TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

"T.I.S.P. Community Meeting 2020"

Berlin, 03.-04.11.2020

Die unsichere Kommunikation von SPS & Co.

Siegfried Müller, MB connect line

Die unsichere Kommunikation von SPS & Co.

©2020 MB Connect Line GmbH, Siegfried Müller

Agenda

1. Unterschied IT/OT
2. Demonstration – ICS-Hacking
3. Was tun? / praxisorientierte Schutzmaßnahmen

©2020 MB Connect Line GmbH, Siegfried Müller

Anforderung in der IT und OT

Büronetzwerk (IT)

1.) Vertraulichkeit
2.) Integrität
3.) Verfügbarkeit

Produktionsnetzwerk (OT)

1.) Verfügbarkeit
2.) Integrität
3.) Vertraulichkeit

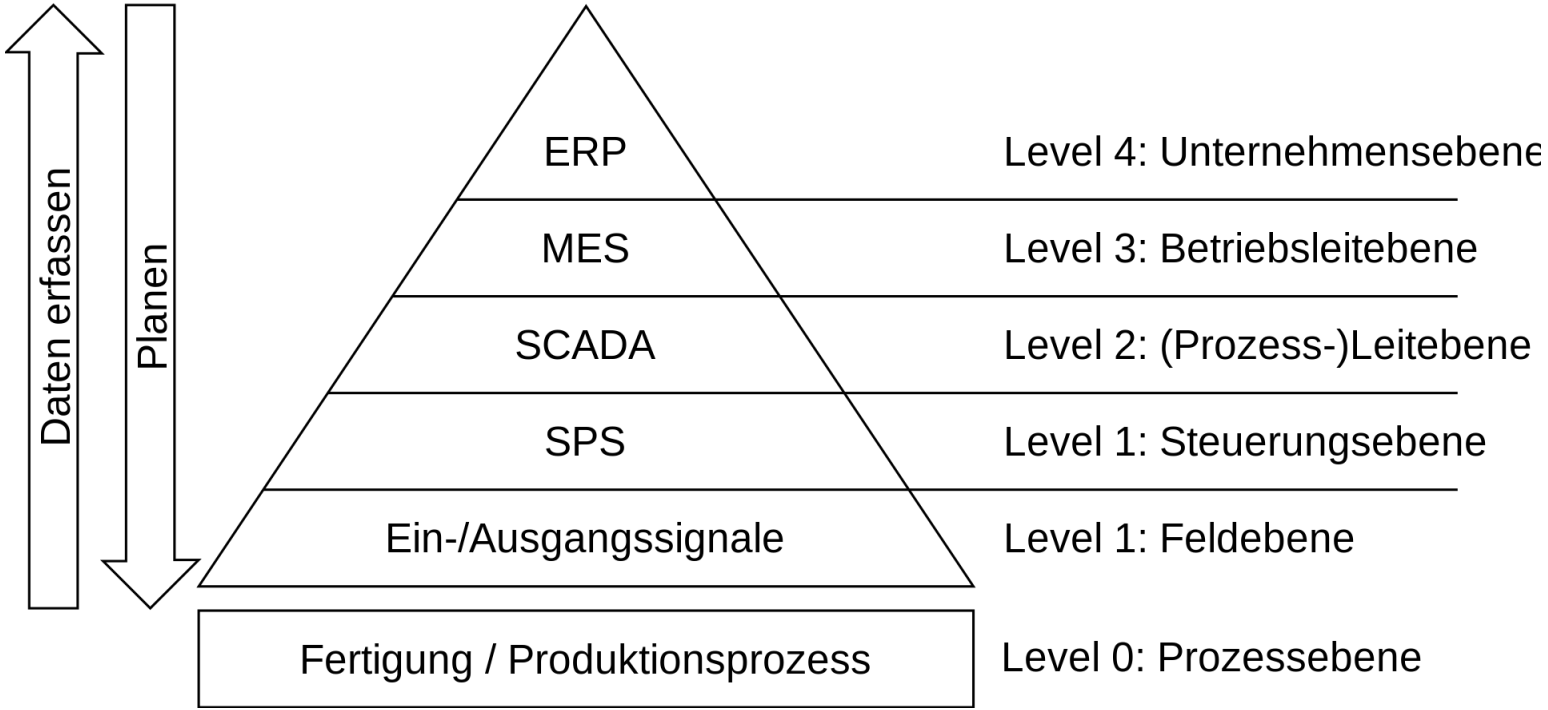
©2020 MB Connect Line GmbH, Siegfried Müller

Anforderung in der IT und OT

	Büronetzwerk IT	Produktionsnetzwerk OT
Latenz	Niedrige Relevanz	Sehr Kritisch
Patch Management	Oft, meist täglich	Selten, Maschinensteuerungen können nur vom Hersteller gepatched werden.
Management	zentralisiert	Meist standalone
Lebenszyklus	3 – 5 Jahre	5-20 Jahre (unsupported OS wie DOS, WIN NT)
Systemänderungen	oft	selten
Verfügbarkeit	Neustart wird toleriert	24x7x365
Virenschutz	Standard	Zu Komplex in den Anlagen, oft nicht möglich
Bewußtsein	Gut	Eher nicht
Schwachstellenprüfung	Standard	Selten und zu komplex
Outsourcing	Üblich	Selten
Zugangssicherheit	Geschlossene Bereiche	Offen zugänglich

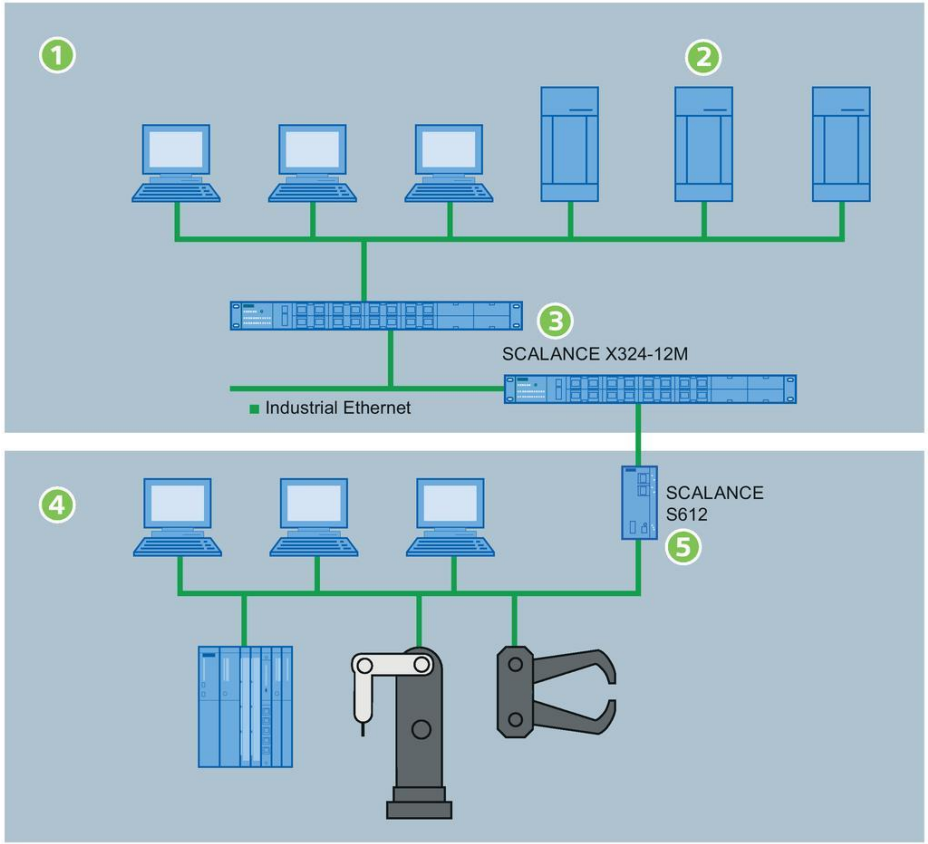
©2020 MB Connect Line GmbH, Siegfried Müller

Netzwerke in der OT



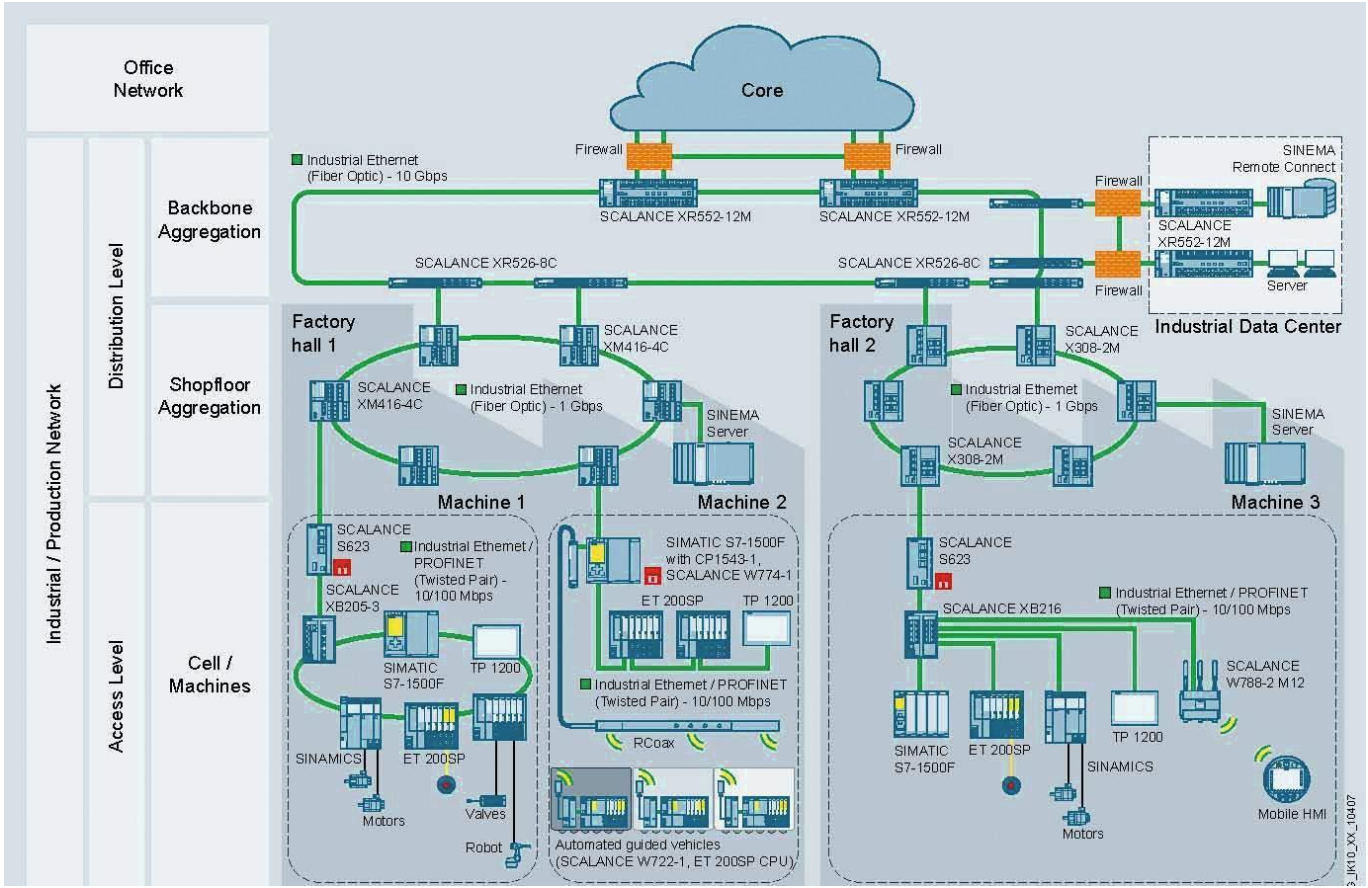
©2020 MB Connect Line GmbH, Siegfried Müller

Netzwerke in der OT



©2020 MB Connect Line GmbH, Siegfried Müller

Netzwerke in der OT



©2020 MB Connect Line GmbH, Siegfried Müller

Anwendungsfall in der Automation

TCP Port 102

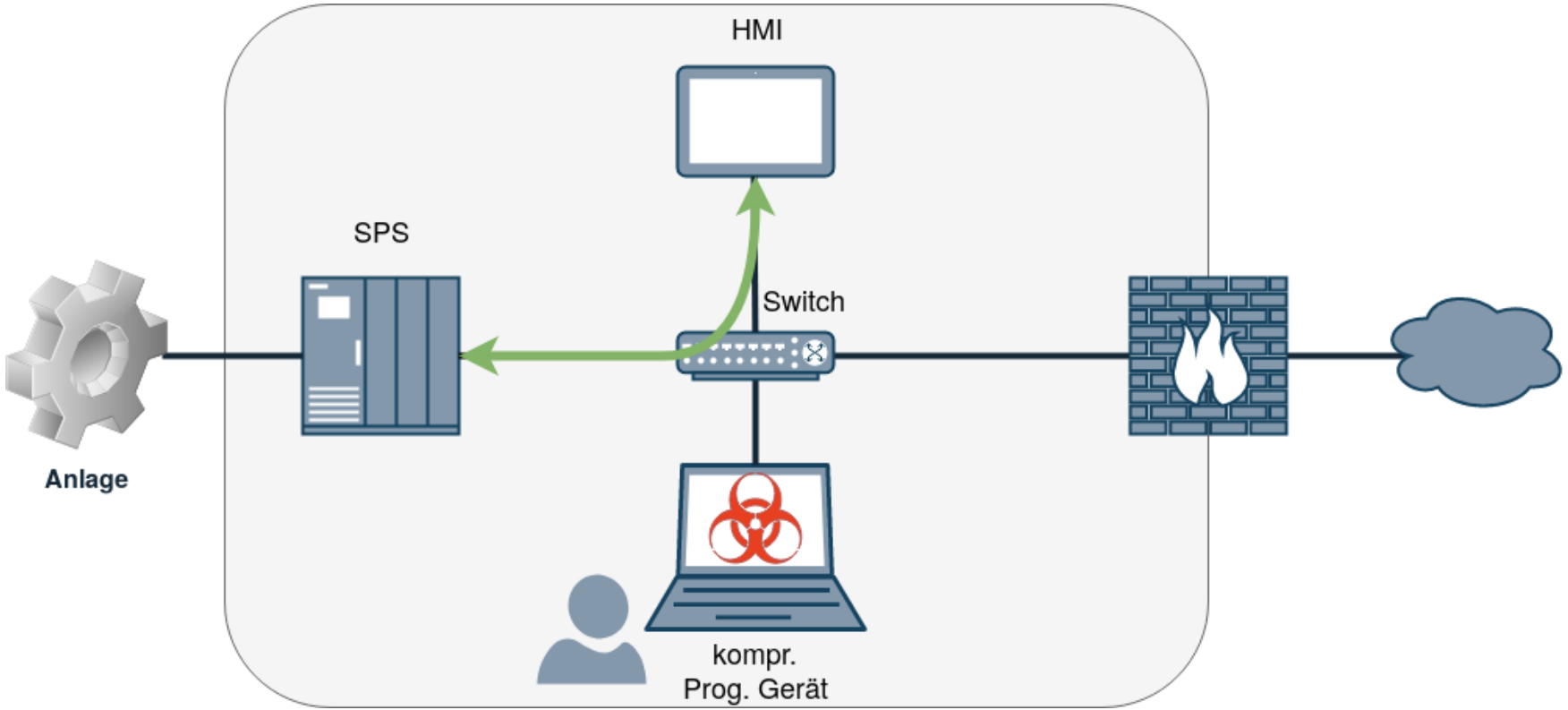
©2020 MB Connect Line GmbH, Siegfried Müller

Risiken

- SPS Programme manipulieren oder löschen
- Sollwerte vom HMI zur SPS manipulieren
- Istwerte von der SPS zum HMI manipulieren
- Kommunikation stören

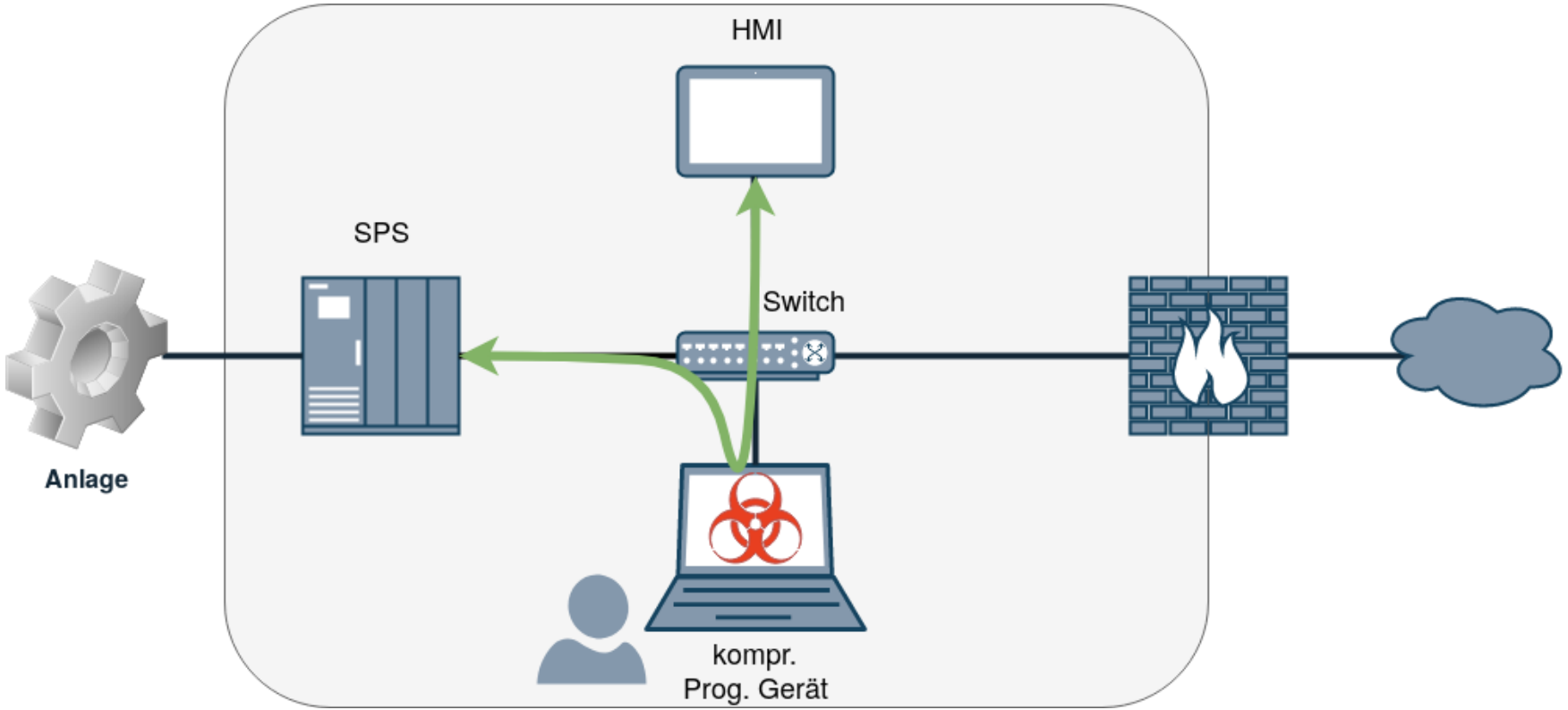
©2020 MB Connect Line GmbH, Siegfried Müller

Szenario



©2020 MB Connect Line GmbH, Siegfried Müller

Man in the Middle



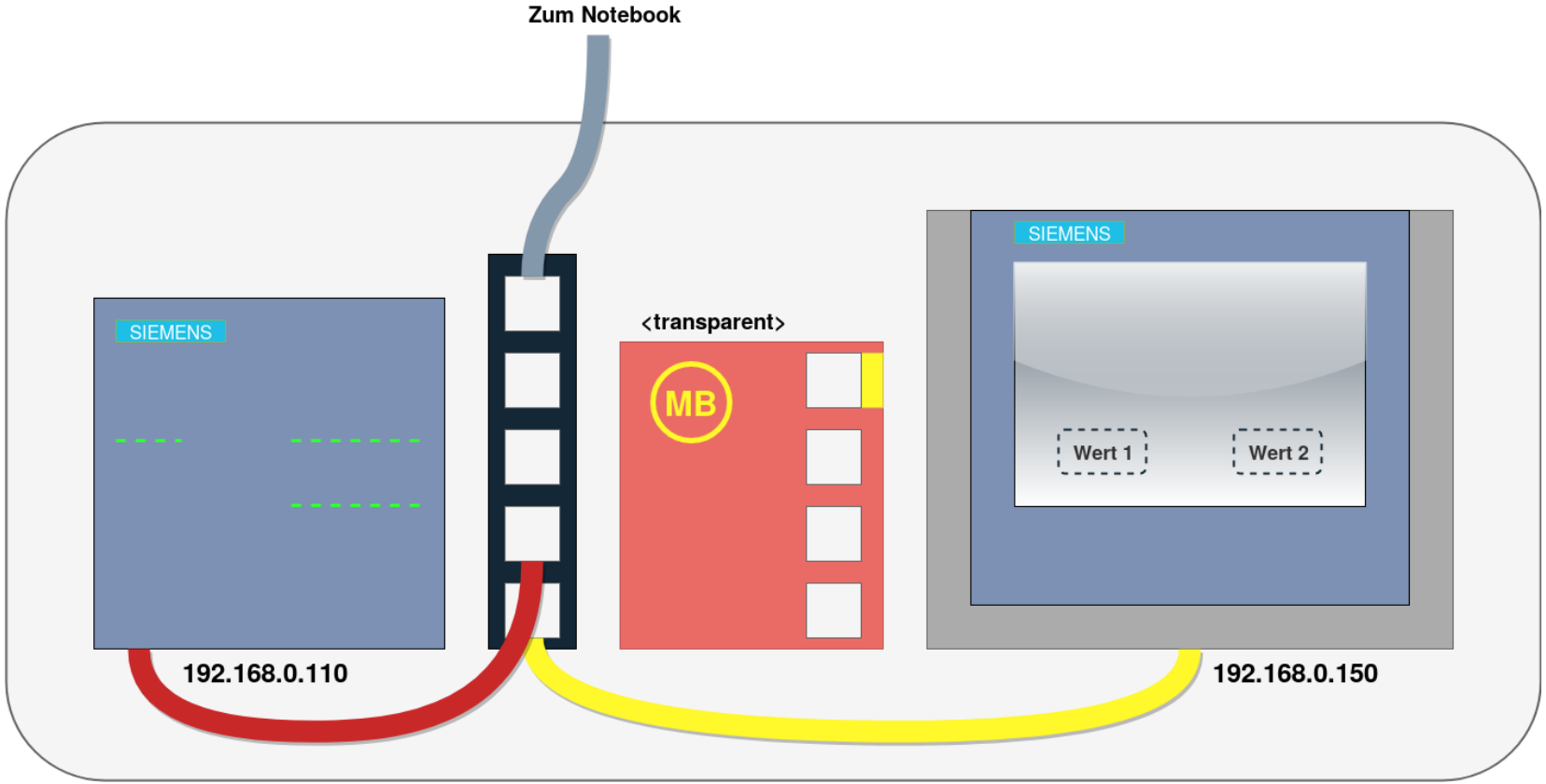
©2020 MB Connect Line GmbH, Siegfried Müller

Demonstration via Video

- Schritt 1: Enumeration
- Schritt 2: Simples DoS
- Schritt 3: Manipulation Datenverkehr

©2020 MB Connect Line GmbH, Siegfried Müller

Szenario



©2020 MB Connect Line GmbH, Siegfried Müller

Demo – Schritt 1: Enumeration

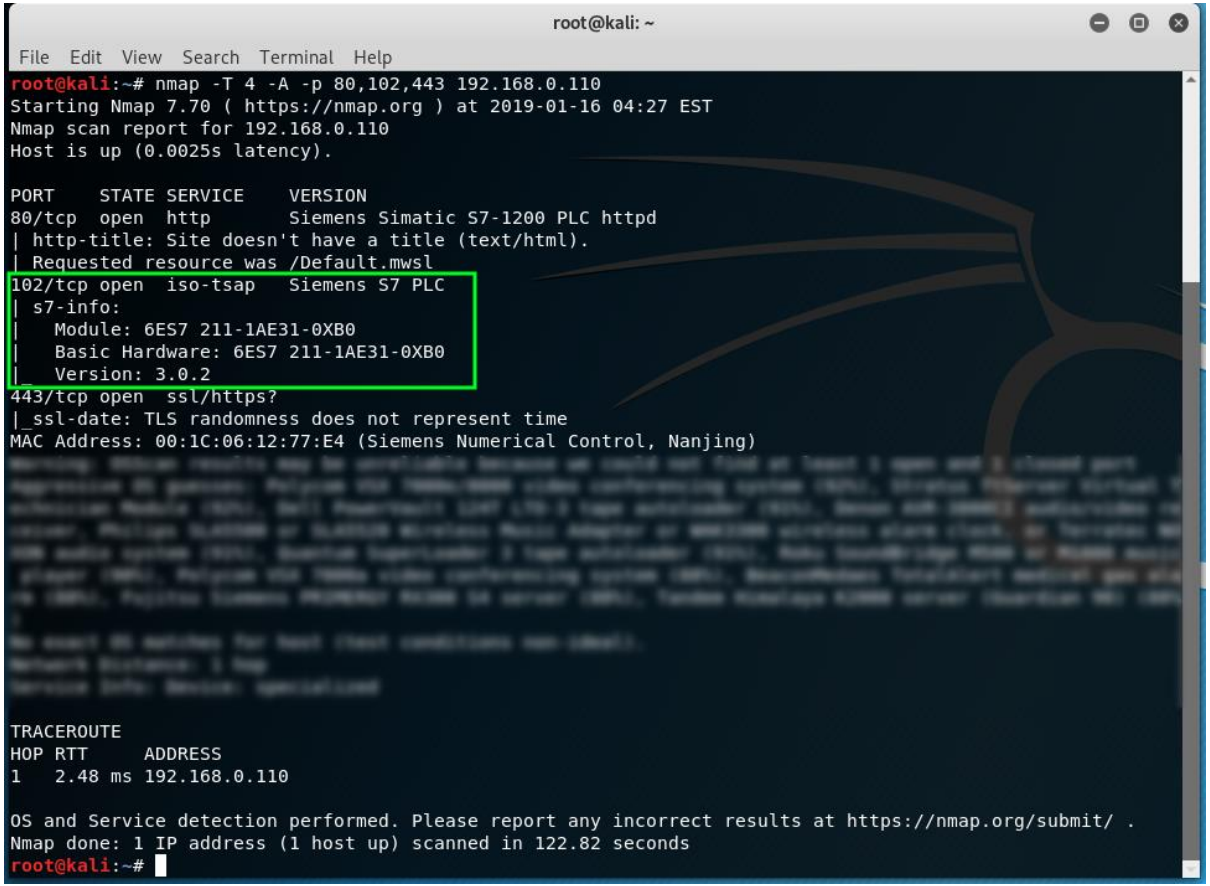
```
nmap -T4 -p 80,102,443 -A 192.168.0.110
```

⇒ Wir sehen S7 Dienst + Version 3.0 Info

⇒ exploit-db.com hat einen Exploit hierfür!

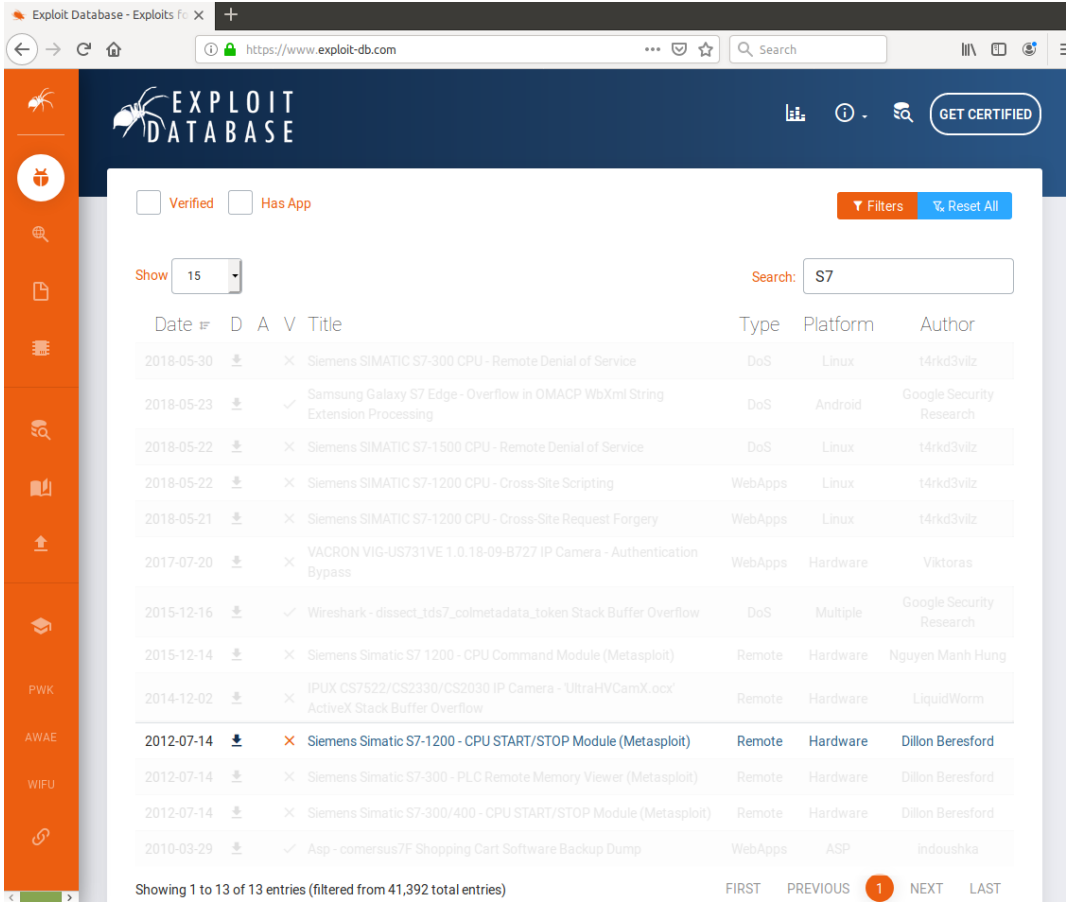
©2020 MB Connect Line GmbH, Siegfried Müller

Demo – Schritt 1: Enumeration



©2020 MB Connect Line GmbH, Siegfried Müller

Demo – Schritt 1: Enumeration



©2020 MB Connect Line GmbH, Siegfried Müller

Demo – Schritt 2: DoS Exploit

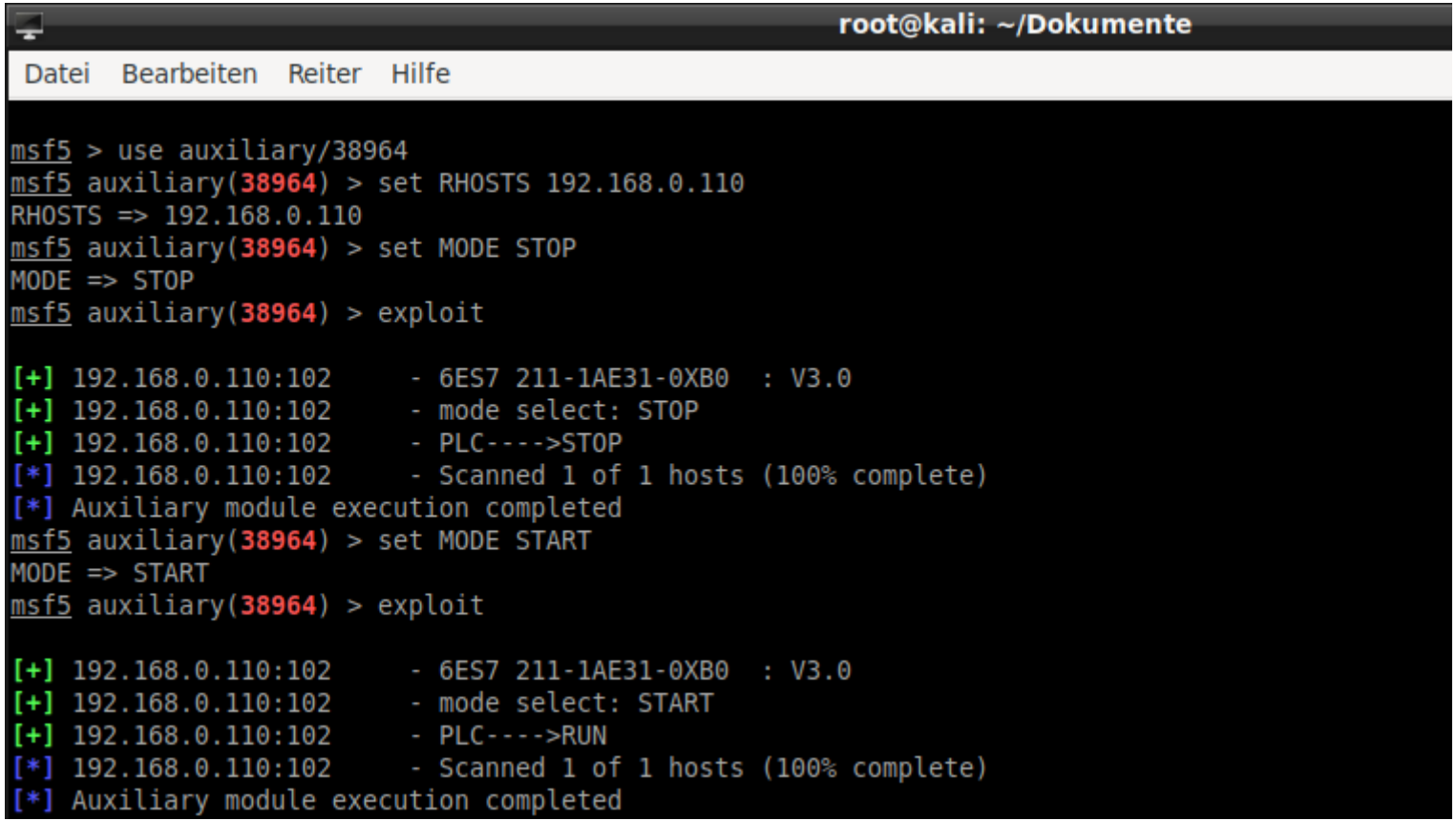
Nutzung von Metasploit für S7 STOP CPU Hack

⇒ CPU stoppt ohne Authentifizierung
(Denial of Service)

⇒ Umstecken hinter die Firewall hilft hier

©2020 MB Connect Line GmbH, Siegfried Müller

Demo – Schritt 2: DoS Exploit



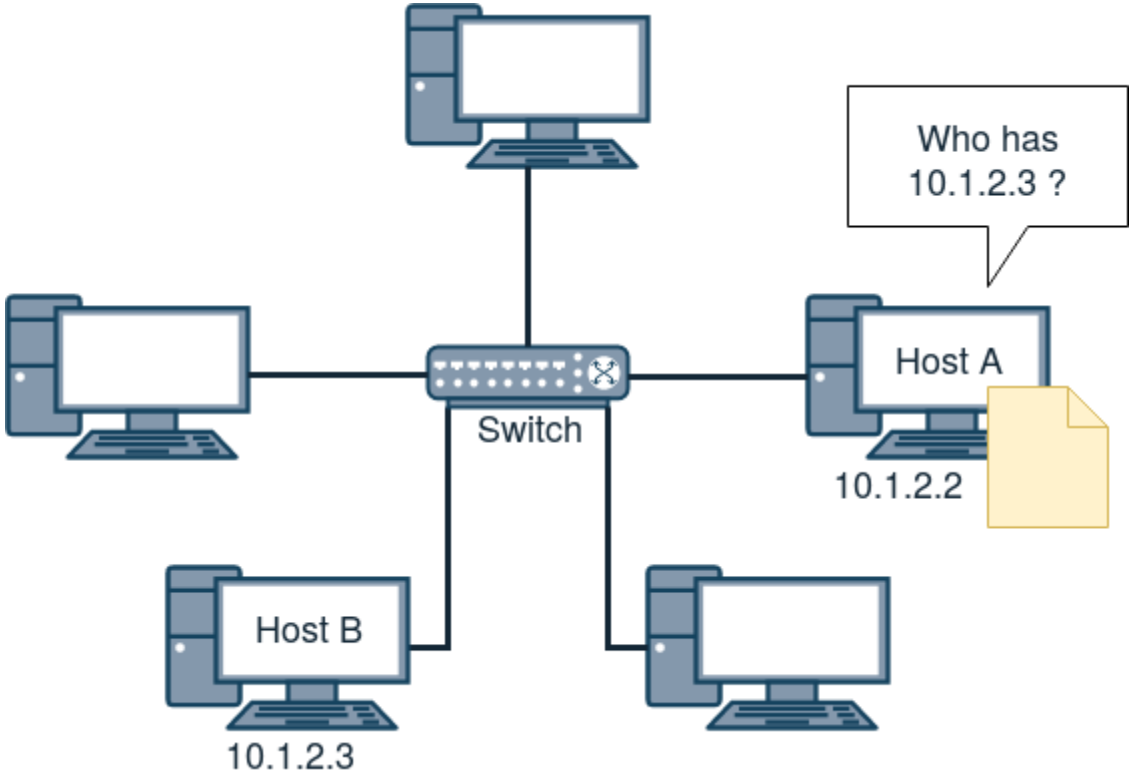
©2020 MB Connect Line GmbH, Siegfried Müller

Demo – Schritt 3: Datenmanipulation per MITM

„Man in the Middle“-Attacke per `ARP-Spoofing`

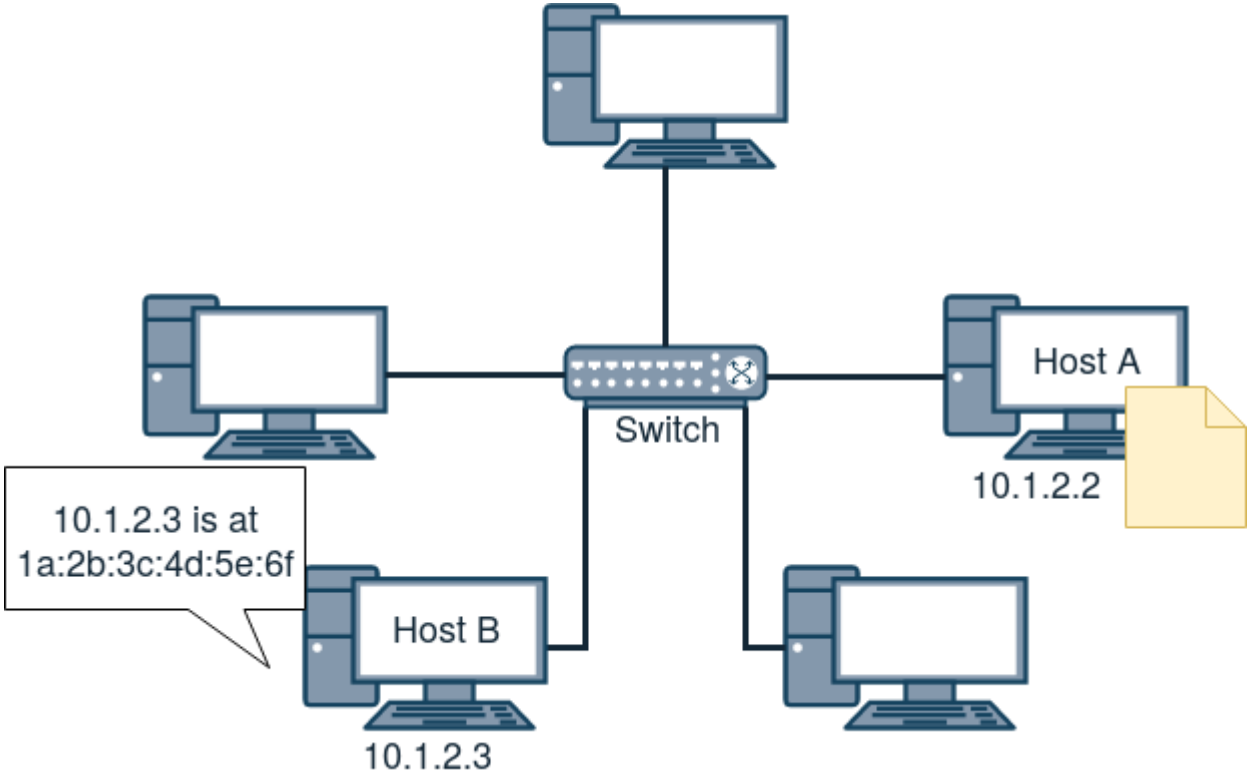
©2020 MB Connect Line GmbH, Siegfried Müller

ARP Request



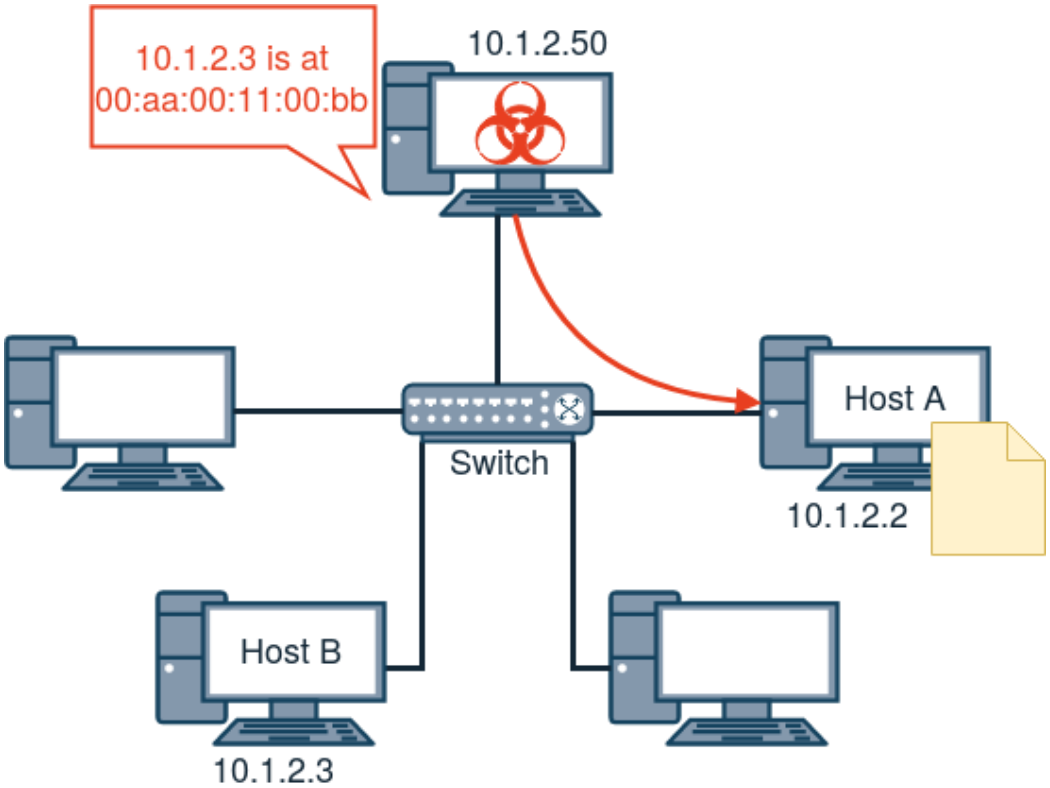
©2020 MB Connect Line GmbH, Siegfried Müller

ARP Reply



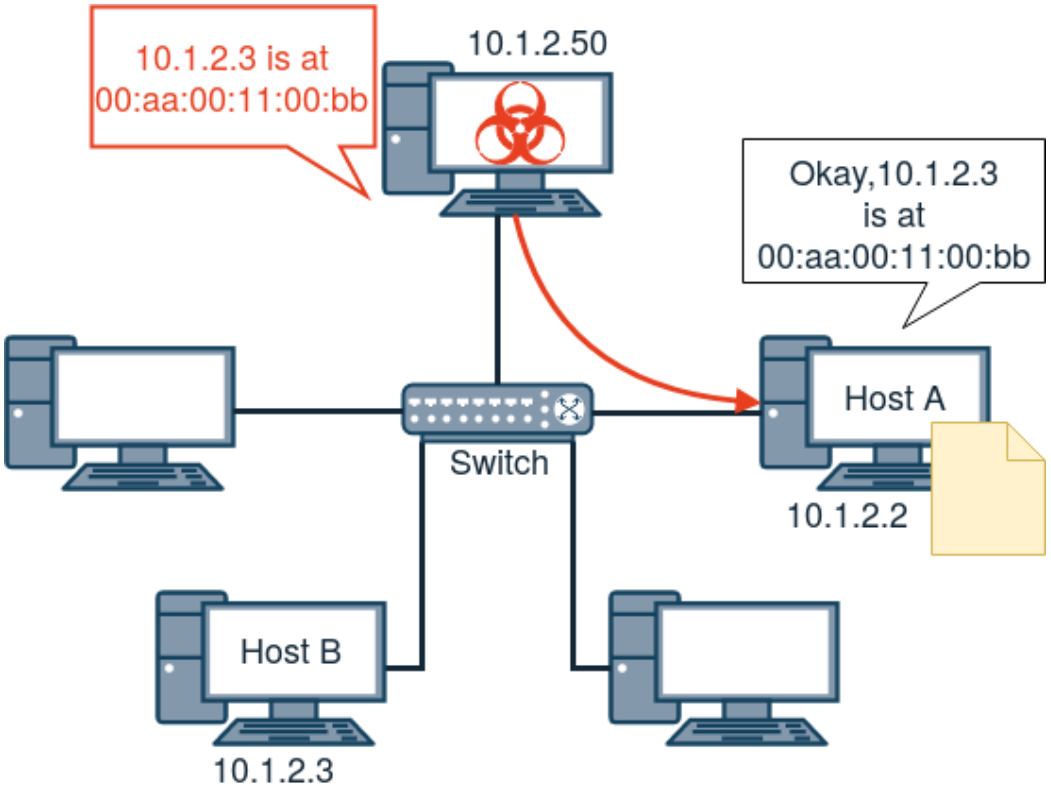
©2020 MB Connect Line GmbH, Siegfried Müller

ARP Spoofing



©2020 MB Connect Line GmbH, Siegfried Müller

ARP Spoofing



©2020 MB Connect Line GmbH, Siegfried Müller

Demo – Schritt 3: Datenmanipulation per MITM

„Man in the Middle“-Attacke per `arpspoof` + scapy (python)

⇒ Verkehr wird über kompromittiertes Notebook geleitet

⇒ Analyse im Wireshark findet Werte, Angreifer kann diese verändern

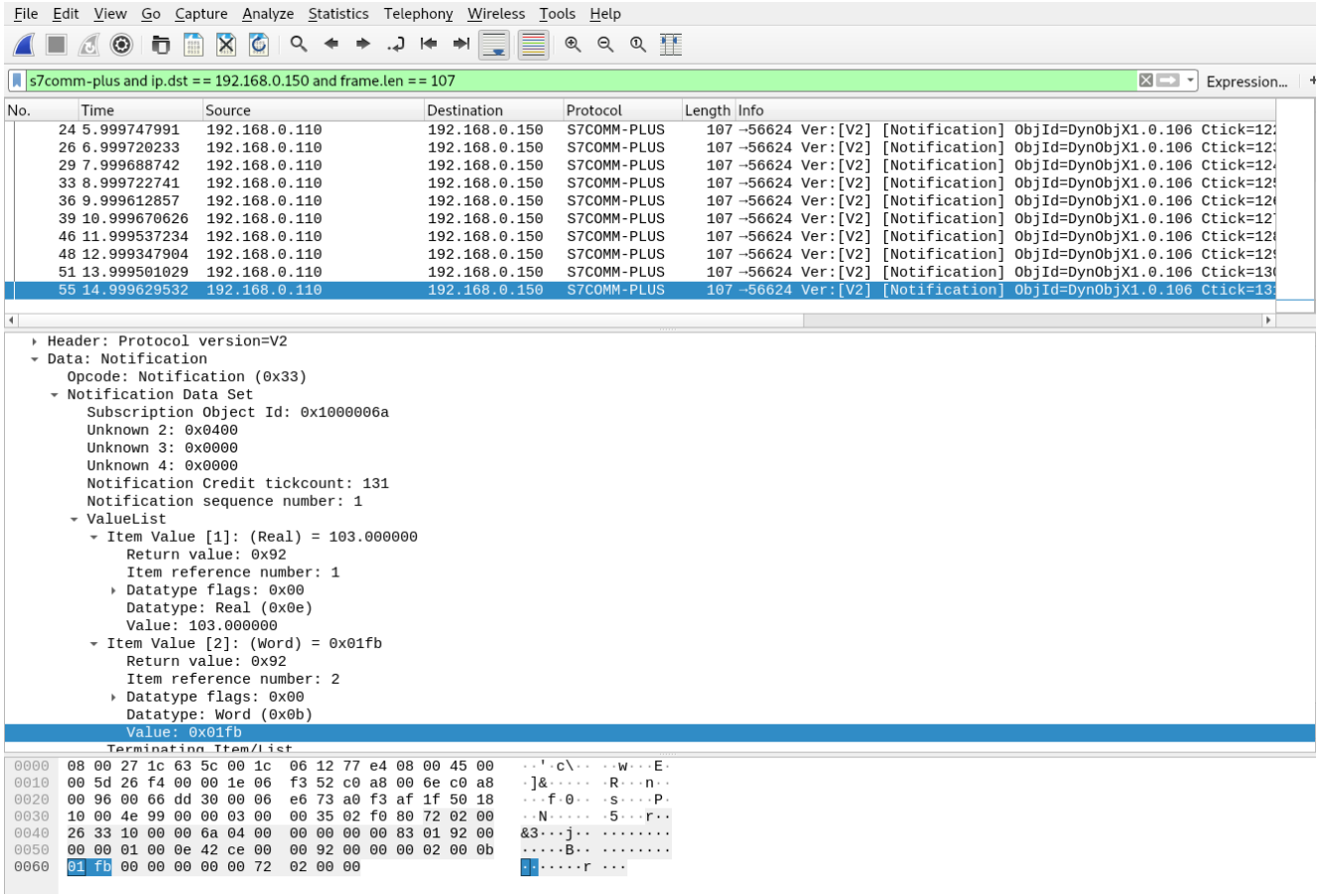
⇒ Bediener vor Ort können sich nicht auf HMI /SCADA Ausgaben verlassen

©2020 MB Connect Line GmbH, Siegfried Müller

Demo – Schritt 3: Datenmanipulation per MITM

©2020 MB Connect Line GmbH, Siegfried Müller

Demo – Schritt 3: Datenmanipulation per MITM



©2020 MB Connect Line GmbH, Siegfried Müller

Demo – Schritt 3: Datenmanipulation per MITM

```
root@kali:~/Dokumente# ./inject_s7_counter.py --value_offset 9 --pkt_len 107 --value 4711
-------------------------------------------
Running packet manipulation, quit with ctrl+c
-------------------------------------------

Injecting value 4711 into S7 communication
Injecting value 4711 into S7 communication
Injecting value 4711 into S7 communication
Injecting value 4711 into S7 communication
Injecting value 4711 into S7 communication
Injecting value 4711 into S7 communication
Injecting value 4711 into S7 communication
```

©2020 MB Connect Line GmbH, Siegfried Müller

Wie sichere ich meine Automationsprozesse ab?

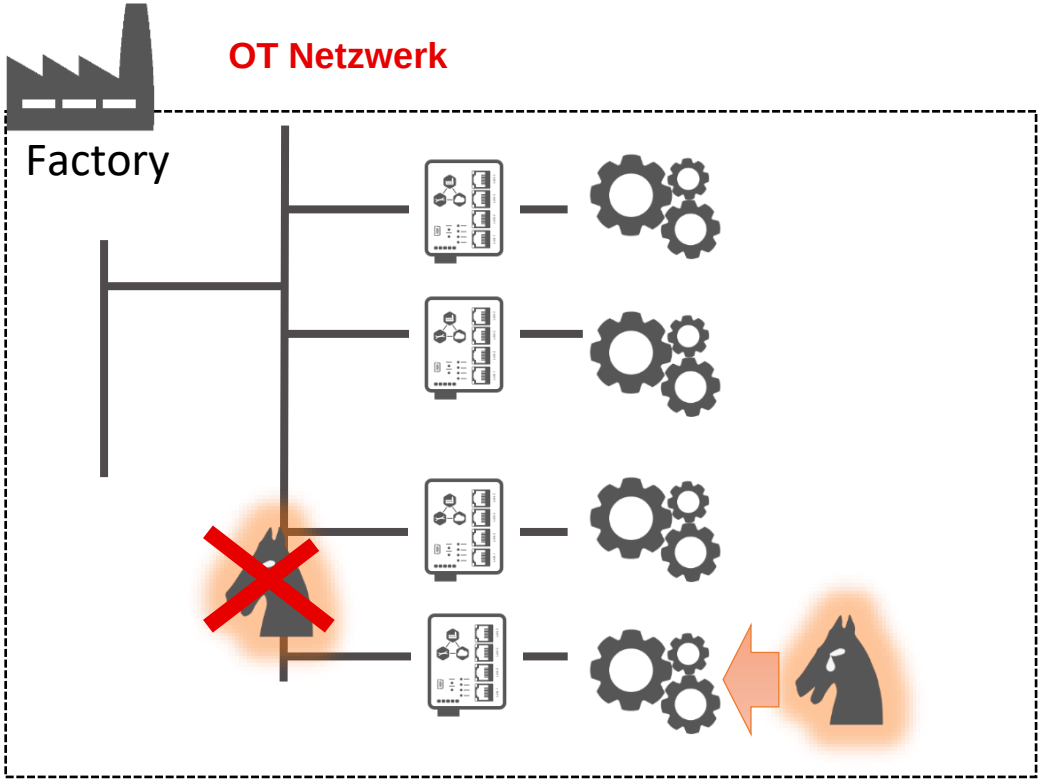
©2020 MB Connect Line GmbH, Siegfried Müller

Maßnahmen zum Stand der Technik

- Automation Firewall
- Sichere Fernwartung
- Daten-Dioden in der Automation

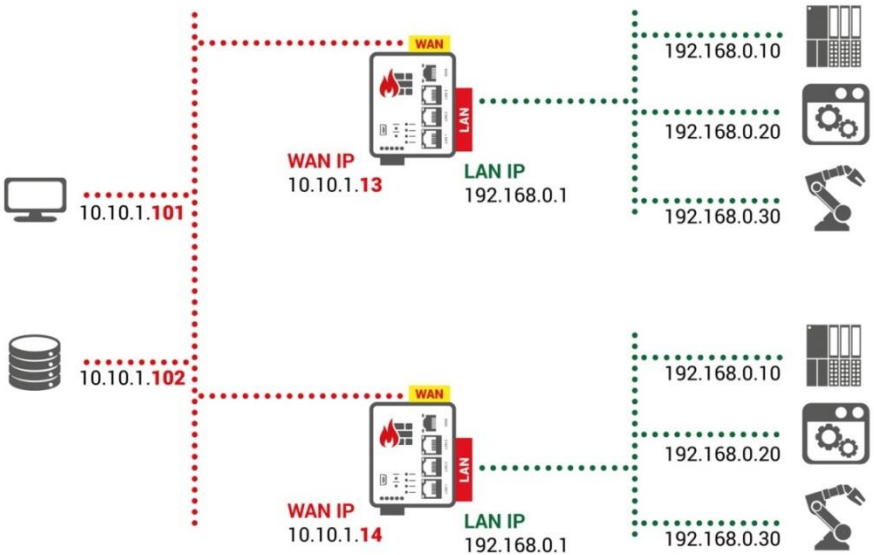
©2020 MB Connect Line GmbH, Siegfried Müller

Automation Firewall



©2020 MB Connect Line GmbH, Siegfried Müller

Micro Netzwerk Segmentierung

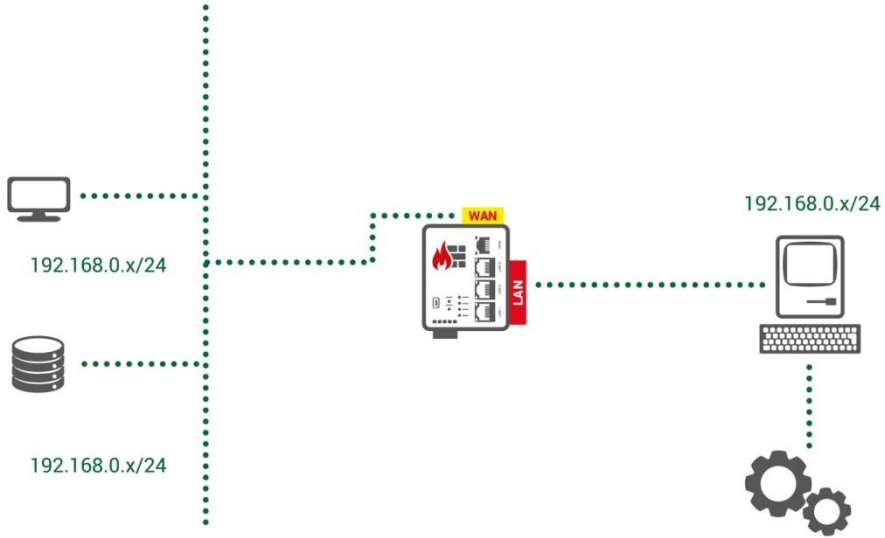


Um einen transparenten Datenfluss zu gewährleisten ist es wichtig, das interne Netzwerk der Maschine vom Produktionsnetz zu isolieren und nur kontrollierten Zugriff zuzulassen.

Durch das Ausblenden des internen Netzwerks hinter einer Firewall können Adresskonflikte bei der Installation neuer Maschinen vermieden werden.

©2020 MB Connect Line GmbH, Siegfried Müller

Absicherung bereits existierender Infrastruktur

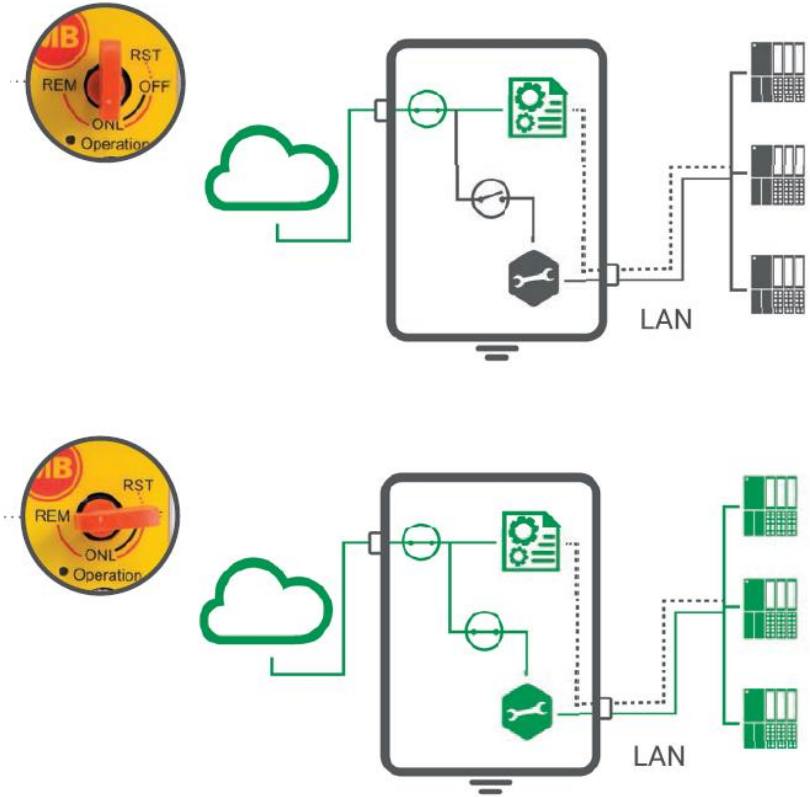


Der Maschinenpark von heute ist vernetzt. Für eine effiziente Produktion ist es entscheidend, auch ältere Bestandsanlagen und Maschinen anzubinden.

Veraltete Betriebssysteme sind jedoch besonders anfällig für Cyberangriffe.

©2020 MB Connect Line GmbH, Siegfried Müller

Sichere Fernwartung



1. Stufe:
Mit der Stellung „ONL“ verbindet sich der Router zum Fernwartungsportal mbCONNECT24 und wird dort als „online“ verbunden angezeigt.
Der Fernwarter hat nun Zugriff auf interne Dienste des Routers (Webserver, Datenmonitoring, etc.), kann aber nicht in das LAN-Segment routen.

2. Stufe:
In der Stellung „REM" ist das Routing zwischen dem Fernwarter und dem LAN-Segment freigeschaltet. Alle Teilnehmer im LAN-Segment können nun transparent erreicht werden. Durch das Zurückstellen auf „ONL“ kann der Betreiber vorort jederzeit die Fernwartung unterbrechen.

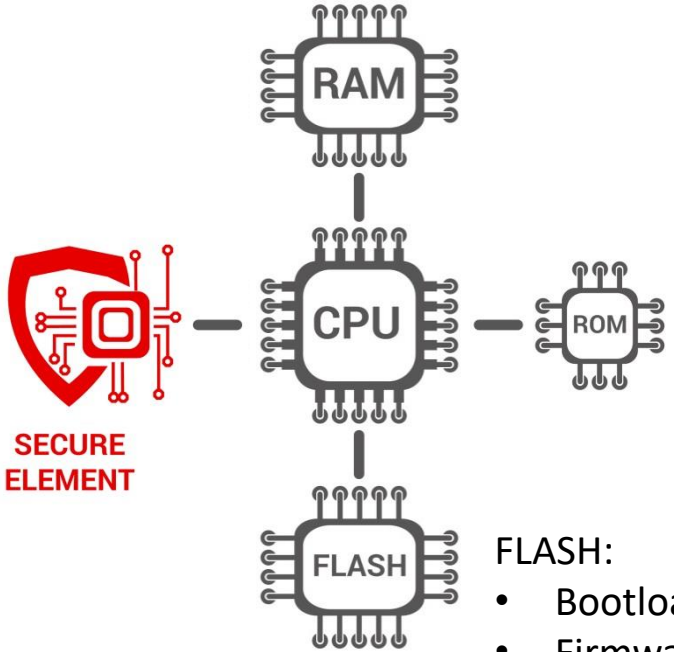
©2020 MB Connect Line GmbH, Siegfried Müller

Hardware Design

<u>Secure Element:</u>

Hardware-IC stores

Passwords and Keys



ROM:

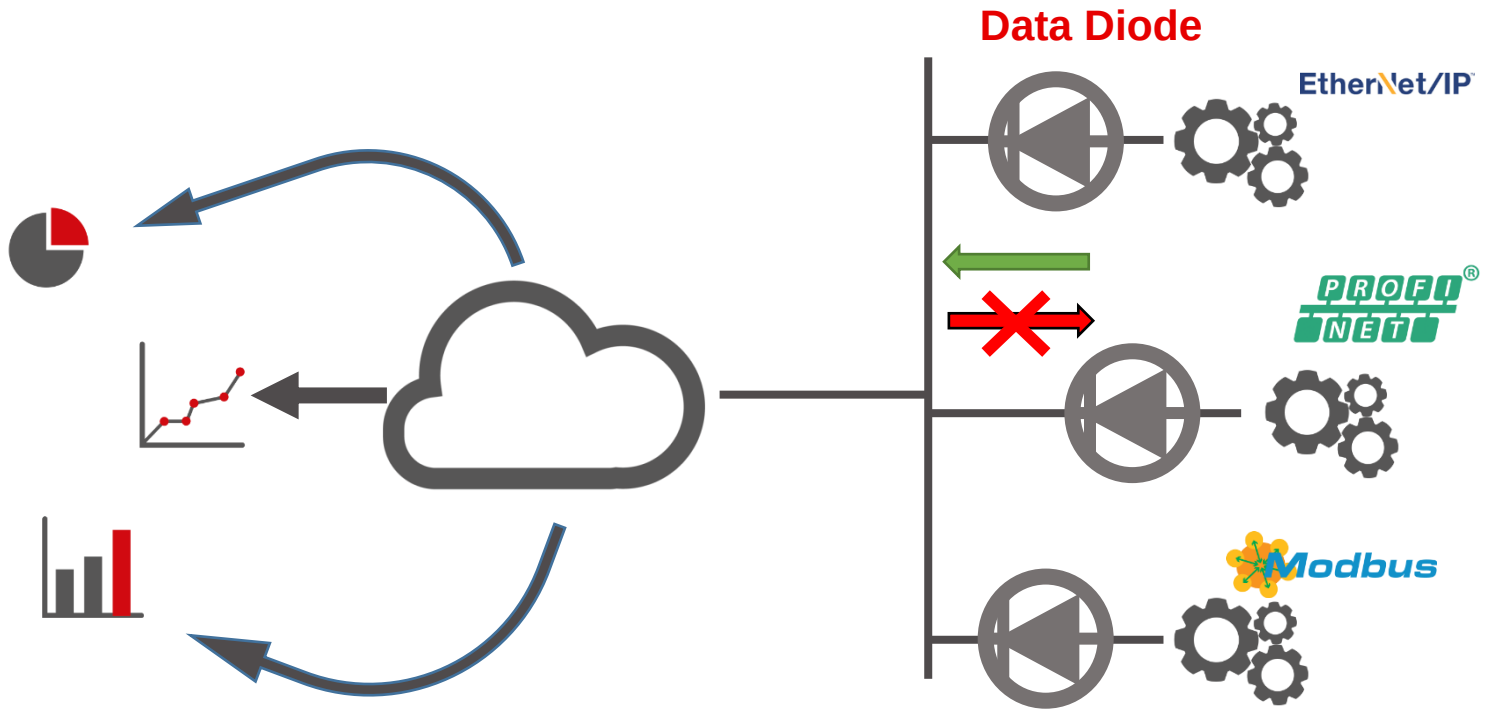
- Bootloader
- MB Connect Line Certificate

FLASH:

- Bootloader
- Firmware
- Userspace

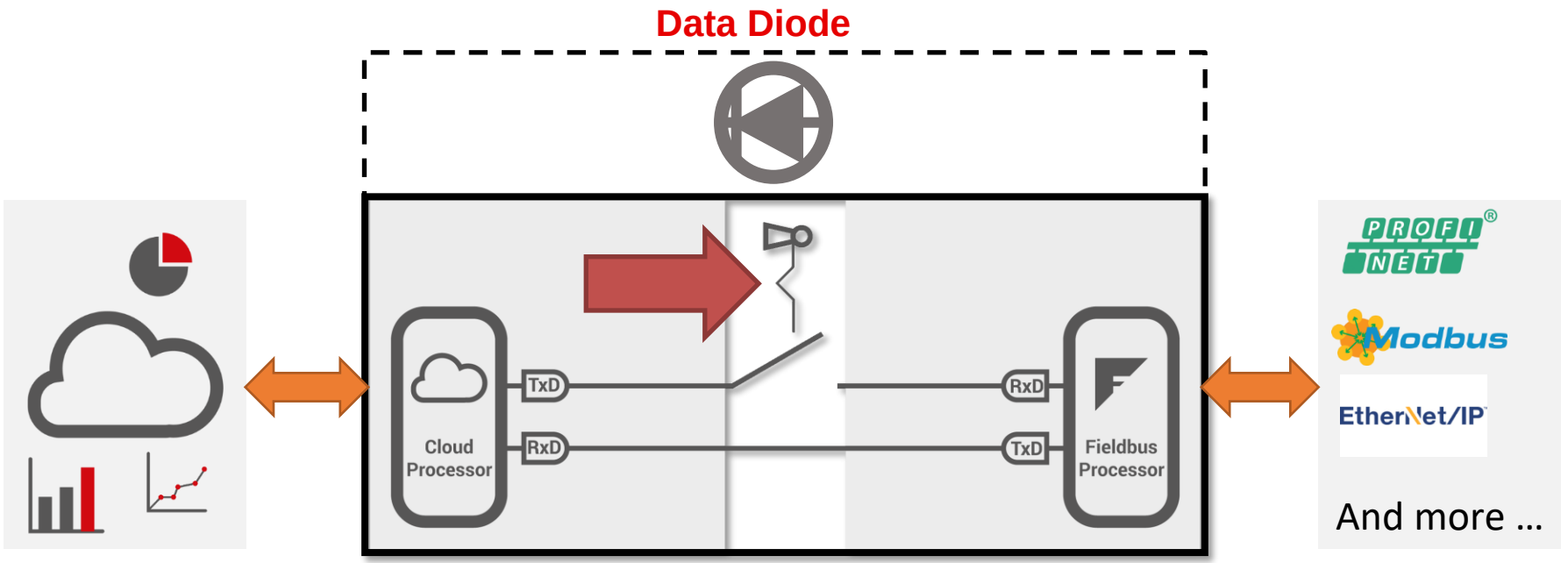
©2020 MB Connect Line GmbH, Siegfried Müller

Daten vom Feldbus in die Cloud



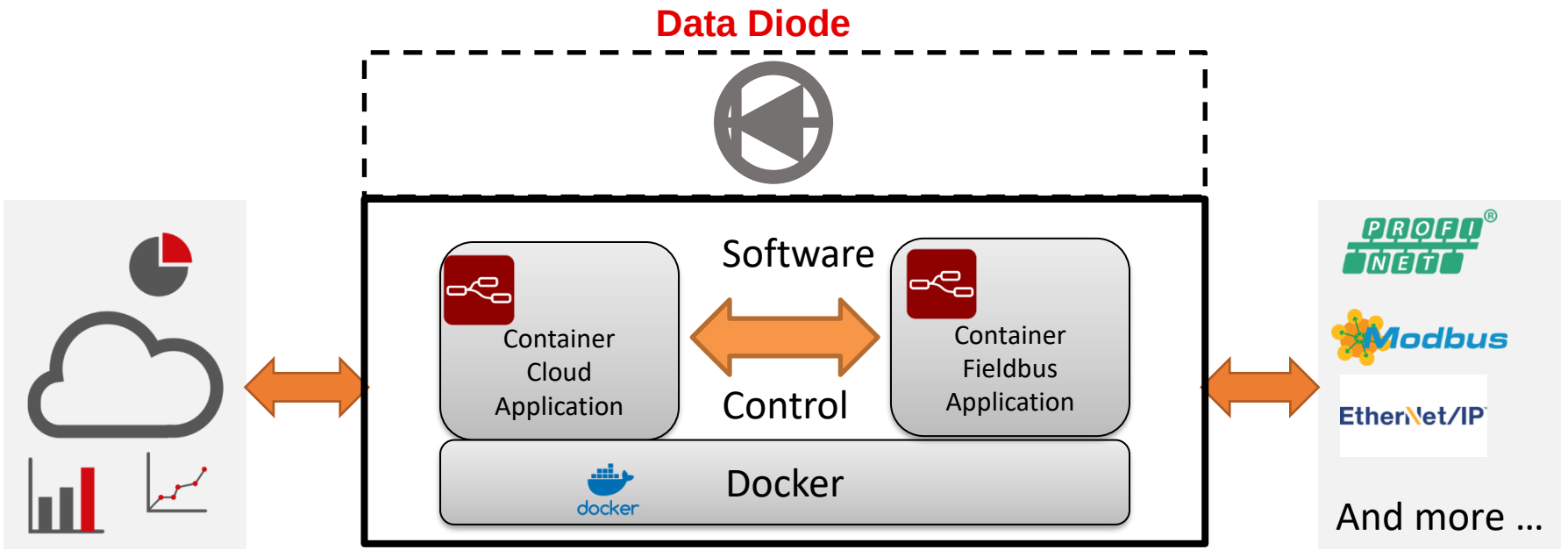
©2020 MB Connect Line GmbH, Siegfried Müller

Security by Hardware



©2020 MB Connect Line GmbH, Siegfried Müller

Security by Software



©2020 MB Connect Line GmbH, Siegfried Müller

Vielen Dank

MB connect line GmbH
Siegfried Müller
mueller@mbconnectline.de
https://www.mbconnectline.com

https://www.sichere-industrie.de

©2020 MB Connect Line GmbH, Siegfried Müller