BERICHT

Risikobewertung nach IEC 62443-3-2

Hartkäserei im Bestand, Planungsstand Index C

Auftraggeber	[Betreiber, Ort]
Projekt	Umspannwerke, 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

Netzleitstelle, Umspannwerke und Ortsnetz sind in 16 Zonen und 10 Conduits gegliedert. 9 Zonen erhalten SL-T 3, darunter Leitsystem, Fernwirk-WAN, beide Stationen und der Prozessbus.

Von 14 bewerteten Bedrohungen sind ohne Maßnahmen 3 kritisch und 4 hoch. Mit den Maßnahmen liegt keine über MITTEL. Die größten Lücken liegen bei den Konten der Leitstelle, beim Funknetz der Ortsnetzstationen und beim Prozessbus.

GESAMTBEWERTUNG

Zonen und das getrennte Fernwirk-WAN halten Angriffe aus der IT ab. Mikrosegmente verhindern, dass ein Funkrouter andere Stationen oder ein fremdes Gerät den Schutz erreicht. Den regulären Steuerweg der Leitstelle schützt nur die Befehlsprüfung in den Stationen.

Klasse	Ohne Maßnahmen	Mit Maßnahmen
KRITISCH	3	0
HOCH	4	2
MITTEL	6	5
NIEDRIG	1	7

2 System under Consideration (ZCR 1)

Betrachtet werden Netzleitstelle, beide Umspannwerke, fernwirktechnisch angebundene Ortsnetzstationen und die Schnittstelle zum PV-Park, einschließlich aller Fernzugänge. Grenzen sind die Übergänge zur IT (K01), zum Internet (K02) und zum Übertragungsnetzbetreiber (K07).

- **Nicht betrachtet:** physische Sicherheit des Geländes und Prozesse des Betreibers (Managementsystem nach IEC 62443-2-1).
- **Annahmen:** Schutz eigenständig in den SIPROTEC-Geräten, Buchholz und Druckentlastung hart; Kundenanlage PV-Park hinter SC646; Ortsnetzstationen über privates APN.
- **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	Betrieb, Finanzen
1	keine Gefährdung	keine Unterbrechung	unter 10.000 €
2	Erste Hilfe	einzelne Ortsnetzstationen kurz ohne Strom	unter 100.000 €
3	leichte Verletzung	Stadtteile bis 1 h ohne Strom	unter 1 Mio. €
4	schwere Verletzung	große Teile der Stadt mehrere Stunden ohne Strom	über 1 Mio. €
5	Lebensgefahr: Lichtbogen, Brand, Ausfall kritischer Verbraucher	gesamte Stadt ohne Strom, Störung im Verbundnetz	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, Abrufweg	4	KRITISCH
Z04	Netzleitsystem	Versorgung der Stadt	5	KRITISCH

Zone	Bezeichnung	Schlimmster Fall	A	Risiko
Z05	Engineering	Schutz und Stationen	5	KRITISCH
Z06	OT-Management	Trennung aller Zonen	4	KRITISCH
Z07	Fernwirk-WAN	Steuerweg zu allen Stationen	4	KRITISCH
Z08	Kopplung ÜNB	Verbundnetz	4	KRITISCH
Z09	UW Nord Station	Versorgung Nord	5	KRITISCH
Z10	UW Süd Station	Versorgung Süd	5	KRITISCH
Z11	UW Süd Prozessbus	Messwerte des Schutzes	5	KRITISCH
Z12	Ortsnetzstationen	Straßenzüge	3	HOCH
Z13	PV-Park	Spannung Netz Süd	3	HOCH
Z14	Hilfsenergie	Schutz ohne Hilfsenergie	4	KRITISCH
Z15	Gebäudeleittechnik	Raumklima	2	MITTEL
Z17	Gebäudesicherheit	unbesetzte Stationen	3	HOCH
Z18	Temporär verbundene Geräte	Schutzgeräte	4	KRITISCH
Z16	Schutzfunktionen hart	Mensch, Anlage	5	KRITISCH

5 Zonen, Conduits, Mikrosegmente (ZCR 3)

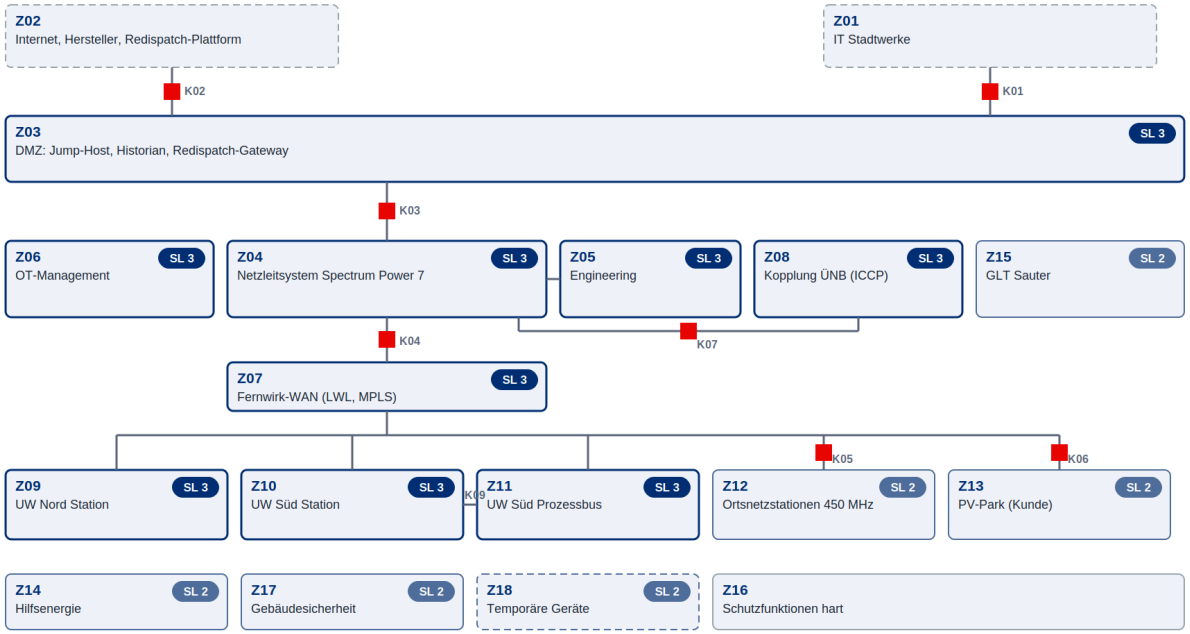


Abbildung: Zonen und Conduits mit SL-T

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); Kundenanlage und ÜNB-Kopplung sind eigene Zonen.

Zone	Bezeichnung	Inhalt	SL-T
Z03	DMZ	Jump-Host, Historian, Redispatch-Gateway	3
Z04	Netzleitsystem	Spectrum Power 7, Front-End, Arbeitsplätze	3
Z05	Engineering	Leitsystem, DIGSI 5, Device Manager	3
Z06	OT-Management	Firewalls, Switches, Zeit, Monitoring	3
Z07	Fernwirk-WAN	MPLS-Router	3
Z08	Kopplung ÜNB	ICCP-Gateway	3
Z09	UW Nord Station	SICAM, SIPROTEC, Regler	3
Z10	UW Süd Station	SICAM, SIPROTEC, Regler	3
Z11	UW Süd Prozessbus	Merging Units, PTP	3
Z12	Ortsnetzstationen	Fernwirkstationen, Funkrouter	2
Z13	PV-Park	Parkregler, Übergabeschutz	2
Z14	Hilfsenergie	Gleichrichter, Batterie	2
Z15	Gebäudeleittechnik	Sauter modulo 6	2
Z17	Gebäudesicherheit	Einbruchmelde, Zutritt, Video	2
Z18	Temporär verbundene Geräte	Service-Laptops, Prüfkoffer	2
Z16	Schutzfunktionen hart	Buchholz, Druckentlastung, Notauslösung	hart verdrahtet

CONDUITS

Conduit	Verbindet	Datenflüsse	Schutz	SL-T
K01	Z01 IT ↔ Z03	Berichte	Firewall (R23)	3
K02	Z02 ↔ Z03	Fernwartung, Redispatch-Plattform	Firewall, MFA (R20, R24)	3
K03	Z03 ↔ Z04, Z05	Administration, Abrufe, Archiv	Firewall (R18, R19, R21, R25)	3
K04	Z04 ↔ Z09, Z10 über Z07	IEC 104	Fernwirk-WAN, Firewall (R01, R02)	3
K05	Z04 ↔ Z12	IEC 104 über 450 MHz	Kopfstelle, IPsec (R03, R04, R28)	3
K06	Z04 ↔ Z13	IEC 104 PV-Park	SC646 (R05, R06)	3
K07	Z04 ↔ Z08	ICCP	Firewall (R26, R27)	3
K08	Z05 ↔ Z09 bis Z11	Engineering	Firewall (R15, R16)	3
K09	Z11 ↔ Z10	Sampled Values	Prozessbus (R11, R12)	3
K10	Z06 ↔ alle	Zeit, Überwachung	Management (R32)	3

MIKROSEGMENTE

Zone	Segmente
Z03	Jump-Host: 1 Geräte; Historian: 1 Geräte; Redispatch-Gateway: 1 Geräte; Dienste: 2 Geräte
Z04	Leitsystem-Server: 2 Geräte; Front-End: 2 Geräte; Arbeitsplätze: 5 Geräte
Z05	Engineering Leitsystem: 1 Geräte; Engineering Schutz: 1 Geräte
Z09	Stationsrechner Nord: 3 Geräte; Schutz 110 kV Nord: 5 Geräte; Schutz 20 kV Nord: 14 Geräte; Regler Nord: 4 Geräte; Zeit Nord: 1 Geräte
Z10	Stationsrechner Süd: 3 Geräte; Schutz 110 kV Süd: 5 Geräte; Schutz 20 kV Süd: 12 Geräte; Regler Süd: 4 Geräte
Z11	Merging Units: 4 Geräte; Zeit Süd: 1 Geräte
Z12	Fernwirkstationen: 8 Geräte; Funkrouter: 9 Geräte
Z13	Parkregler: 1 Geräte; Übergabeschutz: 1 Geräte
Z15	Vision Center: 1 Geräte; Automationsstationen: 3 Geräte

Firewallregeln R01 bis R32 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	Jump-Host mit gestohlenen Daten (U1, U6)	5	4	KRITISCH	MFA, Freigabe je Sitzung (SR 1.1, 1.13)	2	HOCH
T03-2	Redispatch-Gateway übernommen (U5)	3	3	MITTEL	Whitelisting, Plausibilisierung (SR 3.2, 3.5)	1	NIEDRIG

6.1.2 Z04 Netzleitsystem

Nr.	Bedrohung	A	Wo	Ohne	Maßnahmen	Wm	Mit
T04-1	Massenschaltbefehle (U1)	5	3	KRITISCH	Befehlsprüfung, Monitoring	2	HOCH
T04-2	Ransomware in der Leitstelle (U6)	4	3	HOCH	Whitelisting, Offline-Sicherung	1	NIEDRIG

6.1.3 Z05 Engineering

Nr.	Bedrohung	A	Wo	Ohne	Maßnahmen	Wm	Mit
T05-1	Schutzparameter verändert	5	2	HOCH	Vier-Augen, Rollen nach IEC 62351-8	1	MITTEL

6.1.4 Z07 Fernwirk-WAN

Nr.	Bedrohung	A	Wo	Ohne	Maßnahmen	Wm	Mit
T07-1	Fernwirk-WAN abgehört oder manipuliert	4	2	MITTEL	eigenes LWL, MPLS-VRF, IEC 62351-3	1	NIEDRIG

6.1.5 Z08 Kopplung ÜNB

Nr.	Bedrohung	A	Wo	Ohne	Maßnahmen	Wm	Mit
T08-1	Falsche Daten zum ÜNB	4	2	MITTEL	Secure ICCP	1	NIEDRIG

6.1.6 Z09 UW Nord Station

Nr.	Bedrohung	A	Wo	Ohne	Maßnahmen	Wm	Mit
T09-1	Station-HMI mit Schadsoftware	4	3	HOCH	Härtung, Whitelisting	2	MITTEL

6.1.7 Z11 UW Süd Prozessbus

Nr.	Bedrohung	A	Wo	Ohne	Maßnahmen	Wm	Mit
T11-1	Gefälschte Sampled Values (U3)	4	2	MITTEL	Port Security, SV-Plausibilisierung	1	NIEDRIG
T11-2	PTP-Zeit manipuliert	4	2	MITTEL	PTP-Überwachung, Holdover	1	NIEDRIG

6.1.8 Z12 Ortsnetzstationen

Nr.	Bedrohung	A	Wo	Ohne	Maßnahmen	Wm	Mit
T12-1	Funkrouter übernommen (U2)	3	4	HOCH	Firmware, Zertifikate, Trennung der Router	2	MITTEL

6.1.9 Z13 PV-Park

Nr.	Bedrohung	A	Wo	Ohne	Maßnahmen	Wm	Mit
T13-1	Parkregler des Kunden manipuliert (U4)	3	3	MITTEL	Übergabeschutz, Vertragsanforderungen	2	MITTEL

6.1.10 Z14 Hilfsenergie

Nr.	Bedrohung	A	Wo	Ohne	Maßnahmen	Wm	Mit
T14-1	Gleichrichter manipuliert	4	1	NIEDRIG	nur lesend, Überwachung hart	1	NIEDRIG

6.1.11 Z18 Temporär verbundene Geräte

Nr.	Bedrohung	A	Wo	Ohne	Maßnahmen	Wm	Mit
T18-1	Service-Laptop mit Schadsoftware	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	Fernzugriff und Redispatch
Z04	Netzleitsystem	3	3	3	2	3	2	3	3	schaltet das Netz
Z05	Engineering	3	3	3	3	3	2	2	3	kann Schutz verändern
Z06	OT-Management	3	3	3	2	3	2	3	3	steuert die Segmentierung
Z07	Fernwirk-WAN	3	3	3	3	3	2	3	3	verbindet alle Standorte
Z08	Kopplung ÜNB	3	3	3	3	3	2	3	3	externer Partner
Z09	UW Nord Station	3	3	3	1	3	2	3	3	Schutz und Schalten
Z10	UW Süd Station	3	3	3	1	3	2	3	3	Schutz und Schalten
Z11	UW Süd Prozessbus	3	3	3	1	3	2	3	3	Schutz hängt an den Abtastwerten
Z12	Ortsnetzstationen	2	2	3	2	3	2	2	2	öffentlich zugänglich
Z13	PV-Park	2	2	2	2	2	2	2	2	Anlage des Kunden
Z14	Hilfsenergie	2	2	3	1	2	2	3	2	nur lesend angebunden
Z15	Gebäudeleittechnik	2	2	2	1	2	1	2	2	Folgen begrenzt
Z17	Gebäudesicherheit	2	2	2	2	2	1	2	2	Erkennung Vor-Ort-Angriff
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
Z07	Fernwirkrouter UW Nord ROX II 2.14	älterer Stand	3	Aktualisieren, Konfigurationsvergleich
Z09	Station-HMI UW Nord auf Windows 10	kein Herstellersupport	3	Umstellung auf Windows 11 IoT, Whitelisting
Z09	SIPROTEC 7SJ82 J07 Firmware V8.80	unter Sollstand	3	Firmware im Wartungsfenster
Z10	SICAM A8000 Stationsrechner B Süd V5.10	unter Sollstand	3	Firmware nachziehen

Zone	Komponente, Befund	SL-C erwartet	SL-T	Kompensierende Maßnahme
Z12	Fernwirkstation ONS 3 und Funkrouter ONS 6	veraltete Firmware	2	Firmware, Zertifikate
Z13	Parkregler Windows 10 IoT 2019	Anlage des Kunden	2	Anforderung an Betreiber, SC646 davor

Firmwarestände aus dem Asset-Inventar (fiktiv). Zertifikate nach IEC 62443-4-2 für SICAM, SIPROTEC, RUGGEDCOM und Spectrum Power je Produkt beim Hersteller anfordern; SC-600 ist zertifiziert.

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 Leitsystem und Stationsleittechnik	IEC 62443-3-3
L-03	Fernzugriff nur über den Jump-Host mit Freigabe je Sitzung	SR 1.13, IEC 62443-2-4
L-04	Schutzgeräte und Stationsrechner mit Rollen nach IEC 62351-8, TLS nach IEC 62351-3/4	IEC 62351
L-05	Merging Units und Schutz mit SV-Plausibilisierung, PTP nach IEC 61850-9-3	IEC 61850
L-06	Funkrouter mit Zertifikaten je Gerät, keine Standardkonten	SR 1.5
L-07	Kundenanlagen: Anforderungen an Fernzugänge und Parkregler im Netzanschlussvertrag	VDE-AR-N 4110
L-08	Nachweise für den IT-Sicherheitskatalog der Bundesnetzagentur	§ 5c EnWG

10 Freigabe (ZCR 7)

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