BERICHT

Risikobewertung nach IEC 62443-3-2

Hartkäserei im Bestand, Planungsstand Index C

Auftraggeber	[Betreiber, Ort]
Projekt	Klinikum, 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 Klinik-Technik ist in 15 Zonen und 10 Conduits gegliedert. 7 Zonen erhalten SL-T 3, darunter Energie, medizinische Gase und Brandschutz.

Von 11 bewerteten Bedrohungen sind ohne Maßnahmen 2 kritisch und 2 hoch. Mit den Maßnahmen liegt keine über MITTEL. Die größten Lücken liegen bei der Schnittstelle zur OP-Planung, bei den LTE-Zugängen der Dienstleister und bei Herstellersystemen mit veralteten Betriebssystemen.

GESAMTBEWERTUNG

Zonen halten Angriffe aus der IT und von fremden Geräten ab. Gewollte Wege wie die OP-Planung und die Herstellerfernwartung schützen nur Plausibilisierung und Freigabe je Sitzung.

Klasse	Ohne Maßnahmen	Mit Maßnahmen
KRITISCH	2	0
HOCH	2	1
MITTEL	7	4
NIEDRIG	0	6

2 System under Consideration (ZCR 1)

Betrachtet wird die technische Gebäudeausrüstung des Klinikums einschließlich aller Fernzugänge. Medizingeräte, KIS und PACS gehören zur IT und sind nicht Teil der Betrachtung. Grenzen sind die Übergänge zur IT (K01) und zum Internet (K02, K07, K08).

- **Nicht betrachtet:** physische Sicherheit des Geländes und Prozesse des Betreibers (Managementsystem nach IEC 62443-2-1).
- **Annahmen:** Brandfallsteuerung in der BMZ, Netzersatzstart und Druckregelung der medizinischen Gase eigenständig; Gewerke mit Herstellersteuerung 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	Patienten, Personal	Versorgung	Betrieb, Finanzen
1	keine Gefährdung	keine Einschränkung	unter 10.000 €
2	Belästigung	einzelne Leistungen verzögert	unter 100.000 €
3	Gefährdung einzelner Patienten	OPs verschoben, Abmeldung einzelner Bereiche	unter 1 Mio. €
4	Schaden für Patienten	Abmeldung der Notaufnahme, Verlegungen	über 1 Mio. €
5	Lebensgefahr für Patienten	Ausfall der stationären Versorgung	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, Steuerweg OP	4	KRITISCH
Z04	GLT-Leitebene	Übersicht aller Gewerke	5	KRITISCH
Z05	Engineering	alle Steuerungen	4	KRITISCH

Zone	Bezeichnung	Schlimmster Fall	A	Risiko
Z06	OT-Management	Trennung aller Zonen	4	KRITISCH
Z07	RLT, Wärme, Kälte	OP-Lüftung, Trinkwasser	5	KRITISCH
Z08	Energie	Sicherheitsversorgung	5	KRITISCH
Z09	Medizinische Gase	Beatmung, Narkose	5	KRITISCH
Z10	Brandschutz	Menschen im Brandfall	5	KRITISCH
Z11	Rohrpost	Laborproben	3	HOCH
Z12	Parkhaus	Abgase, Strom	3	HOCH
Z13	Aufzüge	Personen im Aufzug	4	KRITISCH
Z14	Lichtruf	Patientenrufe	4	KRITISCH
Z16	Gebäudesicherheit	Zutritt	3	HOCH
Z18	Temporär verbundene Geräte	alle Gewerke	4	KRITISCH
Z15	Sicherheitsfunktionen	Mensch	5	KRITISCH

5 Zonen, Conduits, Mikrosegmente (ZCR 3)

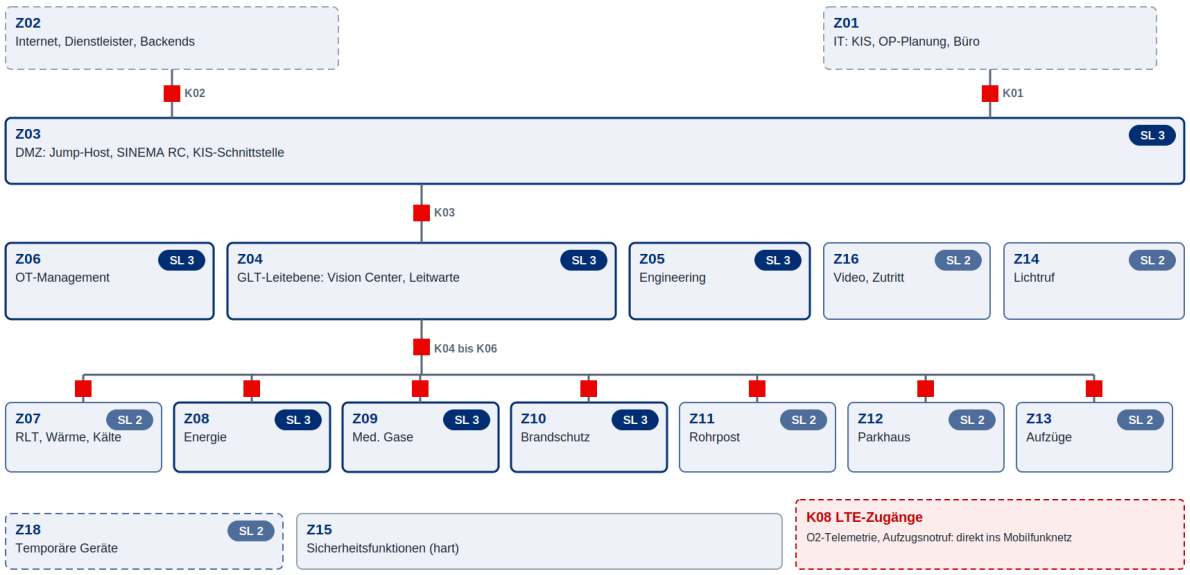


Abbildung: Zonen und Conduits mit SL-T

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); jedes Gewerk ist eine eigene Zone.

Zone	Bezeichnung	Inhalt	SL-T
Z03	DMZ	Jump-Host, Fernwartung, KIS-Schnittstelle	3
Z04	GLT-Leitebene	Vision Center, Leitwarte, Energiemanagement	3
Z05	Engineering	CASE Suite, TIA Portal	3
Z06	OT-Management	Firewalls, Switches, Monitoring	3
Z07	RLT, Wärme, Kälte	Automationsstationen, Kältemaschinen, BSK-Bus	2
Z08	Energie	NSHV, Netzersatz, USV	3
Z09	Medizinische Gase	Kompressoren, Vakuum, Alarmzentralen	3
Z10	Brandschutz	BMZ-Schnittstelle, Sprachalarm, Entrauchung	3
Z11	Rohrpost	Zentrale, Steuerungen	2
Z12	Parkhaus	Parkraummanagement, Ladepunkte, CO-Warnung	2
Z13	Aufzüge	Aufzugssteuerungen, Notruf	2
Z14	Lichtruf	Rufanlage	2
Z16	Gebäudesicherheit	Video, Zutritt	2
Z18	Temporär verbundene Geräte	Service-Laptops	2
Z15	Sicherheitsfunktionen	Brandfallsteuerung, Netzersatzstart, Druckregelung, CO-Lüftung	hart verdrahtet

CONDUITS

Conduit	Verbindet	Datenflüsse	Schutz	SL-T
K01	Z01 IT ↔ Z03	OP-Plan, Administration	Firewall (R01, R29)	3
K02	Z02 ↔ Z03	Herstellerfernwartung	SINEMA RC (R24)	3
K03	Z03 ↔ Z04, Z05	Betriebsart OP, Administration	Firewall (R02, R23)	3
K04	Z04 ↔ Z07	BACnet	Firewall (R03 bis R05)	3
K05	Z04 ↔ Z08, Z09	Modbus, SNMP, OPC UA	Zellenfirewalls (R07 bis R12)	3
K06	Z10 → Z04	BMA-Meldungen	Zellenfirewall (R13)	3
K07	Z12 ↔ Z02	Parkhaus-Backend, OCPP	Zellenfirewall (R18, R20)	2
K08	LTE-Zugänge	O2-Telemetrie, Aufzugsnotruf	keine Firewall	1
K09	Z05 ↔ Zonen	Engineering	Firewall (R26 bis R28)	3
K10	Z06 ↔ alle	Zeit, Überwachung	Management (R30)	3

MIKROSEGMENTE

Zone	Segmente
Z03	Jump-Host: 1 Geräte; Fernwartungsgateway: 1 Geräte; KIS-Schnittstelle: 1 Geräte; Dienste: 2 Geräte
Z04	Vision Center: 2 Geräte; Leitwarte: 3 Geräte; Energiemanagement: 1 Geräte
Z05	Engineering GLT: 1 Geräte; Engineering SPS: 1 Geräte
Z07	OP-Lüftung: 3 Geräte; Intensiv, Labor, Notaufnahme: 3 Geräte; Halle, Bettenhaus: 4 Geräte; Wärme, Kälte, Trinkwasser: 5 Geräte; Energiezentrale, Parkhaus, Außen: 3 Geräte; Brandschutzklappen: 1 Geräte
Z08	Netzersatz: 3 Geräte; Messung, USV, Sicherheitsbeleuchtung: 9 Geräte
Z09	Erzeuger: 4 Geräte; Alarmzentralen: 8 Geräte; Telemetrie Lieferant: 1 Geräte
Z10	BMA: 2 Geräte; Sprachalarm: 1 Geräte; Entrauchung: 1 Geräte
Z11	Rohrpostzentrale: 1 Geräte; Rohrpost-Steuerungen: 6 Geräte
Z12	Parkraummanagement: 1 Geräte; Kassen, Schranken, Kameras: 12 Geräte; CO-Warnung: 1 Geräte; Ladepunkte: 21 Geräte
Z13	Aufzüge: 18 Geräte; Notruf-Gateway: 1 Geräte
Z14	Lichtruf: 2 Geräte

Firewallregeln R01 bis R30 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	Manipulierte Betriebsarten aus der OP-Planung (K1)	5	3	KRITISCH	Plausibilisierung, Bestätigung im Saal	2	HOCH
T03-2	Missbrauch der Herstellerfernwartung (K5)	4	3	HOCH	Freigabe je Sitzung (SR 1.13)	2	MITTEL

6.1.2 Z04 GLT-Leitebene

Nr.	Bedrohung	A	Wo	Ohne	Maßnahmen	Wm	Mit
T04-1	Ransomware im Vision Center (K6)	4	3	HOCH	Whitelisting, Offline-Sicherung	1	NIEDRIG
T04-2	Probelauf mit Last aus dem Energiemanagement (K2)	4	2	MITTEL	Sperre in der SPS	1	NIEDRIG

6.1.3 Z07 RLT, Wärme, Kälte

Nr.	Bedrohung	A	Wo	Ohne	Maßnahmen	Wm	Mit
T07-1	Sollwerte per BACnet verändert (K4)	4	2	MITTEL	Schreibschutz, feste Grenzen	1	NIEDRIG

6.1.4 Z09 Medizinische Gase

Nr.	Bedrohung	A	Wo	Ohne	Maßnahmen	Wm	Mit
T09-1	Alarmzentrale meldet nicht	5	1	MITTEL	Alarm vor Ort, Rundgänge	1	MITTEL
T09-2	O2-Telemetrie über LTE als Einfallstor	3	2	MITTEL	Telemetrie ohne Verbindung ins OT-Netz	1	NIEDRIG

6.1.5 Z10 Brandschutz

Nr.	Bedrohung	A	Wo	Ohne	Maßnahmen	Wm	Mit
T10-1	Brandmeldungen unterdrückt oder gefälscht	5	1	MITTEL	BMZ führend, nur lesende Kopplung	1	MITTEL

6.1.6 Z12 Parkhaus

Nr.	Bedrohung	A	Wo	Ohne	Maßnahmen	Wm	Mit
T12-1	Ladepunkte über das Backend manipuliert (K3)	3	3	MITTEL	Lokale Leistungsgrenze, TLS	1	NIEDRIG

6.1.7 Z13 Aufzüge

Nr.	Bedrohung	A	Wo	Ohne	Maßnahmen	Wm	Mit
T13-1	Aufzüge über LTE-Notruf erreichbar	3	2	MITTEL	Notruf ohne Steuerzugriff	1	NIEDRIG

6.1.8 Z18 Temporär verbundene Geräte

Nr.	Bedrohung	A	Wo	Ohne	Maßnahmen	Wm	Mit
T18-1	Service-Laptop mit Schadsoftware (K4)	4	4	KRITISCH	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	Schnittstelle zur IT
Z04	GLT-Leitebene	3	3	3	2	3	2	3	3	schreibt auf alle AS
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	RLT, Wärme, Kälte	2	2	3	1	3	2	3	2	OP-Lüftung lebenswichtig
Z08	Energie	3	3	3	1	3	2	3	3	Versorgung OP und Intensiv
Z09	Medizinische Gase	3	3	3	1	3	2	3	3	Regelung mechanisch
Z10	Brandschutz	3	3	3	1	3	2	3	3	BMZ führend, hart
Z11	Rohrpost	2	2	2	1	2	2	2	2	Notbetrieb mit Boten
Z12	Parkhaus	2	2	2	2	2	2	2	2	öffentlich zugänglich
Z13	Aufzüge	2	2	3	1	2	2	3	2	LTE-Notruf
Z14	Lichtruf	2	2	3	1	2	2	3	2	eigenes System
Z16	Gebäudesicherheit	2	2	2	2	2	1	2	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
Z11	Rohrpostzentrale Windows 7 Embedded	kein Support	2	Neuaufbau mit Hersteller, bis dahin Zone abschotten
Z09	O2-Telemetrie LTE-Router Firmware 2.1	veraltet, eigener Mobilfunkzugang	3	Firmware, keine Verbindung ins OT-Netz
Z07	AS-02 OP-Lüftung Firmware 1.8	unter Sollstand	2	Update im Wartungsfenster außerhalb des OP-Betriebs
Z12	Kassenautomat 2 Windows LTSB 2016	Support endet	2	Update mit Hersteller
Z12	Ladepunkt 7 Firmware 4.9	unter Sollstand	2	Update, TLS-Profil

Zone	Komponente, Befund	SL-C erwartet	SL-T	Kompensierende Maßnahme
Z13	Notruf-Gateway Aufzüge 2.6	unter Sollstand, LTE	2	Update, Trennung vom OT-Netz

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 Sauter, Cerberus PRO 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 Automationsstationen, Server und Herstellersteuerungen	IEC 62443-4-2
L-02	Keine eigenen LTE- oder Internetzugänge; Fernwartung über den zentralen Zugang	SR 1.13, IEC 62443-2-4
L-03	BACnet mit Schreibschutz bzw. BACnet/SC; Sollwertgrenzen in der Automationsstation	SR 3.5
L-04	OCPP mit TLS und Zertifikaten je Ladepunkt (Security Profile 2 oder 3)	OCPP 1.6J Security
L-05	Unterstützte Betriebssysteme mit Update-Zusage über die Nutzungsdauer	B3S medizinische Versorgung
L-06	Schnittstelle OP-Planung mit Plausibilisierung	SR 3.5
L-07	Dokumentation aller Schnittstellen und Konten	SR 1.1
L-08	Nachweise für § 39 BSIG und § 391 SGB V	BSIG, SGB V

10 Freigabe (ZCR 7)

Rolle	Name	Datum	Unterschrift
Krankenhausleitung	[Name]		
Technischer Leiter	[Name]		
Verfasser	Maximilian Gilg, OT-Cyber.de		