BERICHT

Risikobewertung nach IEC 62443-3-2

Hartkäserei im Bestand, Planungsstand Index C

Auftraggeber	[Betreiber, Ort]
Projekt	Maschinenbau, OT-Sicherheitskonzept
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 Management Summary

2 System under Consideration (ZCR 1)

3 Risikokriterien

4 Erste Risikobewertung (ZCR 2)

5 Zonen, Conduits, Mikrosegmente (ZCR 3)

6 Detaillierte Risikobewertung (ZCR 5)

7 Ziel-Security-Level

8 Vergleich mit den Fähigkeiten (ZCR 4)

9 Anforderungen (ZCR 6)

10 Freigabe (ZCR 7)

1 Management Summary

Die Fertigung ist in 15 Zonen und 10 Conduits gegliedert. 4 Zonen erhalten SL-T 3: DMZ, Leitebene, Engineering und Management; die Zellen SL-T 2, weil ihre Sicherheitsfunktionen eigenständig arbeiten.

Von 11 bewerteten Bedrohungen sind ohne Maßnahmen 1 kritisch und 6 hoch. Mit den Maßnahmen liegt keine über MITTEL. Die größten Lücken liegen bei den Herstellerroutern an den Maschinen, bei Bedienrechnern mit veralteten Betriebssystemen und beim Programmweg aus der IT.

GESAMTBEWERTUNG

Zonen halten Angriffe aus der IT ab, Mikrosegmente verhindern die Ausbreitung von Maschine zu Maschine. Herstellerrouter an den Maschinen umgehen beides, bis sie entfernt sind.

Klasse	Ohne Maßnahmen	Mit Maßnahmen
KRITISCH	1	0
HOCH	6	0
MITTEL	4	7
NIEDRIG	0	4

2 System under Consideration (ZCR 1)

Betrachtet wird die gesamte Fertigung mit Maschinen, Lager, Transportfahrzeugen, Messraum, Versorgung und Gebäudeleittechnik einschließlich aller Fernzugänge. Grenzen sind die Übergänge zur IT (K01, K09) und zum Internet (K02, K08).

- **Nicht betrachtet:** physische Sicherheit des Geländes und Prozesse des Betreibers (Managementsystem nach IEC 62443-2-1).
- **Annahmen:** Sicherheitsfunktionen in Safety Integrated, F-Programmen, Laserscannern und Lichtvorhängen; Herstelleranlagen mit eigener Steuerung hinter SC646.
- **Bewertungsgrundlage:** IEC 62443-3-2:2020 (ZCR 1 bis 7), IEC 62443-3-3:2013, MITRE ATT&CK for ICS v20.

3 Risikokriterien

Stufe	Mensch	Kunde, Qualität	Betrieb, Finanzen
1	keine Gefährdung	keine	unter 10.000 €
2	Erste Hilfe	Nacharbeit im Haus	unter 100.000 €
3	leichte Verletzung	Ausschuss erkannt, Lieferverzug	unter 1 Mio. €
4	schwere Verletzung	fehlerhafte Teile beim Kunden, Rückruf	über 1 Mio. €
5	Lebensgefahr: Maschine, Regal, Pulver	Ausfall sicherheitskritischer Kundenprodukte	Existenz gefährdet

Klasse	A × W	Tolerierbar
KRITISCH	15 bis 25	nein
HOCH	10 bis 14	nein
MITTEL	5 bis 9	mit Freigabe des Betreibers
NIEDRIG	1 bis 4	ja

4 Erste Risikobewertung (ZCR 2)

Schlimmster Fall je Zone ohne Gegenmaßnahmen, Eintrittswahrscheinlichkeit 4.

Zone	Bezeichnung	Schlimmster Fall	A	Risiko
Z03	DMZ	Sprungbrett, Programmweg	4	KRITISCH
Z04	Fertigungsleitebene	Aufträge und Programme	4	KRITISCH
Z05	Engineering	alle Steuerungen	4	KRITISCH

Zone	Bezeichnung	Schlimmster Fall	A	Risiko
Z06	OT-Management	Trennung aller Zonen	4	KRITISCH
Z07	Zelle Zerspanung	Qualität, Maschinen	4	KRITISCH
Z08	Zelle Blech	Maschinen	3	HOCH
Z09	Zelle Additiv	Pulver, Argon	3	HOCH
Z10	Zelle Messraum	Qualität	4	KRITISCH
Z11	Zelle Lager	Regal, Personen bei Wartung	3	HOCH
Z12	Zelle FTS	Transporte	3	HOCH
Z13	Zelle Versorgung	Stillstand, Hautschutz	3	HOCH
Z14	Gebäudeleittechnik	Messqualität	3	HOCH
Z16	Gebäudesicherheit	Zutritt	2	MITTEL
Z18	Temporär verbundene Geräte	alle Zellen	4	KRITISCH
Z15	Sicherheitsfunktionen	Mensch	5	KRITISCH

5 Zonen, Conduits, Mikrosegmente (ZCR 3)

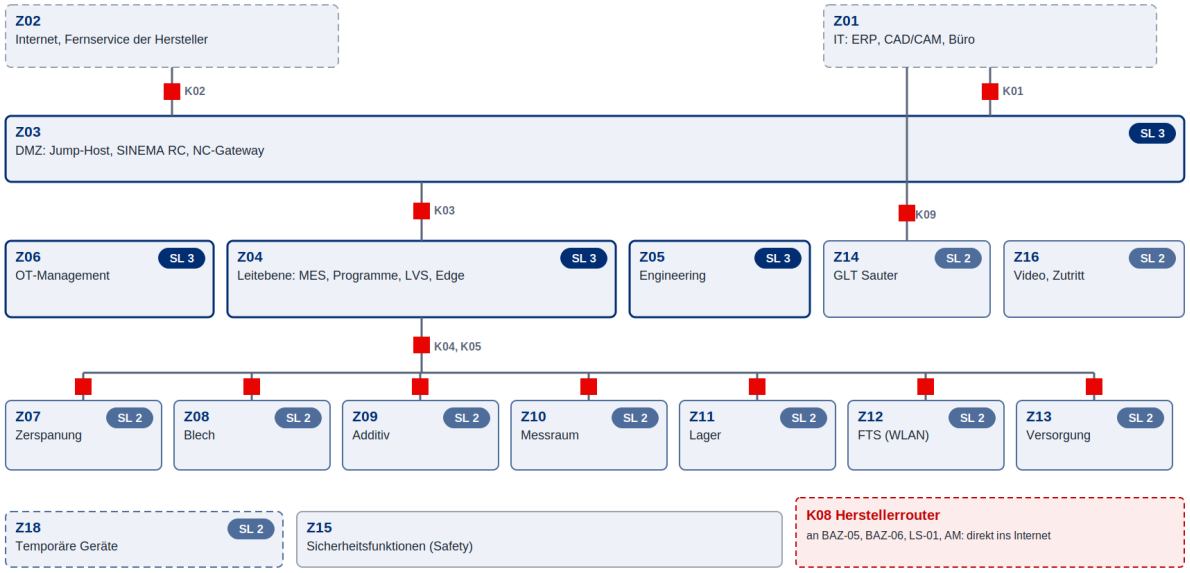


Abbildung: Zonen und Conduits mit SL-T

Getrennt sind Geschäfts- und Steuerungssysteme (ZCR 3.2), Sicherheitsfunktionen (ZCR 3.3, Z15), zeitweise verbundene Geräte (ZCR 3.4) und nicht vertrauenswürdige Netze (ZCR 3.6); jede Fertigungszelle ist eine eigene Zone.

Zone	Bezeichnung	Inhalt	SL-T
Z03	DMZ	Jump-Host, Fernwartung, NC-Gateway, Herstellerrouter	3
Z04	Fertigungsleitebene	MES, Programmverwaltung, Werkzeuge, Edge, LVS	3
Z05	Engineering	TIA Portal, SINUMERIK Service	3
Z06	OT-Management	Firewalls, Switches, WLAN-Controller	3
Z07	Zelle Zerspanung	BAZ, Dreh-Fräszentren, Schleifmaschine, Roboter	2
Z08	Zelle Blech	Laser, Abkantpresse	2
Z09	Zelle Additiv	3D-Drucker, Pulverstation	2
Z10	Zelle Messraum	Koordinatenmessmaschine	2
Z11	Zelle Lager	HRL, AKL, Fördertechnik	2
Z12	Zelle FTS	Flottenmanager, Fahrzeuge, WLAN	2
Z13	Zelle Versorgung	Druckluft, KSS, Argon	2
Z14	Gebäudeleittechnik	Sauter, Messraumklima	2
Z16	Gebäudesicherheit	Video, Zutritt	2
Z18	Temporär verbundene Geräte	Service-Laptops	2
Z15	Sicherheitsfunktionen	Safety Integrated, Not-Halt, Lichtvorhänge, O2-Mangel	hart verdrahtet

CONDUITS

Conduit	Verbindet	Datenflüsse	Schutz	SL-T
K01	Z01 IT ↔ Z03	NC-Programme, Berichte	Firewall (R01, R14)	3
K02	Z02 ↔ Z03	Herstellerfernwartung	SINEMA RC (R21)	3
K03	Z03 ↔ Z04, Z05	Programme, Administration	Firewall (R02, R20)	3
K04	Z04 ↔ Z07 bis Z10	OPC UA, Programme	Zellenfirewalls (R03 bis R06)	2
K05	Z04 ↔ Z11, Z12	Lager- und Transportaufträge	Zellenfirewalls (R09, R11)	2
K06	Z05 ↔ Zellen	Engineering	Firewall (R16 bis R19)	3
K07	Z03 ↔ Zellen	Fernbedienung nach Freigabe	SINEMA RC (R22)	3
K08	Herstellerrouter ↔ Maschine	Fernwartung direkt	keine Firewall	1
K09	Z01 ↔ Z14	Haustechnik	Firewall (R29)	2
K10	Z06 ↔ alle	Zeit, Überwachung	Management (R28)	3

MIKROSEGMENTE

Zone	Segmente
Z03	Jump-Host: 1 Geräte; Fernwartungsgateway: 1 Geräte; NC-Gateway: 1 Geräte; Dienste: 2 Geräte; OEM-Router: 4 Geräte
Z04	MES: 2 Geräte; Programmverwaltung: 1 Geräte; Werkzeuge, Edge: 2 Geräte; Lagerverwaltung: 1 Geräte; Meisterplätze: 2 Geräte
Z05	Engineering SPS: 1 Geräte; Service CNC: 1 Geräte
Z07	BAZ-01: 2 Geräte; BAZ-02: 2 Geräte; BAZ-03: 2 Geräte; BAZ-04: 2 Geräte; BAZ-05: 2 Geräte; BAZ-06: 3 Geräte; DZ-01: 2 Geräte; DZ-02: 2 Geräte; DZ-03: 2 Geräte; SG-01: 2 Geräte; Voreinstellgerät: 1 Geräte
Z08	LS-01: 2 Geräte; AP-01: 1 Geräte
Z09	AM-01: 1 Geräte; AM-02: 1 Geräte; Pulverstation: 1 Geräte
Z10	KMG-01: 2 Geräte
Z11	Lagersteuerung: 2 Geräte; Regalbediengeräte: 2 Geräte; Kleinteilelager: 4 Geräte
Z12	Flottenmanager: 1 Geräte; Fahrzeuge: 6 Geräte; Access Points: 8 Geräte
Z13	Versorgung: 2 Geräte; Kompressoren: 2 Geräte
Z14	Vision Center: 1 Geräte; Automationsstationen: 4 Geräte

Firewallregeln R01 bis R29 mit Quelle, Ziel, Dienst und Stufe stehen im Kommunikationskonzept und im HTML-Leitstand (Reiter Segmentierung).

6 Detaillierte Risikobewertung (ZCR 5)

6.1.1 Z03 DMZ

Nr.	Bedrohung	A	Wo	Ohne	Maßnahmen	Wm	Mit
T03-1	NC-Programme verändert auf dem Weg aus der IT (M1)	4	4	KRITISCH	Freigabe mit Prüfsumme (SR 3.4)	2	MITTEL
T03-2	Herstellerrouter umgeht die Firewall (M2)	3	4	HOCH	Router entfernen, zentraler Zugang (SR 1.13)	2	MITTEL

6.1.2 Z04 Fertigungsleitebene

Nr.	Bedrohung	A	Wo	Ohne	Maßnahmen	Wm	Mit
T04-1	Ransomware auf MES und Programmverwaltung (M6)	3	4	HOCH	Whitelisting, Offline-Sicherung	2	MITTEL
T04-2	Lagerbestand verfälscht (M3)	4	2	MITTEL	Schattenbestand in der SPS	1	NIEDRIG

6.1.3 Z05 Engineering

Nr.	Bedrohung	A	Wo	Ohne	Maßnahmen	Wm	Mit
T05-1	Engineering-Station verändert SPS	4	2	MITTEL	Versionsverwaltung, Vier-Augen	1	NIEDRIG

6.1.4 Z07 Zelle Zerspanung

Nr.	Bedrohung	A	Wo	Ohne	Maßnahmen	Wm	Mit
T07-1	Bedientafel mit veraltetem Windows (M2)	3	4	HOCH	Mikrosegment, Whitelisting	2	MITTEL

6.1.5 Z09 Zelle Additiv

Nr.	Bedrohung	A	Wo	Ohne	Maßnahmen	Wm	Mit
T09-1	3D-Drucker-Parameter verändert	3	2	MITTEL	Freigabe der Bauaufträge, Prüfteile	1	NIEDRIG

6.1.6 Z10 Zelle Messraum

Nr.	Bedrohung	A	Wo	Ohne	Maßnahmen	Wm	Mit
T10-1	Messergebnisse verfälscht (M5)	4	3	HOCH	Prüfnormal, unabhängiger Logger	2	MITTEL

6.1.7 Z12 Zelle FTS

Nr.	Bedrohung	A	Wo	Ohne	Maßnahmen	Wm	Mit
T12-1	Fremdes Gerät im WLAN steuert Fahrzeuge (M4)	3	3	MITTEL	WPA3-Enterprise, Zertifikate	1	NIEDRIG

6.1.8 Z14 Gebäudeleittechnik

Nr.	Bedrohung	A	Wo	Ohne	Maßnahmen	Wm	Mit
T14-1	Raumklima aus dem Büro verstellt (M5)	4	3	HOCH	Bedienung nur aus der OT, Logger	2	MITTEL

6.1.9 Z18 Temporär verbundene Geräte

Nr.	Bedrohung	A	Wo	Ohne	Maßnahmen	Wm	Mit
T18-1	Service-Laptop mit Schadsoftware	3	4	HOCH	Prüfung vor Anschluss, NAC	2	MITTEL

7 Ziel-Security-Level

SL-T je Grundanforderung FR1 bis FR7 (Spalten 1 bis 7). FR3 Integrität ist in allen Zonen mit Steuer- und Schutzfunktion erhöht, weil verfälschte Sollwerte, Befehle und Parameter dort Menschen, Netz oder Anlage gefährden.

Zone	Bezeichnung	1	2	3	4	5	6	7	SL-T	Begründung
Z03	DMZ	3	3	3	3	3	2	2	3	Programm- und Fernwartungsweg
Z04	Fertigungsleitebene	3	3	3	3	3	2	3	3	versorgt alle Maschinen
Z05	Engineering	3	3	3	3	3	2	2	3	kann Programme ändern
Z06	OT-Management	3	3	3	2	3	2	3	3	steuert die Segmentierung
Z07	Zelle Zerspanung	2	2	3	1	3	2	2	2	Sicherheit in Safety Integrated
Z08	Zelle Blech	2	2	2	1	2	2	2	2	Herstellersteuerung
Z09	Zelle Additiv	2	2	2	1	2	2	2	2	O2-Mangel hart
Z10	Zelle Messraum	2	2	3	1	2	2	2	2	Freigabe hängt am Klima
Z11	Zelle Lager	2	2	3	1	2	2	2	2	F-Programm RBG
Z12	Zelle FTS	2	2	2	2	2	2	3	2	Funk, Scanner eigenständig
Z13	Zelle Versorgung	2	2	2	1	2	2	2	2	Grenzen in der SPS
Z14	Gebäudeleittechnik	2	2	3	1	2	1	2	2	beeinflusst Messungen
Z16	Gebäudesicherheit	2	2	2	2	2	1	1	2	eigenes Netz
Z18	Temporär verbundene Geräte	2	2	3	1	3	2	1	2	ZCR 3.4

8 Vergleich mit den Fähigkeiten (ZCR 4)

Zone	Komponente, Befund	SL-C erwartet	SL-T	Kompensierende Maßnahme
Z07	SG-01: Windows 7 Embedded, NC unter Sollstand	kein Support	2	Mikrosegment, Austausch mit Hersteller planen
Z03	Herstellerrouter BAZ-05 mit Firmware 3.4	veraltet, eigener Internetzugang	3	entfernen bzw. hinter die Firewall
Z09	AM-02: Windows LTSB 2016	Support endet	2	Update mit Hersteller, Mikrosegment
Z11	Shuttle-Steuerung Gasse 3 Firmware V2.9.7	kein Zertifikat unter V3.1	2	Firmware auf V3.1

Zone	Komponente, Befund	SL-C erwartet	SL-T	Kompensierende Maßnahme
Z12	Fahrzeug AGV-4 Firmware 5.1	unter Sollstand	2	Update im Wartungsfenster
Z14	Sauter-Station Messraum 1.8	unter Sollstand	2	Update, Bedienung nur aus der OT

Firmwarestände aus dem Asset-Inventar (fiktiv). S7-1500 ab V3.1, SCALANCE Layer-2 managed und SC-600 sind nach IEC 62443-4-2 zertifiziert; für SINUMERIK und Herstelleranlagen je Produkt anfordern.

9 Anforderungen (ZCR 6)

Nr.	Anforderung an Lieferanten	Bezug
L-01	Nachweis SL-C nach IEC 62443-4-2 für Steuerungen und Bedienrechner der Maschinen	IEC 62443-4-2
L-02	Keine eigenen Fernwartungsrouter; Fernzugang über den zentralen Zugang des Betreibers	SR 1.13, IEC 62443-2-4
L-03	Bedienrechner mit unterstütztem Betriebssystem und Update-Zusage über die Nutzungsdauer	CRA, Maschinenverordnung
L-04	OPC UA nur mit SignAndEncrypt und lesenden Rechten	SR 3.1, 4.1
L-05	Fahrzeuge mit Zertifikaten, VDA 5050 über MQTT mit TLS	SR 1.9
L-06	Programmübertragung mit Prüfsumme und Freigabe	SR 3.4
L-07	Meldewege für Schwachstellen (Art. 14 CRA) und Sicherheitsupdates	CRA
L-08	Cybersicherheit als Teil der Konformitätsbewertung (Anhang III 1.1.9)	Maschinenverordnung (EU) 2023/1230

10 Freigabe (ZCR 7)

Rolle	Name	Datum	Unterschrift
Geschäftsführung, Betreiber	[Name]		
Fertigungsleitung	[Name]		
Verfasser	Maximilian Gilg, OT-Cyber.de		