BERICHT

Risikobewertung Cyberangriffe

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 Ausgangslage und Methode

3 Ergebnisse

4 Maßnahmen

5 Nächste Schritte

1 Management Summary

Für den fiktiven Verteilnetzbetreiber mit zwei Umspannwerken 110/20 kV, Netzleitstelle, Ortsnetzstationen und PV-Park wurden sechs Angriffe bewertet: Massenschaltbefehle aus der Leitstelle, Angriff über das 450-MHz-Funknetz, gefälschte Abtastwerte im Prozessbus, manipulierter Parkregler beim Kunden, gefälschte Redispatch-Abrufe und Ransomware in der Netzleitstelle.

Ohne Härtung sind 1 Szenarien kritisch. Im Planungsstand sind 1 hoch und 5 mittel. Am schwersten wiegt der Angriff über die Netzleitstelle selbst: Er nutzt den regulären Fernwirkweg; nur Konten mit MFA und die Befehlsprüfung im Stationsrechner halten ihn auf. Mikrosegmentierung hilft bei Funknetz und Prozessbus deutlich.

GESAMTBEWERTUNG

Der Schutz arbeitet in den Schutzgeräten eigenständig und verhindert Schäden an Anlage und Menschen. Die Versorgung schützt er nicht: Ein Angreifer mit Zugang zur Leitstelle kann über den regulären Weg schalten. Dagegen helfen Konten mit MFA, Befehlsprüfung in den Stationen und eingeübte Ortsbedienung.

SZENARIEN NACH RISIKOKLASSE

Klasse	Ohne Härtung	Planungsstand	Mikrosegmentierung	Vollständig
KRITISCH	1	0	0	0
HOCH	1	1	1	0
MITTEL	4	5	3	0
NIEDRIG	0	0	2	6

2 Ausgangslage und Methode

Grundlage sind die Übersichtsschaltpläne UW-US-001, das Kommunikations- und Schutzkonzept und der HTML-Leitstand (Umspannwerke_Leitstand_PurpleTeam.html) mit Simulation, Netzwerkverkehr, Segmentierung und den Szenarien U1 bis U6. Jedes Szenario ist dort nachgestellt; der Mitschnitt zeigt denselben Verlauf.

- **Risiko** ist Auswirkung (A) mal Eintrittswahrscheinlichkeit (W), je 1 bis 5, in Anlehnung an IEC 62443-3-2.
- **Auswirkung** nach der schwersten Kategorie: Mensch, Lebensmittelsicherheit und Umwelt, Betrieb und Finanzen.
- **Vier Stände:** Ohne Härtung (flaches Netz, keine Maßnahme); Planungsstand (Zonen, getrenntes Fernwirk-WAN, H05, H07, H10); Mikrosegmentierung (Planungsstand plus Mikrosegmente); Vollständig (Mikrosegmentierung und H01 bis H14).
- **Klassen:** KRITISCH ab 15, HOCH 10 bis 14, MITTEL 5 bis 9, NIEDRIG bis 4. Tolerierbar ist NIEDRIG, MITTEL mit Freigabe des Betreibers.

HÄRTUNGSMASSNAHMEN

Nr.	Maßnahme	Planungsstand
H01	Fernzugriff nur über Jump-Host mit Freigabe je Sitzung, keine direkten Herstellerzugänge	fehlt
H02	Eigene Benutzerverwaltung im OT mit MFA, Konten je Person in Leitsystem und Jump-Host	fehlt
H03	Zugriffsschutz für Schutzgeräte und Stationsrechner: Rollen nach IEC 62351-8, Passwörter, Konfigurationsschutz	fehlt
H04	Plausibilisierung von Redispatch-Abrufen, ICCP-Daten und Massenschaltungen im Leitsystem	fehlt
H05	Befehlsprüfung und feste Grenzen im Stationsrechner: Befehlsliste, Ratenbegrenzung, Spannungsband, PV-Gradient	umgesetzt
H06	Engineering nur von der Engineering-Station, Schutzparameter mit Vier-Augen-Freigabe	fehlt
H07	Schutz eigenständig in den Schutzgeräten, Buchholz und Druckentlastung hart, Reserveschutz der Gegenstation	umgesetzt
H08	Ortsteuerung als Rückfallebene mit Schaltberechtigung; Mehrfachschaltungen aus der Leitstelle nur mit zweitem Bediener	fehlt
H09	Härtung, Whitelisting und Patches nach Herstellerfreigabe für Station-HMI, Jump-Host und Engineering	fehlt
H10	Offline-Sicherung von Leitsystem, Stationsprojekten und Schutzparametern, geübter Wiederanlauf und Schwarzfall	umgesetzt
H11	OT-Monitoring mit Auswertung von IEC 104, IEC 61850 und Prozessbus	fehlt
H12	Prozessbus mit festen Teilnehmern, Plausibilisierung der Abtastwerte und PTP-Überwachung im Schutz	fehlt
H13	Port Security und NAC in Stationen, Laptops nur geprüft, USB-Kontrolle	fehlt

Nr.	Maßnahme	Planungsstand
H14	Reaktionsplan mit Übertragungsnetzbetreiber, Nachbarnetzbetreibern und Krisenstab, jährliche Übung	fehlt
SEG	Zonen mit Firewall und Zellenfirewalls, Mikrosegmente	Zonen ja, Mikro fehlt

3 Ergebnisse

3.1 Übersicht

ID	Szenario	Ohne Härtung	Planungsstand	Mikrosegmentierung	Vollständig
U1	Massenhafte Schaltbefehle aus der Netzleitstelle	KRITISCH	HOCH	HOCH	NIEDRIG
U2	Ortsnetzstationen über das 450-MHz-Funknetz	MITTEL	MITTEL	NIEDRIG	NIEDRIG
U3	Gefälschte Abtastwerte im Prozessbus	MITTEL	MITTEL	NIEDRIG	NIEDRIG
U4	Parkregler des PV-Parks manipuliert	MITTEL	MITTEL	MITTEL	NIEDRIG
U5	Gefälschte Redispatch-Abrufe	MITTEL	MITTEL	MITTEL	NIEDRIG
U6	Ransomware in der Netzleitstelle	HOCH	MITTEL	MITTEL	NIEDRIG

Tabelle 1: Risikoklasse je Szenario in vier Ständen

3.2 Szenarien im Detail

3.2.1 U1 Massenhafte Schaltbefehle aus der Netzleitstelle

Ohne Härtung	**KRITISCH** (A 5 × W 3 = 15)
Betroffene Systeme	Jump-Host (Z03), Leitsystem und Front-End (Z04), Fernwirkgateways (Z09, Z10)
Ort	Netzleitstelle, beide Umspannwerke
Angriffsweg	1. Admin-Daten für Jump-Host und Leitsystem erbeutet (T0859) 2. SSH vom Jump-Host auf den Leitsystem-Server (T0886) 3. Schadsoftware sendet IEC 104 über das Front-End (T1692.001, T0885) 4. Abgänge und Leitungen aus (T0831, T0813)
Folgen	Große Teile der Stadt ohne Strom; Wiederversorgung nur mit Personal vor Ort in den Stationen, Stunden bis zur Normalversorgung.
Planungsstand	**HOCH** (A 4 × W 3 = 12); gelingt, Wirkung begrenzt durch H05
Mit Mikrosegmentierung	**HOCH** (A 4 × W 3 = 12); gelingt, Wirkung begrenzt durch H05
Vollständig	**NIEDRIG** (A 3 × W 1 = 3); gestoppt in Schritt 1 durch H02
Restrisiko	Die Leitstelle muss schalten können; Befehlsprüfung im Stationsrechner, Ortsteuerung und Personal vor Ort begrenzen die Wirkung.
Schaden im Ernstfall	Versorgungsunterbrechung für große Teile der Stadt, 1 bis 10 Mio. € einschließlich Folgeschäden
Referenz	MITRE ATT&CK for ICS v20: T0859, T0886, T1692.001, T0885, T0831, T0813; IEC 62443-3-3 SR 1.1, SR 2.1, SR 3.5; Industroyer2 als Vorbild

3.2.2 U2 Ortsnetzstationen über das 450-MHz-Funknetz

Ohne Härtung	**MITTEL** (A 3 × W 3 = 9)
Betroffene Systeme	450-MHz-Router und Fernwirkstationen der Ortsnetzstationen (Z12)
Ort	Ortsnetzstationen
Angriffsweg	1. Funkrouter ONS 6 mit alter Firmware übernommen (T0866, T0859) 2. Vom Router zu anderen Fernwirkstationen (T0886) 3. IEC-104-Befehle an die Lasttrennschalter (T1692.001) 4. Straßenzüge ohne Strom (T0813)
Folgen	Mehrere Straßenzüge ohne Strom, Monteure müssen jede Station anfahren.
Planungsstand	**MITTEL** (A 3 × W 3 = 9); gelingt
Mit Mikrosegmentierung	**NIEDRIG** (A 3 × W 1 = 3); gestoppt in Schritt 2 durch Mikrosegmentierung
Vollständig	**NIEDRIG** (A 2 × W 1 = 2); gestoppt in Schritt 1 durch H09
Restrisiko	Funkrouter stehen öffentlich zugänglich; Firmware, Zertifikate und Trennung der Router voneinander sind Pflicht.
Schaden im Ernstfall	0,1 bis 0,5 Mio. €, Straßenzüge ohne Strom
Referenz	MITRE ATT&CK for ICS v20: T0866, T0859, T0886, T1692.001, T0813; IEC 62443-3-3 SR 1.2, SR 5.1; IEC 62351-5

3.2.3 U3 Gefälschte Abtastwerte im Prozessbus

Ohne Härtung	**MITTEL** (A 4 × W 2 = 8)
Betroffene Systeme	Prozessbus UW Süd (Z11), Trafodifferenzialschutz (Z10)
Ort	UW Süd, GIS-Gebäude
Angriffsweg	1. Gerät am Prozessbus-Switch angeschlossen (T0847) 2. Gefälschte Sampled Values im Prozessbus (T0830, T1692.002) 3. Schutz wertet gefälschte Ströme aus (T0832) 4. Trafo T1 aus (T0813)
Folgen	Trafo T1 aus, eine Hälfte des UW Süd ohne Strom, bis über die Kupplung umgeschaltet ist; bei beiden Trafos die gesamte Station.
Planungsstand	**MITTEL** (A 4 × W 2 = 8); gelingt
Mit Mikrosegmentierung	**NIEDRIG** (A 4 × W 1 = 4); gestoppt in Schritt 2 durch Mikrosegmentierung
Vollständig	**NIEDRIG** (A 2 × W 1 = 2); gestoppt in Schritt 1 durch H13
Restrisiko	Ein Täter vor Ort bleibt möglich; Zutritt, Port Security und SV-Plausibilisierung im Schutz halten den Angriff auf.
Schaden im Ernstfall	0,2 bis 1 Mio. €, Teilausfall des UW Süd
Referenz	MITRE ATT&CK for ICS v20: T0847, T0830, T1692.002, T0832, T0813; IEC 61850-9-2, IEC 62351-6; IEC 62443-3-3 SR 1.2

3.2.4 U4 Parkregler des PV-Parks manipuliert

Ohne Härtung	**MITTEL** (A 3 × W 3 = 9)
Betroffene Systeme	Parkregler und Übergabeschutz PV-Park (Z13, Anlage des Kunden)
Ort	PV-Park, Übergabestation
Angriffsweg	1. Fernwartung des PV-Betreibers kompromittiert (T0822) 2. Parkregler übernommen (T0859) 3. Einspeisung ohne Rücksicht auf die Vorgabe (T0836, T0831) 4. Überspannung, Netzengpass (T0879)
Folgen	Überspannung im Netz Süd, Schäden bei Kunden möglich, Netzengpass; der Übergabeschutz schaltet den Park ab.
Planungsstand	**MITTEL** (A 2 × W 3 = 6); gelingt, Wirkung begrenzt durch H07
Mit Mikrosegmentierung	**MITTEL** (A 2 × W 3 = 6); gelingt, Wirkung begrenzt durch H07
Vollständig	**NIEDRIG** (A 2 × W 2 = 4); gelingt, Wirkung begrenzt durch H07
Restrisiko	Kundenanlagen liegen außerhalb des eigenen Einflusses; Anforderungen im Netzanschlussvertrag und eigenständiger Übergabeschutz sind die Barrieren.
Schaden im Ernstfall	0,1 bis 1 Mio. €, Überspannung bei Kunden
Referenz	MITRE ATT&CK for ICS v20: T0822, T0859, T0836, T0831, T0879; VDE-AR-N 4110

3.2.5 U5 Gefälschte Redispatch-Abrufe

Ohne Härtung	**MITTEL** (A 3 × W 3 = 9)
Betroffene Systeme	Redispatch-Gateway (Z03), Leitsystem (Z04)
Ort	Netzleitstelle
Angriffsweg	1. Redispatch-Gateway in der DMZ übernommen (T0866) 2. Gefälschter Abruf an das Leitsystem (T0843) 3. Leitsystem übernimmt Abregelung und Sollspannung (T0836) 4. Abregelung, Spannungsprobleme (T0831)
Folgen	Unnötige Abregelung mit Entschädigungspflicht, Spannungsprobleme, fehlerhafte Daten an den Übertragungsnetzbetreiber.
Planungsstand	**MITTEL** (A 2 × W 3 = 6); gelingt, Wirkung begrenzt durch H05
Mit Mikrosegmentierung	**MITTEL** (A 2 × W 3 = 6); gelingt, Wirkung begrenzt durch H05
Vollständig	**NIEDRIG** (A 2 × W 1 = 2); gestoppt in Schritt 1 durch H09
Restrisiko	Abrufe kommen auf regulärem Weg; nur Plausibilisierung und Grenzen im Stationsrechner halten sie auf.
Schaden im Ernstfall	0,1 bis 1 Mio. €: Entschädigung für Abregelung, Ausgleichsenergie
Referenz	MITRE ATT&CK for ICS v20: T0866, T0843, T0836, T0831; IEC 62443-3-3 SR 3.5

3.2.6 U6 Ransomware in der Netzleitstelle

Ohne Härtung	**HOCH** (A 4 × W 3 = 12)
Betroffene Systeme	Jump-Host (Z03), Leitsystem und Engineering (Z04, Z05)
Ort	Netzleitstelle
Angriffsweg	1. Admin-Daten aus der IT gestohlen (T0859) 2. SSH und RDP vom Jump-Host (T0886) 3. Server und Engineering verschlüsselt (T0809) 4. Leitstelle blind (T0815)
Folgen	Netzleitstelle blind; Stationen und Schutz arbeiten weiter, Schalten nur vor Ort; Störungen werden spät erkannt.
Planungsstand	**MITTEL** (A 3 × W 3 = 9); gelingt, Wirkung begrenzt durch H10
Mit Mikrosegmentierung	**MITTEL** (A 3 × W 3 = 9); gelingt, Wirkung begrenzt durch H10
Vollständig	**NIEDRIG** (A 2 × W 1 = 2); gestoppt in Schritt 1 durch H02
Restrisiko	Stationen und Schutz arbeiten weiter; Offline-Sicherung, Konten und Whitelisting begrenzen den Schaden.
Schaden im Ernstfall	0,5 bis 3 Mio. €: Wiederherstellung, Personal in Stationen
Referenz	MITRE ATT&CK for ICS v20: T0859, T0886, T0809, T0815; IEC 62443-3-3 SR 1.1, SR 3.2, SR 7.3

4 Maßnahmen

Bezug zeigt, in welchen Szenarien die Maßnahme einen Schritt stoppt oder die Wirkung begrenzt.

Nr.	Maßnahme	Bezug	Priorität
H01	Fernzugriff nur über Jump-Host mit Freigabe je Sitzung, keine direkten Herstellerzugänge	alle	**Mittel**
H02	Eigene Benutzerverwaltung im OT mit MFA, Konten je Person in Leitsystem und Jump-Host	U1, U6	**Hoch**
H03	Zugriffsschutz für Schutzgeräte und Stationsrechner: Rollen nach IEC 62351-8, Passwörter, Konfigurationsschutz	U2	**Hoch**
H04	Plausibilisierung von Redispatch-Abrufen, ICCP-Daten und Massenschaltungen im Leitsystem	U5	**Mittel**
H05	Befehlsprüfung und feste Grenzen im Stationsrechner: Befehlsliste, Ratenbegrenzung, Spannungsband, PV-Gradient	U1, U5	umgesetzt
H06	Engineering nur von der Engineering-Station, Schutzparameter mit Vier-Augen-Freigabe	alle	**Mittel**
H07	Schutz eigenständig in den Schutzgeräten, Buchholz und Druckentlastung hart, Reserveschutz der Gegenstation	U4	umgesetzt
H08	Ortsteuerung als Rückfallebene mit Schaltberechtigung; Mehrfachschaltungen aus der Leitstelle nur mit zweitem Bediener	U2, U3	**Mittel**
H09	Härtung, Whitelisting und Patches nach Herstellerfreigabe für Station-HMI, Jump-Host und Engineering	U2, U5, U6	**Hoch**
H10	Offline-Sicherung von Leitsystem, Stationsprojekten und Schutzparametern, geübter Wiederanlauf und Schwarzfall	U6	umgesetzt
H11	OT-Monitoring mit Auswertung von IEC 104, IEC 61850 und Prozessbus	alle	**Mittel**
H12	Prozessbus mit festen Teilnehmern, Plausibilisierung der Abtastwerte und PTP-Überwachung im Schutz	U3	**Hoch**
H13	Port Security und NAC in Stationen, Laptops nur geprüft, USB-Kontrolle	U3	**Hoch**
H14	Reaktionsplan mit Übertragungsnetzbetreiber, Nachbarnetzbetreibern und Krisenstab, jährliche Übung	alle	**Mittel**
SEG	Mikrosegmente: Front-End, Funkrouter, Prozessbus, Schutzgeräte getrennt	U2, U3	**Hoch**

Tabelle 2: Maßnahmen und Priorität im Planungsstand

Eine Stadt ohne Strom (U1) trifft Krankenhäuser, Pflegeheime und Wasserversorgung. Die Maßnahmen mit Priorität Hoch sind dagegen überschaubar.

4.1 Rechtlicher Rahmen

- **Netzbetreiber:** Betreiber von Energieversorgungsnetzen unterliegen unabhängig von ihrer Größe den §§ 5c und 5d EnWG: IT-Sicherheitskatalog der Bundesnetzagentur (bis zur neuen Festlegung gilt der Katalog für Strom- und Gasnetze von 2015) und Dokumentationspflicht.
- **Meldepflichten:** erhebliche Sicherheitsvorfälle nach § 5d Abs. 3 EnWG an die Meldestelle nach § 32 BSIG: Erstmeldung spätestens 24 h, Meldung mit Bewertung spätestens 72 h, Abschlussmeldung entsprechend § 32 Abs. 2 BSIG.
- **KRITIS:** Stromverteilernetze sind ab 3.700 GWh entnommener Jahresarbeit kritische Anlagen; dieses Netz liegt mit rund 250 GWh darunter. Die Pflichten aus dem EnWG gelten trotzdem.
- **Technische Regeln:** VDE-AR-N 4110 und 4120 für Netzanschlüsse, IEC 61850 und IEC 62351 für Stationsautomatisierung und deren Sicherheit.

HINWEIS

Werte und Szenarien beziehen sich auf eine fiktive Anlage. Für einen realen Betrieb sind Bewertung, Kosten und Fristen mit Betreiber, Behörden und Lieferanten abzustimmen.

5 Nächste Schritte

- MFA und eigene Konten für Jump-Host und Leitsystem (H02).
- Funkrouter: Firmware, Zertifikate und Trennung voneinander (H09, Mikrosegmente).
- Prozessbus: Port Security und SV-Plausibilisierung im Schutz (H12, H13).
- Planspiel mit Ortsbedienung aller Stationen (H08, H14).