Building an ICS Firing Range (in our kitchen)

Sharing Our Journey & Lessons Learned

6 October 2022

Table of content

About Me

Olaf Schwarz

Incident Response, Forensic & Threat Intelligence

NVISO since April 2021

Past:

- National CERT & GovCERT & EnergyCERT Österreich
- Informationssicherheit in der Finanzbranche
- + 10 Jahre in InfoSec

oschwarz@nviso.eu

NVISO

NVISO is a pure play **Cyber Security consulting firm** since 2013 with 150+ specialized security experts.

Initially founded in **Belgium**, we opened offices in **Germany** (Frankfurt & Munich), **Austria** and **Greece**!

We invest 10% of our annual revenue in research and development of new security techniques and the development of new solutions.

About the team

Nico Leidecker
Penetration Testing / Red Team Lead
15 years in IT security
nleidecker@nviso.eu

Moritz Thomas
Security Consultant and R&D
IoT & ICS Enthusiast
mthomas@nviso.eu

Firing Ranges and OT & ICS

What is a Firing Range?

- Controlled, interactive environment
- Abstraction of real environment
- As realistic as possible
- Re-usable
- “Playground”
- **Full virtual environment becomes more of an issue**

Why a Firing Range?

What are some of the benefits of having a firing range?

Training

Security Assessments

Awareness

Visual Impact

Testing

Security Testing

Development

Detection and Forensic Readiness

Attacks against ICS

Common Attacker Objectives

LOSS

view

DENIAL

control

safety

MANIPULATION

view

control

sensors and instruments

safety

The impact on ICS by reaching these objectives can be severe:

- Failure can harm human life.
- Expensive & hard to replace hardware involved.

Example 1

Crashoverride/Industroyer

TARGET

Energy sector
Attributed to 2016 attack on Ukraine's power grid causing a power outage in Kiev

FUNCTION

Standard backdoor/RAT functionality;
A modular framework to add functionality

MODULES

Implemented as DLLs and controlled by config file

- **Data wiper**: Aims to delete ICS configuration files and render infected system unusable
- **IEC 101 and 104**: Switching states of IOAs (for example open a circuit breaker)
- **IEC 61850**: Tried to identify nodes related to circuit breakers, for selected nodes it sends write requests
- **OPC DA**: Iterates all OPC servers/items and tries to switch state for selected items
- **SIPROTEC DoS**: Leverages CVE-2015-5374 to mess up protection relays

Source: BBC

Example 1.2

Industroyer V2

TARGET

Energy sector
Reported in April 2022 targeting again Ukraine's power grid

FUNCTION

- Similar code segments to 104.dll from original Industroyer
- Not a framework anymore
- Implementing just IEC 104
- Hardcoded configuration in binaries
- Config includes IP Addresses to target

Source: BBC

Example 2

TRISIS / Triton

2017	Deployed at least against one victim in the Middle East; reporting on Malware late 2017
TARGET	Safety Instrumented Systems (SIS) Schneider Electric's Triconex
FUNCTION	TRISIS has the capabilities to delete and upload the safety logic, utilizing the native TriStation protocol
DAMAGE	▪ Attackers gained access to an SIS engineering workstation ▪ Plant shut down initiated by a fail safe condition triggered – unwanted side effect of the changes performed by the attackers ▪ Affected device had the physical keyswitch in programming mode → "Run mode" would have prevented the changes

Image-Source

Building an ICS firing range of a bridge

(in our kitchen)

How it all started…

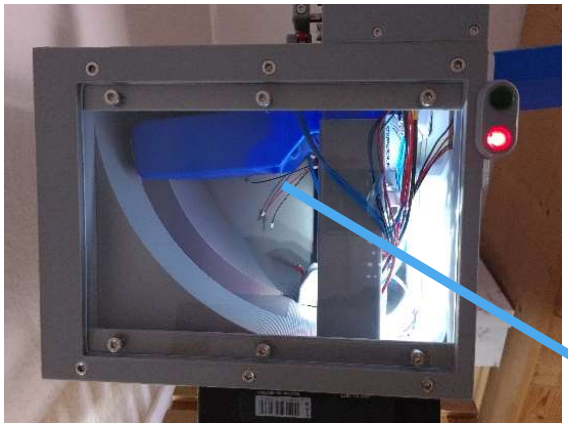
Concept

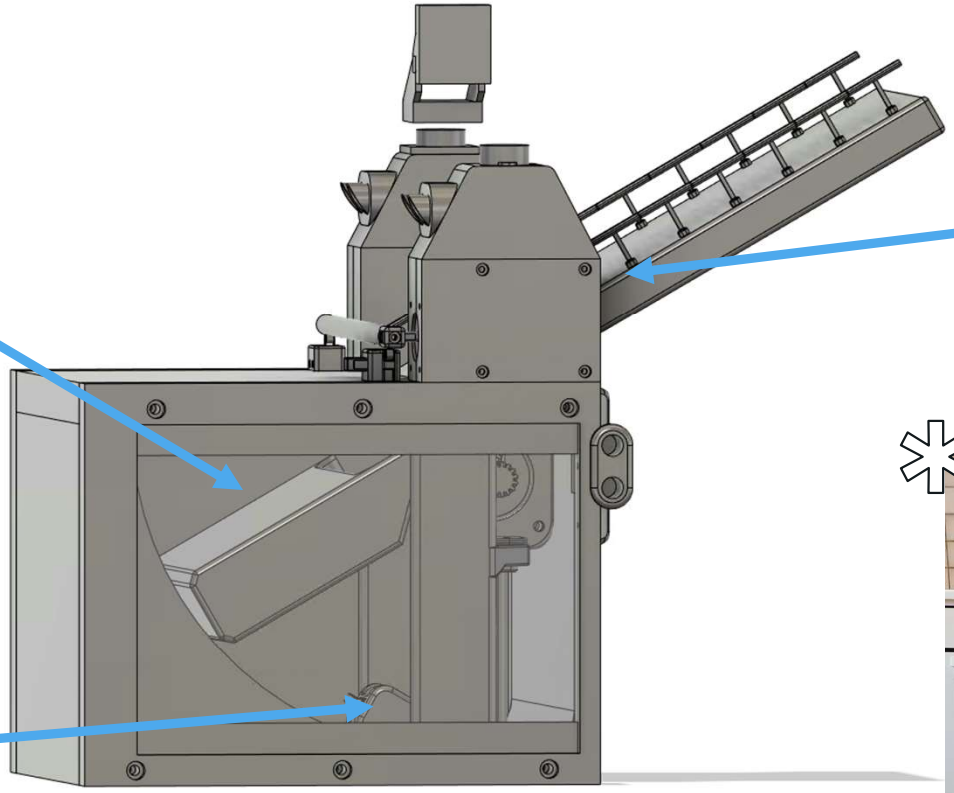
- Model of a **Water Treatment Plant** comprised of
  - Three stage water filtration system
  - Pumping stations
  - Virtualized IT network infrastructure

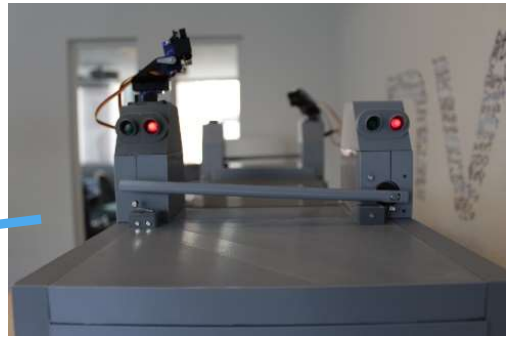
Requirements

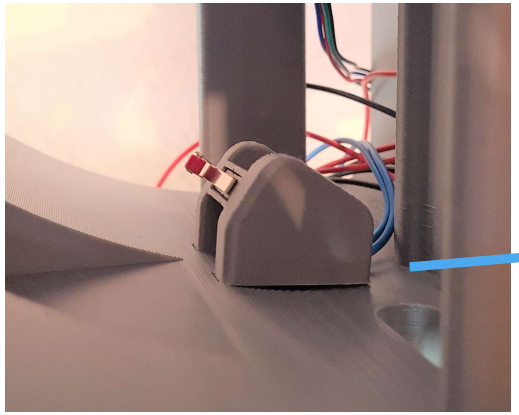
- Mobile solution
- Scenario-based training for DFIR teams

3D Printed Model

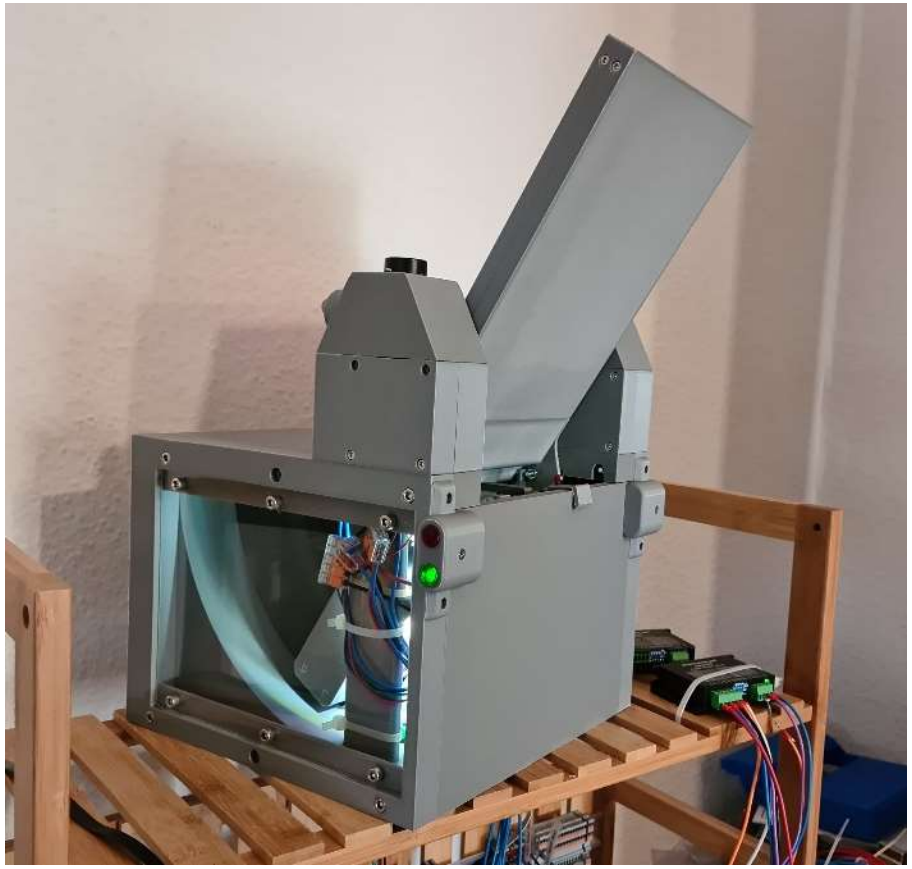






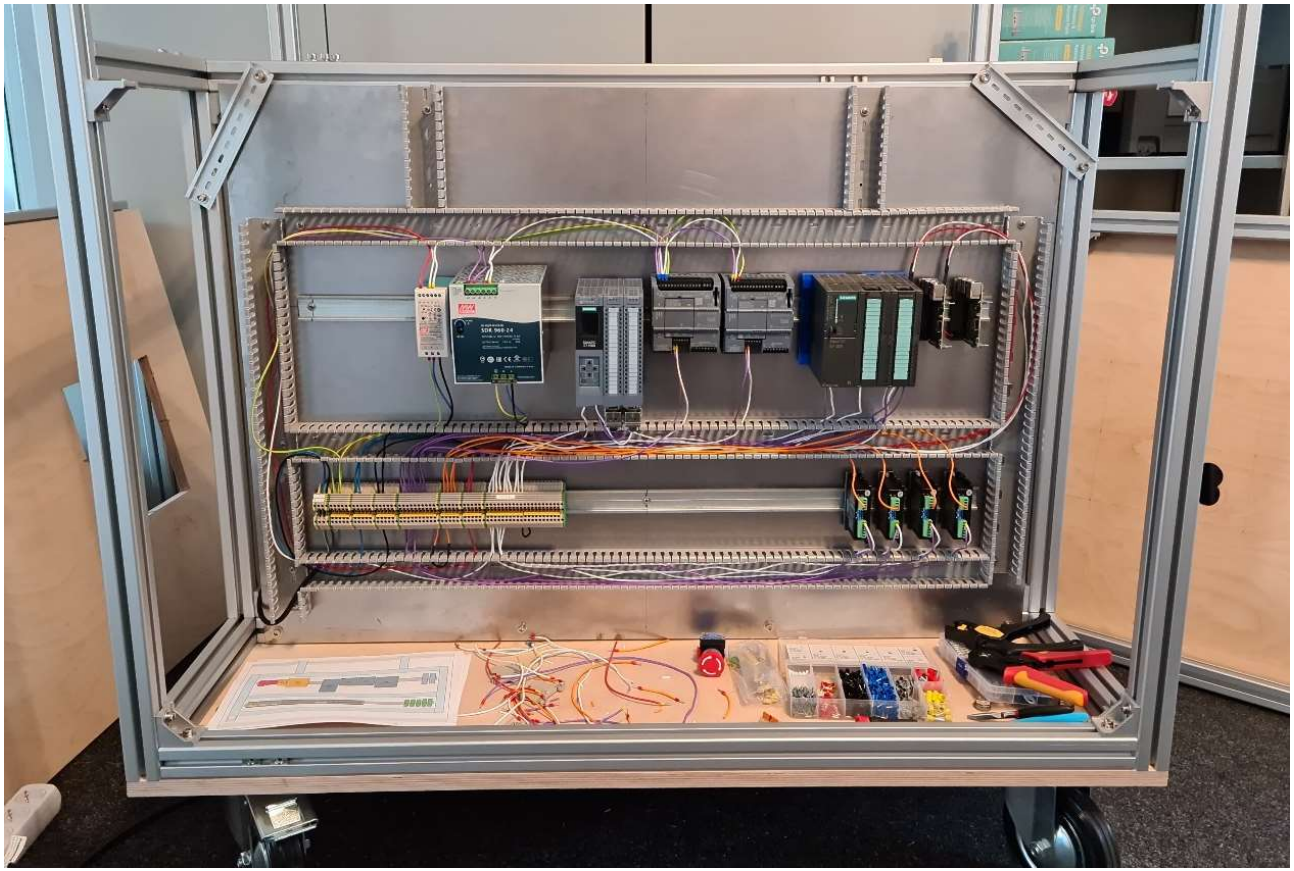


Putting it all Together

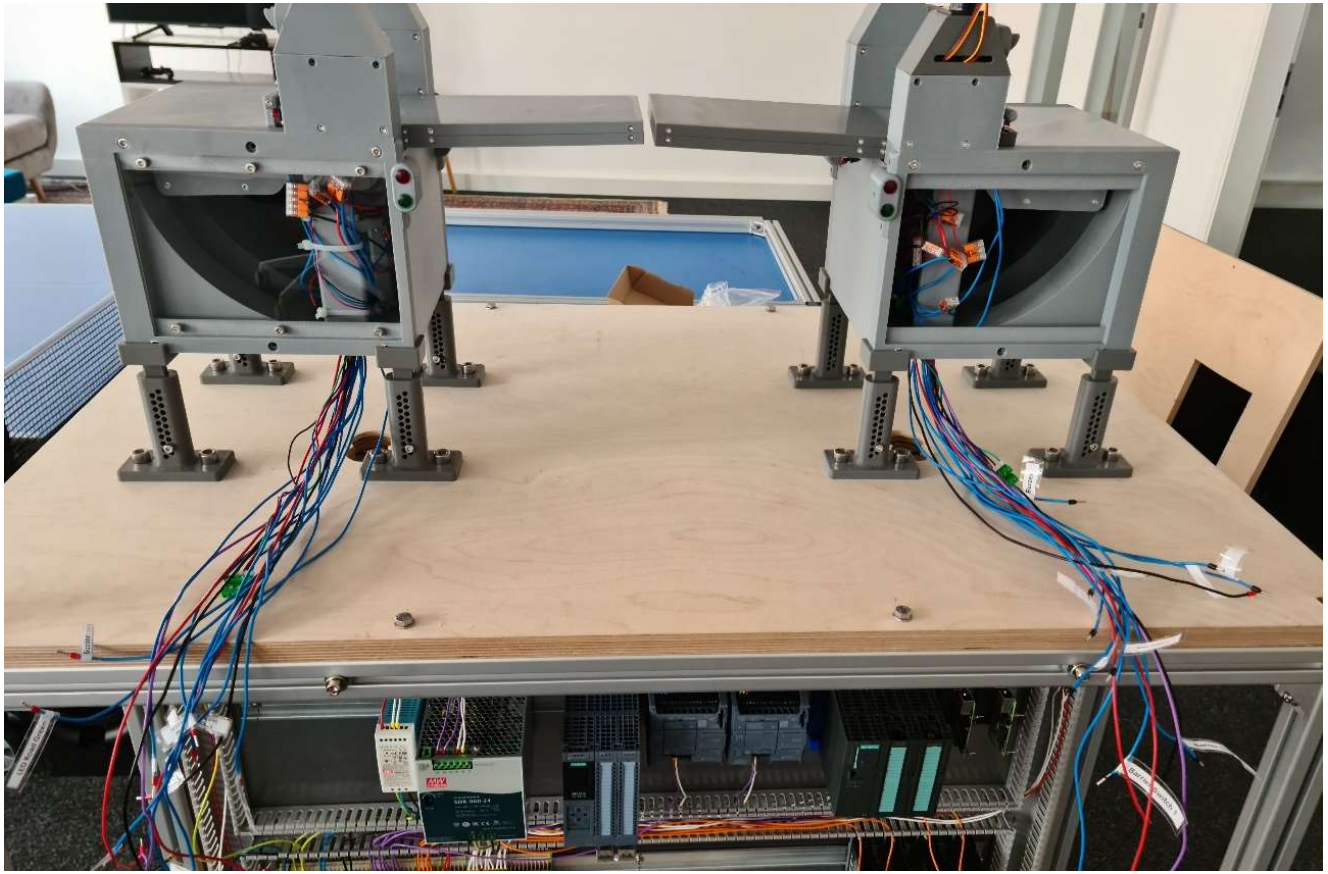


Putting it all Together

Putting it all Together

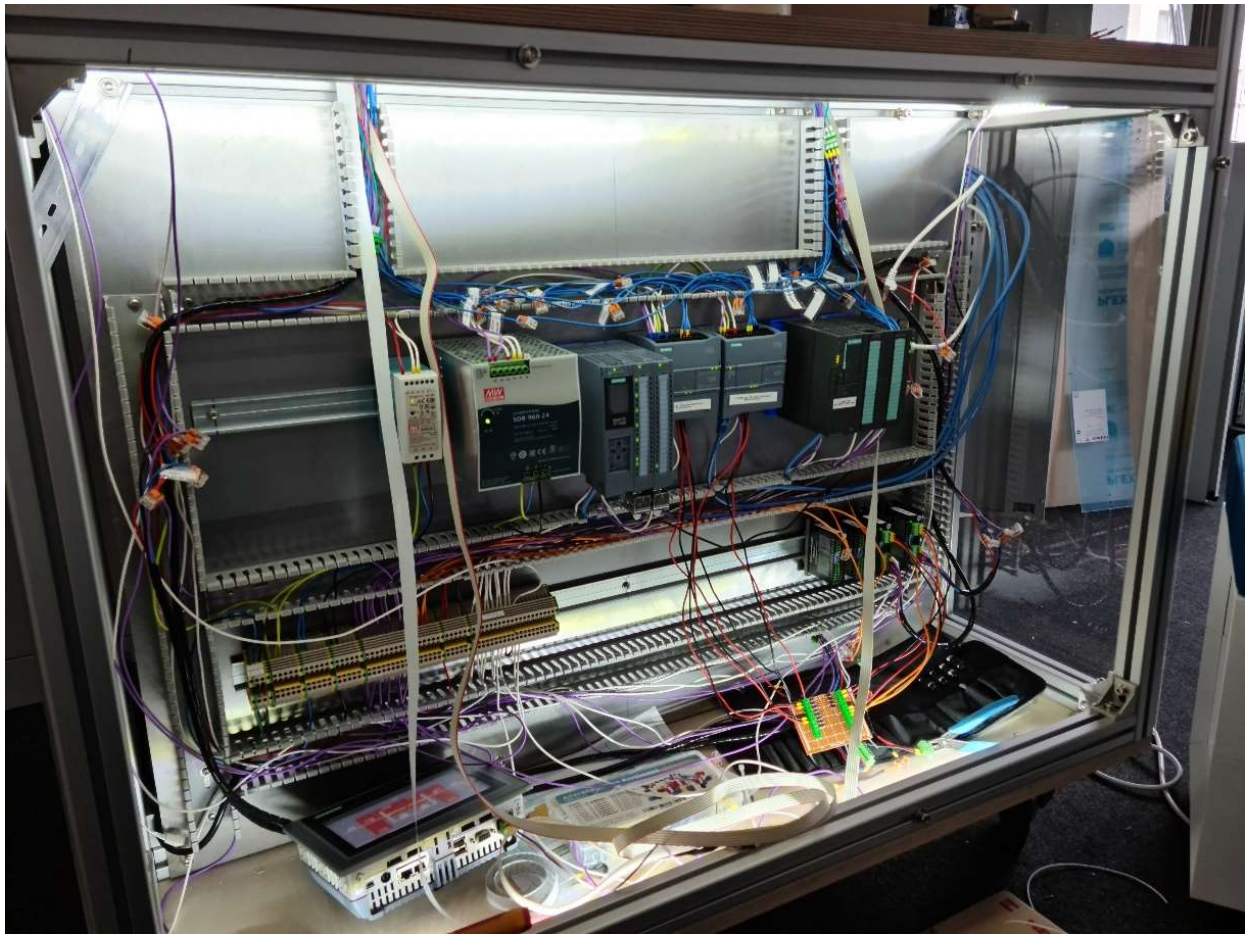


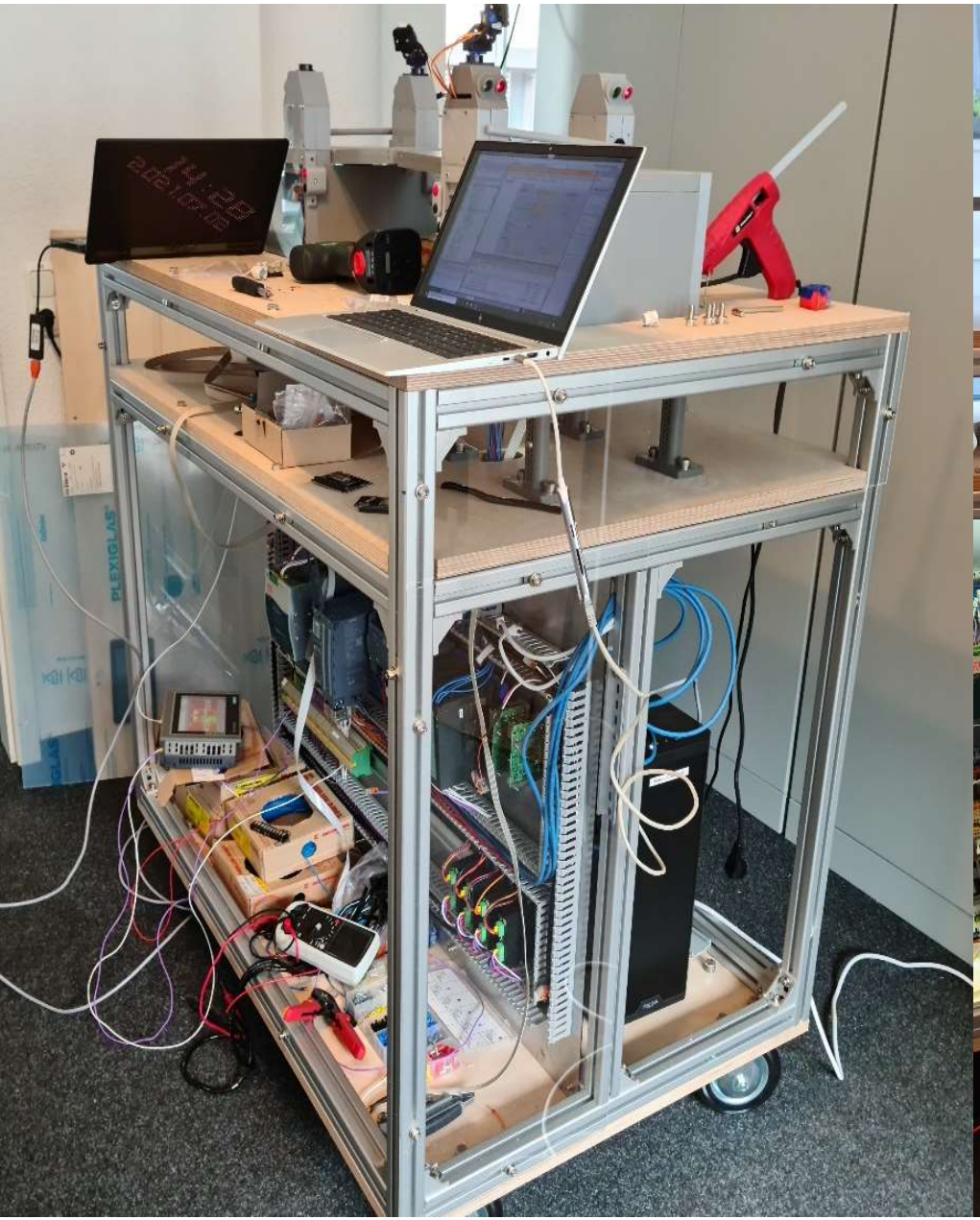
Putting it all Together



Putting it all Together

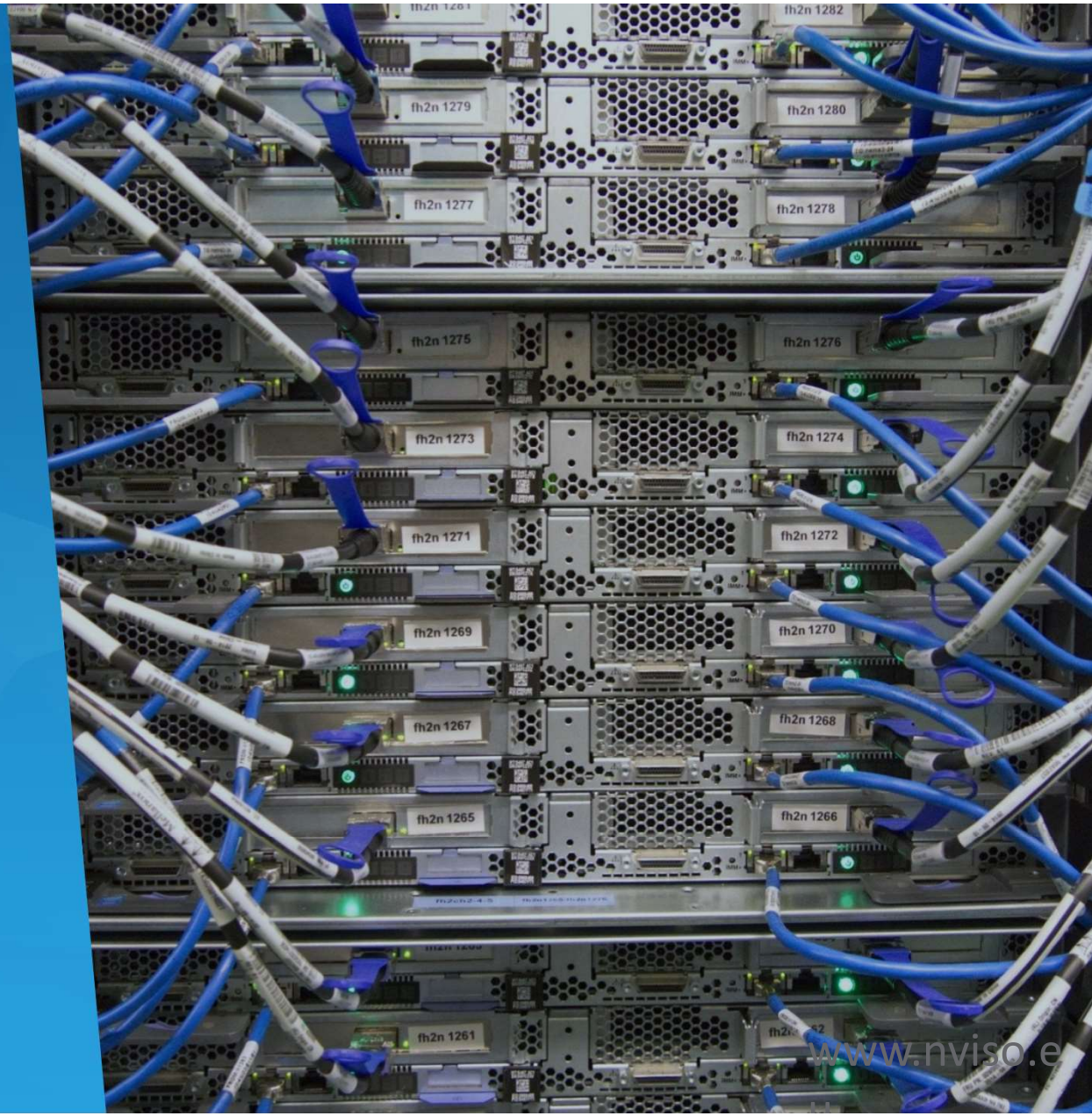
Putting it all Together



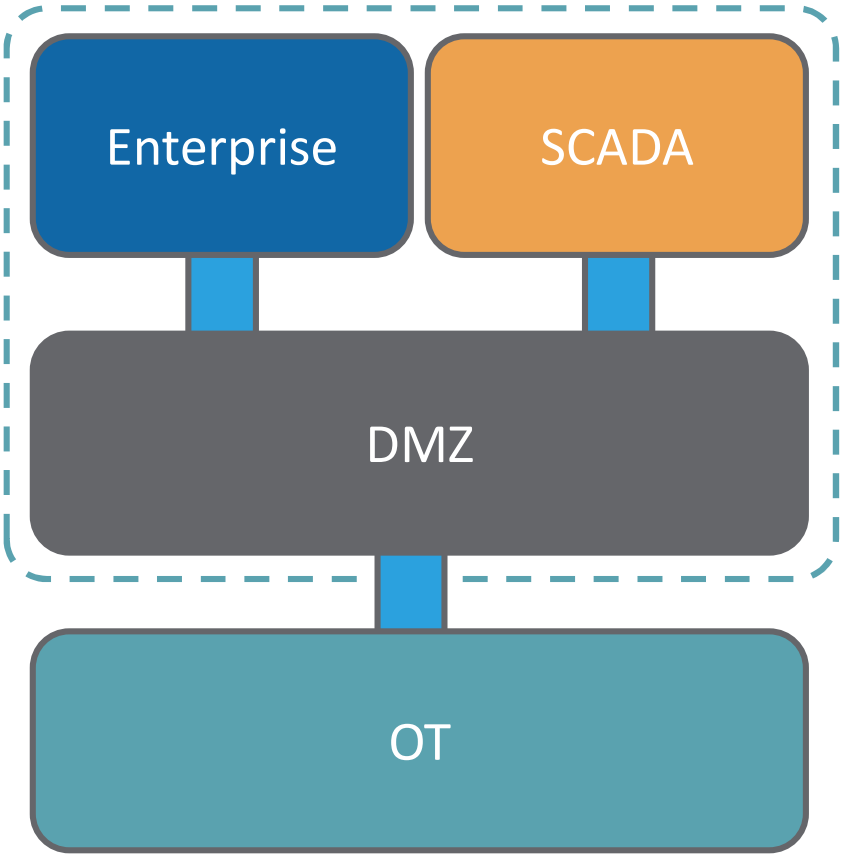

PLEXIGLAS

Network Infrastructure

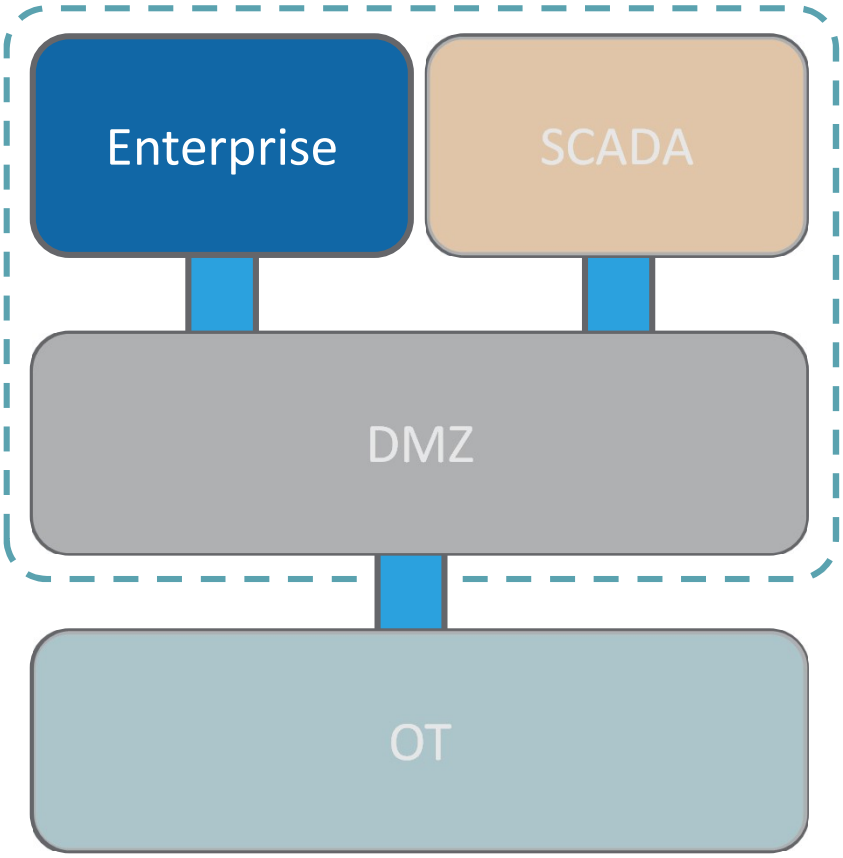
- Realistic environment
- Extensible

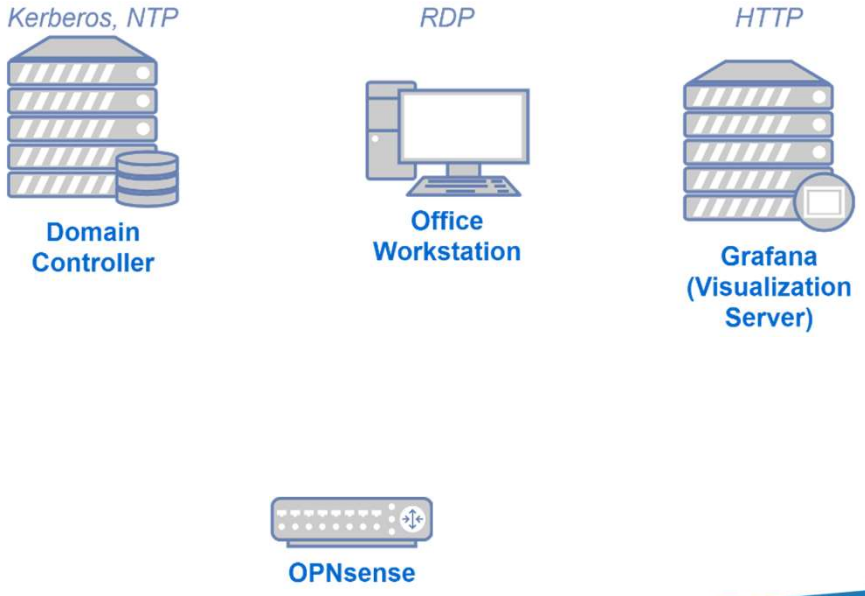


Network Infrastructure

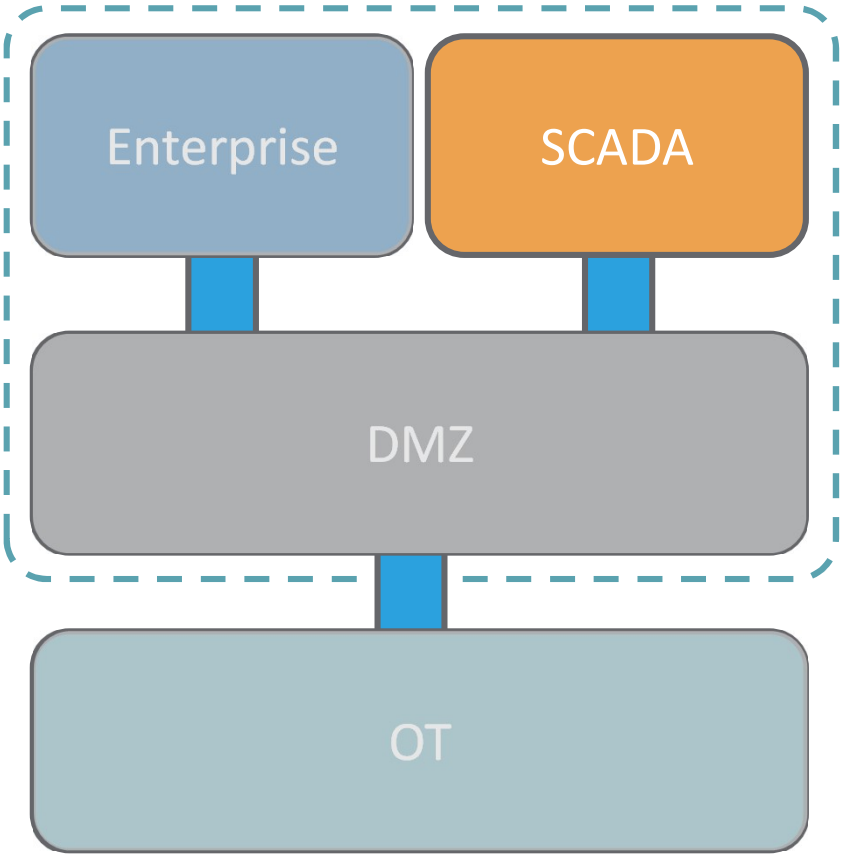


Network Infrastructure

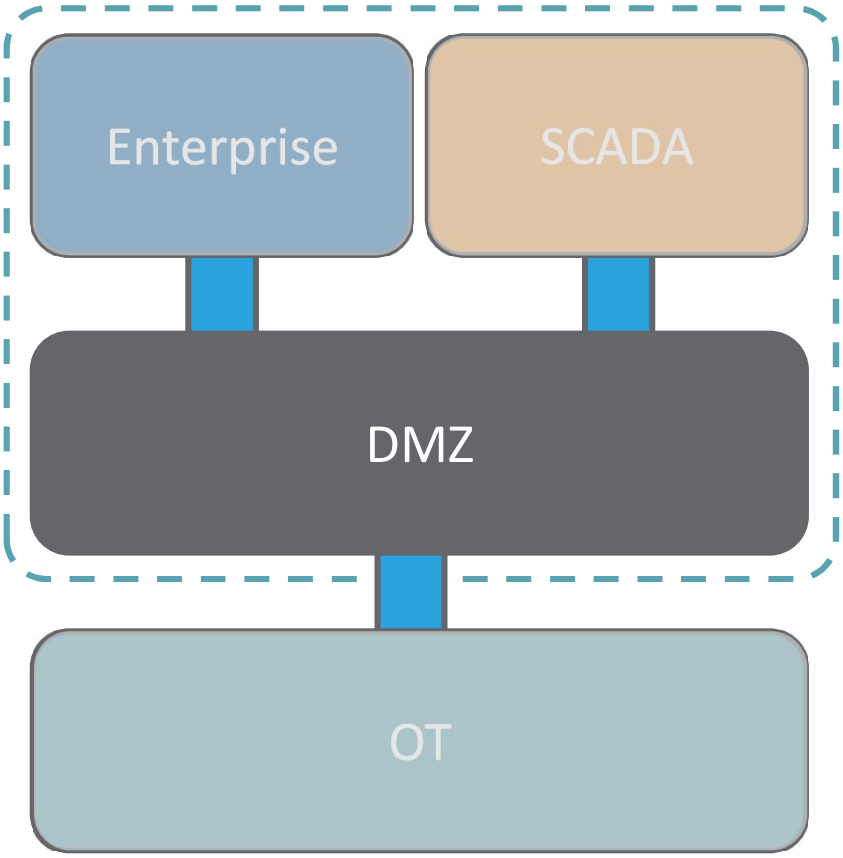




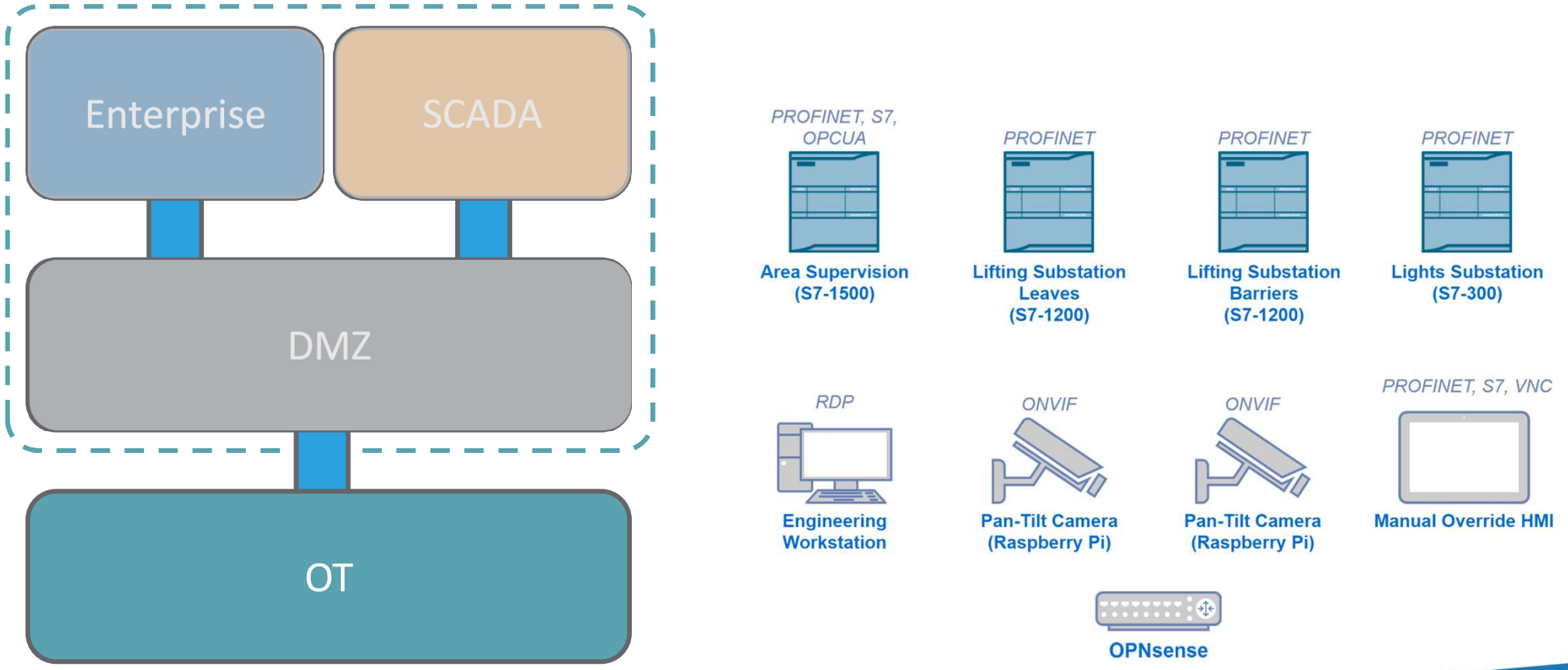
Network Infrastructure



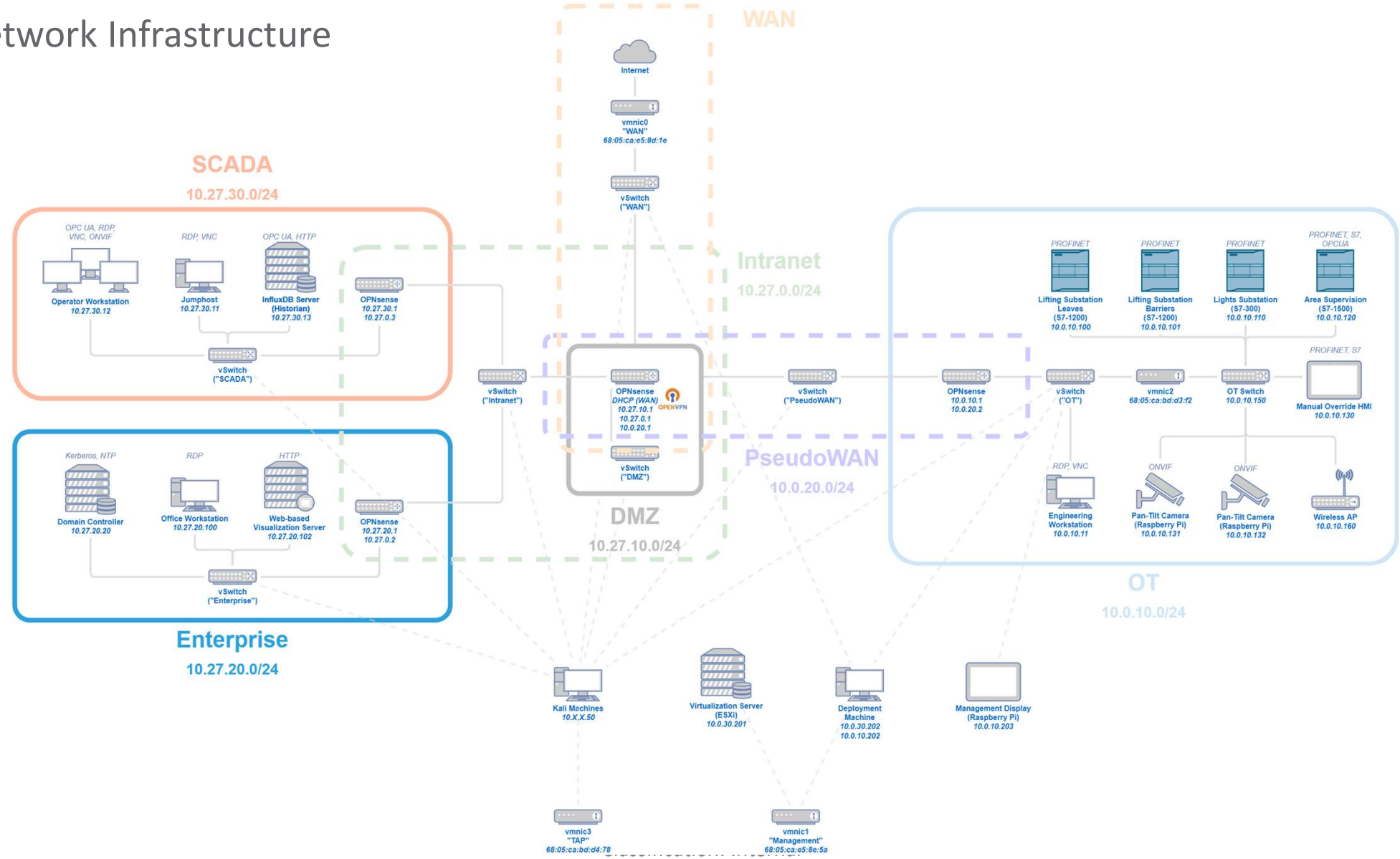
Network Infrastructure



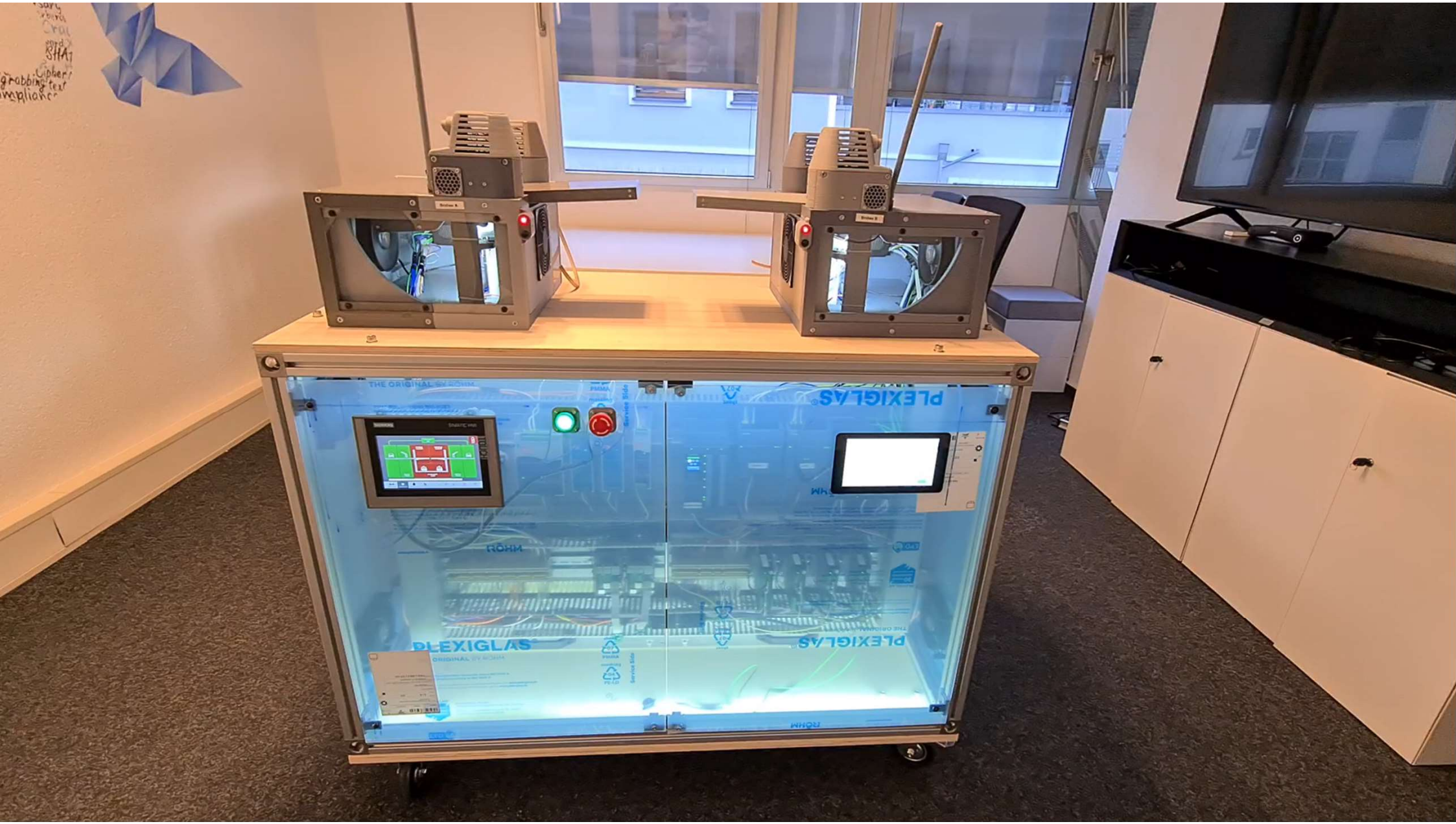
Network Infrastructure



Network Infrastructure



Demonstration


PLEXIGLAS
PLEXIGLAS
PLEXIGLAS
RÖHM

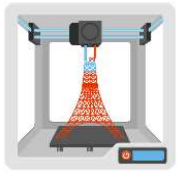
Lessons Learned

Challenges and Lessons Learned

ICS Lab Setup

- Complicated assembly
- Hardware dependencies & compatibilities
- Software Licenses are pricey
- Stepper motors overheating

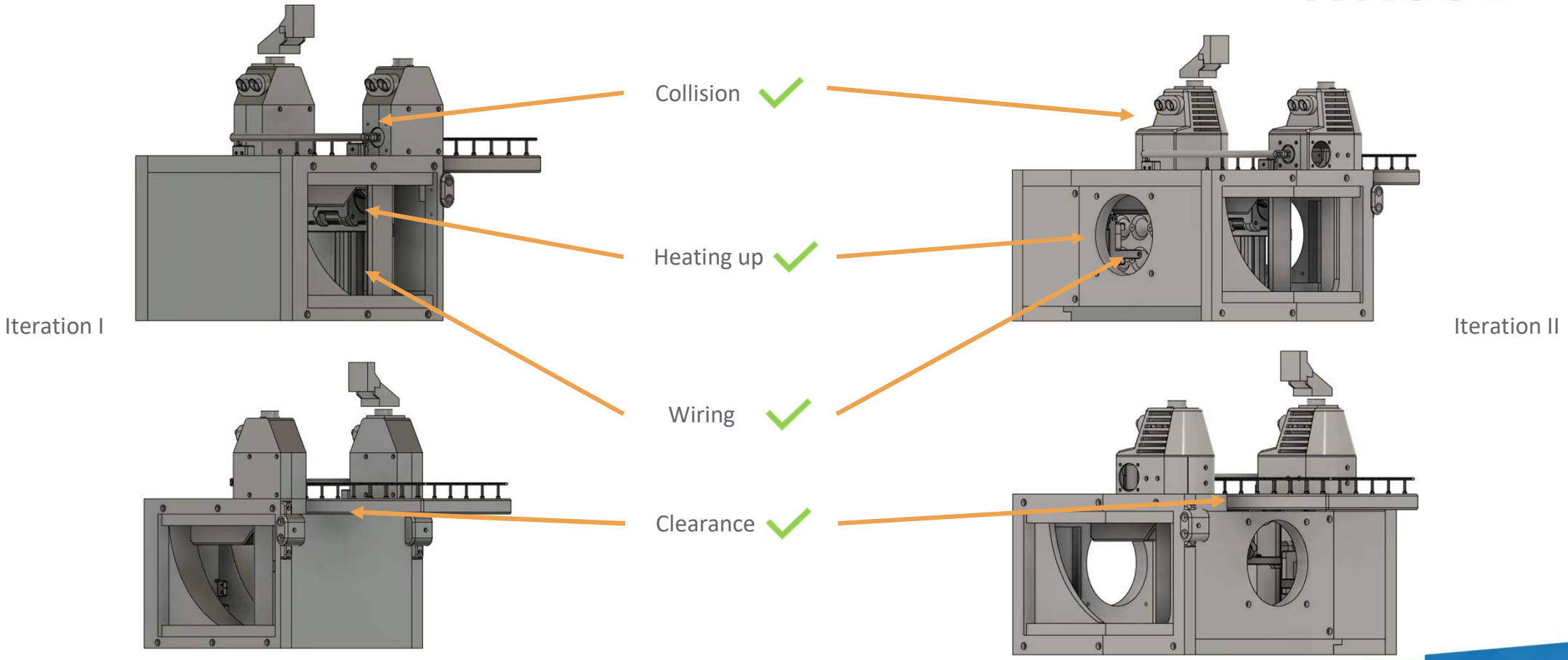
3D Printing



- Challenging mechanical design
- Printing is time consuming
- 3D printers are error-prone
- Learning CAD from scratch

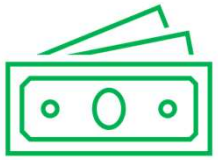
Practical Problems I

Practical Problems II



The Bottom Line

- Started in January 2021
- 1050 hours manual work
- 900 hours net 3D printing time
- 8kg filament used



- 3500 USD for licenses
- 14k USD for hardware
- 570 USD worth of coffee

- 2 stepper motors
- 1 PLC
- 1 motor driver
- Our sanity

The training

What did we cover?

IR & Forensics workshop focus points

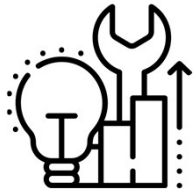
- Analysis methods & Reporting
- Network Forensics
- Classic Host-based Windows Forensics
- Memory Forensics
- Cobalt Strike beacon analysis
- ICS specifics
  - TIA Portal usage
  - TIA Portal host-based evidence
  - S7comm & S7comm+

What did it end with?

- 2 day workshop
- A slide deck of 404 pages covering background
- 11 hands-on exercises
- A workbook of 100+ pages describing the exercises
- 3.5 GB compressed archive of data for analysis
- A public 4 part blog post series on blog.nviso.eu

What‘s next?

What's next?



Room for improvements:

- Mobility could be better
- Modularization to replace model on top

Develop scenarios:

- Penetration Testing & Red Teaming
- OT monitoring and detection

More Information

Interested in this project or got any follow-up questions?

info@nviso.eu

Check out NVISO's contribution to ICS Security:

https://ics.nviso.eu

Series of blog posts, covering the ICS Firing Range and some excerpts from the training:

@NVISOsecurity and @NVISO_Labs

https://blog.nviso.eu

Thank You!

Questions?

www.nviso.eu