BERICHT

Risikobewertung Cyberangriffe

Hartkäserei im Bestand, Hochrisiko-Szenarien

Auftraggeber	[Betreiber, Ort]
Projekt	Käserei, 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 die geplante Hartkäserei (Vorplanung Index C) wurden sechs Angriffe bewertet, die Verbraucher, Mitarbeiter und Betrieb am stärksten treffen: abgesenkte Kesselmilch-Erhitzung, Lauge im Produkt über den Ventilknoten, Manipulation der Ammoniak-Kälte, verstellte Füllmenge und Röntgenprüfung über die Fernwartung, ein fremder Laptop im Schaltschrank und Ransomware im Leitstand.

Ohne Härtung sind 4 Szenarien kritisch. Im Planungsstand Index C bleiben 1 kritisch und 5 mittel. Virtual-Wire-Firewalls vor Erhitzer, AS-100, Kälte und Röntgen senken die gefährlichsten Wege deutlich; mit allen Maßnahmen liegt kein Szenario über NIEDRIG.

GESAMTBEWERTUNG

Die gefährlichsten Wege führen über Fernwartung und Bedienplätze direkt in Steuerungen, an denen Lebensmittelsicherheit und Personenschutz hängen. Firewalls direkt vor diesen Steuerungen und hart verdrahtete Schutzfunktionen (Schreiber auf dem Umschaltventil, Mannlochschalter, Druckbegrenzer) halten auch dann, wenn ein Zugang missbraucht wird.

SZENARIEN NACH RISIKOKLASSE

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

2 Ausgangslage und Methode

Grundlage sind das R&I-Fließbild KAE-RI-001, das Netzwerk- und Automatisierungskonzept Index C und der HTML-Leitstand (Kaeserei_Leitstand_PurpleTeam.html) mit SPS-Simulation, Netzwerkverkehr, Segmentierung und den Angriffsszenarien K1 bis K6. 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 (Index C: Zonen mit FortiGate und SC646, H04, H07, H10); Mikrosegmentierung (Planungsstand plus Virtual-Wire-Firewalls); 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	Fernwartung nur über SINEMA RC und Jump-Host mit Freigabe je Sitzung; Schlüsselschalter mit Rückmeldung ins Leitsystem und automatischer Rückstellung	fehlt
H02	Eigene Benutzerverwaltung im OT, keine Konten der IT, Admin-Konten je Person	fehlt
H03	Zugriffsschutz der CPUs, PUT/GET aus, auch in den OEM-Steuerungen	fehlt
H04	Feste Grenzen in der SPS: KZE 72 °C, Sollgewicht, Reifelagertemperatur	umgesetzt
H05	Verriegelung Ventilknoten gegen Produkt in der SPS, Mannlochschalter in der CIP-Freigabe	fehlt
H06	Engineering nur von der Engineering-Station mit MFA und Wartungsschalter	fehlt
H07	Sicherheitsfunktionen autark: RSG45-Grenzkontakt hart auf FDV-302, Mannlochschalter, Not-Halt, unabhängige Temperaturüberwachung Reifelager mit GSM	umgesetzt
H08	Vier-Augen-Freigabe für Rezepte, Sollwerte und Grenzwerte im Leitsystem	fehlt
H09	Härtung und Anwendungs-Whitelisting der WinCC-Server und Bedienplätze	fehlt
H10	Offline-Sicherung mit octoplant, geübter Wiederanlauf	umgesetzt
H11	OT-Monitoring mit Anomalieerkennung am Spiegelport	fehlt
H12	Kontrolle von USB-Datenträgern und Service-Laptops	fehlt
H13	Port Security und NAC an den Feld-Switches	fehlt
H14	Reaktionsplan, Schulung, Übung mit Rückrufszenario	fehlt
SEG	Zonen mit FortiGate und SC646, Virtual-Wire-Firewalls	Zonen ja, VW fehlt

3 Ergebnisse

3.1 Übersicht

ID	Szenario	Ohne Härtung	Planungsstand	Mikrosegmentierung	Vollständig
K1	Kesselmilch-Erhitzung KZE-302 manipuliert	KRITISCH	MITTEL	NIEDRIG	NIEDRIG
K2	Ventilknoten und CIP: Lauge ins Produkt	KRITISCH	MITTEL	NIEDRIG	NIEDRIG
K3	Kälteanlage KA-802 mit Ammoniak manipuliert	KRITISCH	MITTEL	NIEDRIG	NIEDRIG
K4	Fernwartung der Würfellinie: Füllgewicht und Röntgen verstellt	KRITISCH	KRITISCH	MITTEL	NIEDRIG
K5	Fremder Laptop im Schaltschrank der Käsefertigung	MITTEL	MITTEL	NIEDRIG	NIEDRIG
K6	Ransomware legt den Leitstand lahm	HOCH	MITTEL	MITTEL	NIEDRIG

Tabelle 1: Risikoklasse je Szenario in vier Ständen

3.2 Szenarien im Detail

3.2.1 K1 Kesselmilch-Erhitzung KZE-302 manipuliert

Ohne Härtung	**KRITISCH** (A 5 × W 3 = 15)
Betroffene Systeme	Erhitzersteuerung KZE-302 (Z11), SINEMA RC (Z03)
Ort	Prozessraum: WT-302, HH-302, FDV-302, RSG45
Angriffsweg	1. Zugangsdaten des Erhitzer-Lieferanten erbeutet, Tunnel über SINEMA RC (T0859, T0822) 2. S7-Verbindung aus dem Fernwartungsnetz zur Erhitzersteuerung (T0886) 3. Umschaltgrenze und Sollwert auf 62 °C geschrieben (T0836) 4. Kesselmilch unter 72 °C im Vorlauf, Rückruf (T0880, T0828)
Folgen	Rohmilch mit 63 °C wird zu verzehrfertigem Käse; Listerien- oder EHEC-Gefahr für Verbraucher, Sperrung und Rückruf mehrerer Tage Produktion.
Planungsstand	**MITTEL** (A 3 × W 3 = 9); gelingt, Wirkung begrenzt durch H07
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 H01
Restrisiko	Ein Angreifer an der Engineering-Station im Wartungsfenster bleibt möglich; deshalb bleibt der unabhängige Schreiber mit Grenzkontakt Pflicht.
Schaden im Ernstfall	1,5 bis 5 Mio. €: Rückruf, Sperrung, Vertragsstrafe, dazu Personenschäden
Referenz	MITRE ATT&CK for ICS v20: T0859, T0822, T0886, T0836, T0880; IEC 62443-3-3 SR 1.13, SR 2.1, SR 5.1; VO (EG) 853/2004

3.2.2 K2 Ventilknoten und CIP: Lauge ins Produkt

Ohne Härtung	**KRITISCH** (A 5 × W 3 = 15)
Betroffene Systeme	Bedienplätze und AS-100 (Z04), Ventilknoten VK-301, CIP-601
Ort	Prozessraum, Käsefertigung
Angriffsweg	1. Bedienplatz übernommen, Projektpasswort vom Dienstleister-Laptop (T0859) 2. Engineering-Verbindung vom Bedienplatz zur AS-100 (T1692.001) 3. Wegeverriegelung im Ventilknoten aufgehoben (T0889, T0836) 4. Lauge im Produkt, CIP bei offenem Mannloch (T0880)
Folgen	Lauge in Kesselmilch und Käsefertiger; im schlimmeren Fall startet CIP in einen Behälter mit offenem Mannloch: Verbrühung und Verätzung eines Mitarbeiters.
Planungsstand	**MITTEL** (A 3 × W 3 = 9); gelingt, Wirkung begrenzt durch H07
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 H02
Restrisiko	Manipulation über die legitime Engineering-Station bleibt möglich; dagegen helfen Freigabeprozess, octoplant-Vergleich und Zugriffsschutz.
Schaden im Ernstfall	1 bis 5 Mio. €: Rückruf, Personenschaden
Referenz	MITRE ATT&CK for ICS v20: T0859, T1692.001, T0889, T0836, T0880; IEC 62443-3-3 SR 1.1, SR 2.1, SR 3.5, SR 5.1

3.2.3 K3 Kälteanlage KA-802 mit Ammoniak manipuliert

Ohne Härtung	**KRITISCH** (A 5 × W 3 = 15)
Betroffene Systeme	Kälteregler KA-802 (Z16), Jump-Host (Z03)
Ort	Technikanbau, Kälte
Angriffsweg	1. Zugang zum Jump-Host mit Daten des Kältelieferanten (T0859) 2. Modbus vom Jump-Host zum Kälteregler (T0886) 3. Hochdruckgrenze hochgesetzt, Verdichter gegen geschlossene Ventile (T0836, T0831) 4. Sicherheitsventil bläst NH3 ab (T0880, T0879)
Folgen	Druck steigt, das Sicherheitsventil bläst Ammoniak ins Freie; Gaswarnung, Evakuierung, Nachbarn betroffen. Ohne Kälte verderben Reifebestand und Rohmilch.
Planungsstand	**MITTEL** (A 3 × W 3 = 9); gelingt, Wirkung begrenzt durch H07
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 H01
Restrisiko	Der hart verdrahtete Sicherheitsdruckbegrenzer nach DIN EN 378 muss unabhängig bleiben; mit CO2 oder Propan sinkt die Gefahr deutlich.
Schaden im Ernstfall	0,5 bis 3 Mio. € plus Gefahr für Mitarbeiter und Anwohner
Referenz	MITRE ATT&CK for ICS v20: T0859, T0886, T0836, T0831, T0880; IEC 62443-3-3 SR 2.1, SR 5.1; TRAS 110

3.2.4 K4 Fernwartung der Würfellinie: Füllgewicht und Röntgen verstellt

Ohne Härtung	**KRITISCH** (A 4 × W 4 = 16)
Betroffene Systeme	Liniensteuerung, Kontrollwaage KK-484, Röntgen XR-487 (Z14), SINEMA RC
Ort	Südanbau, Würfellinie
Angriffsweg	1. Zugangsdaten des Linienlieferanten, Schlüsselschalter vergessen (T0859, T0822) 2. OPC UA aus dem Fernwartungsnetz zur Linie (T0886) 3. Sollgewicht 199 g in der Liniensteuerung (T0836) 4. Röntgen-Ausschleusung aus (T0836) 5. Ware mit Untergewicht und Fremdkörpern beim Handel (T0828)
Folgen	Unterfüllte Packungen und Fremdkörper gehen an den Handel: Verletzungsgefahr, Bußgeld nach Fertigpackungsverordnung, Rückruf, Auslistung.
Planungsstand	**KRITISCH** (A 4 × W 4 = 16); gelingt
Mit Mikrosegmentierung	**MITTEL** (A 4 × W 2 = 8); gestoppt in Schritt 4 durch Mikrosegmentierung
Vollständig	**NIEDRIG** (A 3 × W 1 = 3); gestoppt in Schritt 1 durch H01
Restrisiko	Der Lieferant braucht Fernzugriff auf die Linie. Täglicher Test mit Prüfkörpern bleibt Pflicht; er deckt auch Fehler ohne Angriff auf.
Schaden im Ernstfall	0,5 bis 2 Mio. € plus Verletzungsgefahr beim Verbraucher
Referenz	MITRE ATT&CK for ICS v20: T0859, T0822, T0886, T0836, T0828; IEC 62443-3-3 SR 1.13, SR 2.1, SR 5.1; Fertigpackungsverordnung

3.2.5 K5 Fremder Laptop im Schaltschrank der Käsefertigung

Ohne Härtung	**MITTEL** (A 3 × W 3 = 9)
Betroffene Systeme	Feld-Switch SW-F5, ET 200SP Käsefertigung (Z08)
Ort	Käsefertigung
Angriffsweg	1. Infizierter Laptop am Feld-Switch SW-F5 (T0847) 2. PROFINET DCP zur ET 200SP der Käsefertigung (T0846, T0806) 3. Gerätename geändert, Station fällt aus (T0816) 4. Charge verloren, Stillstand (T0828)
Folgen	Käsefertiger stehen mitten in der Charge, rund 10.000 l Milch verloren, Stillstand bis zur Neuinbetriebnahme.
Planungsstand	**MITTEL** (A 2 × W 3 = 6); gelingt, Wirkung begrenzt durch H10
Mit Mikrosegmentierung	**NIEDRIG** (A 2 × W 1 = 2); gestoppt in Schritt 2 durch Mikrosegmentierung
Vollständig	**NIEDRIG** (A 2 × W 1 = 2); gestoppt in Schritt 1 durch H12, H13
Restrisiko	Physischer Zugang zu Schaltschränken bleibt; abschließbare Schränke und Laptopkontrolle ergänzen die Netzmaßnahmen.
Schaden im Ernstfall	20.000 bis 100.000 € je Charge plus Stillstand
Referenz	MITRE ATT&CK for ICS v20: T0847, T0846, T0806, T0816, T0828; IEC 62443-3-3 SR 1.2, SR 2.3, SR 5.1

3.2.6 K6 Ransomware legt den Leitstand lahm

Ohne Härtung	**HOCH** (A 4 × W 3 = 12)
Betroffene Systeme	Jump-Host (Z03), WinCC Unified (Z04), Büro-IT (Z01)
Ort	OT-Serverraum, Leitstand
Angriffsweg	1. Admin-Daten für den Jump-Host aus der IT gestohlen (T0859) 2. RDP vom Jump-Host zum WinCC-Server (T0886) 3. WinCC-Server verschlüsselt (T0809) 4. Leitstand blind, Produktion steht (T0826, T0815)
Folgen	Leitstand ohne Bilder, Produktion mit Handbetrieb oder Stillstand, Chargenprotokolle fehlen, Wiederanlauf über Tage.
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 und bleibt erlaubt; Konten, Whitelisting und Sicherung begrenzen den Schaden.
Schaden im Ernstfall	0,2 bis 1 Mio. €: Stillstand, Wiederherstellung
Referenz	MITRE ATT&CK for ICS v20: T0859, T0886, T0809, T0826, 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	Fernwartung nur über SINEMA RC und Jump-Host mit Freigabe je Sitzung; Schlüsselschalter mit Rückmeldung ins Leitsystem und automatischer Rückstellung	K1, K3, K4	**Hoch**
H02	Eigene Benutzerverwaltung im OT, keine Konten der IT, Admin-Konten je Person	K2, K6	**Mittel**
H03	Zugriffsschutz der CPUs, PUT/GET aus, auch in den OEM-Steuerungen	K1, K2	**Hoch**
H04	Feste Grenzen in der SPS: KZE 72 °C, Sollgewicht, Reifelagertemperatur	alle	umgesetzt
H05	Verriegelung Ventilknoten gegen Produkt in der SPS, Mannlochschalter in der CIP-Freigabe	K2	**Hoch**
H06	Engineering nur von der Engineering-Station mit MFA und Wartungsschalter	K2	**Mittel**
H07	Sicherheitsfunktionen autark: RSG45-Grenzkontakt hart auf FDV-302, Mannlochschalter, Not-Halt, unabhängige Temperaturüberwachung Reifelager mit GSM	K1, K2, K3	umgesetzt
H08	Vier-Augen-Freigabe für Rezepte, Sollwerte und Grenzwerte im Leitsystem	K4	**Hoch**
H09	Härtung und Anwendungs-Whitelisting der WinCC-Server und Bedienplätze	K6	**Mittel**
H10	Offline-Sicherung mit octoplant, geübter Wiederanlauf	K5, K6	umgesetzt
H11	OT-Monitoring mit Anomalieerkennung am Spiegelport	alle	**Mittel**
H12	Kontrolle von USB-Datenträgern und Service-Laptops	K5	**Mittel**
H13	Port Security und NAC an den Feld-Switches	K5	**Hoch**
H14	Reaktionsplan, Schulung, Übung mit Rückrufszenario	alle	**Mittel**
SEG	Virtual-Wire-Firewalls vor Erhitzer, AS-100, Kälte, Röntgen und AS-900	K1 bis K5	**Hoch**

Tabelle 2: Maßnahmen und Priorität im Planungsstand

Ein einziger Rückruf wegen unzureichender Erhitzung oder Fremdkörpern (K1, K4) oder ein Ammoniakaustritt (K3) kann Menschen gefährden und den Betrieb in seiner Existenz treffen; die Maßnahmen mit Priorität Hoch sind dagegen überschaubar.

4.1 Rechtlicher Rahmen

- **Lebensmittelrecht:** Erhitzung und Fremdkörperprüfung sind kritische Kontrollpunkte nach HACCP (VO (EG) 852/2004), Hygiene für Lebensmittel tierischen Ursprungs nach VO (EG) 853/2004, Rückverfolgbarkeit und Rücknahme nach VO (EG) 178/2002 Art. 18 und 19.

- **Fertigpackungsverordnung:** Nennfüllmenge 200 g, Zielmittelwert 205 g; Untergewicht durch Manipulation ist ein Verstoß des Herstellers.
- **Arbeitsschutz und Anlagensicherheit:** Ammoniak nach BetrSichV, DIN EN 378 und TRAS 110; Reinigung mit Lauge und Säure nach GefStoffV. Die Wirkung von Cyberangriffen gehört in die Gefährdungsbeurteilung.
- **NIS2:** Lebensmittel ist ein Sektor nach Anlage 2 BSIG; mit 5 Beschäftigten liegt die Käserei voraussichtlich unter den Schwellen (50 Beschäftigte oder 10 Mio. €). Für den Betreiber zu prüfen.
- **Maschinenverordnung (EU) 2023/1230:** ab 20.01.2027 für neue Maschinen, Anhang III Nr. 1.1.9 Schutz gegen Korrumpierung.

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

- Virtual-Wire-Firewalls vor Erhitzer, AS-100, Kälte und Röntgen in die Lastenhefte (L-04 bis L-07).
- Fernwartung je Sitzung freigeben, Schlüsselschalter mit Rückmeldung und Rückstellung (H01).
- PUT/GET in allen OEM-Steuerungen aus, Zugriffsschutz (H03); Erhitzer-Firmware auf V3.1.
- Reaktionsplan mit Rückrufszenario üben.