Building an ICS Firing Range (in our kitchen)

Sharing Our Journey & Lessons Learned

May 2022
Bsides Munich

About Us

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

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) in 2018!

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

Table of content

Firing Ranges and OT

What is a Firing Range?

- Controlled, interactive environment
- Abstraction of real environment
- As realistic as possible

Why a Firing Range?

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

Training

Security Assessments

Awareness

Visual Impact

Testing

Patch Management
Security Testing

Development

Detection and Forensic Readiness

What are OT and ICS?

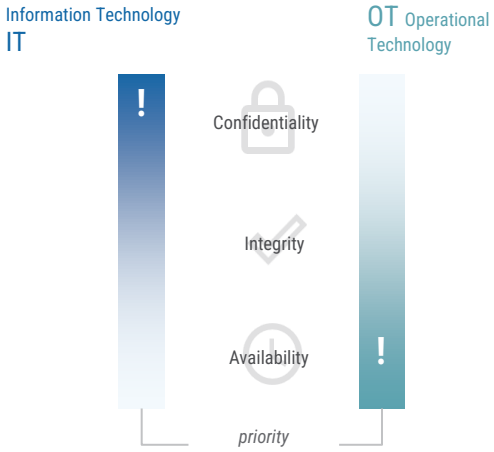
Operational **T**echnology

Computing systems that are used to manage industrial operations (e.g. manufacturing)

Industrial **C**ontrol **S**ystems

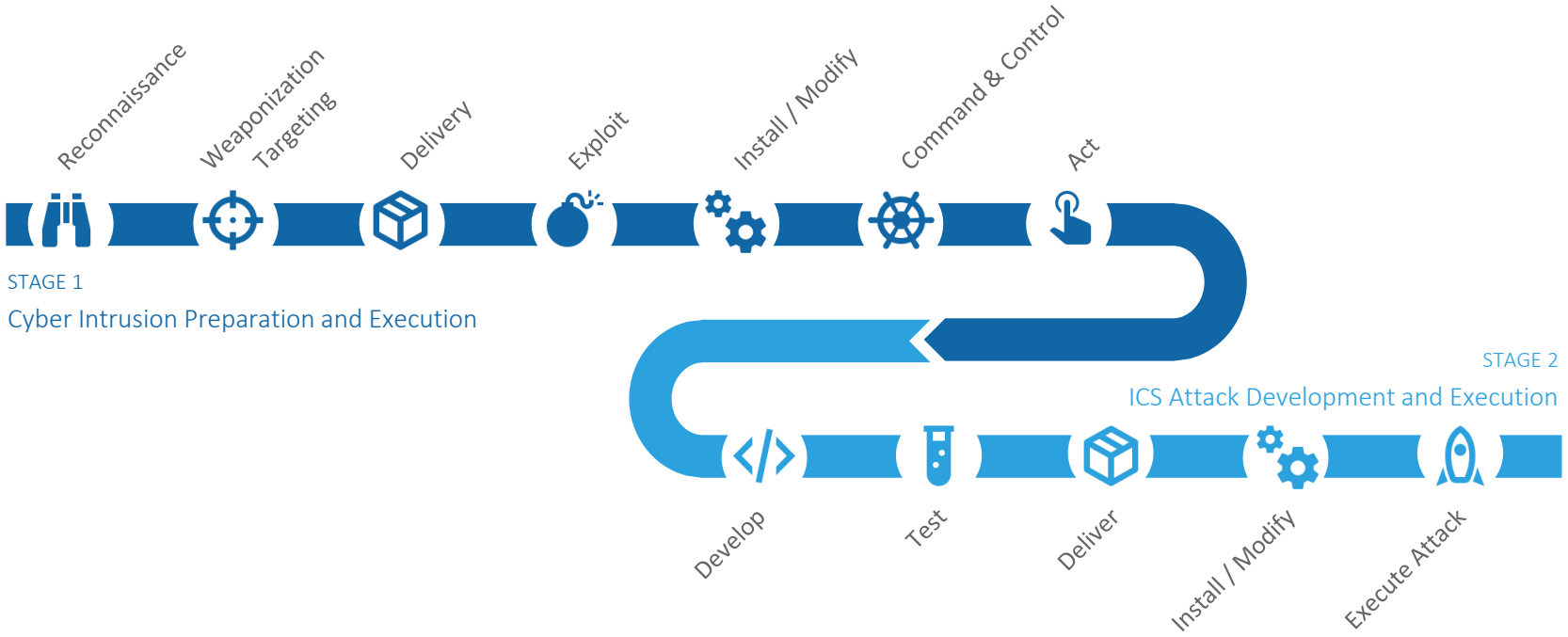
The integration of hardware and software components to control processes for automation or instrumentalization.

OT vs IT


Information Technology
IT
OT Operational Technology
!
Confidentiality
Integrity
Availability
!
priority

Attacks against ICS

SANS ICS Cyber Kill Chain



Attacks against ICS

Attacker Objectives Based on SANS ICS Kill Chain

LOSS

view
control

DENIAL

view
control
safety

MANIPULATION

view
control
sensors and instruments
safety

The impact on ICS by reaching these objectives can be severe, e.g. failure of safety systems can harm human life.

Jun

2017

TRISIS/Triton

Triton is the world's most murderous malware […]

The rogue code can disable safety systems designed to prevent catastrophic industrial accidents.

MIT Technology Review article

Building an ICS firing range of a bridge

(in our kitchen)

How it all started…

Requirements

- IT and OT have **different security requirements**
- Security assessment approaches are different
- OT specific awareness and skills

Motivation

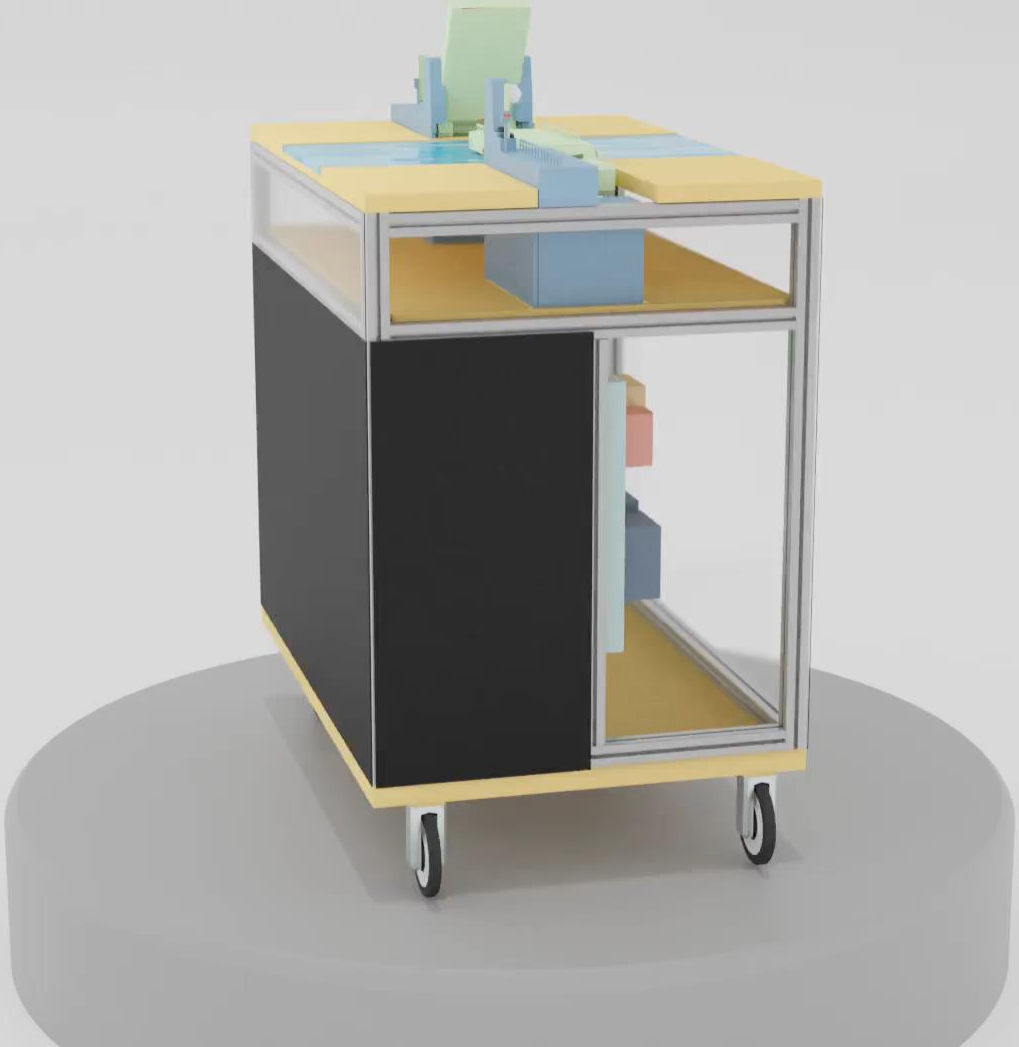
- Have a training ground for **internal training** of offense and defense
- Research & Development
- Provide an environment for **testing of isolated OT components**

Concept

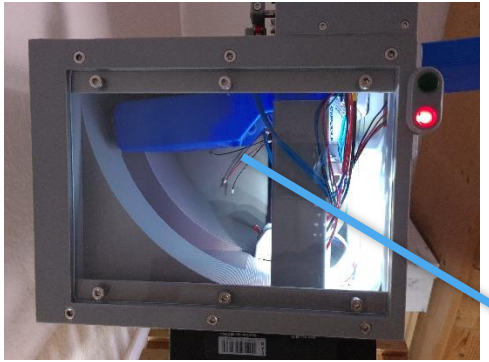
- Model of a **Water Treatment Plant** comprised of
  - Three stage water filtration system
  - Pumping stations
  - Virtualized IT network infrastructure

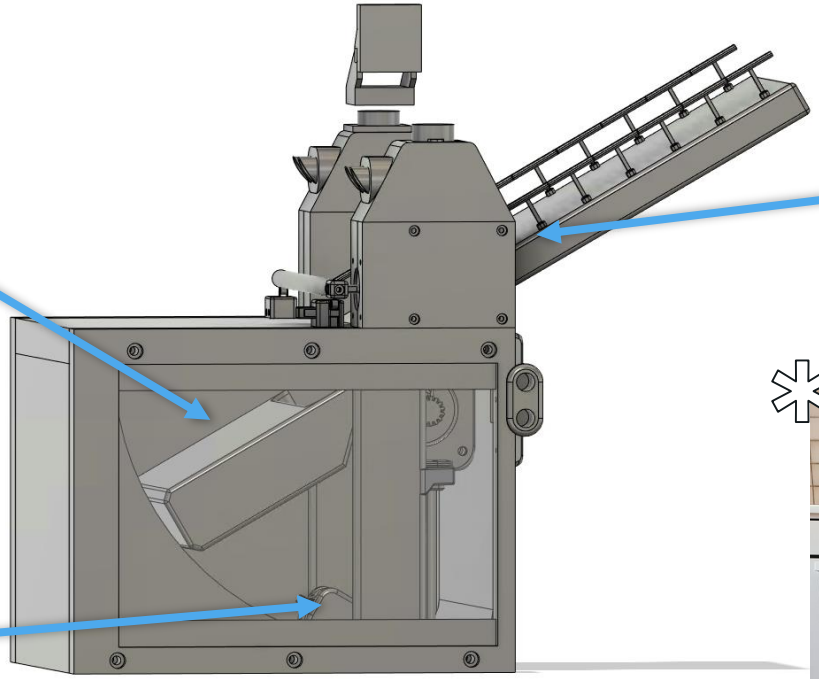
Requirements

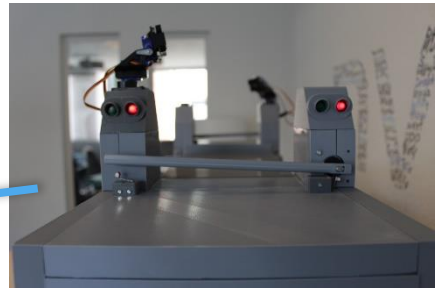
- Mobile solution
- Scenario-based training for DFIR teams

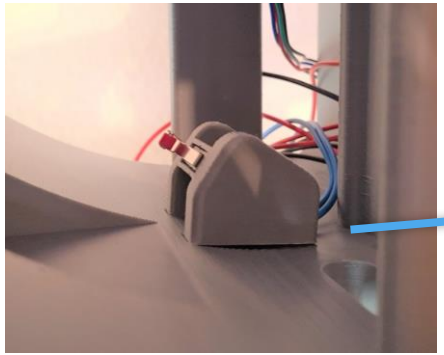


3D Printed Model





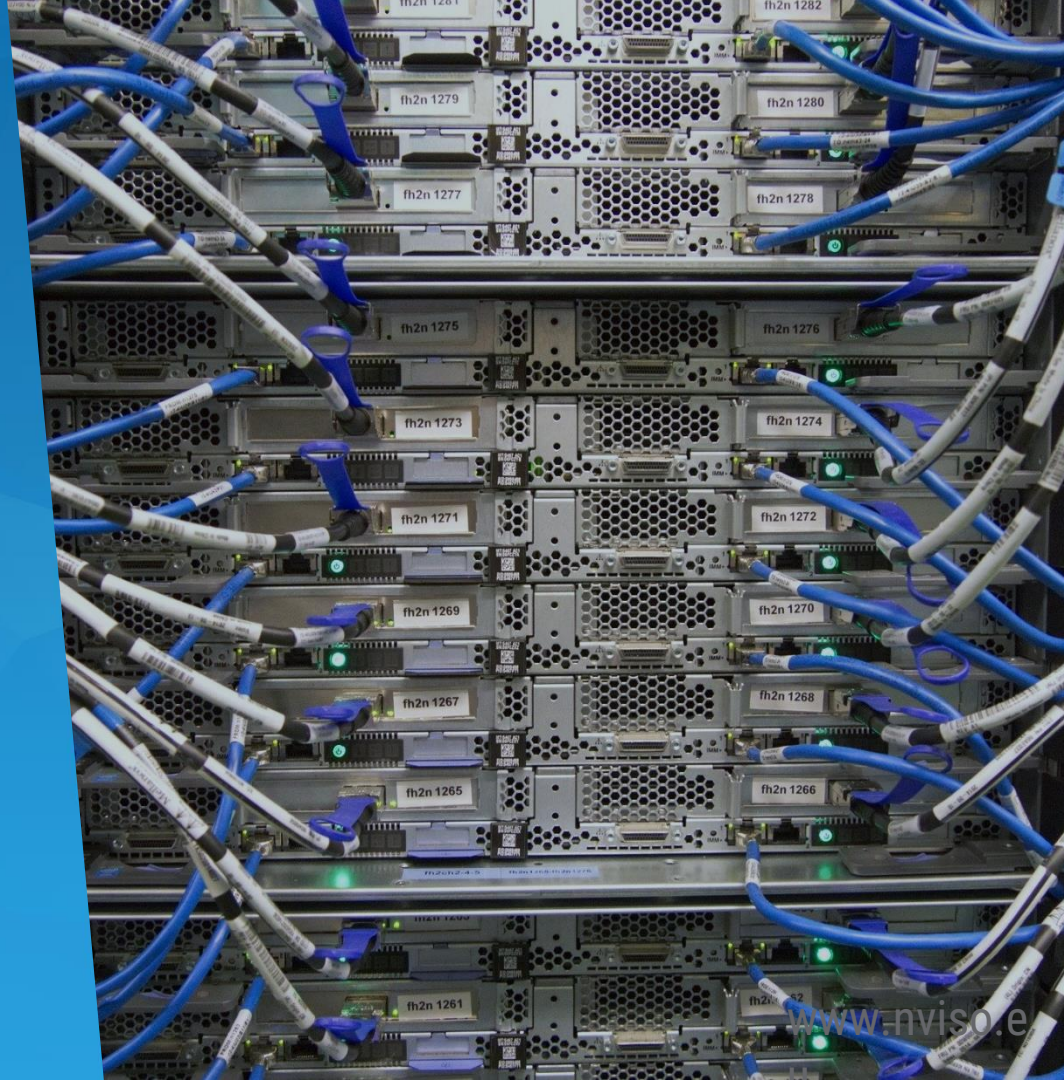




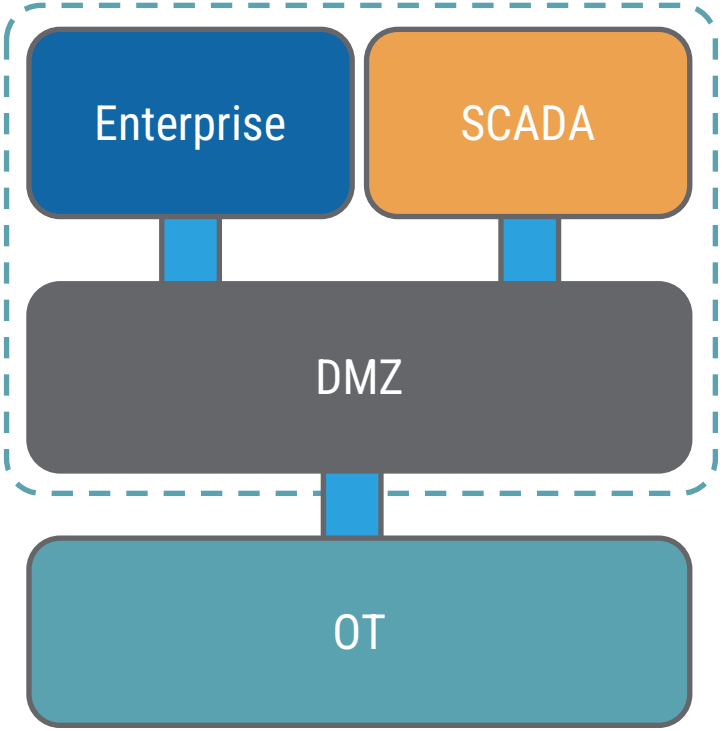
Putting it all Together

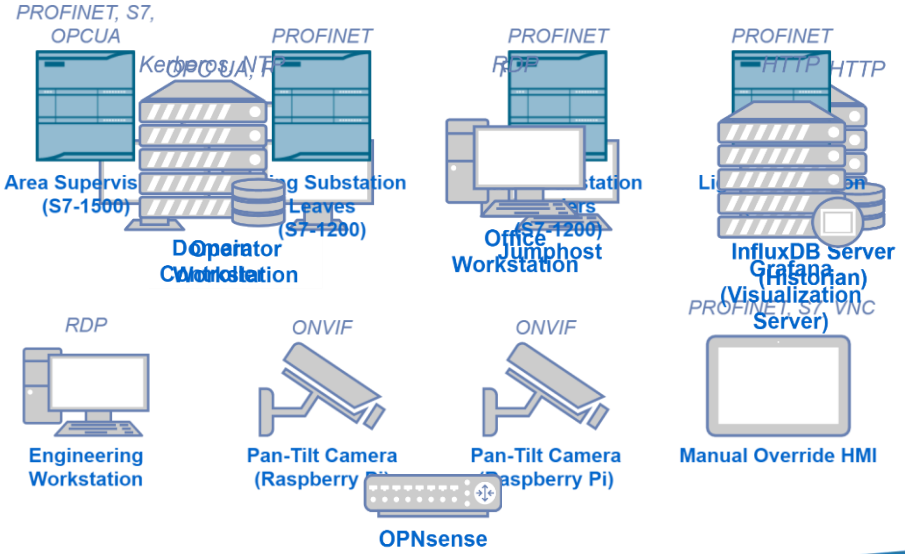
Network Infrastructure

- Realistic environment
- Extensible

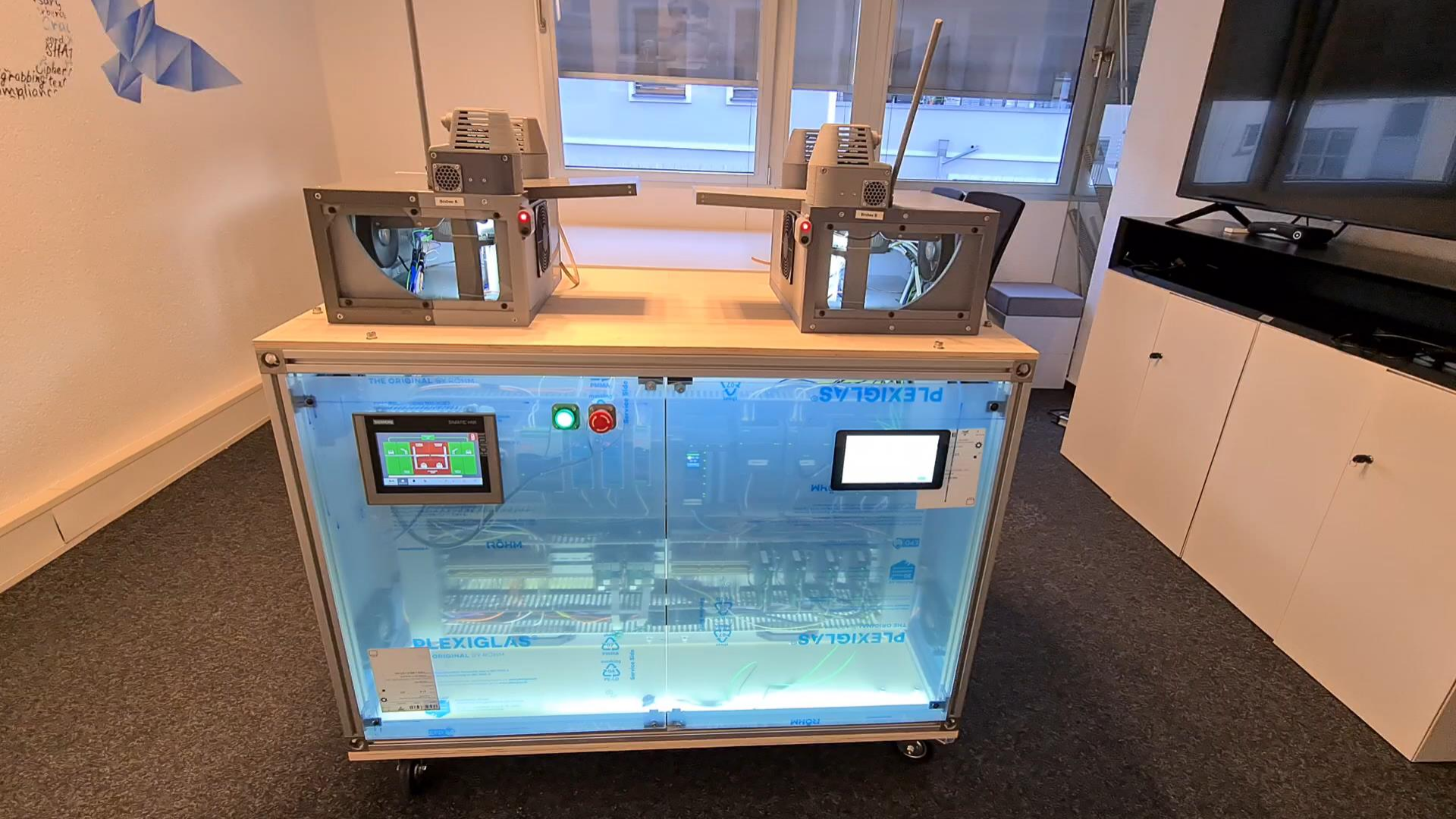


Network Infrastructure





Demonstration


PLEXIGLAS
PLEXIGLAS
PLEXIGLAS
ROHM

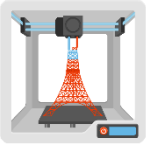
Lessons Learned

Challenges and Lessons Learned

ICS Lab Setup

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

3D Printing

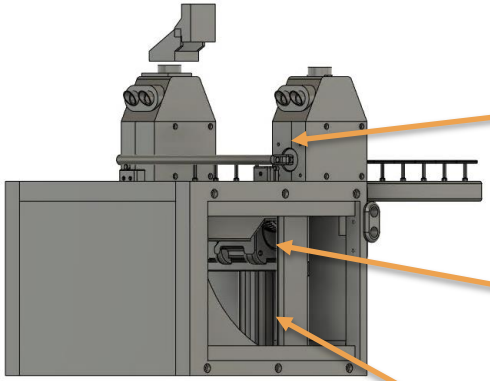


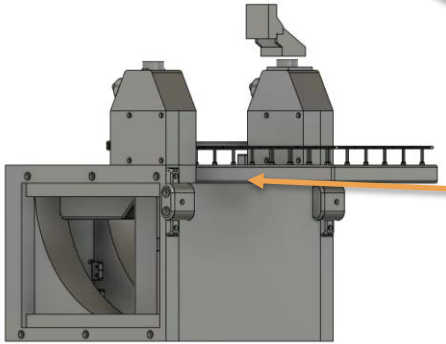
- Challenging mechanical design
- Printing is time consuming
- 3D printers are error-prone
- Learning CAD from scratch

Practical Problems I

Practical Problems II

Iteration I





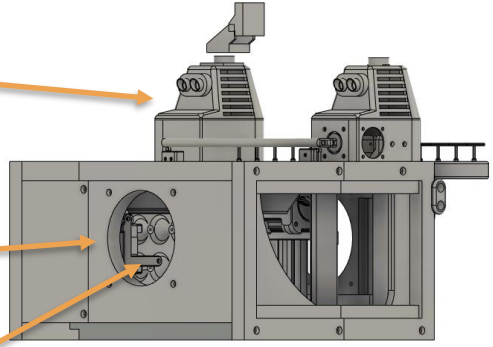
Collision ✓

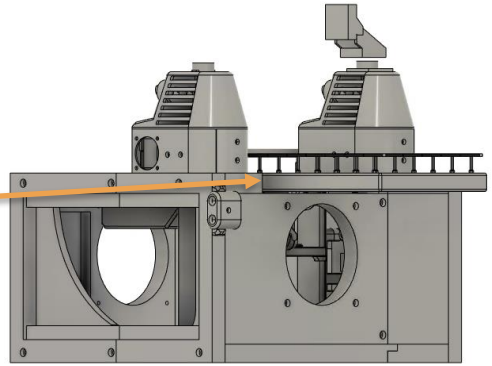
Heating up ✓

Wiring ✓

Clearance ✓

Iteration 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

What‘s next?

What's next?

Room for improvements:
- Mobility could be better
- Modularization to replace model on top

Develop further workshops and training scenarios for
- Penetration Testing & Red Teaming
- OT monitoring and detection

Interested in OT or this project?

More Information

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

nleidecker@nviso.eu

mthomas@nviso.eu

Check out NVISO's contribution to ICS Security:

https://ics.nviso.eu

Series of blog posts coming up, covering the ICS Firing Range in more detail:

@NVISOsecurity and @NVISO_Labs

https://blog.nviso.eu

Thank You!

Questions?

www.nviso.eu