BERICHT

Risikobewertung nach IEC 62443-3-2

Hartkäserei im Bestand, Planungsstand Index C

Auftraggeber	[Betreiber, Ort]
Projekt	GuD-Heizkraftwerk, 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

Das Heizkraftwerk ist in 15 Zonen und 10 Conduits gegliedert. 8 Zonen erhalten SL-T 3, darunter Kraftwerksleittechnik, Gaszelle, elektrische Anlagen mit Schutz und die Fernwirkverbindung zum Netzbetreiber.

Von 14 bewerteten Bedrohungen sind ohne Maßnahmen 3 kritisch und 6 hoch. Mit den Maßnahmen liegt keine über MITTEL. Die größten Lücken liegen bei den Steuerwegen von außen (Fahrplan, Fernwirk) und beim Engineering-Zugriff auf die Schutzgeräte.

GESAMTBEWERTUNG

Zonen trennen IT, Leitsystem, Zellen und Station. Mikrosegmente verhindern, dass ein Bedienplatz oder ein fremdes Gerät direkt Steuerungen oder Schutzgeräte erreicht. Für die legitimen Steuerwege von außen sind fachliche Prüfungen nötig.

Klasse	Ohne Maßnahmen	Mit Maßnahmen
KRITISCH	3	0
HOCH	6	1
MITTEL	5	7
NIEDRIG	0	6

2 System under Consideration (ZCR 1)

Betrachtet wird die gesamte Leit-, Schutz- und Automatisierungstechnik des Heizkraftwerks von der Gasübernahme bis zum 110-kV-Netzanschluss und zur Fernwärmeübergabe, einschließlich aller Fernzugänge. Grenzen sind die Übergänge zur IT (K01), zum Internet (K02) und zum Fernwirk-WAN des Netzbetreibers (K07).

- **Nicht betrachtet:** physische Sicherheit des Geländes und Prozesse des Betreibers (Managementsystem nach IEC 62443-2-1).
- **Annahmen:** Turbinen- und Kesselschutz im F-Teil bzw. hart, Sicherheitsabsperr- und Abblaseventile mechanisch, Netzschutz eigenständig; Zellen 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	Versorgung, Umwelt	Betrieb, Finanzen
1	keine Gefährdung	keine	unter 10.000 €
2	Erste Hilfe	kurzer Leistungsausfall ohne Folgen	unter 100.000 €
3	leichte Verletzung	Fernwärme eingeschränkt, Regelleistung nicht erbracht	unter 1 Mio. €
4	schwere Verletzung	Fernwärmeausfall über Stunden, Grenzwertüberschreitung	über 1 Mio. €
5	Lebensgefahr: Explosion, Brand, Dampf	Versorgungsausfall, Netzstörung, Gasaustritt	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, Fahrplanweg	4	KRITISCH
Z04	Leitsystem Bedienebene	gesamte Anlage über Bedienung	5	KRITISCH

Zone	Bezeichnung	Schlimmster Fall	A	Risiko
Z05	Engineering	Programme und Schutzparameter	5	KRITISCH
Z06	OT-Management	Trennung aller Zonen, Zeit für Schutz	4	KRITISCH
Z07	Kraftwerksleittechnik	Turbinen, Kessel	5	KRITISCH
Z09	Zelle Gas	Gasaustritt, Explosion	5	KRITISCH
Z10	Zelle Fernwärme	Wärmeversorgung	3	HOCH
Z11	Zelle Hilfssysteme	Kesselschaden nach Wochen	3	HOCH
Z12	Elektrische Anlagen	Netz, Trafo, Personen	5	KRITISCH
Z13	Fernwirk Netzbetreiber	Netz	4	KRITISCH
Z14	Emissionsüberwachung	Genehmigung	2	MITTEL
Z15	Gebäudeleittechnik	Raumklima Schaltanlagen	2	MITTEL
Z17	Gebäudesicherheit	Zutritt	2	MITTEL
Z18	Temporär verbundene Geräte	alle Zellen	4	KRITISCH
Z16	Sicherheitsfunktionen	Mensch	5	KRITISCH

5 Zonen, Conduits, Mikrosegmente (ZCR 3)

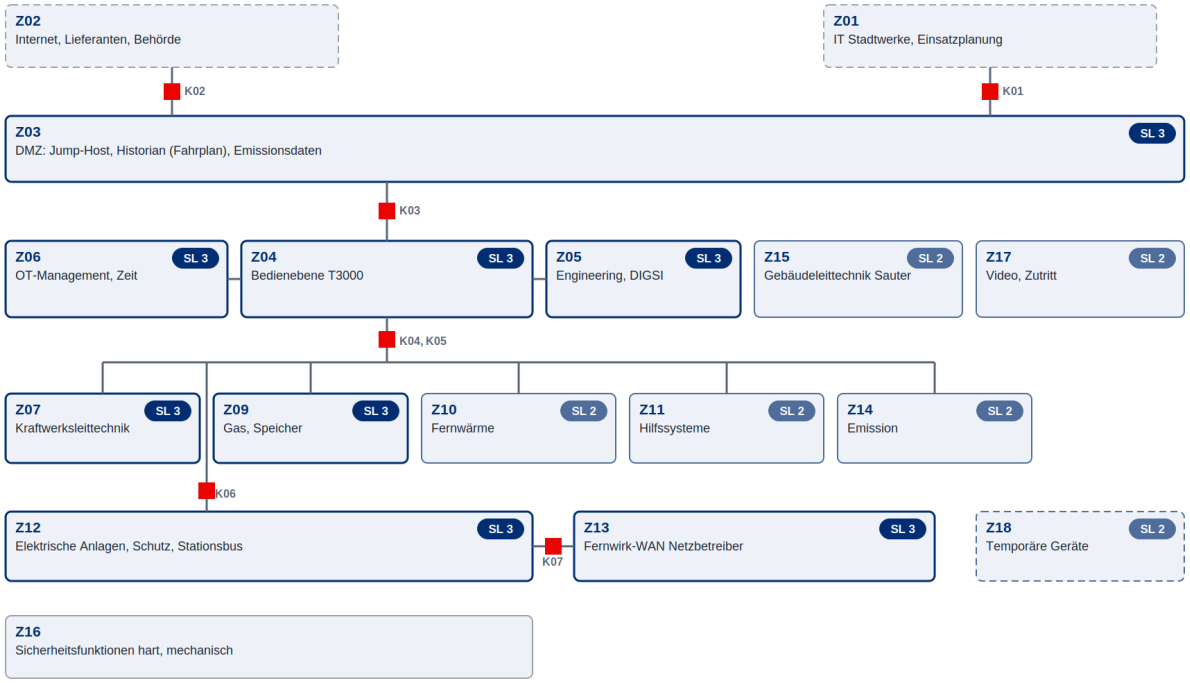


Abbildung: Zonen und Conduits mit SL-T

Getrennt sind Geschäfts- und Steuerungssysteme (ZCR 3.2), Sicherheitsfunktionen (ZCR 3.3, Z16), zeitweise verbundene Geräte (ZCR 3.4) und nicht vertrauenswürdige Netze (ZCR 3.6); das Fernwirk-WAN des Netzbetreibers ist eine eigene Zone.

Zone	Bezeichnung	Inhalt	SL-T
Z03	DMZ	Jump-Host, Historian, Patch, Emissionsdaten, Log	3
Z04	Leitsystem Bedienebene	T3000-Server, Bedienplätze	3
Z05	Engineering	T3000 Engineering, TIA Portal, DIGSI 5	3
Z06	OT-Management	Firewalls, Switches, Zeit, Monitoring	3
Z07	Kraftwerksleittechnik	T3000 AS mit F-Teil, Antriebe	3
Z09	Zelle Gas	AS-GAS, GDRM, Verdichter, Speicher	3
Z10	Zelle Fernwärme	AS-FW, Pumpen, Spitzenkessel	2
Z11	Zelle Hilfssysteme	AS-WA, Vollentsalzung	2
Z12	Elektrische Anlagen	SICAM, SIPROTEC 5, Stationsbus	3
Z13	Fernwirk Netzbetreiber	IEC 104 zur Netzleitstelle	3
Z14	Emissionsüberwachung	Analysatoren, Emissionsrechner	2
Z15	Gebäudeleittechnik	Sauter modulo 6, Vision Center	2
Z17	Gebäudesicherheit	Video, Zutritt	2
Z18	Temporär verbundene Geräte	Service-Laptops	2
Z16	Sicherheitsfunktionen	Gaswarnung, Löschanlage, Brandmelder, Schnellschluss hart	hart verdrahtet

CONDUITS

Conduit	Verbindet	Datenflüsse	Schutz	SL-T
K01	Z01 IT ↔ Z03	Fahrplan, Berichte	Firewall (R25, R26)	3
K02	Z02 ↔ Z03	Fernwartung, Ferndiagnose, Emissionsdaten	Firewall, MFA (R20, R22, R29)	3
K03	Z03 ↔ Z04, Z05	Administration, Fahrplan, Archiv	Firewall (R19, R23, R27)	3
K04	Z04 ↔ Z07	T3000 Systembus	Firewall (R01, R02)	3
K05	Z04 ↔ Z09 bis Z11, Z14	OPC UA lesen	Zellenfirewalls (R03, R04)	3
K06	Z04 ↔ Z12	IEC 61850 MMS	Firewall (R05, R06)	3
K07	Z12 ↔ Z13	IEC 60870-5-104	Fernwirkrouter (R10, R11)	3
K08	Z05 ↔ Zellen, Z12	Engineering, DIGSI	Firewall (R13 bis R18)	3
K09	Z06 ↔ alle	Zeit, Überwachung	Management (R35)	3
K10	Z15 ↔ Z04	GLT-Bedienung	Firewall (R31)	2

MIKROSEGMENTE

Zone	Segmente
Z03	Jump-Host: 1 Geräte; Historian: 1 Geräte; Emissionsdaten: 1 Geräte; Dienste: 2 Geräte
Z04	T3000-Server: 2 Geräte; Bedienplätze: 6 Geräte
Z05	Engineering T3000: 1 Geräte; Engineering TIA, DIGSI: 1 Geräte
Z07	Gasturbine: 4 Geräte; Kessel: 5 Geräte; Dampfturbine: 4 Geräte; Nebenanlagen: 3 Geräte
Z09	Gas-Steuerung: 6 Geräte; Verdichter V-120: 1 Geräte; Verdichter V-121: 1 Geräte
Z10	FW-Steuerung: 6 Geräte; Spitzenkessel SK-1: 1 Geräte; Spitzenkessel SK-2: 1 Geräte
Z11	Wasser-Steuerung: 3 Geräte; Vollentsalzung: 1 Geräte
Z12	Stationsleittechnik: 3 Geräte; Schutz 110 kV: 7 Geräte; Schutz 10 kV: 4 Geräte; Notstrom: 1 Geräte
Z13	Fernwirkrouter: 1 Geräte; Netzleitstelle: 1 Geräte
Z15	Vision Center: 1 Geräte; Automationsstationen: 6 Geräte

Firewallregeln R01 bis R35 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	Fahrplan über den Historian manipuliert (G1)	3	4	HOCH	Plausibilisierung, signierte Fahrpläne (SR 3.5)	2	MITTEL
T03-2	Jump-Host mit gestohlenen Daten (G3, G5, G6)	5	4	KRITISCH	MFA, Freigabe je Sitzung (SR 1.1, 1.13)	2	HOCH

6.1.2 Z04 Leitsystem Bedienebene

Nr.	Bedrohung	A	Wo	Ohne	Maßnahmen	Wm	Mit
T04-1	Ransomware auf T3000-Servern (G6)	4	3	HOCH	Whitelisting (SR 3.2), Sicherung (SR 7.3)	1	NIEDRIG

6.1.3 Z05 Engineering

Nr.	Bedrohung	A	Wo	Ohne	Maßnahmen	Wm	Mit
T05-1	Schutzparameter mit DIGSI verändert (G3)	5	2	HOCH	Vier-Augen, Rollen (SR 2.1), Buchholz und Reserveschutz	1	MITTEL

6.1.4 Z06 OT-Management

Nr.	Bedrohung	A	Wo	Ohne	Maßnahmen	Wm	Mit
T06-1	Zeitserver manipuliert, Schutz und Archiv mit falscher Zeit	3	2	MITTEL	GNSS-Überwachung, redundante Zeitquelle	1	NIEDRIG

6.1.5 Z07 Kraftwerksleittechnik

Nr.	Bedrohung	A	Wo	Ohne	Maßnahmen	Wm	Mit
T07-1	Turbinenregelung verstellt	5	2	HOCH	F-Teil und hart verdrahteter Schutz	1	MITTEL

6.1.6 Z09 Zelle Gas

Nr.	Bedrohung	A	Wo	Ohne	Maßnahmen	Wm	Mit
T09-1	Gasdruck per S7 verstellt (G4)	5	3	KRITISCH	Grenzen in der SPS, SAV und SBV mechanisch (SR 3.5)	1	MITTEL

6.1.7 Z10 Zelle Fernwärme

Nr.	Bedrohung	A	Wo	Ohne	Maßnahmen	Wm	Mit
T10-1	Vorlauftemperatur oder Pumpen verstellt	3	2	MITTEL	Grenzen in der SPS, Druckhaltung autark	1	NIEDRIG

6.1.8 Z11 Zelle Hilfssysteme

Nr.	Bedrohung	A	Wo	Ohne	Maßnahmen	Wm	Mit
T11-1	Vollentsalzung über Fernwartung manipuliert (G5)	3	3	MITTEL	Freigabe je Sitzung, VE-Sperre in AS-WA	1	NIEDRIG

6.1.9 Z12 Elektrische Anlagen

Nr.	Bedrohung	A	Wo	Ohne	Maßnahmen	Wm	Mit
T12-1	GOOSE gefälscht, Schalter fallen oder Verriegelung wird umgangen	5	2	HOCH	Stationsbus nur bekannte Geräte, IEC 62351-6 prüfen	1	MITTEL

6.1.10 Z13 Fernwirk Netzbetreiber

Nr.	Bedrohung	A	Wo	Ohne	Maßnahmen	Wm	Mit
T13-1	Schaltbefehle über die Netzleitstelle (G2)	4	3	HOCH	Befehlsliste, IEC 62351 bzw. IPsec, Reaktionsplan mit Netzbetreiber	2	MITTEL

6.1.11 Z14 Emissionsüberwachung

Nr.	Bedrohung	A	Wo	Ohne	Maßnahmen	Wm	Mit
T14-1	Emissionsdaten verfälscht	3	2	MITTEL	Signierte Datenübertragung, unabhängige Kalibrierung	1	NIEDRIG

6.1.12 Z15 Gebäudeleittechnik

Nr.	Bedrohung	A	Wo	Ohne	Maßnahmen	Wm	Mit
T15-1	Raumklima der Schaltanlagen abgeschaltet	3	2	MITTEL	Temperaturüberwachung der Leittechnikräume unabhängig	1	NIEDRIG

6.1.13 Z18 Temporär verbundene Geräte

Nr.	Bedrohung	A	Wo	Ohne	Maßnahmen	Wm	Mit
T18-1	Service-Laptop mit Schadsoftware (G4)	4	4	KRITISCH	Prüfung vor Anschluss, NAC (SR 1.2, 2.3)	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	Fahrplan und Fernzugriff
Z04	Leitsystem Bedienebene	3	3	3	2	3	2	3	3	Bedienweg zu allen AS
Z05	Engineering	3	3	3	3	3	2	2	3	kann Schutz verändern
Z06	OT-Management	3	3	3	2	3	2	3	3	PTP für Schutz
Z07	Kraftwerksleittechnik	3	3	3	1	3	2	3	3	Prozessführung
Z09	Zelle Gas	3	3	3	1	3	2	3	3	Störfall-Betriebsbereich
Z10	Zelle Fernwärme	2	2	3	1	2	2	3	2	Folgen begrenzt durch Speicher
Z11	Zelle Hilfssysteme	2	2	2	1	2	2	2	2	Folgen begrenzt
Z12	Elektrische Anlagen	3	3	3	1	3	2	3	3	Schutz und Schalten
Z13	Fernwirk Netzbetreiber	3	3	3	2	3	2	3	3	externer Steuerweg
Z14	Emissionsüberwachung	2	2	2	1	2	2	2	2	Folgen begrenzt
Z15	Gebäudeleittechnik	2	2	2	1	2	1	2	2	Folgen begrenzt
Z17	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
Z09	AS-GAS Firmware V2.9.7	kein Zertifikat unter V3.1	3	Firmware auf V3.1, Grenzen in der SPS, SAV mechanisch
Z10	Brennersteuerungen SK-1, SK-2 mit S7-300	abgekündigt, keine Updates	2	nur lesend, Sicherheitskette autark, Ersatz planen
Z13	Fernwirkrouter ROX II 2.14	älterer Stand	3	Aktualisieren mit dem Netzbetreiber, IPsec
Z12	SIPROTEC 7UT86 MT1 Firmware V9.40	Sollstand V9.80	3	Aktualisieren im Wartungsfenster, Rollen nach IEC 62351-8

Zone	Komponente, Befund	SL-C erwartet	SL-T	Kompensierende Maßnahme
Z04	Omnivise T3000	je Produkt beim Hersteller anfordern	3	Nachweis IEC 62443-3-3 durch Siemens Energy, Härtungsleitfaden
Z11	Vollentsalzung Firmware V3.0.2	kein Zertifikat unter V3.1	2	Firmware auf V3.1, VE-Sperre in AS-WA

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; für T3000, SICAM, SIPROTEC und RUGGEDCOM je Produkt 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	Systemnachweis nach IEC 62443-3-3 für T3000 und Stationsleittechnik	IEC 62443-3-3
L-03	Fernzugriff nur über den Jump-Host mit Freigabe je Sitzung; Ferndiagnose nur als Datenexport	SR 1.13, IEC 62443-2-4
L-04	Schutzgeräte mit Rollen nach IEC 62351-8 und sicherer Kommunikation, wo verfügbar	IEC 62351
L-05	Fernwirk: Befehlsliste und Absicherung mit dem Netzbetreiber vereinbaren	VDE-AR-N 4120, IEC 62351-3
L-06	Zellen-SPS mit Zugriffsschutz und festen Grenzen	SR 2.1, 3.5
L-07	Sicherheitsupdates nach Herstellerfreigabe über die Nutzungsdauer	IEC 62443-4-1, CRA
L-08	Nachweise für den IT-Sicherheitskatalog Energieanlagen	§ 5c EnWG

10 Freigabe (ZCR 7)

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