BERICHT

Kommunikation, Steuerungs- und Schutzkonzept

Fertigung Maschinenbau: Zonen, Kommunikationsmatrix, Protokolle, Sicherheitsfunktionen, SPS-Programme, Datenflüsse

Auftraggeber	[Betreiber, Ort]
Projekt	Maschinenbau, OT-Konzept
Version	0.1 Entwurf
Datum	04.11.2026
Autor	Maximilian Gilg, OT-Cyber.de
Klassifizierung	TLP:CLEAR – Veröffentlichung, fiktive Demonstrationsanlage

Dieses Dokument enthält vertrauliche Informationen über die Sicherheitslage der betrachteten Anlagen. Weitergabe, Vervielfältigung oder Veröffentlichung nur mit Zustimmung des Auftraggebers.

Dokumentinformationen

VERSIONSHISTORIE

Version	Datum	Autor	Änderung
0.1	04.11.2026	M. Gilg	Erstentwurf

VERTEILER

Name	Organisation	Rolle
[Name]	[Auftraggeber]	Geschäftsführung
[Name]	[Auftraggeber]	Technische Leitung, Betriebsleitung

Inhalt

1 Architektur

2 Zonen und Segmente

3 Kommunikationsmatrix

4 Protokolle und ihre Absicherung

5 Sicherheitsfunktionen

6 SPS-Programme

7 Datenflüsse der Fertigung

1 Architektur

Die Fertigung gliedert sich in eine Leitebene mit MES, Programm- und Werkzeugverwaltung, Industrial Edge und Lagerverwaltung sowie in Zellen für Zerspanung, Blech, Additiv, Messraum, Lager, fahrerlose Transportfahrzeuge und Versorgung. Jede Zelle liegt hinter einer SCALANCE SC646-2C. Die IT mit ERP und CAD/CAM erreicht die Fertigung nur über die DMZ.

- **NC-Programme:** CAM legt freigegebene Programme im NC-Gateway der DMZ ab; die Programmverwaltung holt sie dort ab und überträgt sie an die Bedientafeln.
- **Maschinendaten:** OPC UA nach umati von den SINUMERIK-Steuerungen an MES und Edge.
- **Fernwartung:** zentral über SINEMA Remote Connect mit Freigabe; an BAZ-05, BAZ-06, LS-01 und den 3D-Druckern hängen zusätzlich Router der Hersteller mit eigenem Internetzugang. Sie umgehen die Firewall, bis sie entfernt oder hinter die Firewall gelegt sind.
- **Transportfahrzeuge:** VDA 5050 über MQTT mit TLS im Industrie-WLAN, Personenschutz durch Sicherheitslaserscanner in jedem Fahrzeug.

2 Zonen und Segmente

Zone	Bezeichnung	SL-T	Segmente (Stufe 2)
Z01	IT	-	ein Segment
Z02	Internet, Lieferanten	-	ein Segment
Z03	DMZ	3	Jump-Host; Fernwartungsgateway; NC-Gateway; Dienste; OEM-Router
Z04	Fertigungsleitebene	3	MES; Programmverwaltung; Werkzeuge, Edge; Lagerverwaltung; Meisterplätze
Z05	Engineering	3	Engineering SPS; Service CNC
Z06	OT-Management	3	ein Segment
Z07	Zelle Zerspanung	2	BAZ-01; BAZ-02; BAZ-03; BAZ-04; BAZ-05; BAZ-06; DZ-01; DZ-02; DZ-03; SG-01; Voreinstellgerät
Z08	Zelle Blech	2	LS-01; AP-01
Z09	Zelle Additiv	2	AM-01; AM-02; Pulverstation
Z10	Zelle Messraum	2	KMG-01
Z11	Zelle Lager	2	Lagersteuerung; Regalbediengeräte; Kleinteilelager
Z12	Zelle FTS	2	Flottenmanager; Fahrzeuge; Access Points
Z13	Zelle Versorgung	2	Versorgung; Kompressoren
Z14	Gebäudeleittechnik	2	Vision Center; Automationsstationen
Z15	Sicherheitsfunktionen	hart verdrahtet	ein Segment
Z16	Gebäudesicherheit	2	ein Segment

Zone	Bezeichnung	SL-T	Segmente (Stufe 2)
Z18	Temporär verbundene Geräte	2	ein Segment

Stufe 1 trennt Zonen mit Firewall und Zellenfirewalls. Stufe 2 trennt jede Werkzeugmaschine in ein eigenes Segment: Programmverwaltung nur zu den Bedientafeln, Server nur lesend per OPC UA, Service nur von der Service-Station.

3 Kommunikationsmatrix

Erlaubt ist nur, was eine Regel ausdrücklich zulässt. Spalte Stufe: Z gilt in der Zonenstufe, M in der Mikrosegmentierung. Lange Gerätelisten sind gekürzt.

Regel	Quelle	Ziel	Dienst	Zweck	Stufe
R01	CAD/CAM-Arbeitsplatz Konstruktion (IT)	NC-Programm-Gateway (IT zu OT)	SMB (TCP 445)	CAM legt freigegebene NC-Programme im Gateway ab	Z, M
R02	Programmverwaltung NC (DNC)	NC-Programm-Gateway (IT zu OT)	SMB (TCP 445)	Programmverwaltung holt Programme aus dem Gateway	Z, M
R03	Programmverwaltung NC (DNC)	Z07, Z08	SMB (TCP 445)	Programmverwaltung zu den Maschinen	Z
R04	Programmverwaltung NC (DNC)	Bedientafel BAZ-01 (IPC, Windows), Bedientafel BAZ-02 (IPC, Window …	SMB (TCP 445)	nur zu den Bedientafeln, nicht zur NCU	M
R05	Z04	Z07, Z08, Z09, Z10	OPCUA (TCP 4840)	MES, Edge, Werkzeugverwaltung lesen Maschinendaten (umati)	Z
R06	MES-Server Opcenter, Industrial Edge, Werkzeugverwaltung	NCU BAZ-01, NCU BAZ-02, NCU BAZ-03, NCU BAZ-04, NCU BAZ-05, NCU BA …	OPCUA (TCP 4840)	nur Server zu den Maschinen	M
R07	Messrechner KMG-01 (Windows)	MES-Server Opcenter	HTTPS (TCP 443)	Messprotokolle an das MES	Z, M
R08	Werkzeugvoreinstellgerät	Werkzeugverwaltung	HTTPS (TCP 443)	Werkzeugmaße an die Werkzeugverwaltung	Z, M
R09	LVS und Materialflussrechner	Steuerung Lager AS-LAG, Shuttle-Steuerung AKL Gasse 1, Shuttle-Ste …	TEL (TCP 2000)	Fahraufträge an Lagersteuerung und Shuttles	Z, M
R10	Steuerung Lager AS-LAG	Steuerung RBG-1 (F-CPU), Steuerung RBG-2 (F-CPU)	S7 (TCP 102)	Lagersteuerung an die Regalbediengeräte	M
R11	LVS und Materialflussrechner	Flottenmanager FTS	HTTPS (TCP 443)	Transportaufträge an den Flottenmanager	Z, M
R12	Flottenmanager FTS	Transportfahrzeug AGV-1, Transportfahrzeug AGV-2, Transportfahrzeu …	MQTT (TCP 8883)	VDA 5050: Aufträge an die Fahrzeuge	Z, M

Regel	Quelle	Ziel	Dienst	Zweck	Stufe
R13	Transportfahrzeug AGV-1, Transportfahrzeug AGV-2, Transportfahrzeu …	Flottenmanager FTS	MQTT (TCP 8883)	VDA 5050: Zustand der Fahrzeuge	Z, M
R14	ERP-Server (IT)	MES-Server Opcenter, LVS und Materialflussrechner	HTTPS (TCP 443)	Aufträge und Material aus dem ERP	Z, M
R15	Meisterarbeitsplatz 1, Fertigungsleitstand Großbild	MES-Server Opcenter, LVS und Materialflussrechner	HTTPS (TCP 443)	Meisterplätze zu MES und LVS	M
R16	Engineering-Station TIA Portal	Z09, Z11, Z13	S7 (TCP 102)	Engineering SPS	Z
R17	Engineering-Station TIA Portal	Steuerung Lager AS-LAG, Steuerung RBG-1 (F-CPU), Steuerung RBG-2 (…	S7 (TCP 102)	Engineering SPS	M
R18	Service-Station SINUMERIK	Z07	S7 (TCP 102)	Service SINUMERIK	Z
R19	Service-Station SINUMERIK	NCU BAZ-01, NCU BAZ-02, NCU BAZ-03, NCU BAZ-04, NCU BAZ-05, NCU BA …	S7 (TCP 102)	Service SINUMERIK	M
R20	Jump-Host	Z04, Z05	RDP (TCP 3389)	Administration über den Jump-Host	Z, M
R21	Fernservice Werkzeugmaschinenhersteller, Fernservice Blechmaschine …	Fernwartungsgateway SINEMA RC	VPN (UDP 1194)	Herstellerfernwartung über SINEMA RC	Z, M
R22	Fernwartungsgateway SINEMA RC	Bedientafel BAZ-01 (IPC, Windows), Bedientafel BAZ-02 (IPC, Window …	VNC (TCP 5900)	Fernbedienung nach Freigabe	Z, M
R23	Steuerung Versorgung AS-VS	Kompressor K-01, Kompressor K-02	MODBUS (TCP 502)	Versorgung liest Kompressoren	Z, M
R24	MES-Server Opcenter	Steuerung Versorgung AS-VS	OPCUA (TCP 4840)	Energie- und Verbrauchsdaten	Z, M
R25	Sauter modulo 6 Halle, Sauter modulo 6 Messraum, Sauter modulo 6 B …	Sauter Vision Center	BACNET (UDP 47808)	Automationsstationen zum Vision Center	Z, M

Regel	Quelle	Ziel	Dienst	Zweck	Stufe
R26	Sauter Vision Center	MES-Server Opcenter	HTTPS (TCP 443)	Messraumklima an das MES (Freigabe Messprotokolle)	Z, M
R27	WLAN-Controller	Access Point WLAN 1, Access Point WLAN 2, Access Point WLAN 3, Acc …	CAPWAP (UDP 5246)	WLAN-Controller zu den Access Points	Z, M
R28	OT-Monitoring, Zeitserver, Firewall OT	alle	MGMT (UDP 161)	Zeit, Überwachung, Verwaltung	Z, M

4 Protokolle und ihre Absicherung

Protokoll	Einsatz	Absicherung
OPC UA (umati)	Maschinendaten an MES, Edge, Werkzeugverwaltung	SignAndEncrypt, Zertifikate, nur lesende Rechte
SMB	NC-Programme CAM zum Gateway, Programmverwaltung zu den Bedientafeln	SMB 3 mit Signatur, Freigabe-Workflow, keine Schreibrechte von der Maschine zurück
S7 mit TLS	Engineering der S7-1500, Service der SINUMERIK	TLS ab Firmware V3.1, Zugriffsschutz, nur von den Engineering-Stationen
Telegramme TCP	Lagerverwaltung zur Lagersteuerung	nur feste Partner, Plausibilisierung der Aufträge in der SPS
MQTT mit TLS (VDA 5050)	Flottenmanager und Fahrzeuge	Zertifikate je Fahrzeug, WLAN mit WPA3-Enterprise
VPN, VNC	Herstellerfernwartung	SINEMA RC mit Freigabe je Sitzung; Herstellerrouter entfernen
Modbus/TCP	Kompressoren	nur lesend
BACnet/IP	Gebäudeleittechnik Sauter	eigene Zone; BACnet Secure Connect prüfen
PROFINET, PROFIsafe	Antriebe, E/A, Sicherheit	nur innerhalb der Zelle, Port Security
RDP, HTTPS	Administration, Bedienung	Jump-Host, MFA

5 Sicherheitsfunktionen

Die folgenden Funktionen schützen Menschen und Maschinen. Sie bleiben wirksam, wenn MES, Lagerverwaltung oder Netz gestört oder manipuliert sind.

Funktion	Auslöser	Wirkung	Ausführung
Sichere Geschwindigkeit, Türzuhaltung	Tür offen, Einrichtbetrieb	Spindel und Achsen sicher begrenzt bzw. Stillstand	SINUMERIK Safety Integrated
Not-Halt	Taster an Maschine, Roboter, Lager	Stillsetzen Kategorie 0 bzw. 1	hart, PROFIsafe
Lichtvorhang Abkantpresse	Hand im Schutzfeld	Stopp der Presse	Sicherheitssteuerung der Presse
Gassenabsicherung RBG	Wartungstür, Lichtgitter	RBG sicher still	F-Programm RBG
Personenschutz FTS	Person im Schutzfeld	Fahrzeug bremst bzw. hält	Sicherheitslaserscanner
Laserschutz	Kabine offen	Laser aus	Sicherheitskreis der Anlage
Sauerstoffmangel	O2 im Raum zu niedrig	Alarm, Lüftung, Argon zu	hart verdrahtet
Explosionsschutz Pulver	Pulverhandling	Inertisierung, Erdung, Zone 22	Anlagentechnik, organisatorisch

6 SPS-Programme

Baustein	Steuerung	Funktion
FB_Lagerauftrag_Pruefung	AS-LAG	Fachnummer, Gewicht, Kontur, Doppelbelegung, höchstens 60 Aufträge je Minute
FB_FTS_Uebergabe	AS-LAG	Übergabe nur bei angedocktem und freigegebenem Fahrzeug, Zeitüberwachung
FB_RBG_Gassenfreigabe	RBG-1/2	Standardseitige Freigabe; Sicherheitsabschaltung im F-Programm
FB_KSS_Ueberwachung	AS-VS	Konzentration 4 bis 9 % fest, pH, Temperatur
FB_Druckluft_Folge	AS-VS	Führung nach Betriebsstunden, Leckagealarm außerhalb der Schicht
FB_Argon_Versorgung	AS-VS	Freigabe der Drucker nur bei Argondruck und ohne O2-Alarm

Die Programme liegen als Maschinenbau_SPS_Programme.scl bei. Die Steuerungen der Werkzeugmaschinen und der Herstelleranlagen gehören zum Lieferumfang der Maschinenhersteller.

7 Datenflüsse der Fertigung

- **Auftrag:** ERP an MES und LVS; MES plant fein, LVS lagert aus, Flottenmanager fährt das Material an die Maschine.
- **Programm:** CAM über NC-Gateway an die Programmverwaltung, von dort mit Freigabe an die Bedientafel.
- **Qualität:** Messrechner schickt Messprotokolle an das MES; das MES gibt sie nur frei, wenn die Gebäudeleittechnik den Messraum im Toleranzband meldet.
- **Werkzeuge:** Voreinstellgerät an die Werkzeugverwaltung, von dort per OPC UA an die Maschine.