Enotrac

Webinar

Cyber Security im Bahnbereich

Richtlinien, regulatorische Anforderungen und Einführung des Konzepts für Cybersicherheit

Vortragende

- **Jens Schulze, Moderation**
  Mitglied der Geschäftsleitung, Bereichsleiter RAMSS

- **Michael Aebischer, Referent**
  OT Sicherheit RAMSS

- **Juan Carlos Lopez Ruggiero, Referent**
  Head of Cyber Security

- **Prof. Dr. Ernst Zollinger, Referent**
  Senior Berater RAMSS

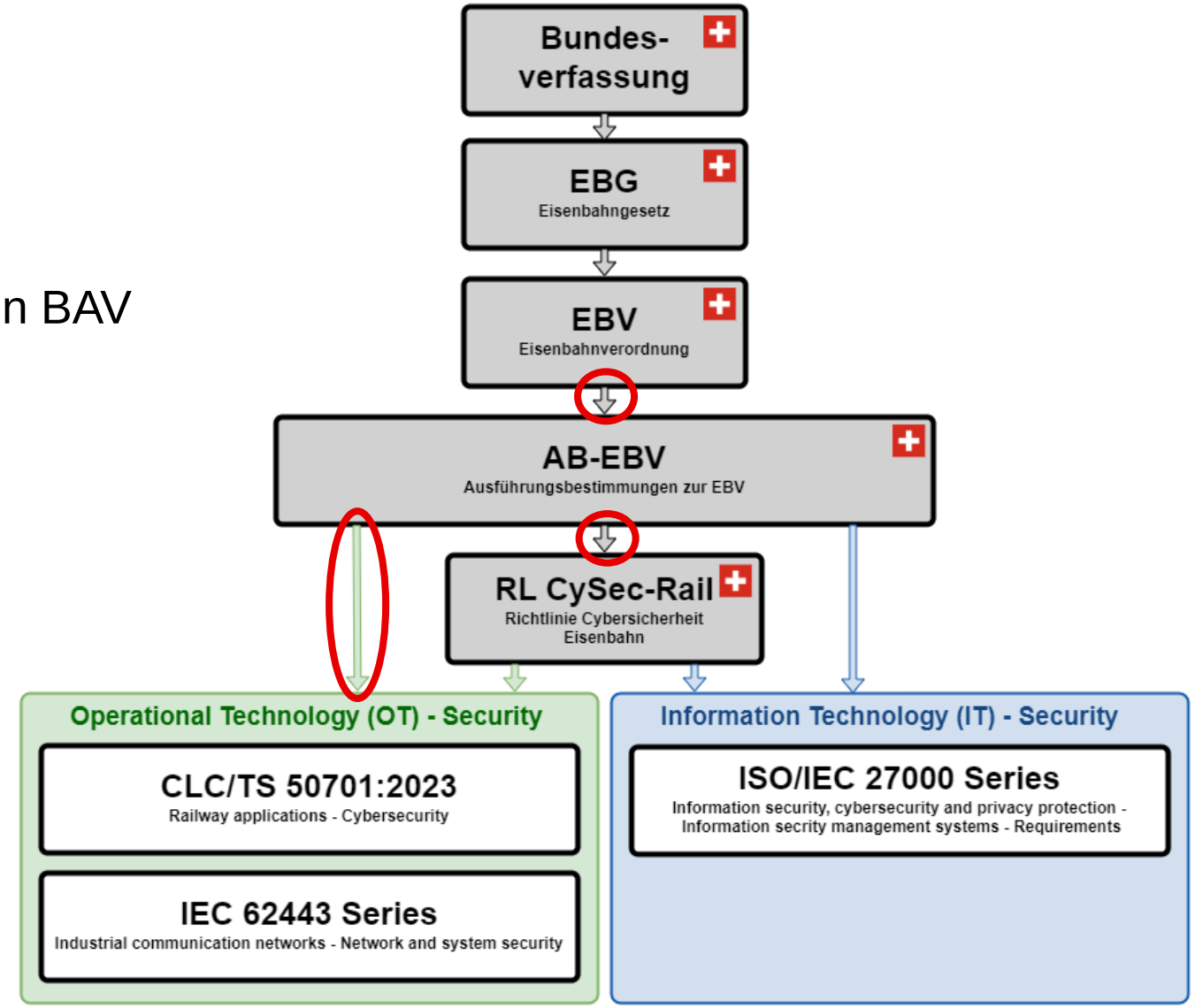
Agenda

- Regulatorische Anforderungen und Normen
- Mögliche Folgen bei Nichteinhaltung
- Cybersicherheit (ISMS)
- OT-Security
- Fragen und Antworten (Q&A)
- Zusammenfassung und Schlusswort

Regulatorische Ausgangslage CH

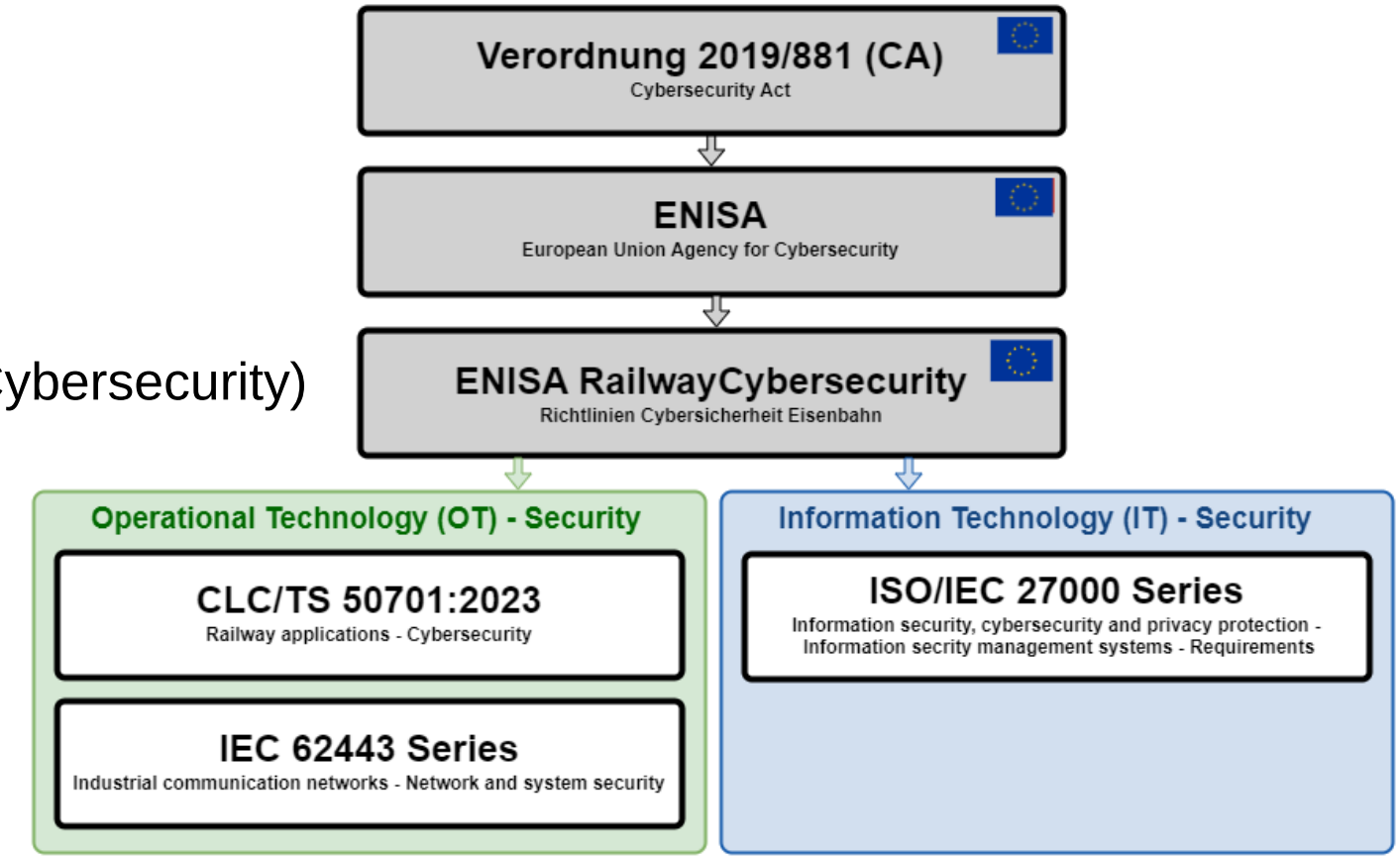
Neue Anforderungen CH

- Änderungen EBV und AB-EBV im 2024
- Richtlinie Cybersicherheit Eisenbahn von BAV
  (RL Cysec-Rail in Kraft ab 01.07.24)



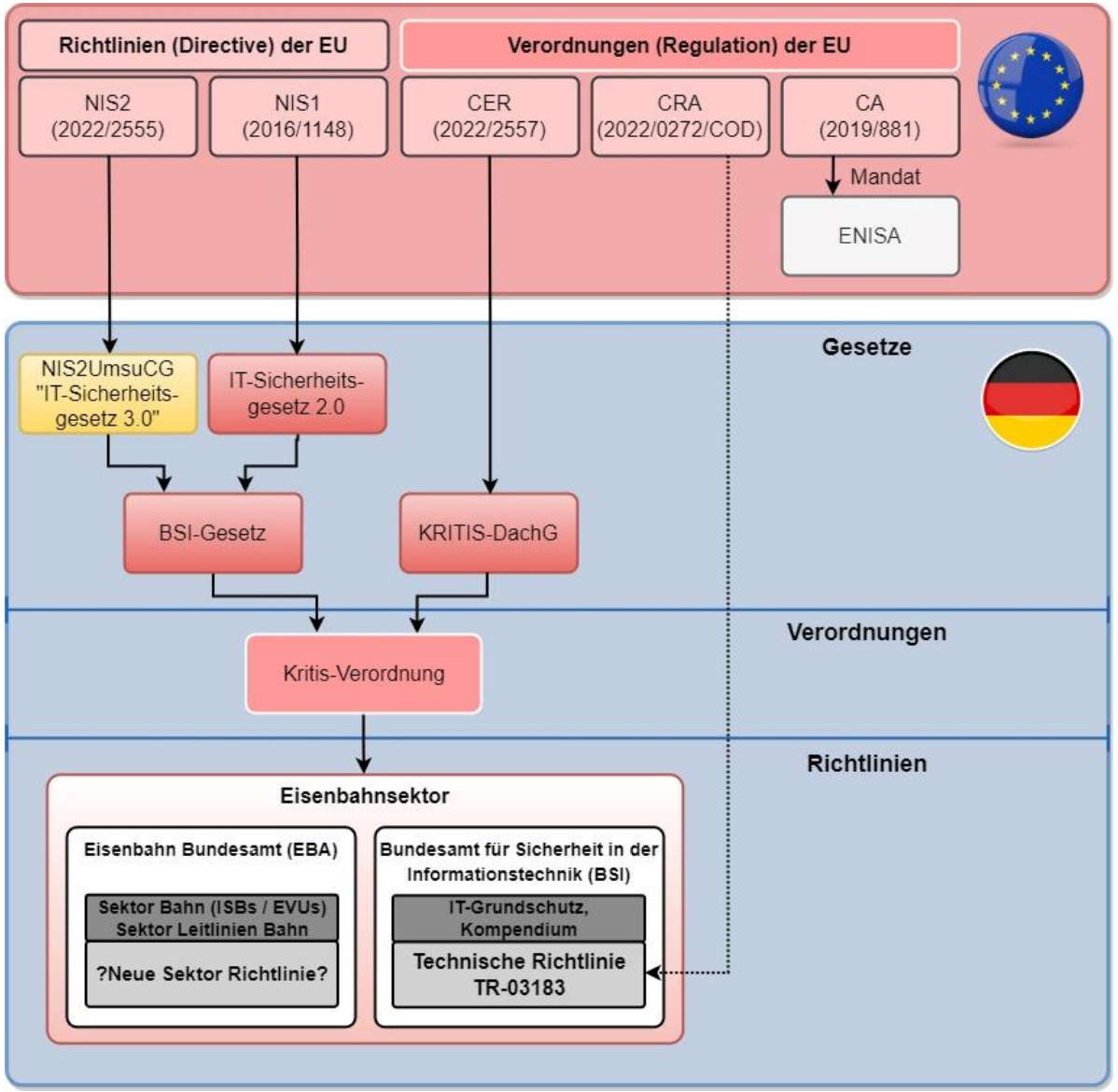
Regulatorische Ausgangslage EU

- **Cybersecurity Act (CA)**
  - Verordnung (kein Gesetz)
  - Gilt länderübergreifend
- **ENISA** (European Union Agency for Cybersecurity)
  - Richtlinien für Bahnbereich



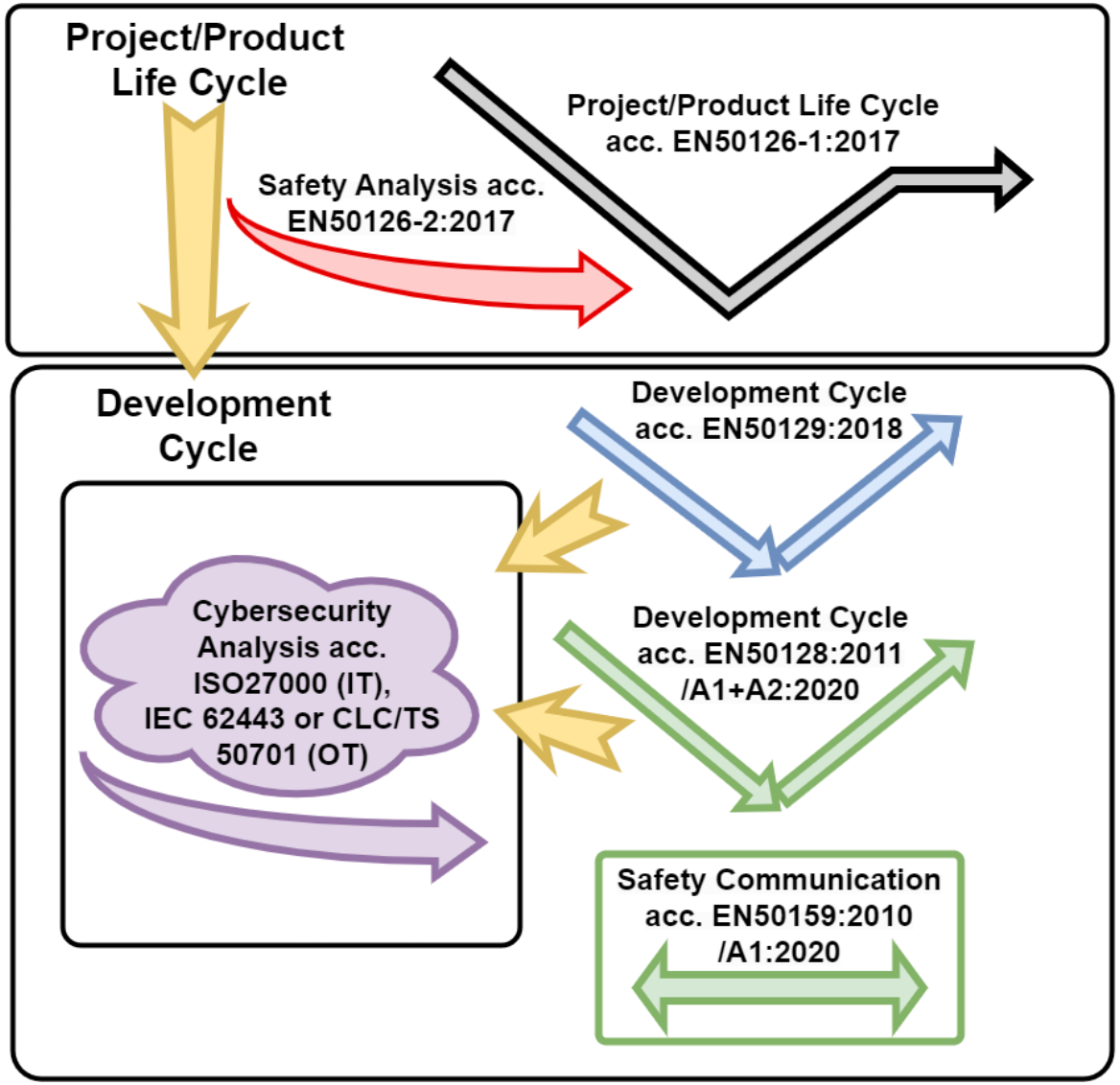
Regulatorischer Aufbau EU, DE

- **Exemplarischer Aufbau EU → DE**
  - EU erlässt europäische Richtlinien / Verordnungen
  - Land erlässt nationale Gesetze
  - Aus Gesetzen entstehen nationale Verordnungen
  - Aus nationalen Verordnungen entstehen nationale Richtlinien
- **EU-Richtlinien** **(z.B. *EU-Network and Information Security* V2- NIS2)**
  - Müssen in nationale Gesetze überführt werden (EU weit)
- **EU-Verordnungen** ***(z.B. EU Cyber Resilience Act- CRA)***
  - EU, sind länderübergreifend gültig
  - Beeinflussen nationale Gesetze



Anforderungen aus den CENELEC-Normen

- **Betrachtung der funktionalen Sicherheit**
  - Normative Vorgaben (kein Gesetz)
  - Verlinkung des Projekt-/Produktlebenszyklus mit Entwicklungszyklus
  - Anforderung: für die funktionale Sicherheit muss auch die Cybersicherheit gewährleistet sein z.B.:
    - Information Technology (IT)-Sicherheit: ISO 27000ff
    - Operational Technology (OT)-Sicherheit: CLC/TS 50701 (IEC 62443)



Regulatorische Compliance Matrix

	CH	EU	DE	CENELEC
Gesetz	EBG	CA (2019/881)	BEVVG / AEG	EN 50126-1/-2:2017
Behörde	BAV	ENISA	EBA	ISA
Richtlinie	RL CySec-Rail	ENISA Railway Cybersecurity	Sektor Leitlinie Bahn	EN 50129:2018 & EN 50128:2011 +A1/A2:2020 oder EN 50657:2017
Anforderung	Minimal	Maximal	Maximal	Maximal
Umfang	Einzelne Aspekte	Komplett	Komplett	Komplett
IT-Sicherheit	ISO 27001 & ISO 27002	ISO 27000ff	ISO 27000ff	ISO 27000ff
OT-Sicherheit	CLC/TS 50701:2023	CLC/TS 50701	CLC/TS 50701	CLC/TS 50701
Ziel Umsetzung	Offen, 8.2024 (1. Paket)	KA	2024 (Stichproben BSI) 2027 (Audits)	

Regulatorische Matrix Deutschland

	Kritische Anlage		Unternehmen
Gesetz	NIS2UmsuCG	DachG	NIS2UmsuCG
Behörde	BSI	BBK	BSI
Zeitraum	2024-2027	2024 -2026	2024
Inhalt	IT-Sicherheit Meldepflicht Systeme zur Angriffserkennung	Physische Resilienz	IT-Sicherheit Meldepflicht
Überprüfungs-intervall	Alle 3 Jahre Audits	Stichproben	Stichproben Bei Anlass
Pflicht	§39 Nachweise	§11 Min. Vorgaben	§64 BSI Prüfrecht §65 BSI Prüfrecht
Ziel Umsetzung	2027	2026	2024 (Stichprobe BSI) 2027 (Audits)

Legende:
- BSI: Bundesamt für Sicherheit in der Informationstechnik
- BBK: Bundesamt für Bevölkerungsschutz und Katastrophenhilfe
- NIS2UmsuCG: NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetz
- EU-NIS: EU Network & Information Security

Anwendungsgebiete der IT- & OT-Sicherheit in einer Firma

Cybersecurity (IT / OT)

Cybersecurity für die Firma (IT)

Physischer Schutz

IT-Sicherheit

Cybersecurity für ein Projekt (IT / OT)

Projekt (IT)

System (IT/OT)

Enotrac

Konsequenzen

Linked in

EU Meldepflichten

- Sicherheitsvorfall unverzüglich der Behörde melden
- Schwerwiegende Betriebsstörungen oder Finanzieller Verlust
- Natürliche Juristische Personen materielle immaterielle Schäden hat.

- Unverzüglich
  - 24 Stunden wenn der Verdacht besteht dass er böswillige rechtswidrige Handlung.
  - 72 Stunden Aktualisierung von erster Meldung erste Bewertung einschliesslich Schweregrads
    - Und Auswirkungen, Komprimmitierungsindikatioren.

EU Penalties (NIS2 §A34)

Verstösse	Wesentliche Einrichtungen	Wichtige Einrichtungen	Verantwortung.
• Verbindliche Warnungen, Anweisungen, Fristen einhalten, Empfehlung umsetzen, • Wird überwacht	• €10’000’000 Busse • Oder 2% des gesamten Umsatzes des Unternehmens	• €7’000’000 Busse • Oder 1.4 % des gesamten Umsatzes des Unternehmens	• CEOs und VRs

Information Security Management System – ISMS

(Managementsystem für Informationssicherheit)

Information Security Management System: Was ist das

Ein **Information Security Management System** (ISMS, englisch für „*Managementsystem für Informationssicherheit*“) ist die Aufstellung von **Verfahren** und **Regeln** innerhalb einer Organisation, die dazu dienen, die Informationssicherheit dauerhaft zu definieren, zu steuern, zu kontrollieren, aufrechtzuerhalten und fortlaufend zu verbessern.

Der Begriff wird im Standard **ISO/IEC 27002** definiert. **ISO/IEC 27001** definiert ein ISMS. (Source: Wikipedia)

Das Haupt-Ziel eines ISMS ist es, die **Vertraulichkeit**, **Integrität** und **Verfügbarkeit** von Informationen unter Anwendung eines *risikobasierten Vorgehens* zu steuern und sicherzustellen. Ein ISMS unterstützt die Verantwortlichen dabei, risikogerecht und zielgerichtet zu entscheiden sowie geeignete Massnahmen zum Schutz von Informationen vorzunehmen.

Das BAV (Bundesamt für Verkehr) hat am 22.09.2023 die "Richtlinie Cybersicherheit Eisenbahn (RL CySec-Rail)" herausgegeben, die Unternehmen verpflichtet, sich bis zum **01.07.2024** an dieser Richtlinie zu orientieren.

Die Richtlinie dient zudem als Grundlage für die Prüfungen im Rahmen der Aufsichtstätigkeit des BAV.


Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation UVEK

Bundesamt für Verkehr BAV
Abteilung Sicherheit

Aktenzeichen: BAV-041.4-3/11/6/15/1/4/1
Datum: 22.09.2023
Version: V1.0

Richtlinie

Cybersicherheit Eisenbahn

RL CySec-Rail

Auf Grundlage von Art. 5c der Verordnung über Bau und Betrieb der Eisenbahnen (Eisenbahnverordnung, EBV – SR 742.141.1) und deren Ausführungsbestimmungen.

Minimale Anforderungen und ISMS-Einführung

Die obligatorische Einführung gemäss den Minimalanforderungen der RL CySec-Rail stärkt proaktiv die Widerstandsfähigkeit gegenüber Cyberbedrohungen.

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Bundesamt für Verkehr BAV

MINIMALE ANFORDERUNGEN (Beispiele)

Informationssicherheits-strategie (A-01)	Rollen und Verantwortlichkeiten (A-02 & B-01)	Richtlinien und Organisation (A-03)	Regelmässige Überprüfung der Informationssicherheit / Audits (A-04)
Kontinuierliche Verbesserung (A-05)	Dokumentation (A-06 & B-12 & B-16)	Risikobeurteilung und – Behandlung (A-07))	Massnahmen zum Schutz von Endgeräten (B-13 & B-14)
Systemintegrität (B-25)	Business Continuity Management (B-09)	Management von Informationssicherheits-Vorfällen (B-08)	Informationssicherheit in Projekten mit IT- und OT-Bezug (B-05)

und zusätzlich andere mehr...

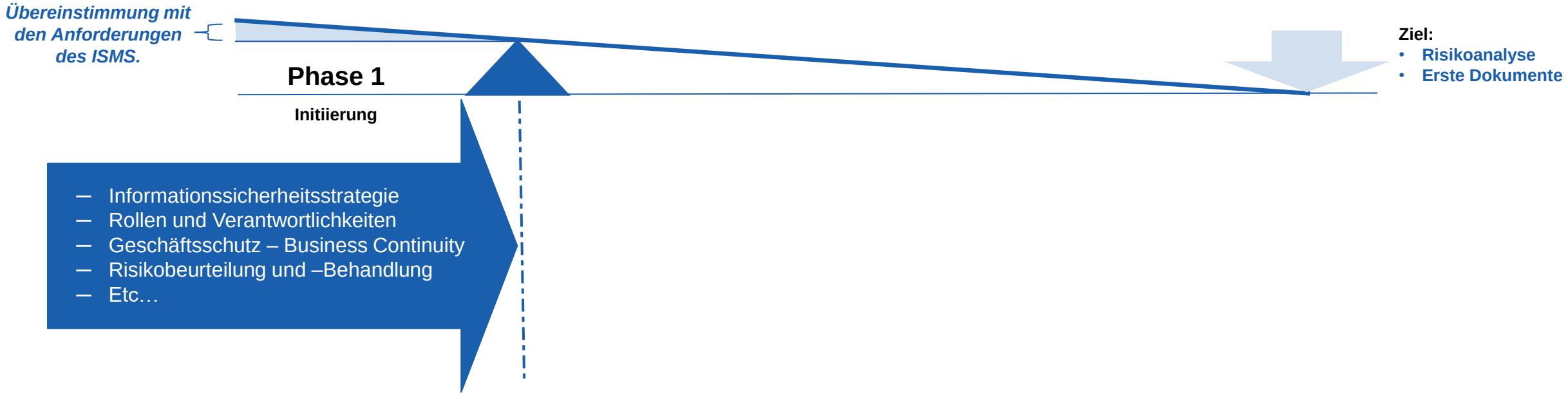
Herausforderungen des ISMS

1. **Sicherheitsrisiken kennen**
   - Fachkräftemange
   - **Integration von OT- und IT-Sicherheit**
2. Veraltete Technologie
   - Budgetbeschränkungen und Kosten
   - **Zeit- und Ressourcenbedarf**
3. Datenschutz und Datenschutzanforderungen
   - **Reduzierung der Bedrohungslage**
   - Kompromittierung- Index
4. Krisenmanagement
   - **Geschäftskontinuität**
   - Sensibilisierungs- Schulungen
5. **Drittanbieterrisiken**/kritische Lieferanten
   - Prozesse und Prozeduren schreiben
   - **Integration von Sicherheit in Unternehmen** (Cyber-Massnahmen)
6. **Sicherheit von IoT-Geräten und -Systemen**
   - Komplexität der Infrastruktur und Systeme
   - **Internationale Zusammenarbeit**

ISMS konkrete Umsetzung: Phase 1 (Initiation)

Bevorzugt wird ein **dreiphasiger Ansatz**, der kurzfristig Kompatibilität und Akzeptanz gewährleisten könnte. Die Erstellung einer **Cyberstrategie** ist ein wesentlicher Bestandteil dieses Prozesses.

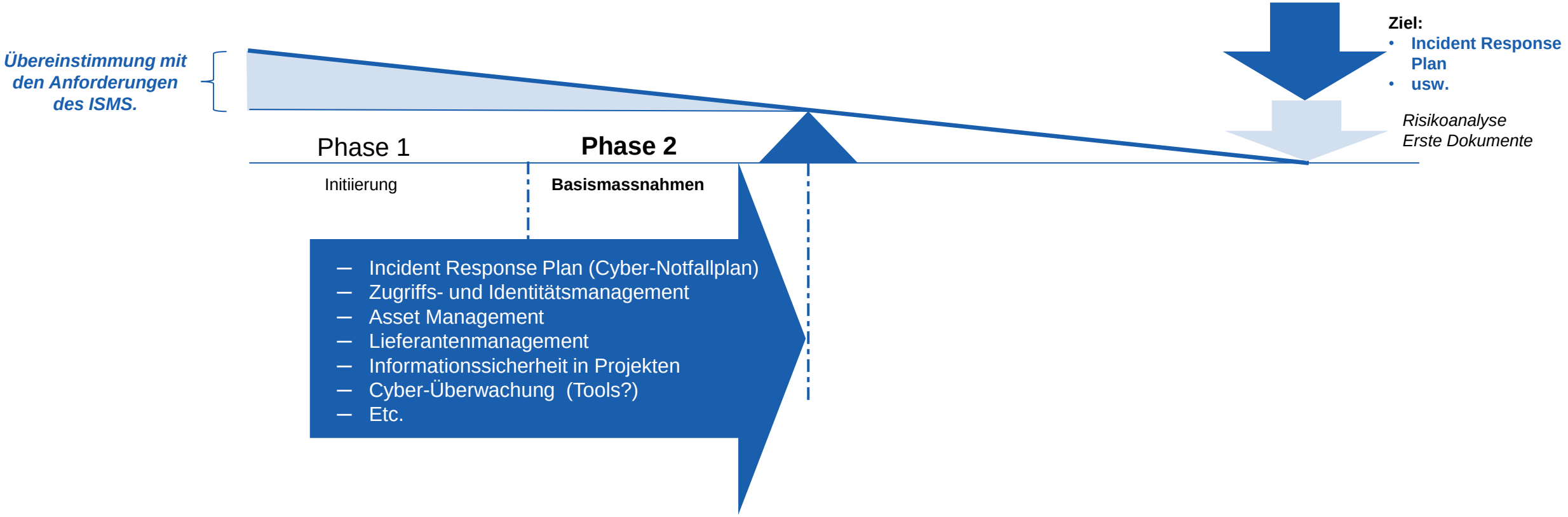
In dieser ersten Phase erfolgt **eine Analyse der Cyber-Risiken**, die Bildung des ISMS/Cyber-Teams, die **Zuweisung des Budgets** und die **Festlegung der Prioritäten**.



ISMS konkrete Umsetzung: Phase 2 (Basismassnahmen)

Während dieses Prozesses werden grundlegende Massnahmen identifiziert, darunter **Zugriffs- und Identitätsmanagement, Asset Management, Lieferantenmanagement**, **Informationssicherheit in Projekten** und so weiter.

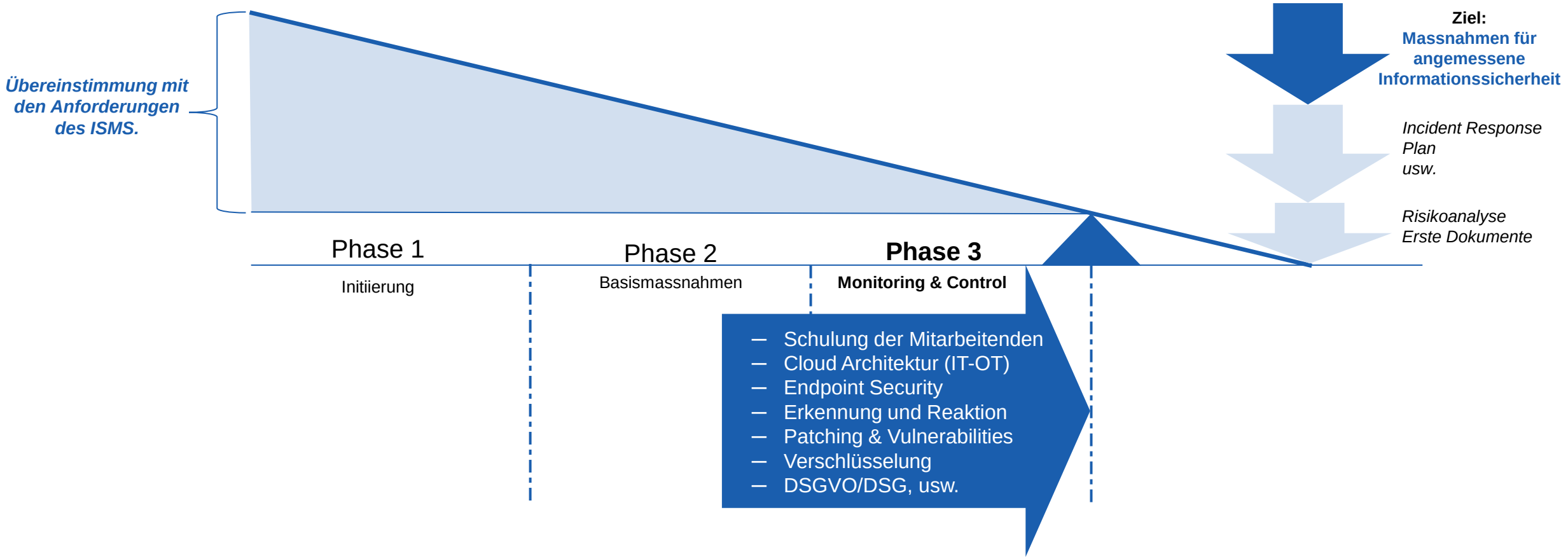
Ein entscheidender Aspekt ist die Erstellung eines **Cyber-Notfallplans** im Falle eines Cyberangriffs.



ISMS konkrete Umsetzung: Phase 3 Monitoring & Control

Hier ist es entscheidend, **Cybersecurity-Tools zu implementieren** (Endpoint-Sicherheit, Erkennung und Reaktion auf Cyberangriffe), sowie **Schulungen der Mitarbeitenden**, Netzwerkpläne und Konzepte, **Cloud-Sicherheit, Patching und Vulnerabilities Management** usw.

Zudem müssen alle Aspekte im Zusammenhang mit der DSGVO oder DSG-CH umgesetzt werden.



Enotrac

Operational Technology (OT) Security

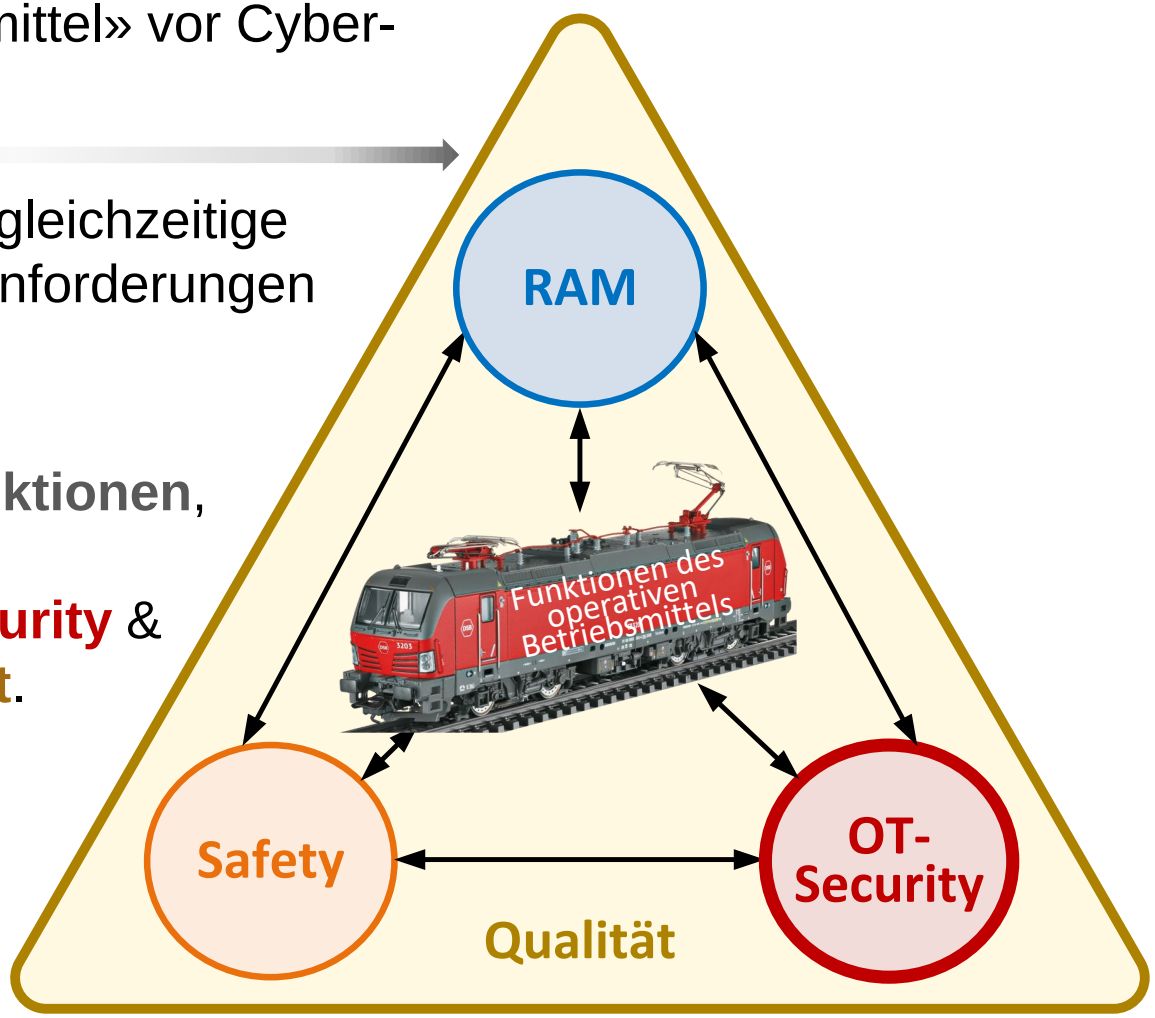
Worum geht es?

Es geht um den **Schutz** der Funktionen «operativen Betriebsmittel» vor Cyber-angriffen.

Schutz der **Funktionen** aller **“operativen Betriebsmittel”** durch **OT-Security**

Es geht um die gleichzeitige Erfüllung aller Anforderungen der Bereiche

- **RAM**,
- **die Funktionen**,
- **Safety**,
- **OT-Security** &
- **Qualität**.

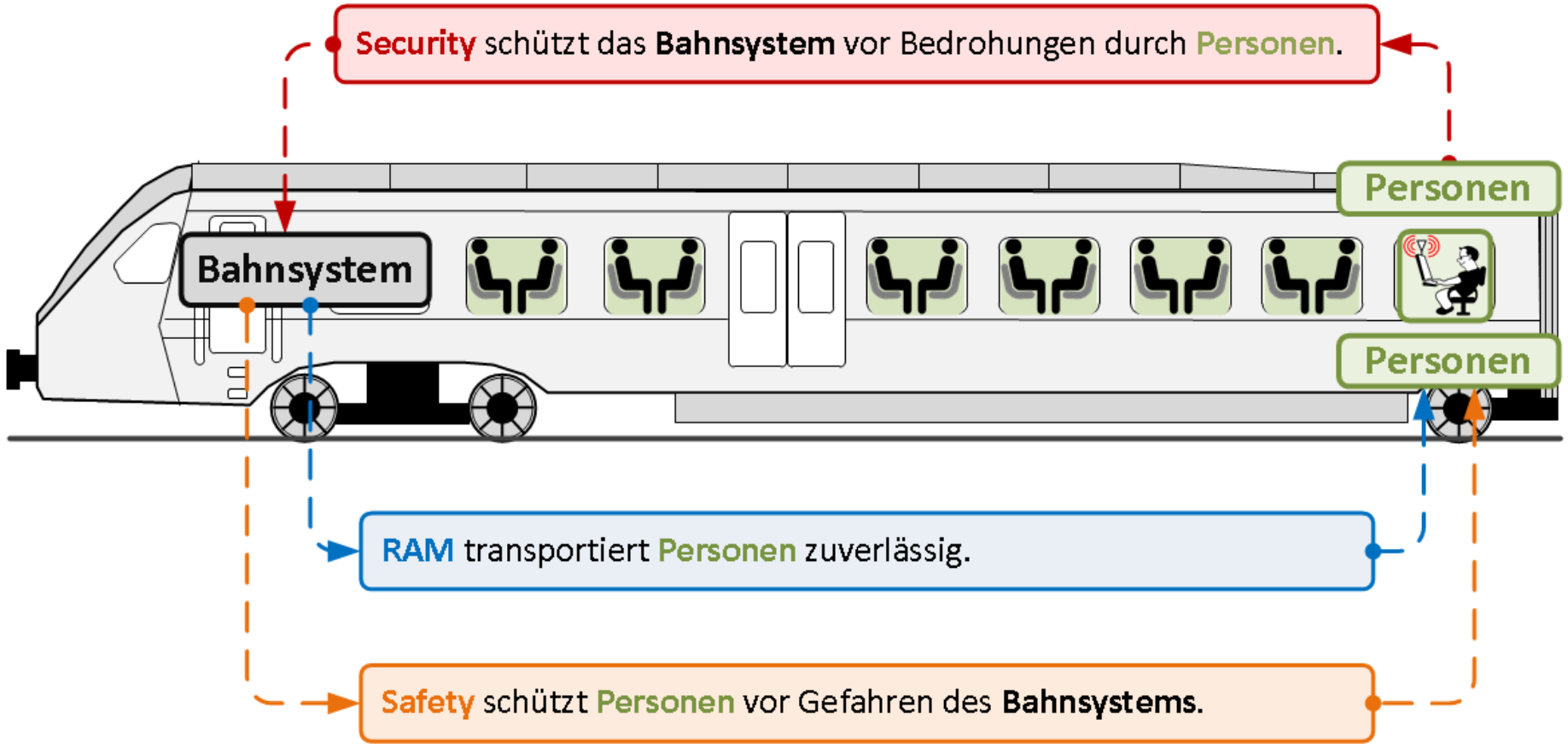


RAM-, Safety- & Cybersecurity-Anforderungen stehen in konflikthaft Beziehung zueinander

If the **rail system** is not **Secure**,

it's unlikely to be

- **R**eliable,
- **A**vailable,
- **M**aintainable or
- **S**afe!



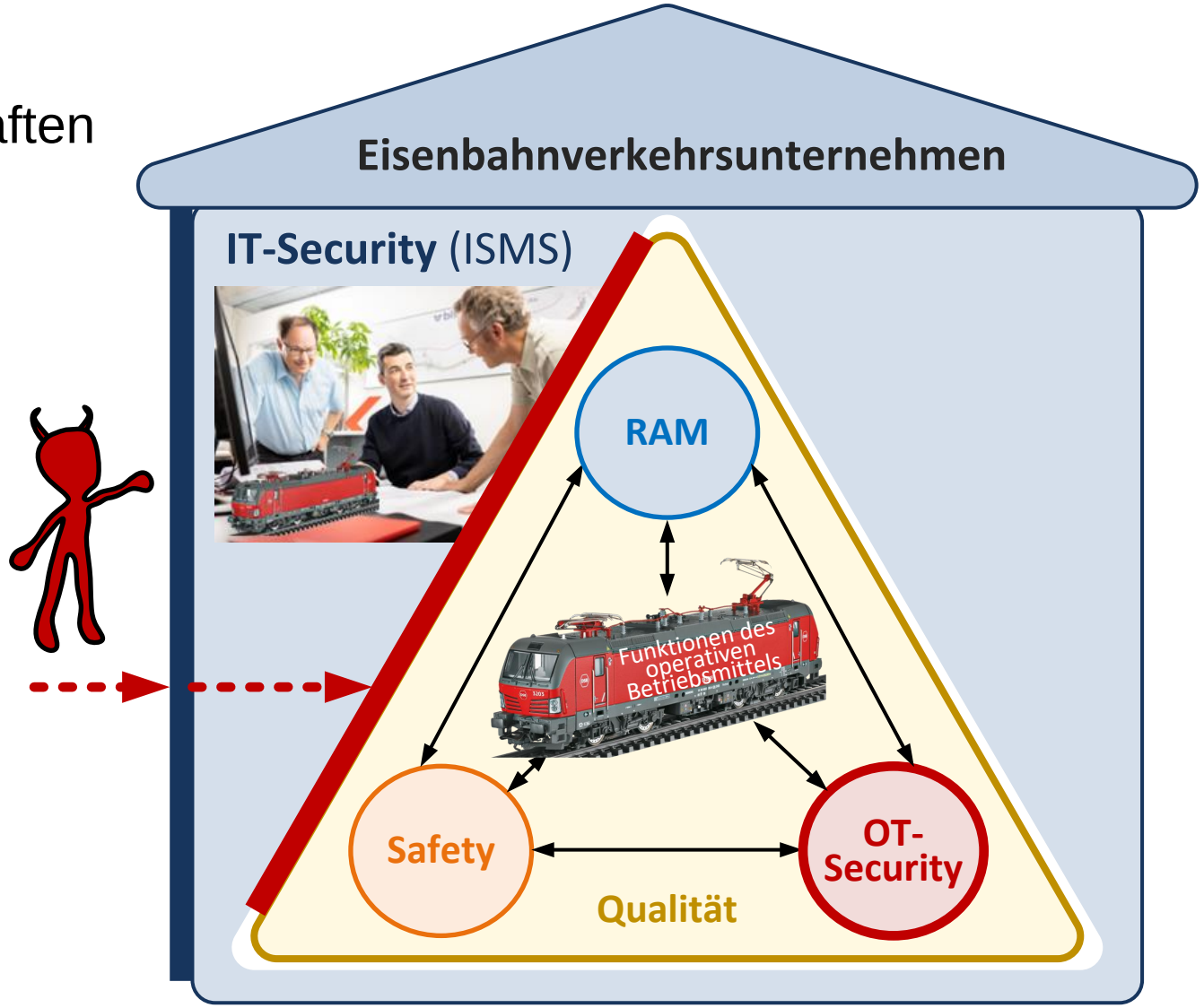
Daher geht es ums Ganze!

Die gleichzeitige Erfüllung der konflikthaften Anforderungen gelingt nur durch

Co-Engineering

der Bereiche

- **RAM**[1],
- **operative Funktionen**,
- **Safety**,
- **OT-Security** &
- **Qualität**.



[1] Reliability, Availability, Maintainability

OT-Security erfordert mehr als «nur» Technik!

Die Gewährleistung von OT-Security erfordert zudem

- **technische**,
- **organisatorische** und
- **personenbezogene**

Massnahmen zum Schutz der

- Verfügbarkeit,
- Integrität und
- Vertraulichkeit

von Informationen, Daten und Systemen.

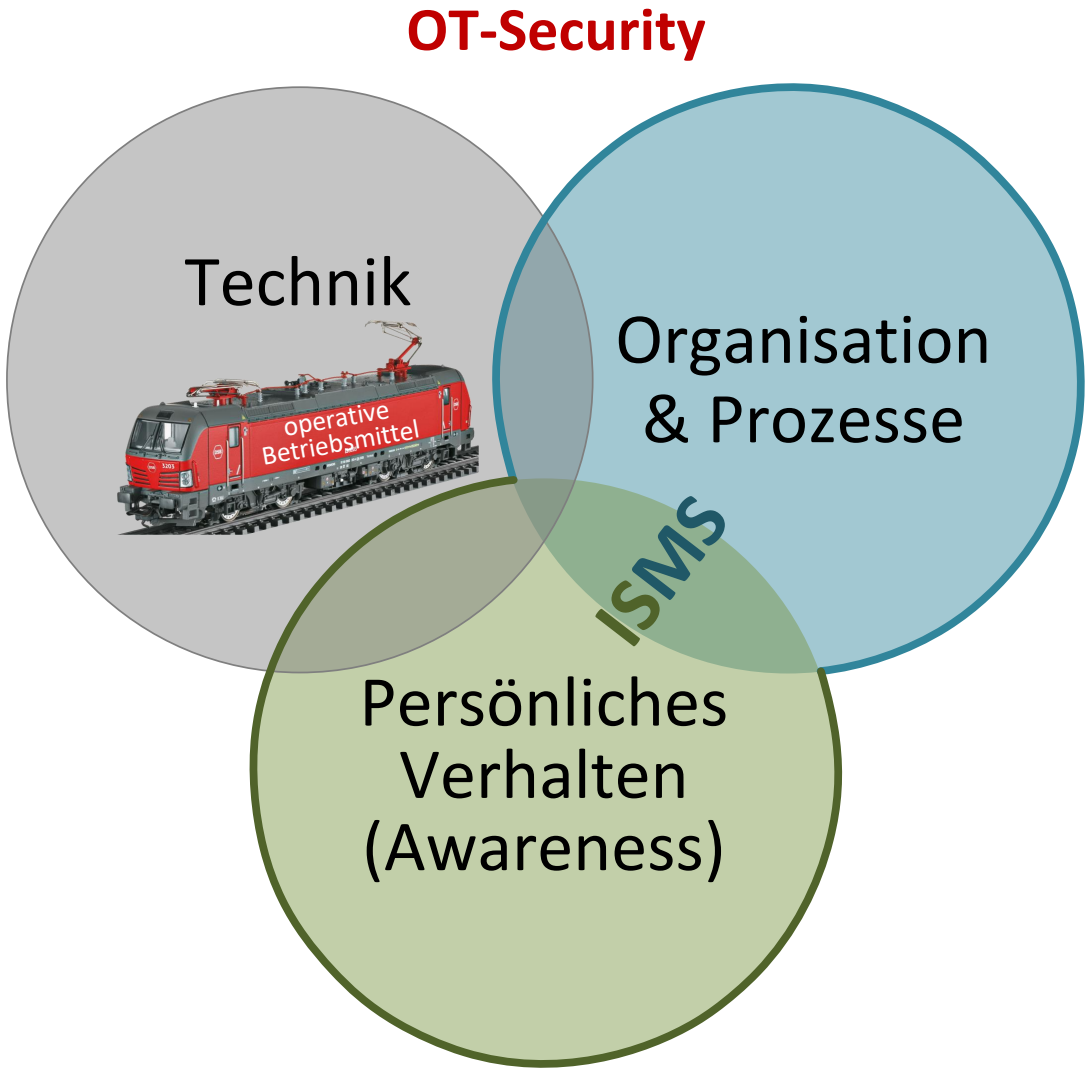
OT-Security erfordert damit ein

- Information Security Management System (ISMS)

möglichst als Bestandteil des

- Integrierten Managementsystems (IMS)

des jeweiligen Unternehmens.



Zusammenfassung

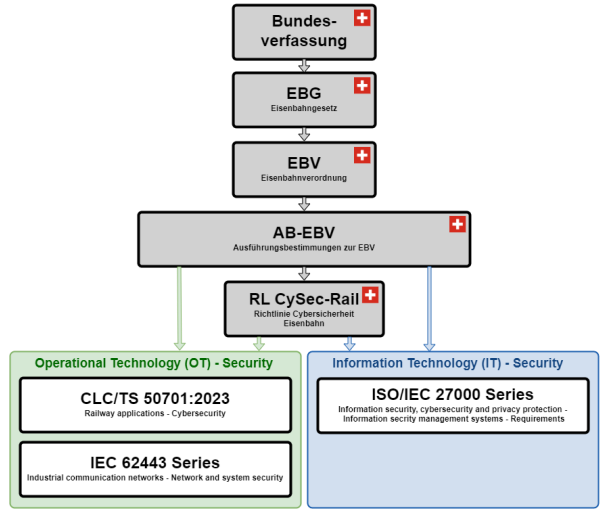
Das Wichtigste in Kürze

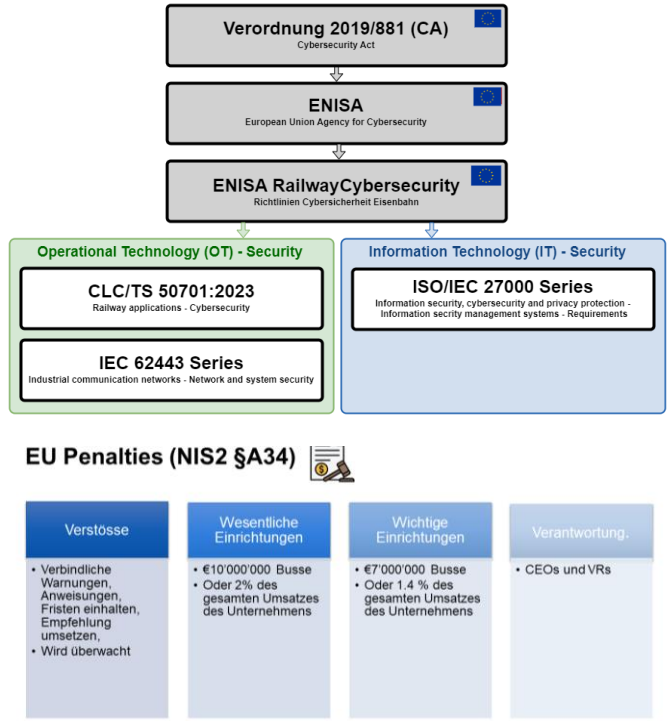
Neue Anforderungen CH

- Operational Technology (OT):
  - CLS/TS 50701:2023 (Railway applications Cybersecurity)
  - IEC 62443 Series (Industrial Communication Networks/System Security)
- Neu RL Cysec-Rail ab den 01.07.2024 (Grundlagen für ein ISMS)

Regulatorische Ausgangslage EU

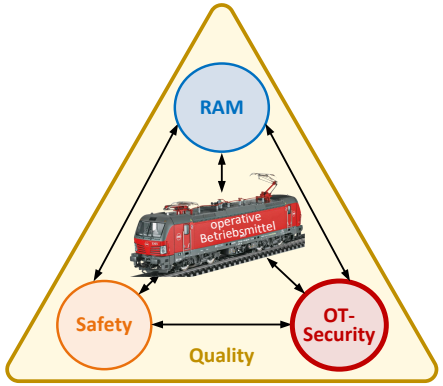
- Cybersecurity Act (Landübergreifend)
- ENISA Richtlinien Cybersicherheit Eisenbahn
- EU Meldepflichten
- EU Penalties (NIS2 §A34)



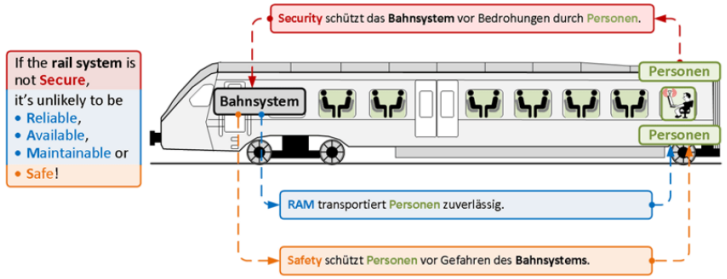


Das Wichtigste in Kürze

- **OT: Ganzheitliche Betrachung**
  - OT-Security
  - **C**o-**E**ngineering zu RAMS



- **Funktionale Sicherheit (Safety) bedingt Cybersicherheit (Security)**
  - Informations- und Kommunikations-Technologie (IKT) durch IT-Security und
  - Information and Communication Systems (ICS) durch OT-Security
  - Organisation und Prozesse
  - Persönliches Verhalten (Awareness)



Unterlagen und Feedback

- Alle Informationen zum heutigen Webinar finden Sie hier:
  - https://enotrac.com/de/cybersecurity-webinar/

- Geben Sie uns hier Feedback zum Webinar

- Und bleiben Sie auf dem Laufenden via LinkedIn

Fragen und Antworten

Kontakte unserer Referenten

Jens Schulze
Bereichsleiter RAMSS
Mitglied der Geschäftsleitung

jens.schulze@enotrac.com
+41 33 346 66 30

Michael Aebischer
Projektleiter / Projektingenieur
Bereich RAMSS

michael.aebischer@enotrac.com
+41 33 346 66 32

Juan Carlos Lopez Ruggiero
Teamleiter Cyber Security
Bereich RAMSS

juancarlos.lopezruggiero@enotrac.com
+41 52 224 03 44

Prof. Dr. Ernst Zollinger
Senior Berater
Bereich RAMSS

ernst.zollinger@enotrac.com
+41 33 346 66 08

Wichtige Abkürzungen

ISMS	Information Security Management System
OT	Operatonal Technology
IT	Information Technology
NIS	EU Network and Information Security (EU-Cybersicherheitspolitik)
CRA	Cyber Resilience Act
ENISA	European Union Agency for Cybersecurity
RL Cysec-Rail	Richtlinie Cybersicherheit Eisenbahn von Bundesamt für Verkehr
BSI	Bundesamt für Sicherheit in der Informationstechnik (Deutschland)