BERICHT

Kommunikation, Steuerungs- und Schutzkonzept

Klinikum: Zonen, Kommunikationsmatrix, Protokolle, Sicherheitsfunktionen, SPS-Programme, Datenflüsse

Auftraggeber	[Betreiber, Ort]
Projekt	Klinikum, 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 des Betriebs

1 Architektur

Die Technik des Klinikums gliedert sich in die GLT-Leitebene mit Sauter Vision Center, Leitwarte und Energiemanagement sowie in Zonen für RLT, Wärme und Kälte, Energie, medizinische Gase, Brandschutz, Rohrpost, Parkhaus, Aufzüge und Lichtruf. Gewerke mit eigener Herstellersteuerung liegen hinter SCALANCE SC646. Die IT mit KIS und OP-Planung erreicht die Technik nur über die DMZ.

- **OP-Planung:** Die Schnittstelle in der DMZ übernimmt den OP-Plan und setzt im Vision Center die Betriebsart der Säle (OP, Bereitschaft, Aus).
- **Brandschutz:** Die Brandmeldeanlage ist führend; die GLT liest per BACnet nur mit. Brandfallsteuerung und Entrauchung laufen hart bzw. in der BMZ.
- **Fernwartung:** zentral über SINEMA Remote Connect mit Freigabe je Sitzung. Die Telemetrie des Gaselieferanten am O2-Tank und das Notruf-Gateway der Aufzüge haben eigene LTE-Zugänge; sie umgehen die Firewall, bis sie getrennt sind.
- **Parkhaus:** Ladepunkte sprechen OCPP mit dem Lastmanagement, das Lastmanagement mit dem Backend des Betreibers.

2 Zonen und Segmente

Zone	Bezeichnung	SL-T	Segmente (Stufe 2)
Z01	IT Klinikum	-	ein Segment
Z02	Internet, Dienstleister	-	ein Segment
Z03	DMZ	3	Jump-Host; Fernwartungsgateway; KIS-Schnittstelle; Dienste
Z04	GLT-Leitebene	3	Vision Center; Leitwarte; Energiemanagement
Z05	Engineering	3	Engineering GLT; Engineering SPS
Z06	OT-Management	3	ein Segment
Z07	RLT, Wärme, Kälte	2	OP-Lüftung; Intensiv, Labor, Notaufnahme; Halle, Bettenhaus; Wärme, Kälte, Trinkwasser; Energiezentrale, Parkh
Z08	Energie	3	Netzersatz; Messung, USV, Sicherheitsbeleuchtung
Z09	Medizinische Gase	3	Erzeuger; Alarmzentralen; Telemetrie Lieferant
Z10	Brandschutz	3	BMA; Sprachalarm; Entrauchung
Z11	Rohrpost	2	Rohrpostzentrale; Rohrpost-Steuerungen
Z12	Parkhaus	2	Parkraummanagement; Kassen, Schranken, Kameras; CO-Warnung; Ladepunkte
Z13	Aufzüge	2	Aufzüge; Notruf-Gateway
Z14	Lichtruf	2	Lichtruf
Z15	Sicherheitsfunktionen	hart verdrahtet	ein Segment

Zone	Bezeichnung	SL-T	Segmente (Stufe 2)
Z16	Gebäudesicherheit	2	ein Segment
Z18	Temporär verbundene Geräte	2	ein Segment

Stufe 1 trennt Zonen mit Firewall und Zellenfirewalls. Stufe 2 trennt innerhalb der Gewerke: nur das Vision Center schreibt auf die Automationsstationen, Messgeräte und Alarmzentralen nur lesend, Ladepunkte nur zum Lastmanagement.

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	OP-Planung (IT)	Schnittstelle OP-Planung zur GLT	HTTPS (TCP 443)	OP-Plan an die Schnittstelle	Z, M
R02	Schnittstelle OP-Planung zur GLT	Sauter Vision Center A, Sauter Vision Center B	HTTPS (TCP 443)	Betriebsart der OP-Säle an die GLT	Z, M
R03	Sauter Vision Center A, Sauter Vision Center B	Z07	BACNET (UDP 47808)	Vision Center zu den Automationsstationen	Z
R04	Sauter Vision Center A, Sauter Vision Center B	Sauter modulo 6 AS-01 OP 1 bis 4, Sauter modulo 6 AS-02 OP 5 bis 8 …	BACNET (UDP 47808)	nur Vision Center zu den Automationsstationen	M
R05	Sauter modulo 6 AS-01 OP 1 bis 4, Sauter modulo 6 AS-02 OP 5 bis 8 …	Sauter Vision Center A, Sauter Vision Center B	BACNET (UDP 47808)	Ereignismeldungen (COV) an das Vision Center	Z, M
R06	Sauter modulo 6 AS-11 Kälte, Sauter modulo 6 AS-12 Wärme, Sauter m …	Kältemaschine KM-01, Kältemaschine KM-02	MODBUS (TCP 502)	Kältemaschinen	Z, M
R07	Sauter Vision Center A, Sauter Vision Center B, Energiemanagement	Z08	MODBUS (TCP 502)	Energiedaten lesen	Z
R08	Sauter Vision Center A, Sauter Vision Center B, Energiemanagement	Messgerät NSHV AV T1, Messgerät NSHV AV T2, Messgerät NSHV SV, Mes …	MODBUS (TCP 502)	Energiedaten lesen	M
R09	Sauter Vision Center A, Sauter Vision Center B	USV OP A, USV OP B, USV ITS A, USV ITS B	SNMP (UDP 161)	USV-Zustand	Z, M
R10	Energiemanagement	Steuerung Netzersatz und Umschaltung	OPCUA (TCP 4840)	Probelauf Netzersatz anfordern	Z, M
R11	Sauter Vision Center A, Sauter Vision Center B	Z09	MODBUS (TCP 502)	Meldungen medizinische Gase	Z

Regel	Quelle	Ziel	Dienst	Zweck	Stufe
R12	Sauter Vision Center A, Sauter Vision Center B	Kompressor med. Druckluft 1, Kompressor med. Druckluft 2, Vakuumpu …	MODBUS (TCP 502)	Meldungen medizinische Gase, lesend	M
R13	BACnet-Schnittstelle Brandmelderzentrale	Sauter Vision Center A, Sauter Vision Center B	BACNET (UDP 47808)	Brandmeldungen an die GLT (nur lesend)	Z, M
R14	Sauter Vision Center A, Sauter Vision Center B	Steuerung Entrauchung	BACNET (UDP 47808)	Zustand Entrauchung	Z, M
R15	Leitwarte Technik Platz 1, Leitwarte Technik Platz 2, Leitwarte Te …	Sauter Vision Center A, Sauter Vision Center B, Rohrpostzentrale (…	HTTPS (TCP 443)	Bedienoberflächen in der Leitwarte	Z, M
R16	Rohrpostzentrale (Windows)	Rohrpost-Steuerung 1, Rohrpost-Steuerung 2, Rohrpost-Steuerung 3, …	S7 (TCP 102)	Rohrpostzentrale zu den Steuerungen	M
R17	Parkraummanagement-Server	Kassenautomat 1, Schranke Einfahrt 1, Kennzeichenkamera 1, Kassena …	PARK (TCP 22100)	Parkraummanagement zu Kassen, Schranken, Kameras	M
R18	Parkraummanagement-Server	Parkhaus-Backend (Cloud)	HTTPS (TCP 443)	Parkhaus-Backend	Z, M
R19	Ladepunkt 1, Ladepunkt 2, Ladepunkt 3, Ladepunkt 4, Ladepunkt 5, L …	Lastmanagement Ladepunkte	OCPP (TCP 8443)	Ladepunkte zum Lastmanagement	Z, M
R20	Lastmanagement Ladepunkte	Backend Ladepunktbetreiber	OCPP (TCP 8443)	Lastmanagement zum Betreiber-Backend	Z, M
R21	Sauter modulo 6 AS-15 Parkhaus Lüftung	CO/NO2-Warnzentrale	MODBUS (TCP 502)	CO-Werte an die GLT	Z, M
R22	Lichtrufserver	Lichtruf-Gateway DECT	ESPA (TCP 22200)	Rufe an DECT	Z, M
R23	Jump-Host	Z04, Z05	RDP (TCP 3389)	Administration über den Jump-Host	Z, M
R24	Fernwartung GLT-Errichter, Fernwartung Rohrposthersteller, Fernwar …	Fernwartungsgateway SINEMA RC	VPN (UDP 1194)	Fernwartung über SINEMA RC	Z, M

Regel	Quelle	Ziel	Dienst	Zweck	Stufe
R25	Fernwartungsgateway SINEMA RC	Sauter Vision Center A, Rohrpostzentrale (Windows), Bedienstation …	RDP (TCP 3389)	Fernbedienung nach Freigabe	Z, M
R26	Engineering Sauter CASE Suite	Z07	BACNET (UDP 47808)	Engineering GLT	Z
R27	Engineering Sauter CASE Suite	Sauter modulo 6 AS-01 OP 1 bis 4, Sauter modulo 6 AS-02 OP 5 bis 8 …	BACNET (UDP 47808)	Engineering GLT	M
R28	Engineering TIA Portal	Steuerung Netzersatz und Umschaltung, Steuerung Entrauchung, Rohrp …	S7 (TCP 102)	Engineering SPS	Z, M
R29	Büro-PC Technische Abteilung (IT)	Jump-Host	RDP (TCP 3389)	Technische Abteilung über den Jump-Host	Z, M
R30	OT-Monitoring, Zeitserver, Firewall OT	alle	MGMT (UDP 161)	Zeit, Überwachung, Verwaltung	Z, M

4 Protokolle und ihre Absicherung

Protokoll	Einsatz	Absicherung
BACnet/IP	Vision Center zu den Automationsstationen, BMA-Meldungen, BSK-Bus	nur das Vision Center schreibt, BACnet/SC prüfen
Modbus/TCP	Energie, Kältemaschinen, medizinische Gase, CO-Warnung	nur lesend, feste Partner
SNMPv3	USV-Anlagen, Netzwerk	authPriv
OPC UA	Energiemanagement zum Netzersatz	SignAndEncrypt, Freigabe in der SPS
S7 mit TLS	Rohrpost, Netzersatz, Entrauchung	nur von Zentrale bzw. Engineering
OCPP 1.6J über TLS	Ladepunkte, Lastmanagement, Betreiber-Backend	Zertifikate je Ladepunkt, lokale Leistungsgrenze
HTTPS	OP-Planung, Leitwarte, Parkhaus-Backend	Zertifikate, feste Partner
VPN, RDP	Herstellerfernwartung	SINEMA RC mit Freigabe je Sitzung
ESPA 4.4.4	Lichtruf zu DECT	eigene Zone

5 Sicherheitsfunktionen

Die folgenden Funktionen schützen Patienten, Personal und Gebäude. Sie bleiben wirksam, wenn Gebäudeleittechnik oder Netz gestört oder manipuliert sind.

Funktion	Auslöser	Wirkung	Ausführung
Brandfallsteuerung	Brandmeldung	RLT aus, BSK zu, Aufzüge, Türen, RWA, Entrauchung, Sprachalarm	BMZ, Ansteuermodule
Netzersatzstart	Netzausfall	Start ≤ 15 s, Lastzuschaltung in Stufen	Aggregatsteuerung, AS-NEA
USV OP und Intensiv	Netzunterbrechung	unterbrechungsfrei	USV-Anlagen
Isolationsüberwachung	Isolationsfehler Gruppe 2	Meldung, keine Abschaltung	IT-System
Druckregelung med. Gase	Druckabfall	Umschaltung auf Reserve	mechanisch, Anlagensteuerung
CO-Lüftung Parkhaus	CO über 35 ppm	Lüftung ein, Warnung	CO-Warnzentrale
Aufzug Brandfallfahrt	BMA	Fahrt in die Hauptebene	Aufzugssteuerung

6 SPS-Programme

Baustein	Steuerung	Funktion
FB_NEA_Probelauf	AS-NEA	Probelauf nur mit Freigabe, Lastumschaltung nie während OP-Betrieb, Zeitfenster
FB_NEA_Lastzuschaltung	AS-NEA	Lastzuschaltung in fünf Stufen nach Priorität
FB_SV_Ueberwachung	AS-NEA	Dieselvorrat, Zentralbatterie, USV-Bypass
FB_Entrauchung_Freigabe	ENT	Auslösung nur durch BMZ oder Feuerwehr, GLT nur Test mit Schlüsselschalter

Die Programme liegen als Klinikum_SPS_Programme.scl bei. Die Gebäudeleittechnik wird in der Sauter CASE Suite programmiert; Herstellersteuerungen gehören zum Lieferumfang der Gewerke.

7 Datenflüsse des Betriebs

- **OP-Betrieb:** OP-Planung an die Schnittstelle, Betriebsart an das Vision Center, Druckhaltung und Temperatur zurück an die Leitwarte.
- **Energie:** Messgeräte und Aggregate an Energiemanagement und Vision Center; Probelauf nur mit Freigabe.
- **Alarme:** Alarmzentralen der medizinischen Gase, BMA-Meldungen und Störungen aller Gewerke laufen in der Leitwarte zusammen.
- **Parkhaus:** Kassen und Schranken am Parkraummanagement, Ladepunkte am Lastmanagement, Abrechnung über die Backends.