OTScan 3

Network check: devices and security

Version 3.0.0 | 13.11.2026

Network: Montage_Anlagennetz

YELLOW - Action required Insecure services found

Devices found	Open services	Insecure services
22	70	38

SCAN INFORMATION

Network:	Montage_Anlagennetz	**Scan started:**	10.11.2026 14:20
CIDR:	192.168.30.0/24	**Duration:**	1 h 28 min
Scan profile:	Staged scan complete	**Nmap version:**	7.94
Port set:	ICS_OT_CORE	**Hosts found:**	22

CONTENTS OF THIS REPORT

1. **Cover page** this page
2. **At a glance** Result in simple terms - for everyone
3. **What needs to be done?** Steps, insecure services explained, affected devices
4. **Technical section: summary** Key figures, findings, recommendations for specialists
5. **Network heatmap** Overview by subnet and device type
6. **Critical hosts** Detail view of all devices with findings
7. **Host inventory** Complete device list
8. **Comparison** Changes since the last full scan (if available)
9. **Technical details** Scan parameters and appendix
10. **ICS/OT glossary** Protocol explanations and classification

2 AT A GLANCE - THE RESULT IN SIMPLE TERMS

Network Montage_Anlagennetz (192.168.30.0/24), scanned on 10.11.2026 14:20, duration: 1 h 28 min

YELLOW

Action required

Overall assessment: Action required

Some devices offer services that are considered insecure. This is not an attack, but an open door that should be closed in a planned way.

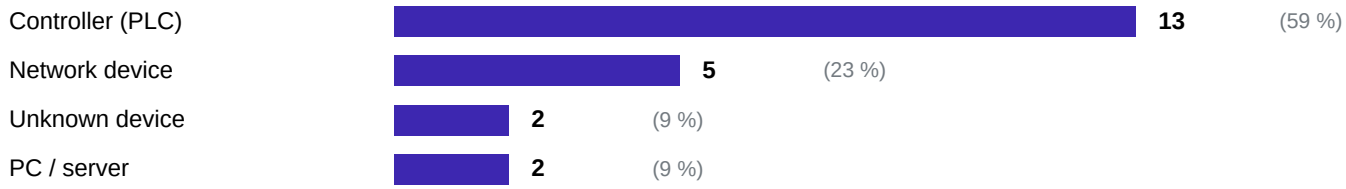
What now? Agree on the suggested actions with the people responsible for the plant and schedule them.

Devices found	Devices with findings	Insecure services
22	**19**	**38**
responded to the scan	offer at least one insecure service	open services considered insecure

Key points

- 22 devices were found in network Montage_Anlagennetz.
- 19 of 22 devices offer at least one insecure service.
- 9 devices are affected according to vendor advisories (firmware in the affected range); for 2 devices, the model matches an advisory - check the firmware on the device.
- 2 devices are visible only in firewall traffic (Splunk 02.11.2026 - 08.11.2026), not in the scan - 2 of them not in the CMDB.
- 38 of 38 insecure services had no traffic through the firewall during the Splunk period 02.11.2026 - 08.11.2026 - candidates for disabling.
- Most common: HTTP on 15 devices, SNMP on 10 devices, Telnet on 5 devices.
- Most devices are: Controller (PLC) (13 of 22).

Which devices are in the network?



Change since the last scan

No complete previous scan of this network available for comparison. After the next full scan, this section shows what has changed.

Good to know: this report shows which services are reachable in the network. It does not say whether a device has been attacked. Control protocols such as S7, Modbus or OPC UA are normal in production networks and are not counted as findings.

3 WHAT NEEDS TO BE DONE?

The most important steps, most important first. Agree with the people responsible for the plant - do not disable anything on controllers without consultation.

1. **HTTP on 15 devices**
   Switch to HTTPS or disable; logging in over HTTP is not permitted under the traffic rules.
2. **SNMP on 10 devices**
   SNMPv1/v2c and 'public' are not permitted under the traffic rules: switch to SNMPv3.
3. **Telnet on 5 devices**
   Not permitted under the traffic rules: disable, use SSH for remote access.
4. **FTP on 2 devices**
   Not permitted under the traffic rules: disable, otherwise use SFTP or FTPS.
5. **Check firewall rules**
   Allow insecure services only for the computers that really need them.
6. **Search the network for 2 Splunk-only devices (MAC/switchport) and add them to the CMDB - template**
   File "..._CMDB-Nachtrag.xlsx".

Insecure services briefly explained

Service	What is it?	Why risky?	What to do?	Devices
HTTP (Port 80/tcp)	Device web interface	Login and settings are sent unencrypted over the network.	Switch to HTTPS or disable; logging in over HTTP is not permitted under the traffic rules.	**15**
SNMP (Port 161/udp)	Device data query	With v1/v2c, the password (community) is sent unencrypted over the network.	SNMPv1/v2c and 'public' are not permitted under the traffic rules: switch to SNMPv3.	**10**
Telnet (Port 23/tcp)	Command-line remote access	Passwords and commands are sent unencrypted over the network.	Not permitted under the traffic rules: disable, use SSH for remote access.	**5**
FTP (Port 21/tcp)	File transfer	User name, password and files are sent unencrypted over the network.	Not permitted under the traffic rules: disable, otherwise use SFTP or FTPS.	**2**
SMB (Port 445/tcp)	Windows file sharing	Old versions (SMBv1) are a common path for malware.	Disable SMBv1 (not permitted under the traffic rules), use SMBv3 with signing, restrict access.	**2**
VNC (Port 5900/tcp)	Remote screen control	Screen, input and often the password are sent unencrypted over the network.	Not permitted under the traffic rules: disable or use only encrypted (TLS, VPN, SSH tunnel).	**2**
RPC (Port 135/tcp)	Windows remote control service	Common attack point; shows which Windows services are running.	Only if technically necessary and only for approved computers; otherwise block via firewall.	**2**

Which devices are affected?

IP address	Device	Vendor	Insecure services
192.168.30.3	Network device	Cisco Systems	HTTP, SNMP, Telnet
192.168.30.4	Network device	Hirschmann Automation and Control GmbH	HTTP, SNMP, Telnet
192.168.30.20	Controller (PLC)	Schneider Electric	FTP, HTTP, SNMP
192.168.30.30	Unknown device	Moxa Technologies	HTTP, SNMP, Telnet
192.168.30.31	Unknown device	Moxa Technologies	HTTP, SNMP, Telnet
192.168.30.102	Network device	Hirschmann Automation and Control GmbH	HTTP, SNMP, Telnet
192.168.30.22	Controller (PLC)	Wago Kontakttechnik GmbH	FTP, HTTP
192.168.30.25	Controller (PLC)	Siemens AG	HTTP, VNC
192.168.30.26	Controller (PLC)	Siemens AG	HTTP, VNC
192.168.30.60	PC / server	Fujitsu Technology Solutions GmbH	RPC, SMB
192.168.30.61	PC / server	Fujitsu Technology Solutions GmbH	RPC, SMB
192.168.30.10	Controller (PLC)	Siemens AG	HTTP, SNMP
192.168.30.11	Controller (PLC)	Siemens AG	HTTP, SNMP
192.168.30.1	Network device	Fortinet	SNMP
192.168.30.2	Network device	Siemens AG	SNMP
192.168.30.15	Controller (PLC)	Siemens AG	HTTP
192.168.30.16	Controller (PLC)	Siemens AG	HTTP
192.168.30.21	Controller (PLC)	OMRON Corporation	HTTP
192.168.30.101	Controller (PLC)	Siemens AG, Automations & Drives,	HTTP

From the next page on, the technical section follows with all details for specialists.

4 SUMMARY FOR SPECIALISTS

YELLOW - Action required - Insecure services found

WHAT DOES THE RISK VALUE MEAN?

OTScan 3 compares the open ports of each device exclusively against the traffic rules (HanselCraft default, based on IEC 62443, customizable by the user) - 15 protocol families such as Telnet, SMB, FTP, HTTP or SNMP that should not be used or only when secured. For each open protocol from the traffic rules the tool adds a weight (3 = not permitted and remote control/file access possible, 2 = not permitted, plain-text login or information leakage, 1 = secondary port or permitted with TLS); the sum is the "Risk" value of this device as shown in the title line, badge and sections 6 and 7 of this report. OT control protocols such as S7, Modbus, CODESYS or OPC-UA are NOT included - they are expected communication in OT networks and not a finding. Traffic light: GREEN = no protocol from the traffic rules open, YELLOW = at least one open, INFO = device reachable but no port data. The Risk value is a sorting/prioritization aid (higher = more insecure IT services open), not a standardized metric like CVSS. A port scan does not show version and login method (e.g. SMBv1/v3, SNMPv1/v3); they must be checked on the device. Complete catalog: Excel sheet "Ports", column "Verkehrsregel" (traffic rule).

KEY FIGURES AT A GLANCE

Scanned hosts:	**22**	**Open ports:**	70
Insecure ports open:	**38**	**Scan date:**	10.11.2026 14:20

KEY FINDINGS

- ⚠ **WARNING: 22 devices scanned - MEDIUM risk level (YELLOW)**
- ⚠ **38 insecure ports open under the traffic rules (e.g. Telnet, SMB, FTP, HTTP, SNMP) - OT control protocols such as S7/Modbus/OPC-UA are NOT included**
- ℹ ***Most common vendor: Siemens AG (10 of 22)***
- ⚠ **SECURITY RISK: 5 devices with Telnet (port 23) open**

RECOMMENDED ACTIONS

1. Analyze critical ports and secure them with firewall rules
2. Check firmware updates for all OT devices
3. CRITICAL: disable Telnet (port 23) on 5 devices -> use SSH
4. Implement network segmentation (separate the OT network from the IT network)
5. Replace FTP (port 21) with SFTP/FTPS on 2 devices

5 NETWORK HEATMAP - RISK BY SUBNET & DEVICE TYPE

INSECURE: at least one protocol from the traffic rules found
RECOMMENDATION: no protocols from the traffic rules open

Subnet	Hosts	Insecure	FW crit.	FW Blk	Top device type	Risk
192.168.30.0/24	22	38	0	0	PLC (Siemens S7)	INSECURE

DEVICE TYPE DISTRIBUTION

Device type	Qty.	Share	Bar
PLC (Siemens S7)	10	45%	10
Network (firewall/switch)	4	18%	4
Unknown	2	9%	2
Windows PC / workstation	2	9%	2
Network (Siemens SCALANCE)	1	5%	1
PLC (Schneider Modicon)	1	5%	1
PLC (Rockwell/Allen-Bradley)	1	5%	1
PLC (Phoenix/WAGO)	1	5%	1

SPS/PLC HMI/SCADA Network Windows/Linux Other

6 CRITICAL HOSTS - DETAIL VIEW (19 DEVICES)

192.168.30.3 Network (firewall/switch) | Cisco Systems | Risk points: 7

MAC address:	00:00:0C:1E:18:BD	**Device type:**	Network (firewall/switch)
Vendor:	Cisco Systems	**OS detection:**	Cisco IOS 17
TCP ports:	22,443,23,80	**UDP ports:**	161
Crit. ports:	161/udp, 23/tcp, 80/tcp		

192.168.30.4 Network (firewall/switch) | Hirschmann Automation and C... | Risk points: 7

MAC address:	00:80:63:1E:1F:CA	**Device type:**	Network (firewall/switch)
Vendor:	Hirschmann Automation and Control GmbH	**TCP ports:**	23,80
UDP ports:	161		
Crit. ports:	161/udp, 23/tcp, 80/tcp		

192.168.30.20 PLC (Schneider Modicon) | Schneider Electric | Risk points: 7

MAC address:	00:00:54:1E:8F:9A	**Device type:**	PLC (Schneider Modicon)
Vendor:	Schneider Electric	**TCP ports:**	21,80,502
UDP ports:	161		
Crit. ports:	161/udp, 21/tcp, 80/tcp		

192.168.30.30 - | Moxa Technologies | Risk points: 7

MAC address:	00:90:E8:1E:D5:1C	**Device type:**	-
Vendor:	Moxa Technologies	**TCP ports:**	23,80
UDP ports:	161		
Crit. ports:	161/udp, 23/tcp, 80/tcp		

192.168.30.31 - | Moxa Technologies | Risk points: 7

MAC address:	00:90:E8:1E:DC:29	**Device type:**	-
Vendor:	Moxa Technologies	**TCP ports:**	23,80
UDP ports:	161		
Crit. ports:	161/udp, 23/tcp, 80/tcp		

192.168.30.102 Network (firewall/switch) | Hirschmann Automation and C... | Risk points: 7

MAC address:	64:60:38:1E:CD:C4	**Device type:**	Network (firewall/switch)
Vendor:	Hirschmann Automation and Control GmbH	**TCP ports:**	23,80
UDP ports:	161		
Crit. ports:	161/udp, 23/tcp, 80/tcp		

192.168.30.22 PLC (Phoenix/WAGO) | Wago Kontakttechnik GmbH | Risk points: 5

MAC address:	00:30:DE:1E:9D:B4	**Device type:**	PLC (Phoenix/WAGO)
Vendor:	Wago Kontakttechnik GmbH	**OS detection:**	Linux 4.x
TCP ports:	21,22,80,443,502,2455		
Crit. ports:	21/tcp, 80/tcp		

192.168.30.25 PLC (Siemens S7) | Siemens AG | Risk points: 5

MAC address:	00:1B:1B:1E:B2:DB	**Device type:**	PLC (Siemens S7)
Vendor:	Siemens AG	**TCP ports:**	80,5900,102
Crit. ports:	5900/tcp, 80/tcp		

192.168.30.26 PLC (Siemens S7) | Siemens AG | Risk points: 5

MAC address:	00:1B:1B:1E:B9:E8	**Device type:**	PLC (Siemens S7)
Vendor:	Siemens AG	**TCP ports:**	80,5900,102
Crit. ports:	5900/tcp, 80/tcp		

192.168.30.60 Windows PC / workstation | Fujitsu Technology Solution... | Risk points: 5

MAC address:	00:19:99:1E:A7:A2	**Device type:**	Windows PC / workstation
Vendor:	Fujitsu Technology Solutions GmbH	**OS detection:**	Microsoft Windows 10
TCP ports:	135,445,3389		
Crit. ports:	135/tcp, 445/tcp		

192.168.30.61 Windows PC / workstation | Fujitsu Technology Solution... | Risk points: 5

MAC address:	00:19:99:1E:AE:AF	**Device type:**	Windows PC / workstation
Vendor:	Fujitsu Technology Solutions GmbH	**OS detection:**	Microsoft Windows 10
TCP ports:	135,445		
Crit. ports:	135/tcp, 445/tcp		

192.168.30.10 H3-MO-SPS-L1 PLC (Siemens S7) | Siemens AG | Risk points: 4

Device name:	H3-MO-SPS-L1 (S7)	**MAC address:**	00:1B:1B:1E:49:18
Device type:	PLC (Siemens S7)	**Vendor:**	Siemens AG
S7 System:	H3-MO-SPS-L1	**S7 Module:**	6ES7 315-2EH14-0AB0 CPU 315-2 PN/DP
TCP ports:	80,102	**UDP ports:**	161,34964
Crit. ports:	161/udp, 80/tcp		

192.168.30.11 H3-MO-SPS-L2 PLC (Siemens S7) | Siemens AG | Risk points: 4

Device name:	H3-MO-SPS-L2 (S7)	**MAC address:**	00:1B:1B:1E:50:25
Device type:	PLC (Siemens S7)	**Vendor:**	Siemens AG
S7 System:	H3-MO-SPS-L2	**S7 Module:**	6ES7 317-2EK14-0AB0 CPU 317-2 PN/DP
TCP ports:	80,102	**UDP ports:**	161,34964
Crit. ports:	161/udp, 80/tcp		

192.168.30.1 Network (firewall/switch) | Fortinet | Risk points: 2

MAC address:	00:09:0F:1E:0A:A3	**Device type:**	Network (firewall/switch)
Vendor:	Fortinet	**OS detection:**	FortiOS 7.2
TCP ports:	443	**UDP ports:**	161
Crit. ports:	161/udp		

192.168.30.2 Network (Siemens SCALANCE) | Siemens AG | Risk points: 2

MAC address:	00:0E:8C:1E:11:B0	**Device type:**	Network (Siemens SCALANCE)
Vendor:	Siemens AG	**TCP ports:**	22,443
UDP ports:	161		
Crit. ports:	161/udp		

192.168.30.15 H3-MO-SPS-ST01 PLC (Siemens S7) | Siemens AG | Risk points: 2

Device name:	H3-MO-SPS-ST01 (S7)	**MAC address:**	00:1B:1B:1E:6C:59
Device type:	PLC (Siemens S7)	**Vendor:**	Siemens AG
S7 System:	H3-MO-SPS-ST01	**S7 Module:**	6ES7 214-1AG40-0XB0 CPU 1214C DC/DC/DC
TCP ports:	102,80,443		
Crit. ports:	80/tcp		

192.168.30.16 H3-MO-SPS-ST02 PLC (Siemens S7) | Siemens AG | Risk points: 2

Device name:	H3-MO-SPS-ST02 (S7)	**MAC address:**	00:1B:1B:1E:73:66
Device type:	PLC (Siemens S7)	**Vendor:**	Siemens AG
S7 System:	H3-MO-SPS-ST02	**S7 Module:**	6ES7 215-1AG40-0XB0 CPU 1215C DC/DC/DC
TCP ports:	102,80,443		
Crit. ports:	80/tcp		

192.168.30.21 PLC (Rockwell/Allen-Bradley) | OMRON Corporation | Risk points: 2

MAC address:	00:00:0A:1E:96:A7	**Device type:**	PLC (Rockwell/Allen-Bradley)
Vendor:	OMRON Corporation	**TCP ports:**	80,9600,44818
UDP ports:	9600		
Crit. ports:	80/tcp		

192.168.30.101 PLC (Siemens S7) | Siemens AG, Automations & D... | Risk points: 2

MAC address:	30:13:89:1E:C6:B7	**Device type:**	PLC (Siemens S7)
Vendor:	Siemens AG, Automations & Drives,	**TCP ports:**	80,102,443
Crit. ports:	80/tcp		

7 HOST INVENTORY - 22 DEVICES (SORTED BY RISK SCORE)

Risk points: sum of the weights of all insecure services of a device (0 = normal). Red from 6 points.

IP address	MAC address	Device type	Vendor	Risk points	Operating system	Name	Open TCP ports
192.168.30.3	00:00:0C:1E:18:BD	Network (firewall/switch)	Cisco Systems	7	Cisco IOS 17		22, 443, 23, 80
192.168.30.4	00:80:63:1E:1F:CA	Network (firewall/switch)	Hirschmann Automation and Control GmbH	7			23, 80
192.168.30.20	00:00:54:1E:8F:9A	PLC (Schneider Modicon)	Schneider Electric	7			21, 80, 502
192.168.30.30	00:90:E8:1E:D5:1C	-	Moxa Technologies	7			23, 80
192.168.30.31	00:90:E8:1E:DC:29	-	Moxa Technologies	7			23, 80
192.168.30.102	64:60:38:1E:CD:C4	Network (firewall/switch)	Hirschmann Automation and Control GmbH	7			23, 80
192.168.30.22	00:30:DE:1E:9D:B4	PLC (Phoenix/WAGO)	Wago Kontakttechnik GmbH	5	Linux 4.x		21, 22, 80, 443, 502, 2455
192.168.30.25	00:1B:1B:1E:B2:DB	PLC (Siemens S7)	Siemens AG	5			80, 5900, 102
192.168.30.26	00:1B:1B:1E:B9:E8	PLC (Siemens S7)	Siemens AG	5			80, 5900, 102
192.168.30.60	00:19:99:1E:A7:A2	Windows PC / workstation	Fujitsu Technology Solutions GmbH	5	Microsoft Windows 10		135, 445, 3389
192.168.30.61	00:19:99:1E:AE:AF	Windows PC / workstation	Fujitsu Technology Solutions GmbH	5	Microsoft Windows 10		135, 445
192.168.30.10	00:1B:1B:1E:49:18	PLC (Siemens S7)	Siemens AG	4		H3-MO-SPS-L1	80, 102
192.168.30.11	00:1B:1B:1E:50:25	PLC (Siemens S7)	Siemens AG	4		H3-MO-SPS-L2	80, 102
192.168.30.1	00:09:0F:1E:0A:A3	Network (firewall/switch)	Fortinet	2	FortiOS 7.2		443
192.168.30.2	00:0E:8C:1E:11:B0	Network (Siemens SCALANCE)	Siemens AG	2			22, 443
192.168.30.15	00:1B:1B:1E:6C:59	PLC (Siemens S7)	Siemens AG	2		H3-MO-SPS-ST 01	102, 80, 443
192.168.30.16	00:1B:1B:1E:73:66	PLC (Siemens S7)	Siemens AG	2		H3-MO-SPS-ST 02	102, 80, 443
192.168.30.21	00:00:0A:1E:96:A7	PLC (Rockwell/Allen-Bradley)	OMRON Corporation	2			80, 9600, 44818
192.168.30.101	30:13:89:1E:C6:B7	PLC (Siemens S7)	Siemens AG, Automations & Drives,	2			80, 102, 443
192.168.30.12	00:1B:1B:1E:57:32	PLC (Siemens S7)	Siemens AG	0		H3-MO-SPS-L3	102, 443, 4840
192.168.30.17	00:1B:1B:1E:7A:73	PLC (Siemens S7)	Siemens AG	0		H3-MO-SPS-ST 03	102
192.168.30.100	30:B8:51:1E:BF:AA	PLC (Siemens S7)	Siemens AG	0			102, 4840

Found in scan but NOT in CMDB (undocumented) - 3 devices

Note: check undocumented devices in the OT network (asset registration / segmentation, IEC 62443).

IP address	MAC address	Vendor	Device type	TCP ports	Risk
192.168.30.1	00:09:0F:1E:0A:A3	Fortinet	Network (FW/switch)	443	2
192.168.30.17	00:1B:1B:1E:7A:73	Siemens AG	PLC (Siemens S7)	102	0
192.168.30.26	00:1B:1B:1E:B9:E8	Siemens AG	PLC (Siemens S7)	80,5900,102	5

Only in firewall traffic (Splunk), not in scan - 2 devices

Splunk data 02.11.2026 - 08.11.2026. Yellow = device is probably present (search the network). New and affected CMDB rows are in the file "..._CMDB-Nachtrag.xlsx". Search help (MAC, partner) in the Excel sheet "Only in Splunk" (Nur in Splunk).

IP address	Assessment	Splunk ports	MAC / vendor	Last seen	CMDB
192.168.30.90	Present - outbound only	-	00:1B:1B:5A:0E:DE	2026-11-08	no
192.168.30.91	Present - outbound only	-	00:30:DE:5A:11:E9	2026-11-08	no

9 TECHNICAL DETAILS & APPENDIX

CRITICAL OPEN PORTS (OVERVIEW)

Port/Proto	Service (traffic rules)	Number of hosts	Risk assessment
80/tcp	HTTP	15	Medium (weight 2) - check
161/udp	SNMP (v1/v2c?)	10	Medium (weight 2) - check
23/tcp	Telnet	5	High (weight 3) - check first
21/tcp	FTP	2	High (weight 3) - check first
5900/tcp	VNC (RFB)	2	High (weight 3) - check first
135/tcp	RPC/EPMAP	2	Medium (weight 2) - check
445/tcp	SMB (check version)	2	High (weight 3) - check first

Traffic rules 1.0 for these services

HTTP - no login over HTTP / HTTPS recommended
HTTPS should be used; logging in (e.g. HTTP Basic) over unencrypted HTTP should not be used. Secure alternative: HTTPS (TCP 443) with current TLS (1.2 or newer).
SNMP - do not use (v1/v2c, public/private)
SNMPv1/v2c and default communities (public, private) should not be used. Secure alternative: SNMPv3 with authPriv (AES, SHA-2), read-only.
Telnet - do not use
Telnet should not be used; disable service and client. Secure alternative: SSH with public key login and current encryption.
FTP - do not use
Unencrypted FTP should not be used (insecure login, no encryption). Secure alternative: SFTP (preferred), FTPS or HTTPS; SCP only for legacy systems.
VNC - do not use (without TLS)
VNC without encryption should not be used and should never be directly reachable from other networks (across zone boundaries). Secure alternative: VNC with TLS or via SSH/VPN tunnel, preferably central remote access.
RPC/EPMAP - do not use (unless technically necessary)
RPC/EPMAP only if technically necessary - then only for approved internal systems, never across zone boundaries from other networks. Secure alternative: Kerberos, RPC encryption (PKT_PRIVACY), host firewall.
SMB - do not use (SMBv1, NTLMv1, LM)
SMBv1, NTLMv1 and LAN Manager should not be used; SMBv3 with signing should be used. Secure alternative: SMBv3 with Kerberos, signing and encryption.
Note: OTScan 3 assesses open ports. Version and login method (e.g. SMBv1/v3, SNMPv1/v3, LDAP with or without TLS, NFS with or without Kerberos) cannot be reliably determined from them and must be checked on the device.

NMAP SCAN ARGUMENTS

Montage_Anlagennetz_20261110_154840_stufenlauf:
(file not in output folder)

Montage_Anlagennetz_20261110_154840_stufenlauf.xml:
nmap -sS -sU -Pn -n -T2 --max-retries 3 --host-timeout 1800s --reason --open -sV --version-intensity 5 -O -p T:21,22,23,80,102,135,443,445,502,1200,2455,3389,4840,5900,8000,9600,44818,U:161,3671,9600,34964,47808 --script banner,http-server-header,http-title,ssl-cert,snmp-sysdescr,s7-info_robust,modbus-identity,codesys-v2-discover,knx-gateway-info,bacnet-info -oX <Ergebnisdatei> 192.168.30.0/24

10 ICS/OT GLOSSARY - PROTOCOLS & CLASSIFICATION

Ports were found in this scan that indicate the following OT protocols. The table explains each protocol and its security relevance:

Modbus / Modbus-TCP (502/TCP)

One of the oldest and most widespread OT protocols. Controls PLCs, sensors and actuators. No built-in authentication - anyone with network access can read and write.

Risk: HIGH - unauthenticated write access to controllers possible.

Siemens S7 / S7comm (102/TCP (ISO-TSAP))

Communication protocol for Siemens SIMATIC S7 PLCs. Program, configuration and process data are exchanged via port 102.

Risk: HIGH - reading of CPU type, firmware, serial number; on older CPUs manipulation is also possible.

CODESYS (1200/TCP, 2455/TCP) [IM SCAN GEFUNDEN]

Runtime environment for PLCs from many vendors (incl. Bosch Rexroth, WAGO, Beckhoff). Allows programming and control of the devices.

Risk: HIGH - older CODESYS V2 runtimes allow unauthenticated stopping/starting of the PLC.

OPC UA (4840/TCP) [IM SCAN GEFUNDEN]

Modern, platform-independent industrial standard for secure machine-to-machine communication. Supports encryption and authentication (if configured).

Risk: MEDIUM - can be configured securely, but often used without encryption.

EtherNet/IP (CIP) (44818/TCP, 2222/UDP)

Industrial protocol from Rockwell/Allen-Bradley (ODVA). Widespread in factory automation, based on the Common Industrial Protocol (CIP).

Risk: HIGH - device identification and sometimes configuration access without auth.

BACnet (47808/UDP)

Standard for building automation (HVAC, lighting, access). Found in heating, ventilation and air conditioning controls.

Risk: MEDIUM - reading of device and object information.

KNX / KNXnet-IP (3671/UDP)

European standard for building automation (often Weinzierl gateways). Controls lighting, blinds, heating.

Risk: MEDIUM - unauthenticated access to building functions possible.

DNP3 (20000/TCP+UDP)

Protocol for SCADA systems, mainly in energy supply and water management.

Risk: HIGH - critical infrastructure; often without authentication.

PROFINET (DCP (Layer 2), 34962-34964/UDP)

Real-time Ethernet standard from Siemens/PI for factory automation. Device discovery runs via Layer 2 broadcast (DCP).

Risk: MEDIUM - device names and IP assignment can be manipulated.

VxWorks (WDB) (17185/UDP)

Real-time operating system (Wind River) on many embedded OT devices. The WDB debug agent was historically a severe vulnerability.

Risk: HIGH - WDB agent allows memory access/code execution.

WHY DO SOME NSE SCRIPTS RETURN NO RESULTS?

An NSE script only returns results if the matching port on the target device is actually open. Empty results usually mean:

1. The port is closed or filtered (firewall). Example: if 's7-info' returns nothing, port 102 is not open on the device - so the device does not speak S7.

2. The device speaks a different protocol. Many OT devices (e.g. VxWorks embedded, printers, switches) use FTP/Telnet/SNMP instead of OT protocols such as Modbus or S7.

3. The device did not respond within the time limit (script/host timeout). Dead or very slow devices are skipped on purpose so the scan does not hang.

4. UDP protocols (BACnet, KNX, DNP3) only respond if the device is actively listening - no response here does not necessarily mean 'no device'.

So an empty NSE result is normally NOT a tool error but a correct statement: 'this protocol was not found on this device'.

TIP - Data collection (FORCE): The profile 'Fully comprehensive FORCE' uses the '+' prefix to force every script to run on EVERY open port, regardless of the normal port rule. This finds OT services on unusual ports too, but takes much longer and produces many empty attempts. Useful in the learning phase - afterwards, use the collected data to trim back to the scripts actually needed.

SOURCES & BASIS OF THE RISK ASSESSMENT

Every port assessment is tied to a stated source. OT/ICS protocols: framework IEC 62443 (zones and conduits) + technical port reference. Insecure IT protocols: traffic rules (HanselCraft default, customizable by the user). Weights and traffic light are a prioritization aid of this tool, not a requirement of the standard.

VR	Traffic rules 1.0 (HanselCraft default, as of 12.11.2026) - insecure IT protocols in OT networks; customizable by the user (verkehrsregeln.json)
IEC-62443	IEC 62443 - zones and conduits; foundational requirements incl. identification/authentication, data confidentiality, restricted data flow
IANA	IANA Service Name and Transport Protocol Port Number Registry
CISA	CISA ICS Advisory (incl. CVE-2025-7405: MODBUS/TCP without authentication)
ODVA	ODVA - EtherNet/IP (CIP) specification
ITI-PORTS	ITI/ICS-Security-Tools PORTS.md (ICS protocol port list)