BERICHT

# Risikobewertung nach IEC 62443-3-2

Kläranlage 110.000 EW mit Kanalnetz: Zonen, Conduits und Ziel-Security-Level

| | |
|---|---|
| **Auftraggeber** | [Betreiber, Ort] |
| **Projekt** | Kläranlage, 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 und Conduits (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

Die Kläranlage mit Kanalnetz ist in 15 Zonen und 13 Conduits gegliedert. 8 Zonen erhalten SL-T 3: DMZ, Leitsystem, Engineering, OT-Management, Fernwirkzentrale, die Außenstationen im Kanalnetz, Gas und Energie sowie die BHKW. Die übrigen Prozesszellen erhalten SL-T 2, die Sicherheitsfunktionen sind hart verdrahtet und ohne Netzanbindung.

Von 18 bewerteten Bedrohungen sind ohne Maßnahmen 8 kritisch und 3 hoch. Mit den Maßnahmen liegt keine über MITTEL. Die größte Lücke zwischen Ziel und Fähigkeit liegt in der Fernwirktechnik: IEC 60870-5-104 hat ohne Zusatzmaßnahmen keine Authentisierung, die Außenstationen sind öffentlich zugänglich und unbemannt.

**GESAMTBEWERTUNG**

**Das Leitsystem erhält hier SL-T 3, anders als bei vielen Produktionsanlagen: Über den regulären Bedienweg lassen sich Pumpwerke und Gasanlage schalten. Schutz muss deshalb auch in den Unterstationen und Steuerungen selbst sitzen.**

| Klasse | Ohne Maßnahmen | Mit Maßnahmen |
|---|---|---|
| KRITISCH | 8 | 0 |
| HOCH | 3 | 0 |
| MITTEL | 7 | 9 |
| NIEDRIG | 0 | 9 |

# 2 System under Consideration (ZCR 1)

Betrachtet wird die gesamte Automatisierung der Kläranlage einschließlich Kanalnetz mit vier Pumpwerken und zwei Regenüberlaufbecken, Fernwirktechnik, Gas- und Energieanlage sowie aller Fernzugänge. Grenzen sind die Übergänge zur IT der Stadtwerke (K01) und zum Internet (K02).

- **Nicht betrachtet:** physische Sicherheit des Geländes, Prozesse des Betreibers (gehören in ein Managementsystem nach IEC 62443-2-1 bzw. DWA-M 1060).
- **Bewertungsgrundlage:** IEC 62443-3-2:2020 (ZCR 1 bis 7), Anforderungen nach IEC 62443-3-3:2013, Angriffstechniken nach MITRE ATT&CK for ICS v20.
- **Annahmen:** Fernwirk über Mobilfunk mit IPsec bis zum Router; Sicherheitsfunktionen der Gasanlage hart verdrahtet bzw. mechanisch; BHKW mit Herstellerzugang.

# 3 Risikokriterien

| Stufe | Mensch | Gewässer, Umwelt | Betrieb, Finanzen |
|---|---|---|---|
| 1 | keine Gefährdung | keine | unter 10.000 € |
| 2 | Erste Hilfe | kurzzeitig, ohne Folgen | unter 100.000 € |
| 3 | leichte Verletzung | Überschreitung eines Überwachungswerts | unter 1 Mio. € |
| 4 | schwere Verletzung | Gewässerschaden, Fischsterben | über 1 Mio. € |
| 5 | Lebensgefahr, Explosion, Rückstau in Wohngebiete | großflächig, Badegewässer | Entsorgungssicherheit 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 | Mensch, Gewässer (als Sprungbrett) | 5 | KRITISCH |
| Z04 | Leitsystem | Mensch, Gewässer über Bedienung | 5 | KRITISCH |
| Z05 | Engineering | alle Prozesse | 5 | KRITISCH |

| Zone | Bezeichnung | Schlimmster Fall | A | Risiko |
|---|---|---|---|---|
| Z06 | OT-Management | Trennung aller Zonen | 4 | KRITISCH |
| Z07 | Fernwirkzentrale | Kanalnetz | 5 | KRITISCH |
| Z08 | Außenstationen Kanalnetz | Rückstau, Gewässer | 5 | KRITISCH |
| Z09 | Zelle Zulauf, Mechanik | Betrieb | 3 | HOCH |
| Z10 | Zelle Biologie | Gewässer | 4 | KRITISCH |
| Z11 | Zelle Schlamm, Faulung | Betrieb | 3 | HOCH |
| Z12 | Zelle Gas, Energie | Mensch (Explosion), Umwelt | 5 | KRITISCH |
| Z13 | OEM BHKW | Mensch, Umwelt über Gas | 5 | KRITISCH |
| Z14 | Ablaufmessstation | Nachweis Überwachungswerte | 3 | HOCH |
| Z15 | Temporär verbundene Geräte | alle Zellen | 4 | KRITISCH |
| Z17 | Gebäudesicherheit | Betrieb, Zutritt | 3 | HOCH |
| Z16 | Sicherheitsfunktionen | Mensch | 5 | KRITISCH |

# 5 Zonen und Conduits (ZCR 3)

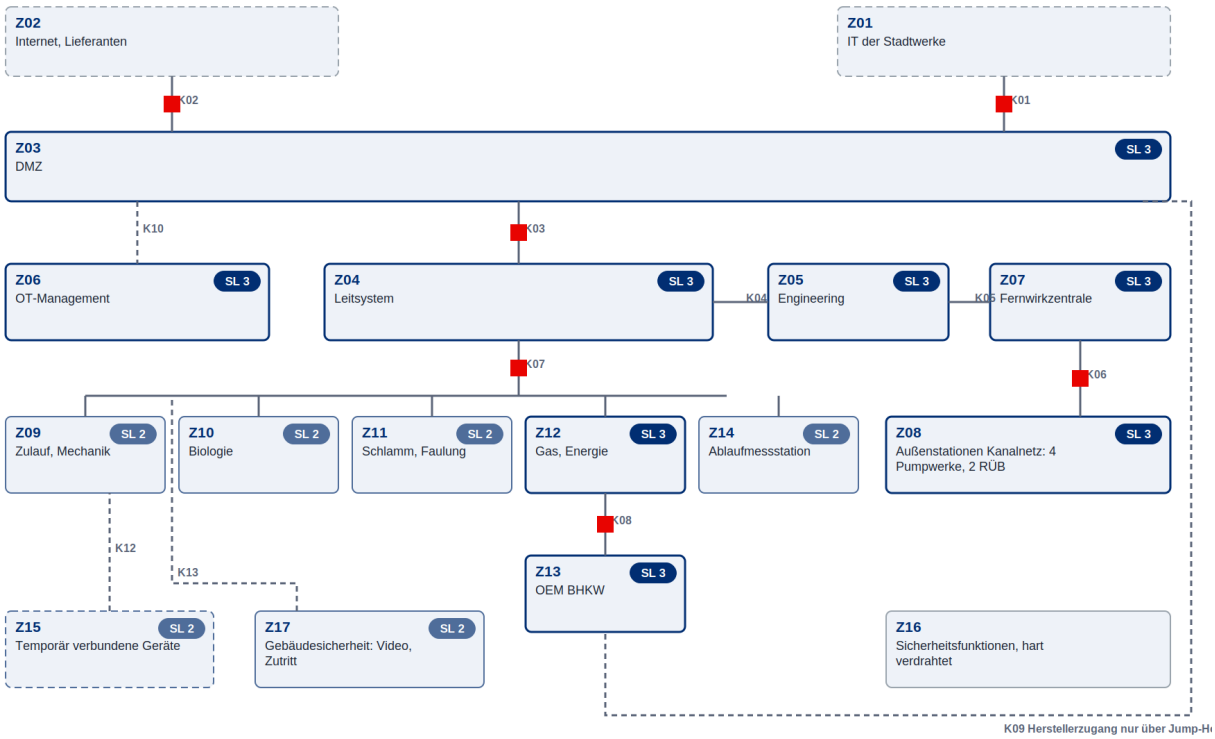



Abbildung: Zonen und Conduits mit SL-T

Getrennt sind Geschäfts- und Steuerungssysteme (ZCR 3.2), Sicherheitsfunktionen (ZCR 3.3, Z16 hart verdrahtet), zeitweise verbundene Geräte (ZCR 3.4) und nicht vertrauenswürdige Netze (ZCR 3.6). Die Außenstationen bilden eine eigene Zone, weil sie öffentlich zugänglich sind und über Mobilfunk angebunden werden.

| Zone | Bezeichnung | Inhalt | SL-T |
|---|---|---|---|
| Z03 | DMZ | Jump-Host, Historian, Log-Sammler, DNS, Patch-Server | 3 |
| Z04 | Leitsystem | Server A/B, Bedienplätze, Webclients Bereitschaft | 3 |
| Z05 | Engineering | Engineering-Station, Fernwirk-Parametrierung, Sicherungen | 3 |
| Z06 | OT-Management | Firewalls, Switches, Zeitserver, Monitoring, USV | 3 |
| Z07 | Fernwirkzentrale | Fernwirk-Frontend, VPN-Konzentrator | 3 |
| Z08 | Außenstationen Kanalnetz | RTU, S7-1200, LTE-Router in 4 Pumpwerken und 2 RÜB | 3 |
| Z09 | Zelle Zulauf, Mechanik | AS-10, Schnecken, Rechen, Sandfang | 2 |
| Z10 | Zelle Biologie | AS-20, Gebläse, Fällung, Nachklärung | 2 |
| Z11 | Zelle Schlamm, Faulung | AS-30, Faulbehälter, Heizung, Entwässerung | 2 |
| Z12 | Zelle Gas, Energie | AS-40, Gasspeicher, Fackel, Gasanalyse, NSHV | 3 |
| Z13 | OEM BHKW | 2 BHKW-Steuerungen, Herstellerzugang | 3 |
| Z14 | Ablaufmessstation | Analysatoren, Probenehmer | 2 |
| Z15 | Temporär verbundene Geräte | Service-Laptops, Programmiergeräte | 2 |
| Z17 | Gebäudesicherheit | Videokameras, Videorekorder, Zutrittskontrolle | 2 |
| Z16 | Sicherheitsfunktionen | Gaswarnanlage, Not-Aus, Störmelder, mechanische Sicherungen | hart verdrahtet |

## CONDUITS

| Conduit | Verbindet | Datenflüsse | Schutz | SL-T |
|---|---|---|---|---|
| K01 | Z01 IT ↔ Z03 DMZ | Berichte HTTPS, Updates über Proxy | Firewall OT | 3 |
| K02 | Z02 Internet ↔ Z03 DMZ | Fernwartung VPN, nur über Jump-Host | Firewall, MFA | 3 |
| K03 | Z03 DMZ ↔ Z04 Leitsystem | Historian OPC UA, WSUS, RDP Jump-Host, Syslog | Firewall OT | 3 |
| K04 | Z04 ↔ Z05 Engineering | S7 mit TLS (Engineering) | Firewall, Wartungsfenster | 3 |
| K05 | Z04 ↔ Z07 Fernwirkzentrale | Kopplung Leitsystem und Frontend | Firewall OT | 3 |
| K06 | Z07 ↔ Z08 Außenstationen | IEC 60870-5-104 in IPsec über Mobilfunk | VPN-Konzentrator, Allowlist (H02) | 3 |
| K07 | Z04 ↔ Z09 bis Z12 | S7 mit TLS (HMI) | Firewall Zellen (H01) | 3 |
| K08 | Z12 ↔ Z13 BHKW | Modbus/TCP lesend | Firewall vor BHKW (H09) | 3 |
| K09 | Z02 ↔ Z13 Herstellerzugang | Fernüberwachung | nur über Jump-Host (H11) | 3 |
| K10 | Z06 ↔ alle | SNMPv3, Syslog, NTP | Management-VLAN | 3 |
| K11 | Spiegelports → Monitoring | Kopie des Verkehrs | unidirektional | 2 |
| K12 | Z15 ↔ Z05, Zellen | Engineering, Diagnose | nur über Engineering-Zugang | 2 |
| K13 | Z17 ↔ Z04 Leitwarte | Videobilder zur Leitwarte, Zutrittsmeldungen | Firewall OT, nur vom Rekorder | 2 |

# 6 Detaillierte Risikobewertung (ZCR 5)

### 6.1.1 Z03 DMZ

| Nr. | Bedrohung | A | Wo | Ohne | Maßnahmen | Wm | Mit |
|---|---|---|---|---|---|---|---|
| T03-1 | Jump-Host mit gestohlenen Admin-Daten übernommen (A5) | 4 | 4 | KRITISCH | MFA, Sitzungsfreigabe und Aufzeichnung (SR 1.1, 1.13, 2.8) | 2 | MITTEL |
| T03-2 | Herstellerzugang missbraucht (A3) | 5 | 3 | KRITISCH | nur über Jump-Host, Freigabe je Sitzung (SR 1.13) | 1 | MITTEL |

### 6.1.2 Z04 Leitsystem

| Nr. | Bedrohung | A | Wo | Ohne | Maßnahmen | Wm | Mit |
|---|---|---|---|---|---|---|---|
| T04-1 | Bedienplatz übernommen, reguläre Befehle an Pumpwerke (A1) | 5 | 4 | KRITISCH | Plausibilisierung in den Unterstationen (SR 3.5), Rechtekonzept (SR 2.1), Monitoring (SR 6.2) | 1 | MITTEL |
| T04-2 | Ransomware auf Leitsystem-Servern (A5) | 4 | 4 | KRITISCH | Whitelisting (SR 3.2), Offline-Sicherung (SR 7.3, 7.4), Störmelder | 2 | MITTEL |

### 6.1.3 Z05 Engineering

| Nr. | Bedrohung | A | Wo | Ohne | Maßnahmen | Wm | Mit |
|---|---|---|---|---|---|---|---|
| T05-1 | Infizierte Engineering-Station lädt Programme | 5 | 3 | KRITISCH | USB-Schleuse (SR 2.3), Vier-Augen und Sollstandvergleich (SR 3.4) | 1 | MITTEL |

### 6.1.4 Z06 OT-Management

| Nr. | Bedrohung | A | Wo | Ohne | Maßnahmen | Wm | Mit |
|---|---|---|---|---|---|---|---|
| T06-1 | Firewall- oder Switch-Konfiguration manipuliert | 4 | 2 | MITTEL | MFA, Konfigurationssicherung (SR 7.6) | 1 | NIEDRIG |

### 6.1.5 Z07 Fernwirkzentrale

| Nr. | Bedrohung | A | Wo | Ohne | Maßnahmen | Wm | Mit |
|---|---|---|---|---|---|---|---|
| T07-1 | Frontend kompromittiert, Befehle an alle Stationen (A1) | 5 | 2 | HOCH | Plausibilisierung in den Stationen (SR 3.5), Härtung (SR 7.7) | 1 | MITTEL |

### 6.1.6 Z08 Außenstationen Kanalnetz

| Nr. | Bedrohung | A | Wo | Ohne | Maßnahmen | Wm | Mit |
|---|---|---|---|---|---|---|---|
| T08-1 | Einbruch, Laptop im Schaltschrank, gefälschte Werte (A2) | 5 | 3 | KRITISCH | Türkontakt, Port Security, IPsec bis RTU (SR 3.1, 7.7) | 1 | MITTEL |
| T08-2 | Router oder SIM entwendet, VPN missbraucht (A2) | 4 | 2 | MITTEL | Zertifikat je Station, Allowlist (SR 1.2, 2.1) | 1 | NIEDRIG |

### 6.1.7 Z09 Zelle Zulauf, Mechanik

| Nr. | Bedrohung | A | Wo | Ohne | Maßnahmen | Wm | Mit |
|---|---|---|---|---|---|---|---|
| T09-1 | Schneckenpumpen abgeschaltet, Rückstau im Zulauf | 3 | 2 | MITTEL | Firewall Zellen (SR 5.2), Zugriffsschutz (SR 2.1) | 1 | NIEDRIG |

### 6.1.8 Z10 Zelle Biologie

| Nr. | Bedrohung | A | Wo | Ohne | Maßnahmen | Wm | Mit |
|---|---|---|---|---|---|---|---|
| T10-1 | Sauerstoff-Sollwert manipuliert (A4) | 4 | 3 | HOCH | PUT/GET aus, Sollwertgrenzen (SR 2.1, 3.5) | 1 | NIEDRIG |
| T10-2 | Fällmittel abgeschaltet (A6) | 3 | 3 | MITTEL | Mindestdosierung (SR 3.5) | 1 | NIEDRIG |

### 6.1.9 Z11 Zelle Schlamm, Faulung

| Nr. | Bedrohung | A | Wo | Ohne | Maßnahmen | Wm | Mit |
|---|---|---|---|---|---|---|---|
| T11-1 | Faulbehälterheizung verstellt | 3 | 2 | MITTEL | Zugriffsschutz (SR 2.1), Grenzwerte (SR 3.5) | 1 | NIEDRIG |

### 6.1.10 Z12 Zelle Gas, Energie

| Nr. | Bedrohung | A | Wo | Ohne | Maßnahmen | Wm | Mit |
|---|---|---|---|---|---|---|---|
| T12-1 | Fackelfreigabe entzogen, Gasspeicher läuft voll (A3) | 5 | 3 | KRITISCH | Druckschalter startet Fackel hart verdrahtet, Rechtekonzept | 1 | MITTEL |

### 6.1.11 Z13 OEM BHKW

| Nr. | Bedrohung | A | Wo | Ohne | Maßnahmen | Wm | Mit |
|---|---|---|---|---|---|---|---|
| T13-1 | BHKW per Modbus gesperrt (A3) | 4 | 3 | HOCH | Firewall nur lesen (SR 5.2), kein Herstellerrouter | 1 | NIEDRIG |

### 6.1.12 Z14 Ablaufmessstation

| Nr. | Bedrohung | A | Wo | Ohne | Maßnahmen | Wm | Mit |
|---|---|---|---|---|---|---|---|
| T14-1 | Messwerte der Ablaufstation verfälscht | 3 | 2 | MITTEL | Plausibilität mit Labor und Probenehmer, Modbus nur lesen (SR 3.1) | 1 | NIEDRIG |

### 6.1.13 Z17 Gebäudesicherheit

| Nr. | Bedrohung | A | Wo | Ohne | Maßnahmen | Wm | Mit |
|---|---|---|---|---|---|---|---|
| T17-1 | Kamera mit veralteter Firmware oder Standardpasswort als Einstieg ins OT-Netz | 3 | 3 | MITTEL | eigenes VLAN, Firewall nur vom Rekorder (SR 5.1, 5.2), Firmware nach Sollstand (SR 7.6) | 1 | NIEDRIG |

### 6.1.14 Z15 Temporär verbundene Geräte

| Nr. | Bedrohung | A | Wo | Ohne | Maßnahmen | Wm | Mit |
|---|---|---|---|---|---|---|---|
| T15-1 | Infizierter Service-Laptop in einer Zelle (A4) | 4 | 4 | KRITISCH | Prüfung vor Anschluss (SR 2.3, 3.2), Port Security (SR 7.7) | 2 | MITTEL |

# 7 Ziel-Security-Level

SL-T je Grundanforderung FR1 bis FR7 (Spalten 1 bis 7). FR4 Vertraulichkeit liegt in den Prozesszellen niedrig, in DMZ und Engineering hoch. FR3 Integrität ist in Fernwirk, Biologie und Ablaufmessung erhöht, weil verfälschte Werte und Befehle die Wirkung bestimmen.

| Zone | Bezeichnung | 1 | 2 | 3 | 4 | 5 | 6 | 7 | SL-T | Begründung |
|---|---|---|---|---|---|---|---|---|---|---|
| Z03 | DMZ | 3 | 3 | 2 | 3 | 3 | 2 | 2 | 3 | einziger Übergang für Fernzugriff und IT |
| Z04 | Leitsystem | 3 | 3 | 2 | 2 | 3 | 2 | 3 | 3 | reguläre Befehle an Pumpwerke und Gas |
| Z05 | Engineering | 3 | 3 | 3 | 3 | 3 | 2 | 2 | 3 | kann jedes Programm ändern |
| Z06 | OT-Management | 3 | 3 | 2 | 2 | 3 | 2 | 2 | 3 | steuert die Segmentierung |
| Z07 | Fernwirkzentrale | 3 | 3 | 3 | 2 | 3 | 2 | 3 | 3 | Befehle an alle Außenstationen |
| Z08 | Außenstationen Kanalnetz | 3 | 3 | 3 | 2 | 3 | 2 | 3 | 3 | öffentlich zugänglich, unbemannt |
| Z09 | Zelle Zulauf, Mechanik | 2 | 2 | 2 | 1 | 2 | 2 | 2 | 2 | Folge ist Rückstau im Zulauf, begrenzt |
| Z10 | Zelle Biologie | 2 | 2 | 3 | 1 | 2 | 2 | 2 | 2 | Überwachungswerte; FR3 erhöht wegen Sollwerten |
| Z11 | Zelle Schlamm, Faulung | 2 | 2 | 2 | 1 | 2 | 2 | 2 | 2 | Faulung reagiert langsam |
| Z12 | Zelle Gas, Energie | 3 | 3 | 3 | 1 | 3 | 2 | 3 | 3 | Explosionsschutz |
| Z13 | OEM BHKW | 3 | 3 | 3 | 1 | 3 | 2 | 2 | 3 | Herstellerzugang, Gasverbrauch |
| Z14 | Ablaufmessstation | 2 | 2 | 3 | 1 | 2 | 2 | 2 | 2 | Integrität der Messwerte |
| Z15 | Temporär verbundene Geräte | 2 | 2 | 3 | 1 | 3 | 2 | 1 | 2 | ZCR 3.4: eigene Zone |
| Z17 | Gebäudesicherheit | 2 | 2 | 2 | 2 | 2 | 1 | 1 | 2 | eigenes VLAN, nur Video zur Leitwarte |

# 8 Vergleich mit den Fähigkeiten (ZCR 4)

| Zone | Komponente, Befund | SL-C erwartet | SL-T | Kompensierende Maßnahme |
|---|---|---|---|---|
| Z08 | IEC 60870-5-104 ohne Authentisierung, Klartext zwischen Router und RTU | 1 in FR1, FR3, FR4 | 3 | TLS nach IEC 62351-3 und Secure Authentication nach IEC 60870-5-7 (z. B. TIM 1531 IRC, CP 1243-8 IRC); IPsec endet am Router. Allowlist, Plausibilisierung |

| Zone | Komponente, Befund | SL-C erwartet | SL-T | Kompensierende Maßnahme |
|---|---|---|---|---|
| Z08 | Außenstationen: S7-1200 G2 mit Fernwirk-CP, LTE-Router im öffentlichen Raum | S7-1200 G2 nach 62443-4-2 zertifiziert; Bestandsgeräte der ersten Generation und Router je Gerät prüfen | 3 | Türkontakt, Port Security, Plausibilisierung, Zertifikat je Station; Bestand der ersten Generation ersetzen |
| Z09 bis Z12 | S7-1500, Firmware ab V3.1 | Zertifikat IEC 62443-4-2 (TÜV SÜD), überwiegend SL 2 | 2 bis 3 | PUT/GET aus, Zugriffsschutz, Sollwertgrenzen in der SPS; Firmwarestand prüfen |
| Z13 | BHKW-Steuerungen mit Modbus und Herstellerzugang | 1 in FR1, FR2 | 3 | Firewall nur lesen, Herstellerzugang über Jump-Host |
| Z04, Z05 | Leitsystem und Windows-Systeme | Zertifikat je Produkt prüfen, keins pauschal angenommen | 3 | Härtung, Whitelisting, Konten je Person, MFA; Nachweis 62443-3-3 durch den Integrator |
| Z14 | Analysatoren mit Modbus | 1 | 2 | nur lesen, Plausibilisierung mit Laborwerten |

SL-C-Angaben sind Erwartungen für die beschriebene Konfiguration. Nachweise nach IEC 62443-4-2 sind bei den Herstellern anzufordern.

# 9 Anforderungen (ZCR 6)

| Nr. | Anforderung an Lieferanten | Bezug |
|---|---|---|
| L-01 | Nachweis SL-C nach IEC 62443-4-2 je Komponente (Zertifikat oder Herstellererklärung getrennt ausweisen) mit Firmwarestand | IEC 62443-4-2 |
| L-01a | Nachweis der Systemanforderungen nach IEC 62443-3-3 für das konkrete System durch den Integrator | IEC 62443-3-3 |
| L-02 | Prozesse des Dienstleisters für Fernwartung, Patches, Sicherung | IEC 62443-2-4 |
| L-03 | Fernwirk: Allowlist der Master-Adressen, IPsec bis in die RTU oder IEC 62351, Plausibilisierung von Befehlen | SR 2.1, 3.1, 3.5 |
| L-04 | Steuerungen: PUT/GET aus, Zugriffsschutz, Sollwertgrenzen für sicherheits- und umweltrelevante Sollwerte | SR 2.1, 3.5 |
| L-05 | BHKW und OEM: keine eigenen Router, Fernzugang nur über Jump-Host, Modbus-Schreiben abschaltbar | SR 1.13, 5.2 |

| Nr. | Anforderung an Lieferanten | Bezug |
|---|---|---|
| L-06 | Kommunikationsmatrix aller Ports und Protokolle zur Abnahme | SR 7.7 |
| L-07 | Sicherheitsupdates und Schwachstellenmeldungen über die Nutzungsdauer | IEC 62443-4-1, CRA |
| L-08 | Sicherungs- und Wiederherstellungsanleitung, Sollstände übergeben | SR 7.3, 7.4 |

# 10 Freigabe (ZCR 7)

| Rolle | Name | Datum | Unterschrift |
|---|---|---|---|
| Werkleitung, Betreiber | [Name] | | |
| Betriebsleitung | [Name] | | |
| Verfasser | Maximilian Gilg, OT-Cyber.de | | |