BERICHT

Risikobewertung nach IEC 62443-3-2

Brauerei 120.000 hl/a: Zonen, Conduits, Mikrosegmente und Ziel-Security-Level

Auftraggeber	[Betreiber, Ort]
Projekt	Brauerei, 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 Brauerei ist in 17 Zonen und 13 Conduits gegliedert; innerhalb der Zellen sind Mikrosegmente je Steuerung und Maschine vorgesehen. 10 Zonen erhalten SL-T 3, darunter der Gär- und Lagerkeller (CO2), die Flaschenlinie (Pasteurisation), CIP (Lauge im Produkt) und die OEM-Kälteanlage (NH3).

Von 18 bewerteten Bedrohungen sind ohne Maßnahmen 9 kritisch und 2 hoch. Mit den Maßnahmen liegt keine über MITTEL. Die größte Lücke liegt bei den Lieferantenzugängen: Kälteanlage mit eigenem Router und Firmware unter V3.1, Füller unter V3.1, Inspektor-PC mit Windows 10.

GESAMTBEWERTUNG

Zonen trennen IT, Leitsystem und Zellen. Erst Mikrosegmente verhindern, dass ein Gerät innerhalb einer Zelle alle anderen erreicht. Gegen Missbrauch des Bedienwegs helfen nur Grenzen in der SPS, Freigaben und autarke Sicherheitsfunktionen.

Klasse	Ohne Maßnahmen	Mit Maßnahmen
KRITISCH	9	0
HOCH	2	1
MITTEL	7	7
NIEDRIG	0	10

2 System under Consideration (ZCR 1)

Betrachtet wird die gesamte Automatisierung der Brauerei von der Malzannahme bis zur Abfüllung, einschließlich Energie, NH3-Kälte, CIP, MES 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:** Sicherheitsfunktionen für NH3, CO2 und Dampfkessel hart verdrahtet; Linienmaschinen von OEM mit eigener Steuerung; MES in eigener Zone.
- **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 im Lager	unter 1 Mio. €
4	schwere Verletzung	Rückruf ausgelieferter Ware	über 1 Mio. €
5	Lebensgefahr: NH3, CO2, Lauge im Produkt	öffentlicher Rückruf, Gesundheitsgefahr für Verbraucher	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	Mensch, Lebensmittel über Bedienung	5	KRITISCH
Z05	Engineering	alle Prozesse	5	KRITISCH

Zone	Bezeichnung	Schlimmster Fall	A	Risiko
Z06	OT-Management	Trennung aller Zonen	4	KRITISCH
Z07	MES, Linienmanagement	Rückverfolgung, Abfüllung	4	KRITISCH
Z08	Zelle Rohstoff	Betrieb, Staubexplosion mechanisch geschützt	3	HOCH
Z09	Zelle Sudhaus	Fehlsud, Betrieb	3	HOCH
Z10	Zelle Gär- und Lagerkeller	Mensch (CO2), Produkt	5	KRITISCH
Z11	Zelle Filtration	Produkt	3	HOCH
Z12	Zelle Flaschenlinie	Verbraucher (Pasteurisation)	5	KRITISCH
Z13	Zelle KEG-Linie	Betrieb	3	HOCH
Z14	Zelle CIP	Verbraucher (Lauge im Produkt)	5	KRITISCH
Z15	Zelle Energie, Medien	Betrieb; Kesselsicherheit hart verdrahtet	4	KRITISCH
Z16	OEM Kälteanlage NH3	Mensch (NH3), Umgebung	5	KRITISCH
Z18	Temporär verbundene Geräte	alle Zellen	4	KRITISCH
Z19	Gebäudesicherheit	Zutritt	3	HOCH
Z17	Sicherheitsfunktionen	Mensch	5	KRITISCH

5 Zonen, Conduits, Mikrosegmente (ZCR 3)

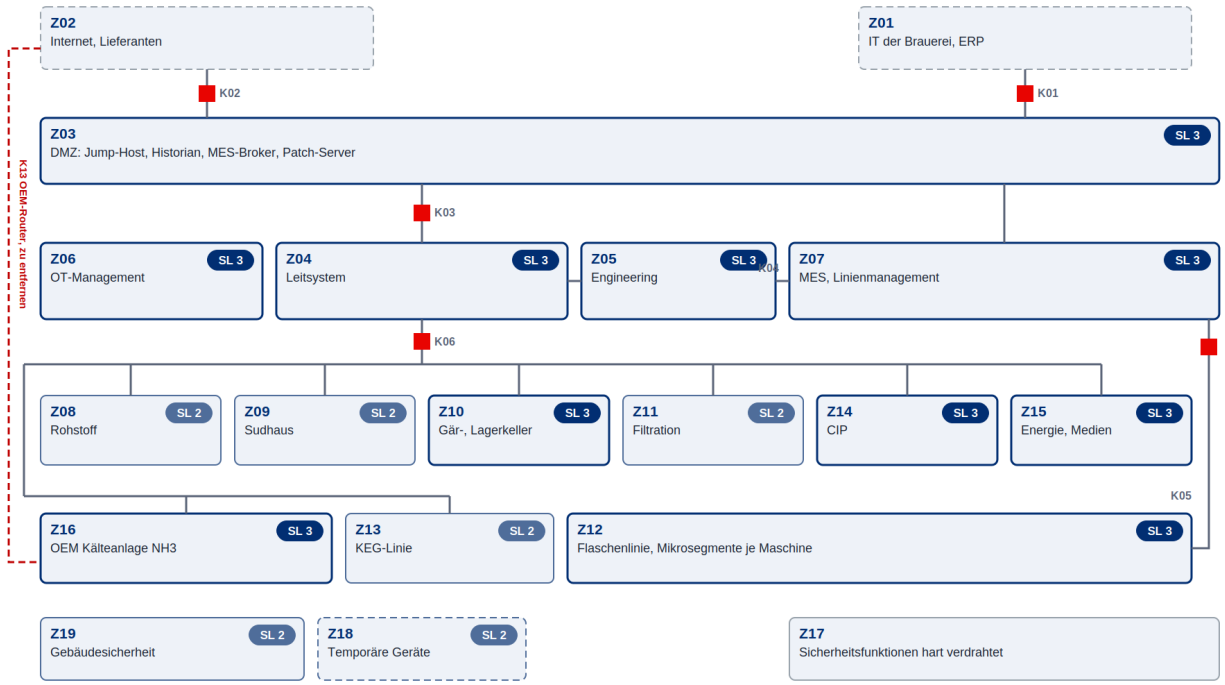


Abbildung: Zonen und Conduits mit SL-T

Getrennt sind Geschäfts- und Steuerungssysteme (ZCR 3.2), Sicherheitsfunktionen (ZCR 3.3, Z17 hart verdrahtet), zeitweise verbundene Geräte (ZCR 3.4) und nicht vertrauenswürdige Netze (ZCR 3.6). Die OEM-Kälteanlage ist eine eigene Zone; ihr Router mit eigenem Internetzugang ist zu entfernen.

Zone	Bezeichnung	Inhalt	SL-T
Z03	DMZ	Jump-Host, Historian, MES-Broker, Patch-Server, Log, DNS	3
Z04	Leitsystem	Server A/B, Bedienplätze, Großbildwand	3
Z05	Engineering	Engineering-Station	3
Z06	OT-Management	Firewall, Switches, Zeitserver, Monitoring, USV	3
Z07	MES, Linienmanagement	MES mit Rückverfolgung, Linienmanagement	3
Z08	Zelle Rohstoff	AS-10, Silos, Schroterei, Waage	2
Z09	Zelle Sudhaus	AS-20, 5 Geräte, Würzekühlung	2
Z10	Zelle Gär- und Lagerkeller	AS-30, 20 ZKT, Ventilknoten, Hefe	3
Z11	Zelle Filtration	AS-35, Crossflow, Drucktanks	2
Z12	Zelle Flaschenlinie	AS-60 KZE, 7 OEM-Maschinen	3
Z13	Zelle KEG-Linie	KEG-Anlage, Palettierer	2
Z14	Zelle CIP	AS-40, 3 CIP-Stationen	3
Z15	Zelle Energie, Medien	AS-50, Kessel, Druckluft, Wasser, CO2, Abwasser	3
Z16	OEM Kälteanlage NH3	Kälte-SPS, Bedienpanel, Fernwartungsrouter	3
Z18	Temporär verbundene Geräte	Service-Laptops	2
Z19	Gebäudesicherheit	Kameras, Videorekorder, Zutrittskontrolle	2
Z17	Sicherheitsfunktionen	NH3- und CO2-Gaswarnung, Druckbegrenzer, Kessel-Sicherheitskette, Not-Halt	hart verdrahtet

CONDUITS

Conduit	Verbindet	Datenflüsse	Schutz	SL-T
K01	Z01 IT ↔ Z03 DMZ	Aufträge, Rückmeldungen über den MES-Broker	Firewall (R07)	3
K02	Z02 Internet ↔ Z03 DMZ	Fernwartung nur zum Jump-Host	Firewall, MFA (R12)	3
K03	Z03 ↔ Z04, Z05	Administration, Historian	Firewall (R09 bis R11)	3
K04	Z04 ↔ Z07	MES holt Chargendaten	Firewall (R05, R06)	3
K05	Z07 ↔ Z12, Z13	Linienmanagement WS Pack über OPC UA	Firewall (R03, R04)	3
K06	Z04 ↔ Z08 bis Z16	Leitsystem zu den Steuerungen	Firewall (R01, R02)	3
K07	Z05 ↔ Zellen	Engineering	Firewall, Wartungsfenster (R14, R15)	3
K08	Z14 ↔ Z09, Z10, Z12	CIP-Freigaben	Firewall (R16)	3
K09	Z03 ↔ Z12, Z15, Z16	OEM-Wartung nach Freigabe	Jump-Host (R13)	3
K10	Z06 ↔ alle	Zeit, Überwachung, Verwaltung	Management-VLAN (R20)	3
K11	Z19 ↔ Z04	Videobilder zur Leitwarte	Firewall (R19)	2
K12	Z18 ↔ Zellen	Diagnose, Engineering vor Ort	nur über Engineering-Zugang	2
K13	Z16 ↔ Internet (Planungsstand)	Tunnel des OEM-Routers	zu entfernen (H01)	3

MIKROSEGMENTE

Zone	Segmente
Z03	Jump-Host: 1 Geräte; Historian: 1 Geräte; MES-Broker: 1 Geräte; Dienste: 3 Geräte
Z04	Server: 2 Geräte; Bedienplätze: 5 Geräte; Drucker: 1 Geräte
Z07	MES: 1 Geräte; Linienmanagement: 1 Geräte
Z08	Steuerung Rohstoff: 4 Geräte; Schrotmühle: 1 Geräte
Z09	Steuerung Sudhaus: 8 Geräte
Z10	Steuerung Keller: 5 Geräte; Hefereinzucht: 1 Geräte
Z11	Steuerung Filtration: 2 Geräte; Crossflow-Filter: 1 Geräte
Z12	KZE: 1 Geräte; Füller: 2 Geräte; Waschmaschine: 1 Geräte; Inspektor: 1 Geräte; Etikettierer: 1 Geräte; Verpackung: 3 Geräte
Z13	KEG-Linie: 2 Geräte
Z14	Steuerung CIP: 4 Geräte

Zone	Segmente
Z15	Steuerung Energie: 7 Geräte; Kessel: 1 Geräte; Druckluft: 1 Geräte; Wasser: 1 Geräte; CO2: 1 Geräte
Z16	Kälte-SPS: 2 Geräte; OEM-Router: 1 Geräte
Z19	Video: 7 Geräte; Zutritt: 1 Geräte

Firewallregeln R01 bis R23 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	Jump-Host mit gestohlenen Daten übernommen (B5)	4	4	KRITISCH	MFA, Freigabe je Sitzung, Aufzeichnung (SR 1.1, 1.13, 2.8)	2	MITTEL

6.1.2 Z04 Leitsystem

Nr.	Bedrohung	A	Wo	Ohne	Maßnahmen	Wm	Mit
T04-1	Bedienerkonto übernommen, Missbrauch des regulären Bedienwegs (B2, B4)	5	4	KRITISCH	Vier-Augen-Freigabe (SR 2.1), Sollwertgrenzen in der SPS (SR 3.5), autarke Sicherheit	2	HOCH
T04-2	Ransomware auf Leitsystem-Servern (B6)	4	3	HOCH	Whitelisting (SR 3.2), Offline-Sicherung (SR 7.3, 7.4), Segmentierung zum MES	1	NIEDRIG

6.1.3 Z05 Engineering

Nr.	Bedrohung	A	Wo	Ohne	Maßnahmen	Wm	Mit
T05-1	Infizierte Engineering-Station lädt Programme	5	3	KRITISCH	USB-Schleuse (SR 2.3), Vier-Augen und Sollstandvergleich (SR 3.4)	1	MITTEL

6.1.4 Z06 OT-Management

Nr.	Bedrohung	A	Wo	Ohne	Maßnahmen	Wm	Mit
T06-1	Firewall-Regeln oder Switch-Konfiguration manipuliert	4	2	MITTEL	MFA, Konfigurationssicherung, Änderungskontrolle (SR 7.6)	1	NIEDRIG

6.1.5 Z07 MES, Linienmanagement

Nr.	Bedrohung	A	Wo	Ohne	Maßnahmen	Wm	Mit
T07-1	MES aus der IT verschlüsselt (B6)	4	4	KRITISCH	Kopplung nur über Broker (SR 5.2), OT-Konten getrennt (SR 1.1)	1	NIEDRIG
T07-2	Chargendaten im MES verfälscht, falsche Freigabe	4	2	MITTEL	Signierte Chargenprotokolle (SR 3.1), Laborfreigabe	1	NIEDRIG

6.1.6 Z08 Zelle Rohstoff

Nr.	Bedrohung	A	Wo	Ohne	Maßnahmen	Wm	Mit
T08-1	Schrotmühle oder Malzannahme manipuliert	3	2	MITTEL	Zugriffsschutz, Staub-Ex mechanisch und hart verdrahtet	1	NIEDRIG

6.1.7 Z09 Zelle Sudhaus

Nr.	Bedrohung	A	Wo	Ohne	Maßnahmen	Wm	Mit
T09-1	Rezeptur im Sudhaus verfälscht, Fehlsude	3	3	MITTEL	Rezeptgrenzen in der SPS (SR 3.5), Vier-Augen-Freigabe	1	NIEDRIG

6.1.8 Z10 Zelle Gär- und Lagerkeller

Nr.	Bedrohung	A	Wo	Ohne	Maßnahmen	Wm	Mit
T10-1	Lüftung und CO2-Meldung im Tankkeller abgeschaltet (B2)	5	3	KRITISCH	Gaswarnanlage CO2 autark (H07), Vier-Augen (H08)	1	MITTEL
T10-2	Gärtemperaturen verstellt, Charge verdorben	3	3	MITTEL	Sollwertgrenzen je Phase (SR 3.5)	1	NIEDRIG

6.1.9 Z12 Zelle Flaschenlinie

Nr.	Bedrohung	A	Wo	Ohne	Maßnahmen	Wm	Mit
T12-1	PE-Sollwert am KZE gesenkt (B4)	5	3	KRITISCH	PE-Grenzen in der SPS, Umleitung fest (SR 3.5)	1	MITTEL

Nr.	Bedrohung	A	Wo	Ohne	Maßnahmen	Wm	Mit
T12-2	OEM-Fernwartung des Füllers missbraucht, Ausbreitung in der Linie (B5)	3	4	HOCH	Freigabe je Sitzung (SR 1.13), Mikrosegmente je Maschine (SR 5.1)	1	NIEDRIG

6.1.10 Z14 Zelle CIP

Nr.	Bedrohung	A	Wo	Ohne	Maßnahmen	Wm	Mit
T14-1	Fremder Laptop am CIP-Switch öffnet den Ventilknoten (B3)	5	3	KRITISCH	Port Security (SR 1.2), Mikrosegmente (SR 5.1), Verriegelung und Leitfähigkeit (SR 3.5)	1	MITTEL

6.1.11 Z15 Zelle Energie, Medien

Nr.	Bedrohung	A	Wo	Ohne	Maßnahmen	Wm	Mit
T15-1	Druckluft oder Wasseraufbereitung über Modbus gestört	3	2	MITTEL	Modbus nur lesend, Mikrosegmente	1	NIEDRIG

6.1.12 Z16 OEM Kälteanlage NH3

Nr.	Bedrohung	A	Wo	Ohne	Maßnahmen	Wm	Mit
T16-1	Kälte-SPS über OEM-Router manipuliert (B1)	5	4	KRITISCH	Router entfernen, Jump-Host (SR 1.13), Hochdruckbegrenzer hart (H07)	1	MITTEL

6.1.13 Z18 Temporär verbundene Geräte

Nr.	Bedrohung	A	Wo	Ohne	Maßnahmen	Wm	Mit
T18-1	Service-Laptop mit Schadsoftware (B3)	4	4	KRITISCH	Prüfung vor Anschluss (SR 2.3, 3.2), NAC (SR 1.2)	2	MITTEL

6.1.14 Z19 Gebäudesicherheit

Nr.	Bedrohung	A	Wo	Ohne	Maßnahmen	Wm	Mit
T19-1	Kamera mit alter Firmware als Einstieg	3	3	MITTEL	eigenes VLAN, Firewall nur vom Rekorder (SR 5.1, 5.2)	1	NIEDRIG

7 Ziel-Security-Level

SL-T je Grundanforderung FR1 bis FR7 (Spalten 1 bis 7). FR3 Integrität ist in Keller, Flaschenlinie, CIP, Energie 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	einziger Übergang für IT und Fernwartung
Z04	Leitsystem	3	3	2	2	3	2	3	3	regulärer Weg zu allen Steuerungen
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
Z07	MES, Linienmanagement	3	3	3	2	3	2	3	3	Chargenfreigabe und Rückverfolgung
Z08	Zelle Rohstoff	2	2	2	1	2	2	2	2	Folgen begrenzt
Z09	Zelle Sudhaus	2	2	3	1	2	2	2	2	FR3 erhöht wegen Rezeptdaten
Z10	Zelle Gär- und Lagerkeller	3	3	3	1	3	2	3	3	CO2 und Ventilknoten
Z11	Zelle Filtration	2	2	3	1	2	2	2	2	Folgen begrenzt
Z12	Zelle Flaschenlinie	3	3	3	1	3	2	3	3	Lebensmittelsicherheit, viele OEM-Zugänge
Z13	Zelle KEG-Linie	2	2	2	1	2	2	2	2	Folgen begrenzt
Z14	Zelle CIP	3	3	3	1	3	2	3	3	Ventilknoten zur Produktleitung
Z15	Zelle Energie, Medien	3	3	3	1	3	2	3	3	versorgt alle Bereiche
Z16	OEM Kälteanlage NH3	3	3	3	1	3	2	3	3	NH3, Lieferantenzugang
Z18	Temporär verbundene Geräte	2	2	3	1	3	2	1	2	ZCR 3.4: eigene Zone
Z19	Gebäudesicherheit	2	2	2	2	2	1	1	2	eigenes VLAN

8 Vergleich mit den Fähigkeiten (ZCR 4)

Zone	Komponente, Befund	SL-C erwartet	SL-T	Kompensierende Maßnahme
Z16	Kälte-SPS Firmware V2.9.7, Fernwartungsrouter Ewon Cosy 14.4 mit eigenem Tunnel	kein Zertifikat unter V3.1; Router je Gerät prüfen	3	Firmware auf V3.1, Router entfernen, Zugang nur über Jump-Host
Z12	Füller V3.0.2, Inspektor-PC Windows 10 IoT 2019, Bedienplatz 3 Windows 10	kein Zertifikat, Betriebssystem ohne Sollstand	3	Firmware auf V3.1, Inspektor auf 2021 LTSC, Whitelisting, Mikrosegmente je Maschine
Z11	AS-35 Firmware V2.9.7	kein Zertifikat unter V3.1	2	Firmware auf V3.1
Z08	Schrotmühle mit S7-300 (abgekündigt)	kein Zertifikat, keine Sicherheitsupdates	2	Mikrosegment, nur lesender Zugriff, Ersatz einplanen
Z07	Linienmanagement über OPC UA	abhängig von Security Mode	3	OPC UA mit SignAndEncrypt und Zertifikaten je Maschine
Z15	Druckluft und Waage über Modbus/TCP	Modbus ohne Authentisierung	2 bis 3	nur lesend, Mikrosegment
Z04, Z05	Windows-Systeme	je Produkt prüfen	3	Härtung, Whitelisting, Konten je Person, MFA; Nachweis 62443-3-3 durch den Integrator

Firmwarestände aus dem Asset-Inventar (fiktiv). Zertifikate nach IEC 62443-4-2 liegen laut Hersteller vor für S7-1500 ab V3.1, S7-1200 G2, SCALANCE Layer-2 managed und SC-600; 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; Zertifikat und Herstellererklärung getrennt ausweisen	IEC 62443-4-2
L-02	Nachweis der Systemanforderungen nach IEC 62443-3-3 für das konkrete System durch den Integrator	IEC 62443-3-3
L-03	Maschinenhersteller: keine eigenen Router, Fernwartung nur über Jump-Host mit Freigabe je Sitzung	SR 1.13, IEC 62443-2-4
L-04	Linienmaschinen: Weihenstephaner Standards über OPC UA mit SignAndEncrypt, Benutzerverwaltung, Kommunikationsmatrix	SR 3.1, 4.1, 7.7

Nr.	Anforderung an Lieferanten	Bezug
L-05	Kälteanlagenbauer: Hochdruckabschaltung und Gaswarnung hart verdrahtet nach DIN EN 378 und TRAS 110, Prüfnachweise	BetrSichV, TRAS 110
L-06	Steuerungen: PUT/GET aus, Zugriffsschutz, Grenzen für sicherheits- und lebensmittelrelevante Sollwerte in der SPS	SR 2.1, 3.5
L-07	Sicherheitsupdates und Schwachstellenmeldungen über die Nutzungsdauer	IEC 62443-4-1, CRA
L-08	Sicherungs- und Wiederherstellungsanleitung, Sollstände übergeben	SR 7.3, 7.4

10 Freigabe (ZCR 7)

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