BERICHT

Risikobewertung nach IEC 62443-3-2

Hartkäserei im Bestand: Zonen, Conduits, Mikrosegmente und Ziel-Security-Level

Auftraggeber	[Betreiber, Ort]
Projekt	Käserei, 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 Käserei ist in 15 Zonen und 9 Conduits gegliedert; jede OEM-Zelle liegt hinter einer SC646-2C mit NAT. 9 Zonen erhalten SL-T 3, darunter die Erhitzung KZE-302, die Zelle Milch und Käserei mit dem Ventilknoten, CIP, die Würfellinie mit Röntgen und die Kälte mit Ammoniak.

Von 15 bewerteten Bedrohungen sind ohne Maßnahmen 6 kritisch und 4 hoch. Mit den Maßnahmen liegt keine über MITTEL. Die größte Lücke liegt in der Erhitzersteuerung (Firmware unter V3.1, PUT/GET offen) und darin, dass die Steuerungen im Leitsystem-VLAN von jedem Bedienplatz erreichbar sind.

GESAMTBEWERTUNG

Zonen und Zellenfirewalls trennen IT, Leitsystem und OEM-Anlagen. Erst Firewalls direkt vor den Steuerungen der kritischen Kontrollpunkte verhindern, dass ein missbrauchter Fernwartungs- oder Bedienzugang dort schreiben kann.

Klasse	Ohne Maßnahmen	Mit Maßnahmen
KRITISCH	6	0
HOCH	4	1
MITTEL	5	7
NIEDRIG	0	7

2 System under Consideration (ZCR 1)

Betrachtet wird die gesamte Automatisierung der Käserei von der Milchannahme bis zum Versand, einschließlich Kälte, CIP, Versorgung und aller Fernzugänge. Grenzen sind die Übergänge zur IT (K01) und zum Internet (K02).

- **Nicht betrachtet:** physische Sicherheit des Geländes und Prozesse des Betreibers (Managementsystem nach IEC 62443-2-1).
- **Annahmen:** Schreiber RSG45 mit Grenzkontakt, Mannlochschalter und Kälte-Druckbegrenzer hart; OEM-Anlagen mit eigener Steuerung hinter SC646; Historian und MES in der DMZ.
- **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	Lebensmittelsicherheit, Umwelt	Betrieb, Finanzen
1	keine Gefährdung	keine	unter 10.000 €
2	Erste Hilfe	Qualitätsabweichung ohne Auslieferung	unter 100.000 €
3	leichte Verletzung	Sperrung von Chargen	unter 1 Mio. €
4	schwere Verletzung	Rückruf ausgelieferter Ware, Fremdkörper	über 1 Mio. €
5	Lebensgefahr: NH3, Lauge, Erreger im Produkt	Erkrankungen bei Verbrauchern, öffentlicher Rückruf	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 in alle Zonen	4	KRITISCH
Z04	Leitsystem	Verbraucher, Mensch über die Steuerungen	5	KRITISCH

Zone	Bezeichnung	Schlimmster Fall	A	Risiko
Z05	Engineering	alle Programme	5	KRITISCH
Z06	OT-Management	Trennung aller Zonen	4	KRITISCH
Z08	Zelle Milch, Käserei	Ventilknoten, Lauge im Produkt	5	KRITISCH
Z09	Zelle CIP	Lauge, Mensch	5	KRITISCH
Z10	Zelle Versorgung	Betrieb, Neutralisation	3	HOCH
Z11	OEM KZE-302	Erreger im Produkt	5	KRITISCH
Z12	OEM Käsefertiger	Charge	3	HOCH
Z13	OEM Pressen, Salzbad	Charge	3	HOCH
Z14	OEM Würfellinie	Fremdkörper, Füllmenge	4	KRITISCH
Z15	OEM RBG, LVS	Bestand, Mensch im Lager	3	HOCH
Z16	OEM Kälte, Klima	Mensch, Umgebung, Reifebestand	5	KRITISCH
Z18	Temporär verbundene Geräte	alle Zellen	4	KRITISCH
Z17	Sicherheitsfunktionen	Mensch, Verbraucher	5	KRITISCH

5 Zonen, Conduits, Mikrosegmente (ZCR 3)

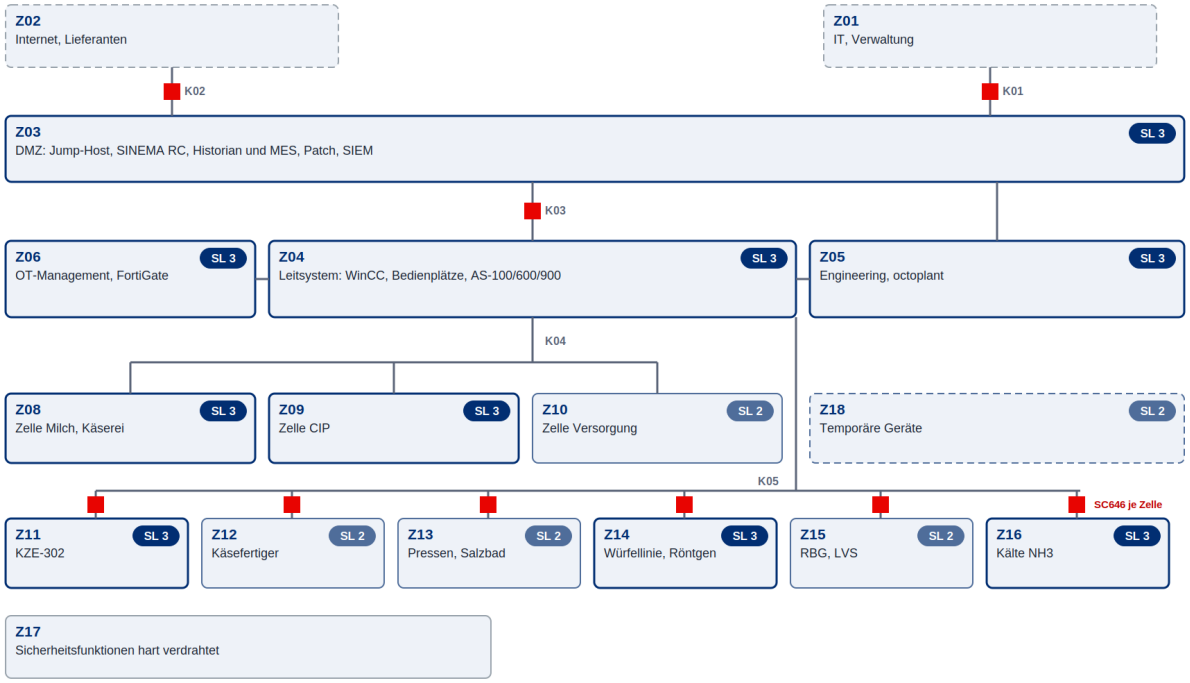


Abbildung: Zonen und Conduits mit SL-T

Getrennt sind Geschäfts- und Steuerungssysteme (ZCR 3.2), Sicherheitsfunktionen (ZCR 3.3, Z17 hart verdrahtet), zeitweise verbundene Geräte (ZCR 3.4) und nicht vertrauenswürdige Netze (ZCR 3.6). Jede OEM-Anlage ist eine eigene Zone hinter einer SC646-2C.

Zone	Bezeichnung	Inhalt	SL-T
Z03	DMZ	Patch, Jump-Host, Historian und MES, SINEMA RC, SIEM, DNS	3
Z04	Leitsystem	WinCC A/B, Bedienplätze, AS-100/600/900 (X1)	3
Z05	Engineering	Engineering-Station, octoplant	3
Z06	OT-Management	FortiGate, SC646, Switches, Zeitserver, Monitoring	3
Z08	Zelle Milch, Käserei	PROFINET AS-100, Fahrerterminal	3
Z09	Zelle CIP	PROFINET AS-600	3
Z10	Zelle Versorgung	PROFINET AS-900, Energiezähler	2
Z11	OEM KZE-302	Erhitzer hinter SC646-201	3
Z12	OEM Käsefertiger	Bertsch hinter SC646-202	2
Z13	OEM Pressen, Salzbad	Alpma hinter SC646-203	2
Z14	OEM Würfellinie	Linie, Röntgen, Kontrollwaage hinter SC646-204	3
Z15	OEM RBG, LVS	Regalbediengerät hinter SC646-205	2
Z16	OEM Kälte, Klima	Kälte mit NH3 hinter SC646-206	3
Z18	Temporär verbundene Geräte	Service-Laptops	2
Z17	Sicherheitsfunktionen	RSG45-Grenzkontakt, Mannlochschalter, Not-Halt, Kälte-Hochdruck	hart verdrahtet

CONDUITS

Conduit	Verbindet	Datenflüsse	Schutz	SL-T
K01	Z01 IT ↔ Z03 DMZ	Berichte aus Historian und MES	FortiGate (R15)	3
K02	Z02 Internet ↔ Z03	Fernwartung nur zu SINEMA RC	FortiGate, MFA (R07)	3
K03	Z03 ↔ Z04, Z05	Administration, Archiv	FortiGate (R12 bis R14)	3
K04	Z04 ↔ Z08 bis Z10	PROFINET der Steuerungen (X2)	Steuerung als Grenze	3
K05	Z04 ↔ Z11 bis Z16	OPC UA lesen, Modbus Kälte lesen	SC646 mit NAT (R02, R03, R26)	3
K06	Z05 ↔ Z04, OEM	Engineering, Sicherung	FortiGate, SC646 (R05, R06, R16)	3
K07	Z03 ↔ OEM-Zellen	Fernwartung bei Schlüsselschalter	SINEMA RC, SC646 (R08 bis R11)	3
K08	Z06 ↔ alle	Zeit, Überwachung, Verwaltung	Management-VLAN (R22)	3
K09	Z18 ↔ Zellen	Diagnose vor Ort	nur über Engineering	2

MIKROSEGMENTE

Zone	Segmente
Z03	Jump-Host: 1 Geräte; SINEMA RC: 1 Geräte; Historian, MES: 1 Geräte; Dienste: 3 Geräte
Z04	WinCC-Server: 2 Geräte; Bedienplätze: 3 Geräte; AS-100 hinter VW-Firewall: 1 Geräte; AS-600: 1 Geräte; AS-900 hinter VW-Firewall: 1 Geräte
Z05	Engineering: 2 Geräte
Z08	Peripherie AS-100: 8 Geräte; Fahrerterminal: 1 Geräte
Z14	Würfellinie-SPS: 1 Geräte; Röntgen hinter VW-Firewall: 1 Geräte; Kontrollwaage: 1 Geräte

Firewallregeln R01 bis R26 mit Quelle, Ziel, Dienst und Stufe stehen im HTML-Leitstand (Reiter Segmentierung); dort lassen sie sich einzeln abschalten und mit dem Flusstester prüfen.

6 Detaillierte Risikobewertung (ZCR 5)

6.1.1 Z03 DMZ

Nr.	Bedrohung	A	Wo	Ohne	Maßnahmen	Wm	Mit
T03-1	SINEMA RC mit gestohlenen Daten, Schlüsselschalter vergessen (K1, K4)	5	4	KRITISCH	Freigabe je Sitzung, Rückmeldung Schlüsselschalter (SR 1.13)	2	HOCH
T03-2	Jump-Host mit Admin-Daten aus der IT (K3, K6)	4	3	HOCH	OT-Konten (SR 1.1), MFA	1	NIEDRIG

6.1.2 Z04 Leitsystem

Nr.	Bedrohung	A	Wo	Ohne	Maßnahmen	Wm	Mit
T04-1	Bedienplatz baut Engineering-Verbindung zur AS-100 auf (K2)	5	3	KRITISCH	VW-Firewall vor AS-100 (SR 5.1), Zugriffsschutz (SR 2.1)	1	MITTEL
T04-2	Ransomware auf WinCC-Servern (K6)	4	3	HOCH	Whitelisting (SR 3.2), Sicherung (SR 7.3, 7.4)	1	NIEDRIG

6.1.3 Z05 Engineering

Nr.	Bedrohung	A	Wo	Ohne	Maßnahmen	Wm	Mit
T05-1	Engineering-Station lädt manipulierte Programme	5	2	HOCH	octoplant-Vergleich, Vier-Augen, USB-Kontrolle	1	MITTEL

6.1.4 Z06 OT-Management

Nr.	Bedrohung	A	Wo	Ohne	Maßnahmen	Wm	Mit
T06-1	Regeln der FortiGate oder SC646 verändert	4	2	MITTEL	MFA, Konfigurationssicherung, Änderungskontrolle (SR 7.6)	1	NIEDRIG

6.1.5 Z08 Zelle Milch, Käserei

Nr.	Bedrohung	A	Wo	Ohne	Maßnahmen	Wm	Mit
T08-1	Fremder Laptop am Feld-Switch, PROFINET DCP (K5)	3	3	MITTEL	Port Security (SR 1.2), Mikrosegmente, Laptopkontrolle	1	NIEDRIG

6.1.6 Z09 Zelle CIP

Nr.	Bedrohung	A	Wo	Ohne	Maßnahmen	Wm	Mit
T09-1	CIP startet in Behälter mit offenem Mannloch (K2)	5	2	HOCH	Mannlochschalter hart und im F-Programm (H07)	1	MITTEL

6.1.7 Z10 Zelle Versorgung

Nr.	Bedrohung	A	Wo	Ohne	Maßnahmen	Wm	Mit
T10-1	Neutralisation per Modbus verstellt, pH über 12 in den Kanal	3	3	MITTEL	Modbus nur lesend, unabhängiger pH-Grenzwertschalter	1	NIEDRIG

6.1.8 Z11 OEM KZE-302

Nr.	Bedrohung	A	Wo	Ohne	Maßnahmen	Wm	Mit
T11-1	Umschaltgrenze der Erhitzung per S7 PUT/GET gesenkt (K1)	5	3	KRITISCH	VW-Firewall, PUT/GET aus, RSG45 hart (H07)	1	MITTEL

6.1.9 Z14 OEM Würfellinie

Nr.	Bedrohung	A	Wo	Ohne	Maßnahmen	Wm	Mit
T14-1	Sollgewicht und Röntgen-Ausschleusung über Fernwartung verstellt (K4)	4	4	KRITISCH	Freigabe je Sitzung, VW-Firewall Röntgen, Vier-Augen	2	MITTEL

6.1.10 Z15 OEM RBG, LVS

Nr.	Bedrohung	A	Wo	Ohne	Maßnahmen	Wm	Mit
T15-1	Regalbediengerät fährt falsch, Kisten stürzen	3	2	MITTEL	Sicherheitsfunktionen des RBG hart, Zugang nur über LVS	1	NIEDRIG

6.1.11 Z16 OEM Kälte, Klima

Nr.	Bedrohung	A	Wo	Ohne	Maßnahmen	Wm	Mit
T16-1	Kälteregler per Modbus: Hochdruck, NH3 bläst ab (K3)	5	3	KRITISCH	VW-Firewall, Modbus nur lesend, Druckbegrenzer hart	1	MITTEL
T16-2	Reifelagerklima verstellt, 210 t Käse verderben	4	2	MITTEL	unabhängige Temperaturüberwachung mit GSM (H07)	1	NIEDRIG

6.1.12 Z18 Temporär verbundene Geräte

Nr.	Bedrohung	A	Wo	Ohne	Maßnahmen	Wm	Mit
T18-1	Service-Laptop mit Schadsoftware (K5)	4	4	KRITISCH	Prüfung vor Anschluss (SR 2.3), NAC (SR 1.2)	2	MITTEL

7 Ziel-Security-Level

SL-T je Grundanforderung FR1 bis FR7 (Spalten 1 bis 7). FR3 Integrität ist in Erhitzung, Ventilknoten, CIP, Würfellinie und Kälte erhöht, weil verfälschte Sollwerte und Befehle dort Menschen oder Verbraucher gefährden.

Zone	Bezeichnung	1	2	3	4	5	6	7	SL-T	Begründung
Z03	DMZ	3	3	2	3	3	2	2	3	Fernwartung und IT-Übergang
Z04	Leitsystem	3	3	3	2	3	2	3	3	Steuerungen im selben VLAN
Z05	Engineering	3	3	3	3	3	2	2	3	kann jedes Programm ändern
Z06	OT-Management	3	3	2	2	3	2	2	3	steuert die Segmentierung
Z08	Zelle Milch, Käserei	2	2	3	1	3	2	3	3	Ventilknoten und Käsefertigung
Z09	Zelle CIP	2	2	3	1	3	2	3	3	Reinigung mit Lauge und Säure
Z10	Zelle Versorgung	2	2	2	1	2	2	2	2	Folgen begrenzt
Z11	OEM KZE-302	3	3	3	1	3	2	3	3	kritischer Kontrollpunkt Erhitzung
Z12	OEM Käsefertiger	2	2	2	1	2	2	2	2	Folgen begrenzt
Z13	OEM Pressen, Salzbad	2	2	2	1	2	2	2	2	Folgen begrenzt
Z14	OEM Würfellinie	3	3	3	1	3	2	2	3	kritischer Kontrollpunkt Fremdkörper
Z15	OEM RBG, LVS	2	2	2	1	2	2	2	2	Folgen begrenzt
Z16	OEM Kälte, Klima	3	3	3	1	3	2	3	3	Ammoniak, Reifebestand 210 t
Z18	Temporär verbundene Geräte	2	2	3	1	3	2	1	2	ZCR 3.4: eigene Zone

8 Vergleich mit den Fähigkeiten (ZCR 4)

Zone	Komponente, Befund	SL-C erwartet	SL-T	Kompensierende Maßnahme
Z11	Erhitzersteuerung Firmware V2.9.7, PUT/GET für das Lieferanten-Panel offen	kein Zertifikat unter V3.1	3	Firmware auf V3.1, PUT/GET aus, VW-Firewall, RSG45 hart

Zone	Komponente, Befund	SL-C erwartet	SL-T	Kompensierende Maßnahme
Z16	Kälteregler Firmware V3.0.2, Modbus schreibbar	kein Zertifikat, Modbus ohne Authentisierung	3	VW-Firewall nur lesend, Schreiben nur am Panel
Z14	Röntgen-PC Windows 10 IoT 2019, SC646-204 Firmware V2.4.1	Betriebssystem ohne Sollstand	3	Röntgen-PC auf 2021 LTSC, VW-Firewall, SC646 aktualisieren
Z04	WinCC Unified, Bedienplatz 3 Windows 10	WinCC nicht nach 4-2 zertifiziert	3	Härtung, Whitelisting, Nachweis 62443-3-3 durch den Integrator
Z08	ET 200SP Käsefertigung Firmware V5.0.1	nicht bewertet	3	Firmware auf Sollstand, Port Security

Firmwarestände aus dem Asset-Inventar (fiktiv). Zertifikate nach IEC 62443-4-2 liegen laut Hersteller vor für S7-1500 ab V3.1, SCALANCE Layer-2 managed und SC-600; WinCC Unified ist nicht nach 4-2 zertifiziert; für alle anderen Produkte je Gerät anfordern.

9 Anforderungen (ZCR 6)

Nr.	Anforderung an Lieferanten	Bezug
L-01	Nachweis SL-C nach IEC 62443-4-2 je Komponente mit Firmwarestand	IEC 62443-4-2
L-02	Nachweis der Systemanforderungen nach IEC 62443-3-3 durch den Integrator	IEC 62443-3-3
L-03	Lieferanten: Fernwartung nur über SINEMA RC mit Freigabe je Sitzung, keine eigenen Router	SR 1.13, IEC 62443-2-4
L-04	OEM-Steuerungen: PUT/GET aus, Zugriffsschutz, Sollwerte für CCP nur mit Grenzen	SR 2.1, 3.5
L-05	Erhitzer: Umschaltung über unabhängigen Grenzkontakt, nicht nur in der Software	VO (EG) 853/2004, HACCP
L-06	Kälte: Druckbegrenzer und Gaswarnung hart nach DIN EN 378, Modbus nur lesend	TRAS 110, BetrSichV
L-07	OPC UA nur mit SignAndEncrypt und Benutzerverwaltung	SR 3.1, 4.1
L-08	Sicherheitsupdates und Schwachstellenmeldungen über die Nutzungsdauer	IEC 62443-4-1, CRA

10 Freigabe (ZCR 7)

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