OTScan 3

OT-/ICS-NETZWERKSCANNER · HANSELCRAFT

DEVICE DETAILS

Montage_Anlagennetz

Cards per device with firewall communication (zone · service · policy)

DEVICES	NETWORKS	CONNECTIONS	STATUS
24	1	5 per direction + all blocked	13.11.2026

How to read

Per device: details from the scan, name and location from the CMDB, and communication through the firewall from Splunk – per direction the 5 most frequent allowed connections and all blocked ones, each with source and destination zone, service, policy, action and count. Critical ports are written out in full with a plain-language explanation. Below the partner, where known, is the system or application from the documentation database.

	Risk 7–10: several critical ports and/or vendor advisory CVSS ≥ 7
	Risk 4–6
	Risk 1–3
	Risk 0: no critical ports
	only in firewall traffic (Splunk), not in scan

Montage_Anlagennetz · 24 devices · scan 10.11.2026 15:48 · Splunk 2026-11-02 – 2026-11-08

192.168.30.20 PLC (Schneider Modicon) | Schneider Electric | Risk: 8

MAC address:	00:00:54:1E:8F:9A	**Device type:**	PLC (Schneider Modicon)
Vendor:	Schneider Electric	**OS detection:**	–
Firmware:	V2.70	**UDP ports:**	161
TCP ports:	21,80,502	**Lastboot:**	–
CMDB name:	H3-MO-SPS-FT	**Location (CMDB):**	Halle 3, Fördertechnik Montage
Advisory:	SEVD-2021-313-05 (CVSS 9.8, quality model) +2	**Advisories:**	3
Critical ports:	**Port 21/TCP** – FTP: File transfer **Port 80/TCP** – HTTP: device web interface **Port 161/UDP** – SNMP: querying device data		

Firewall communication (Splunk)

Source · Zone	Destination · Zone	Port	Service	Policy	Action	Count
Firewall Inbound						
10.20.10.20 Z-Leitebene SCADA-01 · Prozessleitsystem	192.168.30.20 Z-Montage-Anlagennetz	502/6	MODBUS	31	accept	58.222
Firewall Outbound						
192.168.30.20 Z-Montage-Anlagennetz	10.20.10.30 Z-Infrastruktur NTP-01 · Zeitdienst und Protokollierung	123/17	NTP	12	accept	1.210

192.168.30.3 Network (firewall/switch) | Cisco Systems | Risk: 6

MAC address:	00:00:0C:1E:18:BD	**Device type:**	Network (firewall/switch)
Vendor:	Cisco Systems	**OS detection:**	Cisco IOS 17
Firmware:	17.9.4	**UDP ports:**	161
TCP ports:	22,443,23,80	**Lastboot:**	–
CMDB name:	H3-MO-SW-02	**Location (CMDB):**	Halle 3, Montagelinie 2, Schaltschrank +A1
Critical ports:	**Port 23/TCP** – Telnet: remote access to the command line **Port 80/TCP** – HTTP: device web interface **Port 161/UDP** – SNMP: querying device data		

Firewall communication (Splunk)

Source · Zone	Destination · Zone	Port	Service	Policy	Action	Count
Firewall Inbound						
no incoming connections during the Splunk period						
Firewall Outbound						
192.168.30.3 Z-Montage-Anlagennetz	10.20.10.40 Z-Infrastruktur SYSLOG-01 · Zeitdienst und Protokollierung	514/17	SYSLOG	14	accept	3.552
192.168.30.3 Z-Montage-Anlagennetz	10.20.10.30 Z-Infrastruktur NTP-01 · Zeitdienst und Protokollierung	123/17	NTP	12	accept	1.167

192.168.30.4 Network (firewall/switch) | Hirschmann Automation and Cont | Risk: 6

MAC address:	00:80:63:1E:1F:CA	**Device type:**	Network (firewall/switch)
Vendor:	Hirschmann Automation and Control GmbH	**OS detection:**	–
Firmware:	08.7.02	**UDP ports:**	161
TCP ports:	23,80	**Lastboot:**	–
CMDB name:	H3-MO-SW-03	**Location (CMDB):**	Halle 3, Montagelinie 3, Schaltschrank +A1
Critical ports:	**Port 23/TCP** – Telnet: remote access to the command line **Port 80/TCP** – HTTP: device web interface **Port 161/UDP** – SNMP: querying device data		

Firewall communication (Splunk)

Source · Zone	Destination · Zone	Port	Service	Policy	Action	Count
Firewall Inbound						
no incoming connections during the Splunk period						
Firewall Outbound						
192.168.30.4 Z-Montage-Anlagennetz	10.20.10.40 Z-Infrastruktur SYSLOG-01 · Zeitdienst und Protokollierung	514/17	SYSLOG	14	accept	3.366
192.168.30.4 Z-Montage-Anlagennetz	10.20.10.30 Z-Infrastruktur NTP-01 · Zeitdienst und Protokollierung	123/17	NTP	12	accept	1.870

192.168.30.10 PLC (Siemens S7) | Siemens AG | Risk: 6

MAC address:	00:1B:1B:1E:49:18	**Device type:**	PLC (Siemens S7)
Vendor:	Siemens AG	**OS detection:**	–
Firmware:	3.2.14	**UDP ports:**	161,34964
TCP ports:	80,102	**Lastboot:**	–
CMDB name:	H3-MO-SPS-L1	**Location (CMDB):**	Halle 3, Montagelinie 1
Advisory:	SSA-473245 (CVSS 7.5, quality exact) +10	**Advisories:**	11
Critical ports:	**Port 80/TCP** – HTTP: device web interface **Port 161/UDP** – SNMP: querying device data		

Firewall communication (Splunk)

Source · Zone	Destination · Zone	Port	Service	Policy	Action	Count
Firewall Inbound						
10.20.30.25 Z-Produktion MES-01 · MES Produktionsdaten	192.168.30.10 Z-Montage-Anlagennetz	102/6	S7	51	accept	103.421
10.20.30.26 Z-Engineering ENG-PG-01 · MES Produktionsdaten	192.168.30.10 Z-Montage-Anlagennetz	102/6	S7	53	accept	212
Firewall Outbound						
192.168.30.10 Z-Montage-Anlagennetz	10.20.10.30 Z-Infrastruktur NTP-01 · Zeitdienst und Protokollierung	123/17	NTP	12	accept	1.034

192.168.30.11 PLC (Siemens S7) | Siemens AG | Risk: 6

MAC address:	00:1B:1B:1E:50:25	**Device type:**	PLC (Siemens S7)
Vendor:	Siemens AG	**OS detection:**	–
Firmware:	3.2.15	**UDP ports:**	161,34964
TCP ports:	80,102	**Lastboot:**	–
CMDB name:	H3-MO-SPS-L2	**Location (CMDB):**	Halle 3, Montagelinie 2
Advisory:	SSA-473245 (CVSS 7.5, quality exact) +10	**Advisories:**	11
Critical ports:	**Port 80/TCP** – HTTP: device web interface **Port 161/UDP** – SNMP: querying device data		

Firewall communication (Splunk)

Source · Zone	Destination · Zone	Port	Service	Policy	Action	Count
Firewall Inbound						
10.20.30.25 Z-Produktion MES-01 · MES Produktionsdaten	192.168.30.11 Z-Montage-Anlagennetz	102/6	S7	51	accept	53.756
10.20.30.26 Z-Engineering ENG-PG-01 · MES Produktionsdaten	192.168.30.11 Z-Montage-Anlagennetz	102/6	S7	53	accept	123
Firewall Outbound						
192.168.30.11 Z-Montage-Anlagennetz	10.20.10.30 Z-Infrastruktur NTP-01 · Zeitdienst und Protokollierung	123/17	NTP	12	accept	1.860

192.168.30.25 PLC (Siemens S7) | Siemens AG | Risk: 6

MAC address:	00:1B:1B:1E:B2:DB	**Device type:**	PLC (Siemens S7)
Vendor:	Siemens AG	**OS detection:**	–
Firmware:	Siemens SIMATIC HMI web	**UDP ports:**	–
TCP ports:	80,5900,102	**Lastboot:**	–
CMDB name:	H3-MO-HMI-01	**Location (CMDB):**	Halle 3, Montagelinie 1, Bedienpult
Advisory:	SSA-941426 (CVSS 9.8, quality model) +9	**Advisories:**	10
Critical ports:	**Port 80/TCP** – HTTP: device web interface **Port 5900/TCP** – VNC: Remote screen control		

Firewall communication (Splunk)

Source · Zone	Destination · Zone	Port	Service	Policy	Action	Count
Firewall Inbound						
10.20.30.25 Z-Produktion MES-01 · MES Produktionsdaten	192.168.30.25 Z-Montage-Anlagennetz	102/6	S7	51	accept	105.986
10.20.30.26 Z-Engineering ENG-PG-01 · MES Produktionsdaten	192.168.30.25 Z-Montage-Anlagennetz	102/6	S7	53	accept	100
Blocked (incoming) – all 1 connection, 12 attempts						
10.20.30.26 Z-Engineering ENG-PG-01 · MES Produktionsdaten	192.168.30.25 Z-Montage-Anlagennetz	5900/6	VNC	0	deny	12
Firewall Outbound						
192.168.30.25 Z-Montage-Anlagennetz	10.20.10.30 Z-Infrastruktur NTP-01 · Zeitdienst und Protokollierung	123/17	NTP	12	accept	1.031

192.168.30.30 Unknown device | Moxa Technologies | Risk: 6

MAC address:	00:90:E8:1E:D5:1C	**Device type:**	Unknown device
Vendor:	Moxa Technologies	**OS detection:**	–
Firmware:	3.9	**UDP ports:**	161
TCP ports:	23,80	**Lastboot:**	–
CMDB name:	H3-MO-GW-01	**Location (CMDB):**	Halle 3, Montagelinie 2, Etikettendrucker seriell
Critical ports:	**Port 23/TCP** – Telnet: remote access to the command line **Port 80/TCP** – HTTP: device web interface **Port 161/UDP** – SNMP: querying device data		

Firewall communication (Splunk)

Source · Zone	Destination · Zone	Port	Service	Policy	Action	Count
Firewall Inbound						
no incoming connections during the Splunk period						
Firewall Outbound						
192.168.30.30 Z-Montage-Anlagennetz	10.20.10.30 Z-Infrastruktur NTP-01 · Zeitdienst und Protokollierung	123/17	NTP	12	accept	963

192.168.30.31 Unknown device | Moxa Technologies | Risk: 6

MAC address:	00:90:E8:1E:DC:29	**Device type:**	Unknown device
Vendor:	Moxa Technologies	**OS detection:**	–
Firmware:	3.9	**UDP ports:**	161
TCP ports:	23,80	**Lastboot:**	–
CMDB name:	H3-MO-GW-02	**Location (CMDB):**	Halle 3, Montagelinie 3, Waage seriell
Critical ports:	**Port 23/TCP** – Telnet: remote access to the command line **Port 80/TCP** – HTTP: device web interface **Port 161/UDP** – SNMP: querying device data		

Firewall communication (Splunk)

Source · Zone	Destination · Zone	Port	Service	Policy	Action	Count
Firewall Inbound						
no incoming connections during the Splunk period						
Firewall Outbound						
192.168.30.31 Z-Montage-Anlagennetz	10.20.10.30 Z-Infrastruktur NTP-01 · Zeitdienst und Protokollierung	123/17	NTP	12	accept	1.451

192.168.30.102 Network (firewall/switch) | Hirschmann Automation and Cont | Risk: 6

MAC address:	64:60:38:1E:CD:C4	**Device type:**	Network (firewall/switch)
Vendor:	Hirschmann Automation and Control GmbH	**OS detection:**	–
Firmware:	–	**UDP ports:**	161
TCP ports:	23,80	**Lastboot:**	–
CMDB name:	H3-MO-GER-52	**Location (CMDB):**	Halle 3, Montagelinie 3
Critical ports:	**Port 23/TCP** – Telnet: remote access to the command line **Port 80/TCP** – HTTP: device web interface **Port 161/UDP** – SNMP: querying device data		

Firewall communication (Splunk)

Source · Zone	Destination · Zone	Port	Service	Policy	Action	Count
Firewall Inbound						
no incoming connections during the Splunk period						
Firewall Outbound						
192.168.30.102 Z-Montage-Anlagennetz	10.20.10.30 Z-Infrastruktur NTP-01 · Zeitdienst und Protokollierung	123/17	NTP	12	accept	1.099

192.168.30.2 Network (Siemens SCALANCE) | Siemens AG | Risk: 4

MAC address:	00:0E:8C:1E:11:B0	**Device type:**	Network (Siemens SCALANCE)
Vendor:	Siemens AG	**OS detection:**	–
Firmware:	V4.3	**UDP ports:**	161
TCP ports:	22,443	**Lastboot:**	–
CMDB name:	H3-MO-SW-01	**Location (CMDB):**	Halle 3, Montagelinie 1, Schaltschrank +A1
Advisory:	SSA-699386 (CVSS 9.1, quality exact) +6	**Advisories:**	7
Critical ports:	**Port 161/UDP** – SNMP: querying device data		

Firewall communication (Splunk)

Source · Zone	Destination · Zone	Port	Service	Policy	Action	Count
Firewall Inbound						
no incoming connections during the Splunk period						
Firewall Outbound						
192.168.30.2 Z-Montage-Anlagennetz	10.20.10.40 Z-Infrastruktur SYSLOG-01 · Zeitdienst und Protokollierung	514/17	SYSLOG	14	accept	2.827
192.168.30.2 Z-Montage-Anlagennetz	10.20.10.30 Z-Infrastruktur NTP-01 · Zeitdienst und Protokollierung	123/17	NTP	12	accept	1.387

192.168.30.15 PLC (Siemens S7) | Siemens AG | Risk: 4

MAC address:	00:1B:1B:1E:6C:59	**Device type:**	PLC (Siemens S7)
Vendor:	Siemens AG	**OS detection:**	–
Firmware:	4.2.3	**UDP ports:**	–
TCP ports:	102,80,443	**Lastboot:**	–
CMDB name:	H3-MO-SPS-ST01	**Location (CMDB):**	Halle 3, Schraubstation
Advisory:	SSA-712929 (CVSS 7.5, quality exact) +8	**Advisories:**	9
Critical ports:	**Port 80/TCP** – HTTP: device web interface		

Firewall communication (Splunk)

Source · Zone	Destination · Zone	Port	Service	Policy	Action	Count
Firewall Inbound						
10.20.30.25 Z-Produktion MES-01 · MES Produktionsdaten	192.168.30.15 Z-Montage-Anlagennetz	102/6	S7	51	accept	77.672
10.20.30.26 Z-Engineering ENG-PG-01 · MES Produktionsdaten	192.168.30.15 Z-Montage-Anlagennetz	102/6	S7	53	accept	176
Firewall Outbound						
192.168.30.15 Z-Montage-Anlagennetz	10.20.10.30 Z-Infrastruktur NTP-01 · Zeitdienst und Protokollierung	123/17	NTP	12	accept	1.863

192.168.30.16 PLC (Siemens S7) | Siemens AG | Risk: 4

MAC address:	00:1B:1B:1E:73:66	**Device type:**	PLC (Siemens S7)
Vendor:	Siemens AG	**OS detection:**	–
Firmware:	4.5.2	**UDP ports:**	–
TCP ports:	102,80,443	**Lastboot:**	–
CMDB name:	H3-MO-SPS-ST02	**Location (CMDB):**	Halle 3, Klebestation
Advisory:	SSA-712929 (CVSS 7.5, quality exact) +4	**Advisories:**	5
Critical ports:	**Port 80/TCP** – HTTP: device web interface		

Firewall communication (Splunk)

Source · Zone	Destination · Zone	Port	Service	Policy	Action	Count
Firewall Inbound						
10.20.30.25 Z-Produktion MES-01 · MES Produktionsdaten	192.168.30.16 Z-Montage-Anlagennetz	102/6	S7	51	accept	58.317
10.20.30.26 Z-Engineering ENG-PG-01 · MES Produktionsdaten	192.168.30.16 Z-Montage-Anlagennetz	102/6	S7	53	accept	287
Firewall Outbound						
192.168.30.16 Z-Montage-Anlagennetz	10.20.10.30 Z-Infrastruktur NTP-01 · Zeitdienst und Protokollierung	123/17	NTP	12	accept	2.025

192.168.30.21 PLC (Rockwell/Allen-Bradley) | OMRON Corporation | Risk: 4

MAC address:	00:00:0A:1E:96:A7	**Device type:**	PLC (Rockwell/Allen-Bradley)
Vendor:	OMRON Corporation	**OS detection:**	–
Firmware:	OMRON NX1P2 web	**UDP ports:**	9600
TCP ports:	80,9600,44818	**Lastboot:**	–
CMDB name:	H3-MO-SPS-ZU	**Location (CMDB):**	Halle 3, Zuführung Kleinteile
Advisory:	ICSA-19-346-02 (CVSS 8.6, quality model)	**Advisories:**	1
Critical ports:	**Port 80/TCP** – HTTP: device web interface		

Firewall communication (Splunk)

Source · Zone	Destination · Zone	Port	Service	Policy	Action	Count
Firewall Inbound						
10.20.10.20 Z-Leitebene SCADA-01 · Prozessleitsystem	192.168.30.21 Z-Montage-Anlagennetz	9600/17	OMRON-FINS	35	accept	21.379
Firewall Outbound						
192.168.30.21 Z-Montage-Anlagennetz	10.20.10.30 Z-Infrastruktur NTP-01 · Zeitdienst und Protokollierung	123/17	NTP	12	accept	1.971

192.168.30.22 PLC (Phoenix/WAGO) | Wago Kontakttechnik GmbH | Risk: 4

MAC address:	00:30:DE:1E:9D:B4	**Device type:**	PLC (Phoenix/WAGO)
Vendor:	Wago Kontakttechnik GmbH	**OS detection:**	Linux 4.x
Firmware:	vsftpd 3.0.5	**UDP ports:**	–
TCP ports:	21,22,80,443,502,2455	**Lastboot:**	–
CMDB name:	H3-MO-AS-01	**Location (CMDB):**	Halle 3, Montagelinie 1, Hilfsantriebe
Critical ports:	**Port 21/TCP** – FTP: File transfer **Port 80/TCP** – HTTP: device web interface		

Firewall communication (Splunk)

Source · Zone	Destination · Zone	Port	Service	Policy	Action	Count
Firewall Inbound						
10.20.10.20 Z-Leitebene SCADA-01 · Prozessleitsystem	192.168.30.22 Z-Montage-Anlagennetz	502/6	MODBUS	31	accept	40.473
Blocked (incoming) – all 1 connection, 6 attempts						
10.20.30.26 Z-Engineering ENG-PG-01 · MES Produktionsdaten	192.168.30.22 Z-Montage-Anlagennetz	21/6	FTP	0	deny	6
Firewall Outbound						
192.168.30.22 Z-Montage-Anlagennetz	10.20.10.30 Z-Infrastruktur NTP-01 · Zeitdienst und Protokollierung	123/17	NTP	12	accept	931

192.168.30.26 PLC (Siemens S7) | Siemens AG | Risk: 4

MAC address:	00:1B:1B:1E:B9:E8	**Device type:**	PLC (Siemens S7)
Vendor:	Siemens AG	**OS detection:**	–
Firmware:	Siemens SIMATIC HMI web	**UDP ports:**	–
TCP ports:	80,5900,102	**Lastboot:**	–
CMDB name:	– not in CMDB –	**Location (CMDB):**	–
Critical ports:	**Port 80/TCP** – HTTP: device web interface **Port 5900/TCP** – VNC: Remote screen control		

Firewall communication (Splunk)

Source · Zone	Destination · Zone	Port	Service	Policy	Action	Count
Firewall Inbound						
10.20.30.25 Z-Produktion MES-01 · MES Produktionsdaten	192.168.30.26 Z-Montage-Anlagennetz	102/6	S7	51	accept	55.890
10.20.30.26 Z-Engineering ENG-PG-01 · MES Produktionsdaten	192.168.30.26 Z-Montage-Anlagennetz	102/6	S7	53	accept	209
Firewall Outbound						
192.168.30.26 Z-Montage-Anlagennetz	10.20.10.30 Z-Infrastruktur NTP-01 · Zeitdienst und Protokollierung	123/17	NTP	12	accept	987

192.168.30.60 Windows PC / workstation | Fujitsu Technology Solutions G | Risk: 4

MAC address:	00:19:99:1E:A7:A2	**Device type:**	Windows PC / workstation
Vendor:	Fujitsu Technology Solutions GmbH	**OS detection:**	Microsoft Windows 10
Firmware:	Microsoft Windows RPC	**UDP ports:**	–
TCP ports:	135,445,3389	**Lastboot:**	–
CMDB name:	H3-MO-ENG-01	**Location (CMDB):**	Halle 3, Meisterbüro Montage
Critical ports:	**Port 135/TCP** – RPC: Windows remote control service **Port 445/TCP** – SMB: Windows file sharing		

Firewall communication (Splunk)

Source · Zone	Destination · Zone	Port	Service	Policy	Action	Count
Firewall Inbound						
10.20.70.8 Z-DMZ FERNWARTUNG-01 · Fernwartung	192.168.30.60 Z-Montage-Anlagennetz	3389/6	RDP	71	accept	61
Firewall Outbound						
192.168.30.60 Z-Montage-Anlagennetz	10.20.10.30 Z-Infrastruktur NTP-01 · Zeitdienst und Protokollierung	123/17	NTP	12	accept	1.693
192.168.30.60 Z-Montage-Anlagennetz	10.20.50.5 Z-Infrastruktur WSUS-01 · Zeitdienst und Protokollierung	443/6	HTTPS	16	accept	1.262

192.168.30.61 Windows PC / workstation | Fujitsu Technology Solutions G | Risk: 4

MAC address:	00:19:99:1E:AE:AF	**Device type:**	Windows PC / workstation
Vendor:	Fujitsu Technology Solutions GmbH	**OS detection:**	Microsoft Windows 10
Firmware:	Microsoft Windows RPC	**UDP ports:**	–
TCP ports:	135,445	**Lastboot:**	–
CMDB name:	H3-MO-BED-01	**Location (CMDB):**	Halle 3, Linienleitstand Montage
Critical ports:	**Port 135/TCP** – RPC: Windows remote control service **Port 445/TCP** – SMB: Windows file sharing		

Firewall communication (Splunk)

Source · Zone	Destination · Zone	Port	Service	Policy	Action	Count
Firewall Inbound						
no incoming connections during the Splunk period						
Firewall Outbound						
192.168.30.61 Z-Montage-Anlagennetz	10.20.10.30 Z-Infrastruktur NTP-01 · Zeitdienst und Protokollierung	123/17	NTP	12	accept	1.774
192.168.30.61 Z-Montage-Anlagennetz	10.20.50.5 Z-Infrastruktur WSUS-01 · Zeitdienst und Protokollierung	443/6	HTTPS	16	accept	1.190

192.168.30.101 PLC (Siemens S7) | Siemens AG, Automations & Driv | Risk: 4

MAC address:	30:13:89:1E:C6:B7	**Device type:**	PLC (Siemens S7)
Vendor:	Siemens AG, Automations & Drives,	**OS detection:**	–
Firmware:	–	**UDP ports:**	–
TCP ports:	80,102,443	**Lastboot:**	–
CMDB name:	H3-MO-SPS-51	**Location (CMDB):**	Halle 3, Montagelinie 2
Advisory:	SSA-001536 (CVSS 10.0, quality vendor) +26	**Advisories:**	27
Critical ports:	**Port 80/TCP** – HTTP: device web interface		

Firewall communication (Splunk)

Source · Zone	Destination · Zone	Port	Service	Policy	Action	Count
Firewall Inbound						
10.20.30.25 Z-Produktion MES-01 · MES Produktionsdaten	192.168.30.101 Z-Montage-Anlagennetz	102/6	S7	51	accept	60.088
10.20.30.26 Z-Engineering ENG-PG-01 · MES Produktionsdaten	192.168.30.101 Z-Montage-Anlagennetz	102/6	S7	53	accept	56
Firewall Outbound						
192.168.30.101 Z-Montage-Anlagennetz	10.20.10.30 Z-Infrastruktur NTP-01 · Zeitdienst und Protokollierung	123/17	NTP	12	accept	1.174

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

MAC address:	00:09:0F:1E:0A:A3	**Device type:**	Network (firewall/switch)
Vendor:	Fortinet	**OS detection:**	FortiOS 7.2
Firmware:	Fortinet FortiGate httpd	**UDP ports:**	161
TCP ports:	443	**Lastboot:**	–
CMDB name:	– not in CMDB –	**Location (CMDB):**	–
Critical ports:	**Port 161/UDP** – SNMP: querying device data		

Firewall communication (Splunk)

No traffic through the firewall during the Splunk period.

192.168.30.12 PLC (Siemens S7) | Siemens AG | Risk: 2

MAC address:	00:1B:1B:1E:57:32	**Device type:**	PLC (Siemens S7)
Vendor:	Siemens AG	**OS detection:**	–
Firmware:	2.9.4	**UDP ports:**	–
TCP ports:	102,443,4840	**Lastboot:**	–
CMDB name:	H3-MO-SPS-L3	**Location (CMDB):**	Halle 3, Montagelinie 3
Advisory:	SSA-452276 (CVSS 9.6, quality exact) +15	**Advisories:**	16

Firewall communication (Splunk)

Source · Zone	Destination · Zone	Port	Service	Policy	Action	Count
Firewall Inbound						
10.20.30.25 Z-Produktion MES-01 · MES Produktionsdaten	192.168.30.12 Z-Montage-Anlagennetz	102/6	S7	51	accept	92.780
10.20.30.25 Z-Produktion MES-01 · MES Produktionsdaten	192.168.30.12 Z-Montage-Anlagennetz	4840/6	OPC-UA	52	accept	82.270
10.20.30.26 Z-Engineering ENG-PG-01 · MES Produktionsdaten	192.168.30.12 Z-Montage-Anlagennetz	102/6	S7	53	accept	93
Firewall Outbound						
192.168.30.12 Z-Montage-Anlagennetz	10.20.10.30 Z-Infrastruktur NTP-01 · Zeitdienst und Protokollierung	123/17	NTP	12	accept	1.379

192.168.30.17 PLC (Siemens S7) | Siemens AG | Risk: 2

MAC address:	00:1B:1B:1E:7A:73	**Device type:**	PLC (Siemens S7)
Vendor:	Siemens AG	**OS detection:**	–
Firmware:	4.4.1	**UDP ports:**	–
TCP ports:	102	**Lastboot:**	–
CMDB name:	– not in CMDB –	**Location (CMDB):**	–
Advisory:	SSA-712929 (CVSS 7.5, quality exact) +6	**Advisories:**	7

Firewall communication (Splunk)

Source · Zone	Destination · Zone	Port	Service	Policy	Action	Count
Firewall Inbound						
10.20.30.25 Z-Produktion MES-01 · MES Produktionsdaten	192.168.30.17 Z-Montage-Anlagennetz	102/6	S7	51	accept	58.730
10.20.30.25 Z-Produktion MES-01 · MES Produktionsdaten	192.168.30.17 Z-Montage-Anlagennetz	102/6	S7	51	ip-conn	312
10.20.30.26 Z-Engineering ENG-PG-01 · MES Produktionsdaten	192.168.30.17 Z-Montage-Anlagennetz	102/6	S7	53	accept	117
Firewall Outbound						
192.168.30.17 Z-Montage-Anlagennetz	10.20.10.30 Z-Infrastruktur NTP-01 · Zeitdienst und Protokollierung	123/17	NTP	12	accept	1.208

192.168.30.100 PLC (Siemens S7) | Siemens AG | Risk: 0

MAC address:	30:B8:51:1E:BF:AA	**Device type:**	PLC (Siemens S7)
Vendor:	Siemens AG	**OS detection:**	–
Firmware:	–	**UDP ports:**	–
TCP ports:	102,4840	**Lastboot:**	–
CMDB name:	H3-MO-SPS-50	**Location (CMDB):**	Halle 3, Montagelinie 1

Firewall communication (Splunk)

Source · Zone	Destination · Zone	Port	Service	Policy	Action	Count
Firewall Inbound						
10.20.30.25 Z-Produktion MES-01 · MES Produktionsdaten	192.168.30.100 Z-Montage-Anlagennetz	102/6	S7	51	accept	86.578
10.20.30.25 Z-Produktion MES-01 · MES Produktionsdaten	192.168.30.100 Z-Montage-Anlagennetz	4840/6	OPC-UA	52	accept	69.065
10.20.30.26 Z-Engineering ENG-PG-01 · MES Produktionsdaten	192.168.30.100 Z-Montage-Anlagennetz	102/6	S7	53	accept	58
Firewall Outbound						
192.168.30.100 Z-Montage-Anlagennetz	10.20.10.30 Z-Infrastruktur NTP-01 · Zeitdienst und Protokollierung	123/17	NTP	12	accept	2.081

192.168.30.90 unknown | Siemens AG | firewall traffic only

MAC address:	00:1B:1B:5A:0E:DE	**Device type:**	unknown
Vendor:	Siemens AG	**OS detection:**	–
Firmware:	–	**UDP ports:**	–
TCP ports:	–	**Lastboot:**	–
CMDB name:	– not in CMDB –	**Location (CMDB):**	–

Firewall communication (Splunk)

Source · Zone	Destination · Zone	Port	Service	Policy	Action	Count
Firewall Inbound						
no incoming connections during the Splunk period						
Firewall Outbound						
192.168.30.90 Z-Montage-Anlagennetz	10.20.30.25 Z-Produktion MES-01 · MES Produktionsdaten	102/6	S7	51	accept	22.140

192.168.30.91 unknown | Wago Kontakttechnik GmbH | firewall traffic only

MAC address:	00:30:DE:5A:11:E9	**Device type:**	unknown
Vendor:	Wago Kontakttechnik GmbH	**OS detection:**	–
Firmware:	–	**UDP ports:**	–
TCP ports:	–	**Lastboot:**	–
CMDB name:	– not in CMDB –	**Location (CMDB):**	–

Firewall communication (Splunk)

Source · Zone	Destination · Zone	Port	Service	Policy	Action	Count
Firewall Inbound						
no incoming connections during the Splunk period						
Firewall Outbound						
192.168.30.91 Z-Montage-Anlagennetz	10.20.10.20 Z-Leitebene SCADA-01 · Prozessleitsystem	502/6	MODBUS	31	accept	15.880