BERICHT

Kommunikation, Steuerungs- und Schutzkonzept

GuD-Heizkraftwerk: Zonen, Kommunikationsmatrix, Protokolle, Schutzfunktionen, SPS-Programme

Auftraggeber	[Betreiber, Ort]
Projekt	GuD-Heizkraftwerk, OT-Konzept
Version	0.1 Entwurf
Datum	04.11.2026
Autor	Maximilian Gilg, OT-Cyber.de
Klassifizierung	TLP:AMBER – Weitergabe nur an den Verteiler

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 Steuerungs- und Schutzkonzept

6 SPS-Programme

7 Netzbetreiber und Behörde

1 Architektur

Die Leittechnik ist in drei Ebenen aufgebaut: Bedienebene mit Kraftwerksleitsystem (DCS) Application-Servern und Thin Clients in der Leitwarte, Automatisierungsebene mit den redundanten DCS-Automatisierungssystemen für Gasturbine, Abhitzedampferzeuger, Dampfturbine und Nebenanlagen sowie Zellen mit eigenen SIMATIC-S7-1500-Steuerungen für Gas, Fernwärme und Wasser. Die elektrische Anlage hat eine eigene Stationsleittechnik mit SICAM A8000 und SIPROTEC 5 nach IEC 61850.

- **Übergänge:** IT der Stadtwerke, Lieferanten und Behörde nur über die DMZ; Netzbetreiber über ein eigenes Fernwirk-WAN mit IEC 60870-5-104.
- **Zellen:** Gas, Fernwärme, Wasser, Emission und Gebäudeleittechnik jeweils hinter einer SCALANCE SC646-2C.
- **Schutz:** Turbinen-, Kessel-, Gas- und Netzschutz wirken hart verdrahtet, mechanisch oder im F-Teil, unabhängig von Bedienebene und Netzwerk.
- **Zeit:** GNSS-Zeitserver mit NTP für die IT-nahen Systeme und PTP nach IEC 61850-9-3 für Stationsbus und Schutz.

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; Emissionsdaten; Dienste
Z04	Leitsystem Bedienebene	3	DCS-Server; Bedienplätze
Z05	Engineering	3	Engineering DCS; Engineering TIA, DIGSI
Z06	OT-Management	3	ein Segment
Z07	Kraftwerksleittechnik Automatisierung	3	Gasturbine; Kessel; Dampfturbine; Nebenanlagen
Z09	Zelle Gas	3	Gas-Steuerung; Verdichter V-120; Verdichter V-121
Z10	Zelle Fernwärme	2	FW-Steuerung; Spitzenkessel SK-1; Spitzenkessel SK-2
Z11	Zelle Hilfssysteme	2	Wasser-Steuerung; Vollentsalzung
Z12	Elektrische Anlagen, Umspannwerk	3	Stationsleittechnik; Schutz 110 kV; Schutz 10 kV; Notstrom
Z13	Fernwirk Netzbetreiber	3	Fernwirkrouter; Netzleitstelle
Z14	Emissionsüberwachung	2	ein Segment
Z15	Gebäudeleittechnik	2	Vision Center; Automationsstationen
Z16	Sicherheitsfunktionen	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 mit Firewall und Zellenfirewalls. Stufe 2 trennt zusätzlich innerhalb der Zonen: Bedienplätze sprechen nur mit den Servern, nur die Server mit den Automatisierungssystemen, das Leitsystem nur mit den Stationsrechnern und nicht direkt mit den Schutzgeräten.

3 Kommunikationsmatrix

Erlaubt ist nur, was eine Regel ausdrücklich zulässt. Spalte Stufe: Z gilt in der Zonenstufe, M in der Mikrosegmentierung.

Regel	Quelle	Ziel	Dienst	Zweck	Stufe
R01	Z04	Z07	T3K (TCP 443)	Leitsystem zu den Automatisierungssystemen	Z
R02	Kraftwerksleitsystem (DCS) Application-Server A, Kraftwerksleitsystem	DCS AS Gasturbine mit F-Teil, DCS AS Abhitzedampferzeuger, DCS AS Damp	T3K (TCP 443)	nur die Server zu den AS	M
R03	Z04	Z09, Z10, Z11, Z14	OPCUA (TCP 4840)	Leitsystem liest Gas, Fernwärme, Wasser, Emission	Z
R04	Kraftwerksleitsystem (DCS) Application-Server A, Kraftwerksleitsystem	AS-GAS Gas, GDRM, Speicher, AS-FW Fernwärme, AS-WA Wasser, Dosierung,	OPCUA (TCP 4840)	nur die Server zu den Zellen-SPS	M
R05	Z04	Z12	MMS (TCP 3782)	Leitsystem zur Stationsleittechnik	Z
R06	Kraftwerksleitsystem (DCS) Application-Server A, Kraftwerksleitsystem	SICAM A8000 Stationsrechner A, SICAM A8000 Stationsrechner B, Fernwirk	MMS (TCP 3782)	nur über die Stationsrechner, nicht zu den Schutzgeräten	M
R07	SICAM A8000 Stationsrechner A, SICAM A8000 Stationsrechner B, Fernwirk	SIPROTEC 7SL86 Leitung Nord, SIPROTEC 7SL86 Leitung Süd, SIPROTEC 7UT8	MMS (TCP 3782)	Stationsrechner zu den Schutzgeräten	M
R08	SIPROTEC 7SL86 Leitung Nord, SIPROTEC 7SL86 Leitung Süd, SIPROTEC 7UT8	SIPROTEC 7SL86 Leitung Nord, SIPROTEC 7SL86 Leitung Süd, SIPROTEC 7UT8	GOOSE (ETH 0x88b8)	Verriegelungen und Schutzsignale (GOOSE)	M
R09	SICAM A8000 Stationsrechner A, SICAM A8000 Stationsrechner B, Fernwirk	Notstromdiesel Steuerung	MODBUS (TCP 502)	Stationsrechner liest Notstromdiesel	M

Regel	Quelle	Ziel	Dienst	Zweck	Stufe
R10	SICAM A8000 Stationsrechner B, Fernwirkgateway	Fernwirkrouter zum Netzbetreiber	IEC104 (TCP 2404)	Fernwirkgateway zum Router	Z, M
R11	Netzleitstelle des Netzbetreibers	SICAM A8000 Stationsrechner B, Fernwirkgateway	IEC104 (TCP 2404)	Netzleitstelle: Messwerte, Sollwerte, Schaltbefehle	Z, M
R12	Bedienplatz Leitwarte 1 (Thin Client), Bedienplatz Leitwarte 2 (Thin C	Kraftwerksleitsystem (DCS) Application-Server A, Kraftwerksleitsystem	HTTPS (TCP 443)	Bedienplätze zu den Servern	M
R13	Engineering-Station DCS	Z04, Z07	T3K (TCP 443)	Engineering DCS	Z
R14	Engineering-Station DCS	Kraftwerksleitsystem (DCS) Application-Server A, Kraftwerksleitsystem	T3K (TCP 443)	Engineering DCS	M
R15	Engineering-Station TIA Portal, DIGSI 5	Z09, Z10, Z11	S7 (TCP 102)	Engineering TIA Portal	Z
R16	Engineering-Station TIA Portal, DIGSI 5	AS-GAS Gas, GDRM, Speicher, AS-FW Fernwärme, AS-WA Wasser, Dosierung	S7 (TCP 102)	Engineering TIA Portal, eigene SPS	M
R17	Engineering-Station TIA Portal, DIGSI 5	Z12	MMS (TCP 3782)	Parametrierung Schutz mit DIGSI 5	Z
R18	Engineering-Station TIA Portal, DIGSI 5	SICAM A8000 Stationsrechner A, SICAM A8000 Stationsrechner B, Fernwirk	MMS (TCP 3782)	Parametrierung Schutz mit DIGSI 5	M
R19	Jump-Host	Z04, Z05	RDP (TCP 3389)	Administration über den Jump-Host	Z, M
R20	Ferndiagnose Turbinenhersteller, Fernwartung Wasseraufbereiter	Jump-Host	HTTPS (TCP 443)	Fernwartung nur zum Jump-Host	Z, M
R21	Jump-Host	Vollentsalzung Steuerung (OEM)	HTTPS (TCP 443)	Wartung Vollentsalzung nach Freigabe	Z, M
R22	Historian	Ferndiagnose Turbinenhersteller	HTTPS (TCP 443)	Ferndiagnose Turbine: nur Datenexport aus dem Historian	Z, M
R23	Z04	Historian	OPCUA (TCP 4840)	Archivdaten	Z

Regel	Quelle	Ziel	Dienst	Zweck	Stufe
R24	Kraftwerksleitsystem (DCS) Application-Server A, Kraftwerksleitsystem	Historian	OPCUA (TCP 4840)	Archivdaten	M
R25	Historian	ERP-Server (IT)	HTTPS (TCP 443)	Berichte zur IT	Z, M
R26	Einsatzplanung, Fahrplanserver (IT)	Historian	HTTPS (TCP 443)	Fahrpläne der Einsatzplanung in die DMZ	Z, M
R27	Historian	Kraftwerksleitsystem (DCS) Application-Server A, Kraftwerksleitsystem	OPCUA (TCP 4840)	Fahrplan als Sollwertvorgabe ans Leitsystem	Z, M
R28	Emissionsrechner	Emissionsdatenrechner, Übertragung zur Behörde	OPCUA (TCP 4840)	Emissionsdaten in die DMZ	Z, M
R29	Emissionsdatenrechner, Übertragung zur Behörde	Emissionsfernüberwachung der Behörde	HTTPS (TCP 443)	Emissionsfernüberwachung	Z, M
R30	Sauter modulo 6 AS Schaltanlagengebäude, Sauter modulo 6 AS Maschinenh	Sauter Vision Center	BACNET (UDP 47808)	Automationsstationen zum Vision Center	M
R31	Bedienplatz Leitwarte 1 (Thin Client), Bedienplatz Leitwarte 2 (Thin C	Sauter Vision Center	HTTPS (TCP 443)	GLT-Bedienung in der Leitwarte	Z, M
R32	AS-GAS Gas, GDRM, Speicher	Verdichter V-120 Steuerung (OEM), Verdichter V-121 Steuerung (OEM)	S7 (TCP 102)	Freigaben an die Verdichter	M
R33	AS-FW Fernwärme	Brennersteuerung SK-1 (OEM), Brennersteuerung SK-2 (OEM)	S7 (TCP 102)	Sollwerte an die Spitzenkessel	M
R34	AS-WA Wasser, Dosierung	Vollentsalzung Steuerung (OEM)	S7 (TCP 102)	Anforderung Vollentsalzung	M
R35	OT-Monitoring, Zeitserver GNSS NTP/PTP, Firewall OT	alle	MGMT (UDP 161)	Zeit, Überwachung, Verwaltung	Z, M

4 Protokolle und ihre Absicherung

Protokoll	Einsatz	Absicherung
Kraftwerksleitsystem (DCS) Systembus	Server zu Automatisierungssystemen	herstellerseitig verschlüsselt und authentisiert; Zugriff nur aus Z04 und Z05
S7 mit TLS (S7comm-plus)	Engineering der S7-1500, Zellen	TLS ab Firmware V3.1, Zugriffsschutz, PUT/GET aus
OPC UA	Leitsystem zu Zellen, Historian, Emission, Fahrplan	SignAndEncrypt, Zertifikate je Gerät, Benutzer
IEC 61850 MMS	Leitsystem und Engineering zur Station	IEC 62351-4 und Rollen nach IEC 62351-8 beim Hersteller prüfen
IEC 61850 GOOSE	Verriegelungen und Schutzsignale	nur im Stationsbus, VLAN, Authentisierung nach IEC 62351-6 prüfen
IEC 60870-5-104	Netzleitstelle des Netzbetreibers	eigenes Fernwirk-WAN, IPsec bzw. IEC 62351-3 mit dem Netzbetreiber abstimmen
Modbus/TCP	Notstrom, Druckluft, Gaszähler	nur lesend, Mikrosegment
BACnet/IP	Gebäudeleittechnik Sauter	eigene Zone; BACnet Secure Connect prüfen
PROFINET, PROFIsafe	E/A und Umrichter	nur innerhalb der Zelle, Port Security
RDP, HTTPS	Administration, Bedienung, Fernwartung	nur über Jump-Host, MFA, Freigabe je Sitzung
NTP, PTP	Zeitsynchronisation	GNSS mit Überwachung; Zeitfehler beeinflussen Schutz und Archiv

5 Steuerungs- und Schutzkonzept

Die folgenden Funktionen schützen Menschen und Anlage. Sie bleiben wirksam, wenn Bedienebene, Netzwerk oder eine Steuerung manipuliert sind.

Funktion	Auslöser	Wirkung	Ausführung
Schnellschluss Gasturbine	Überdrehzahl 2oo3, Flammenausfall, Abgastemperatur, Schwingung	ESV 201 und 202 zu, Entlüftung auf	F-Teil DCS und hart
Dichtheitskontrolle Brennstoff	vor jedem Start	Start nur bei dichten Ventilen	F-Teil DCS
Kesselschutz	Wassermangel HD- und ND-Trommel 2oo3, Drucküberschreitung	Zusatzfeuerung aus, GT auf Bypass bzw. Schnellschluss	hart, Sicherheitsventile mechanisch
Schnellschluss Dampfturbine	Überdrehzahl 2oo3, Vakuumverlust, Schmieröldruck	ESV 501 zu, Umleitstation öffnet	F-Teil DCS und hart
Gasschutz GDRM	Überdruck nach Regler, Gaswarnung	SAV schließt, SBV bläst ab, XV 101 zu	mechanisch und hart
Speicherschutz	Druck über 70 bar	PSV 133 bläst ab	mechanisch
Netzschutz	Fehler auf Leitungen, Trafos, Generatoren	Leistungsschalter aus, Generator vom Netz	SIPROTEC 5, eigenständig
Spitzenkessel	Flammenausfall, Wassermangel, Überdruck	Brenner aus	Sicherheitskette der Brennersteuerung
Brandschutz GT-Einhausung	Brandmelder, Gaswarnung	CO2-Löschung, Lüftung, Schnellschluss	autark

6 SPS-Programme

Baustein	Steuerung	Funktion
FB_GDRM_Strecke	AS-GAS	Druckregelung je Strecke, Vorwärmer, feste Grenzen 28 bis 32 bar
FB_Roehrenspeicher	AS-GAS	Ein- und Ausspeisen, 32 bis 70 bar, Meldung Speicher leer
FB_Verdichterfreigabe	AS-GAS	Führung nach Betriebsstunden, Sperre bei Gasalarm
FB_FW_Vorlauf	AS-FW	Gleitende Vorlauftemperatur 90 bis 130 °C, Netzpumpen nach Schlechtpunkt
FB_Waermespeicher	AS-FW	Laden und Entladen, Anforderung Spitzenkessel
FB_Spitzenkessel	AS-FW	Lastsollwerte an die OEM-Brennersteuerungen
FB_VE_Ueberwachung	AS-WA	Leitfähigkeit und Silikat, Sperre VE-Wasser
FB_Dosierung	AS-WA	Alkalisierung mit pH-Grenzen 9,2 bis 9,8

Die Programme liegen als Kraftwerk_SPS_Programme.scl bei. Gasturbine, Kessel und Dampfturbine sind in Kraftwerksleitsystem (DCS) projektiert und nicht Teil dieser Datei.

7 Netzbetreiber und Behörde

- **Netzbetreiber:** Messwerte, Schaltzustände und Sollwerte (Wirkleistung, Blindleistung) über IEC 60870-5-104 aus der Netzleitstelle; Netzanschluss nach VDE-AR-N 4120. Sollwerte prüft das Leitsystem gegen Betriebsgrenzen.
- **Einsatzplanung:** Fahrpläne aus der IT kommen nur über die DMZ (Historian) ins Leitsystem; die Plausibilisierung im Leitsystem ist Pflicht.
- **Behörde:** Emissionsdaten gehen aus dem Emissionsrechner über die DMZ an die Emissionsfernüberwachung; kein Weg von außen zurück.