VÖV UTP
Verband öffentlicher Verkehr
Union des transports publics
Unione dei trasporti pubblici

Fachtagung Datennetze

D RTE 28100 Nachweisführung Datennetze
Safety und Security - Praxisbeispiele

11. Dezember 2024 in Bern

Herzlich willkommen

Tagungsleitung und Organisation

Dr. Robert Leemann, SBB
Urs Walser, VöV

Referenten

Thierry Bassani, SBB
Patrick Favre, BAV
Martin Gerber, RBS
Matthias Glock, SBB
Jean-Christophe Grandchamp, SBB
Emmerich Horvath, zb
Tobias Hubschmid, BAV
Andreas Klopfenstein, BLS
Kurt Maier, ex-SBB, Projektleiter D RTE 28100
Markus Roth, RhB
Marcel Schmid, VöV
Patrick Waldburger, AB

Herzlich willkommen

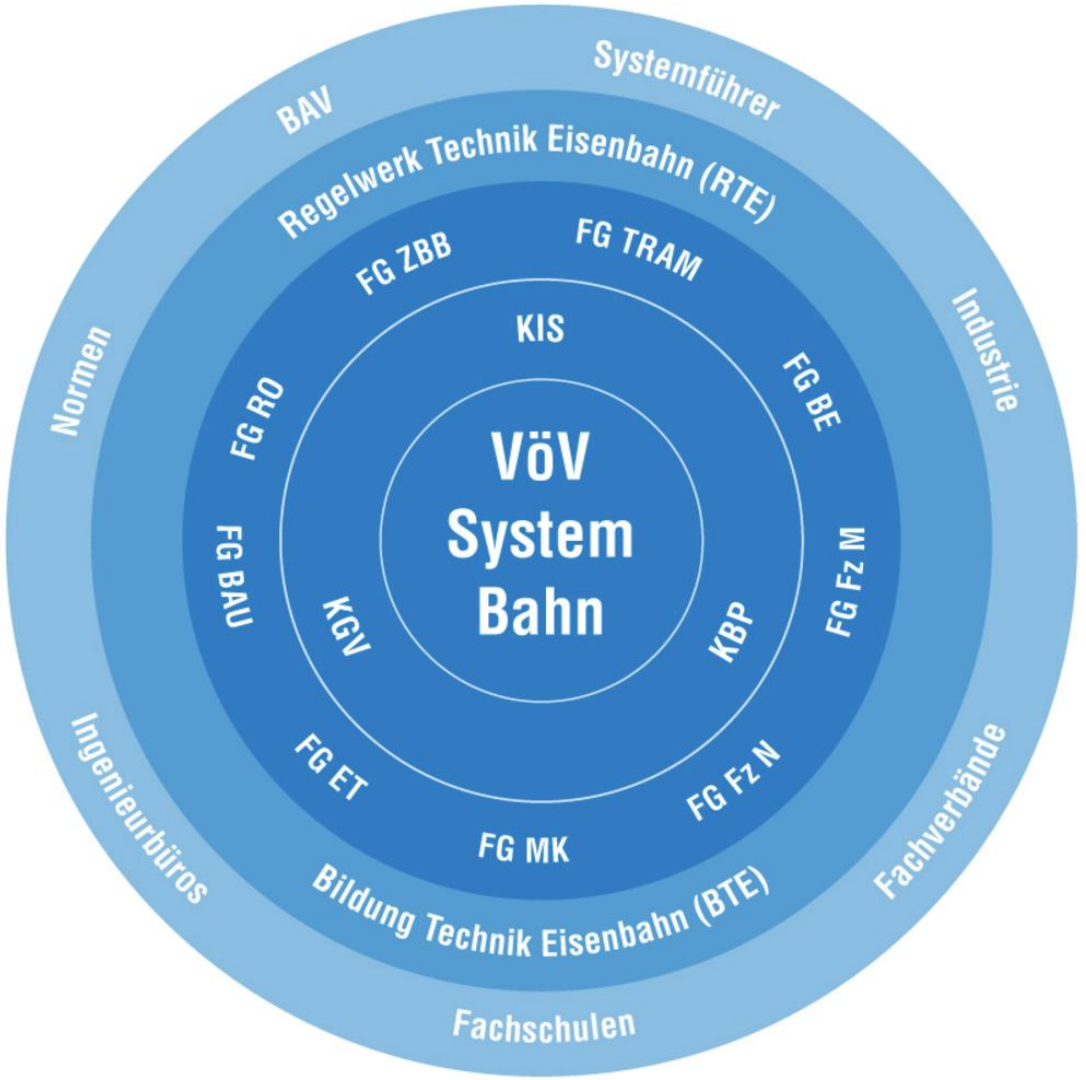
Bernhard Adamek
Vizedirektor VöV

Fachtagung Datennetze

Organisiert durch die
VöV Fachgruppe Elektrotechnik

in enger Zusammenarbeit mit

der Projektgruppe D RTE 28100



Beziehungsnetz System Bahn

VÖV UTP

Fachtagung Datennetze

Hinweise

- Programm gemäss Einladung, mit kleinen Anpassungen
- Kaffeepause und Mittagessen bewusst so angesetzt
  für intensive Gespräche und Kontakte
- Referenten stehen in Fragerunden und auch
  bilateral zur Verfügung
- Simultanübersetzung deutsch → französisch
- Präsentationen zum Download → Link heute morgen per Mail zugestellt

Erinnerung an den Start des RTE-Projekts

- Der Bedarf nach neuen RTE-Regelungen wird in den VöV-Fachgruppen diskutiert
- Einige Themen wecken Interesse, aber sie sind nicht so brisant, dass rasch eine Gruppe zusammengestellt ist.
- Bei “Cybersecurity und Datennetze” war das Gegenteil der Fall: gar viele Fachleute meldeten sich an.
- Freudentag für die Fachgruppe!
  Die Publikation ist erfolgt und wir stellen heute im Format der Fachtagung das Produkt vor.

Programm Vormittag

9:30 Uhr	**Begrüssung und Einführung** Dr. Robert Leemann
9:45 Uhr	**Neue RTE-Regelung**
9:45 Uhr	Handlungsbedarf und Hoheitliche Grundlagen, Safety – Security Patrick Favre, Tobias Hubschmid
10:05 Uhr	D RTE 28100 Nachweisführung Datennetze Einführung und Grundsätze RTE Kap. 1-4 Kurt Maier
10:20 Uhr	Offene Fragen Dr. Robert Leemann
10:35 Uhr	**Pause**

VÖV UTP
Verband öffentlicher Verkehr
Union des transports publics
Unione dei trasporti pubblici

D RTE 28100, Handlungsbedarf und hoheitliche Vorgaben - Safety und Security, 1. Teil

Patrick Favre, Tobias Hubschmid

Bern, Mittwoch, 11.12.2024

Handlungsbedarf und hoheitliche Grundlagen

1. Teil:

– Was muss das BAV überhaupt genehmigen?

– Was wurde früher typenzugelassen?

– Wie wurden die Datennetze früher behandelt?

– Der «Änderungsprozess Datennetze@SA» der SBB

– Ein Änderungsprozess für die Privatbahnen

Inhalt Teil 2: Fokus Security

Was muss das BAV überhaupt genehmigen?

Eisenbahngesetz, Art. 18 zum Plangenehmigungsverfahren (PGV)

[1] Bauten und Anlagen, die **ganz oder überwiegend dem Bau und Betrieb einer Eisenbahn dienen** (Eisenbahnanlagen), dürfen nur mit einer Plangenehmigung erstellt oder geändert werden.
[…]
[2] Genehmigungsbehörde ist das BAV.

➔Nicht nur Sicherheitsrelevantes muss genehmigt werden

Eisenbahnverordnung, Art. 7 zur Typenzulassung (TZL)

[1] Das Gesuch um eine **Typenzulassung** nach Artikel 18x EBG kann gestellt werden, sofern sie geeignet ist, **Bewilligungsverfahren zu vereinfachen**.

➔ Die TZL dient grundsätzlich der Vereinfachung des PGV

Was wurde früher typenzugelassen?

Früher und heute:

– Im Bereich der Sicherungsanlagen wurden vor allem diejenigen Systeme typenzugelassen, die hoch sicherheitsrelevant (SIL 1 – 4) sind.

– Datennetze, die für hoch sicherheitsrelevante Datenübertragung verwendet werden, wurden typenzugelassen.

– Nicht hoch sicherheitsrelevante Telematikanwendungen wie RCS (das damalige TMS) liefen häufig «unter dem Radar».

In Zukunft:

– Auch nicht hoch sicherheitsrelevante Telematikanwendungen sollen systematisch in einem (vereinfachten) Verfahren behandelt werden.

Frühere Behandlung der Datennetze

Typenzulassungen für Datennetze:

– Difonet (SBB)

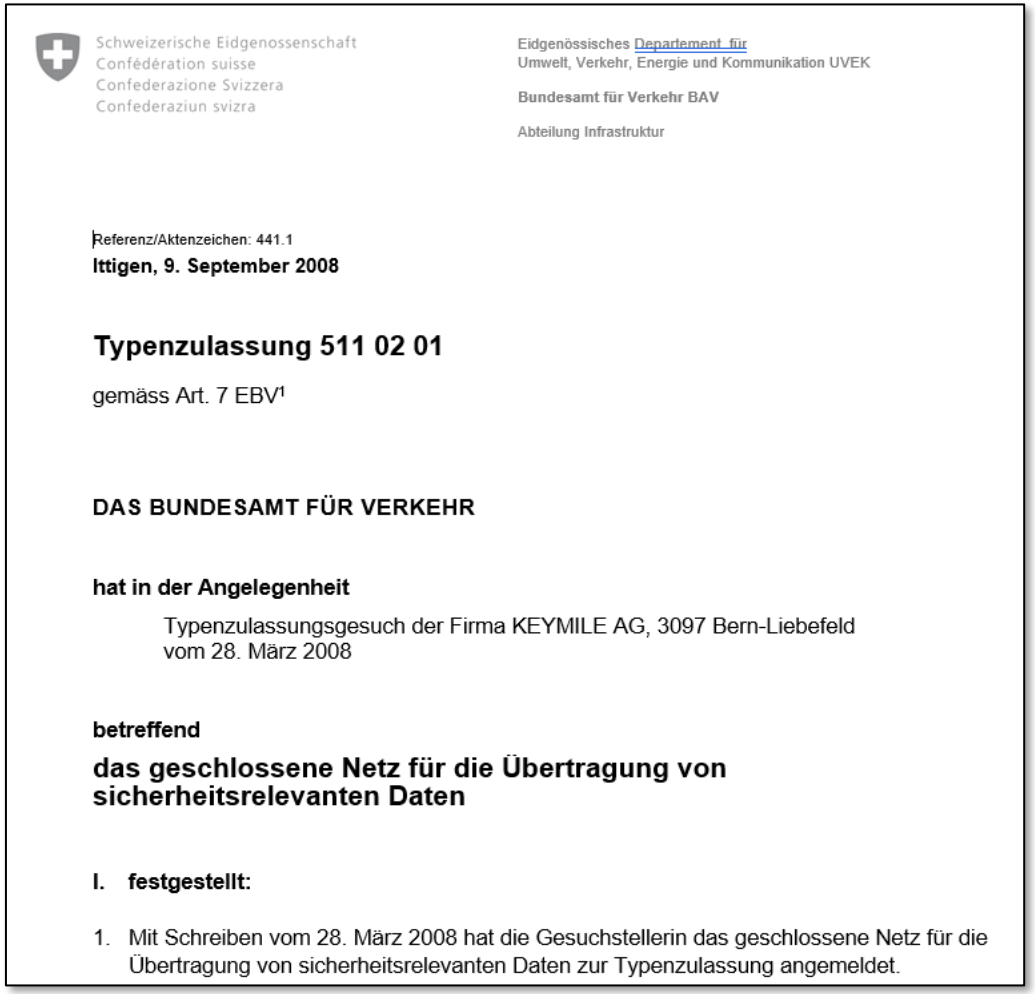
– Rail IP (SBB)

– UMUX / XMC20 (Ascom/Keymile/ABB/Hitachi)

Sie behandeln das Datennetz und enthalten eine Liste der zugelassenen Anwendungen.

Jede Änderung an den Anwendungen muss durch das BAV freigegeben werden.

➔**Weder sehr flexibel noch dynamisch**



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für
Umwelt, Verkehr, Energie und Kommunikation UVEK

Bundesamt für Verkehr BAV

Abteilung Infrastruktur

Referenz/Aktenzeichen: 441.1

Ittigen, 9. September 2008

Typenzulassung 511 02 01

gemäss Art. 7 EBV[1]

DAS BUNDESAMT FÜR VERKEHR

hat in der Angelegenheit

Typenzulassungsgesuch der Firma KEYMILE AG, 3097 Bern-Liebefeld vom 28. März 2008

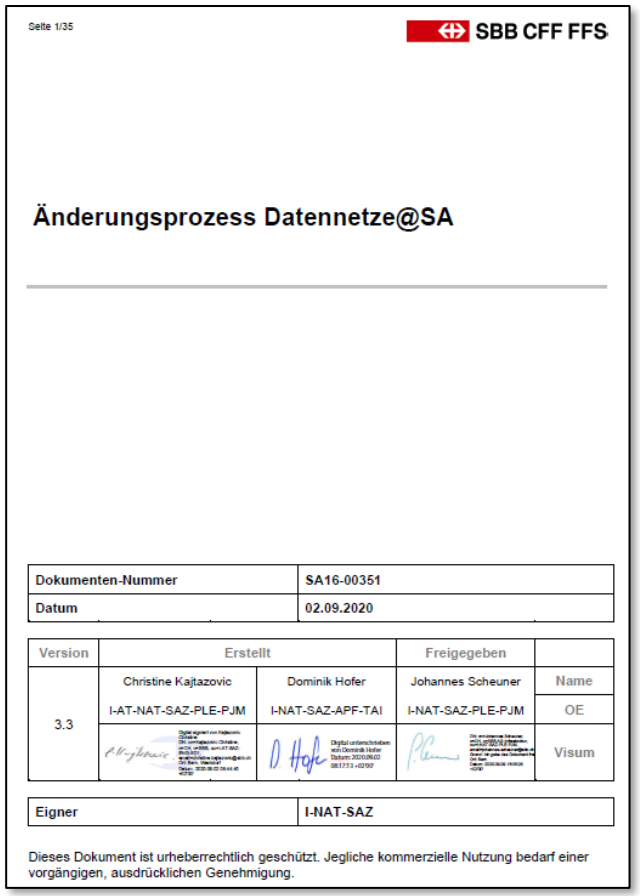
betreffend

das geschlossene Netz für die Übertragung von sicherheitsrelevanten Daten

I. festgestellt:

1. Mit Schreiben vom 28. März 2008 hat die Gesuchstellerin das geschlossene Netz für die Übertragung von sicherheitsrelevanten Daten zur Typenzulassung angemeldet.

Der „Änderungsprozess Datennetze@SA“ der SBB



Seite 1/35

SBB CFF FFS

Änderungsprozess Datennetze@SA

Dokumenten-Nummer	SA16-00351
Datum	02.09.2020

Version	Erstellt		Freigegeben	
	Christine Kajtazovic	Dominik Hofer	Johannes Scheuner	Name
3.3	I-AT-NAT-SAZ-PLE-PJM	I-NAT-SAZ-APF-TAI	I-NAT-SAZ-PLE-PJM	OE
				Visum

Eigner	I-NAT-SAZ

Dieses Dokument ist urheberrechtlich geschützt. Jegliche kommerzielle Nutzung bedarf einer vorgängigen, ausdrücklichen Genehmigung.

- Anlässlich der Ablösung des SDH-Datennetzes der SBB durch ein MPLS-Datennetz wurde eine Lösung gesucht, die bisherigen Typenzulassungen zu flexibilisieren.
- Im Hintergrund stand die aktuelle, europaweite Tendenz, den Eisenbahnunternehmungen mehr Freiheit, aber auch mehr Verantwortung zu übertragen.
- So entstand 2017 – 2020 der «Änderungsprozess Datennetze@SA» mit der Idee, dass **nicht mehr ein Datennetz mit seinen Anwendungen zugelassen** wird, sondern vielmehr **der Prozess, mit dem nachgewiesen wird, wie Anwendungen an das Datennetz aufgeschaltet werden**.
- Dutzende Anwendungen sind seither durch den Prozess gelaufen.

D RTE 28100: Ein Änderungsprozess für die Privatbahnen

– 2021 hat der VöV die Arbeitsgruppe D RTE 28100 zum Leben gerufen, um das Problem moderner Datennetze für hoch sicherheitsrelevante Anwendungen bei Privatbahnen zu lösen.
– Schon am Anfang stand eine Lösung «à la Änderungsprozess Datennetze@SA» der SBB im Raum, aber die Arbeitsgruppe hat lange über den Umfang der Regelung diskutiert.
– Schliesslich entspricht die D RTE 28100 einem auf Privatbahnen übertragenen «Änderungsprozess Datennetze@SA», in welchem die Erfahrungen der SBB eingeflossen sind.

D RTE 28100, Handlungsbedarf und Hoheitliche Grundlagen, Safety – Security, Teil 2: Fokus Security

Patrick Favre, Tobias Hubschmid

Bern, Mittwoch, 11.12.2024

Handlungsbedarf: Fokus Security

1960: Finde die Zutrittskontrolle und die Überwachungskameras

Gesellschaftlicher Wandel
∞
Wandel der Sicherheits-kultur

2024: Neue, kugelsichere Drehtür beim Haupteingang des Bundeshauses

D RTE 28100: Handlungsbedarf – Security

Vergangenheit

- **Überschaubare** Anzahl an IP-Netze im OT-Bereich.
- Datennetze noch wenig cybersicherheits- und betriebskritisch.
- Sicherheitskritische Datenverbindungen wurden **vom Internet getrennt** betrieben (geschlossene Netze, Angriffsfläche primär auf physischer Ebene)
- IT und OT relativ gut trenn- und **überschaubar**.

- Datennetze in sich kaum segmentiert, **Security kaum ein Thema**.

- Wenig **Budget** (wenn überhaupt) für Security Massnahmen vorhanden.

Datennetze Heute

↗ **Betriebsrelevanz**

- IT und OT zunehmend stark vermischt, **unternehmensübergreifende Netzwerke nicht mehr unter der vollen Kontrolle des ISB**
- Industrie 4.0 (IoT, Clouds, etc.), «all IP», **exponentieller Anstieg netzwerkfähiger Geräte**.

- Alte, schwach geschützte Applikationen und Services weiterhin im Einsatz (z.T. wird immer noch mit Telnet gearbeitet).
- **Zunehmende Bedrohungen**
- **steigende Anforderungen an die Netzwerke**

- Mehr (genügend) **Budget** für Security Massnahmen vorhanden **???**

Hoheitliche Grundlagen – AB 38.1

Die Datenverbindungen und -netzwerke müssen in Bezug auf
- Zuverlässigkeit,
- Verfügbarkeit,
- Instandhaltbarkeit,
- Sicherheit (Safety)
- und Cybersicherheit

} RAMS**S**

den Anforderungen der angeschlossenen Anlagen, Systeme und Anwendungen genügen.

AUSFÜHRUNGSBESTIMMUN

Kapitel: Bauten und An
Abschnitt: Sicherungsanla
Artikel: Grundsätze

AB 38.1 Allgemeines

1 Für die Spezifikatio
barkeits-, Instandha
sind die SN EN 501

1.1 Die sicherheitsrelev
Sicherheitsintegrität

1.2 Für die sicherheitsr
tungen ist zudem di

1.3 Die Sicherheitsnach
men mit Funktionen
erfolgen.

1.3.1 Bei Anwendung der SN EN 50129 erübrigt sich die Berücksichtigung der SN EN 50126-2, ausser bei expliziten Verweisen in der SN EN 50129.

1.4 Die Faktoren, die die Zuverlässigkeits-, Verfügbarkeits-, Instandhaltbarkeits- und Sicherheitseigenschaften (RAMS-Eigenschaften) beeinflussen, müssen während der gesamten Lebensdauer der Systeme eingehalten und überwacht werden.

1.5 Für Plangenehmigungs- und Betriebsbewilligungsverfahren regelt das BAV den Umgang mit den SN EN 50126-1 und SN EN 50129 in einer Richtlinie.

rdienstleiter und Triebfahr-

on Ereignissen ist die
Betriebsprozesse soweit

n gegen voraussehbare Fehl-
uchliche Eingriffe geschützt

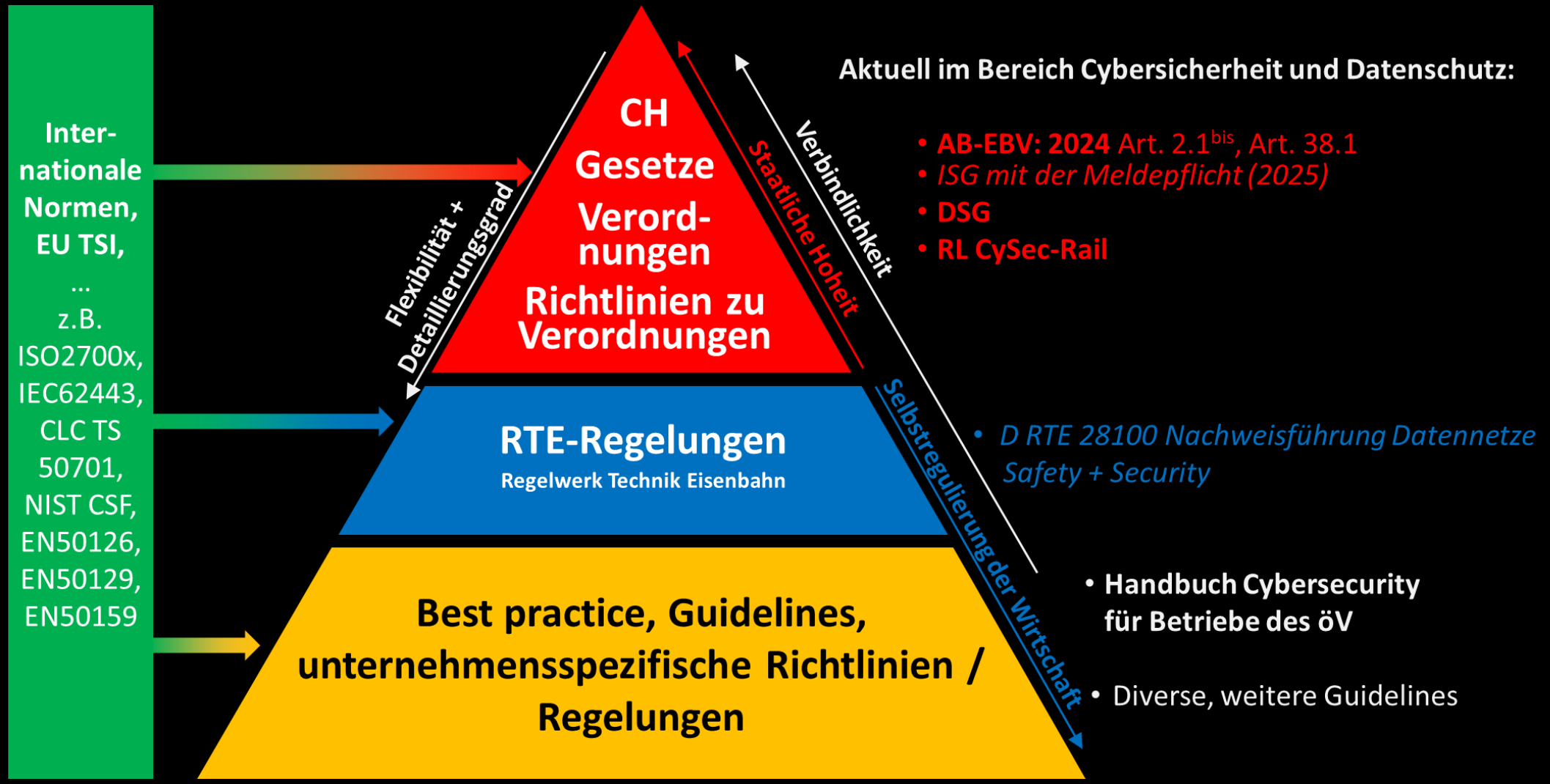
AB-EBV zu Art. 2, AB 2.1^{bis}.

kanwendungen müssen mit
n.

5 Für die Anforderungen an Kabel der Sicherungsanlagen und Telematikanwendungen gilt die AB-EBV zu Art. 44, AB 44.b.

6 **Neu:** Die Datenverbindungen und -netzwerke müssen in Bezug auf Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit, Sicherheit (RAMS-Anforderungen) und Cybersicherheit den Anforderungen der angeschlossenen Anlagen, Systeme und Anwendungen genügen.

Hoheitliche Grundlagen – Safety und Security



Aktuell im Bereich Cybersicherheit und Datenschutz:

- **AB-EBV: 2024** Art. 2.1^{bis}, Art. 38.1
- *ISG mit der Meldepflicht (2025)*
- **DSG**
- **RL CySec-Rail**

- *D RTE 28100 Nachweisführung Datennetze Safety + Security*

- **Handbuch Cybersecurity für Betriebe des öV**
- Diverse, weitere Guidelines

D RTE 28100: Wieso bezüglich Security nicht einfach auf die RL CySec-Rail oder auf eine passende Norm verweisen?

- Die D RTE 28100 geht **konkreter und detaillierter** auf das Thema CySec bei Datennetzen ein (spezifische Zielgruppe).
- Von Seite der Branche gab es keinen Bedarf Teile der Anforderungen wegzulassen und auf die RL CySec-Rail oder pauschal auf eine Norm zu verweisen.
- Unabhängige Entwicklungen der RTE 28100 und der RL CySec-Rail (beim Start der RTE 28100 war noch nicht bekannt, dass es die RL CySec-Rail geben wird). Bei den Normen ist derzeit viel Dynamik drin (z.B. IEC 63452)
- **Vorteil der aktuellen RTE:** Ein Dokument mit sämtlichen Informationen enthalten

Es gilt nun Erfahrungen zu sammeln und bei Bedarf Anpassungen vorzunehmen!

VÖV UTP
Verband öffentlicher Verkehr
Union des transports publics
Unione dei trasporti pubblici

D RTE 28100: Einführung

Kurt Maier, Projektleiter D RTE 28100

Bern, Mittwoch, 11.12.2024

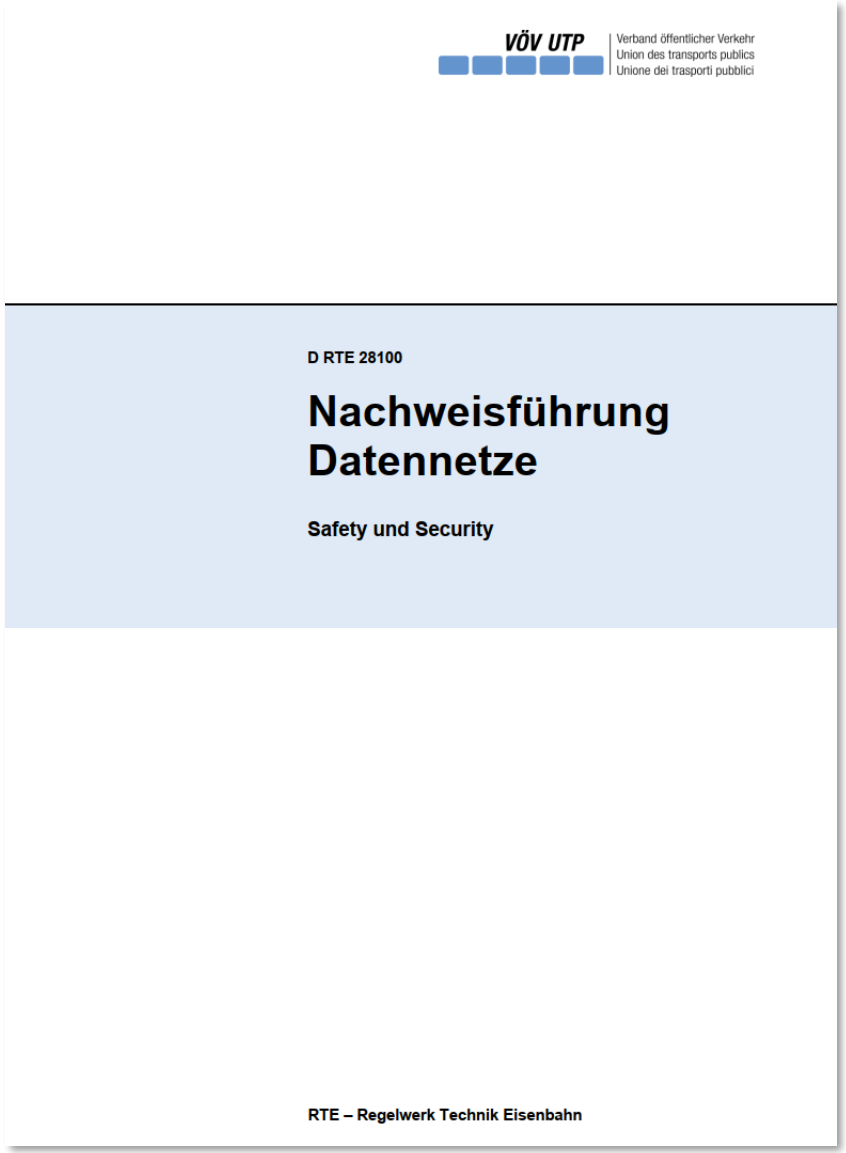
Ausgangslage für die D RTE 28100

An einem Workshop der Fachgruppe Elektrotechnik vom **16.01.2020** wurde u.a. festgestellt:

- Der **Ersatz** der bestehenden Datennetze steht bevor.
- Die **Trennung von abgeschlossenen Netzen** für sicherheitsrelevante Anwendungen wird schwieriger.
- Die **Sicherheitsanforderungen** an Datennetze für sicherheitsrelevante Anwendungen und deren Erfüllung sind unklar.
- Das **richtige Vorgehen** für die Ausschreibung, die Projektierung, die BAV-Zulassung und den Betrieb von Datennetzen ist unklar.
- Das BAV sieht klaren Handlungsbedarf.
- **Cybersecurity** ist ein Teil der notwendigen Anforderungen.

Was bietet die Regelung D RTE 28100?

- Sie zeigt, was beim Einsatz von Infrastruktur-Datennetzen bei Bahnunternehmen in Bezug auf **Safety** und **Security** zu beachten ist.
- Sie beschreibt, wie Bahnunternehmen ihre Datennetze projektieren und betreiben können, damit sie den **hoheitlichen Vorgaben** entsprechen.
- Die Inhalte sind auf dem neusten Stand der hoheitlichen Vorgaben und der **Normen**.



Struktur der Regelung D RTE 28100

Kapitel

- 1 Allgemeines
- 2 Grundlagen
- 3 Abkürzungen und Begriffe
- 4 Grundsätze (informativ)
- 5 Anforderungen an Datennetze (normativ)
- 6 Typenzulassungsverfahren für Datennetze (normativ)
- 7 Freigabeprozess für Datennetze (normativ)
- 8 Datennetzprojekte (informativ)
- 9 Bahnanwendungen (informativ)
- 10 Literatur

Anhänge (informativ)

- A1 Hoheitliche Vorgaben
- A2 Normen zu Safety und Security
- A3 CLC/TS 50701
- A4 SN EN 50159
- A5 Gebäudesicherheit für Safety und Security
- A6 Datennetz Datacom-NG von SBB

- Vorlagen V1 – V7

Kern der RTE 28100

Kapitel der D RTE 28100

Kap. 1 Allgemeines, Kap. 2 Grundlagen (Normen etc.), Kap. 3 Abkürzungen und Begriffe

Kap. 4 Grundsätze (informativ)

→ Datennetze und Anwendungen (4.3), IT und OT (4.4), Safety und Security (4.5)

Kap. 5 Anforderungen an Datennetze (normativ)

→ Anforderungskatalog mit 12 Unterkapitel und 48 Anforderungen

Kap. 6 Typenzulassungsverfahren für Datennetze (normativ)

→ Vereinfachte Typenzulassung für neue Infrastruktur-Datennetze

Kap. 7 Freigabeprozess für Datennetze (normativ)

→ Lifecycle-Prozess für Datennetze

Kap. 8 Datennetzprojekte (informativ)

Kap. 9 Bahnanwendungen (informativ)

Anhänge der D RTE 28100

A1 **Hoheitliche Vorgaben**: EBG, EBV, AB-EBV, RL CySec-Rail, RL TZL

A2 **Normen zu Safety und Security**

→ SN EN 50126-1/2, SN EN 50129, SN EN IEC 62443, SN EN ISO/IEC 27000

A3 CLC/TS 50701 Railway Applications – Cybersecurity

→ Einführung zu den Kapiteln und Anhängen

A4 SN EN 50159 Sicherheitsrelevante Kommunikation in Übertragungssystemen

→ Netzwerk-Kategorien, Bedrohungen und Schutzmassnahmen

A5 **Gebäudesicherheit für Safety und Security** (Schutzziele, Planung etc.)

A6 Datennetz Datacom-NG von SBB

→ Typenzulassung und Änderungsprozess zu Datacom-NG

Vorlagen V1 – V7 → «Liste der vorgesehenen Anwendungen» etc.

Anwendungen im Bahnumfeld (Kap. 4.3.1)

Sicherheitsrelevanz:
Eine Anwendung ist hoch sicherheitsrelevant oder nicht oder gering sicherheits-relevant.

Die Unterscheidung beruht auf dem Sicherheitsintegritätslevel (SIL):

- **SIL 1 bis SIL 4 → hoch sicherheitsrelevant**
- **Basisintegrität → nicht oder gering sicherheitsrelevant**

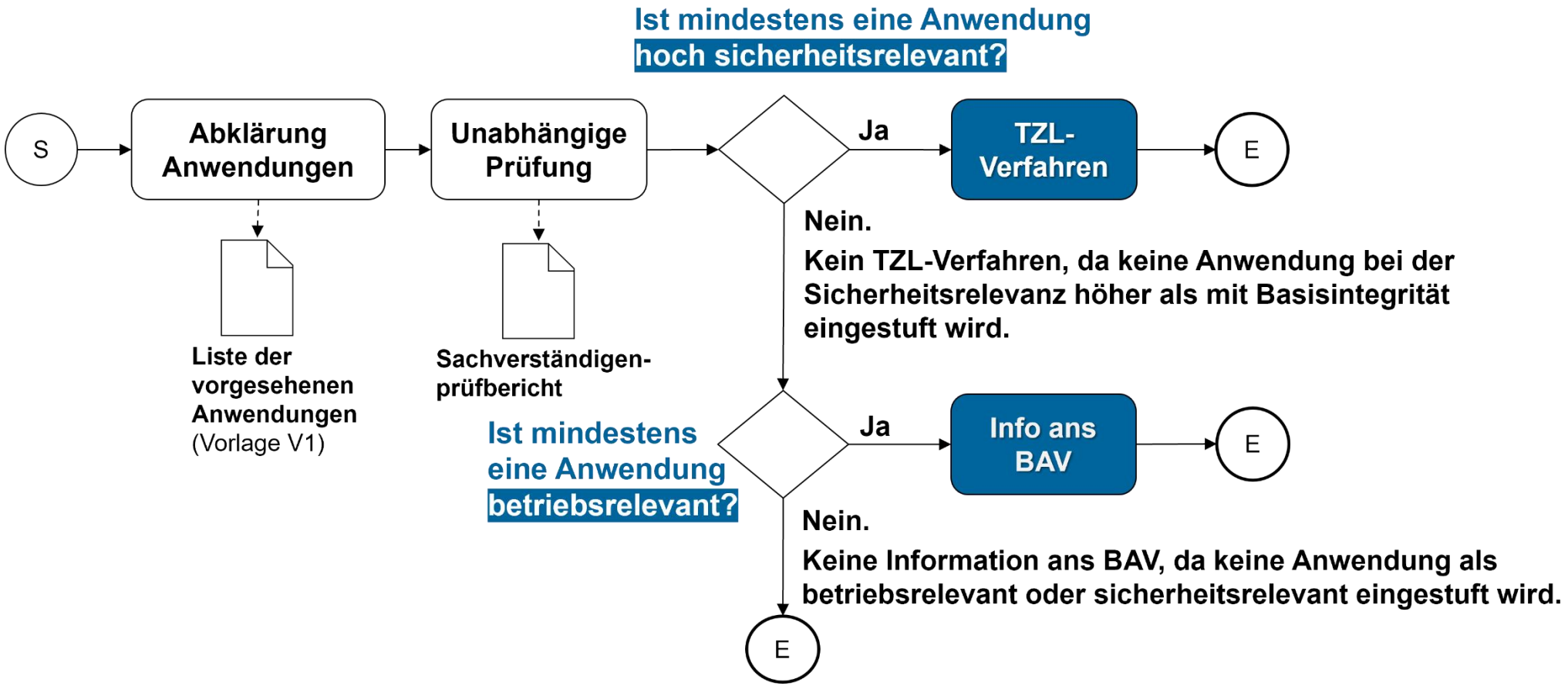
Betriebsrelevanz:
Eine Anwendung ist betriebsrelevant oder nicht betriebsrelevant.

«Betriebsrelevante Systeme oder Anlagen sind wichtig für die Aufrechterhaltung des Bahnbetriebes. Sie haben erhöhte Anforderungen an die Verfügbarkeit, um eine hohe Service- und Transportqualität für die Kunden zu gewährleisten», Kap. 3.2 Begriffe

Die Sicherheits- und Betriebsrelevanz der Anwendungen sind massgebend dafür, welches Verfahren gemäss der Regelung RTE 28100 durchgeführt werden soll.

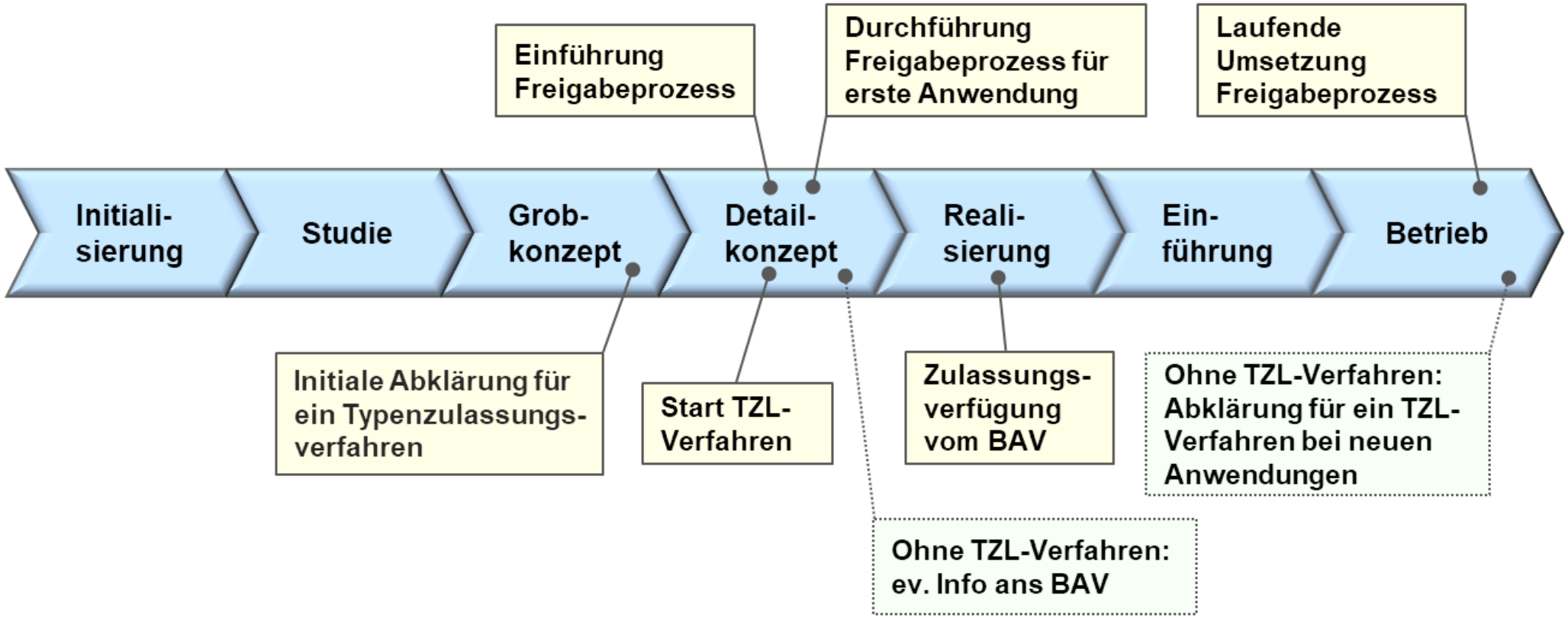
Anwendungen im Bahnumfeld

Abklärungsprozess vor einem Typenzulassungsverfahren (siehe Kap. 6):



Datennetzprojekte (Kap. 8)

Die klassische Projektmethodik ist geeignet, das Vorgehen bei einem Typenzulassungsverfahren aufzuzeigen.



Bahnanwendungen (Kap. 9)

Stellwerke

Funktionen:

- Sicherung von Rangierfahrstrassen
- Sicherung von Zugfahrstrassen

Sicherheitsrelevanz: bis zu SIL 4

Betriebsrelevant: Ja

Beispiele:

- elektronische Stellwerke (eStw)
- Relais-Stellwerke (RStw)

Beispiele für Anwendungsbedingungen aus der Bahnsicherungs- und Bahnleittechnik.

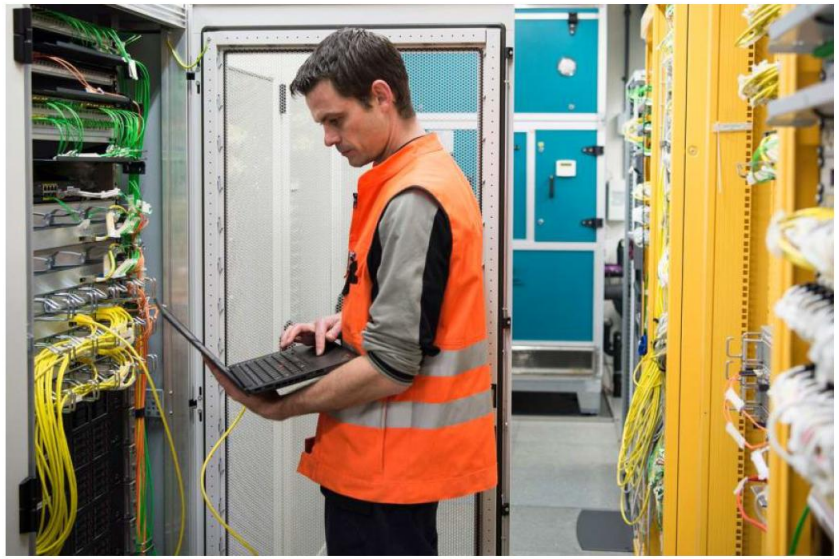
- Die Netzwerkverbindungen (LAN, WAN) innerhalb des Systems müssen den Voraussetzungen an ein **Netz der Kategorie 2** gemäss SN EN 50159 genügen.
- Das Netzwerk muss so ausgelegt sein, dass bei Auslastung im Rahmen der zugesicherten Bandbreite die **Latenzzeit** von max. 25 ms zwischen beliebigen Access-Ports eingehalten wird.

D RTE 28100: Einführung

Besten Dank.

Nachweisführung Datennetze

Safety und Security



Fragen

Getränke und Zwischenverpflegung im Foyer
Bitte um 10:55 wieder Platz nehmen, nächstes Referat beginnt um 11:00

Programm Vormittag

11 Uhr	**Inhalte RTE-Regelung** **D RTE 28100 Nachweisführung Datennetze**
11 Uhr	Anforderungen RTE Kap. 5 (Hoher Security-Anteil, Knackpunkte, Praktische Anwendung inkl. V7 ggf. mit AB-Bsp.) Markus Roth, Emmerich Horvath, Kurt Maier
11:15 Uhr	Typenzulassungsverfahren RTE Kap. 6 Freigabeprozess RTE Kap. 7 mit entsprechenden Vorlagen Patrick Favre, Kurt Maier
11:45 Uhr	Offene Fragen Dr. Robert Leemann
12 Uhr	**Mittagessen**

VÖV UTP
Verband öffentlicher Verkehr
Union des transports publics
Unione dei trasporti pubblici

D RTE 28100, Anforderungen an Datennetze

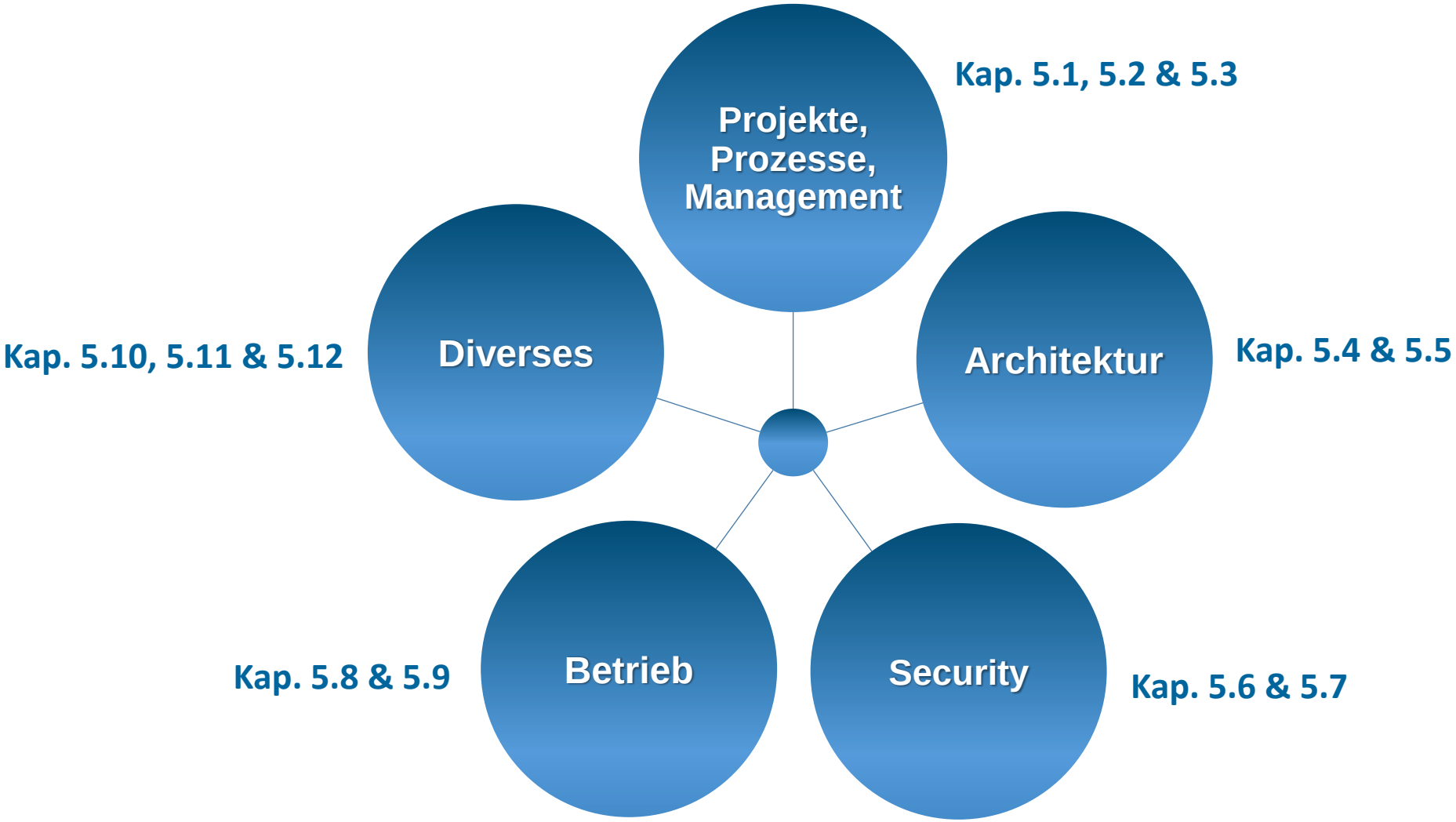
Emmerich Horvath, Markus Roth, Kurt Maier

Bern, Mittwoch, 11.12.2024

Anforderungen an Datennetze (Kap. 5)

VÖV UTP

Unterteilung von Kap. 5

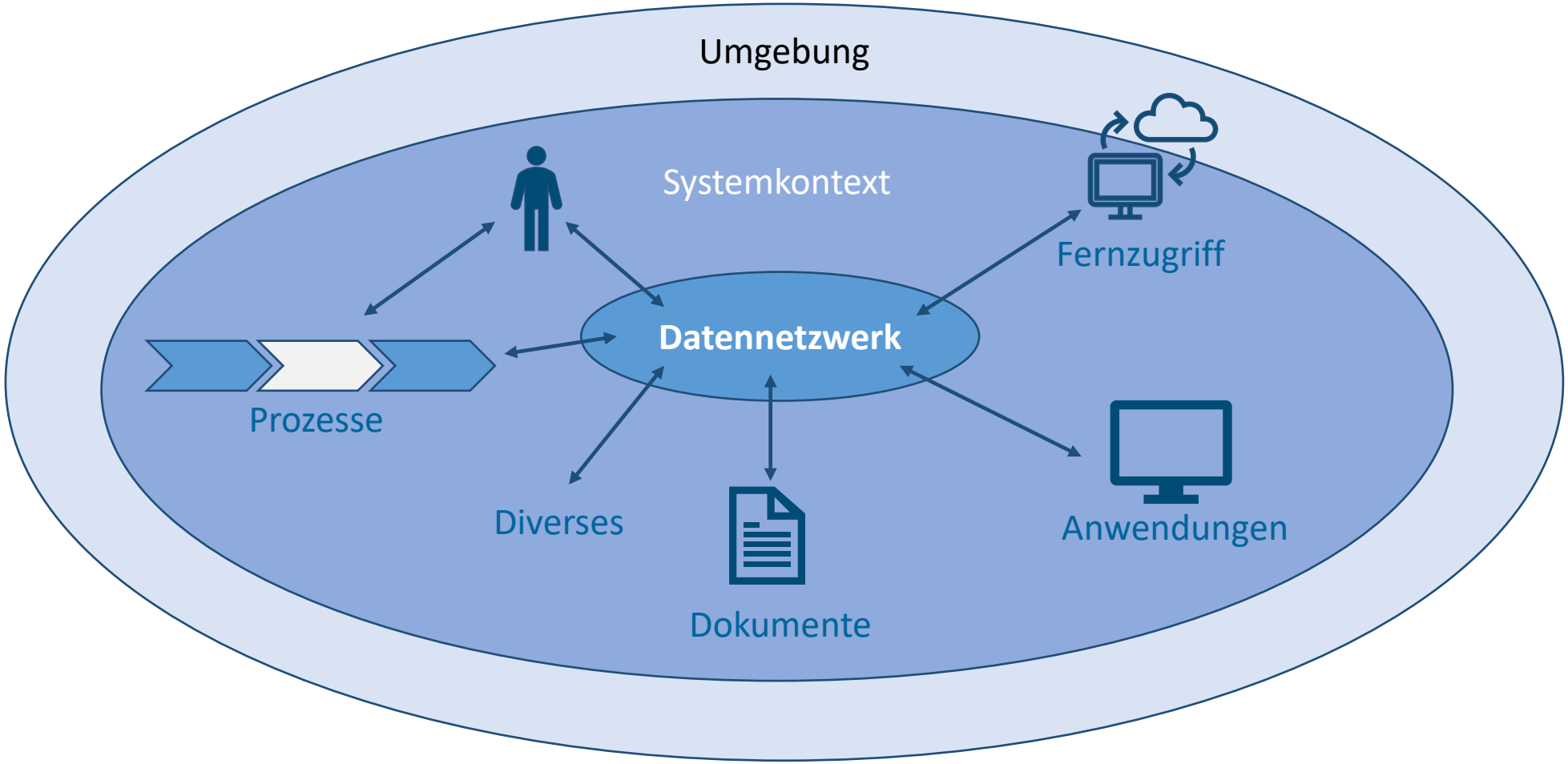


Unterteilung der Anforderungen

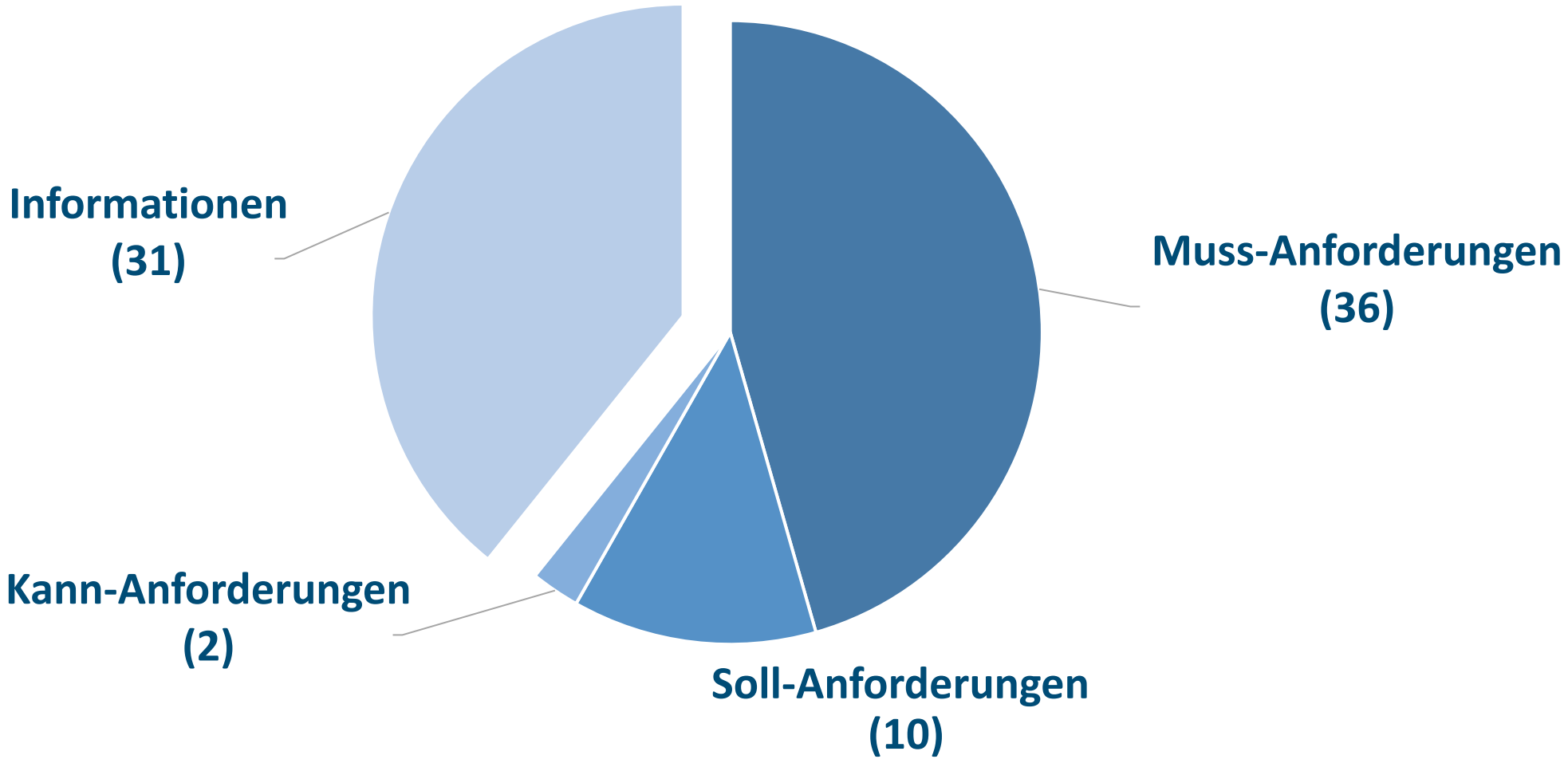
Kap. 5.1	Projektanforderungen zu Safety	**Projekte, Prozesse, Management**
Kap. 5.2	Projektanforderungen zu Security	
Kap. 5.3	Information Security Management System (ISMS)	
Kap. 5.4	Anforderungen an die Architektur und Zonierung	**Architektur**
Kap. 5.5	Redundanzen und Verfügbarkeit	
Kap. 5.6	Anforderungen an Security-Risikoanalysen	**Security**
Kap. 5.7	Minimaler Target Security Level nach CLC/TS 50701	
Kap. 5.8	Anforderungen an die System-Administration und -Konfiguration	**Betrieb**
Kap. 5.9	Anforderungen an das Betriebskonzept des Datennetzes	
Kap. 5.10	Anforderungen an die Dokumentation	**Diverses**
Kap. 5.11	Anforderungen an Sachverständige	
Kap. 5.12	Anforderungen an die Gebäudesicherheit	

D RTE 28100: Anforderungen an Datennetze

Anforderungen: System, Systemkontext, Umgebung



Kategorisierung der Anforderungen in Kap. 5



Kategorisierung der Anforderungen in Kap. 5

Muss-Anforderungen (M) sind bei der Anwendung der D RTE 28100 umzusetzen.

Soll-Anforderungen (S) betreffen wichtige Anliegen, müssen aber nicht in jedem Fall umgesetzt werden. Sie werden risikobasiert behandelt.

Kann-Anforderungen (K) können erfüllt werden, soweit es die Umstände und Ressourcen zulassen.

Informationen (I) sind Ergänzungen zu den Anforderungen.

Kennzeichnung der Anforderungen

Kennzeichnung Rx.y
R steht für **R**equirement bzw. Anforderung,
x entspricht der Nummerierung des **Unterkapitels 5.x**,
y für die **fortlaufende Nummerierung** innerhalb eines Unterkapitels.

5.1 Projektanforderungen zu Safety

(M, R1.1) Die Safety muss von Anfang an in der Projektierung eines Datennetzwerks berücksichtigt werden, falls das Datennetz auch für hoch sicherheitsrelevante Anwendungen vorgesehen ist (Sicherheitsfunktionen mit SIL 1 bis SIL 4).

(M, R1.2) Die Rollen und Verantwortlichkeiten bezüglich Safety sind zu klären. Der Einsatz eines Datennetzes im Umfeld von hoch sicherheitsrelevanten Anwendungen erfordert seitens der ISB fundiertes und detailliertes Fachwissen sowohl in Bezug auf das Datennetz als auch auf die Anwendungen. Bei fehlendem Fachwissen bezüglich Safety sind frühzeitig Massnahmen einzuleiten.

(M, R1.3) Ein Typenzulassungsverfahren gemäss dieser RTE-Regelung wird durchgeführt, wenn die Bedingungen dies verlangen (siehe Abschnitt 6.3.1).

Beispiel: (M, **R1.1**)
→ im Kap. **5.1** die **1. Anforderung** (Muss-Anforderung)

Excel-Vorlage D-RTE-28100-V7

ISB (Abk.) / ISB (vollständige Bezeichnung)

Anforderungen an Datennetze gemäss D RTE 28100, Kapitel 5

Datennetzprojekt

Nicht jede M- oder S-Anforderung muss einzeln behandelt werden. Es kann auch pro Unterkapitel von Kapitel 5 eine Stellungnahme erfolgen. (ev. mit einzelnen Ergänzungen bei den Anforderungen)

Typ	Anforderungstext aus Kapitel 5	Situation, Risiken, Massnahmen, Umsetzung	Status	Kommentar / Ergänzungen
T	**5.1 Projektanforderungen zu Safety**			
M	(M, R1.1) Die Safety muss von Anfang an in der Projektierung eines Datennetzwerks berücksichtigt werden, falls das Datennetz auch für hoch sicherheitsrelevante Anwendungen vorgesehen ist (Sicherheitsfunktionen mit SIL 1 bis SIL 4).			
M	(M, R1.2) Die Rollen und Verantwortlichkeiten bezüglich Safety sind zu klären. Der Einsatz eines Datennetzes im Umfeld von hoch sicherheitsrelevanten Anwendungen erfordert seitens der ISB fundiertes und detailliertes Fachwissen sowohl in Bezug auf das Datennetz als auch auf die Anwendungen. Bei fehlendem Fachwissen bezüglich Safety sind frühzeitig Massnahmen einzuleiten.			
M	(M, R1.3) Ein Typenzulassungsverfahren gemäss dieser RTE-Regelung wird durchgeführt, wenn die Bedingungen dies verlangen (siehe Abschnitt 6.3.1).			
M	(M, R1.4) Die Einhaltung der Anwendungsbedingungen der sicherheitsrelevanten Anwendungen an das Datennetz muss gewährleistet werden. Für den Nachweis dient unter anderem der Freigabeprozess, wie er in dieser RTE-Regelung definiert ist.			

Anforderungen zu Safety und Security

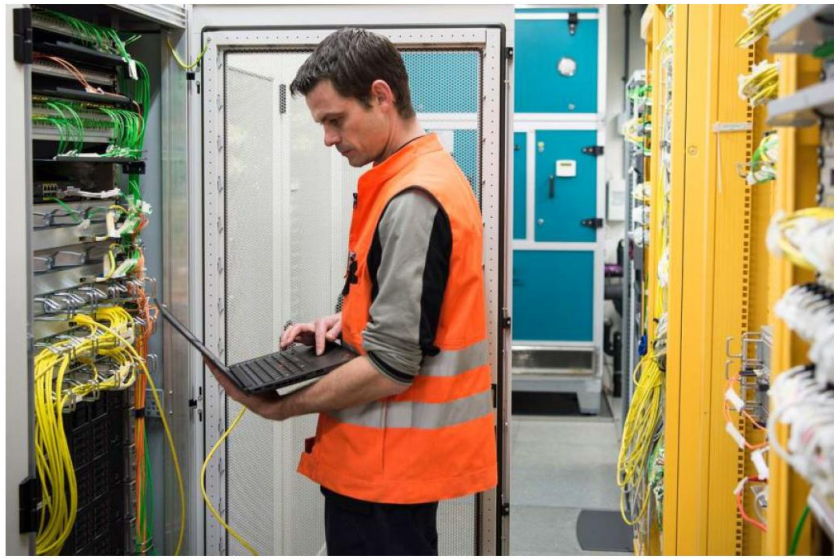
- Die Anforderungen beziehen sich auf Datennetze, mit denen betriebsrelevante und hoch sicherheitsrelevante Bahnanwendungen vernetzt werden.
- Die Anforderungen weisen den Weg, ohne jedes Detail vorzugegeben.
- Für die Bearbeitung der Anforderungen von Kap. 5 gibt es die Excel-Vorlage D-RTE-28100-V7.
- **Die Verantwortung bei der Beurteilung und Umsetzung der Anforderungen liegt in jedem Fall bei den ISB.**

D RTE 28100: Anforderungen an Datennetze

Besten Dank.

Nachweisführung Datennetze

Safety und Security



VÖV UTP
Verband öffentlicher Verkehr
Union des transports publics
Unione dei trasporti pubblici

D RTE 28100, Typenzulassung und Freigabeprozess, 1. Teil

Kurt Maier, Patrick Favre

Bern, Mittwoch, 11.12.2024

Typenzulassung (Kap. 6)

Inhalt 1. Teil:

- Warum eine Typenzulassung?
- Nicht in jedem Fall ist eine Typenzulassung notwendig
- Liste der vorgesehenen Anwendungen
- Vorgehen für Typenzulassungsverfahren
- Vorgehen für Information ans BAV
- Fall ohne Interaktion mit dem BAV
- Regelmässige Informationen an das BAV

Warum eine Typenzulassung?

Für die Genehmigung von Datennetzen wurden zwei mögliche Verfahren mit unterschiedlichen Eigenschaften gegenübergestellt:

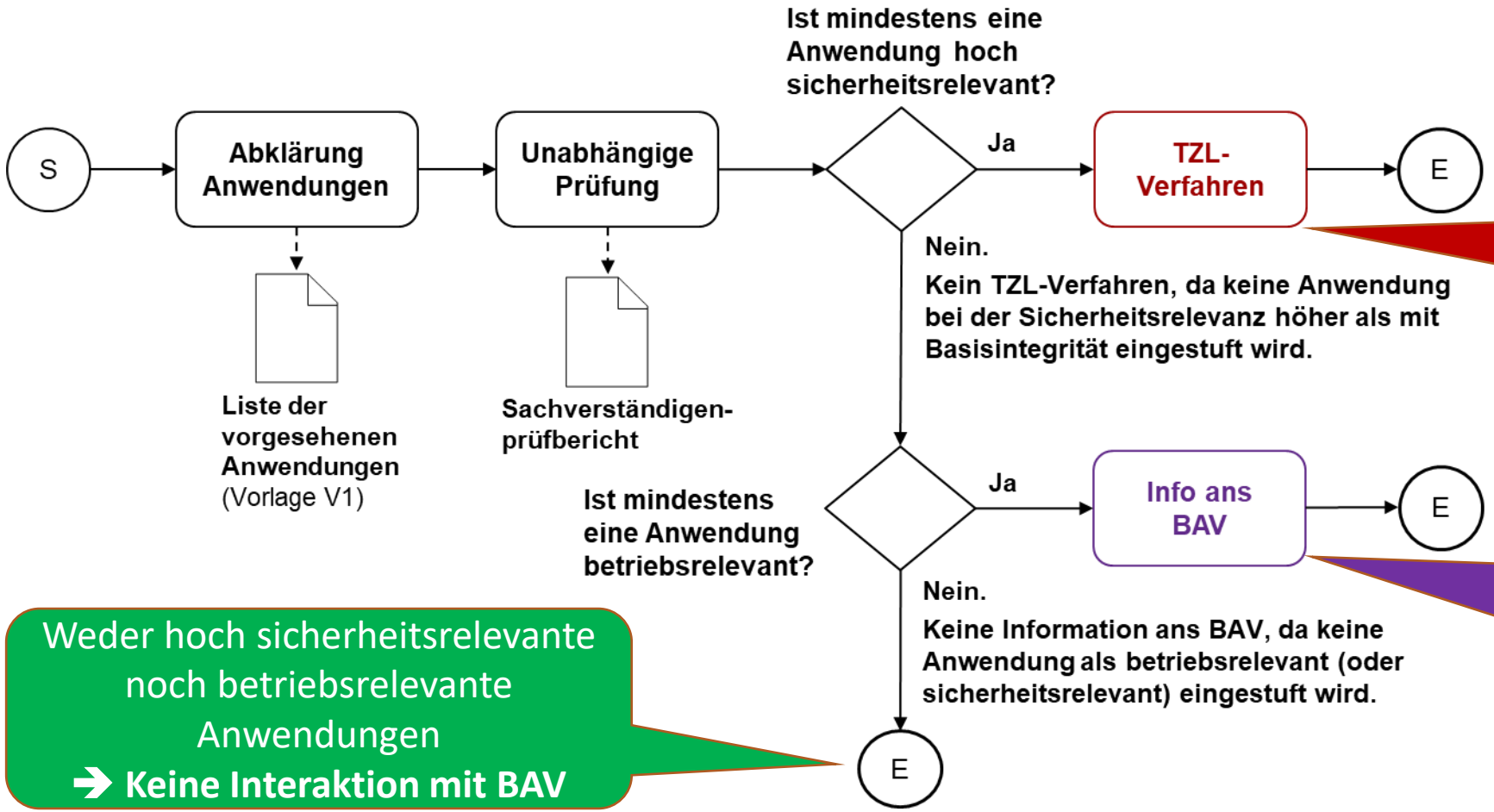
Generisches PGV	TZL
Ein PGV pro ISB und Datennetzwerk	Eine TZL pro ISB und Datennetzwerk
1:1 gemäss den hoheitlichen Vorgaben	Interpretation der hoheitlichen Vorgaben
Passt nicht wirklich zum Bild eines klassischen PGV, es braucht eine «neue Art PGV»	Wenig formalistisch, sehr flexibel, dynamisch
	Wurde bis jetzt für Datennetze angewendet

➔ Die Variante TZL wurde auf Grund ihrer Flexibilität und Einfachheit gewählt.

BEMERKUNG: In der neuen Richtlinie «Sicherheitsnachweisführung Sicherungsanlagen» wird wahrscheinlich für Systeme ohne hohe Sicherheitsrelevanz mit einem speziellen PGV operiert.

Nicht in jedem Fall ist eine TZL notwendig

➔ **Massgebend sind die Anwendungen**, die über das Datennetz vernetzt werden ➔



Min. eine Anwendung ist hoch sicherheitsrelevant
➔ **TZL-Verfahren**

Keine Anwendung ist hoch sicherheitsrelevant, min. eine Anwendung ist betriebsrelevant
➔ **Info ans BAV**

Weder hoch sicherheitsrelevante noch betriebsrelevante Anwendungen
➔ **Keine Interaktion mit BAV**

Liste der vorgesehenen Anwendungen (Vorlage V1)

- In dieser Liste werden alle Anwendungen, die an das Datennetz angeschlossen werden, erfasst und nach ihrer Sicherheits- und Betriebsrelevanz bewertet.
- Nach der Erstellung ist die Liste durch einen Sachverständigen prüfen zu lassen.
- Die Liste wird während des ganzen Lebenszyklus des Datennetzes gepflegt.

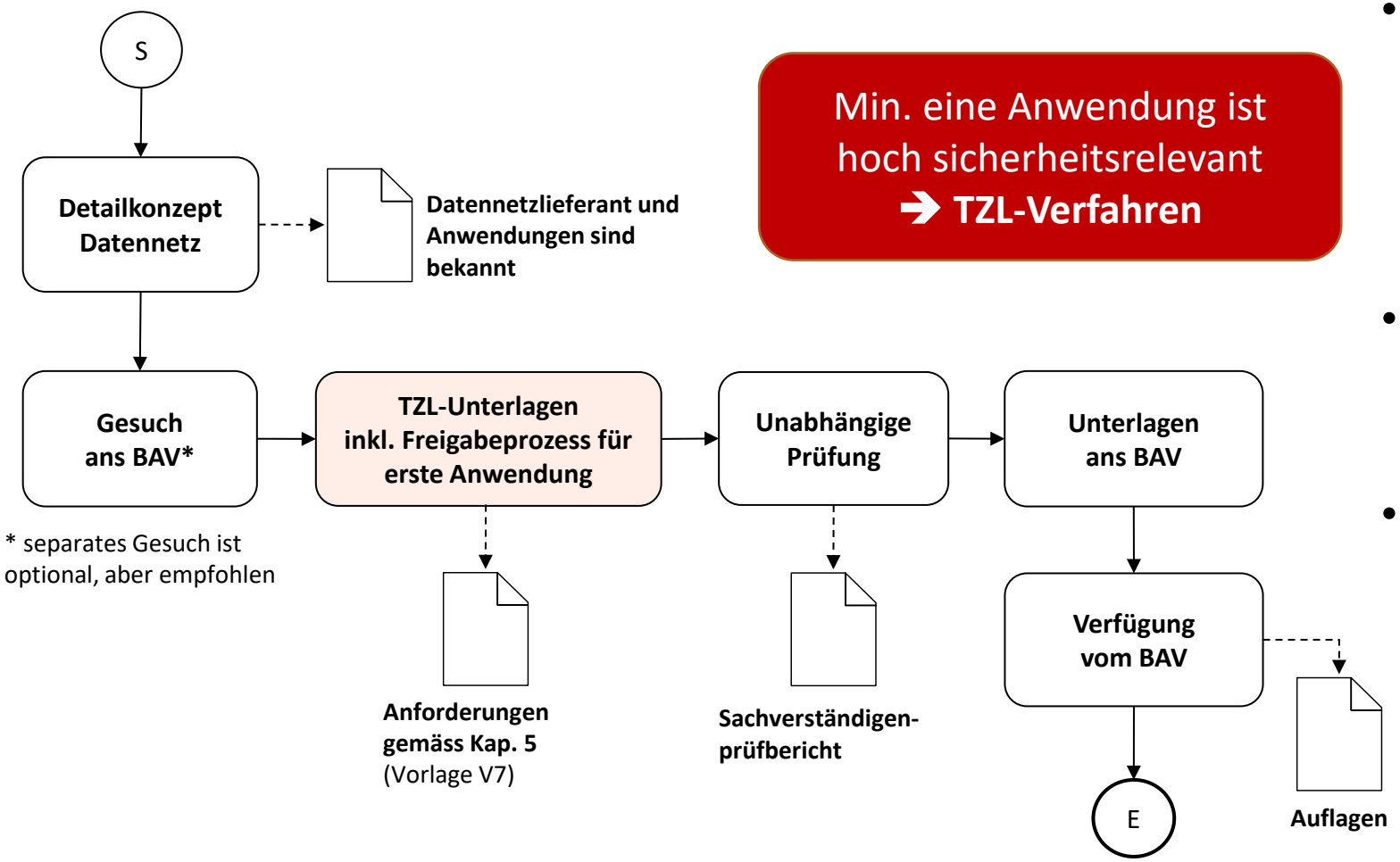
Liste der vorgesehenen Anwendungen ISB-Logo einfügen
ISB (Abk.) / ISB (vollständige Bezeichnung)
Datennetzprojekt

2. Vorgesehene Anwendungen

In der folgenden Tabelle werden die Anwendungen erfasst, die auf das Datennetz aufgeschaltet werden sollen.

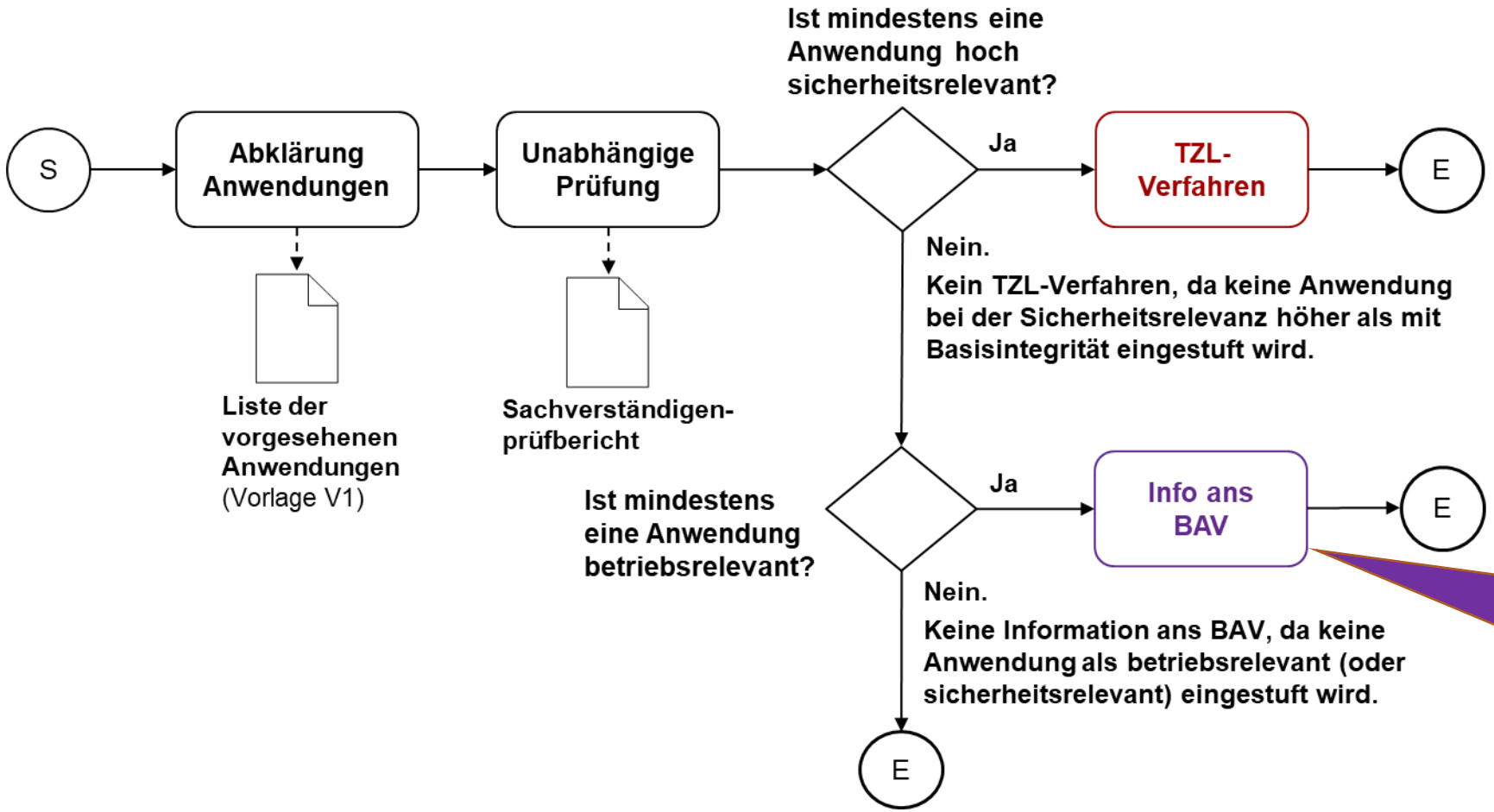
Anwendung	Version (Major)	Lieferant	Funktion, Einsatzgebiet, Eigenschaften	Kategorie EN 50159 [Kat. n, -]	Sicherheitsrelevant? [SIL n, BI]	Betriebsrelevant? [Ja, Nein]
Leit- und Informationssystem			Bahnleittechnik	Kat. 2	SIL 2	Ja
RCI			Bahnleittechnik, Fernübertragung zu RStw	Kat. 2	SIL 2	Ja
rcs95			Bahnleittechnik, Fernübertragung zu RStw	Kat. 1	SIL 2	Ja
Elektra 2 (CC) – Elektra 2 (EC)			Stw-Stw-Verbindung zu abges. Standort	Kat. 1	SIL 4	Ja
Elektra 2 (CC) – Elektra 2 (CC)			Stw-Stw-Verbindung zu Nachbar-Stw	Kat. 2	SIL 4	Ja
VBBa			Bahnleittechnik, Stellwerkfernsteuerung	Kat. 1	SIL 2	Ja
Anzeige KIS			Kundeninformationssystem	-	BI	Ja
Billettautomaten				-	BI	Nein
Datencenter			Rechencenter	-	BI	Ja
Diagnose-Systeme				-	BI	Nein
Digitale Signale				-	BI	Nein
Energieüberwachung				-	BI	Ja

Vorgehen für Typenzulassungsverfahren



- Für eine repräsentative, **hoch sicherheitsrelevante Anwendung**, weist der ISB nach, dass sie sicher auf dem Datennetz aufgeschaltet werden kann.
- Der ISB zeigt auch, dass er die **dazu notwendigen Prozesse im Unternehmen implementiert** hat
- Nach der Erteilung der TZL darf der ISB mittels des implementierten Freigabeprozesses ohne Genehmigung des BAV neue Anwendungen auf dem Datennetz aufschalten.

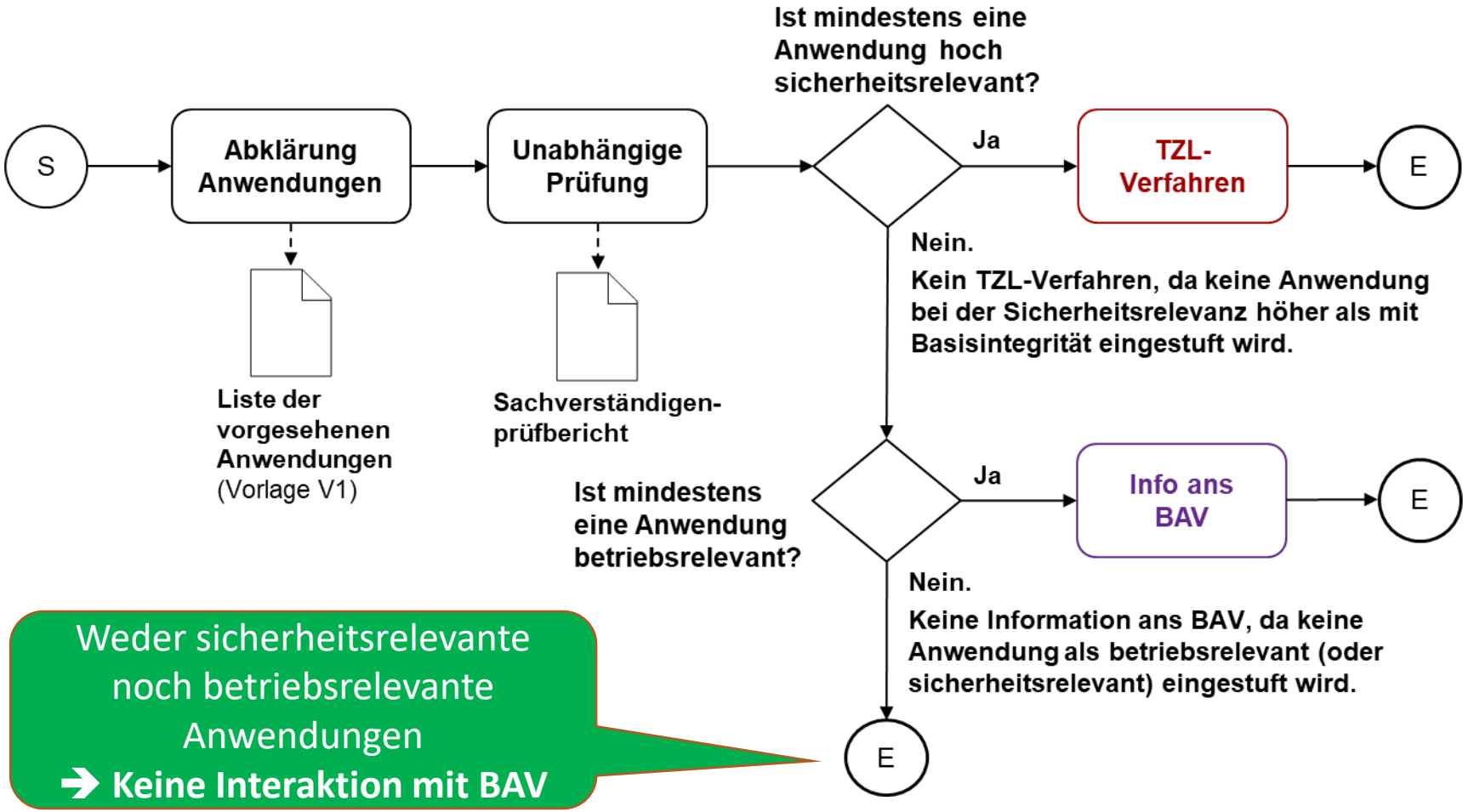
Vorgehen für Information ans BAV (ohne Verfahren)



- Beim Anschluss weiterer Anwendungen läuft dieser Prozess nochmals durch

Keine Anwendung ist hoch sicherheitsrelevant,
min. eine Anwendung ist betriebsrelevant
➔ **Info ans BAV**

Fall ohne Interaktion mit dem BAV



Weder sicherheitsrelevante noch betriebsrelevante Anwendungen
➔ **Keine Interaktion mit BAV**

- Auch wenn das BAV nicht involviert ist, muss die Dokumentation seitens ISB abgelegt werden.
- Beim Anschluss weiterer Anwendungen läuft dieser Prozess nochmals durch.

Aktivitäten im Lebenszyklus des Datennetzes

In den Fällen, in welchen eine TZL verfügt wurde:

- **Jährliche Updates** zum Freigabeprozess sind dem BAV zu schicken (Liste der freigegebenen Anwendungen und Liste der freigegebenen Netzänderungen).
- **Bei relevanten Anpassungen** an den aufgeschalteten Anwendungen und am Datennetz selbst muss jeweils der **Freigabeprozess durchlaufen** werden.

In allen anderen Fällen:

- Wenn eine Information an das BAV erfolgt ist, wird ihm als **jährliches Update** die aktuelle «Liste der vorgesehenen Anwendungen» zugestellt.
- **Bei relevanten Anpassungen** an den aufgeschalteten Anwendungen muss der **Abklärungsprozess erneut gestartet** werden. Eventuell ist eine nachträgliche TZL oder eine Information an das BAV nötig.

VÖV UTP
Verband öffentlicher Verkehr
Union des transports publics
Unione dei trasporti pubblici

D RTE 28100: Typenzulassung und Freigabeprozess, 2. Teil

Kurt Maier

Bern, Mittwoch, 11.12.2024

D RTE 28100: Konzept Freigabeprozess

- Wenn **hoch sicherheitsrelevante Anwendungen** auf ein Datennetz geschaltet werden, sind nicht akzeptable Safety- und Security-Risiken zu vermeiden.
- Es ist systematisch zu prüfen, ob das Datennetz bezüglich Safety und Security die **Anwendungsbedingungen** (AWB) einer hoch sicherheitsrelevanten Anwendung einhalten kann.
- Mit dem **Freigabeprozess** wird geprüft und dokumentiert, dass die Anforderungen ans Datennetz **während des ganzen Lifecycles** eingehalten werden.
- Es gibt zwei separate Prozesse:
  - Prozess für hoch sicherheitsrelevante Anwendungen mit drei Startpunkten
  - Prozess für Änderungen am Datennetz mit einem Startpunkt

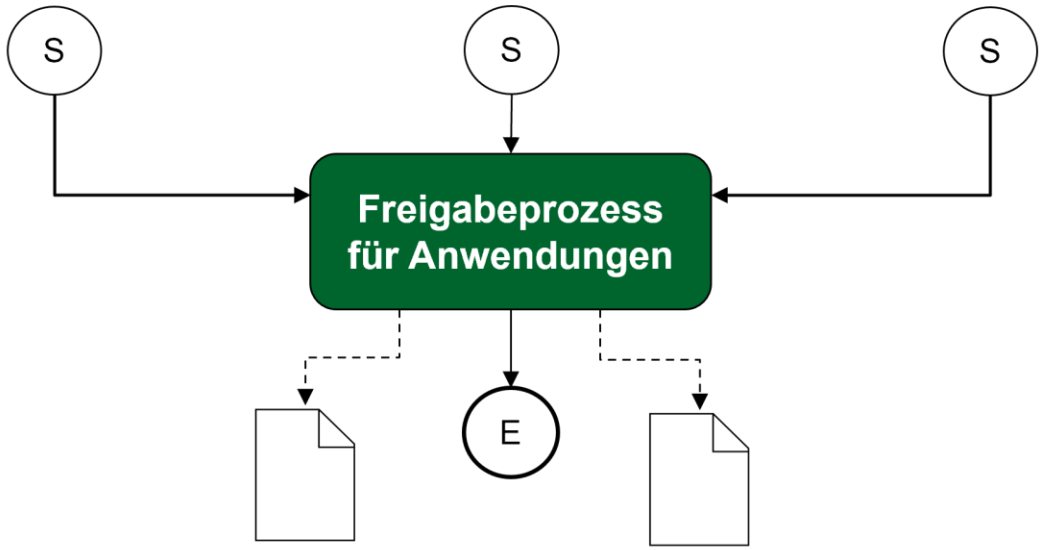
Startpunkte/Anwendungsfälle Freigabeprozess

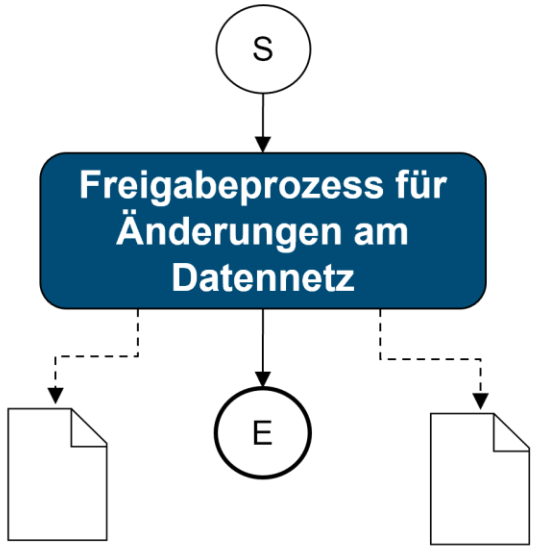
Migration einer bestehenden, hoch sicherheitsrelevanten Anwendung

Aufschaltung einer neuen, hoch sicherheitsrelevanten Anwendung

Neuer Release einer hoch sicherheitsrelevanten Anwendung

Anpassung oder Änderung am Datennetz





Freigabeprozess-dokumente pro Anwendung

→ **Vorlagen V4, V5, V6**

Liste der freigegebenen Anwendungen

→ **Vorlage V2**

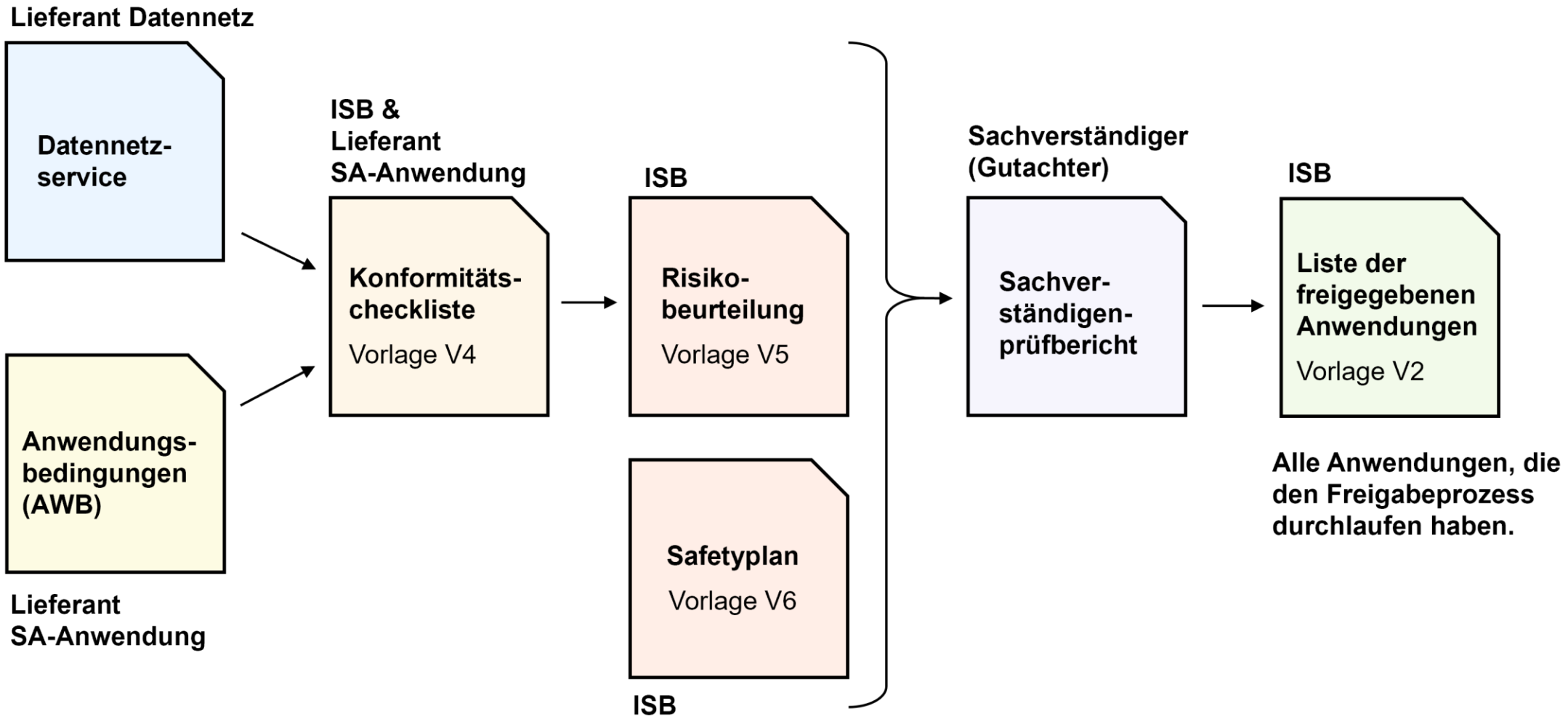
Freigabeprozess-dokumente pro Änderung

(keine Vorlagen)

Liste der freigegebenen Netzänderungen

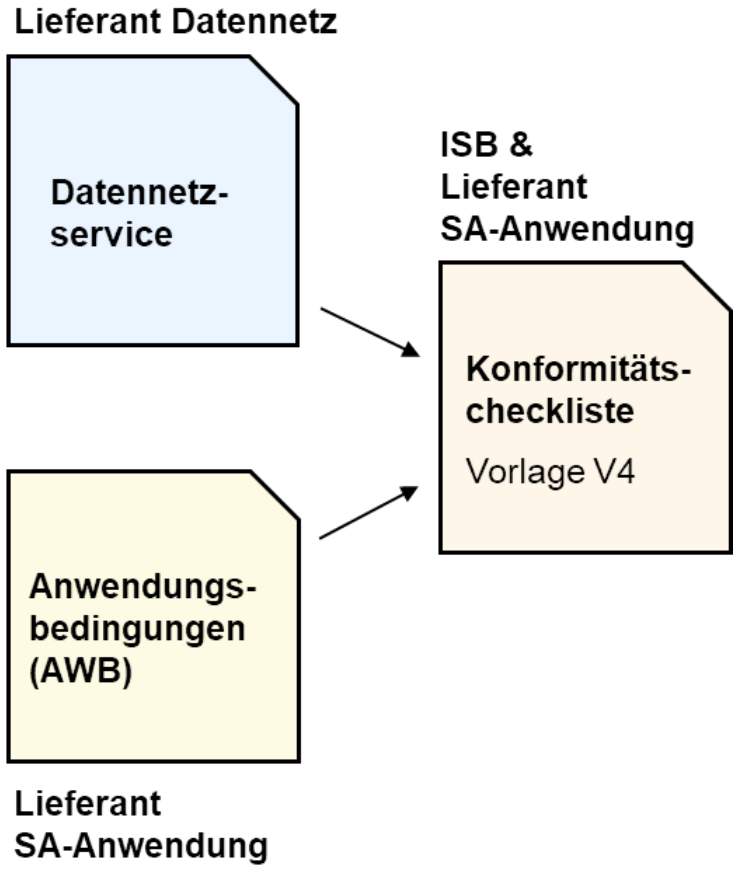
→ **Vorlage V3**

Freigabeprozess für Anwendungen



Konformitätscheckliste

- Mit der Konformitätscheckliste wird geprüft, ob im **Zusammenspiel von Datennetz** und **einer bestimmten sicherheitsrelevanten Anwendung** die AWB bekannt sind und eingehalten werden können.
- Die Konformitätscheckliste schafft einen Überblick zu den **Eigenschaften, Einschränkungen und Grenzen einer Anwendung** im Zusammenhang mit einem Datennetz.
- Die Konformitätscheckliste wird vom **ISB zusammen mit dem Lieferanten der Anwendung** erstellt.
- Für die Konformitätscheckliste gibt es die Vorlage D-RTE-28100-V4. Die Vorlage enthält eine **Tabelle zur Anwendungsübersicht** und eine **Checkliste zu den Bedrohungen gemäss SN EN 50159**.



Konformitätscheckliste, Vorlage V4

2.1. Anwendungseigenschaften

Der Hersteller/Lieferant hat die Angaben in der folgenden Tabelle zu überprüfen. Komm
oder Korrekturen können in die Tabelle oder in das Kap. 2.2 geschrieben (highlighten o
Änderungsmodus).

Merkmal	Eigenschaft/Wert	Bemerkung/Bewertung
Identifikation		
Anwendung	Leit- und Informationssystem	
Systemversion		
Anwendungsgruppe	Bahnleittechnik	
Verbindungstyp		
Verbindung auf Systemebene		
SIL-Zuordnung	SIL 2	
Typenzulassung		
Planungs- / Betriebsstatus	Geplant / in Prüfung / in Betrieb	
Kommunikationssystem der Anwendung		
Übertragungsprotokoll	proprietär	
Protokoll auf OSI-Layer 4	TCP	
Protokoll auf OSI-Layer 3	IP	
Protokoll auf OSI-Layer 2/1	Ethernet	
Konformität EN 50159		
Kategorie-Tauglichkeit gemäss EN 50159 [1]	Kategorie1 / Kategorie 2	
Hersteller-Nachweis EN 50159		

3. Checkliste

Der Hersteller/Lieferant hat die Checkliste in diesem Kapitel auszufüllen. Bemerkungen können in das Kap. 3.8 geschrieben werden.

Checkbox ist markiert. = Der Punkt ist erfüllt.
Checkbox ist nicht markiert. = Der Punkt trifft nicht zu.

3.1. Bedrohung durch «Wiederholung» nach EN 50159

☐ Das Datennetz darf eine beliebige Anzahl von Wiederholungen erzeugen, da diese von den Schutzmassnahmen der Anwendung abgefangen werden können.

→ Es existieren gegen diese Bedrohung keine AWB an das Netz.

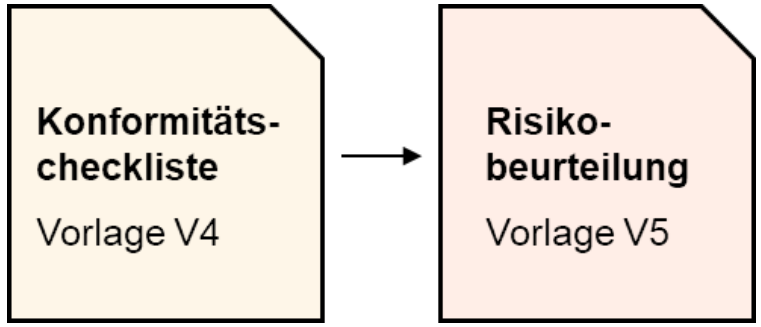
oder

☐ Gegen die Bedrohung «Wiederholung» gibt es Anwendungsbedingungen oder Einschränkungen für das Datennetz:

- AWB bzw. maximaler Grenzwert: .....

Risikobeurteilung

- Die Risikobeurteilung soll zeigen, dass die **AWB**, die mit der Konformitätscheckliste erfasst wurden, durch das Datennetz erfüllt werden können.
- Im Rahmen der Risikobeurteilung erfolgt auch die Bewertung der **IT-Security**.
- Für die Risikobeurteilung gibt es die Vorlage D-RTE-28100-V5.



2.2. Erfüllung der Anforderungen

Im Folgenden sind die Anforderungen bzw. AWB und deren Erfüllung durch das Datennetz aufgeführt.

AWB / ID	(Teil-)Anforderung	Bemerkung	Erfüllt?
[AWB 1]			
[AWB 2]			
V_Netzw_01	**Voraussetzungen an das Übertragungssystem**		
V_Netzw_01.A	Die Übertragungsqualität von LAN und WAN muss …		
V_Netzw_01.B	Das Übertragungssystem stellt genügend Bandbreite bereit.		
S_System_03	**EN50159 – Konformitätsnachweis**		
S_System_03.A	Die Netzwerkverbindungen (LAN, WAN) müssen entweder - den Voraussetzungen an ein Netz der Kategorie 1 gemäss EN 50159 genügen oder		
S_System_03.B	den Voraussetzungen an ein Netz der Kategorie 2 gemäss EN 50159 mit folgender Einschränkung genügen: …		

2.3. Konflikte

Konflikte ergeben sich, wenn Anforderungen nicht (vollständig) erfüllt werden können. Anhand der Detailanforderungen in Kap. 2.2 ergeben sich die folgenden Konflikte.

Nr.	ID der Teilanforderung	Problem bei der Erfüllung	Bedrohung
1	S_System_03.B	Durch technische oder menschliche Fehler (Übersprechen, Falschkonfiguration, usw.) kann es dazu kommen, dass Kommunikation mit andern als den vorgesehenen Rechnern erfolgt.	Einfügung
2			

Safetyplan

- Im Safetyplan werden die Projektinhalte, die betroffenen Anlagen, die Rollen und Verantwortlichkeiten beschrieben.
- Für den Safetyplan gibt es die Vorlage D-RTE-28100-V6.
- Kapitel 3 «Gewährleistung der Sicherheit» der Vorlage V6 umfasst diverse Checkpunkte:
  - Risikobeurteilung
  - Spezifikationsreife und Produktzulassung
  - Produkthandhabung
  - Verifizieren der Dokumente

Safetyplan

Vorlage V6

3.1. Risikobeurteilung

Nr.[1]	Fragestellung		
1	Aus der Risikobeurteilung [9] ergeben sich sicherheitsrelevante Anforderungen oder Massnahmen. Falls Ja: Detailbeschrieb	☐ Ja	☐ Nein

3.2. Spezifikationsreife und Produktzulassung

Die folgenden Checkpunkte zeigen auf, ob Spezifikationsreife und Produktzulassung gegeben sind. Falls nicht alle Punkte mit Ja (=OK) bewertet werden können, ist aufzuzeigen, wie die Spezifikationsreife und die Produktzulassung erreicht werden sollen.

Nr.	Fragestellung	OK	Nicht OK
2	Das Vorhaben betrifft ausschliesslich typenzugelassene Produkte der Sicherungsanlage. Typenzulassungsreferenz BAV: – TZL 512 04 01	☐ Ja	☐ Nein
3	Die Spezifikationsreife ist gegeben, da entweder keine oder nur solche – technischen Funktionalitäten, – Projektierungsmöglichkeiten, – Betriebsprozesse, verwendet werden, die entweder – explizit im Rahmen einer Generischen Anwendung auf der Basis eines Sicherheitsnachweises bei der ISB zugelassen wurden oder – sich bereits in mehrjähriger und breiter Anwendung bei der ISB bewährt haben.	☐ Ja	☐ Nein

Sachverständigenprüfbericht

- Der Sachverständige prüft vor der Inbetriebnahme der Anwendung die Dokumente und die Begründungen für die Einhaltung der Anwendungsbedingungen.
- Erst wenn die allfälligen Auflagen aus dem Sachverständigenprüfbericht erfüllt bzw. berücksichtigt werden, ist die Freigabe der Anwendung auf dem Datennetz gestattet.
- Ein Sachverständigenprüfbericht wird erstellt
  - bei der Abklärung vor einem Typenzulassungsverfahren
  - vor der Einreichung der Typenzulassungsunterlagen
  - **im Ablauf des Freigabeprozesses**
  - bei der nachträglichen Aufschaltung weiterer Anwendungen
- Für den Sachverständigenprüfbericht gibt es keine Vorlage.

Liste der freigegebenen Anwendungen

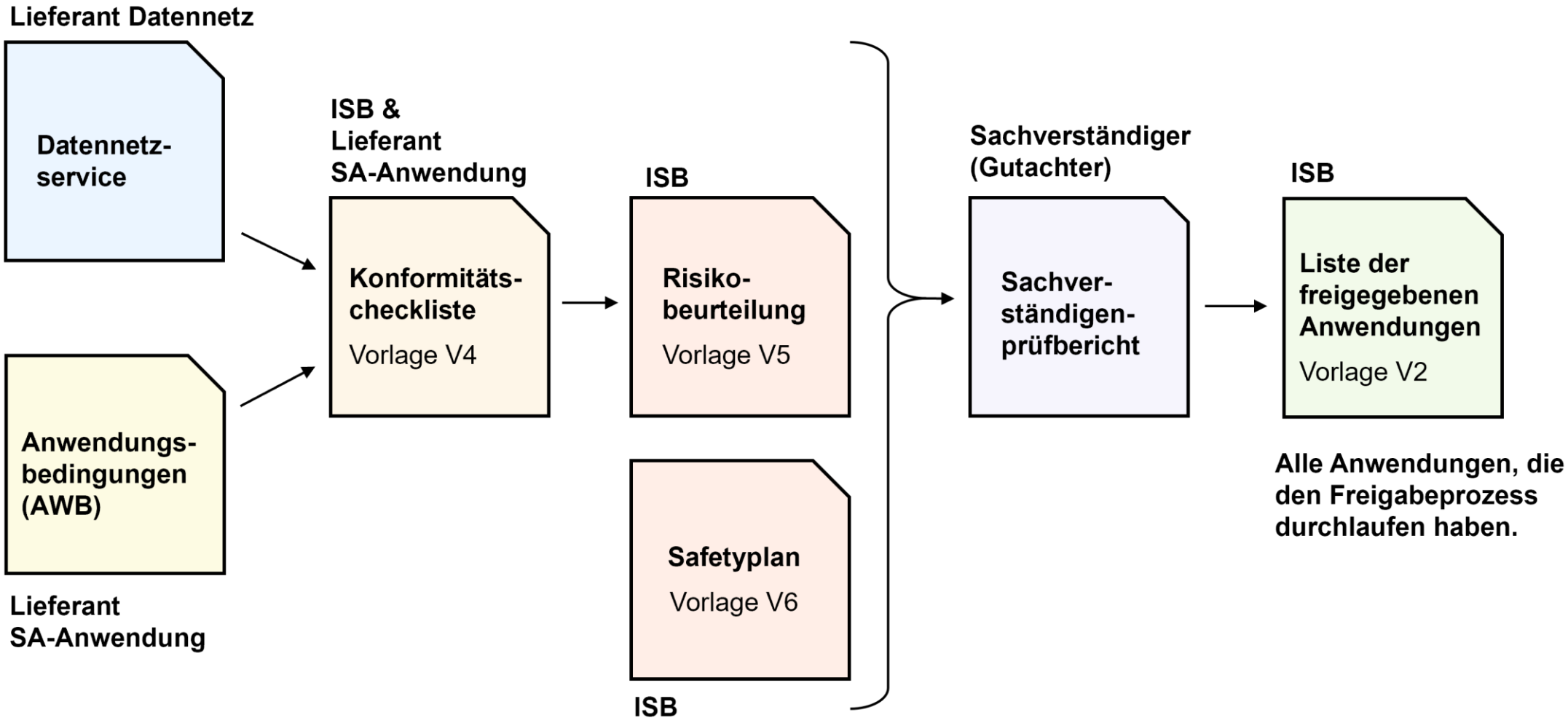
- Die **Resultate des Freigabeprozesses** werden im Dokument «Liste der freigegebenen Anwendungen» erfasst.
- Die «Liste der freigegebenen Anwendungen» wird **jährlich als Update ans BAV** geschickt, falls im abgelaufenen Jahr neue Freigaben erfolgt sind.
- Für das Dokument gibt es die Vorlage D-RTE-28100-V2.

2. Anwendungen

2.1. Anwendung xy

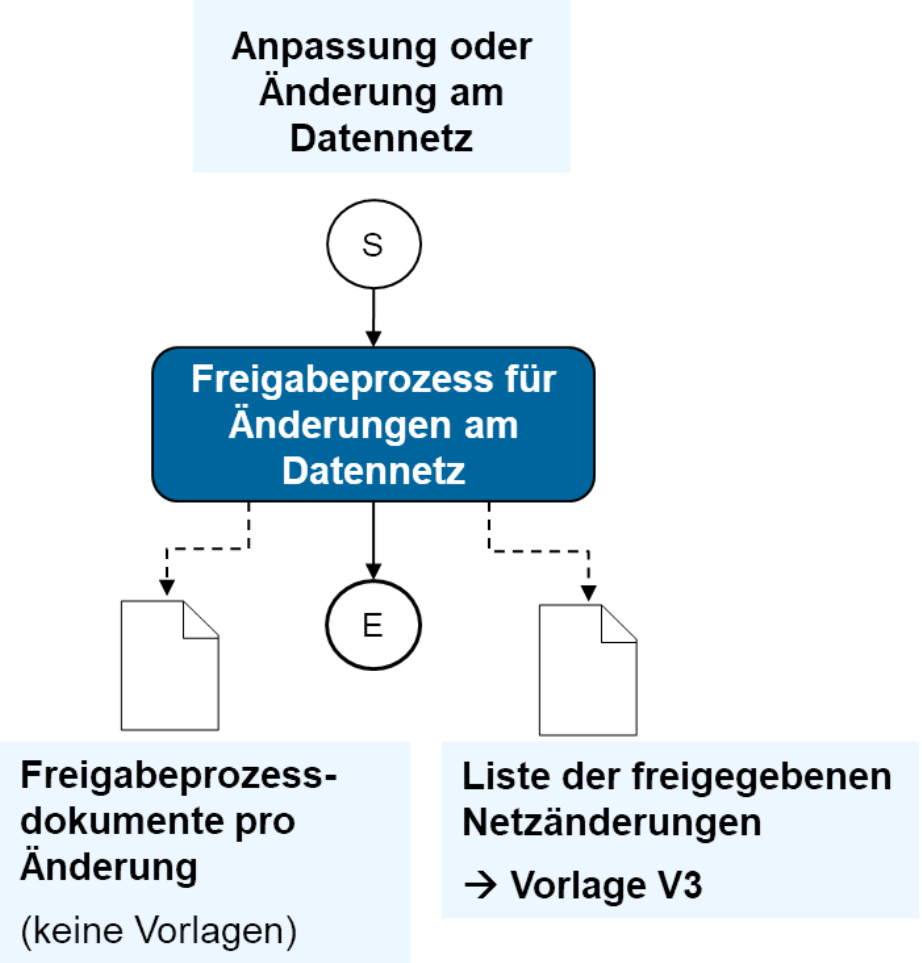
Identifikation	
Anwendung	Leit- und Informationssystem
Systemversion	
Lieferant	
Anwendungsbeschreibung	
Referenzen	Zusätzliche relevante Dokumente
Eigenschaften	
SIL-Zuordnung	SIL 2
Kategorie-Tauglichkeit gemäss EN 50159 [1]	Kategorie 2
Anwendungsbedingungen	
Resultate Freigabeprozess	
Datennetz-Service	
Konformitätscheckliste	
Risikobeurteilung	
Safetyplan	

Freigabeprozess für Anwendungen, Resümee



Freigabeprozess für Änderungen am Datennetz

- Wenn die Möglichkeit besteht, dass es durch eine **Anpassung oder Änderung am Datennetz** zu negativen Auswirkungen auf die Safety und Security von sicherheitsrelevanten Anwendungen kommen könnte, so muss für diese Änderung eine **Risikobeurteilung** durchgeführt werden.
- Beispiele für Änderungen mit Durchführung Freigabeprozess: Architekturkonzept ändert, neuartige Schnittstelle nach aussen.
- Für diese Risikobeurteilung gibt es keine eigene Vorlage. Als Ausgangspunkt für die Risikobeurteilung dienen die Checkpunkte auf der nächsten Folie.



Freigabeprozess für Änderungen am Datennetz

Checkpunkte aus Vorlage V3, «Liste der freigegebenen Netzänderungen», Kap. 2.1.2

Für die Checkpunkte, die nicht mit einem klaren «Ja» beantwortet werden können, muss eine Abklärung vorgenommen werden.

a) ☐ Ja ☐ Nein Es gibt keine negativen Auswirkungen auf die **IT-Security**.

b) ☐ Ja ☐ Nein Es gibt keine negativen Auswirkungen auf die **Netztrennung** (bzw. Netzwerksegmentierung).

c) ☐ Ja ☐ Nein Es gibt keine negativen Auswirkungen bezüglich der **Bedrohungen gemäss EN 50159** (Wiederholung, Auslassung, Einfügung, Resequenzierung, Verfälschung, Verzögerung, Manipulation).

d) ☐ Ja ☐ Nein Es gibt keine negativen Auswirkungen auf die **Anwendungsbedingungen** bei sicherheitsrelevanten oder betriebsrelevanten Systemen.

e) ☐ Ja ☐ Nein Es gibt keine negativen Auswirkungen in Bezug auf **Verzögerungen** (Delays) bei sicherheitsrelevanten oder betriebsrelevanten Systemen.

f) ☐ Ja ☐ Nein Es gibt keine negativen Auswirkungen in Bezug auf die **Verfügbarkeit** bei sicherheitsrelevanten oder betriebsrelevanten Systemen.

Liste der freigegebenen Netzänderungen

- Die **geprüfte Netzänderung** und die Resultate des Freigabeprozesses werden ins Dokument «Liste der freigegebenen Netzänderungen» aufgenommen.
- Die «Liste der freigegebenen Netzänderungen» wird **jährlich als Update ans BAV** geschickt, falls im abgelaufenen Jahr neue Freigaben erfolgt sind.
- Dazu gibt es die Vorlage D-RTE-28100-V3.

Liste der freigegebenen Netzänderungen

(Vorlage V3)

2.1. Netzänderung xy

2.1.1. Änderungsübersicht

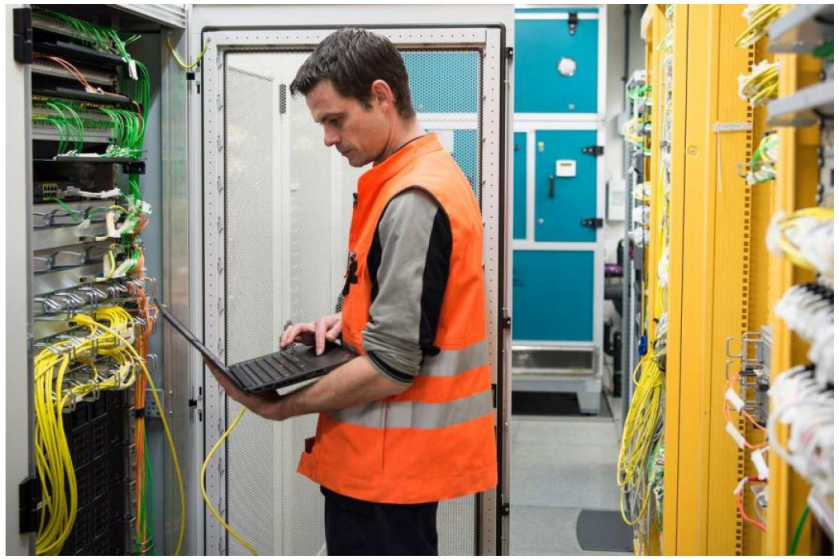
Identifikation	
Titel der Änderung	SW-Upgrade MPLS-Router
Beschreibung der Änderung	Es handelt sich um einen Life-Cycle ter. Upgrade von …. auf
Ziel der Änderung	Der Hersteller-Support für das Date sind gefixt. Bekannte Sicherheitslüc Funktionen stehen zur Verfügung.
Betroffene Netzkomponenten	MPLS-Router
Betroffenes Netz/Subnetz	
Dokumentation zur Änderung	Release Notes, Impact-Analysen
Referenzen	Zusätzliche relevante Dokumente
Organisation	
Antragssteller	
Lieferant der Änderung	
Projektleiter Lieferant	
Projektleiter ISB	
Engineering Lieferant	
Engineering ISB	
Resultate	
Ev. separate Risikobeurteilung	

D RTE 28100: Freigabeprozess

Besten Dank.

Nachweisführung Datennetze

Safety und Security



Fragen

Mittagessen 12.00 – 13.20 Uhr

- Menu und alkoholfreie Getränke sind inbegriffen
- Vegetarisches/Veganes Menu: bitte Karte auf Tisch

En Guete

Bon appétit

Wiederbeginn um 13:30

Programm Nachmittag

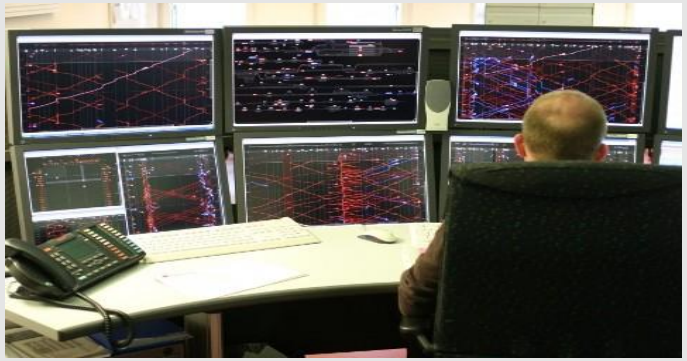
13:30 Uhr	**Praxis**
13:30 Uhr	Datennetzprojekte SBB (AiNET) Thierry Bassani
13:45 Uhr	Datennetzprojekte BLS Andreas Klopfenstein
13:55 Uhr	Datennetzprojekte AB Patrick Waldburger
14:05 Uhr	Datennetzprojekte RBS Martin Gerber
14:15 Uhr	PGV-Erfahrungen BAV Patrick Favre, Tobias Hubschmid
14:25 Uhr	**Pause**

Erneuerung SBB-Datennetz

Mittwoch, 11.12.2024

Thierry Bassani, Jean-Christophe Grandchamp

Das Datennetz steht im Zentrum der Digitalisierung



SBB
Intranet

Warum die Erneuerung ?

- Das sich heute im Betrieb befindende Datennetz erfordert subtanzerhaltende Massnahmen (Lifecycle). Komponenten, deren Wartung abgelaufen ist, müssen 2029 nach ca. 9 Jahren Lebensdauer ersetzt werden.
- Die SBB IT hat aufgrund der Erschliessung von Datacenters und Security-Lösungen die Anforderung an erhöhter Bandbreite (100Gbit/s und mehr).
- Die zukünftige Bahnsteuerung mit FRMCS (Future Railway Mobile Communication System), EESA (ERTMS Evolution Sicherungsanlagen) erfordert funktionale Erweiterungen am Datennetz.

Das Programm AiNET (Intelligent Network)

Ziele des Programms AiNET

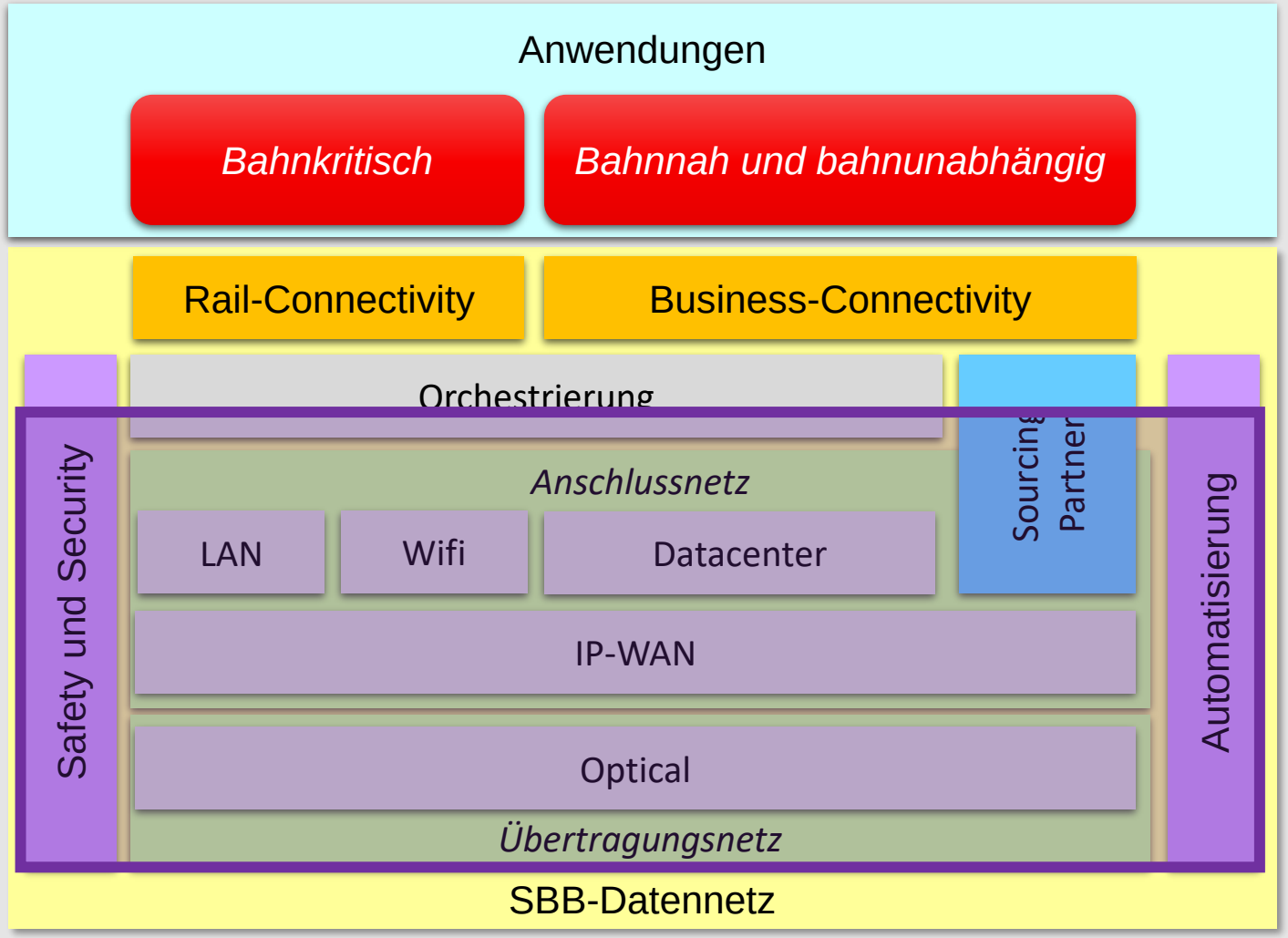
- Evolutionäre funktionale Erweiterung und Substanzerhalt der heutigen Datennetzinfrastruktur durch erprobte, zukunftsgerichtete, skalierbare und multivendor-fähige Technologien.
- Erfüllung der spezifischen Anforderungen von SBB IT, FRMCS und EESA
- Bereitstellung der nötigen Betriebsmittel/Managementsysteme für einen effizienten Betrieb, zur Verbesserung der Servicequalität und Sicherstellung der geforderten Verfügbarkeit im Bahnbetrieb.
- Störungsfreie Transition der Services vom bestehenden zum neuen Datennetz.

Wenn das Programm AiNET nicht umgesetzt wird, hat das Konsequenzen

- Die Komponenten des DCNG erreichen das Ende ihres Lebenszyklusses und fallen aus, was bedeutet, dass das Datennetz nicht mehr verfügbar ist.
- Neue Funktionen für die Bahnsteuerung und IT können nicht bereitgestellt werden.

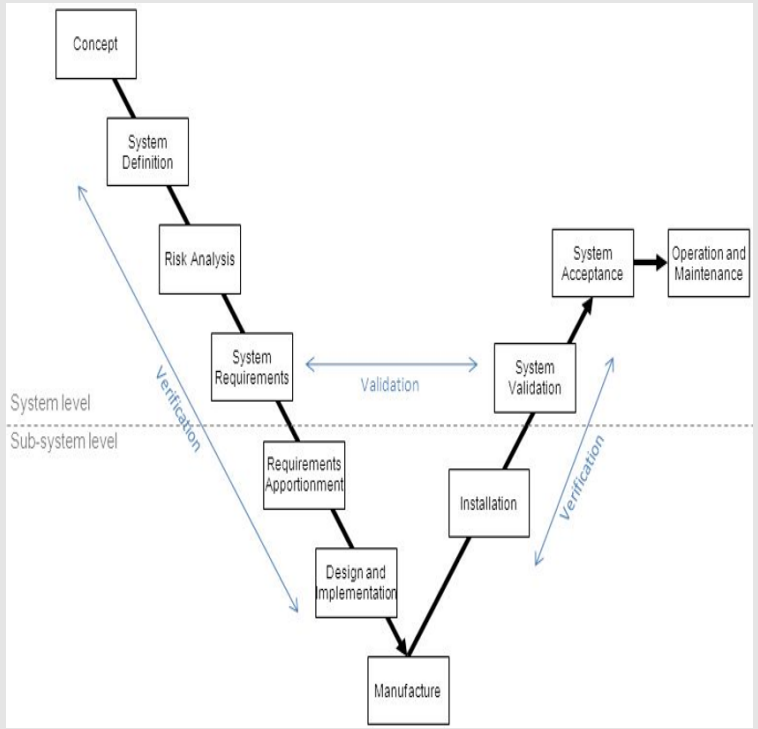
Das Ziel ist es also, **das Datennetz der SBB weiterzuentwickeln** und sicherzustellen, dass es den aktuellen und zukünftigen Anforderungen entspricht.

Architektur



Umgang mit Safety Themen

EN 50126



EN 50159

electrosuisse

Schweizer Norm
Norme Suisse
Norma Svizzera

SN

Fachbereich Elektrotechnik

EN 50159

EINGETRAGENE NORM DER SCHWEIZERISCHEN NORMENVEREINIGUNG SNV

NORME ENREGISTREE DE L'ASSOCIATION SUISSE DE NORMALISATION

Bahnanwendungen - Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme - Sicherheitsrelevante Kommunikation in Übertragungssystemen

Applications ferroviaires - Systèmes de signalisation, de télécommunication et de traitement - Communication de sécurité sur des systèmes de transmission

Railway applications - Communication, signalling and processing systems - Safety-related communication in transmission systems

Diese Norm ist die deutsche Fassung EN 50159:2010

Die Europäische Norm EN 50159:2010 hat den Status einer Schweizer Norm. Sie gilt in der Schweiz als anerkannte Regel der Technik.

Die EN 50159:2010 gilt seit: 01.09.2010.

Für die vorliegende Norm ist das Schweizerische Elektrotechnische Komitee (CES), Technisches Komitee 9 - Elektrische und elektronische Anwendungen für Bahnen - zuständig.

Referenznummer / No. de référence

SNEN 50159:2010(D)

Herausgeber / Vertrieb Editeur / Distributeur

Electrosuisse
Luppmenstrasse 1, CH-8320 Fehraltorf

Satefy@TC Prüfprozess

SBB CFF FFS

Änderungsprozess

Datennetze@SA

VÖV UTP

Verband öffentlicher Verkehr
Union des transports publics
Unione dei trasporti pubblici

D RTE 28100

Nachweisführung Datennetze

Safety und Security

AiNET Programm und Safety Themen

1. Was braucht das Programm AiNET betreffend Safety?
2. Auf was kann das Programm AiNET zurückgreifen?
3. Was muss das Programm AiNET erarbeiten?

Was braucht das Programm AiNET betreffend Safety?

- Freigabe-Prozess
- Nachweis der Erfüllung von Anforderungen der Normen und der Anwendungen
- Safety-Plan, RAM-Plan, Verifizierung, Validierung
- Prüfbericht Sachverständiger
- Verfügung vom BAV (Typenzulassung)

Auf was kann das Programm AiNET zurückgreifen?

(Vieles wurde schon im Programm Datacom-NG erarbeitet)

- Freigabe-Prozess (“Änderungsprozess Datennetze@SA”)
- Safety (Vor-)Prüfung im Betriebsphase/Lifecycle (Milestones / Tollgates)
- Risiko-Analyse zu neuen Technologien (Segment-Routing,…)
- Risiko-Analyse zu Betriebsprozessen (4 Augen-Prinzip, …)

Was muss das Programm AiNET erarbeiten?

- Risiko-Analyse und Nachweis betreffend die neuen Technologien und für die Lösungsumsetzung
- Nachweis nach EN 50159 zum neuen SBB-Datennetz
- Anpassung der Betriebs-Prozesse für Business-Connectivity (Rückwirkungsfrei für Rail-Connectivity)
- Anpassung Cybersecurity-Prozesse bei Rail-Net Änderungen
- Adaptierung vom “Änderungsprozess Datennetze@SA”

VÖV UTP
Verband öffentlicher Verkehr
Union des transports publics
Unione dei trasporti pubblici

Danke, merci, grazie

Mittwoch, 11.12.2024

Thierry Bassani, Jean-Christophe Grandchamp

Projekt SA-EVO
BLS Netz AG

D RTE 28100 Datennetze 11.12.2024
Andreas Klopfenstein, TM Netzwerke & Security

Inhaltsverzeichnis

1. Ausgangslage SDH Technologie EoL

Stärken

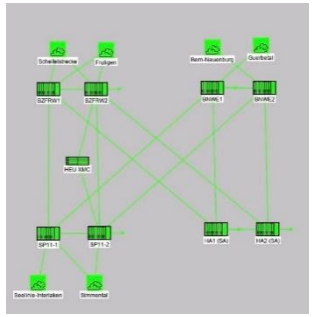
- Robuste Technologie (SDH)
  Ringtopolgie, hohe Verfügbarkeit

Schwächen

- **SDH Technologie EoL**
  - Ersatzmaterial z.T nicht mehr verfügbar
  - Wird mit Rückbauten/Reduktionen überbrückt
- **Unterschiedliches Design**
  - EMME Netz keine Baugruppenredundanz auf Shelf Ebene
  - Stromversorgungskonzept in den Regionen unterschiedlich
- **Unterschiedliche HW Generationen im Einsatz**
  - UMUX1500/XMC/Milegate
  - Dadurch erhöhte Komplexität und Abhängigkeiten

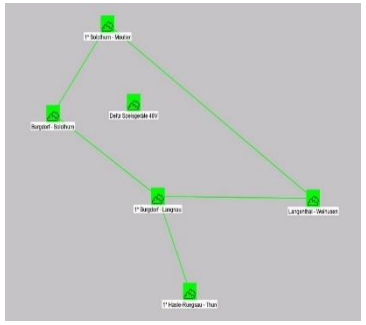
1. Ausgangslage Netze

1. Ausgangslage Netze

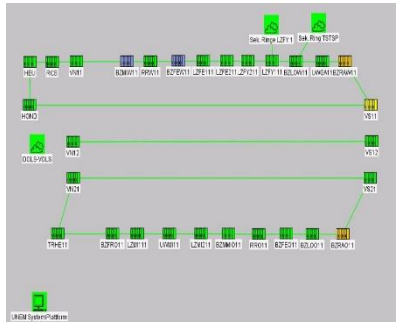


SA

ILTIS,Stw,RCI,RCS95,EC-CC

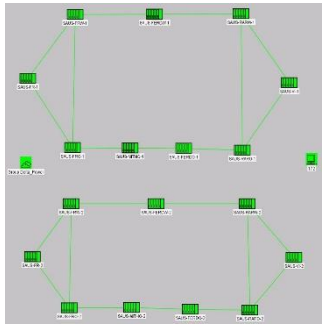


Emme



DT

GSM-R/BTS



SAUS

RBC,eStw,etc)

Milegate

Subraten Konverter TKN(v.24,x.35,etc)

Zielbild

SA-EVO

Ein Netz für alle Safety Relevanten Services
ILTIS
Stellwerk
GSM-R/ BTS
Subraten

Anforderungen

Zulassungsprozess RTE28100	BAV
RL CySec-Rail	BAV
Information Security Anbieter	BLS
Baseline Security Anbieter/Projekte	BLS

Zielbild

Technologie neutrale Ausschreibung

MPLS-TP oder IP/MPLS

Ressourcen LWL

– Definierte Anbindung der Access Standorte
– Soweit möglich, optisch mit BIDI SFP in den Accessketten

Herausforderungen

Regulatorisch:

- Zulassungsprozess pro Service nach RTE28100 mit BAV
- Einhaltung RL CySec-Rail BAV
- Einhaltung Cybersecurity für Betriebe des öffentlichen Verkehrs BWL

Technisch:

- Kat.1 Services auf Packet orientierten Netzen (EN50159) EC-CC, RCS95 nicht zugelassen (gem. SBB-BAV)

Fazit

Administrativer Aufwand für Nachweise und erfüllen der Anforderungen in den Projekten sehr hoch

Security Anforderungen im OT Umfeld «explodieren»

Know-How muss vorhanden sein oder eingekauft werden

Assetmanagement ist der Schlüssel in einem heterogenen Umfeld (LifeCycle Bahnanwendungen !)
Was haben wir im Netz ???

Risikobewertung basiert auf den Assets der einzelnen Anwendungen

Danke!

BLS AG
Genfergasse 11
CH-3001 Bern
bls.ch

Noch Fragen?

Appenzeller Bahnen

Erfahrungsbericht zur Erneuerung des Datennetzes

Fachtagung Datennetze, 11.12.2024

Patrick Waldburger
Spezialist Digitalisierung und Netzwerke

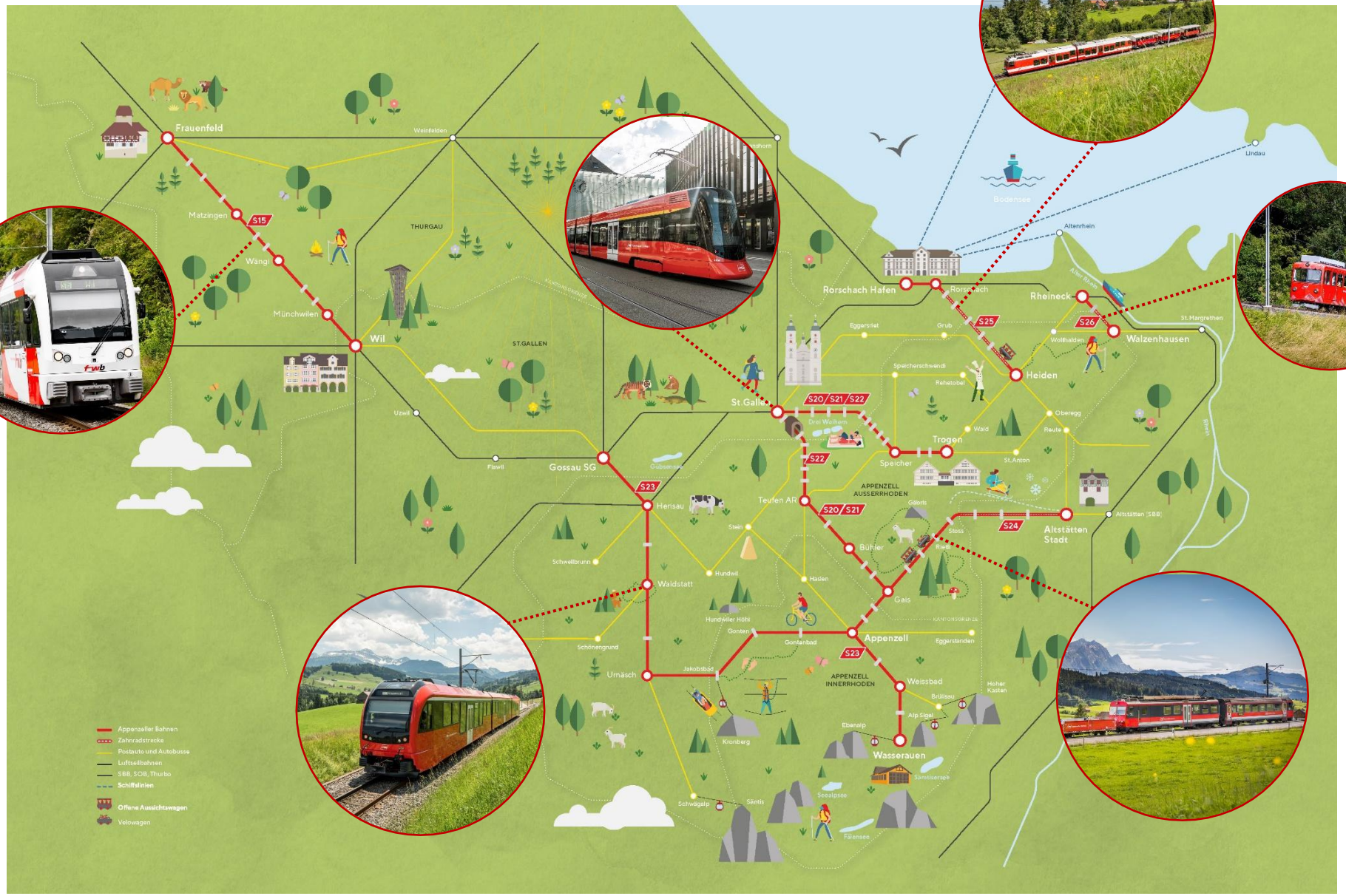
Appenzeller Bahnen

Herzlich willkommen.

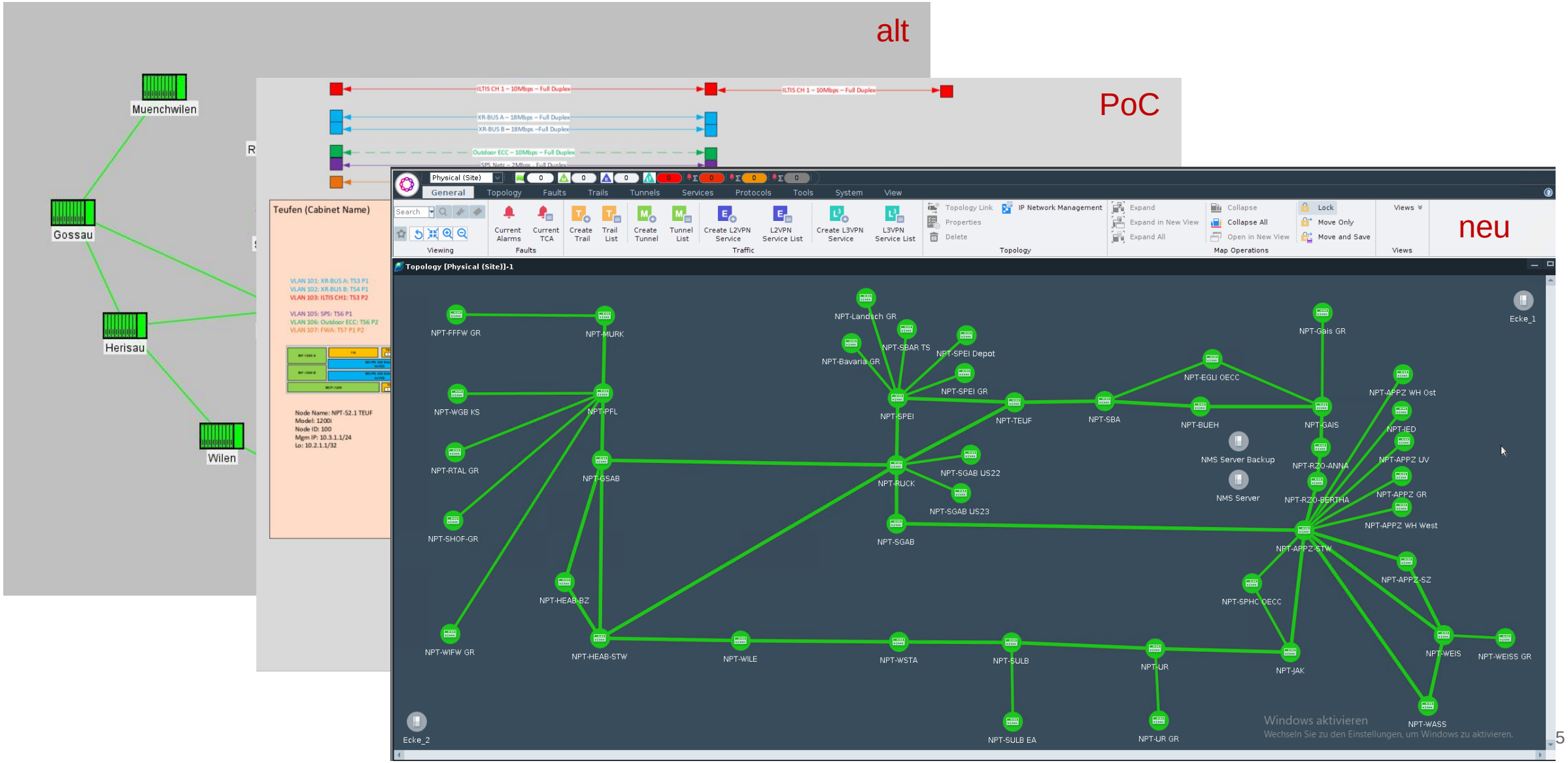
Traktanden

1. Unser Liniennetz
2. Datennetz: Umsetzungsprozess, Zahlen, Anwendungen
3. RTE 28100: Prozesse, Projektablauf
4. Schlussfolgerungen

Unser Liniennetz



Datennetz: Umsetzungsprozess von alt zu neu



Datennetz: in Zahlen

6
Virtuelle Maschinen

340
Service-Endpunkte

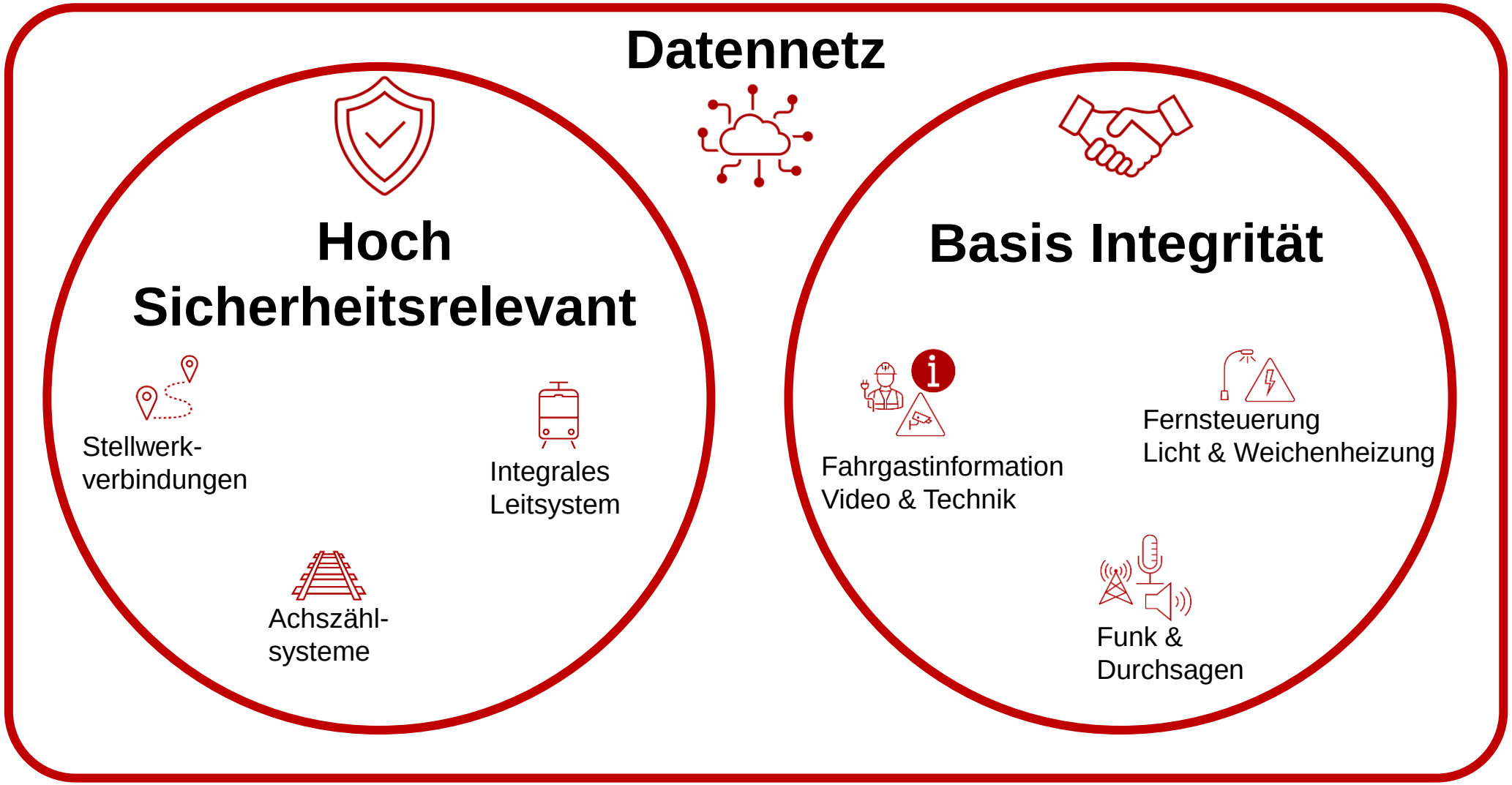
404
MPLS-TP Tunnel

64
Services

286 GB
Speicherplatz

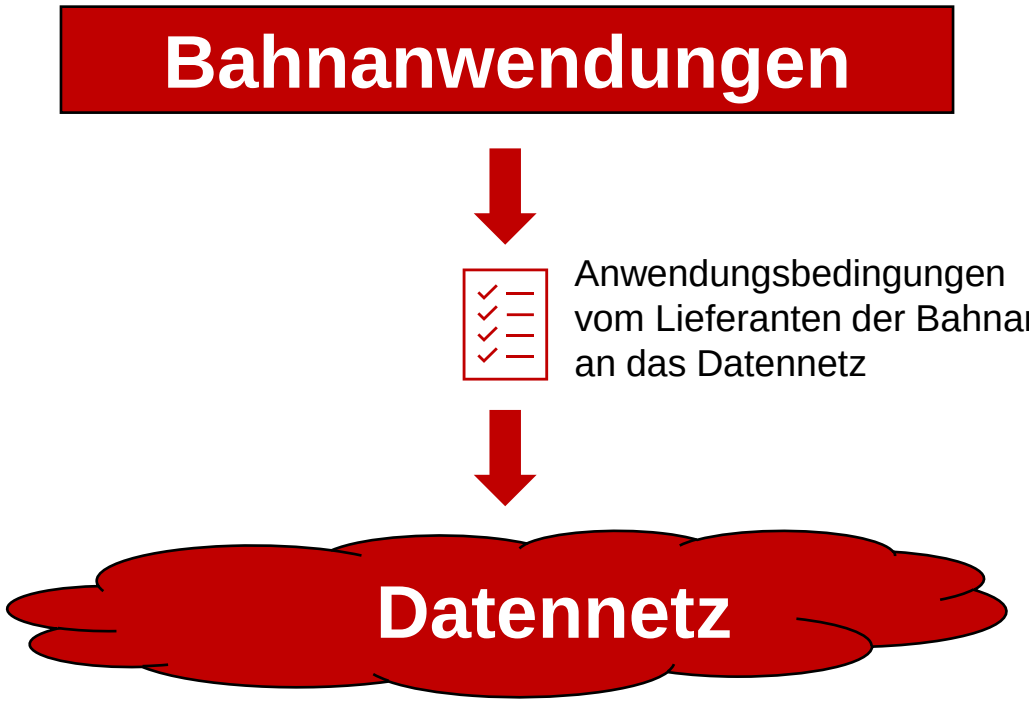
46
Netzwerkknoten

Datennetz: Bahnanwendungen

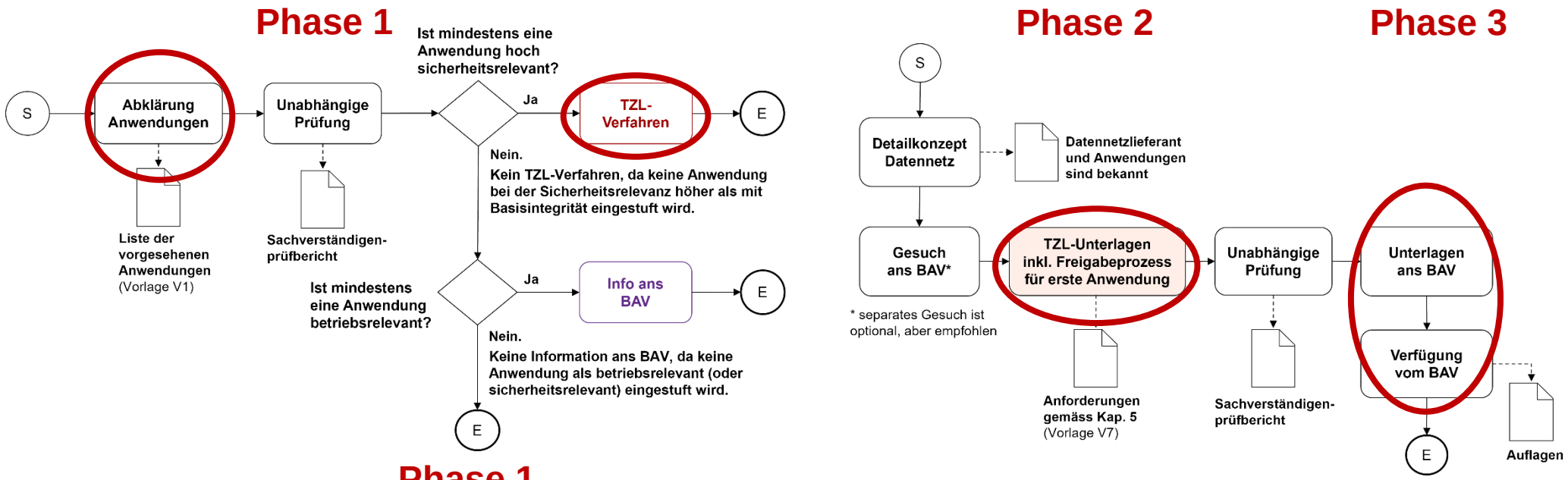


RTE 28100 Nachweisführung Datennetze

RTE 28100 noch nicht veröffentlicht — Typenzulassung der AB als Pilot um erste Erfahrungen in der Anwendung der RTE 28100 zu sammeln — Definierter Freigabeprozess zur Prüfung und Dokumentation der Erfüllung aller Anwendungsbedingungen durch das Datennetz über den ganzen Lifecycle — Regelung und Hilfe für Projektierung und den Betrieb von Datennetzen um den hoheitlichen Vorgaben zu entsprechen



RTE 28100: Prozesse



Phase 1

- Auflistung der Anwendungen → V1
- Prüfung der Anwendungen TZL Ja/Nein → SV

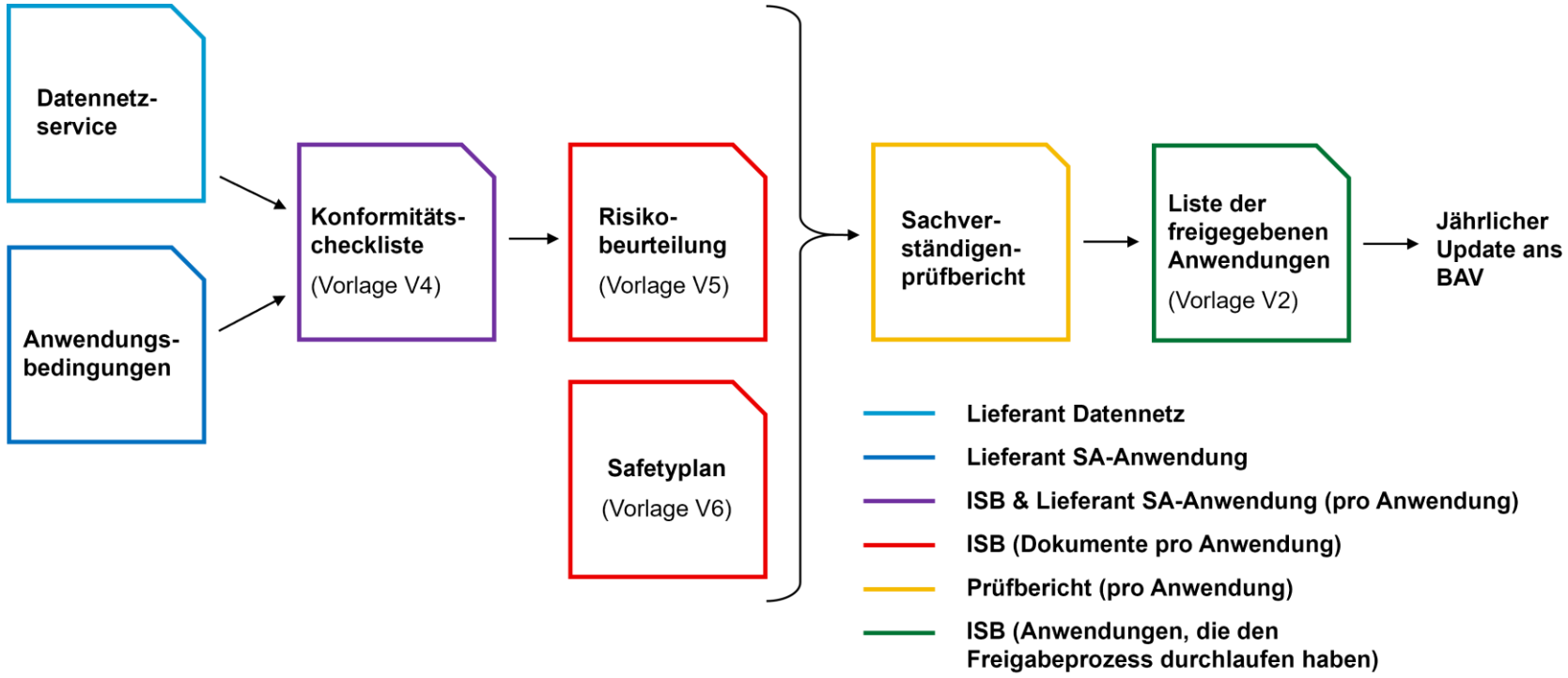
Phase 2

- Freigabeprozess mit erster Anwendung (TZL) → V4 bis V7

Phase 3

- SV-Prüfbericht → Verfügung BAV → V2 & V3

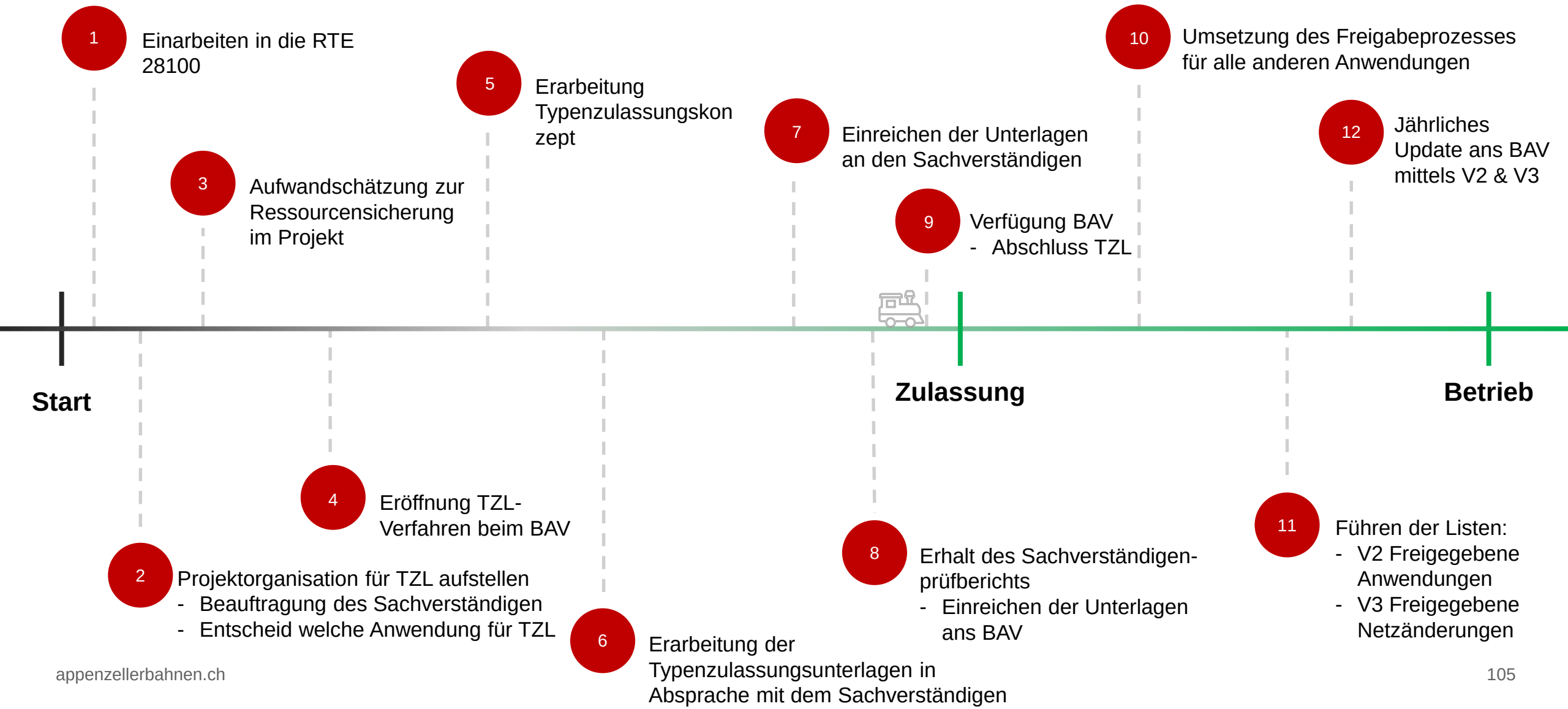
RTE 28100: Prozesse



Phase 4

– Freigabeprozess für restliche Anwendungen

RTE 28100: Projektablauf für die TZL



Erfahrungen mit der Anwendung der RTE 28100

SV-Prüfbericht zur Initiierung TZL Verfahren erforderlich?

Kapitel 5: Normative Anforderungen an das Datennetz
→ Redundanz zur RL CySec-Rail

Granularität Risikobeurteilung & Safetyplan

Wenige Sachverständige «Datennetz»
→ Ressourcenengpass in Zukunft?

Zusätzliche Ressourcen werden auf Seite ISB benötigt um die Prozesse beim einführen zu etablieren.

Kompetenzen sind ISB intern sicherzustellen **!Wichtig!**
Schnittstellenkoordination: Fach – Anwendung – Nachweis

Die <u>Anwendungen</u> stehen im Mittelpunkt und definieren die Anforderungen an das Datennetz

Konformitätschecklisten ergeben Mehraufwand beim Lieferanten der Anwendungen

Freigabeprozess muss bei jedem ISB implementiert und festgehalten werden

Aufwandschätzung für TZL & Freigabeprozess

Die RTE 28100 bietet eine umfassende Grundlage

Hilfe um sicherzustellen, dass an alles gedacht wird

Vereinheitlichung der Nachweisführung


AB
Appenzeller Bahnen
40

Fragen?

Datennetz-Projekt RBS

Martin Gerber, Projektleiter RBS
Mark Bischofberger, Projektleiter Nokia

Datennetz-Projekt RBS

Erneuerung des Infrastruktur Datennetzes von einer SDH-Architektur zu einer MPLS-Architektur (MPLS-TP oder IP/MPLS)

Zeitplan:

- ❑ Ausschreibung: Juli 2020 (Publikation)
- ❑ Angebote: November 2020
- ❑ PoC/Pilot: 2021
- ❑ Rollout: 2022- 2024
- ❑ Migration: 2023 bis 2025

Wichtige Anforderungen:

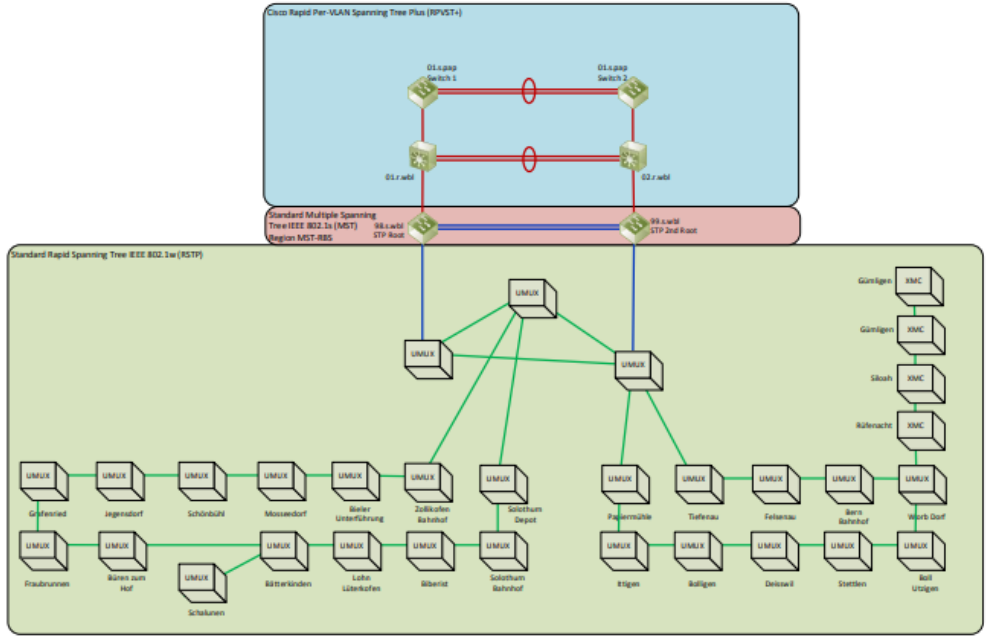
- ❑ Packet-Netz mit entweder zentrale Control (MPLS-TP) oder Base Routing (IP/MPLS)
- ❑ Verfügbarkeit wie im SDH-Netz, Umschaltzeit wie mit der SDH-Technologie
- ❑ Modernes Netz, wird voraussichtlich 12-15 Jahren in Betrieb sein

Migration aller RBS betriebsrelevanten Applikationen, inkl. Stellwerkfernsteuerung VBBa

1. Betriebsrelevanten Applikationen:
2. Sicherheitsrelevanten Applikationen: Stellwerk-Fernsteuerung

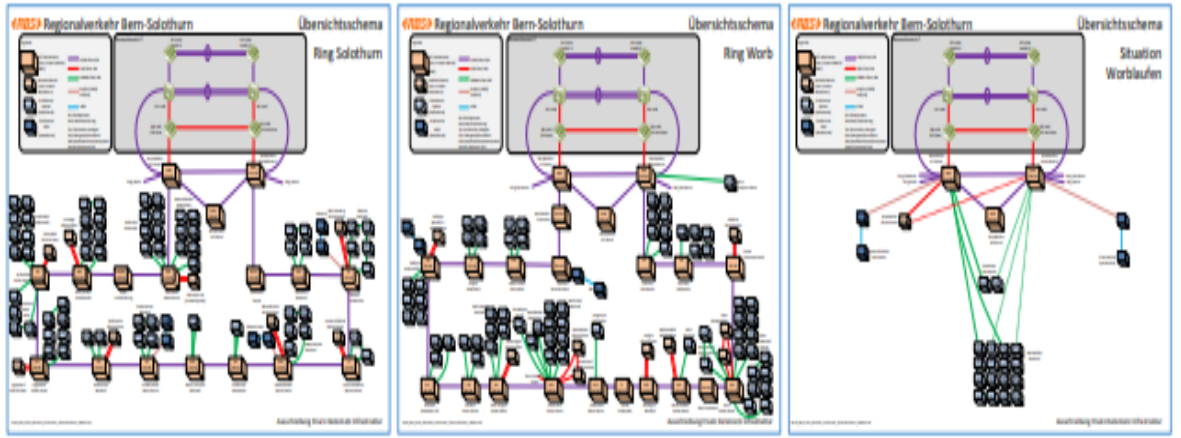
Datennetz-Projekt RBS – Aufbau des Netzes

- **Altes SDH-Netz**
  - E1 Schnittstellen
  - EoS auf E1/VC12 für den Ethernet Verkehr
- 2 x 622M Ringe (Solothurn und Worb, inkl. eine Perlenkette von Worb bis Muri
- Redundante Anschlüsse zu 2 DCs



Modernes Packet-Netz

- IP/MPLS Protokoll
- Ethernet Schnittstellen: Weiterleitung vom L2 und L3 Verkehr
- Stellwerk wird separat auf dark fiber geleitet (EN50195 Cat1)
- 2 x 10G Ringe (Solothurn, Worb und zurück via Bern), Redundante Verbindung über externe LWL Fasern



Datennetz-Projekt RBS – Wahl der NEs

❑IP/MPLS Routers

- ❖ **3 Hauptknoten (DC-Gateways):**
  3 x 7250 IXR-R6 mit redundanten Controllers
- ❖ **Bahnhöfe:**
  32 x 7705 SAR-8 Chassis mit redundanten Controllers

❑L2 Switches

- ❖ **Gleichrichter-Switches:**
  ~30 gehärtete L2 Switches für die Anbindung von allen MVAC-1500VDC Traktion-Gleichrichter
- ❖ **Feld-Switches:**
  Interworking (ERPS) mit den ~450 betriebenen 'Linerunners'

Datennetz-Projekt RBS
Characteristics & Apps Migration

❑IP/MPLS Netz

- ❖ Alle NE redundant mit redundanter DC-Speisung (Batterien)
- ❖ Base Routing: IS-IS -> Switchover: IP/MPLS FRR, 0-50ms

❑L2 Switches

- ❖ Alle Gleichrichter-Switches redundant gespiesen:
- ❖ max 4 Einheiten in einer Perlenkette ->Switchover: ERPS oder LAG, max. 50ms

Applikation-Migration

VBBa	Stellwerk SPS	Funk TETRA	Tunnel-funk	Funk KAIROS	SIP Telefonie	IP KIS Lautsprecher	IP KIS Anzeigen	Fahrstrom-versorgung	Alarme USV&Speisung	Technik (Weichen, Licht, etc.)	VIdeo
Sicherheit	Betrieb	Betrieb	Betrieb	Betrieb	Betrieb	Betrieb	Betrieb	Betrieb	Betrieb	Betrieb	Betrieb
LAN	VLAN	VLAN	VLAN	VLAN	VLAN	VLAN	VLAN	VLAN	VLAN	VLAN	VLAN
eigene Glasfaser	2024	2025	2024	2024	2023	2023/24	2024/25	2024	2023	2023	2023

Datennetz-Projekt RBS
Betrieb und Unterhalt

❑Betrieb und Unterhalt RBS und Nokia

- ❖ First Level Support durch Pikettorganisation RBS
- ❖ Second Level Support durch Nokia Suisse – Pikett und Wartungsvertrag 7x24h/365Tage
- ❖ Support Third Level durch Nokia – Bestandteil vom Pikett- und Wartungsvertrag 7x24h/365Tage

❑Interventionszeiten

- ❖ Critical - Reaktionszeit: 15min - Lösung: 4h
- ❖ Major - Reaktionszeit: 1h - Lösung: 12h
- ❖ Minor - Reaktionszeit: nächster Arbeitstag

VÖV UTP
Verband öffentlicher Verkehr
Union des transports publics
Unione dei trasporti pubblici

D RTE 28100, PGV-Erfahrungen BAV, 1. Teil

Patrick Favre, Tobias Hubschmid

Mittwoch, 11.12.2024

PGV-Erfahrungen BAV

Inhalt 1. Teil:

– «Alte» Typenzulassungen Difonet, Rail IP, UMUX/XMC20

– Änderungsprozess Datennetze@SA

– Erstanwendung der D RTE 28100 bei den Appenzeller Bahnen

Inhalt Teil 2: Fokus Security

«Alte» typenzugelassene Datennetze

Am Beispiel von SBB DIFONET, SBB Rail IP und UMUX/XMC20:

– Die systematische Prüfung der Kompatibilität von Anwendungen mit Datennetzen wurde formalisiert und **einigermassen konsequent** durchgeführt.

– Die (theoretisch) **systematische Involvierung des BAV** beim Entscheid, ob eine Anwendung aufgeschaltet werden durfte, **war wenig zielführend**.

– Im Fall des UMUX/XMC20 besitzt der Lieferant die Typenzulassung und pflegt diese. Die Bahnen spüren kaum etwas davon.

Allgemein dürfte es im Zusammenhang mit der Aufschaltung von hoch sicherheitsrelevanten Anwendungen an Datennetzen eine gewisse Dunkelziffer gegeben haben.

Änderungsprozess «Datennetze@SA» der SBB

- Die Anwendung des **Änderungsprozesses hat sich bewährt**. Damit ist eine systematische Behandlung der Aufschaltung hoch sicherheitsrelevanter Anwendungen sichergestellt.
- Der Aufwand bis zur Typenzulassung war sehr hoch. Hauptgrund dafür dürfte die lange Suche nach dem optimalen Weg sein.
- **Der Aufwand für die Durchführung des Prozesses** nach der Typenzulassung (d.h. ohne BAV) **ist eher hoch**. Er lässt sich durch die Breite und Tiefe der Koordination zwischen den involvierten Fachleuten (Telekom, Sicherungsanlagen, Lieferanten, Sachverständige) erklären.
- **Der Prozess erfordert viel Knowhow**, sowohl auf Seite der Anwendungen wie auch des Datennetzes.

Erstanwendung der D RTE 28100 bei den Appenzeller Bahnen

Erfahrungen zur Anwendung der RTE 28100 (Safety-Aspekte, insb. Freigabeprozess):

– **Die Erstanwendung ist den Appenzeller Bahnen gelungen**.

– Die ausgefüllten Vorlagen V1 – V7 und der Sachverständigenprüfbericht ermöglichten es dem BAV, das Dossier mit vernünftigem Aufwand zu beurteilen.

– **Eine nachvollziehbare Risikobeurteilung ist fundamental**, wenn nicht alle Anforderungen der Anwendung zweifellos erfüllt werden.

– Die **Verankerung des Freigabeprozesses seitens des ISB** ist zentral.

VÖV UTP
Verband öffentlicher Verkehr
Union des transports publics
Unione dei trasporti pubblici

BAV Erfahrungen PGV resp. Bewilligungsverfahren Teil 2: Fokus Security

Patrick Favre, Tobias Hubschmid

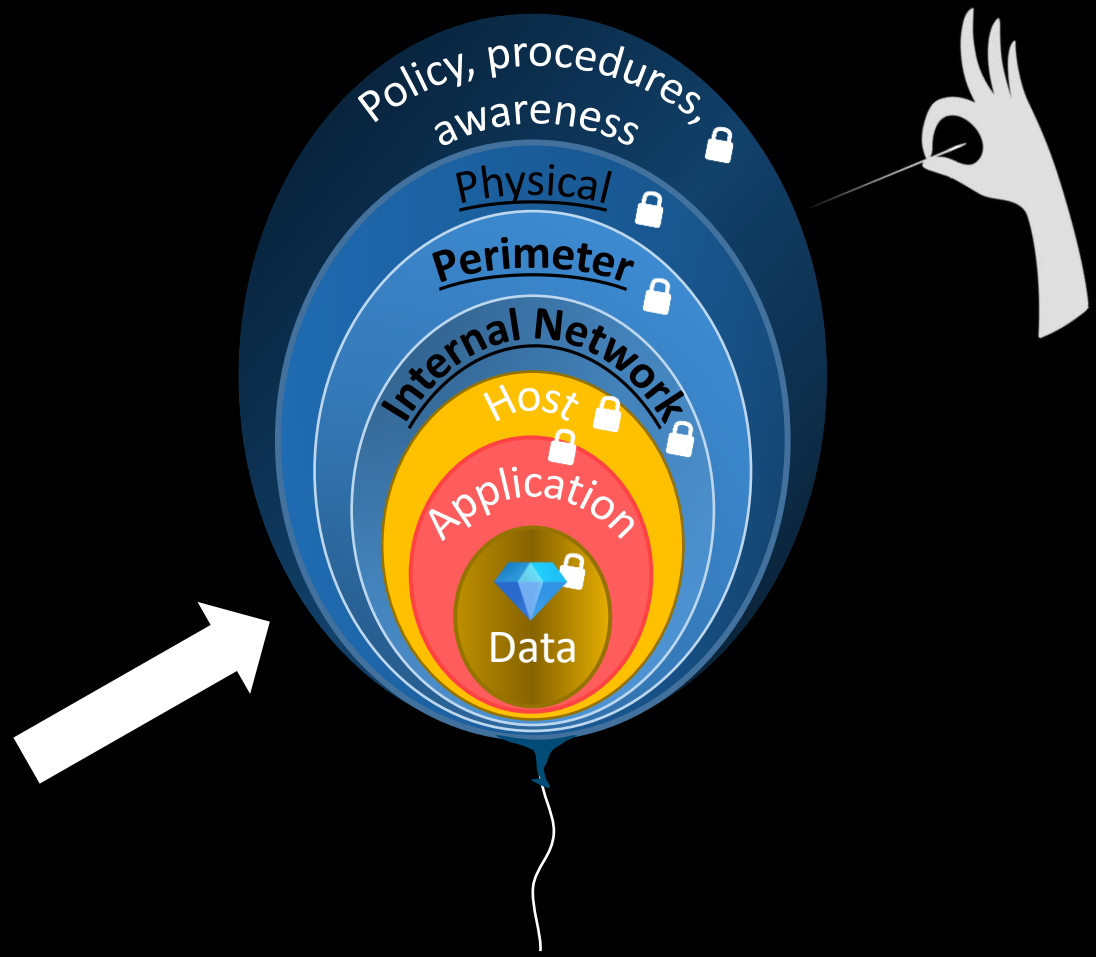
Mittwoch, 11.12.2024

Fokus CySec: BAV Erfahrungen aus den Überwachungstätigkeiten (PGV, TZL, Audits)

- 👍 Zunehmende **Awareness** in der Cybersicherheit in der Branche. Es wird vermehrt in die CySec investiert.
- ☞ **Baustelle ISMS:** Abgrenzung zwischen Tätigkeiten/Massnahmen im Projekt und ISMS-Tätigkeiten schwierig.
- ☞ **Gemeinsames Verständnis zwischen Safety** («never touch a running system») **und Security** (Verwundbarkeiten rasch zu beseitigen) oft noch nicht vorhanden.
- ☞ **Lieferantenmanagement** nach wie vor eine grosse Herausforderung. Rollen und Verantwortungen zwischen ISB und Dienstleister oft ungenügend und zu wenig verbindlich geklärt.

Erkanntes Verbesserungspotential und kritische Erfolgsfaktoren:

- **Zuständigkeiten und Zusammenarbeit:** Klares Festhalten und Kommunikation, inkl. Dokumentation der **AKV** innerhalb den verschiedenen Bereichen.
- Die **«Visibilität»** hat in vielen Datennetzen noch Verbesserungspotential, insbesondere im OT-Bereich. D.h. die Fähigkeit Cyberangriffe zeitnah erkennen zu können und betroffene Netzwerksegmente rasch zu isolieren.
- **Unterstützung** bei erfahrenen Fachexperten holen (kompetente Sachverständige fördern).
- **Lieferantenmanagement – es geht nur zusammen!**
- Security: **Defense-in-Depth Prinzip** konsequent anwenden (bedingt Security by design). Die Datennetzinfrastruktur ist dabei von hoher Wichtigkeit.



Take home message

Timing ist alles:

Cyberangriffe abzuwehren ist eine Frage des Timings. Es erfordert ein rasches Erkennen, Schadensbegrenzung und effektive Wiederherstellungsverfahren.*

Sei vorbereitet!

Den Datennetzen kommt bei der Erkennung von Cyberangriffen und bei der Schadensbegrenzung eine wichtige Rolle zu!

*Lockbit, die bislang schnellste Ransomware, kann gemäss CISCO Talos 100'000 Testdateien - beziehungsweise 53 Gigabyte - in nur 5 Minuten und 50 Sekunden verschlüsseln.

KURZE PAUSE (15 min)

… Wiederbeginn um 14:40 Uhr

Programm Nachmittag

14:40 Uhr	**News im Bereich SA / Cy-Sec**
14:40 Uhr	Regelungen SA Urs Walser
14:50 Uhr	Normen Security-Safety (IEC, CENELEC) Jean-Christophe Grandchamp
15:00 Uhr	Infos VöV Marcel Schmid
15:10 Uhr	**Abschluss** Dr. Robert Leemann
15:30 Uhr	**Ende der Tagung / Informeller Austausch mit Referenten** (Züge ab 16.00 Uhr erreichbar)

VÖV UTP
Verband öffentlicher Verkehr
Union des transports publics
Unione dei trasporti pubblici

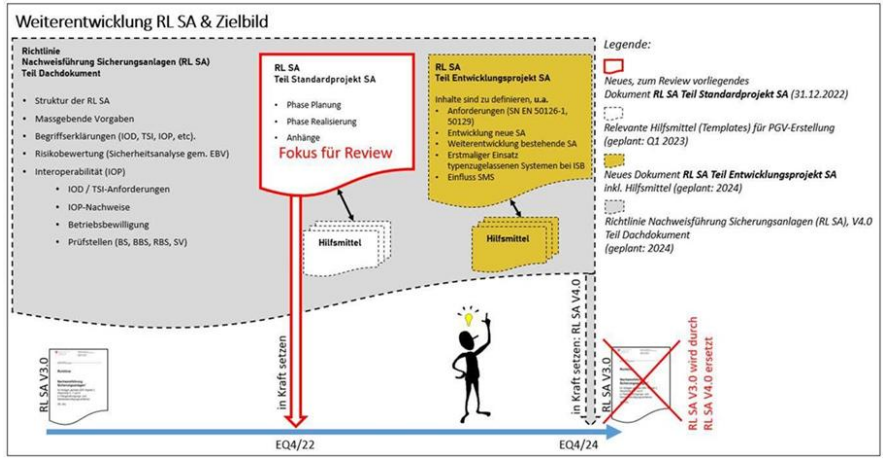
Regelungen SA / BTE

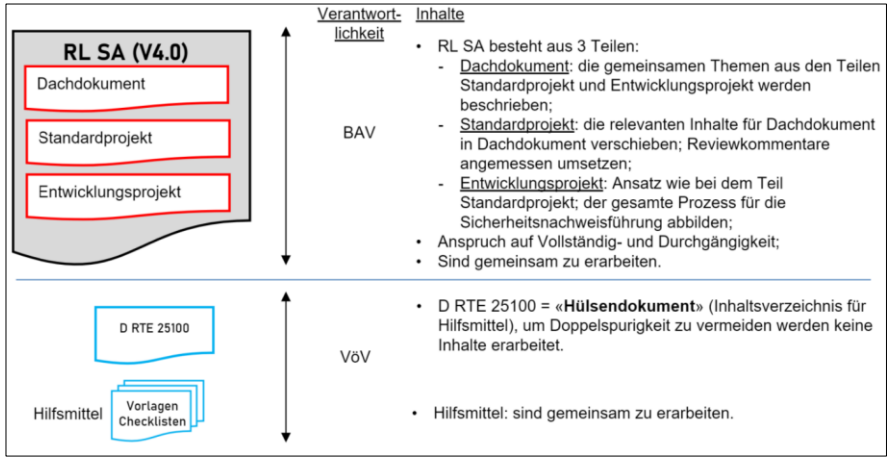
Urs Walser Projektleiter RTE

Mittwoch, 11.12.2024

Richtlinie SA – D RTE 25100 Nachweisführung SA

- Weiterentwicklung notwendig
  - BAV Richtlinie SA V 3.0, 23.10.2015
  - D RTE 25100 Nachweisführung SA, 1.5.2016
  - Info des BAV über RL SA V 4.0 in FG ET 3.Q.22
  - Vernehmlassung eines BAV-Entwurfs RL SA 4.0 Teil Standardprojekt im 4.Q.22
  - Gemeinsamer Projektauftrag BAV-VöV über die Weiterentwicklung der RL SA und des D RTE 25100 im 1.Q.23





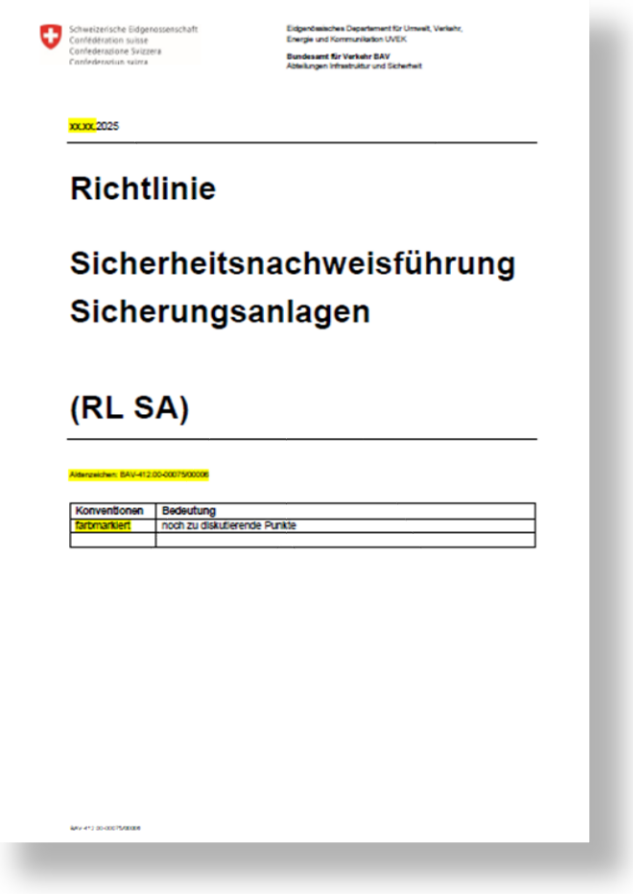
Richtlinie SA – D RTE 25100 Nachweisführung SA

- Projektleitung
  - RL SA Martin Gusset BAV
  - RTE Anne Lehnert BB
- Projektgruppe bestehend aus
  - BAV
  - Branche (Bahnen und Industrie)
  - VöV/RTE
- Untergruppen
  - Standardprojekt
  - Entwicklungsprojekt
  - Relaisstellwerke
  - Cy-Sec

Name	Vorname	Unternehmen		RTE
Bartlome	Marcel	BAV		
Guritanu	Violeta	BAV		
Gusset	Martin	BAV	PL BAV	
Hubschmid	Tobias	BAV		
Studer	Andreas	BAV		
Benz	David	SBB		
Boucher	Adrien	SBB		X
Einer	Stefan	SBB		
Ferrari	Flavio	SBB		
Grünig	Ernst	SBB		
Kajktazovic	Christine	SBB		X
Montani	Mauro	SBB		
Ruch	Peter	SBB		X
Theurillat	Raphael	SBB		
Tomas	Daniel	SBB		
Wermelinger	Roger	SBB		
Hauswirth	Jürg	SOB		
Hofstetter	Roland	Geste		
Huber	Michael	Siemens		
Hurni	Marcel	BLS		X
Lehnert	Anne	Bahnberatung	PL RTE	X
Schenk	Dominic	RBS		X
Veja	Julien	STASIG		
Walser	Urs	VöV		X

Richtlinie SA

- Ziel der Weiterentwicklung
  - Die RL SA dient zur Erfüllung der Anforderungen der EBV Kap. 1 für die Planung und den Bau der SA, welche in den PGV und BBwV genehmigt werden sollen.
  - In der RL SA ist ein einheitliches Vorgehen für die Sicherheitsnachweisführung SA definiert und beschrieben, welche:
    - Vorgaben massgebend sind;
    - Nachweisdokumente für die SA zu erstellen sind;
    - inhaltlichen Anforderungen die Nachweisdokumente erfüllen müssen;
    - Nachweisdokumente dem BAV zu welchem Zeitpunkt einzureichen sind.


Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera

Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation UVEK

Bundesamt für Verkehr BAV
Abteilungen Infrastruktur und Sicherheit

xxxx.2025

Richtlinie

Sicherheitsnachweisführung Sicherungsanlagen

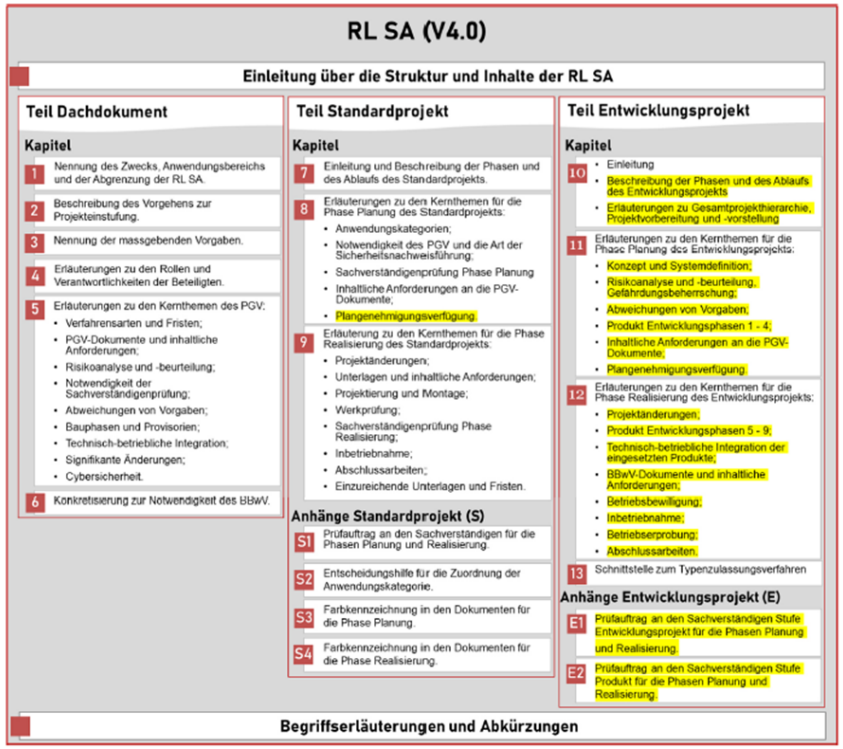
(RL SA)

Aktenzeichen: BAV-412.00-00075/00006

Konventionen	Bedeutung
farbmarkiert	noch zu diskutierende Punkte

Richtlinie SA

- Inhalte:
  - Übergeordnetes (Dachdokument)
  - Standardprojekt
    - Viele Inhalte aus der D RTE 25100 1. Ausgabe sind in der RL SA Teil Standardprojekt aufgegangen.
  - Entwicklungsprojekt
    - Dieser Teil ist neu entstanden
  - Anhänge



D RTE 25100 Nachweisführung SA

- Ziel und Inhalte
  - Praxisnahe Vertiefung der RL SA
  - Detailangaben zu Begriffen und Prozessen der Nachweisführung
  - Praktische Hinweise zur korrekten und effizienten Dokumentation
  - Hilfsmittel

- Hilfsmittel zur RL SA
  - Hilfsmittel angepasst auf die neue RL SA
  - Checklisten:
    - Farbkennzeichnung
    - Dokumente Entwicklungsprojekt
  - Vorlagen:
    - Sicherheitsbericht
    - Sicherheitsnachweis
    - Freigabe Betriebsaufnahme
    - IOP Konformitätserklärung

D RTE 25096 Planungsprozess SA

- Ziele
  - Stellung der SA in Eisenbahnprojekten und der möglichen Schnittstellen zu anderen Gewerken
  - Einordnung der Planung von SA-Projekten in Planungsprozesse
  - Definition eines generischen Planungsprozesses für SA-Projekte
  - SA-Planung besser verstehen, sowie die Eigenheiten und die Notwendigkeit einer Koordination mit anderen Fachbereichen erkennen
  - Einarbeitung von neu auf dem Gebiet tätigen Personen
  - Navigationshilfe durch die hoheitlichen Vorgaben, die verwandten RTE und die bestehenden Planungsprozesse

- Zielgruppe
  - SA-Planer und Personen aus anderen Fachbereichen, welche mit SA-spezifischen Themen in Berührung kommen

D RTE 25096 Planungsprozess SA

- Inhalte
  - Generischer Planungsprozess SA
  - Arbeitspaket 1: Konzept
  - Arbeitspaket 2: Systemdefinition
    - Grundlagenbeschaffung und -verifizierung
    - Projektorganisation
    - Beschreibung des technischen und betrieblichen Umfelds
    - Analyse der Schnittstellen
    - Definition von Fahrstrassen, Geschwindigkeiten und Signalisierung
    - Anforderungen an die Infrastruktur
  - Arbeitspaket 3: Bauprojekt bzw. Bau- und Auflageprojekt
    - Beschaffung weitergehende Grundlagen
    - Technische und betriebliche Planung

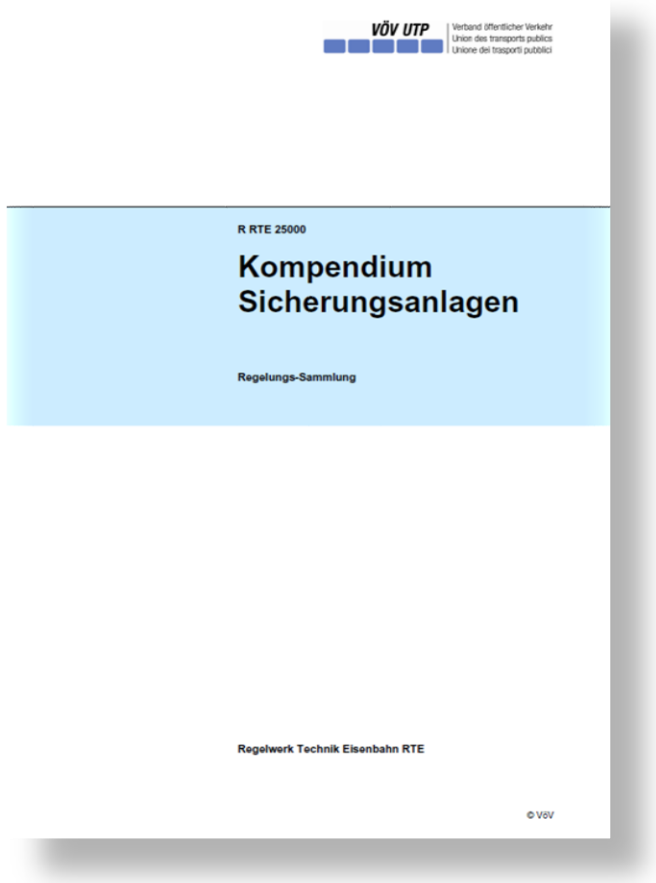
Weitere Schritte

- Terminplan:
  - 1.Q. 2025 — Fertigstellung und Reviews in PGr
  - 2.Q.2025 — Vernehmlassung RL SA 4.0 mit Lesung D RTE 25100 und 25096
  - 2.Q. 2025 — Parallele VöV-Fachtagung RL SA / D RTE 25100
  - 3.Q. 2025 — Publikation RL SA 4.0
Publikation D RTE 25100
Publikation D RTE 25096

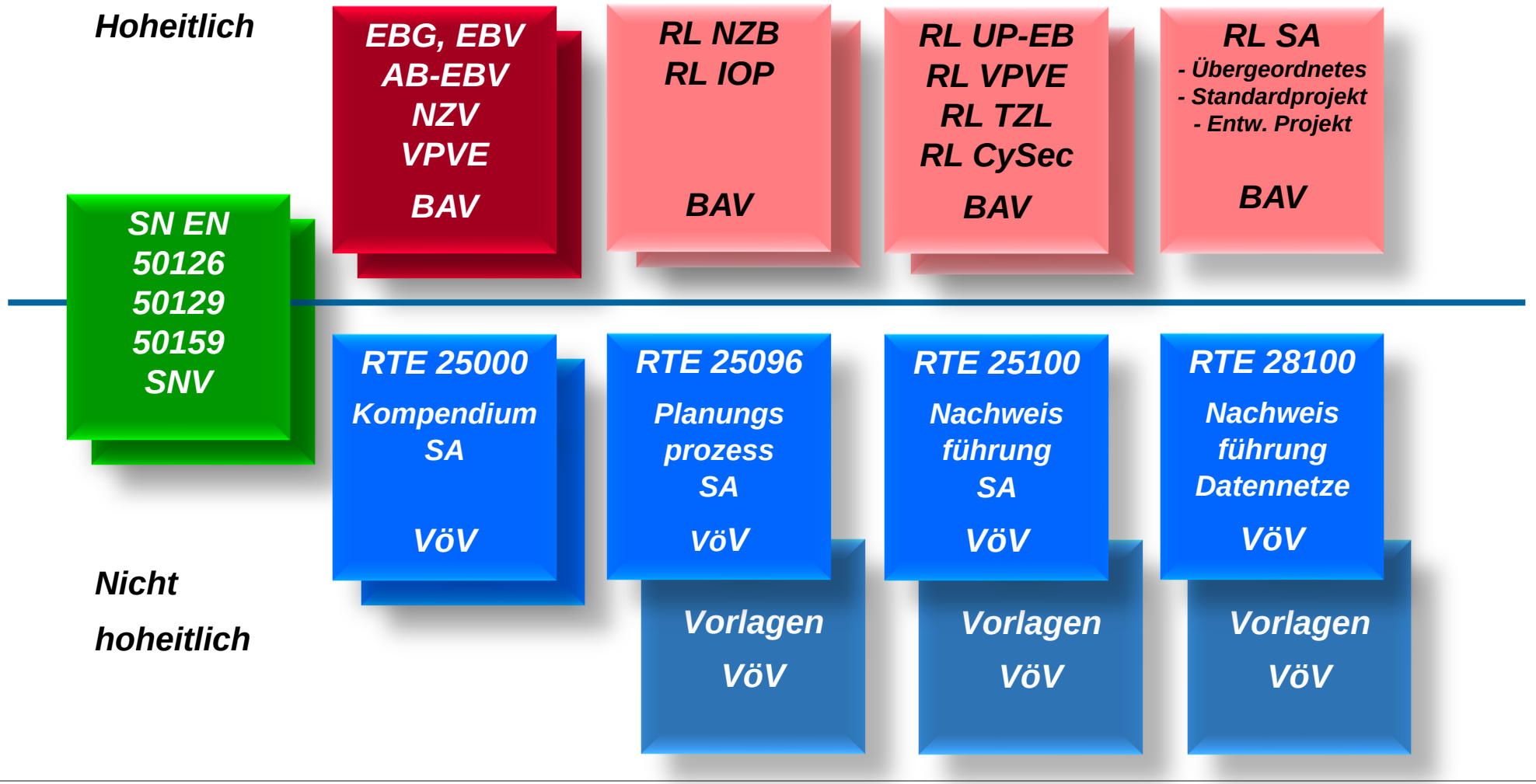
R RTE 25000 Kompendium SA

- Anpassungen in Ausgabe 13:
  - Grössere Themen (R RTE 25053, 25056 und 25063)
  - Kleinere Anpassungen in weiteren 21 Regelungen

- Stand:
  - 2. Lesung erfolgt im 3.Q.24
  - Fertigstellung läuft
  - Publikation geplant für 1.03.2025

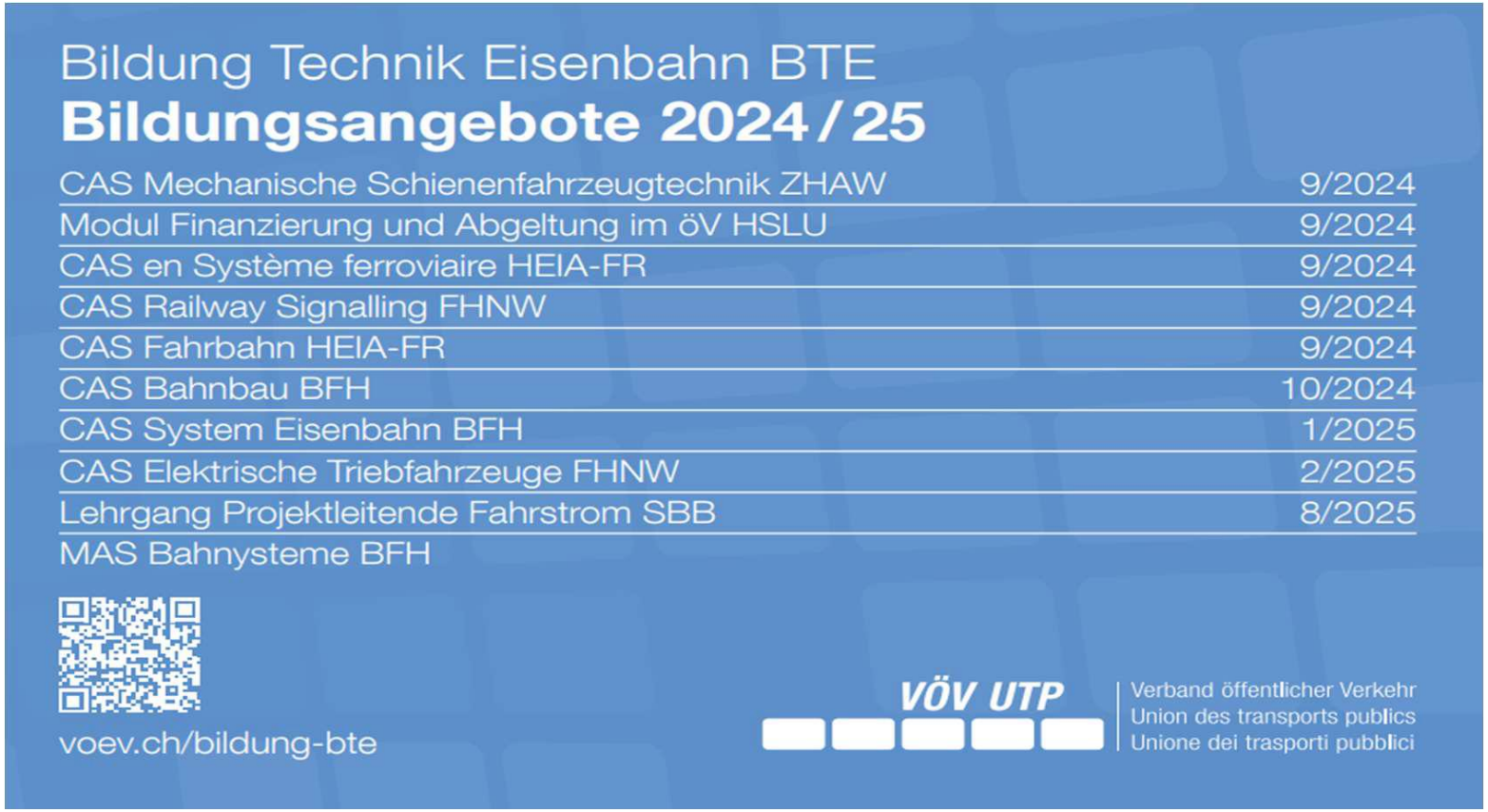


Übersicht Regelungen SA



Bildung Technik Eisenbahn BTE

- Aktuelles Angebot



www.voev.ch/Bildung-BTE

CAS Railway Signalling FHNW

- Neues Angebot der FHNW Windisch in Zusammenarbeit mit eduRail und VöV
- Erstausgabe läuft aktuell mit 14 Teilnehmern
  - STADLER 3, STASIG 2, Ing.Büros 2
    BLS 3, RhB 1, SOB 1, SZU 1, VBZ 1
- Vorbereitungen für 2. Ausgabe 2025/26 gestartet
  - Bitte Info an potentielle Teilnehmer weitergeben

www.fhnw.ch/cas-railway-signalling

Inhalte

- **Aufbaumodul Bahnsicherung**
  Sicherheit im Bahnbetrieb, Planungs- und Realisierungsprozesse, Bahnsicherungsgrundlagen, ERTMS,Zulassungs- und Nachweisprozesse.
- **Vertiefungsmodul Zugbeeinflussung**
  ETCS und ZBMS-Systemfunktionen, ETCS Onboardausrüstung und Streckeninfrastruktur, Migration und Zulassung, ERTMS-Strategie, ATO, CBTC und weitere Zukunftsthemen.
- **Vertiefungsmodul Stellwerktechnik**
  Stellwerke und Aussenanlagen, Leittechnik, Spezialanlagen, Assetmanagement, Digitalisierung und Zukunftsthemen.

Fragen zu den Referaten

VÖV UTP
Verband öffentlicher Verkehr
Union des transports publics
Unione dei trasporti pubblici

Normen Security-Safety (IEC, CENELEC)

Matthias Glock, SBB, Infrastruktur, NAT, IISO
Jean-Christophe Grandchamp, SBB, Infrastruktur, NAT-Telecom
Robert Leemann, Präsident Fachgruppe Elektrotechnik

Mittwoch, 11.12.2024

Normen Security-Safety (IEC, CENELEC)

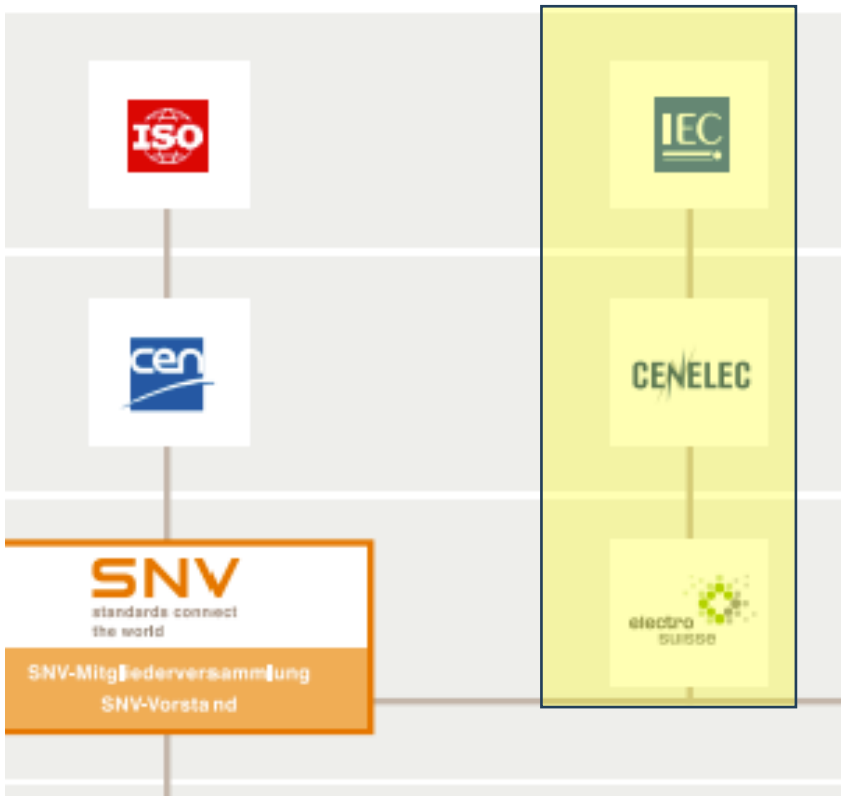
• Allgemeine Informationen	R. Leemann
• Weiterentwicklung EN 50159	J.-Ch.Grandchamp
• Weiterentwicklungen der IEC 63452	M. Glock
• Informationen zu EN 50126 und CENELEC TS 50701	R. Leemann

Normen: Allgemeine Informationen

- NORM
  «*Eine Norm ist ein Dokument, das mit Konsens erstellt und von einer anerkannten Institution angenommen wurde. …*» *[SN EN 45020]*

- Bereich Elektrotechnik
  IEC International Electrotechnical Commission
  und
  CENELEC Comité Européen de Normalisation Électrotechnique

Normen: Allgemeine Informationen



weltweit	IEC – TC9	Technical committee 9
europaweit	CENELEC – TC9X	Technical committee 9X
schweizweit	TK 9	Technisches Komitee 9 Spiegelkomitee CH

Normen: Allgemeine Informationen

- Die CH, vertreten durch CES der electrosuisse, ist Mitglied in der IEC und im CENELEC
- Expertinnen und Experten mit Branchenmitgliedschaft electrosuisse → Mitwirken in working groups und Gremien von IEC und CENELEC
- Alle Eisenbahn-Elektronormen werden in IEC TC 9 oder in CENELEC TC9X betreut.
  Spiegelkomitee ist TK 9.

- TK 9
  - sucht und bestimmt die Expertinnen und Experten
  - konsolidiert die Rückmeldungen CH zu einer Stellungnahme
  - meldet Stellungnahmen und „Namen“ nach Brüssel bzw. Genf

Weiterentwicklung EN 50159 «Sicherheitsrelevante Kommunikation in Übertragungssystemen»

Jean-Christophe Grandchamp,
SBB, Infrastruktur, TC

Mitglied der CENELEC WG 16 IT-Security

Weiterentwicklung EN 50159

Stand der Revision EN 50159

TC 9X/SC 9XA/WG 16:

2023-05	“Decision to revise -> WG16”
2023-09	“NWIP for EN 50159 Maintenance”*
2024-11-20	**“Delivery of ENQ draft”**
2025-02-19	“Submission of enquiry draft”
2025-05-14	“Closure of enquiry”

* New Work Item Proposal

Weiterentwicklung EN 50159

Ziel der Revision der CENELEC EN 50159

1. Anpassungen zur EN 50129 Norm

2. Anpassungen / Ausgliederung der Cybersecurity Themen (CLC/TS 50701)

3. Harmonisierung der Fachausdrücke zu EN 50129 & TS 50701

Weiterentwicklung EN 50159

Die Änderungen der laufenden Revision der CLC EN 50159
(nicht offiziell!)

- Definitionen wurden angepasst
- Cybersecurity Themen angepasst resp. “Stand der Technik”
- Referenzieren, Verweis der Themen von TS 50701
- Referenz Architektur wurde praxis orientiert überarbeitet
- Verständlichere Anforderungen der Kategorie 3 (insbesondere zu Cybersecurity)
- Aktualisierung, Verbesserung der Verständlichkeit betreffend “Safety Code”

Weiterentwicklung
IEC 63452 «Railway applications – Cybersecurity»

Matthias Glock,
SBB, Infrastruktur, NAT-TO-SEY,
Infrastructure Information Security Officer

Mitglied der CENELEC WG 26 und IEC PT 63452

Weiterentwicklung IEC 63452: Schwerpunkt

Dieses Dokument bietet einen einheitlichen Ansatz für das Management der Cybersicherheit von Bahnsystemen. Es gilt für alle Bereiche, die in den Geltungsbereich von IEC TC 9 fallen.

Das Dokument überträgt und passt die Anforderungen der IEC 62443-Standards an den Bereich der Bahnanwendungen und das betriebliche Umfeld an und erläutert, wie diese Anforderungen in diesem Kontext angewendet werden.

Es bietet eine Anleitung dazu, wie der Sicherheitsprozess mit dem generischen Lebenszyklus für Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit und Sicherheit (RAMS) der IEC 62278-Standards verknüpft werden kann.

Weiterentwicklung IEC 63452: Lieferobjekte

Typische Lieferobjekte:

- Cybersecurity Management Plan (CSMP)
- Initiale Risikoanalyse (IRA)
- Detaillierte Risikoanalyse (DRA)
- System under Consideration (SuC)

Rollen, Aufgaben, Verantwortung:

- Operator, System Integrator, Service Provider, Railway Duty Holder, ...

Weiterentwicklung IEC 63452: Diskussionen

Beispiele:
- Einbindung Cybersecurity in RAMS Modell (nicht sinnvoll)
- Verantwortlichkeiten der Hersteller bei Bestandsanlagen
- Mehrdimensionale Rollen (Operator ist auch Systemintegrator)
- Cybersecurity ist kein Addon zu Safety (Principles CLC)

Eingaben (aktuell durch SBB und OeBB):
- Triggerpunkte Cybersecurity und Regulatorik
- Klärung Taxonomy (Solution, Application, System) mappt nicht zu SUC

Danke,
Merci
& Grazie.

In the world of OT Cybersecurity, being ready isn't enough—you must be On Time!

Informationen EN 50126 und TS 50701

Robert Leemann,
Präsident VöV-Fachgruppe Elektrotechnik

(SBB, Regulation und Internationales)

Mitglied TK 9 (längere Zeit SC9XA)

Informationen EN 50126 und TS 50701

EN 50126-x: Spezifikation und Nachweis von Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit und Sicherheit

Gültige Ausgabe	2017; e, d, f
Bearbeitung	in WG 21 → Amendement
Parallel dazu	IEC 62278-x in Weiterentwicklung

xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

CENELEC TS 50701: «Bahnanwendungen – Cybersecurity»

Gültige Ausgabe	2023; e, d.
Bearbeitung	[CLC-WG 26] → offered to IEC, 63452

Fragen zu den Referaten

VÖV UTP
Verband öffentlicher Verkehr
Union des transports publics
Unione dei trasporti pubblici

Infos VöV

Marcel Schmid, Projektleiter System Bahn

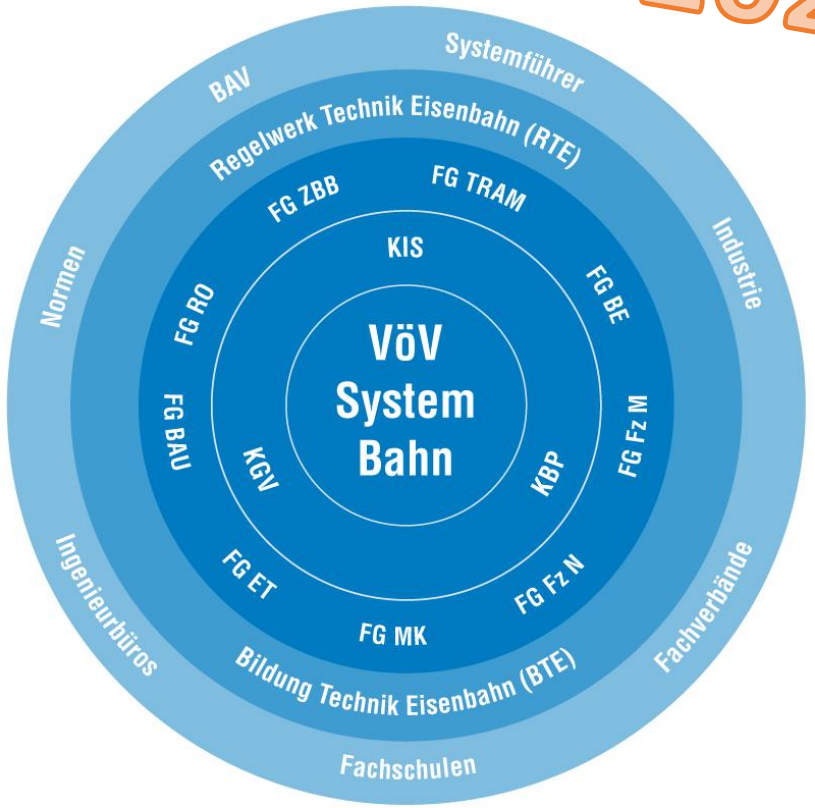
Mittwoch, 11.12.2024

Infos VöV

Publikation
Mitte Dez. 2024

- **Newsletter System Bahn**

- Events: VöV-Agenda, Erfa CyberSec 2025, Gleisbaukurs ZBB,..
- Förderprogramm BAV
- Normenplattform VöV
- SBB-Regelungen
- Systemführer Zugkommunikation
  3G Abschaltung !
- …



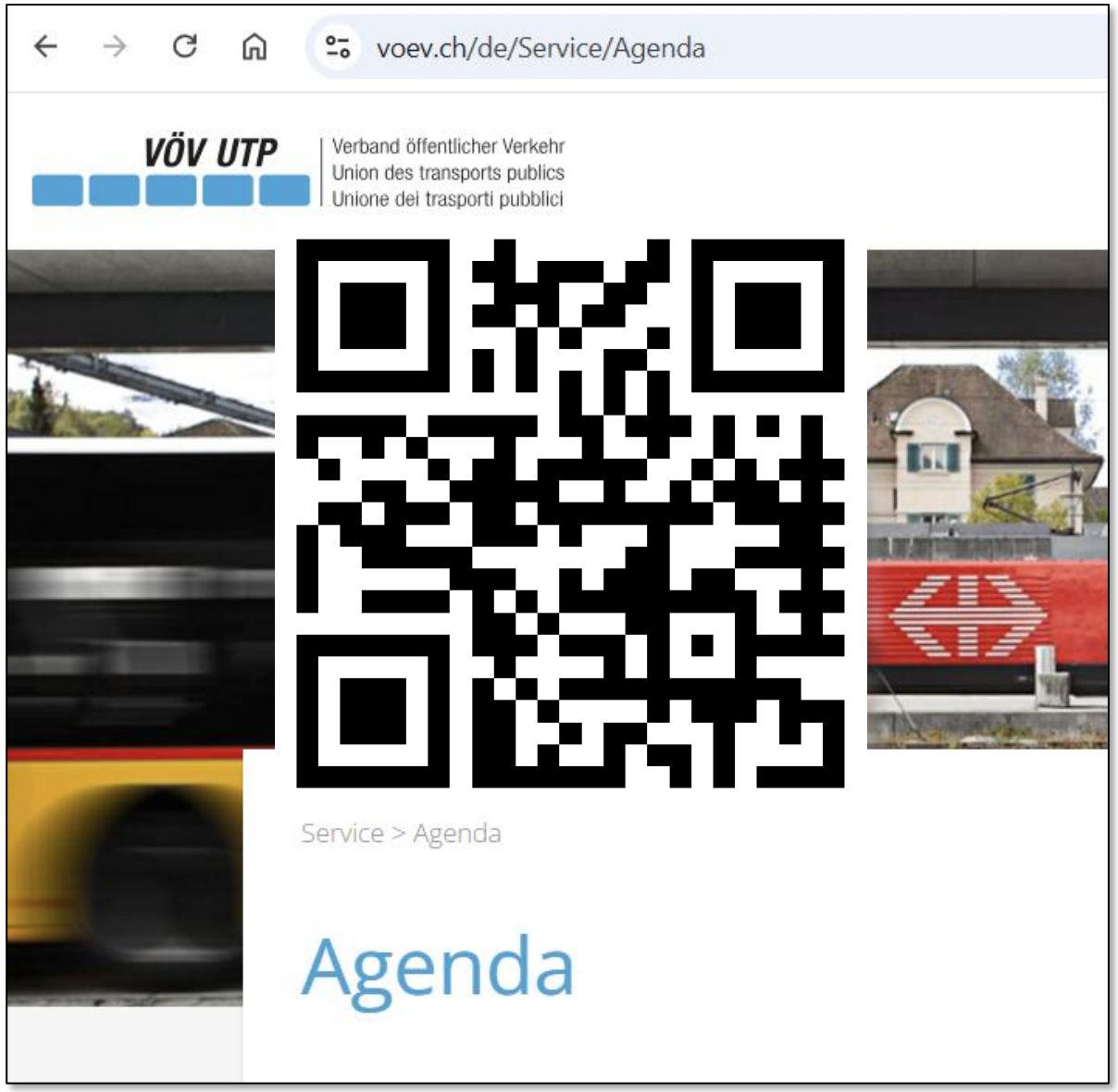
VöV Terminübersicht

Übersicht wichtige VöV Termine

- Tagungen
- Kurse
- weiteren Anlässe

zusammengefasst unter

www.voev.ch/agenda



VöV Agenda

- Terminreservierung
  - Laden Sie hier den Outlook-Termin für ihren Kalender herunter
- Einladungsliste
  - Schreiben Sie sich hierüber in eine Interessentenliste ein. Sie erhalten ein EMail, sobald die Anmeldung freigegeben ist.
- Anmeldung
  - Link direkt auf die Anmeldeplattform

Fachtagung OT CyberSecurity SA

Jetzt Termin vormerken und in der VöV Agenda einschreiben!

- Entwicklung der Tagung 2025 gestartet
  - Termin: **25.06.2025**
  - Ort: **Raum Bern**
  - Grobprogramm / Teilnehmende
    Vormittag: Referate (für Alle offen)
    Nachmittag: Workshop's
    für Mitarbeitende EBU
  - Themen: **Rückmeldungen aus Tagung 2024 & Aktuelles 2025**

Fachgruppensitzungen mit erweitertem Teilnehmerkreis

- Punktuell werden Fachgruppensitzungen für einen erweiterten Teilnehmerkreis geöffnet
- In der Regel 1x jährlich
- **Fachexperten der Bahnunternehmen sind eingeladen an diesen geöffneten Sitzungen teilzunehmen.**
- **Chance nutzen !**
- **Bietet einen direkten Einblick in die Tätigkeit der Fachgruppe.**

Fachgruppensitzungen mit erweitertem Teilnehmerkreis

Fachgruppe Elektrotechnik

Themen aus dem Bereich

- Fahrstrom,
- 50Hz
- und SA Technik.

- AGr Beleuchtung, Bahnübergang, CyberSec SA/OT (in Planung)

«offene Sitzung» findet statt

- Wann: 23.01.2025
- Wo: Wallisellen

Teilnahmebedingung: Mitarbeitende einer Bahnunternehmung (Mitglied VöV)

Bei Interesse melden bei: Marcel.schmid@voev.ch

Fachgruppensitzungen mit erweitertem Teilnehmerkreis

Fachgruppe Mobilkommunikation

Themen aus dem Bereich

- Mobile Bahnkommunikation
- SF Zugkommunikation
- Tunnelfunk
- ERTMS – FRMCS
- GSM-R
- Weitere Funksysteme

«offene Sitzung» findet statt

- am 23.04.2025, in Bern Geschäftsstelle

Teilnahmebedingung: Mitarbeitende einer Bahnunternehmung (Mitglied VöV)

Bei Interesse melden bei: Marcel.schmid@voev.ch

Fragen zu den Referaten

D RTE 28100 Nachweisführung Datennetze

- Erfolgt:
  - Publikation 1.09.2024
  - Fachtagung 11.12.2024

- Weiteres Vorgehen nach Bedarf der Branche:
  - RTE-Schulung (Zielgruppe, Inhalte, Umfang, …)
  - VöV-Erfahrungsgruppe (Periodischer Austausch)
  - RTE-Projektgruppe
    - Anpassung Vorlagen kurzfristig
    - Anpassung Regelung mittelfristig
  - RTE-Datennetze in Fahrzeugen inkl. Schnittstellen
  - …

Herzlichen Dank

- ✓ Herrn F. Fellay, dipl. El.-Ing. ETH,
  für Ihre ausgezeichneten Übersetzungen der Beiträge

- ✓ allen Referenten
  für die Vorbereitung und die Präsentation der Themen

- ✓ dem Organisationsteam VöV
  Nicole Reinhard, Marcel Schmid, Urs Walser und weiteren
  für Bild, Ton, Speis und Trank!

- ✓ den Tagungsteilnehmenden
  für die Aufmerksamkeit und das engagierte Mitwirken

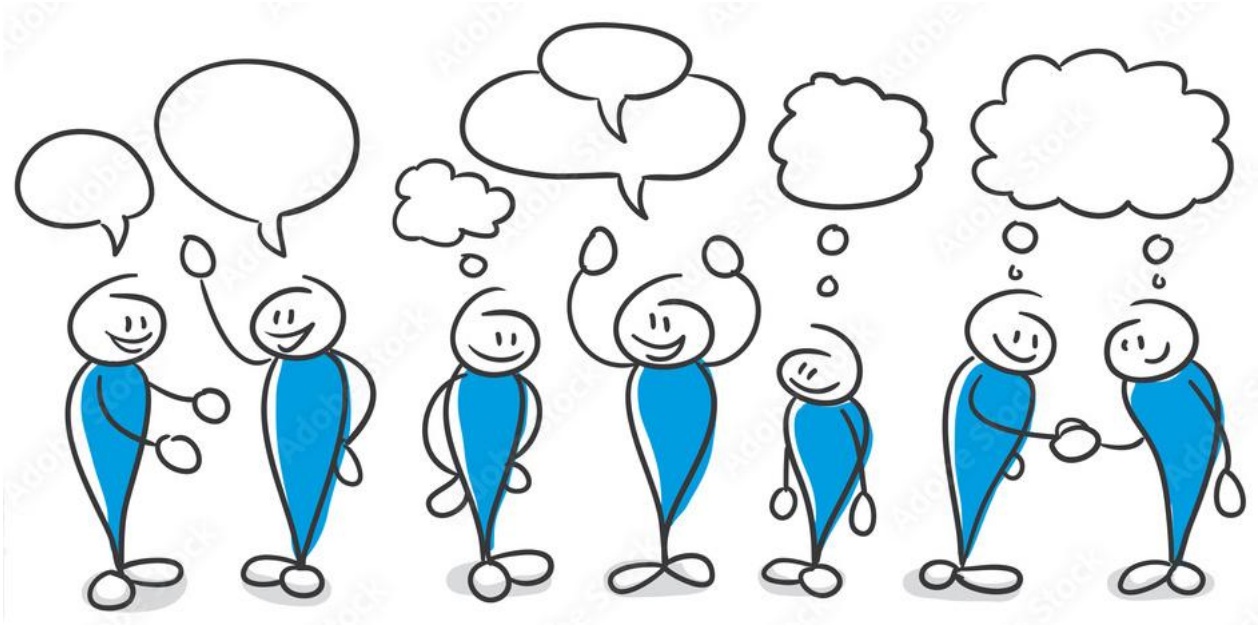
Zum Schluss – drei Wünsche

1. **Feedback – wir wollen besser werden**
   Umfrage folgt per Mail
   - falls Sie nicht zufrieden sind → sagen Sie es nur uns, aber genau
   - falls Sie zufrieden sind → sagen Sie es weiter - und uns auch

2. **Kopfhörer**
   Bitte beim Eingang abgeben

3. **Nutzen Sie die Chance für weitere Kontakte**
   viele Experten sind heute vor Ort, sprechen Sie sie an, fragen Sie.
   Ab Bern verkehren auch 1630 und 1700 Uhr noch viele Verbindungen …

Einladung zum informellen Austausch bei Kaffee und Kuchen



… und kommen Sie gut nach Hause

RESERVE

Verbindlichkeit von RTE-Regelungen

- Grundsatz:
  RTE-Regelungen sind freiwillige Empfehlungen des VöV an die Mitgliedsunternehmen.
  → Die Direktionen entscheiden bei jeder Ausgabe.

- In Verträgen können RTE-Regelungen als Teil des Vertrags vereinbart werden.

- Auch ein Amt kann eine RTE-Regelung als verbindlich erklären.