AI Use Case One-Pager

Autor:	Christos Kapodistrias
Kategorie:	One-Pager
Kunde:	Doppelmayr Holding SE
Datum:	06.02.2026
Version:	1.0
Klassifikation:	**CUSTOMER OPEN ANALYSIS**

Inhaltsverzeichnis

AI Use Case One-Pager

Cybersecurity fuer SCADA und OT-Netzwerke

Kunde: Doppelmayr Holding SE, Wolfurt **Datum:** 6. Februar 2026 **Use Case Prioritaet:** Rang 3 | Score: 4,30/5,00 **Klassifikation:** Regulatorische Pflicht + Safety

Problemstellung

Die IT-Landschaft-Analyse identifiziert Cybersecurity als die groesste Luecke bei Doppelmayr: Reifegrad 2 von 5. Mit der zunehmenden Vernetzung durch AURO (KI-gestuetzter autonomer Betrieb), Doppelmayr Connect (Seilbahnsteuerung mit atvise SCADA), Remote Monitoring und IoT-Sensorik waechst die Angriffsflaeche erheblich. Gleichzeitig verschaerfen die NIS2-Richtlinie und der EU Cyber Resilience Act die regulatorischen Anforderungen fuer Betreiber kritischer Infrastruktur.

Zentrale Herausforderungen:

- **Reifegrad 2/5:** Keine oeffentlich kommunizierte OT-Security-Strategie; wenig Transparenz ueber Schutzstatus
- **NIS2-Pflicht:** Seilbahnen als oeffentliches Verkehrsmittel (urban) werden als potenzielle kritische Infrastruktur eingestuft - Compliance ab 2025/26 verpflichtend
- **Cyber Resilience Act:** Betrifft vernetzte Produkte wie Doppelmayr Connect und AURO direkt ab 2027
- **Wachsende Angriffsflaeche:** AURO-Kameras, Connect-Tablet-App (WLAN), Remote Monitoring, IFS Cloud - jede neue Schnittstelle ist ein potenzielles Einfallstor
- **Reputationsrisiko:** Ein Cyberangriff auf eine urbane Seilbahn (La Paz: 160.000 Passagiere/Tag, Mexiko-Stadt: 100.000+) waere katastrophal
- **IT/OT-Konvergenz:** Profibus, EtherCAT und SCADA-Netzwerke waren historisch isoliert - die Vernetzung erzeugt neue Risiken

Vorgeschlagene Loesung

Umfassendes OT-Cybersecurity-Konzept mit A1 SOC

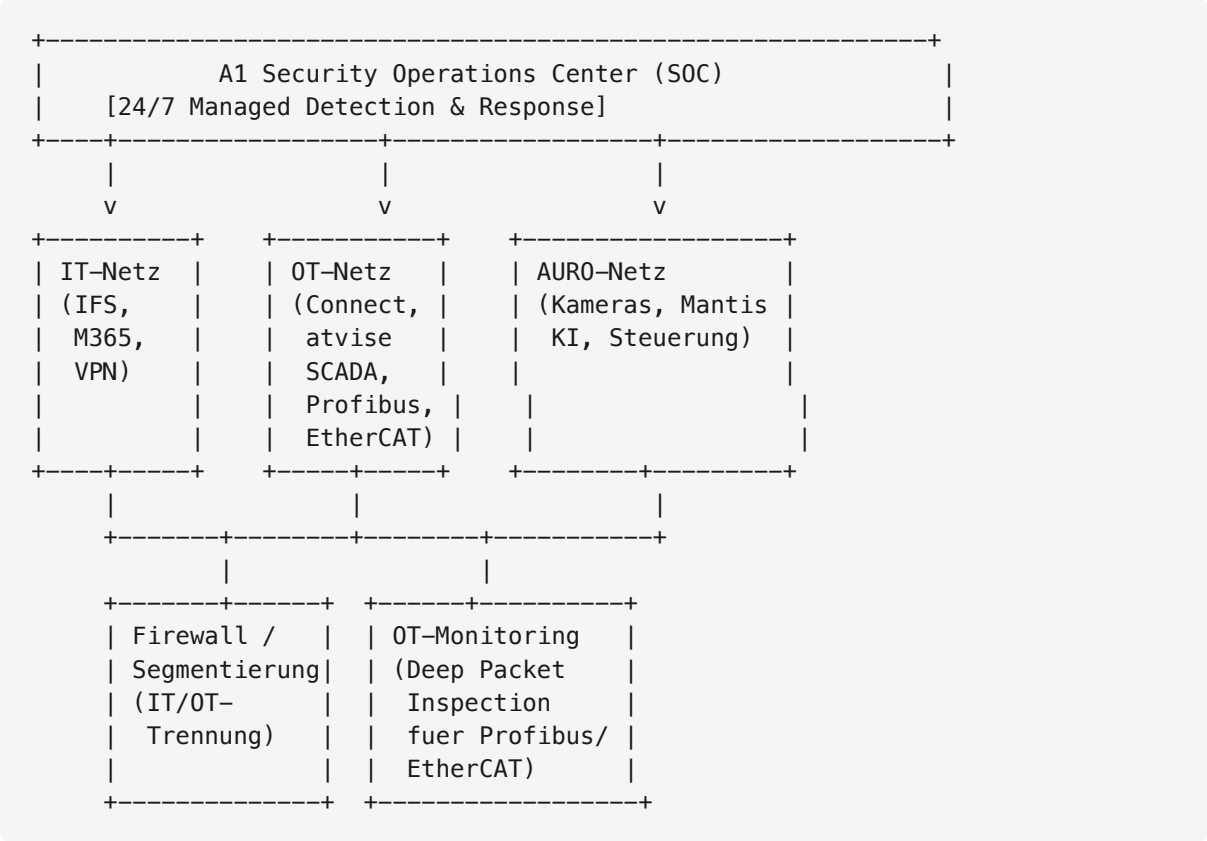
Implementierung eines mehrschichtigen Cybersecurity-Frameworks speziell fuer Doppelmayrs operative Technologie-Netzwerke (OT), bestehend aus Assessment, Haertung, Monitoring und Incident Response.

Kernfunktionalitaeten:

- **OT-Security-Assessment:** Schwachstellenanalyse fuer Connect, atvise SCADA, AURO und Industriebusse
- **Netzwerksegmentierung:** IT/OT-Trennung fuer Connect, AURO und Produktionsnetzwerke
- **24/7 SOC-Monitoring:** Echtzeit-Anomalieerkennung im SCADA-Netzwerk durch A1 Security Operations Center
- **Incident Response:** Notfall-Reaktionsplaene speziell fuer Seilbahnbetreiber

- **NIS2-Advisory:** Gap-Analyse und Compliance-Fahrplan fuer NIS2 und Cyber Resilience Act
- **Adversarial AI Protection:** Schutz der AURO-KI-Systeme gegen Manipulationsangriffe

Architektur:



Erwarteter Nutzen

Quantitative Benefits:

Kennzahl	Ohne OT-Security	Mit A1 OT-Security	Verbesserung
Cybersecurity-Reifegrad	2/5	4/5 (Ziel nach 12 Monaten)	**+2 Stufen**
NIS2-Compliance	0 %	100 %	**Regulatorische Pflicht erfuellt**
Erkennungszeit Cyberangriff	Unbekannt (Tage/Wochen)	< 15 Minuten (SOC)	**> 99 % schneller**
Reaktionszeit Incident	Ad hoc	< 1 Stunde (Incident Response)	**Strukturiert**
Schwachstellen identifiziert	Unbekannt	100 % (nach Assessment)	**Vollstaendige Transparenz**

Qualitative Benefits:

- **Regulatorische Compliance:** NIS2 ab 2025/26 und Cyber Resilience Act ab 2027 - ohne OT-Security drohen Bussgelder
- **Reputationsschutz:** Ein Cyberangriff auf urbane Seilbahnen waere eine globale Nachricht - Praevention ist unverzichtbar
- **Verkaufsargument:** Zertifizierte OT-Security als Differenzierung bei staedtischen Ausschreibungen (Mexiko-Stadt, Lima, Naucalpan)
- **Wettbewerbsvorteil:** HTI Group (Leitner/POMA) hat ebenfalls keine oeffentlich kommunizierte OT-Security - Doppelmayr kann hier fuehren
- **AURO-Absicherung:** Schutz des KI-Systems vor Adversarial Attacks und Datenmanipulation

---

Technische Anforderungen

Infrastruktur:

Komponente	Anforderung	A1-Produkt
Security Operations Center	24/7 Managed Detection & Response fuer OT	A1 SOC
OT-Network-Monitoring	Deep Packet Inspection fuer Profibus/EtherCAT	A1 OT Security Monitoring
Vulnerability Assessment	Schwachstellenscan fuer Connect, SCADA, AURO	A1 Vulnerability Assessment
Penetrationstest	Seilbahnsteuerungsspezifische Tests	A1 Pentesting (OT-Spezialisierung)
NIS2-Beratung	Gap-Analyse und Compliance-Fahrplan	A1 NIS2 Advisory
Incident Response	Notfall-Reaktionsplan und -team	A1 Incident Response Team

Referenzsysteme bei Doppelmayr:

- Doppelmayr Connect (Steuerungssystem, entwickelt von Frey AG Stans)
- atvise SCADA (Bachmann electronic, Feldkirch - regionaler Nachbar in Vorarlberg)
- AURO / Mantis Ropeway Technologies (KI-basierte Bilderkennung)
- Industriebus-Netzwerke: Profibus, EtherCAT (Sensor -> SPS -> Connect)
- Mobile Tablet-App fuer Connect-Fernsteuerung (WLAN-basiert)
- Intercom-Systeme zwischen Stationen

Regulatorische Anforderungen:

Regulierung	Frist	Relevanz fuer Doppelmayr
NIS2-Richtlinie	2025/26	Seilbahnen als potenzielle kritische Infrastruktur (urbaner OEPNV)
EU Cyber Resilience Act	2027	Vernetzte Produkte (Connect, AURO) direkt betroffen
EU Machinery Regulation 2023/1230	2027	Neue Anforderungen an KI und Cybersecurity fuer Maschinen
DSGVO	Laufend	KI-basierte Kamerasysteme (AURO) - Datenschutz bei Bilderkennung

ROI-Highlights

Investitionskosten:

Phase	Zeitraum	Kosten
OT-Security-Assessment + NIS2-Gap-Analyse	4-6 Wochen	EUR 30.000 - 60.000
Netzwerksegmentierung und Haertung	3 Monate	EUR 80.000 - 150.000
SOC-Anbindung und Onboarding	2-3 Monate	EUR 50.000 - 80.000 (Setup)
Laufende SOC-Kosten/ Jahr		**EUR 150.000 - 250.000**
Incident Response Retainer/Jahr		**EUR 30.000 - 50.000**

Return on Investment:

Nutzenkategorie	Berechnung	Jaehrlicher Wert
Vermiedene NIS2-Bussgelder	Bis zu 2 % des Jahresumsatzes (EUR 1.197 Mio.)	**EUR 23.940.000** (Maximalrisiko)
Vermiedene Betriebsunterbrechung	1 Vorfall/5 Jahre x EUR 5 Mio. Schaden	**EUR 1.000.000/Jahr**
Vermiedene Reputationsschaeden	Bewertung: EUR 10+ Mio. bei urbanem Vorfall	**Unschaetzbar**
Wettbewerbsvorteil bei Ausschreibungen	2 urbane Projekte/Jahr x EUR 50.000 Aufpreispotenzial	**EUR 100.000**
Gesamt (konservativ, ohne Bussgelder)		**EUR 1.100.000**

ROI-Kennzahlen:

- **Payback Assessment:** Sofort (regulatorische Pflicht - keine ROI-Frage, sondern Compliance-Frage)

- **ROI SOC-Betrieb:** 250-400 % (basierend auf vermiedenen Vorfallskosten)
- **Compliance-Deadline:** NIS2 ab 2025/26 - Handlung ist zeitkritisch

---

Implementierungs-Timeline

```
Woche 1-2:    Kick-off und Scope-Definition
              +-- Identifikation kritischer Assets (Connect, SCADA, AURO)
              +-- Abstimmung mit Frey AG Stans und atvise/Bachmann
              +-- Zugangsregelungen und NDAs

Woche 3-6:    OT-Security-Assessment
              +-- Netzwerkarchitektur-Analyse (IT/OT-Grenzen)
              +-- Schwachstellenscan fuer Connect-Komponenten
              +-- Penetrationstest an einer Referenzanlage
              +-- NIS2-Gap-Analyse und Compliance-Bewertung

Woche 7-8:    Ergebnispraesentation und Massnahmenplan
              +-- Schwachstellenbericht mit Priorisierung
              +-- NIS2-Compliance-Fahrplan
              +-- Empfehlungen fuer Sofortmassnahmen (Quick Hardening)
              +-- SOC-Anbindungskonzept

Monat 3-6:    Haertung und SOC-Anbindung
              +-- IT/OT-Segmentierung implementieren
              +-- A1 SOC-Anbindung fuer Connect/AURO
              +-- Incident-Response-Plan erstellen und testen
              +-- Mobile App Security (Tablet-Fernsteuerung)

Monat 6-12:   Laufender SOC-Betrieb und Erweiterung
              +-- 24/7-Monitoring aktiv
              +-- Vierteljaeherliche Vulnerability Scans
              +-- AURO Adversarial AI Protection
              +-- Schulung Doppelmayr-Mitarbeitende
```

Empfehlung

Cybersecurity fuer SCADA/OT ist keine optionale Investition - es ist eine regulatorische Pflicht und eine Safety-Anforderung: - **Groesste identifizierte IT-Luecke** (Reifegrad 2 von 5) bei einem Unternehmen, das zunehmend vernetzte Systeme betreibt - **NIS2-Compliance ab 2025/26 verpflichtend** - regulatorischer Kauftreiber mit klarer Deadline - **Cyber Resilience Act** betrifft Connect und AURO direkt ab 2027 - **Reputationsrisiko:** Urbane Seilbahnen mit 100.000+ Passagieren/Tag sind hochsensible Infrastruktur - **A1 SOC mit OT-Expertise** ist ein Differenzierungsmerkmal gegenueber generischen IT-Security-Anbietern

Naechster Schritt: OT-Security-Assessment als Erstengagement mit Arno Inauen (GF Technik) und Gerhard Gassner (GF/IT) beauftragen. Koordination mit Frey AG Stans fuer Zugang zu Connect- und SCADA-Systemen.