BERICHT

Angriffspfade und Reaktionsplan

Hartkäserei im Bestand, Planungsstand Index C

Auftraggeber	[Betreiber, Ort]
Projekt	GuD-Heizkraftwerk, Incident Response
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 Vorgehen

3 Angriffspfade und Playbooks je Szenario

4 Reaktionsplan

5 Nächste Schritte

1 Management Summary

Für die sechs Hochrisiko-Szenarien zeigt dieses Dokument die Wege eines Angreifers bis zur Wirkung, die Barrieren, die ihn stoppen, und die Punkte, an denen Leitwarte, Schichtführer und OT-Security ihn erkennen. Daraus ist je Szenario ein Playbook abgeleitet.

Zwei Grundsätze bestimmen den Plan: Menschen und Netz vor Anlage, und bei jeder ungeplanten Leistungsänderung zuerst den Netzbetreiber informieren. Die Reaktion setzt in der Leitwarte und vor Ort an, während die OT-Security Zugänge trennt.

KERNAUSSAGE

Das Kraftwerk bleibt sicher, wenn Turbinen-, Kessel-, Gas- und Netzschutz unabhängig arbeiten. Für Angriffe über Fahrplan und Fernwirkverbindung braucht es eingeübte Absprachen mit Einsatzplanung und Netzbetreiber.

ID	Szenario	Erster Erkennungspunkt	Playbook
G1	Fahrplan der Einsatzplanung manipuliert	Häufung von Sollwertänderungen über OPC UA	PB-G1
G2	Schaltbefehle über die Fernwirkverbindung des Netzbetreibers	Doppelbefehle auf Generatorfelder	PB-G2
G3	Schutzparameter des Maschinentrafos verändert	DIGSI-Sitzung außerhalb einer Wartung	PB-G3
G4	Gasdruckregelung und Röhrenspeicher manipuliert	Neue MAC-Adresse im Gas-Netz	PB-G4
G5	Fernwartung der Vollentsalzung missbraucht	Sitzung ohne Wartungsauftrag	PB-G5
G6	Ransomware legt die Leitwarte lahm	RDP außerhalb der Wartung	PB-G6

2 Vorgehen

- **Pfade** in fünf Stufen nach MITRE ATT&CK for ICS v20: Erstzugang, Ausbreitung, Zugriff auf Steuerung, Manipulation, Wirkung.
- **Barrieren** (rot) sind die Härtungsmaßnahmen H01 bis H14 und die Segmentierung.
- **Erkennungspunkte** (grün) sind die Auslöser der Playbooks.
- **Playbooks** mit Auslöser, Sofortmaßnahmen, Eindämmen, Beseitigen, Wiederherstellen und Melden, jeweils mit Zuständigkeit.

3 Angriffspfade und Playbooks je Szenario

3.1 G1 Fahrplan der Einsatzplanung manipuliert

Angreifer übernehmen den Fahrplanserver der Einsatzplanung in der IT. Der Fahrplan läuft auf dem regulären Weg über den Historian in der DMZ als Sollwert an das Leitsystem und enthält Lastsprünge zwischen 20 und 97 MW alle zehn Minuten. Risiko: **HOCH** ohne Härtung, **HOCH** im Planungsstand, **HOCH** mit Mikrosegmentierung, **NIEDRIG** vollständig.

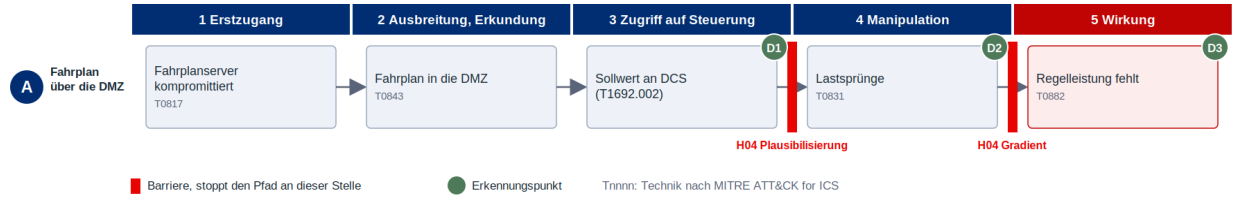


Abbildung: Angriffspfade G1

ERKENNUNGSPUNKTE

Nr.	Woran erkennbar	Wer oder wo
D1	Häufung von Sollwertänderungen über OPC UA	OT-Monitoring
D2	Lastsprünge ohne Anlass	Schichtleiter
D3	Übertragungsnetzbetreiber meldet fehlende Regelleistung	Netzbetreiber, Vermarkter

PLAYBOOK PB-G1

Phase	Maßnahmen	Zuständig
Auslöser	D1, D2, D3	jeder
Sofort	Fahrplanübernahme abschalten, konstante Leistung, Netzbetreiber und Regelleistungsvermarkter informieren.	Schichtleiter
Eindämmen	Verbindung Einsatzplanung zur DMZ sperren, Historian auf Veränderungen prüfen.	OT-Security
Melden	Meldestelle BSI nach § 5d EnWG, Netzbetreiber; Polizei.	Kraftwerksleitung, Geschäftsführung
Wiederherstellen	Plausibilisierung von Fahrplänen im Leitsystem, signierte Fahrpläne, Gradientenbegrenzung.	Kraftwerksleitung, Hersteller

3.2 G2 Schaltbefehle über die Fernwirkverbindung des Netzbetreibers

Ein Angreifer übernimmt ein System in der Netzleitstelle des Netzbetreibers und sendet über IEC 60870-5-104 Doppelbefehle an das Fernwirkgateway: Generatorfelder E04 und E05 aus, Sollwert 0 MW. Risiko: **HOCH** ohne Härtung, **HOCH** im Planungsstand, **HOCH** mit Mikrosegmentierung, **NIEDRIG** vollständig.

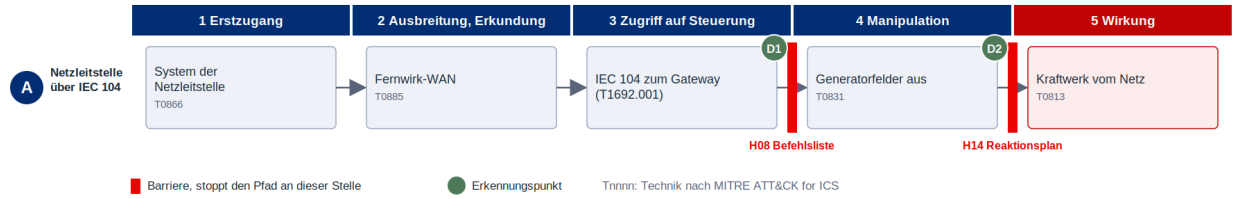


Abbildung: Angriffspfade G2

ERKENNUNGSPUNKTE

Nr.	Woran erkennbar	Wer oder wo
D1	Doppelbefehle auf Generatorfelder	OT-Monitoring
D2	Generatorschalter fällt ohne Schutzauslösung	Leitwarte

PLAYBOOK PB-G2

Phase	Maßnahmen	Zuständig
Auslöser	D1, D2	jeder
Sofort	Fernsteuerung auf Ort, Netzbetreiber telefonisch, Anlage stabil auf Eigenbedarf oder abfahren.	Schichtleiter
Eindämmen	Fernwirkverbindung mit dem Netzbetreiber gemeinsam trennen oder einschränken.	OT-Security
Melden	Meldestelle BSI nach § 5d EnWG, Netzbetreiber, Übertragungsnetzbetreiber.	Kraftwerksleitung, Geschäftsführung
Wiederherstellen	Befehlsliste mit dem Netzbetreiber vereinbaren, IEC 62351 bzw. IPsec auf dem Fernwirk-WAN.	Kraftwerksleitung, Hersteller

3.3 G3 Schutzparameter des Maschinentrafos verändert

Mit gestohlenen Admin-Daten meldet sich der Angreifer am Jump-Host an, springt per RDP auf die Engineering-Station mit DIGSI 5 und setzt den Ansprechwert des Differenzialschutzes für MT1 so hoch, dass ein Fehler im Trafo nicht mehr abgeschaltet wird. Risiko: **HOCH** ohne Härtung, **MITTEL** im Planungsstand, **MITTEL** mit Mikrosegmentierung, **NIEDRIG** vollständig.

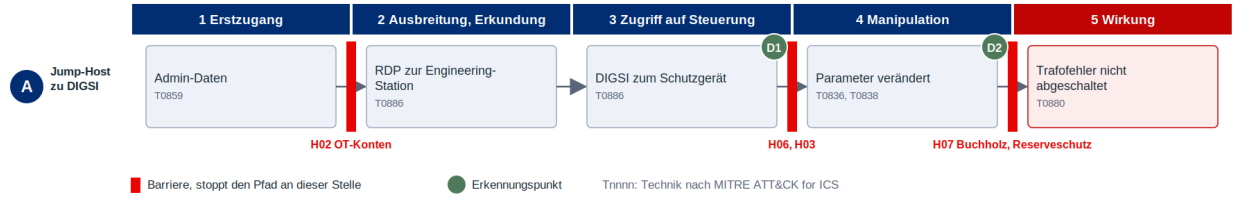


Abbildung: Angriffspfade G3

ERKENNUNGSPUNKTE

Nr.	Woran erkennbar	Wer oder wo
D1	DIGSI-Sitzung außerhalb einer Wartung	OT-Monitoring
D2	Schutzgerät meldet geänderten Parametersatz	Leitwarte, Schutztechnik

PLAYBOOK PB-G3

Phase	Maßnahmen	Zuständig
Auslöser	D1, D2	jeder
Sofort	Engineering-Station vom Netz, Schutzgerät auf freigegebenen Parametersatz prüfen.	Schichtleiter
Eindämmen	Konten sperren, alle Schutzgeräte gegen Sollstand vergleichen.	OT-Security
Melden	Meldestelle BSI nach § 5d EnWG, Netzbetreiber; Polizei.	Kraftwerksleitung, Geschäftsführung
Wiederherstellen	Vier-Augen-Freigabe für Schutzparameter, Rollen nach IEC 62351-8, regelmäßiger Sollstandvergleich.	Kraftwerksleitung, Hersteller

3.4 G4 Gasdruckregelung und Röhrenspeicher manipuliert

Ein infizierter Laptop eines Dienstleisters hängt im Gas-Schaltschrank. Die Schadsoftware schreibt in die AS-GAS einen Ausgangsdruck von 38 bar statt 30 bar und hebt die Höchstdruckgrenze des Speichers an. Risiko: **KRITISCH** ohne Härtung, **NIEDRIG** im Planungsstand, **NIEDRIG** mit Mikrosegmentierung, **NIEDRIG** vollständig.



Abbildung: Angriffspfade G4

ERKENNUNGSPUNKTE

Nr.	Woran erkennbar	Wer oder wo
D1	Neue MAC-Adresse im Gas-Netz	Switch, OT-Monitoring
D2	S7-Schreibzugriff von unbekanntem Gerät	OT-Monitoring
D3	Druckalarm, Sicherheitsabsperrventil zu	Leitwarte

PLAYBOOK PB-G4

Phase	Maßnahmen	Zuständig
Auslöser	D1, D2, D3	jeder
Sofort	Gasbereich räumen, Gaswarnung prüfen, Turbine abfahren, Feuerwehr bei Gasaustritt.	Schichtleiter
Eindämmen	Laptop vom Netz, Port sperren, Programm der AS-GAS prüfen.	OT-Security
Melden	BSI, Feuerwehr, Immissionsschutzbehörde bei Austritt, Gasnetzbetreiber.	Kraftwerksleitung, Geschäftsführung
Wiederherstellen	Firmware der AS-GAS auf V3.1, feste Grenzen, Laptopkontrolle, Port Security.	Kraftwerksleitung, Hersteller

3.5 G5 Fernwartung der Vollentsalzung missbraucht

Mit gestohlenen Zugangsdaten des Wasseraufbereiters verbindet sich der Angreifer über den Jump-Host zur Steuerung der Vollentsalzung, hebt die Leitfähigkeitsgrenze an und unterdrückt die Regeneration. Risiko: **MITTEL** ohne Härtung, **MITTEL** im Planungsstand, **MITTEL** mit Mikrosegmentierung, **NIEDRIG** vollständig.

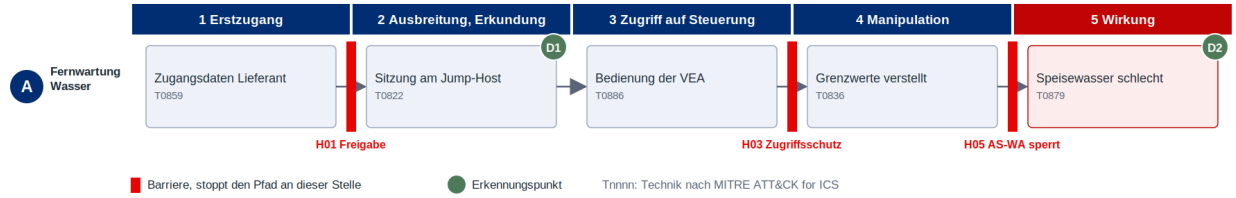


Abbildung: Angriffspfade G5

ERKENNUNGSPUNKTE

Nr.	Woran erkennbar	Wer oder wo
D1	Sitzung ohne Wartungsauftrag	Jump-Host
D2	Leitfähigkeit steigt, VE-Sperre	Leitwarte, Chemie

PLAYBOOK PB-G5

Phase	Maßnahmen	Zuständig
Auslöser	D1, D2	jeder
Sofort	VE-Einspeisung sperren, Laborkontrolle.	Schichtleiter
Eindämmen	Zugang des Lieferanten sperren, Sollstand der VEA prüfen.	OT-Security
Melden	BSI bei erheblicher Wirkung, Versicherung.	Kraftwerksleitung, Geschäftsführung
Wiederherstellen	Freigabe je Sitzung, unabhängige Überwachung der Wasserchemie.	Kraftwerksleitung, Hersteller

3.6 G6 Ransomware legt die Leitwarte lahm

Ransomware aus der IT scheitert am direkten Weg ins Leitsystem. Mit gestohlenen Admin-Daten gelangt der Angreifer über den Jump-Host per RDP auf die DCS-Server und verschlüsselt sie samt Thin Clients. Risiko: **HOCH** ohne Härtung, **MITTEL** im Planungsstand, **MITTEL** mit Mikrosegmentierung, **NIEDRIG** vollständig.

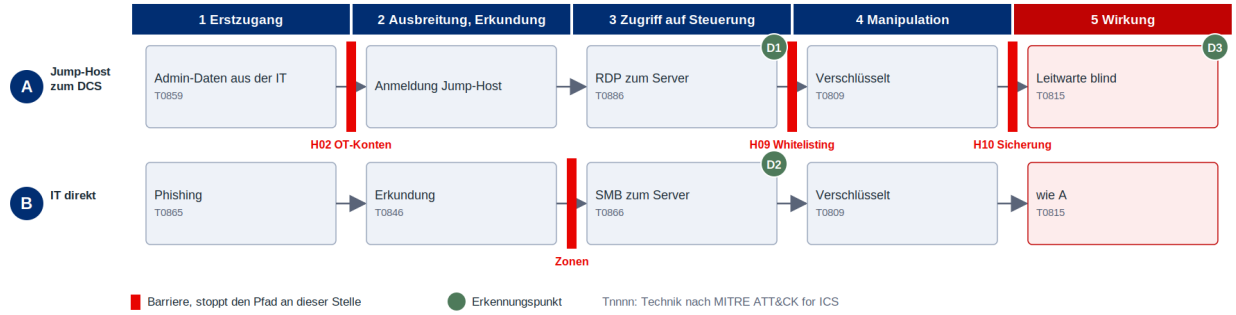


Abbildung: Angriffspfade G6

ERKENNUNGSPUNKTE

Nr.	Woran erkennbar	Wer oder wo
D1	RDP außerhalb der Wartung	OT-Monitoring
D2	Firewall deny vom Büro-PC	Log-Sammler
D3	Erpresserhinweis auf den Bildschirmen	Leitwarte

PLAYBOOK PB-G6

Phase	Maßnahmen	Zuständig
Auslöser	D1, D2, D3	jeder
Sofort	Jump-Host und Verbindungen zur IT sperren, Automatisierung weiterlaufen lassen.	Schichtleiter
Eindämmen	Konten sperren, Umfang feststellen.	OT-Security
Melden	Meldestelle BSI nach § 5d EnWG (24 h, 72 h, Abschluss), Netzbetreiber, Polizei, Versicherung.	Kraftwerksleitung, Geschäftsführung
Wiederherstellen	DCS aus Offline-Sicherung mit Siemens Energy, schrittweiser Wiederanlauf.	Kraftwerksleitung, Hersteller

4 Reaktionsplan

4.1 Grundsätze

- **Reihenfolge:** Menschen, Netz und Versorgung, Anlage, Betrieb.
- **Netzbetreiber zuerst informieren:** bei jeder ungeplanten Leistungsänderung und jedem Verdacht auf manipulierte Sollwerte.
- **Schutz nicht überbrücken:** auch nicht, um die Fernwärme zu halten.
- **Zugänge zuerst trennen:** Fernzugriff, Jump-Host, Verbindung zur IT und Fahrplanweg.
- **Alles mit Uhrzeit festhalten:** Schutzrecorder und Archive sind Beweismittel.

4.2 Notbetrieb ohne Leitsystem

Bereich	Notbetrieb
Gasturbine, Kessel, Dampfturbine	Automatisierungssysteme regeln mit letztem Sollwert; Abfahren vor Ort über Notbedienung
Netzanschluss	Schutz eigenständig; Schalten vor Ort über Station-HMI bzw. Schaltwärter
Gas	GDRM regelt mechanisch, Sicherheitsabsperrventile autark; Speicher hält 2,5 h
Fernwärme	Spitzenkessel mit eigener Brennersteuerung, Wärmespeicher rund 700 MWh
Alarmierung	Gaswarnung, Brandmelder und Kesselschutz unabhängig von der Leitwarte

4.3 Rollen

Rolle	Aufgabe	Besetzung
Schichtleiter	erkennt, setzt Sofortmaßnahmen, alarmiert, spricht mit dem Netzbetreiber	[Name, Telefon]
Kraftwerksleitung	Betrieb, Fahrweise, Fernwärme	[Name, Telefon]
Schutz- und Elektrotechnik	Schutzgeräte, Schaltanlagen	[Name, Telefon]
Gasmeister, Chemie	GDRM, Speicher, Wasserchemie	[Name, Telefon]
OT-Security	Bewertung, Zugänge trennen, Beweise, Wiederherstellung	[Name, Telefon]
Geschäftsführung	Stufe 3, Krisenstab, Meldungen, Öffentlichkeit	[Name, Telefon]

4.4 Stufen

Stufe	Merkmal	Entscheidet
1 Verdacht	einzelne Auffälligkeit ohne Wirkung	Schichtleiter mit OT-Security

Stufe	Merkmal	Entscheidet
2 Angriff bestätigt	keine Gefahr für Menschen, Netz oder Versorgung	Kraftwerksleitung
3 Krise	Gefahr für Menschen, Netzstörung, Fernwärmeausfall	Geschäftsführung Stadtwerke, Krisenstab

4.5 Meldungen

Anlass	Stelle	Frist
erheblicher Sicherheitsvorfall (§ 5d Abs. 3 EnWG)	Meldestelle nach § 32 BSIG (BSI und BBK)	Erstmeldung spätestens 24 h, Meldung mit Bewertung spätestens 72 h nach Kenntnis, Abschlussmeldung entsprechend § 32 Abs. 2 BSIG
Ungeplante Leistungsänderung, Netzstörung	Netzbetreiber bzw. Übertragungsnetzbetreiber	sofort
Störfall, Gasaustritt, Brand	Feuerwehr, Immissionsschutzbehörde	sofort
Emissionsgrenzwert überschritten	Immissionsschutzbehörde	nach Genehmigung
Straftat	Polizei, Zentrale Ansprechstelle Cybercrime	zeitnah

Fristen vor Einführung rechtlich prüfen

4.6 Voraussetzungen und Übungen

- Alarm- und Telefonliste mit Netzbetreiber, Fernwärme, Feuerwehr
- Notbetriebshandbuch je Anlagenteil, Schwarzfall-Prozedur
- Offline-Sicherung von DCS, SPS und Schutzparametern, Wiederanlauf geübt
- Reaktionszeiten von Siemens Energy, Schutz- und Leittechniklieferanten im Vertrag
- Planspiel zweimal im Jahr, eines gemeinsam mit dem Netzbetreiber

5 Nächste Schritte

- Rollen besetzen, Telefonliste mit Netzbetreiber und Fernwärme.
- Playbooks mit Kraftwerksleitung, Schutztechnik und Siemens Energy abstimmen.
- Erstes Planspiel mit Szenario G2 gemeinsam mit dem Netzbetreiber.