BERICHT

# Risikobewertung Cyberangriffe

## Hartkäserei im Bestand, Planungsstand Index C

| | |
|---|---|
| **Auftraggeber** | [Betreiber, Ort] |
| **Projekt** | GuD-Heizkraftwerk, 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 das fiktive Stadtwerke-Heizkraftwerk mit rund 100 MWel, Röhrenspeicher, Fernwärme und 110-kV-Netzanschluss wurden sechs Angriffe bewertet: manipulierter Fahrplan, Schaltbefehle über die Fernwirkverbindung des Netzbetreibers, veränderte Schutzparameter, Angriff auf die Gasdruckregelung, missbrauchte Fernwartung der Wasseraufbereitung und Ransomware in der Leitwarte.

Ohne Härtung sind 1 Szenarien kritisch. Im Planungsstand sind 2 hoch und 3 mittel. Die beiden hohen Szenarien laufen über legitime Wege von außen: Fahrplan und Fernwirkverbindung. Dort hilft keine Segmentierung, sondern nur Plausibilisierung im Leitsystem und eine mit dem Netzbetreiber vereinbarte Befehlsliste.

GESAMTBEWERTUNG

**Turbinen-, Kessel-, Gas- und Netzschutz wirken unabhängig von der Leittechnik und halten die schwersten Folgen ab. Offen sind die Steuerwege von außen: Fahrpläne aus der IT und Befehle aus der Netzleitstelle. Sie brauchen fachliche Plausibilisierung und Absprachen mit dem Netzbetreiber.**

SZENARIEN NACH RISIKOKLASSE

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

# 2 Ausgangslage und Methode

Grundlage sind das R&I-Fließbild GUD-RI-001, das Kommunikations- und Schutzkonzept und der HTML-Leitstand (GuD_Kraftwerk_Leitstand_PurpleTeam.html) mit Simulation, Netzwerkverkehr, Segmentierung und den Szenarien G1 bis G6. 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 mit Firewall und Zellenfirewalls, 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; Ferndiagnose der Turbine nur als Datenexport aus dem Historian | fehlt |
| H02 | Eigene Benutzerverwaltung im OT, keine Konten der IT, Admin-Konten je Person mit MFA | fehlt |
| H03 | Zugriffsschutz für S7-Steuerungen und Schutzgeräte: PUT/GET aus, Passwörter und Rollen nach IEC 62351-8 | fehlt |
| H04 | Plausibilisierung von Sollwerten aus Fahrplan und Netzleitstelle im Leitsystem: Grenzen, Gradienten, Abgleich mit dem Netzbetreiber | fehlt |
| H05 | Feste Grenzen in den Zellen-SPS: GDRM-Druck 28 bis 32 bar, Speicher bis 70 bar, Vorlauf 90 bis 130 °C | umgesetzt |
| H06 | Engineering nur von den Engineering-Stationen, Änderungen an Schutzparametern mit Vier-Augen-Freigabe | fehlt |
| H07 | Schutzfunktionen autark: Turbinen- und Kesselschutz im F-Teil und hart, Sicherheitsabsperr-, Abblase- und Sicherheitsventile mechanisch, Netzschutz eigenständig | umgesetzt |
| H08 | Schaltbefehle an 110-kV-Leistungsschalter aus dem Leitsystem nur mit Bestätigung durch einen zweiten Bediener; Fernsteuerung durch den Netzbetreiber über festgelegte Befehle | fehlt |
| H09 | Härtung, Whitelisting und Patches nach Herstellerfreigabe für DCS-Server, Thin Clients und Station-HMI | fehlt |
| H10 | Offline-Sicherung von DCS, SPS und Schutzparametern, geübter Wiederanlauf und Schwarzfall-Prozedur | umgesetzt |
| H11 | OT-Monitoring mit Auswertung von IEC 61850, IEC 60870-5-104 und DCS-Verkehr | fehlt |
| H12 | USB-Schleuse und Kontrolle von Service-Laptops | fehlt |

| Nr. | Maßnahme | Planungsstand |
|---|---|---|
| H13 | Port Security und NAC; Stationsbus nur mit bekannten Geräten | fehlt |
| H14 | Reaktionsplan mit Netzbetreiber, Fernwärmenetz und Behörden, Meldewege, 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 |
|---|---|---|---|---|---|
| G1 | Fahrplan der Einsatzplanung manipuliert | HOCH | HOCH | HOCH | NIEDRIG |
| G2 | Schaltbefehle über die Fernwirkverbindung des Netzbetreibers | HOCH | HOCH | HOCH | NIEDRIG |
| G3 | Schutzparameter des Maschinentrafos verändert | HOCH | MITTEL | MITTEL | NIEDRIG |
| G4 | Gasdruckregelung und Röhrenspeicher manipuliert | KRITISCH | NIEDRIG | NIEDRIG | NIEDRIG |
| G5 | Fernwartung der Vollentsalzung missbraucht | MITTEL | MITTEL | MITTEL | NIEDRIG |
| G6 | Ransomware legt die Leitwarte lahm | HOCH | MITTEL | MITTEL | NIEDRIG |

Tabelle 1: Risikoklasse je Szenario in vier Ständen

## 3.2 Szenarien im Detail

### 3.2.1 G1 Fahrplan der Einsatzplanung manipuliert

| | |
|---|---|
| **Ohne Härtung** | **HOCH** (A 3 × W 4 = 12) |
| **Betroffene Systeme** | Fahrplanserver der Einsatzplanung (Z01), Historian (Z03), DCS-Server (Z04) |
| **Ort** | IT, DMZ, Leitwarte |
| **Angriffsweg** | 1. Fahrplanserver in der IT kompromittiert (T0817, T0866) 2. Fahrplan auf dem regulären Weg in die DMZ (T0843) 3. Historian schreibt den Fahrplan als Sollwert an DCS (T1692.002) 4. Lastsprünge, Regelleistung fehlt (T0831, T0882) |
| **Folgen** | Thermische Wechselbelastung von Turbinen und Kessel, zugesagte Primärregelleistung nicht verfügbar, Ausgleichsenergie und Vertragsstrafen. |
| **Planungsstand** | **HOCH** (A 3 × W 4 = 12); gelingt |
| **Mit Mikrosegmentierung** | **HOCH** (A 3 × W 4 = 12); gelingt |
| **Vollständig** | **NIEDRIG** (A 2 × W 1 = 2); gestoppt in Schritt 3 durch H04 |
| **Restrisiko** | Der Fahrplanweg ist ein legitimer Schreibweg von außen; nur Plausibilisierung, Gradientenbegrenzung und signierte Fahrpläne halten ihn sicher. |
| **Schaden im Ernstfall** | 0,2 bis 2 Mio. €: Ausgleichsenergie, Pönalen für nicht erbrachte Regelleistung, Verschleiß |
| **Referenz** | MITRE ATT&CK for ICS v20: T0817, T0866, T0843, T1692.002, T0831; IEC 62443-3-3 SR 3.5, SR 5.2 |

### 3.2.2 G2 Schaltbefehle über die Fernwirkverbindung des Netzbetreibers

| | |
|---|---|
| **Ohne Härtung** | **HOCH** (A 4 × W 3 = 12) |
| **Betroffene Systeme** | Netzleitstelle des Netzbetreibers, Fernwirkrouter und SICAM A8000 (Z12, Z13) |
| **Ort** | GIS-Gebäude, Fernwirkschrank |
| **Angriffsweg** | 1. System der Netzleitstelle kompromittiert (T0866) 2. IEC 104 von der Netzleitstelle zum Fernwirkgateway, legitimer Weg (T0885) 3. Doppelbefehle Generatorfelder aus, Sollwert 0 (T1692.001, T0831) 4. Kraftwerk vom Netz, Fernwärme auf Spitzenkessel (T0826, T0813) |
| **Folgen** | Kraftwerk geht unter Last vom Netz, Fernwärme fällt auf Speicher und Spitzenkessel; gleichzeitig bei mehreren Anlagen kann das zu einer Netzstörung beitragen. |
| **Planungsstand** | **HOCH** (A 4 × W 3 = 12); gelingt |
| **Mit Mikrosegmentierung** | **HOCH** (A 4 × W 3 = 12); gelingt |
| **Vollständig** | **NIEDRIG** (A 2 × W 1 = 2); gestoppt in Schritt 3 durch H08 |
| **Restrisiko** | Der Netzbetreiber muss das Kraftwerk fernsteuern können. Eine vereinbarte Befehlsliste und ein abgestimmter Reaktionsplan begrenzen den Schaden. |
| **Schaden im Ernstfall** | 0,5 bis 5 Mio. € plus Beitrag zu Netzstörungen bei gleichzeitigen Angriffen auf mehrere Anlagen |
| **Referenz** | MITRE ATT&CK for ICS v20: T0866, T0885, T1692.001, T0831, T0826, T0813; IEC 62443-3-3 SR 2.1, SR 3.1; IEC 62351 |

### 3.2.3 G3 Schutzparameter des Maschinentrafos verändert

| | |
|---|---|
| **Ohne Härtung** | **HOCH** (A 5 × W 2 = 10) |
| **Betroffene Systeme** | Jump-Host (Z03), Engineering-Station mit DIGSI 5 (Z05), SIPROTEC 7UT86 MT1 (Z12) |
| **Ort** | Leitwarte, GIS-Gebäude |
| **Angriffsweg** | 1. Admin-Daten für den Jump-Host erbeutet (T0859) 2. RDP vom Jump-Host zur Engineering-Station (T0886) 3. DIGSI: Differenzialschutz MT1 unwirksam gemacht (T0836, T0838) 4. Trafofehler ohne schnelle Abschaltung (T0880, T0879) |
| **Folgen** | Ein späterer Windungsschluss im Maschinentrafo wird nicht schnell abgeschaltet: Brand oder Explosion des Trafos, Gefahr für Personen, monatelanger Ausfall. |
| **Planungsstand** | **MITTEL** (A 3 × W 2 = 6); gelingt, Wirkung begrenzt durch H07 |
| **Mit Mikrosegmentierung** | **MITTEL** (A 3 × W 2 = 6); gelingt, Wirkung begrenzt durch H07 |
| **Vollständig** | **NIEDRIG** (A 2 × W 1 = 2); gestoppt in Schritt 1 durch H02 |
| **Restrisiko** | Engineering-Zugriff auf Schutzgeräte bleibt nötig. Buchholzschutz und Reserveschutz sind die letzte Barriere und müssen eigenständig bleiben. |
| **Schaden im Ernstfall** | 5 bis 30 Mio. €: Trafo-Ersatz mit langer Lieferzeit, Stillstand über Monate, Personengefahr |
| **Referenz** | MITRE ATT&CK for ICS v20: T0859, T0886, T0836, T0838, T0880, T0879; IEC 62443-3-3 SR 1.1, SR 2.1; IEC 62351-8 |

### 3.2.4 G4 Gasdruckregelung und Röhrenspeicher manipuliert

| | |
|---|---|
| **Ohne Härtung** | **KRITISCH** (A 5 × W 3 = 15) |
| **Betroffene Systeme** | AS-GAS (Z09), GDRM, Röhrenspeicher |
| **Ort** | GDRM-Gebäude, Röhrenspeicher |
| **Angriffsweg** | 1. Laptop eines Dienstleisters mit Schadsoftware im Gas-Schaltschrank (T0847) 2. S7 vom Laptop zur AS-GAS (T1692.001) 3. Ausgangsdruck 38 bar, Speichergrenze angehoben (T0836) 4. Überdruck, Sicherheitsabsperrventil schließt, GT-Schnellschluss (T0880, T0826) |
| **Folgen** | Überdruck im Brennstoffsystem der Gasturbine, Leckage und Brandgefahr; wirken die mechanischen Sicherheitseinrichtungen, fällt die Gasversorgung aus und die Gasturbine geht in den Schnellschluss. |
| **Planungsstand** | **NIEDRIG** (A 3 × W 1 = 3); gestoppt in Schritt 3 durch H05 |
| **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 H12, H13 |
| **Restrisiko** | Mechanische Sicherheitsabsperr- und Abblaseventile sind unabhängig von der SPS und müssen wiederkehrend geprüft werden. |
| **Schaden im Ernstfall** | Personen- und Sachschaden bei Gasaustritt, mehrere Mio. €; mit wirksamen Sicherheitseinrichtungen Stillstand der Gasturbine |
| **Referenz** | MITRE ATT&CK for ICS v20: T0847, T1692.001, T0836, T0880, T0826; IEC 62443-3-3 SR 1.2, SR 2.3, SR 3.5; DVGW G 491 |

### 3.2.5 G5 Fernwartung der Vollentsalzung missbraucht

| | |
|---|---|
| **Ohne Härtung** | **MITTEL** (A 3 × W 3 = 9) |
| **Betroffene Systeme** | Steuerung der Vollentsalzung (Z11), Jump-Host (Z03) |
| **Ort** | Wasseraufbereitung |
| **Angriffsweg** | 1. Zugangsdaten des Wasseraufbereiters erbeutet (T0859) 2. Sitzung über den Jump-Host zur Vollentsalzung (T0822) 3. Grenzwerte und Regeneration verstellt (T0836) 4. Speisewasser verunreinigt, Schaden nach Wochen (T0879) |
| **Folgen** | Schlechtes Speisewasser: Ablagerungen und Korrosion in Kessel und Turbine, Schaden erst nach Wochen sichtbar, Stillstand für Reinigung. |
| **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 H01 |
| **Restrisiko** | Die unabhängige Überwachung der Wasserchemie in der AS-WA und die Probenahme fangen auch Fehler ohne Angriff ab. |
| **Schaden im Ernstfall** | 0,5 bis 3 Mio. €: Reinigung, Austausch von Heizflächen, Stillstand |
| **Referenz** | MITRE ATT&CK for ICS v20: T0859, T0822, T0836, T0879; IEC 62443-3-3 SR 1.13, SR 3.5; IEC 62443-2-4 |

### 3.2.6 G6 Ransomware legt die Leitwarte lahm

| | |
|---|---|
| **Ohne Härtung** | **HOCH** (A 4 × W 3 = 12) |
| **Betroffene Systeme** | Jump-Host (Z03), DCS-Server und Thin Clients (Z04) |
| **Ort** | Serverraum, Leitwarte |
| **Angriffsweg** | 1. Admin-Daten für den Jump-Host aus der IT gestohlen (T0859) 2. RDP vom Jump-Host zum DCS-Server (T0886) 3. Server und Thin Clients verschlüsselt (T0809) 4. Leitwarte blind, Abfahren vor Ort (T0815, T0826) |
| **Folgen** | Leitwarte ohne Bilder; die Automatisierungssysteme regeln weiter, die Anlage muss vor Ort abgefahren werden, Wiederanlauf über Tage, Fernwärme über Spitzenkessel. |
| **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** | Der Weg über den Jump-Host ist legitim. Konten, Whitelisting und Offline-Sicherung begrenzen den Schaden; die Automatisierungssysteme regeln weiter. |
| **Schaden im Ernstfall** | 0,5 bis 3 Mio. €: Stillstand, Wiederherstellung mit dem Hersteller, Ersatzwärme |
| **Referenz** | MITRE ATT&CK for ICS v20: T0859, T0886, T0809, T0815, T0826; 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; Ferndiagnose der Turbine nur als Datenexport aus dem Historian | G5 | **Mittel** |
| H02 | Eigene Benutzerverwaltung im OT, keine Konten der IT, Admin-Konten je Person mit MFA | G3, G6 | **Hoch** |
| H03 | Zugriffsschutz für S7-Steuerungen und Schutzgeräte: PUT/GET aus, Passwörter und Rollen nach IEC 62351-8 | G3, G4, G5 | **Mittel** |
| H04 | Plausibilisierung von Sollwerten aus Fahrplan und Netzleitstelle im Leitsystem: Grenzen, Gradienten, Abgleich mit dem Netzbetreiber | G1 | **Hoch** |
| H05 | Feste Grenzen in den Zellen-SPS: GDRM-Druck 28 bis 32 bar, Speicher bis 70 bar, Vorlauf 90 bis 130 °C | G4, G5 | umgesetzt |
| H06 | Engineering nur von den Engineering-Stationen, Änderungen an Schutzparametern mit Vier-Augen-Freigabe | G3 | **Hoch** |
| H07 | Schutzfunktionen autark: Turbinen- und Kesselschutz im F-Teil und hart, Sicherheitsabsperr-, Abblase- und Sicherheitsventile mechanisch, Netzschutz eigenständig | G3, G4 | umgesetzt |
| H08 | Schaltbefehle an 110-kV-Leistungsschalter aus dem Leitsystem nur mit Bestätigung durch einen zweiten Bediener; Fernsteuerung durch den Netzbetreiber über festgelegte Befehle | G2 | **Hoch** |
| H09 | Härtung, Whitelisting und Patches nach Herstellerfreigabe für DCS-Server, Thin Clients und Station-HMI | G6 | **Mittel** |
| H10 | Offline-Sicherung von DCS, SPS und Schutzparametern, geübter Wiederanlauf und Schwarzfall-Prozedur | G6 | umgesetzt |
| H11 | OT-Monitoring mit Auswertung von IEC 61850, IEC 60870-5-104 und DCS-Verkehr | alle | **Mittel** |
| H12 | USB-Schleuse und Kontrolle von Service-Laptops | G4 | **Mittel** |
| H13 | Port Security und NAC; Stationsbus nur mit bekannten Geräten | G4 | **Mittel** |
| H14 | Reaktionsplan mit Netzbetreiber, Fernwärmenetz und Behörden, Meldewege, jährliche Übung | G2 | **Hoch** |
| SEG | Mikrosegmente: Bedienplätze, Server, Stationsrechner, Schutzgeräte getrennt | G4, G6 | **Mittel** |

Tabelle 2: Maßnahmen und Priorität im Planungsstand

Ein beschädigter Maschinentrafo (G3) bedeutet Monate Stillstand und Ersatzwärme; ein Gasaustritt (G4) gefährdet Menschen. Die organisatorischen Maßnahmen mit Priorität Hoch sind dagegen überschaubar.

## 4.1 Rechtlicher Rahmen

- **KRITIS und NIS2:** Erzeugungsanlagen sind nach BSI-KritisV ab 104 MW installierter Nettonennleistung kritische Anlagen, bei Präqualifikation für Primärregelleistung ab 36 MW. Das Heizkraftwerk ist präqualifiziert und damit kritische Anlage. Die Pflichten folgen aus §§ 5c und 5d EnWG (IT-Sicherheitskatalog der Bundesnetzagentur; bis zur neuen Festlegung gilt der Katalog für Energieanlagen von 2018); § 28 Abs. 5 BSIG nimmt diese Betreiber von Teilen der BSIG-Pflichten aus.
- **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.
- **Störfall-Verordnung:** Der Röhrenspeicher enthält rund 61 t Erdgas und liegt damit über der Mengenschwelle von 50 t (12. BImSchV Anhang I Nr. 2.1): Betriebsbereich der unteren Klasse. Cyberangriffe gehören in das Konzept zur Verhinderung von Störfällen.
- **Netzanschluss:** VDE-AR-N 4120; Fernsteuerung durch den Netzbetreiber und Redispatch nach Vertrag.
- **Immissionsschutz:** Großfeuerungsanlage nach 13. BImSchV mit Emissionsfernüberwachung; verfälschte Emissionsdaten sind ein eigenes Risiko.

**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

- Plausibilisierung von Fahrplänen und Sollwerten im Leitsystem (H04).
- Befehlsliste und Absicherung der Fernwirkverbindung mit dem Netzbetreiber vereinbaren (H08, L-05).
- Vier-Augen-Freigabe für Schutzparameter, Rollen nach IEC 62351-8 (H06, H03).
- Planspiel gemeinsam mit dem Netzbetreiber (H14).