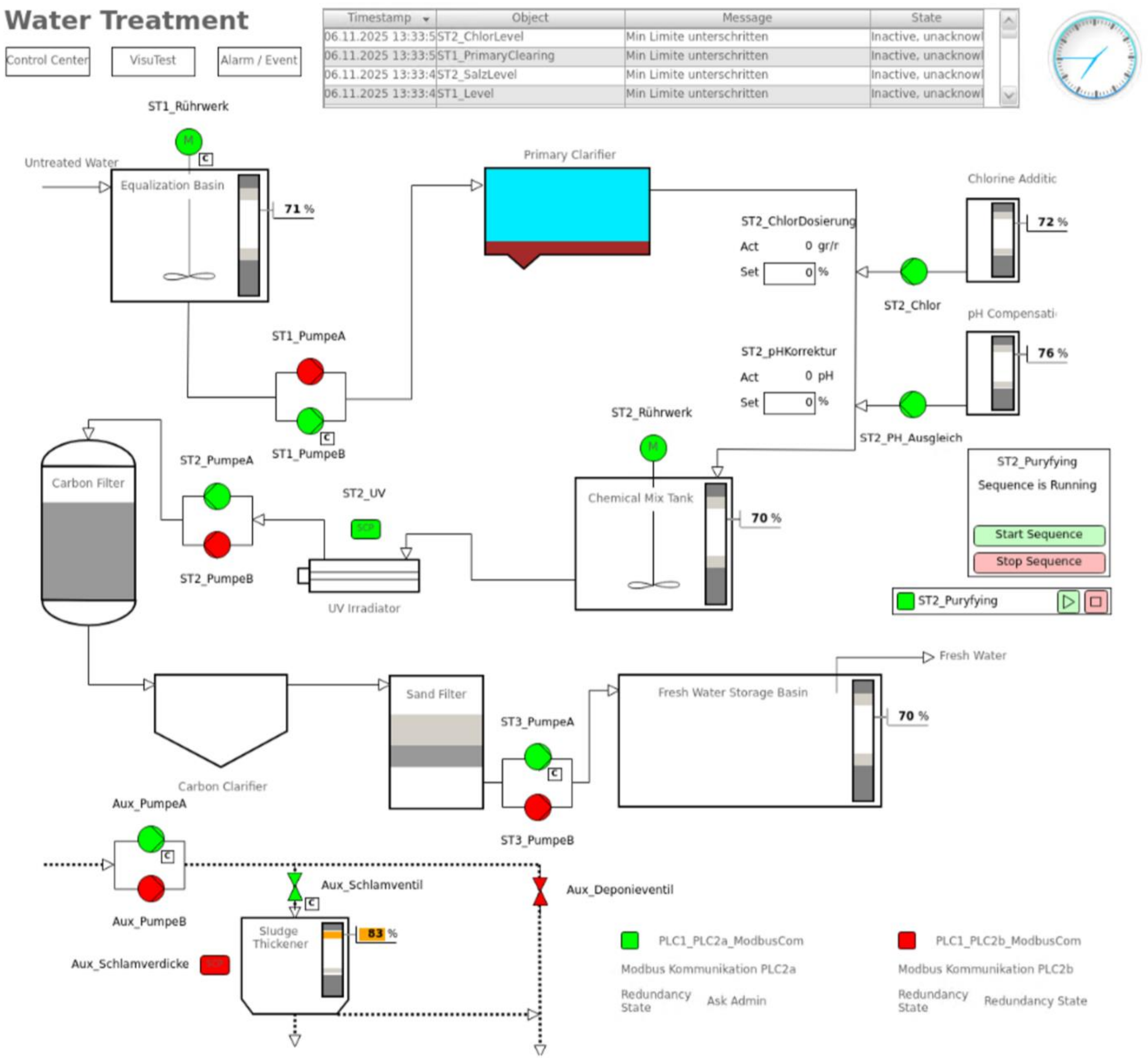
- NAT (Network Address Translation)

- Subnet mask & network/host portion:
  - 255.255.255.0 (or /24)





Exercise:
define Zones and Conduits



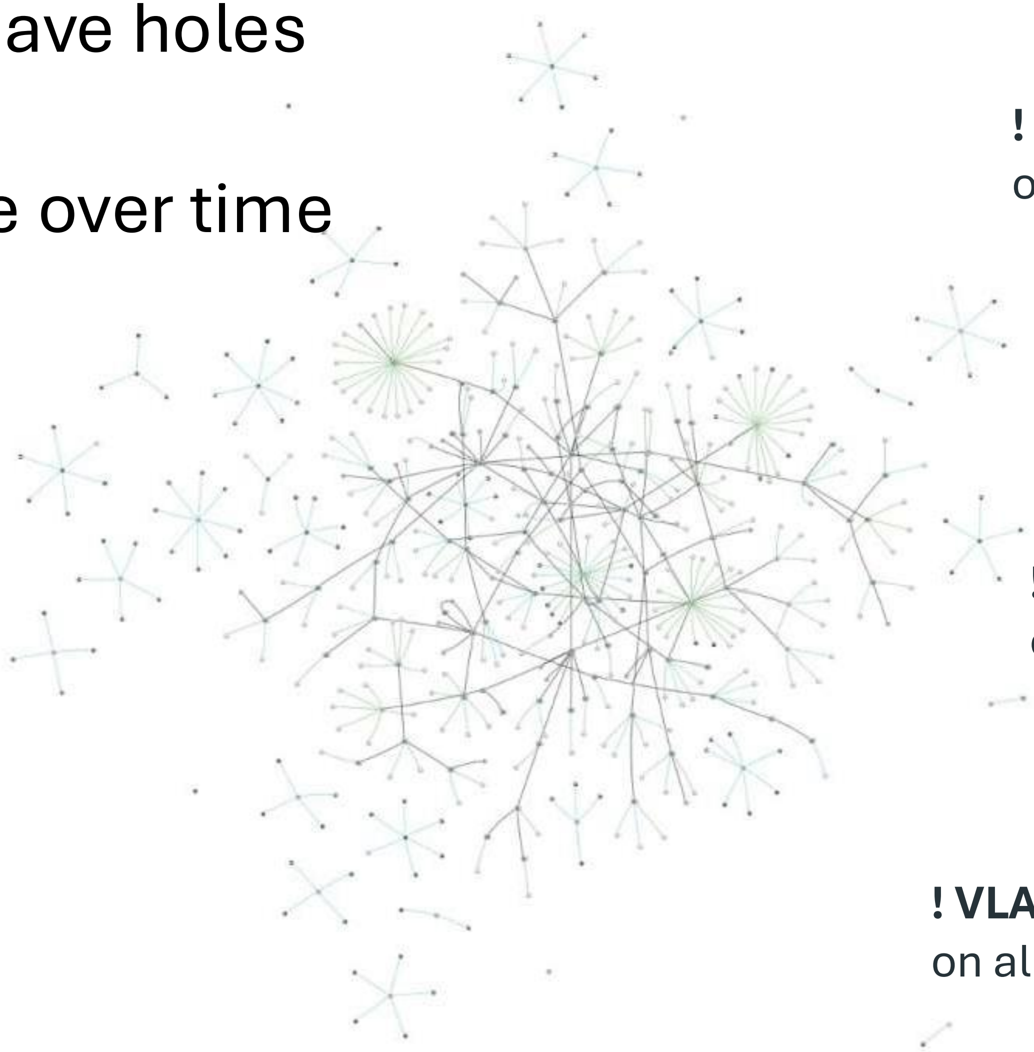
Timestamp	Object	Message	State
06.11.2025 13:33:5	ST2_ChlorLevel	Min Limite unterschritten	Inactive, unacknowl
06.11.2025 13:33:5	ST1_PrimaryClearing	Min Limite unterschritten	Inactive, unacknowl
06.11.2025 13:33:4	ST2_SalzLevel	Min Limite unterschritten	Inactive, unacknowl
06.11.2025 13:33:4	ST1_Level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

A simple Zone Concept

			To									
		Zone	OT DMZ			OT - Operations				OT - Engineering		
			Default	Service	...	Hygiene	Waste Treatment	Main Process	Central Control Room	Management	Configuration	...
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 inventible
And they accumulate over time



! NTP not configured
on 5% of the devices

! Reversible password encryption
on 16 devices

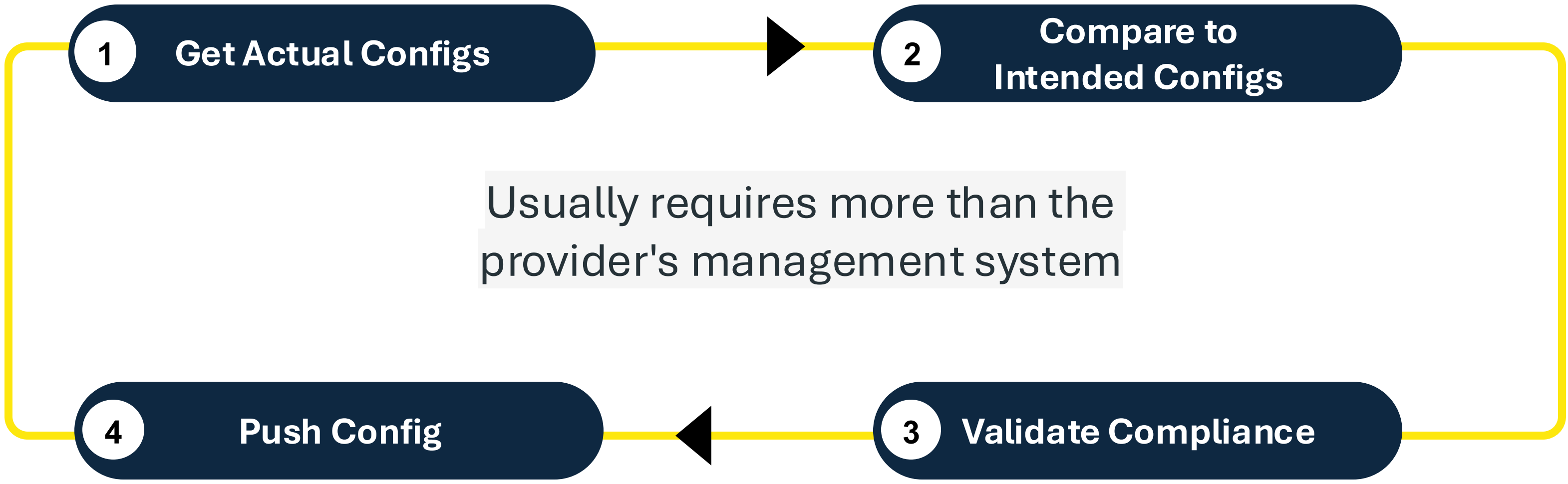
! STP misconfiguration
on 4 devices

! Missing Port security
on 20% of the 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.



1 Get Actual Configs

2 Compare to Intended Configs

3 Validate Compliance

4 Push Config

Usually requires more than the provider's management system

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

Mischa Diehm
Founder narrowin.ch

martin.scheu@switch.ch

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