T.I.S.P./T.P.S.S.E. Community Meeting 2024

Berlin, 05. – 06.11.2024

OT, oh no – Wie Hacker Ihre Produkte zerstören

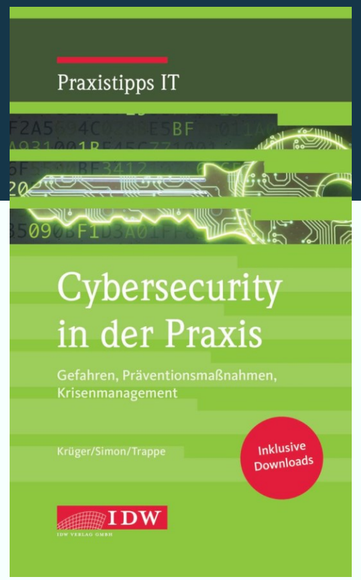
Andreas Krüger, Laokoon Security

06. November 2024

OT, oh no!

Wie Hacker Ihre Produktion zerstören

whoami



Andreas Krüger

- Senior Pentester, Red Team Lead
- Founder & CEO of Laokoon Security
- Author
- M.Sc. Computer Science (Hardware + Security)
- Former Captain (army / CIDS „Cyber Force“)

Laokoon Security

Email

Andreas.Krueger@laokoon-security.com

LinkedIn

Giving AI a Shot

SI

What is OT (Operational Technology)

Operational Technology (OT) refers to the hardware and software systems that are used to control and monitor physical devices, processes, and events in industries such as manufacturing, energy, utilities, and transportation. Unlike Information Technology (IT), which focuses on the management and processing of data, communication, and business operations, OT is primarily concerned with the direct control of physical systems.

CPS (Cyber Physical Systems)

OT Overview

SCADA

LTE / VPN

VPN

LTE / VPN

MODBUS/TCP

PLC

Cloud

- metrics
- remote management

production site

PROFIBUS

RIO

HMI

sensor

actuator

OT Overview

SCADA

LTE / VPN

VPN

LTE / VPN

MODBUS/TCP

PLC

Cloud

- metrics
- remote management

PROFIBUS

RIO

HMI

sensor

actuator

„Little“ Server:

- Unix/Linux OS
- Local Web Frontend (Device Managment)
- Several (very old) network services
  - SSH
  - FTP
  - Telnet

OT Overview

Common Problems
- No/weak authentication
- No/weak encryption
- Default configuration
- Missing updates
- „legacy IT-Problems“
- Depends on IT-Services
- Self-implemented /re-invented
- ...

Cloud
- metrics
- remote management

SCADA

VPN

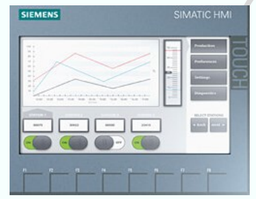
LTE / VPN

LTE / VPN

MODBUS/TCP

PLC

PROFIBUS



HMI

RIO

sensor

actuator

„Little“ Server:
- Unix/Linux OS
- Local Web Frontend (Device Managment)
- Several (very old) network services
  - SSH
  - FTP
  - Telnet

OT Overview

Common Problems
- No/weak authentication
- No/weak encryption
- Default configuration
- Missing updates
- „legacy IT-Problems“
- Depends on IT-Services
- Self-implemented /re-invented
- ...

Cloud
- metrics
- remote management

SCADA

VPN

LTE / VPN

LTE / VPN

MODBUS/TCP

HMI

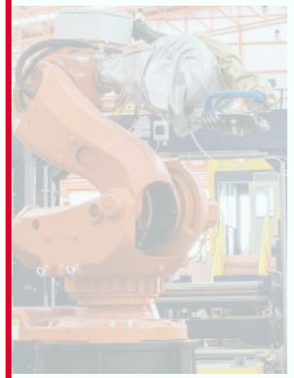
„Little“ Server:
- Unix/Linux OS
- Local Web Frontend (Device Managment)
- Several (very old) network services
  - SSH
  - FTP
  - Telnet

INTERVIEW PRODUKTIONSAUSFALL

IT-Panne bei VW: „Die Folgen sind nicht fatal, aber extrem teuer“

Nach einer IT-Panne ging nichts mehr bei Volkswagen: Die Produktion ruhte in der Nacht

© Moritz Frankenberg/dpa / Picture Alliance



actuator

OT, you mean S7?

SIEMENS

OT, you mean S7?

BELDEN

Honeywell

EMERSON

ABB

HIRSCHMANN
A BELDEN BRAND

SIEMENS

PHOENIX CONTACT

WAGO

Schneider Electric

Rockwell Automation

Primary Research Findings

Primary findings include:

Critical Infrastructure faces rising risks

Critical Infrastructure vertical industries appear in the top five most targeted industries, with several more in the top 10.

Intensely focused on energy

Attacks are most intensely focused on energy sectors – 3X more than the next most frequently attacked vertical.

Aiming to disrupt

Most attacks on OT/ICS systems aim to disrupt operations using a variety of tools and techniques, from phishing to ransomware to lateral tool transfer and exploitation of remote services.

Attackers gaining access to IT networks

Attackers are gaining access to IT networks first in most OT incidents.

Nation-state sponsored

Many attacks were found to be nation-state sponsored, indirectly enabled by internal personnel about one-third of the time.

Phishing

Phishing is the most popular attack technique.

Anatomy of 100+ Cybersecurity Incidents in Industrial Operations; Rockwell Automation; 2022

Primary Research Findings

Primary findings include:

Critical Infrastructure faces rising risks

Critical Infrastructure vertical industries appear in the top five most targeted industries, with several more in the top 10.

Intensely focused on energy

Attacks are most intensely focused on energy sectors – 3X more than the next most frequently attacked vertical.

Aiming to disrupt

Most attacks on OT/ICS systems aim to disrupt operations using a variety of tools and techniques, from phishing to ransomware to lateral tool transfer and exploitation of remote services.

Attackers gaining access to IT networks

Attackers are gaining access to IT networks first in most OT incidents.

Nation-state sponsored

Many attacks were found to be nation-state sponsored, indirectly enabled by internal personnel about one-third of the time.

Phishing

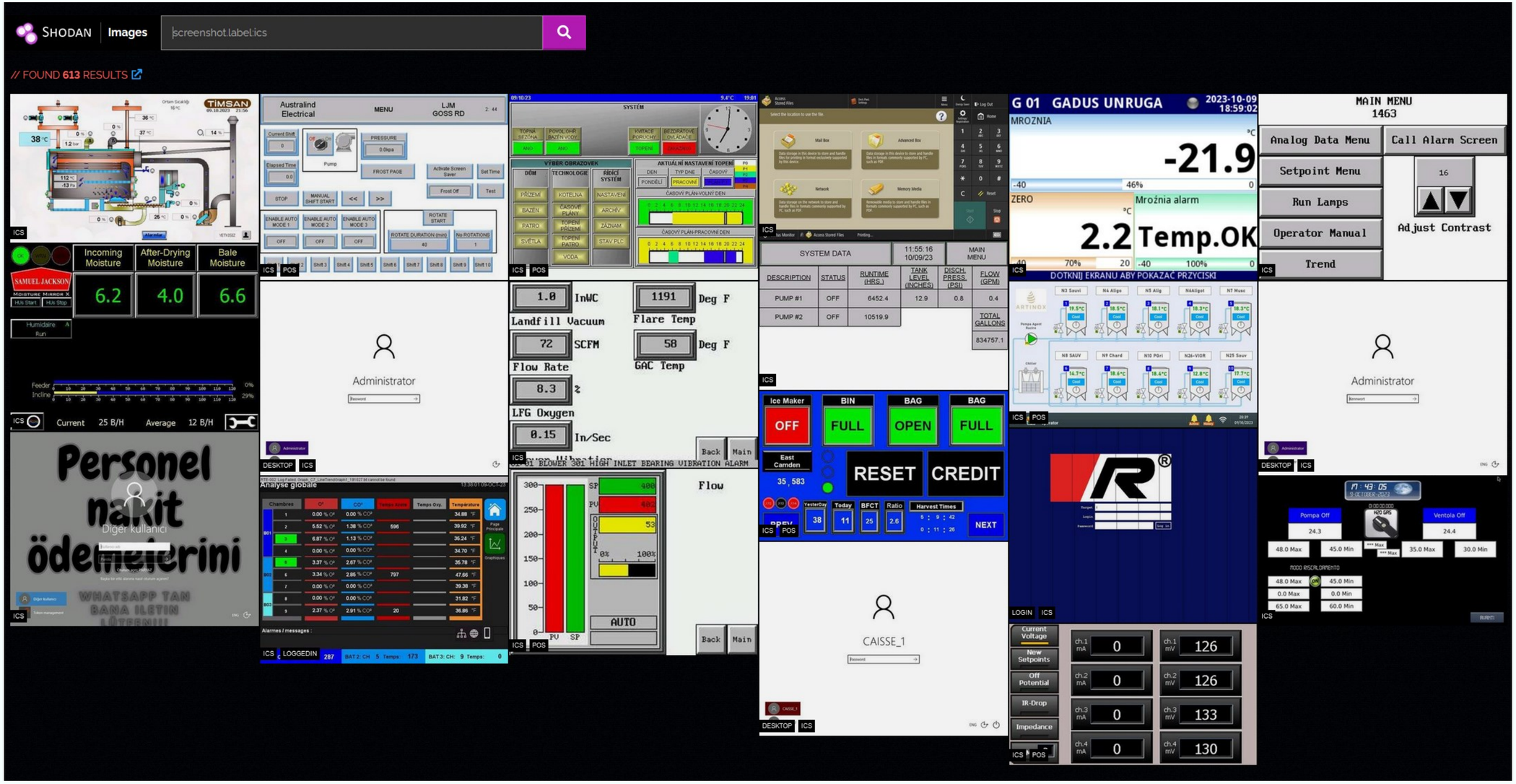
Phishing is the most popular attack technique.

Anatomy of 100+ Cybersecurity Incidents in Industrial Operations; Rockwell Automation; 2022

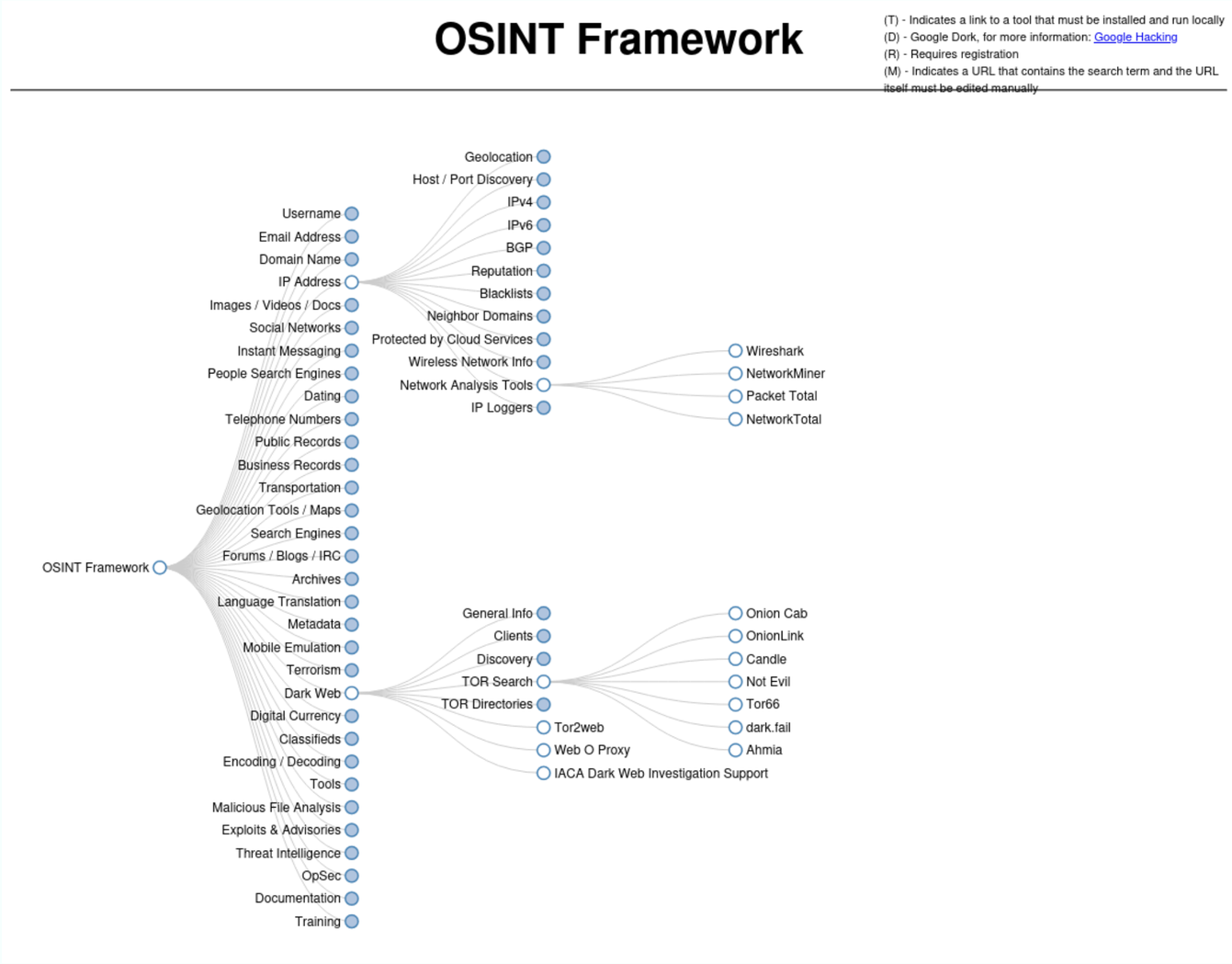
06. November 2024

Attacking OT

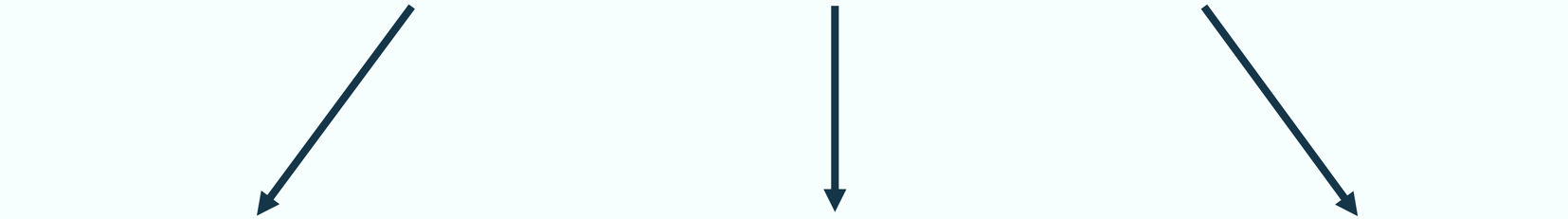
Reconnaissance



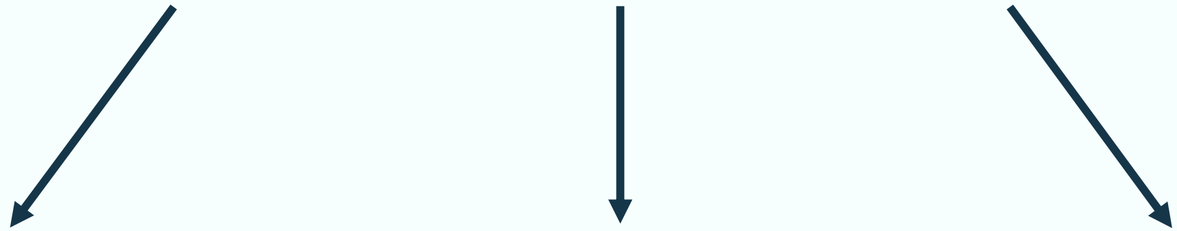
Reconnaissance



How to approach OT Systems?



How to approach OT Systems?



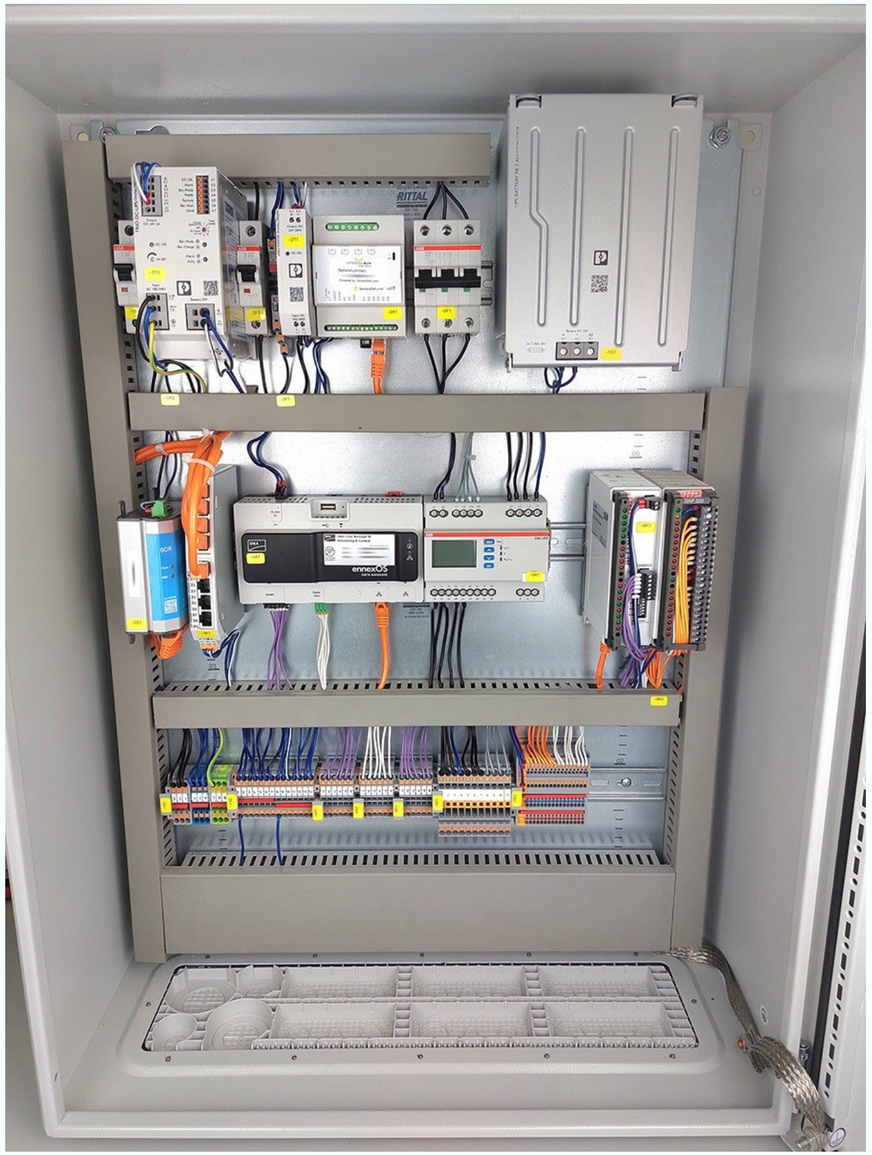
Physical Access

Virtual Access

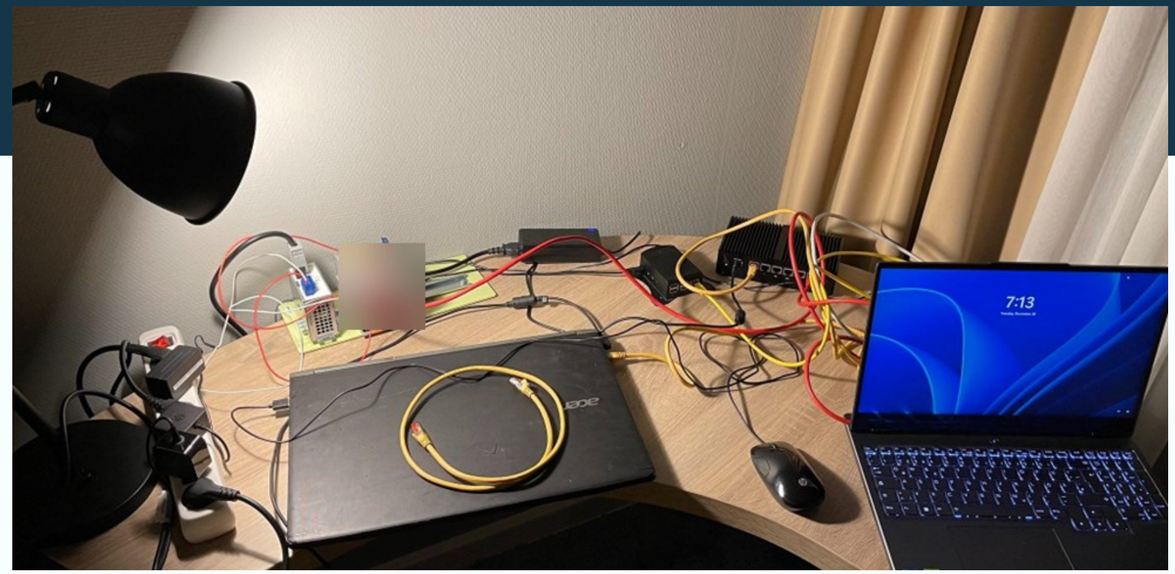
Cloud Access

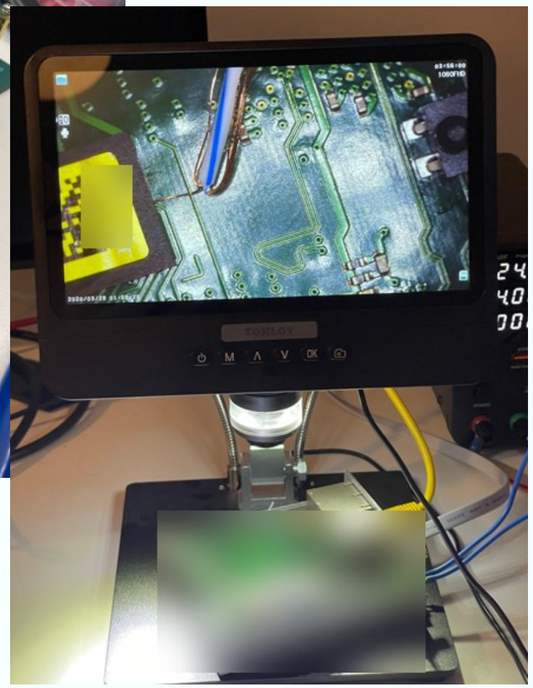
Physical Access

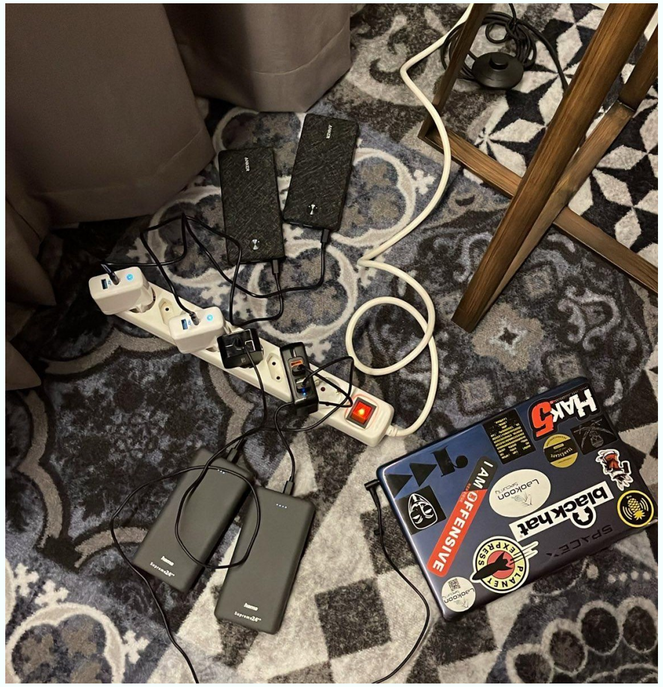
Physical Access



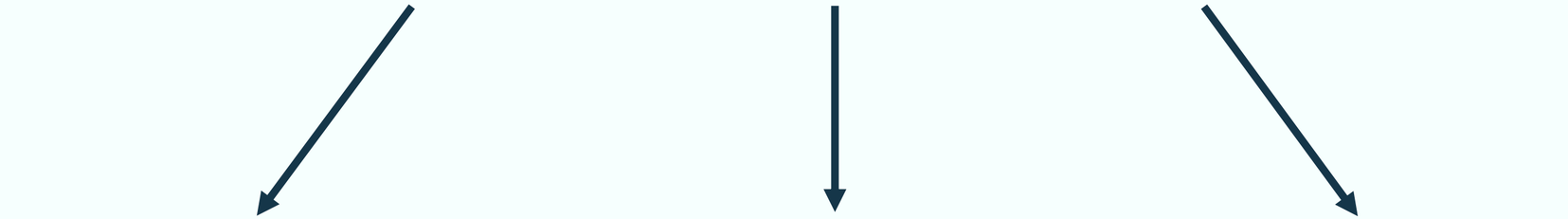
Physical Access







How to approach OT Systems?



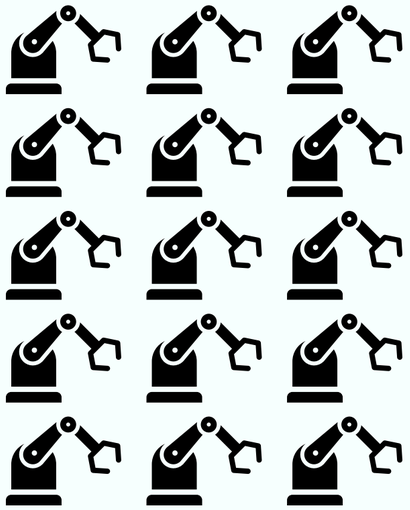
Physical Access

Virtual Access (Network)

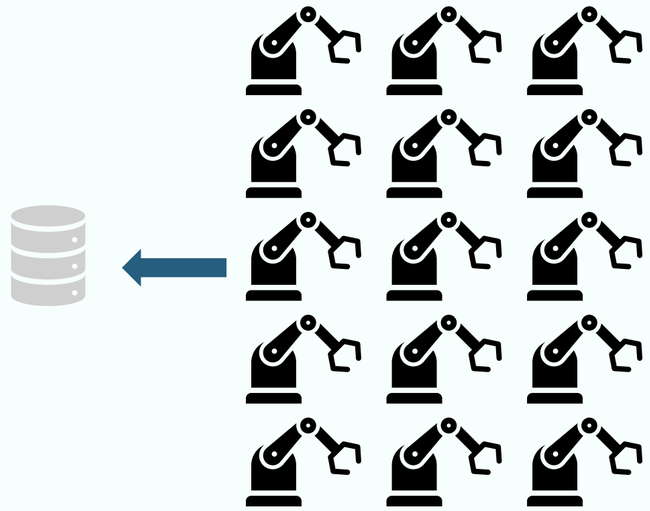
Cloud Access

Virtual Access

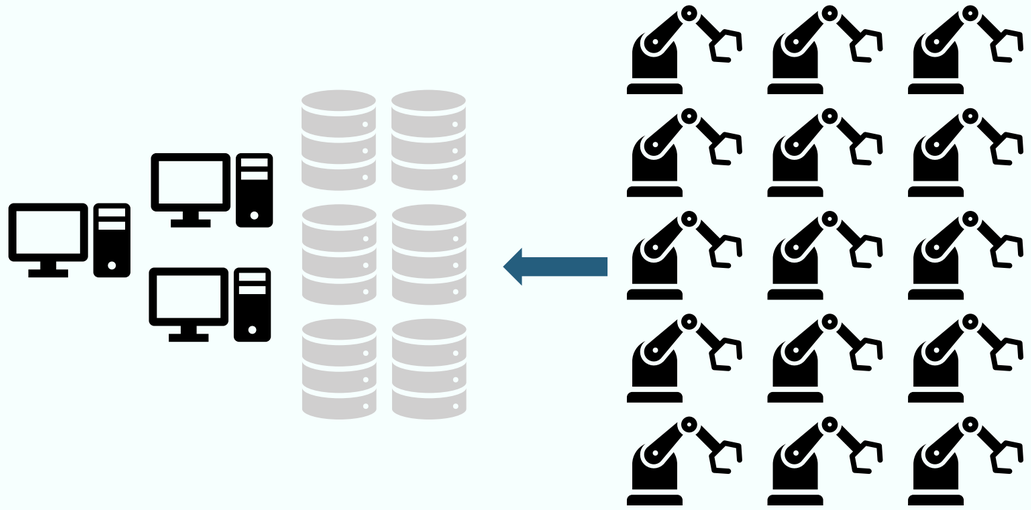
Virtual Access



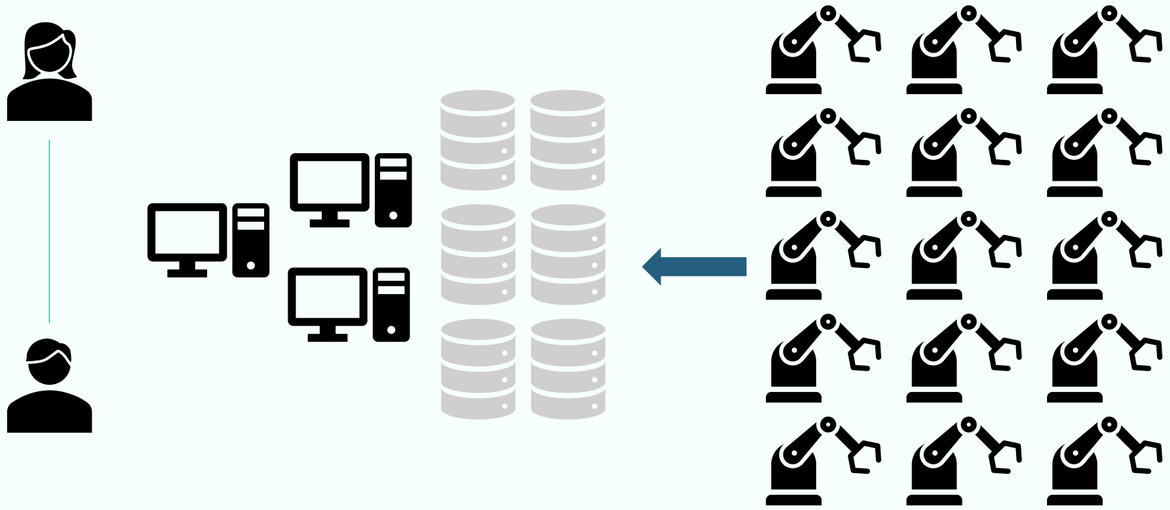
Virtual Access



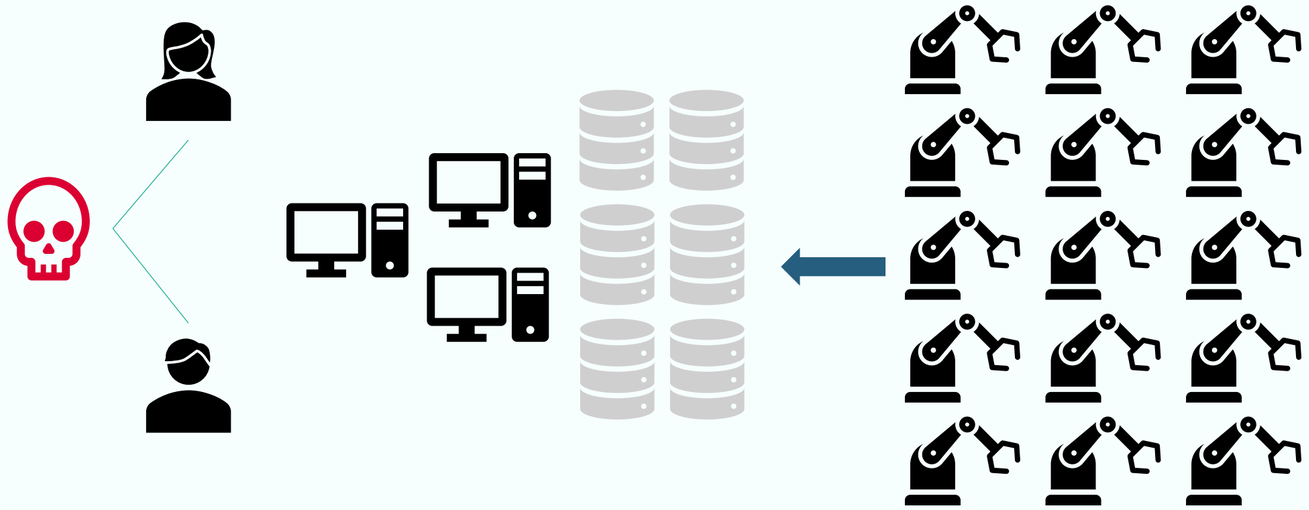
Virtual Access



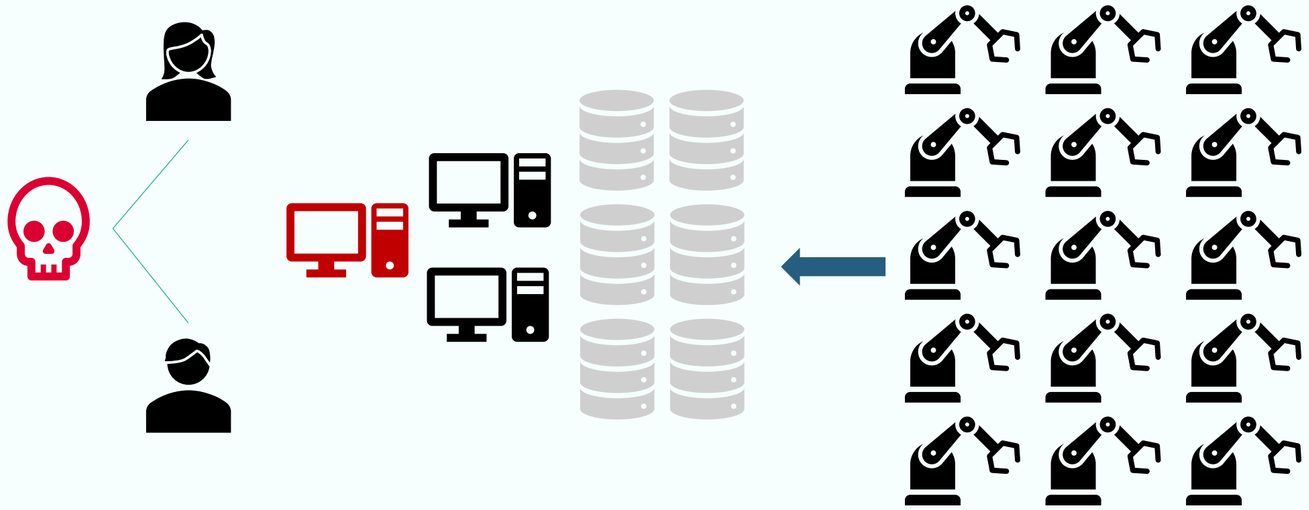
Virtual Access



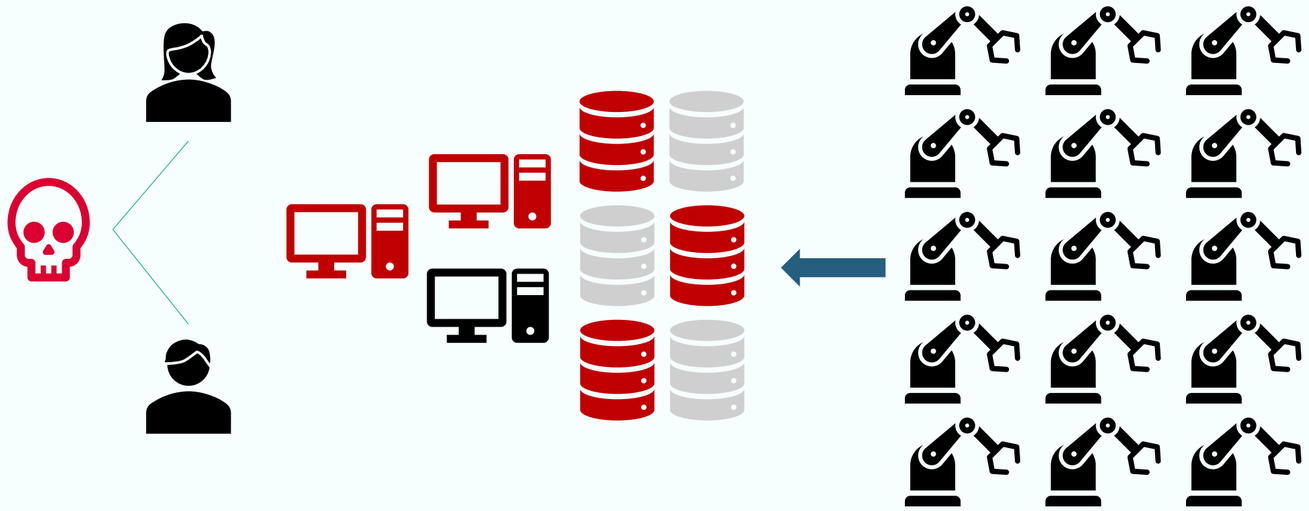
Virtual Access



Virtual Access

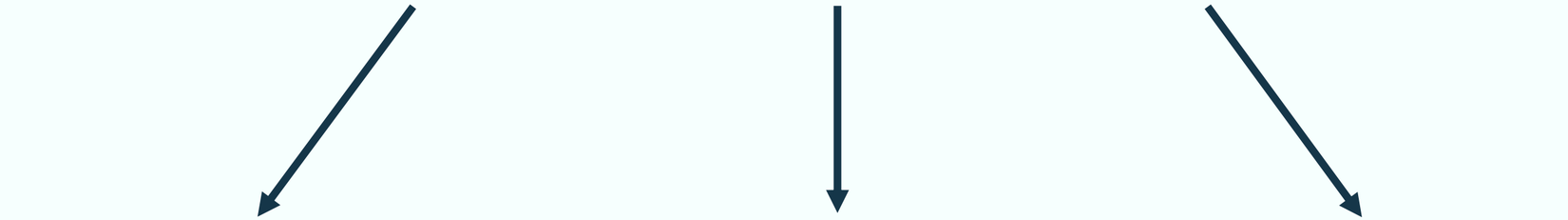


Virtual Access

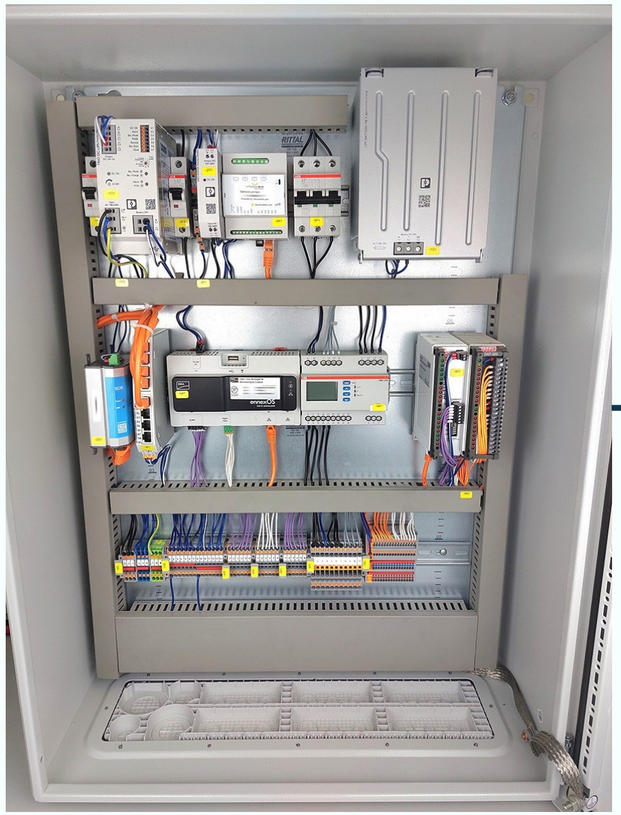


Virtual Access

How to approach OT Systems?

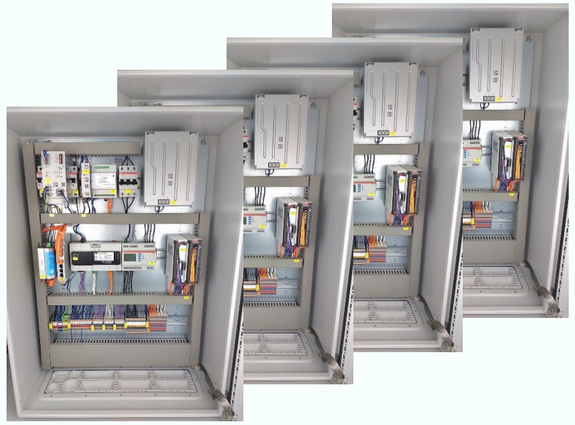


Cloud Access



Cloud

- metrics
- remote management



Cloud Access

```
root@                  /data/conf# ls -la
total 68
-rw-r--r-- 1 root root     0 Mar 27 14:15 '"<src>'
drwxr-xr-x 2 root root  4096 Mar 27 14:15  .
drwxr-xr-x 6 root root  4096 Mar 27 13:06  ..
[redacted]
-rw-r--r-- 1 root root     0 Mar 27 11:52  test.evil
```

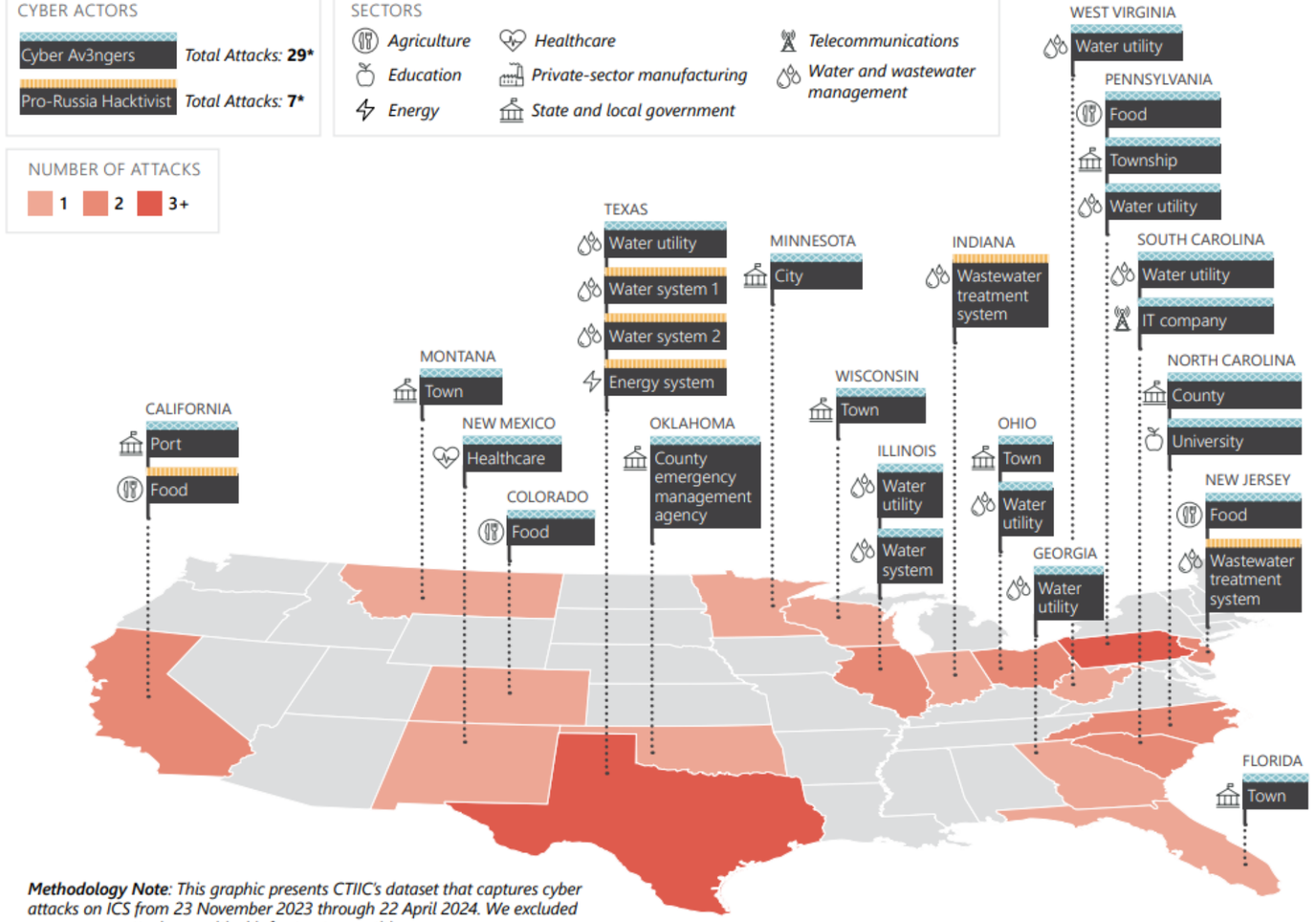
		300	Edit
		Warn	Edit
		TT . MM . JJJJ , -- : --	Edit
OtauTimeoutBetweenMessagesInstallationMode	Float	0.2	Edit
OtauTimeoutBetweenMessagesRunningMode	Float	1.5	Edit
[redacted]			Edit
[redacted]			Edit
" class="form-control" disabled/>	File	" href="data:application/octet-stream;base64,null" > Download	Edit
[redacted]			Edit
[redacted]			Edit
[redacted]			Edit
test.evil	File	Download	Edit

+ Add

06. November 2024

Recent OT Attacks

REPORTED CYBER ATTACKS ON US ICS, 23 NOVEMBER 2023 THROUGH 22 APRIL 2024



***Methodology Note**: This graphic presents CTIIC's dataset that captures cyber attacks on ICS from 23 November 2023 through 22 April 2024. We excluded ransomware attacks on critical infrastructure entities.*

*Including seven attacks at additional US locations.

Recent Cyber Attacks on US Infrastructure Underscore Vulnerability of Critical US Systems, November 2023–April 2024 (dni.gov)

USA is Popular Target

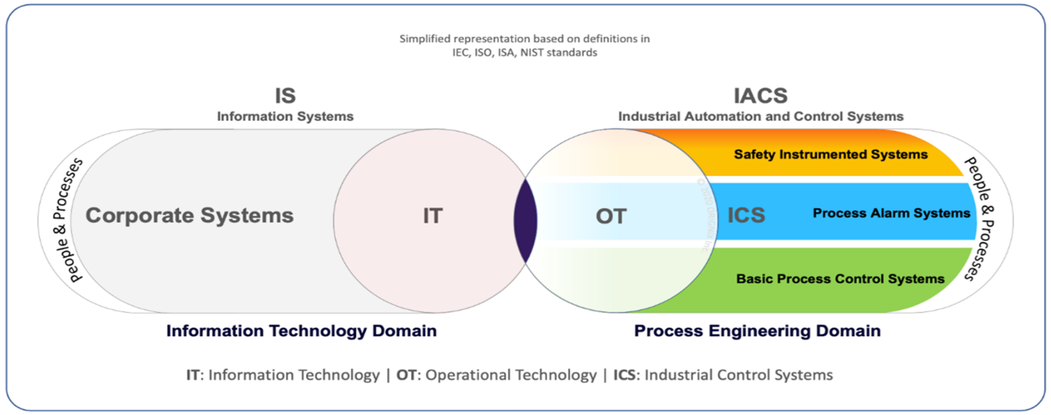
- Within 6 months:
  - Targeted sectors: Water, Healthcare, Agriculture, Energy
  - Iranian APT „Cyber Av3ngers“ attacks Isreali-made Unitronics
  - Pro-russian hacktivists target HMIs, water pumps and alarms

ICS – Specific Malware

- FrostyGoop (January 2024)
  - Uses ModbusTCP to disrupt ENCO controllers of heat control
  - Loss of heat for over 600 apartment buildings in Ukraine for ~2 days
  - Can utilize different configs to attack other ModbusTCP devices
- Fuxnet (~June 2023)
  - Compromised at least 500 sensors of Russia‘s CRITIS monitors via ssh
  - Tried to hamper gas, water and other controls

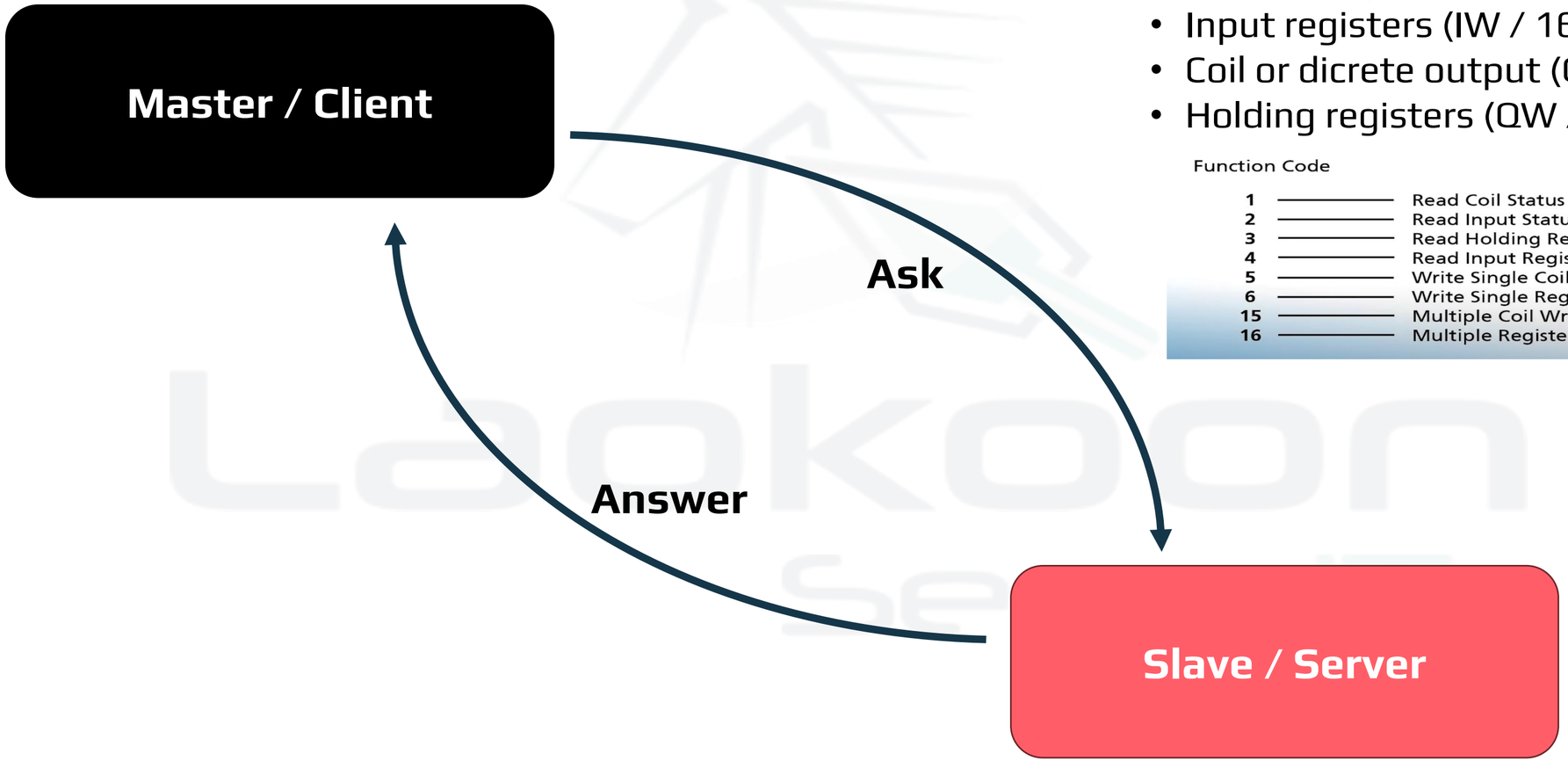
Indirect OT Attacks in Germany

- Hubergroup (October 2024)
  - Delays in production and delivery for at least 2 weeks
- BerlinerLuft (March 2024)
  - Disruption in production and delivery
- Battery manufacturer Varta (February 2024)
  - Cyberattack forced production stop at 5 plants for 1 month
- Wildeboer Bauteile GmbH (Juli 2023)
  - Production shutdown for 1 month



Live-Demo

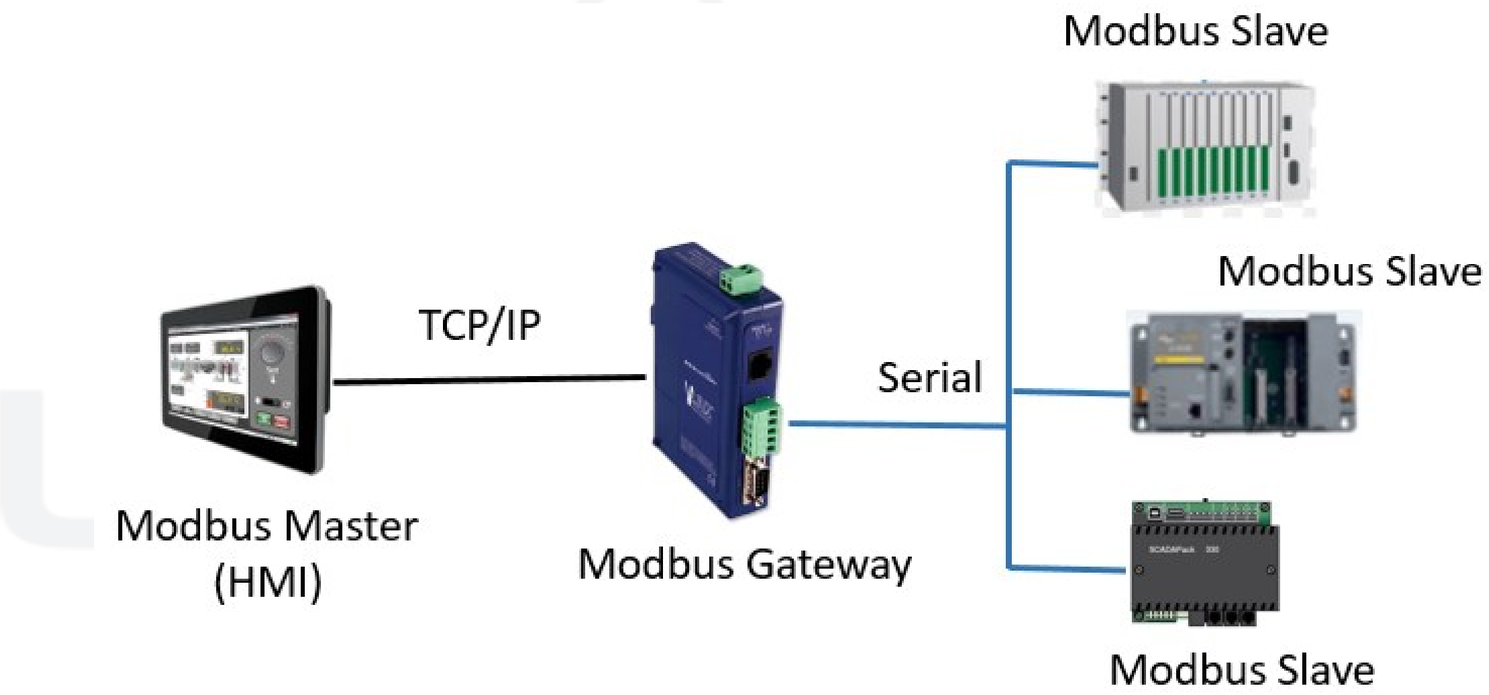
Modbus Overview



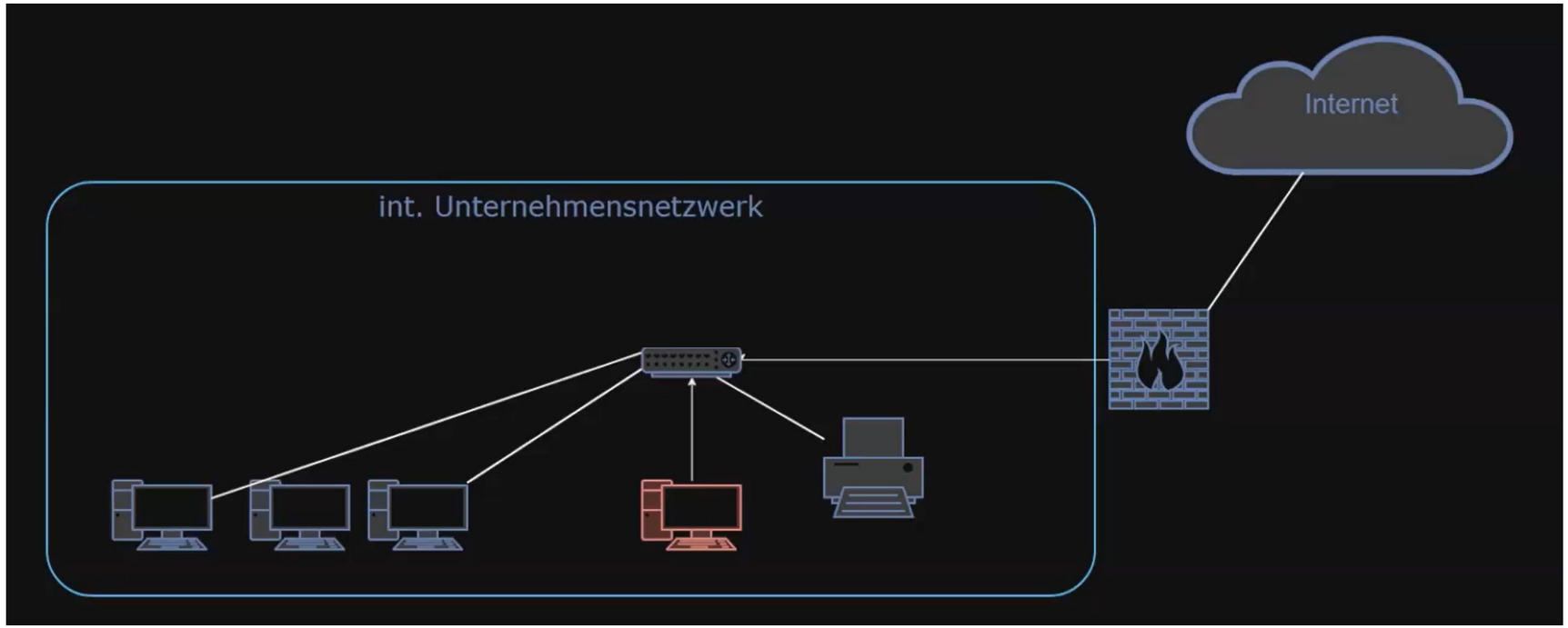
How to address data:

- Discrete Input (IX / 1 bit)
- Input registers (IW / 16 bit)
- Coil or dicrete output (QX / 1 bit)
- Holding registers (QW / 16 bit)

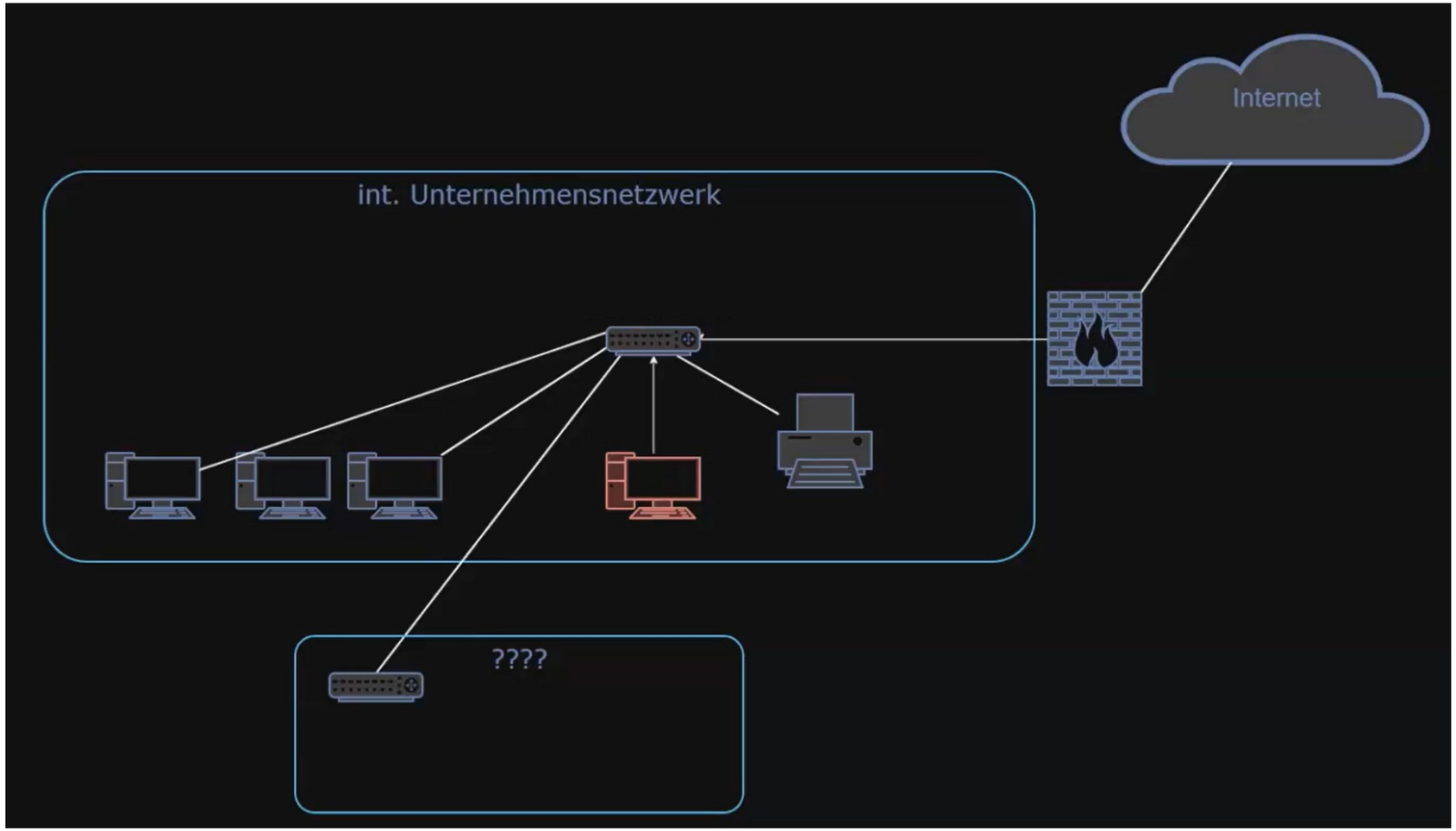
Typical ModbusTCP Setup



Chemical Plant Example



Chemical Plant Example

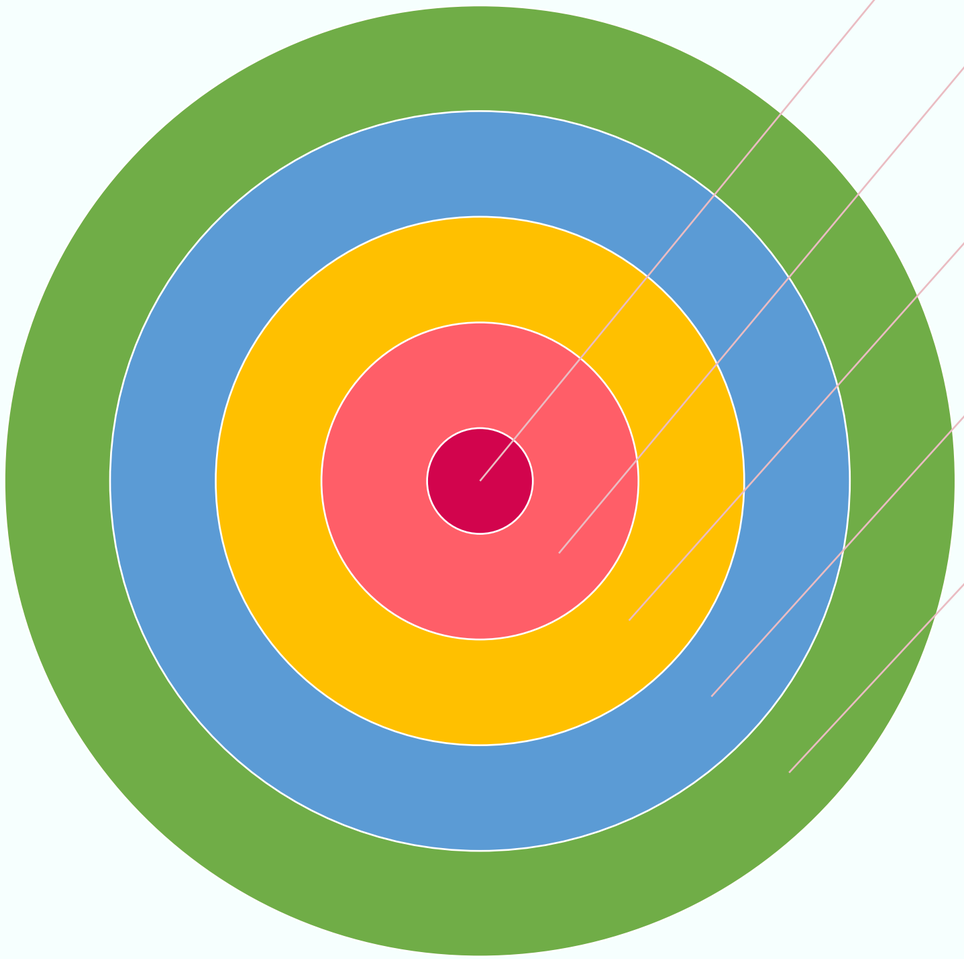


Chemical Plant Example

Mitigations

How to protect...?

Defense in Depth



device hardening

patch and update management

net. segmentation

net. monitoring

do your IT homeworks!

ICS Threat Analysis

ICS Matrix

Below are the tactics and techniques representing the MITRE ATT&CK® Matrix for ICS.

View on the ATT&CK® Navigator

Version Permalink

Initial Access	Execution	Persistence	Privilege Escalation	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
12 techniques	9 techniques	6 techniques	2 techniques	6 techniques	5 techniques	7 techniques	11 techniques	3 techniques	14 techniques	5 techniques	12 techniques
Drive-by Compromise	Change Operating Mode	Hardcoded Credentials	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	Default Credentials	Adversary-in-the-Middle	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Exploit Public-Facing Application	Command-Line Interface	Modify Program	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Automated Collection	Connection Proxy	Alarm Suppression	Modify Parameter	Denial of Control
Exploitation of Remote Services	Execution through API	Module Firmware		Indicator Removal on Host	Remote System Discovery	Hardcoded Credentials	Data from Information Repositories	Standard Application Layer Protocol	Block Command Message	Module Firmware	Denial of View
External Remote Services	Graphical User Interface	Project File Infection		Masquerading	Remote System Information Discovery	Lateral Tool Transfer	Data from Local System		Block Reporting Message	Spoof Reporting Message	Loss of Availability
Internet Accessible Device	Hooking	System Firmware		Rootkit	Wireless Sniffing	Program Download	Detect Operating Mode		Block Serial COM	Unauthorized Command Message	Loss of Control
Remote Services	Modify Controller Tasking	Valid Accounts		Spoof Reporting Message		Remote Services	I/O Image		Change Credential		Loss of Productivity and Revenue
Replication Through Removable Media	Native API					Valid Accounts	Monitor Process State		Data Destruction		Loss of Protection
Rogue Master	Scripting						Point & Tag Identification		Denial of Service		Loss of Safety
Spearphishing Attachment	User Execution						Program Upload		Device Restart/Shutdown		Loss of View
Supply Chain Compromise							Screen Capture		Manipulate I/O Image		Manipulation of Control
Transient Cyber Asset							Wireless Sniffing		Modify Alarm Settings		Manipulation of View
Wireless Compromise									Rootkit		Theft of Operational Information
									Service Stop		
									System Firmware		

Contact

Let's secure your business - together!

Phone	Email	Website	LinkedIn
+49 228 50443980	info@laokoon-security.com	https://laokoon-security.com	

Laokoon SecurITy GmbH, Celsiusstraße 43, 53125 Bonn