BERICHT

Kommunikation, Steuerungs- und Schutzkonzept

Umspannwerke 110/20 kV mit Netzleitstelle: Zonen, Kommunikationsmatrix, Protokolle, Schutz, Stationsautomatisierung, Datenpunkte

Auftraggeber	[Betreiber, Ort]
Projekt	Umspannwerke, 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 Schutz- und Automatisierungskonzept
6 Stationsautomatisierung
7 Datenpunkte zur Netzleitstelle
8 Schnittstellen nach außen

1 Architektur

Die Netzleitstelle führt beide Umspannwerke, acht fernwirktechnisch angebundene Ortsnetzstationen und den PV-Park. Jedes Umspannwerk hat eine eigene Stationsleittechnik mit redundanten SICAM-A8000-Stationsrechnern, Station-HMI für die Ortsbedienung und SIPROTEC-5-Schutz am PRP-Stationsbus. Im UW Süd liefern Merging Units die Messwerte über den Prozessbus nach IEC 61850-9-2; die Zeit kommt per PTP vom Grandmaster.

- **Fernwirk-WAN:** eigenes LWL-Netz mit RUGGEDCOM RX1500 und MPLS, getrennte VRF für Fernwirk, Sicherheitstechnik und Management.
- **Ortsnetzstationen:** 450-MHz-Funk mit privatem APN und IPsec zur Kopfstelle in der Netzleitstelle.
- **Schutz:** arbeitet in den Schutzgeräten eigenständig, auch ohne Stationsrechner und Netzleitstelle; Buchholzschutz und Druckentlastung der Trafos wirken mechanisch bzw. hart.
- **Unbesetzte Stationen:** Zutritt, Einbruchmeldung und Video melden über das WAN an die Netzleitstelle.

2 Zonen und Segmente

Zone	Bezeichnung	SL-T	Segmente (Stufe 2)
Z01	IT Stadtwerke	-	ein Segment
Z02	Internet, Lieferanten	-	ein Segment
Z03	DMZ	3	Jump-Host; Historian; Redispatch-Gateway; Dienste
Z04	Netzleitsystem	3	Leitsystem-Server; Front-End; Arbeitsplätze
Z05	Engineering	3	Engineering Leitsystem; Engineering Schutz
Z06	OT-Management	3	ein Segment
Z07	Fernwirk-WAN	3	ein Segment
Z08	Kopplung Übertragungsnetzbetreiber	3	ein Segment
Z09	UW Nord Station	3	Stationsrechner Nord; Schutz 110 kV Nord; Schutz 20 kV Nord; Regler Nord; Zeit Nord
Z10	UW Süd Station	3	Stationsrechner Süd; Schutz 110 kV Süd; Schutz 20 kV Süd; Regler Süd
Z11	UW Süd Prozessbus	3	Merging Units; Zeit Süd
Z12	Ortsnetzstationen	2	Fernwirkstationen; Funkrouter
Z13	PV-Park	2	Parkregler; Übergabeschutz
Z14	Hilfsenergie	2	ein Segment
Z15	Gebäudeleittechnik	2	Vision Center; Automationsstationen
Z16	Schutzfunktionen hart	hart verdrahtet	ein Segment

Zone	Bezeichnung	SL-T	Segmente (Stufe 2)
Z17	Gebäudesicherheit	2	ein Segment
Z18	Temporär verbundene Geräte	2	ein Segment

Stufe 1 trennt Zonen, das Fernwirk-WAN führt nur die freigegebenen Dienste. Stufe 2 trennt innerhalb der Stationen: Netzleitstelle nur zu den Fernwirkgateways, Merging Units nur zum 110-kV-Schutz, Engineering nur über die Engineering-Station.

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	Z04	Z09, Z10	IEC104 (TCP 2404)	Netzleitstelle zu den Stationsrechnern (über Fernwirk-WAN)	Z
R02	Front-End-Server A (IEC 104), Front-End-Server B (IEC 104)	SICAM A8000 Stationsrechner B, Fernwirkgateway UW Nord, SICAM A800 …	IEC104 (TCP 2404)	nur Front-End zu den Fernwirkgateways	M
R03	Z04	Z12	IEC104 (TCP 2404)	Netzleitstelle zu Ortsnetzstationen (450 MHz)	Z
R04	Front-End-Server A (IEC 104), Front-End-Server B (IEC 104)	Fernwirkstation Ortsnetzstation 1 (Netz Nord), Fernwirkstation Ort …	IEC104 (TCP 2404)	nur Front-End zu den Fernwirkstationen	M
R05	Z04	Z13	IEC104 (TCP 2404)	Sollwerte und Messwerte PV-Park	Z
R06	Front-End-Server A (IEC 104), Front-End-Server B (IEC 104)	Parkregler PV-Park	IEC104 (TCP 2404)	nur Front-End zum Parkregler	M
R07	SICAM A8000 Stationsrechner A UW Nord, SICAM A8000 Stationsrechner …	SIPROTEC 7SA86 Distanz Freileitung ÜNB UW Nord, SIPROTEC 7SL86 Kab …	MMS (TCP 3782)	Stationsrechner und Station-HMI zu Schutz und Reglern Nord	M
R08	SICAM A8000 Stationsrechner A UW Süd, SICAM A8000 Stationsrechner …	SIPROTEC 7SA86 Distanz Leitung ÜNB UW Süd, SIPROTEC 7SL86 Kabel zu …	MMS (TCP 3782)	Stationsrechner und Station-HMI zu Schutz und Reglern Süd	M
R09	SIPROTEC 7SA86 Distanz Freileitung ÜNB UW Nord, SIPROTEC 7SL86 Kab …	SIPROTEC 7SA86 Distanz Freileitung ÜNB UW Nord, SIPROTEC 7SL86 Kab …	GOOSE (ETH 0x88b8)	Verriegelungen und Schutzsignale Nord	M
R10	SIPROTEC 7SA86 Distanz Leitung ÜNB UW Süd, SIPROTEC 7SL86 Kabel zu …	SIPROTEC 7SA86 Distanz Leitung ÜNB UW Süd, SIPROTEC 7SL86 Kabel zu …	GOOSE (ETH 0x88b8)	Verriegelungen und Schutzsignale Süd	M

Regel	Quelle	Ziel	Dienst	Zweck	Stufe
R11	Z11	Z10	SV (ETH 0x88ba)	Abtastwerte der Merging Units an den Schutz	Z
R12	Merging Unit 6MU85 Q01 UW Süd, Merging Unit 6MU85 Q02 UW Süd, Merg …	SIPROTEC 7SA86 Distanz Leitung ÜNB UW Süd, SIPROTEC 7SL86 Kabel zu …	SV (ETH 0x88ba)	Abtastwerte nur an den 110-kV-Schutz	M
R13	Zeitserver PTP UW Nord, Zeitserver PTP-Grandmaster UW Süd	alle	PTP (ETH 0x88f7)	Zeit für Schutz und Merging Units	Z, M
R14	SICAM A8000 Stationsrechner A UW Nord, SICAM A8000 Stationsrechner …	Gleichrichter und Batterie UW Nord, Gleichrichter und Batterie UW Süd	MODBUS (TCP 502)	Stationsrechner liest Gleichrichter	Z, M
R15	Engineering-Station DIGSI 5, SICAM Device Manager	Z09, Z10, Z11	MMS (TCP 3782)	DIGSI 5 und Device Manager zu den Stationen	Z
R16	Engineering-Station DIGSI 5, SICAM Device Manager	SICAM A8000 Stationsrechner A UW Nord, SICAM A8000 Stationsrechner …	MMS (TCP 3782)	Engineering Schutz und Stationsrechner	M
R17	Engineering-Station Leitsystem	Spectrum Power 7 Server A, Spectrum Power 7 Server B, Front-End-Se …	SSH (TCP 22)	Engineering Leitsystem	Z, M
R18	Jump-Host	Engineering-Station Leitsystem, Engineering-Station DIGSI 5, SICAM …	RDP (TCP 3389)	Administration über den Jump-Host	Z, M
R19	Jump-Host	Spectrum Power 7 Server A, Spectrum Power 7 Server B	SSH (TCP 22)	Administration Leitsystem	Z, M
R20	Fernwartung Hersteller Leitsystem	Jump-Host	HTTPS (TCP 443)	Fernwartung Hersteller nur zum Jump-Host	Z, M
R21	Z04	Historian	OPCUA (TCP 4840)	Archivdaten	Z
R22	Spectrum Power 7 Server A, Spectrum Power 7 Server B	Historian	OPCUA (TCP 4840)	Archivdaten	M
R23	Historian	ERP und Marktkommunikation (IT)	HTTPS (TCP 443)	Berichte zur IT	Z, M

Regel	Quelle	Ziel	Dienst	Zweck	Stufe
R24	Redispatch-Gateway	Plattform Redispatch 2.0 (extern)	HTTPS (TCP 443)	Redispatch 2.0: Datenaustausch mit der Plattform	Z, M
R25	Redispatch-Gateway	Spectrum Power 7 Server A, Spectrum Power 7 Server B	OPCUA (TCP 4840)	Redispatch-Abrufe als Sollwerte an das Leitsystem	Z, M
R26	Spectrum Power 7 Server A, Spectrum Power 7 Server B	ICCP-Gateway zum Übertragungsnetzbetreiber	ICCP (TCP 102)	Leitsystem zum ICCP-Gateway	Z, M
R27	ICCP-Gateway zum Übertragungsnetzbetreiber	Leitstelle des Übertragungsnetzbetreibers	ICCP (TCP 102)	Kopplung zur Leitstelle des ÜNB	Z, M
R28	450-MHz-Router Ortsnetzstation 1, 450-MHz-Router Ortsnetzstation 2 …	Kopfstelle 450-MHz-Funknetz	IPSEC (UDP 4500)	Tunnel der Funkrouter zur Kopfstelle	Z, M
R29	Sauter modulo 6 UW Nord, Sauter modulo 6 UW Süd, Sauter modulo 6 N …	Sauter Vision Center	BACNET (UDP 47808)	Automationsstationen zum Vision Center	Z, M
R30	Service-Laptop Schutztechnik (temporär)	Z09, Z10	MMS (TCP 3782)	Service-Laptop der Schutztechnik vor Ort	Z
R31	Service-Laptop Schutztechnik (temporär)	SIPROTEC 7SA86 Distanz Freileitung ÜNB UW Nord, SIPROTEC 7SL86 Kab …	MMS (TCP 3782)	Service-Laptop nur zu Schutz und Reglern	M
R32	OT-Monitoring, Zeitserver Netzleitstelle, Firewall-Cluster Netzlei …	alle	MGMT (UDP 161)	Zeit, Überwachung, Verwaltung	Z, M

4 Protokolle und ihre Absicherung

Protokoll	Einsatz	Absicherung
IEC 60870-5-104	Netzleitstelle zu Stationen, Ortsnetzstationen, PV-Park	MPLS-VRF bzw. IPsec; IEC 62351-3 (TLS) mit Herstellern prüfen; Befehlsprüfung im Stationsrechner
IEC 61850 MMS	Stationsrechner, Station-HMI und Engineering zu Schutz und Reglern	TLS nach IEC 62351-4 (Port 3782), Rollen nach IEC 62351-8
IEC 61850 GOOSE	Verriegelungen, Schutzsignale	nur im Stationsbus; Authentisierung nach IEC 62351-6 prüfen
IEC 61850-9-2 Sampled Values	Merging Units zum Schutz UW Süd	nur im Prozessbus, feste Teilnehmer, Plausibilitätsprüfung im Schutz
PTP (IEC 61850-9-3)	Zeit für Schutz und Merging Units	GNSS mit Überwachung, Holdover, Alarm bei Sprung
TASE.2 (ICCP)	Kopplung zum Übertragungsnetzbetreiber	eigenes Netz, Secure ICCP mit Zertifikaten
OPC UA	Historian, Redispatch-Abrufe	SignAndEncrypt, nur aus der DMZ
Modbus/TCP	Gleichrichter	nur lesend
BACnet/IP	Gebäudeleittechnik Sauter	eigene Zone, BACnet Secure Connect prüfen
RDP, SSH, HTTPS	Administration, Fernwartung	nur über Jump-Host, MFA, Freigabe je Sitzung
IPsec	Funkrouter der Ortsnetzstationen	Zertifikate je Router, privates APN

5 Schutz- und Automatisierungskonzept

Die folgenden Funktionen schützen Netz, Anlage und Menschen. Sie bleiben wirksam, wenn Netzleitstelle, WAN oder Stationsrechner gestört oder manipuliert sind.

Funktion	Auslöser	Wirkung	Ausführung
Distanz- und Leitungsdifferenzialschutz	Fehler auf 110-kV-Leitung oder Kabel	Leistungsschalter aus, Wiedereinschaltung bei Freileitung	SIPROTEC 5, eigenständig
Sammelschienenschutz	Fehler auf der 110-kV-Sammelschiene	alle Felder der betroffenen Schiene aus	SIPROTEC 7SS85
Trafodifferenzialschutz, Buchholz	Fehler im Trafo, Gas oder Ölstrom	Trafo beidseitig aus	SIPROTEC 7UT85; Buchholz mechanisch und hart
Abgangsschutz 20 kV	Kurzschluss, Überlast	Abgang aus	SIPROTEC 7SJ82/85
Erdschlusskompensation	Erdschluss im 20-kV-Netz	Lichtbogen erlischt, Meldung und Ortung	Petersen-Spule, REG-DPA, wattmetrische Erfassung
Feldverriegelung	Schaltbefehl	Schaltfehler verhindert	SIPROTEC CFC und Stationsrechner
Befehlsprüfung Fernwirk	Befehl aus der Netzleitstelle	nur vereinbarte Befehle, Select-before-Operate, Ratenbegrenzung	SICAM A8000
Spannungsband	Sollwert aus der Netzleitstelle	Sollwert auf 20,0 bis 21,5 kV begrenzt	SICAM A8000, REG-DA
Leistungsvorgabe PV-Park	Redispatch, Netzengpass	Sollwert mit Grenzen und Gradient	SICAM A8000, Parkregler

6 Stationsautomatisierung

Baustein	Funktion
FB_Stationsverriegelung	Schaltfehlerschutz für Leistungs-, Trenn- und Erdungsschalter, Sammelschienenwechsel
FB_Befehlspruefung	Befehlsliste, Ortsteuerung, Select-before-Operate, höchstens 6 Befehle je Minute
FB_PV_Sollwert	Wirkleistungsvorgabe 0 bis 100 %, Gradient rund 10 % je Minute, letzter gültiger Wert bei Verbindungsverlust
FB_Spannung_Ueberwachung	Sollspannung begrenzt, Alarm Spannungsband und Stufenschaltungen je Stunde
FB_Erdschluss	Verlagerungsspannung, Abgangsauswahl, Alarm nach 2 h

Die Bausteine liegen als Umspannwerke_Stationsautomatisierung.st (Strukturierter Text nach IEC 61131-3) bei.

7 Datenpunkte zur Netzleitstelle

Gemeinsame Adresse UW Nord 101, UW Süd 102, Ortsnetzstationen 201 bis 208, PV-Park 301. Auszug der Adressbereiche je Station.

IOA	Typ	Inhalt	Richtung
1001 bis 1099	M_ME_TF_1	Messwerte: Spannung, Strom, Wirk- und Blindleistung je Feld	Station an Leitstelle
1101 bis 1110	M_ME_TF_1	Verlagerungsspannung, Spulenstrom, Trafo-Öltemperatur	Station an Leitstelle
2001 bis 2099	M_DP_TB_1	Stellungen Leistungs-, Trenn-, Erdungsschalter	Station an Leitstelle
2101 bis 2199	M_SP_TB_1	Schutzanregungen und -auslösungen, Erdschluss, Störungen	Station an Leitstelle
2201 bis 2210	M_ST_TB_1	Stufenstellung der Trafos	Station an Leitstelle
3101 bis 3199	C_DC_NA_1	Befehle Leistungs- und Trennschalter (Select-before-Operate)	Leitstelle an Station
3201 bis 3299	C_RC_NA_1	Stufensteller höher und tiefer	Leitstelle an Station
4001 bis 4010	C_SE_NC_1	Sollspannung 20 kV, Wirkleistungsvorgabe PV-Park	Leitstelle an Station
5001 bis 5010	M_SP_TB_1	Zutritt, Einbruch, Tür Schaltanlage, Batterie, Gleichrichter	Station an Leitstelle

8 Schnittstellen nach außen

- **Übertragungsnetzbetreiber:** TASE.2 (ICCP) über ein eigenes Netz; Austausch von Messwerten, Schaltzuständen und Netzsicherheitsmaßnahmen.
- **Redispatch 2.0:** Abrufe kommen über die Plattform in die DMZ und von dort als Sollwert ins Leitsystem; dort Plausibilisierung gegen Netzzustand und Anlagengrenzen.
- **PV-Park:** Anlage des Kunden hinter einer SC646; nur Sollwerte hin, Mess- und Zustandswerte zurück.
- **Hersteller:** Fernwartung nur über den Jump-Host mit Freigabe je Sitzung.