PROSE

Shaping tomorrow's mobility

Safety trifft Security

Effiziente Cybersecurity im Lebenszyklus vernetzter Schienenfahrzeuge

Patrick Grossmann

10. November 2026



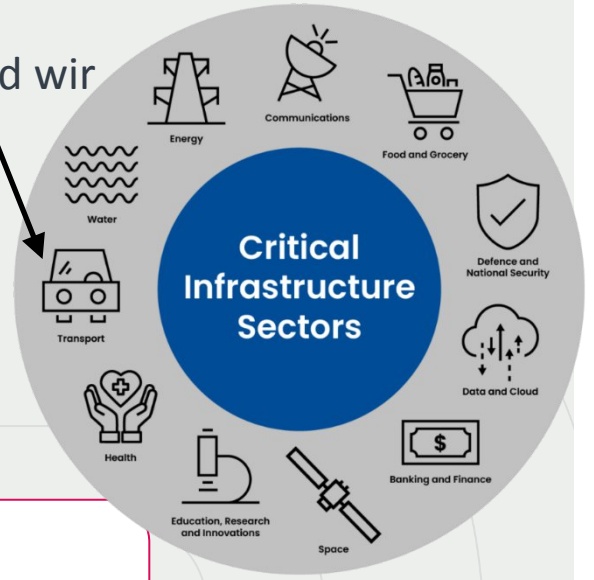
Worüber werden wir reden?

1. Unsere Bahnwelt im Jahr 2026
2. Praxis Beispiel Entwicklung – NEWAG E4MSU Lokomotive Fahrzeugsteuerung
3. Praxis Beispiel Im Betrieb – Türsteuerung / Zugbeeinflussung in Australien
4. Ableiten eines **pragmatischen** und **effizienten** Ansatzes aus diesen Erfahrungen
5. Und jetzt ist Feierabend ☺

Unsere Bahnwelt im Jahr 2026

Ein Zug ist eine vernetzte Plattform

Das sind wir



Modernes Fahrzeug

TCMS · Türen · ATP

Wartung

Servicegeräte · Fernzugriff

Umfeld

Cloud · Lieferanten · IT

Weitere Fahrzeuge

Signalling

ATP, Interlocking, TMS etc.

Mehr Vernetzung = mehr potenzielle Fehler- und Angriffspfade

Unsere Bahnwelt im Jahr 2026

Safety und Security wirken auf dieselben Systeme



SAFETY

Unbeabsichtigte Fehler

Gefährliche Zustände verhindern

SECURITY

Manipulation / unautorisierter Zugriff

Integrität und Verfügbarkeit schützen

Gemeinsame Objekte: Hardware · Software · Parameter · Zugänge · Konfigurationen

Unsere Bahnwelt im Jahr 2026

Wichtige Regularien, Standards und Normen - Was verlangt der Rahmen?

CRA	**Produktverantwortung**	Schwachstellen, Updates, Dokumentation
NIS 2	**Betreiberverantwortung**	Technische und organisatorische Risikomassnahmen
EN 50126	**RAM, Safety**	Bekannte Bahnnorm zum Thema RAMS
IEC 62443	**OT-Grundlage**	Zone, Risiko, technische Anforderungen
CLC/TS 50701	**Bahnanwendung**	Security in den RAMS-Lebenszyklus integrieren

Praxis Entwicklung NEWAG E4MSU Lokomotive

Fahrzeugsteuerung



Sechs-Länder-Lokomotive: Safety, Security und Zulassung zusammen denken

Als erste komplett in Polen entwickelte Lokomotive erreicht sie 240 km/h und bricht damit etablierte Marktmonopole -> Geopolitik!

1 Systemgrenze

Assets und Verantwortungen definieren

→

2 Risikoanalyse

High-Level → Detail

→

3 Anforderungen

Gefahr → Massnahme

→

4 Nachweise

V&V → Freigabe

Zauberwort: Neben einem Safety Case gibt es jetzt auch einen Security Case

Den Security Case als integrierter, nachvollziehbarer Nachweis – kein zweiter Engineering-Prozess

Praxis Entwicklung NEWAG E4MSU Lokomotive

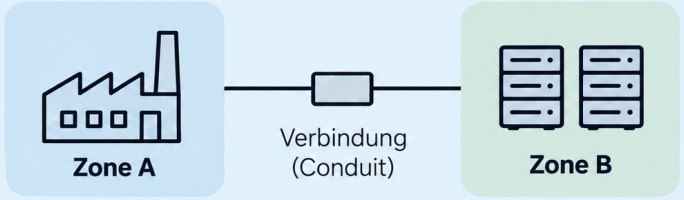
Von Hoher Flugebene zu den Details

High-Level-Risikoanalyse nach IEC 62443

Wir definieren den Gesamtüberblick und priorisieren die Risiken.

High-Level-Risikoanalyse

Gesamtüberblick und Priorisierung



- Betrachtet das gesamte System auf Zonen und Verbindungen
- Bewertet Risiken auf hoher Ebene
- Priorisiert, wo vertiefte Analysen nötig sind
- Legt den Ziel-Sicherheitslevel (SL) pro Zone und Verbindung fest

Grenzen ausarbeiten

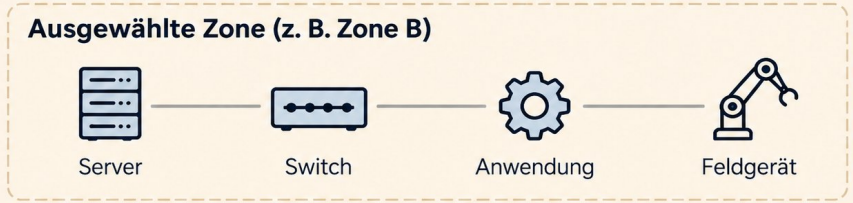


Detail-Risikoanalyse nach IEC 62443

Vertiefte Analyse der ausgewählten Bereiche.

Detail-Risikoanalyse

Vertiefte Analyse der ausgewählten Bereiche



- Betrachtet einzelne Assets und Komponenten innerhalb der ausgewählten Zonen/Verbindungen
- Analysiert konkrete Bedrohungen und Schwachstellen
- Bewertet Risiken detailliert
- Definiert und bewertet spezifische Schutzmassnahmen

Praxis Entwicklung NEWAG E4MSU Lokomotive

Aus der Gefahrenanalyse – Hohe Flugebene

Erste Einschätzung – Cyber-Bedrohungen

Asset / Funktion	Bedrohungen	Potenzielle Auswirkungen	Beobachtungen / Lücken
CPU 835 (TCMS Core, SIL 2)	Fernübernahme, Malware-Einschleusung, Konfigurations-manipulation	Katastrophale Auswirkungen, wenn Sicherheitsfunktionen betroffen sind	Bewertet als SIL 2, hängt jedoch von der Isolation der BI-Komponenten und Schnittstellen ab
BI-Funktionalitäten (CPU 833)	Datenexfiltration, Spoofing, laterale Bewegung	Manipulation von operativen Daten, Fehlalarme	Wenn nicht getrennt, kann dies die SIL 2-Core-Funktionalität gefährden

Erste Einschätzung – Physische Bedrohungen

Asset / Funktion	Bedrohungen	Potenzielle Auswirkungen	Beobachtungen / Lücken
TCMS CPU 833/835	Sabotage, unbefugter Konsolenzugriff	Vollständige Systemkompromittierung oder Ausfall der Steuerung	Chassis-Eindringungsschutz, BIOS-Schutz, verschlossene Schränke

Praxis Entwicklung NEWAG E4MSU Lokomotive

Aus der Gefahrenanalyse – Detail Level

- Wichtig sind nicht alle Details, sondern dass Safety ein zentraler Bestandteil ist (Orange)
- Analyse ist auf Englisch, da EU weites Feld

								Initial Risk Classification Before hazard mitigation				Preventative Actions			Residual Risk Classification After hazard mitigation				Management		
Hazard ID	Date raised	Phase	Asset	Sub-System / Component / Function	Threat Scenario	Threat Actor / Description of Risk	Vulnerability / Impact Description	Likelihood Category		Severity Category		Risk Acceptance Category	Polarion ID	Mitigation / Control Measure	Safety related	Likelihood Category		Severity Category		Risk Acceptance Category	Entity in Charge	Remarks	Status
SEC-1009	12.05.2025	Operational	TCMS BI & TCMS SIL	Diagnostic Ports	Debug ports exposed inside cab without locking	Insider or attacker with brief access	Unrestricted physical access to debug ports	Easy	C	Catastrophic	1	Intolerable	E4MSUa_-111183	Ethernet diagnostics port disabled in switch configuration.	No, open ports could not be used to manipulate safety related functions	Very hard	F	Catastrophic	1	Tolerable	NEWAG	Mitigations mentioned in column "Mitigation/Control Measure" must fail in conjunction with each other to result in a successful attack.	In progress
SEC-1009													E4MSUa_-111181	Entry is permitted only to authorized personnel, typically via a key-based mechanism.							NEWAG		
SEC-1009													E4MSUa_-111216	Regular inspection physical locks, sealings during maintenance.							NEWAG		

Okay – aber was wenn Entwicklung fertig?

Praxis Beispiel Betrieb

Der Fall: Nach einem “SW-Update” ist plötzlich eine Tür der Sydney Metro während der Fahrt aufgegangen

Security-Ziel

Schwachstelle schliessen

Zertifikate / Kommunikation aktualisieren

Unbefugte Zugriffe verhindern

Safety-Auswirkung?

Timing und Telegrammfolgen

Watchdogs und Fehlerreaktionen

Meldung «Türen verriegelt»

Potentieller Hardware Einfluss – Rewiring missbraucht – Türfehler im Betrieb

Delta-Nachweis → Regressionstest → Vier-Augen-Freigabe → getesteter Rollback

Praxis Beispiel Betrieb

Beispiel – Sydney Trains ATP / ETCS OBU Update, Australien



Angriffspfad

Servicekonto / Updatepfad / Schlüssel

→

Manipulation

Software oder Parameter verändert

→

Wirkung

Bremskurven / Geschwindigkeit / Betriebsart

Bspw L2 -> L1 via L0

Zugänge sichern · Rollen trennen · Integrität prüfen · Rückfall definieren



Ableiten eines pragmatischen und effizienten Ansatzes aus diesen Erfahrungen

Ablauf

01	**Abgrenzen**	System, Assets, Datenflüsse, Servicezugänge
02	**Bewerten**	Zonen, Conduits, Risiken inkl. Safety-Folgen
03	**Umsetzen**	Requirements, Zuständigkeiten, Lieferverträge
04	**Nachweisen**	Gemeinsame V&V, Restrisiko, Betrieb & Updates

Ableiten eines pragmatischen und effizienten Ansatzes aus diesen Erfahrungen

Die wirksamsten Massnahmen sind oft erstaunlich einfach

Software-Baselines

Inventar, Versionen, Hashes

Wartungszugänge

Schloss, Siegel, Portliste

Freigegebene Servicegeräte

Geräte-ID, Rollen, Hardening

Kontrollierte Updates

Signatur, Vier-Augen-Prinzip, Rollback

Incident-Meldeweg

Schwellenwerte und Zuständigkeit

Und nein deswegen gilt nicht:

Schnell umsetzbar ≠ ohne Nachweis

Ableiten eines pragmatischen und effizienten Ansatzes aus diesen Erfahrungen

Die Nachweiskette



Diese Kette muss auch bei jeder Änderung als Delta-Nachweis funktionieren. Das wars.

Ableiten eines pragmatischen und effizienten Ansatzes aus diesen Erfahrungen

Safety + Security + Zulassung: eine Engineering-Logik

Risikobasiert denken.

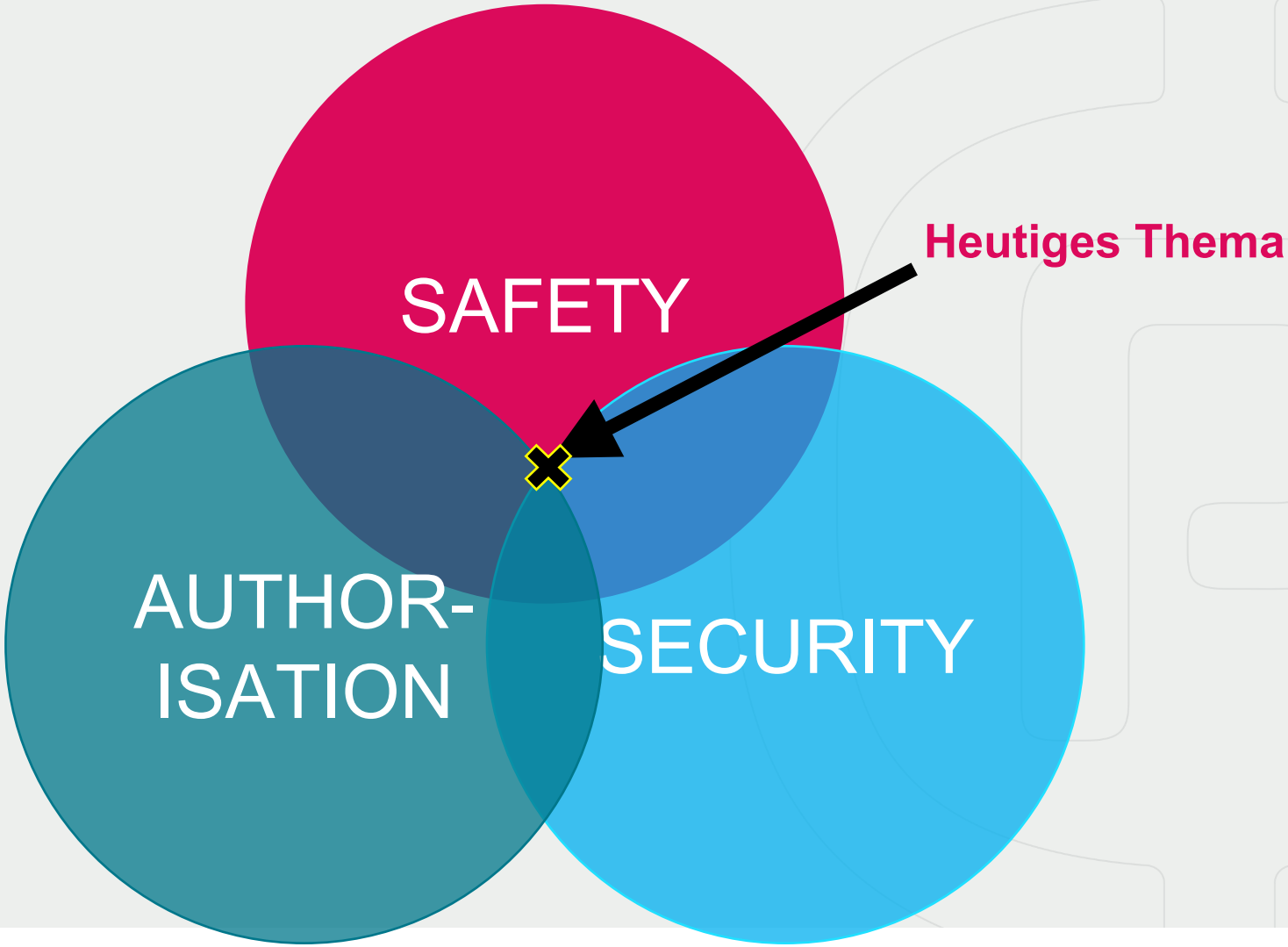
Änderungen gemeinsam (Kein Silo Denken) bewerten.

Wirksamkeit nachweisen.

Pragmatische Cybersecurity beginnt an der Systemgrenze – nicht beim Tool.

Ableiten eines pragmatischen und effizienten Ansatzes aus diesen Erfahrungen

Keine Zulassung ohne Safety, keine Safety ohne Security



Ausblick

Appell – Nicht auf Regulierung warten, sondern selbst handeln!

- Positiv: Man arbeitet an einer Vereinheitlichung - Der **IEC 63452.** Jedoch hinkt die Politik hinterher.

Daher Selbst handeln!

- **Silodenken überwinden:** Ohne gemeinsames Verständnis entstehen gefährliche Lücken.
- **Risiken kennen statt Sicherheit annehmen:** Wer seine Risiken nicht systematisch bewertet, kann weder sinnvoll priorisieren noch gezielt schützen.
- **Vorfälle erkennen und Reaktion trainieren:** Konzepte auf Papier reichen nicht. Wer Erkennung und Reaktion nicht regelmässig übt, wird im Ernstfall scheitern.
- **Verantwortung übernehmen statt auf Standards warten:** Wirksame Prävention beginnt im eigenen Unternehmen – und ist bereits heute für jeden umsetzbar.

PROSE

Shaping tomorrow’s mobility

Danke

Patrick Grossmann

Patrick.grossmann@prose.one

10.11.2026