Sicherheitsanforderungen an eine Zugintegritätsprüfung – der Mythos von SIL 4

Ergebnisse von Studien der M2C Expert Control GmbH
Im Auftrag der SBB und ÖBB

Welche Sicherheitsintegrität muss eine Zugintegritätsprüfung haben?

Eckehard Schnieder
Jörg May
Jürg Suter
Florian Peche
Andreas Dodinoiu

Zugintegrität

Qualitative Anforderungen der Use Cases 1.1 Gleisfreimeldung und 1.2 Zugendeposition

1.1	Use Case „Schnelle und präzise Freimeldung Gleis, Weiche, Barriere“	SIL3/ SIL4
1.1.1	Fast vollständige Reduktion der GFM, GFM nur noch in Netzzugangsbereichen zur Detektion nicht ausgerüsteter Fahrzeuge	
1.1.2	Schnelle Umstellung Weichen / Öffnung Barriere nach Zugüberfahrt (je nach heutiger Fahrstraßenlogik) mit weniger Komplexität / Systemaufwand möglich als mit heutigen GFM.	
1.1.3	Bessere, da dynamische Ausnutzung der Topologie mit Zügen (weniger Topologiereserven)	
1.1.4	Stärkere Mehrfachbelegung von heutigen Gleisen in der vollen Länge ohne Notwendigkeit von kurzen GFM-Abschnitten	
1.1.5	Vermeidung von Topologieanpassungen oder hohen Balisenmengen aufgrund der heute ungenauen oder nicht vertrauenswürdigen Lokalisierung der ETCS OBU	

1.2	„Präzise Zugendeposition (insbesondere Güterzüge)“	SIL ?
1.2.1	Zugintegrität, um ETCS L3 und moving block zu ermöglichen	?
1.2.2	Automatische Zuglängenberechnung	?

Use Case Analyse

Zugintegrität

Stand der Technik

- Im Rahmen der Überlegungen, welche Aufgaben unter Wegfall bisheriger streckenseitiger Lokalisierungseinrichtungen bei einer ausschließlich auf Fahrzeugen platzierten Fahrzeuglokalisierung wahrgenommen werden sollen, wird für den Use Case 1.2.1 „Zugintegrität“ die quasi unumstößliche Notwendigkeit postuliert, das Zugende technisch zu identifizieren, zu lokalisieren und zu kommunizieren. Dies erfolgte vermutlich infolge der früher vom Streckenpersonal wahrgenommenen Zugschlusserkennung, z.B. durch Tafeln am letzten Waggon des Zugverbandes zur Gleisfreimeldung.

- Im EU-Großforschungsvorhaben Shift2Rail wird gegenwärtig mit großem Aufwand nach Lösungen gesucht, die stillschweigend die höchste Sicherheitsintegritätsstufe SIL4 als Anforderung voraussetzen.

- Im Rahmen von Untersuchungen zum SBB Proof of Concept wurden 25 Lösungstypen in insgesamt 609 Dokumente identifiziert, von denen aber keine eine Anwendungsreife erlangte.

- Nach eigenen Recherchen und ist keine Untersuchung bekannt, um für eine entsprechende Zugschlussanzeige die Forderung der höchsten Sicherheitsintegritätsstufe zu begründen.

- Persönliche Aussage bei einem Gespräch Prof. Schnieder mit Dr. Josef Doppelbauer, Präsident der ERA, am 18./19.03.2019 in Wien anlässlich der GSA/ESA Tagung GNSS for Railways: "Mir ist keine belastbare Grundlage bekannt, das Zugende mit einer Sicherheitsintegrität SIL 4 zu bestimmen."

Quellen für die Sicherheitsanforderung nach CSM VO

- **Regelwerke**

  Analogie aus bestehenden Regelwerken oder Lastenheften

  (VDV 331, VDV 332, ETCS TSI Subsets, Cenelec-Normen, EBO, EisbVO, AEBV..)

- **Referenzsysteme**

  aus Sicherheitstatistiken (z.B. Szenarienhandbuch der SBB)

  aus Statistiken der Verfügbarkeit (z.B. ungewollte Zugtrennung)

  z.T. Harmonisierung der Bezugsgrößen und -werte notwendig

- **Explizite Risikoabschätzung**

  mittels Expertenbefragungen

  mittels modellgestützten Analysen und Simulationen

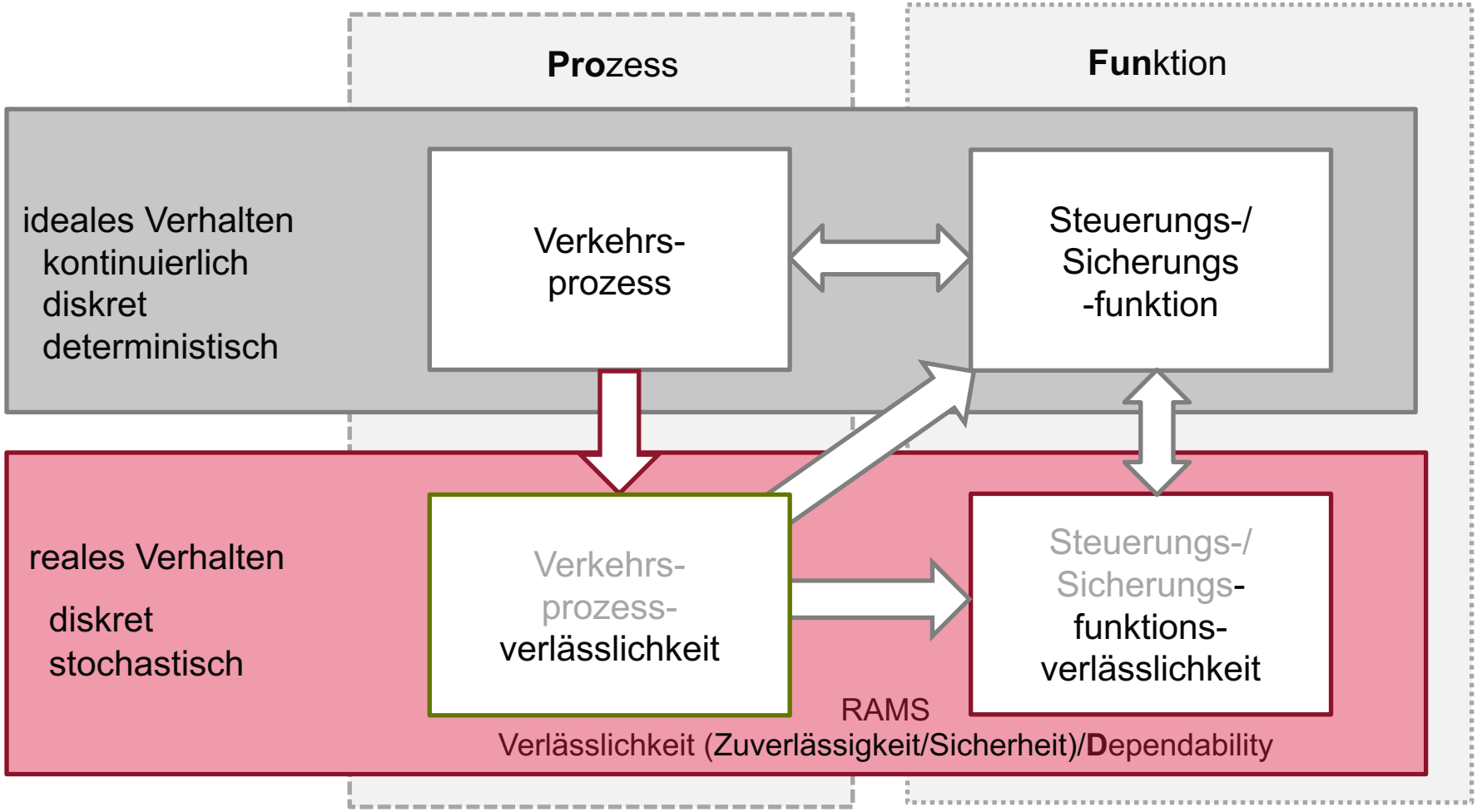
  Verwertung von Forschungsprojekten

  Betriebliche Leistungsfähigkeit (Zugfolge, Durchrutschweg)

  eigene Erfahrung und Expertise

ProFunD Modellkonzept nach IEC 62551:2012

Methodischer Ansatz zur Ermittlung von Sicherheitsanforderungen



ProFunD Modellkonzept nach IEC 62551:2012

Anwendung von Regelwerken

Prozess | **Funktion**

ideales Verhalten
kontinuierlich
diskret
deterministisch

Regelwerke
Analogie aus bestehenden Regelwerken oder Lastenheften
(VDV 331, VDV 332, ETCS TSI Subsets, Cenelec-Normen, EBO, EisbVO, AEBV..)

reales Verhalten
diskret
stochastisch

AB 52.1 Anforderungen an Bremssysteme
1 Die Eisenbahnfahrzeuge sind in der Regel mit einer automatischen Bremse auszurüsten:
- mit der jederzeit angehalten werden kann;
- die bei Zugtrennung auf jedem Zugteil selbsttätig wirkt;
- die unabhängig von einer Energiequelle ausserhalb des Fahrzeugs ausreichend lange wirksam ist;

Zugunglück infolge Zugtrennung

Berichterstattung in der Presse: **KURIER** am 2.12.2015

Zugunglück infolge Zugtrennung

Amtlicher Untersuchungsbericht: Klärung der Ursache (Seite 48/64)

Untersuchungsbericht

Sicherheitsuntersuchungsstelle des Bundes
GZ: BMVIT-795.369-IV/SUB/SCH/2015

12.1.2 Zugtrennung

Während der Fahrt des Z 42322 auf dem Streckengleis 1 zwischen Bf Breitenstein und Bf Semmering ereignete sich eine **Zugtrennung** zwischen dem Zug-Tfz und dem ersten Wagen. Z 42322 kam im Gleisabschnitt zwischen dem Sbl „Bt1“ und dem Bf Semmering im Strecken-km 102,300 vor dem ES „A“ des Bf Semmering zum Stillstand.

Bei der durch den Tfzf des Z 42322 durchgeführten Prüfung wurde festgestellt, dass auf Grund der Schäden an der Zugeinrichtung des ersten Wagens eine Wiedervereinigung nicht möglich war.

Zur **Klärung der Ursache der Zugtrennung** wurde eine technische Untersuchung der Zugeinrichtung des betreffenden Wagens durchgeführt. Bei dem Wagen mit der Wagennummer 31 75 4540 158-8 handelt es sich um einen Wagen der Gattung „Lgjs“ des VK „Türkische Staatsbahnen (TCDD)“. Dieser wies eine gültige Eintragung im Europäischen Register genehmigter Fahrzeugtypen gemäß Artikel 34 der der RL 2008/57/EG auf.

Bei der technischen Untersuchung konnte bei der Zugeinrichtung **ein Gewaltbruch mit Vorschädigungen** sowie im Bereich der Bruchstelle Einkerbungen und Schweißraupen festgestellt werden. **Gemäß den zum Zeitpunkt gültigen Regelwerken dürfen Schweißungen im Bereich der Zugeinrichtung nicht durchgeführt werden.**

ProFunD Modellkonzept nach IEC 62551:2012

Maßnahmen laut Regelwerken

Prozess

Funktion

ideales Verhalten
kontinuierlich
diskret
deterministisch

Verkehrs-
prozess

Regelwerke
Analogie aus
bestehenden
Regelwerken oder
Lastenheften
(EisbVO, AEBV..)

Steuerungs-/
Sicherungs
-funktion

reales Verhalten

diskret
stochastisch

Explizite
Risikoabschätzung
mittels
Expertenbefragungen

verkehrs-
prozess-
verlässlichkeit

RAMS
Verlässlichkeit (Zuverlässigkeit/Sicherheit)/**D**ependability

Dynamisches Eisenbahn System Modell
Modèle dynamique d'un système ferroviaire
Dynamic model of a railway system

Normative Maßnahmen der Risikoreduktion

- Gegenwärtig sind zur Reduktion der Risiken im Zusammenhang mit Zugtrennungen vor allem normative Maßnahmen umgesetzt worden. Dies sowohl durch das Bundesamt für Verkehr BAV auf hoheitlicher Ebene als auch im Rahmen von Betriebsvorschriften durch die verantwortlichen Eisenbahnunternehmungen.

- So zum Beispiel wurde das Verfahren nach einer festgestellten Zugtrennung im Rahmen der Sicherheitsvorschriften standardisiert. Als Grundlage dazu verfährt der Lokführer nach klaren Handlungsanweisungen gemäß den internen Betriebsvorschriften (z.B. SBB: Betriebsvorschrift Sofortmaßnahmen Lokpersonal Tabelle 5-1), und der Fahrdienstleiter nach den verbindlich anzuwendenden Checklisten Fahrdienst (CL-F).

Detektion einer Zugtrennung

- Eine Zugtrennung wird in den allermeisten Fällen zuerst durch den Lokführer festgestellt, indem er einen Druckabfall in der Hauptleitung der Druckluftbremse bemerkt. In der Regel gibt es keine Anzeigeinstrumente oder besondere Einrichtungen für das Melden von Zugtrennungen.
- Die folgerichtige Interpretation des Lokführers ist Ausbildungs- und Erfahrungssache. Auch dem Fahrdienstleiter werden allfällige Zugtrennungen grundsätzlich nicht gemeldet bzw. angezeigt.
- Die Zeit vom Auftreten einer Zugtrennung bis zu ihrer eindeutigen Feststellung hängt von der Beobachtung, der Erfahrung und der Aufmerksamkeit des Lokführers, aber auch von externen Faktoren (Sicht vom Führerstand auf den Zug) ab. Im Rahmen seiner Verantwortlichkeiten und Tätigkeiten kann der Lokführer das Manometer der Hauptleitung bzw. die relevanten Anzeigen nicht dauernd, sondern nur zeitweise beobachten.
- Es sind Fälle und Umstände bekannt, nach welchen eine Zugtrennung durch den Lokführer nicht sofort oder überhaupt nicht bemerkt werden. Diese sind bei der konventionellen Schraubenkupplung als eher selten einzustufen.
- Mit der Einführung der vom Führerstand aus bedienten Automatischen Zug- und Druckkupplung AZDK sind Fehlhandlungen möglich, bei welchen ein Zugteil unbewusst bzw. unbeabsichtigt abgekoppelt

Zugintegrität

Maßnahmen zur Sicherung bei ungewollten Zugtrennungen

Dynamisches Eisenbahn System Modell
Modèle dynamique d'un système ferroviaire
Dynamic model of a railway system

Bewältigung einer Zugtrennung

- Das Vorgehen nach Feststellen einer Zugtrennung ist in den Schweizerischen Fahrdienstvorschriften FDV [(Tabelle 5-1, Nr. 1)] und in den Betriebsvorschriften (z.B. Tabelle 5-1, geregelt.
- Diese Vorschriften können mittels Ausführungsbestimmungen bzw. Betriebsvorschriften ergänzt werden
- Die Lokführer werden im Rahmen ihrer periodischen Prüfungen stichprobenweise abgefragt.
- Die Bewältigung einer Zugtrennung basiert auf eindeutig definierten Sofortmaßnahmen zur Schadensbegrenzung, auf der Basis der Kommunikation zwischen Lokführer und Fahrdienstleiter sowie auf standardisierten Sicherheitsvorschriften im Sinne von Handlungsanweisungen.
- Sonderfälle, wie unbemerkte Zugtrennungen können heute durch die Automatisierungstechnik mangels geeigneter Sensorik nicht im gleichen Umfang bewältigt werden wie durch menschliche Kognition.

Zugintegrität

Maßnahmen zur Sicherung bei ungewollten Zugtrennungen

Für das sehr geringe Risiko ungewollter Zugtrennungen sind mehrere Sicherungsmaßnahmen verantwortlich, welche die gefährlichen Folgen nahezu ausschliessen.

Fahrzeugseitige Sicherung

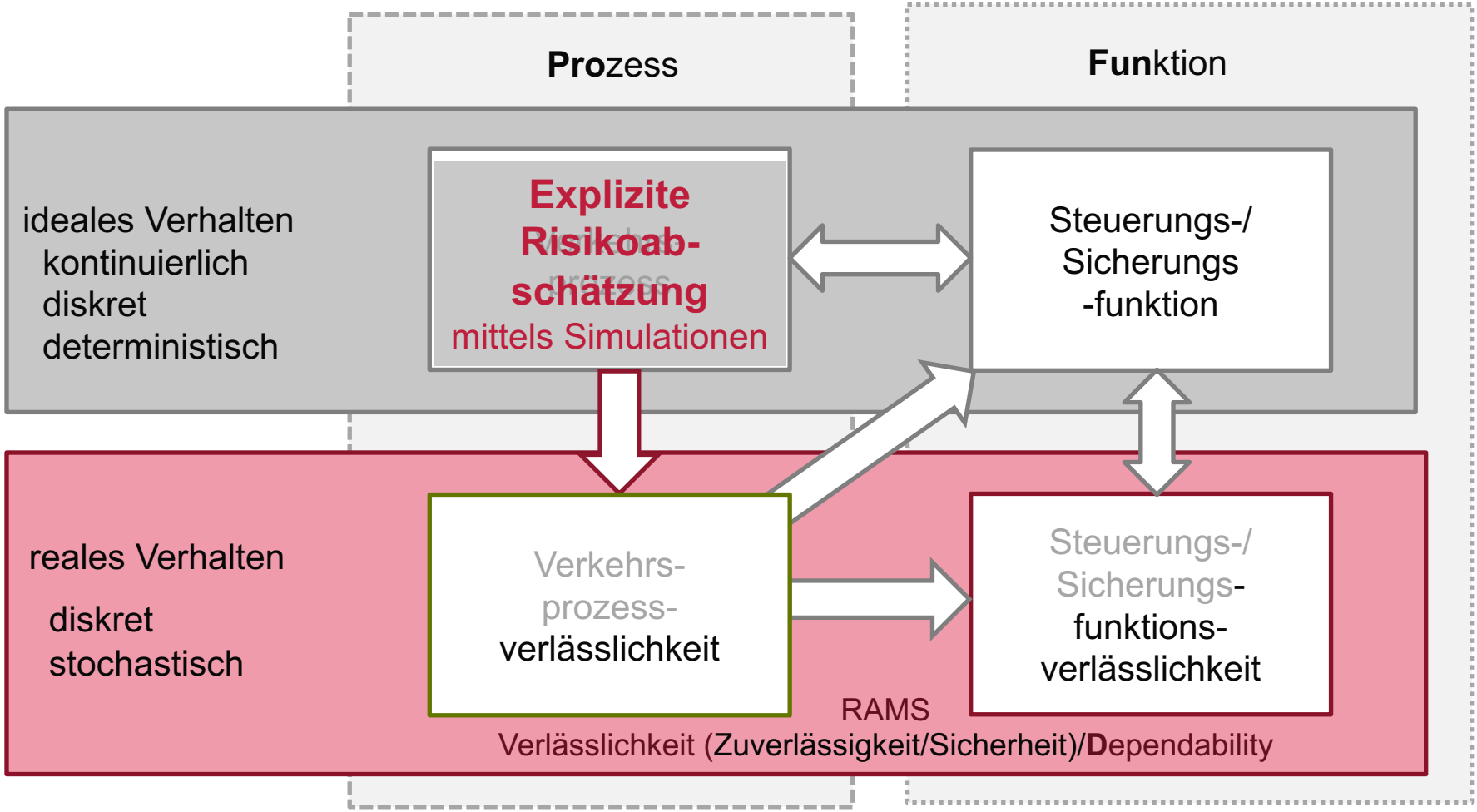
1. Fail-safe automatische Bremsung durch Trennung der Hauptluftleitung
2. Wahrnehmung der Zugtrennung im Führerstand
3. Maßnahmen des Fahrzeugführers

4. Bestehende Gleisfreimeldeeinrichtungen (4a.) und Fahrwegsicherung (4b.)
5. Anzeige der Fahrdienstleitung
6. Maßnahmen der Fahrdienstleitung.

Streckenseitige Sicherung

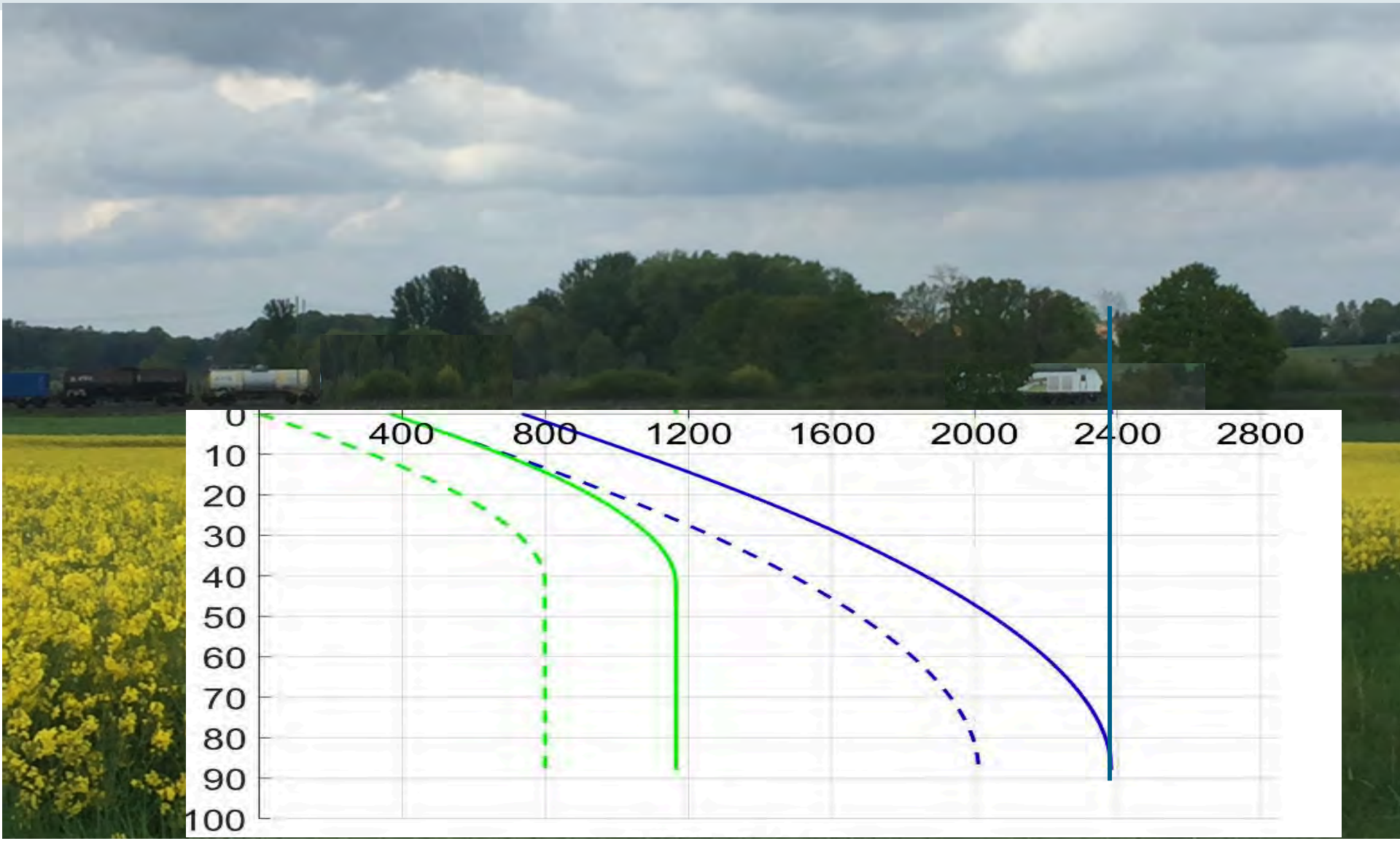
Diese Maßnahmen werden in der **sicheren Überwachung** zusammengefasst

ProFunD Modellkonzept nach IEC 62551:2012



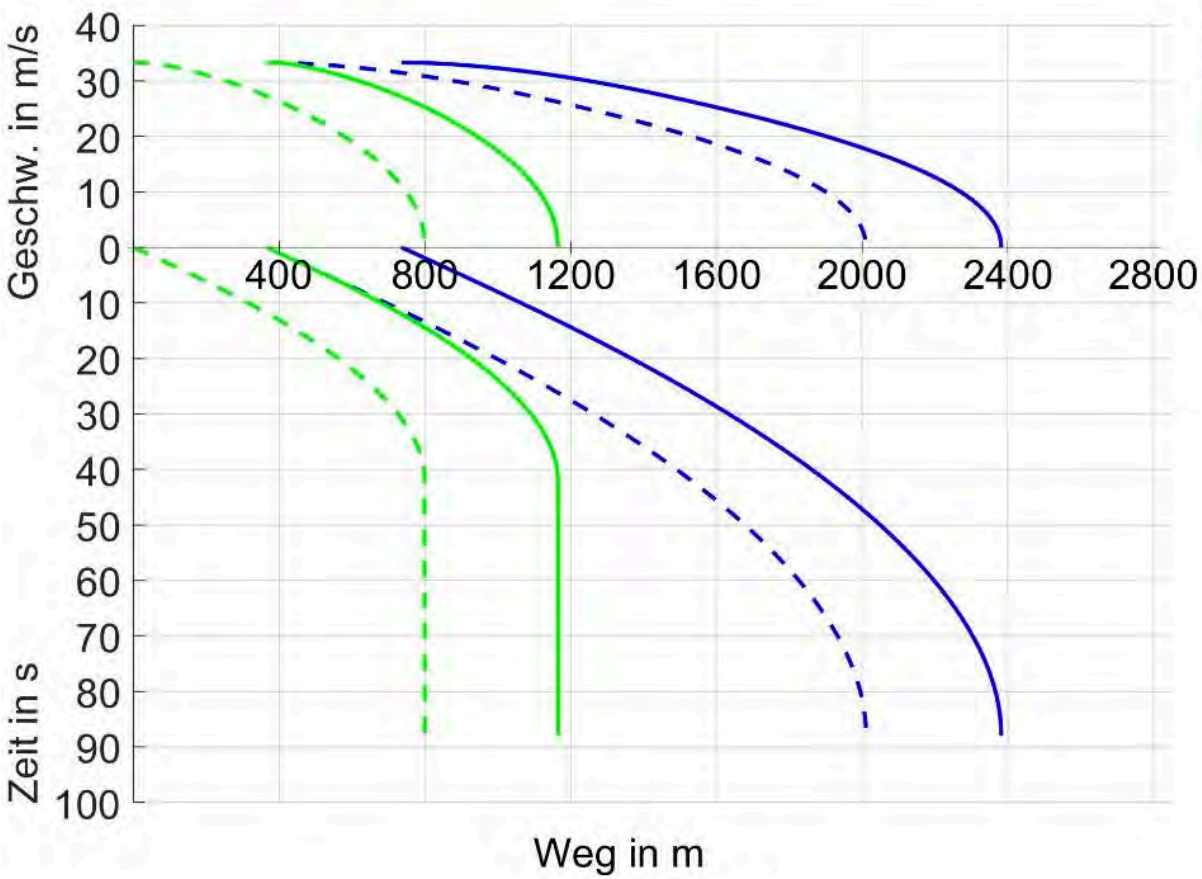
Zugintegrität

Explizite Risikoabschätzung mittels Simulation



Zugintegrität

Explizite Risikoabschätzung mittels Simulation



Bremsen o. Fkt.:
vorne konzentriert

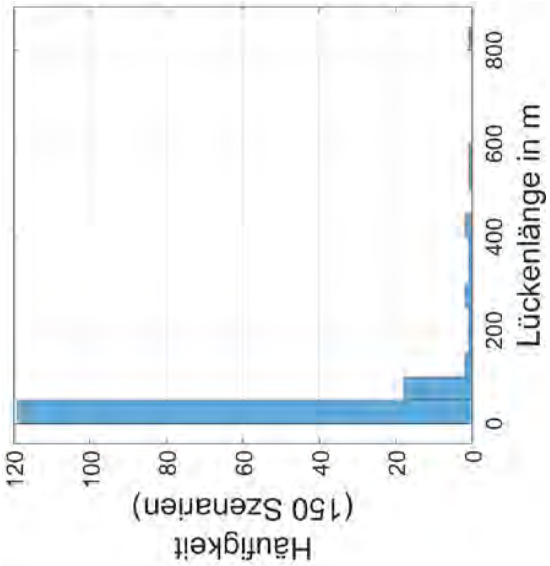
Beladungszustand:
voll-leer

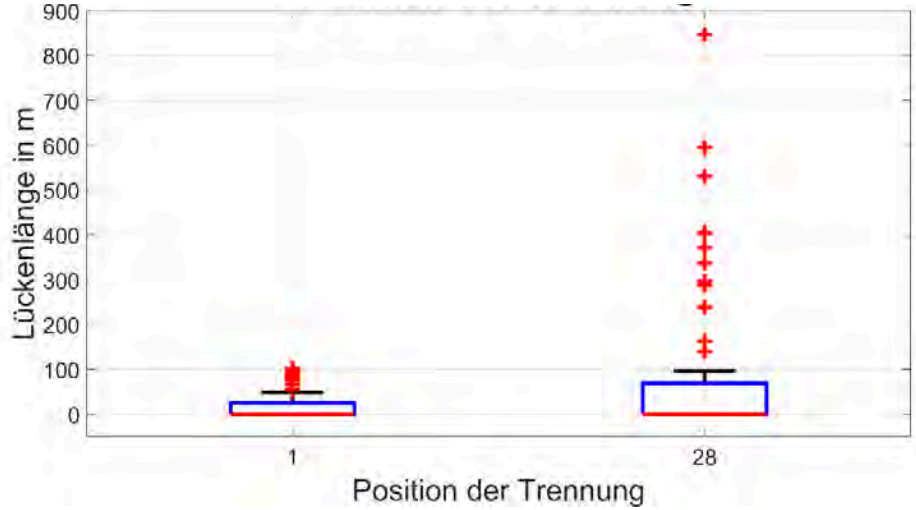
Fahrzustand:
120 km/h

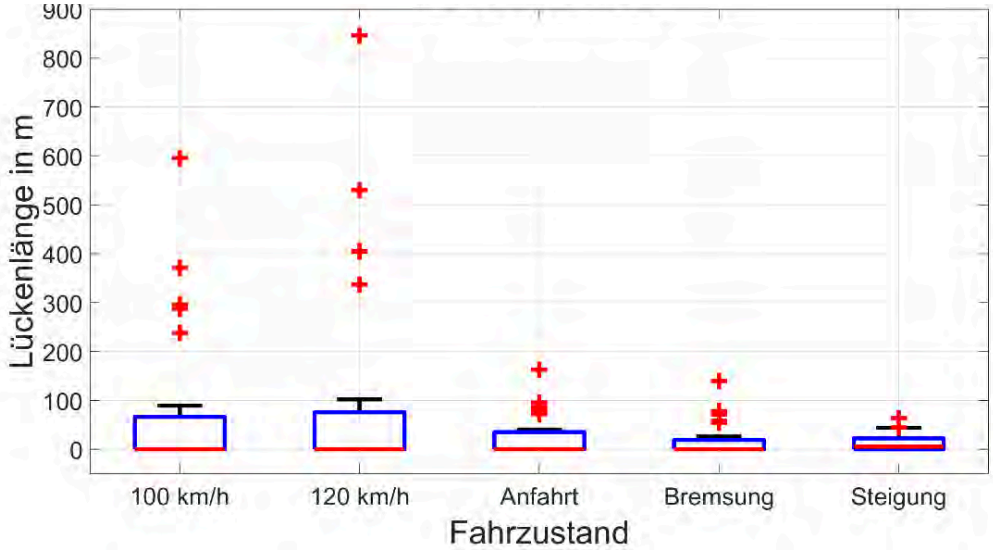
Trennposition:
28

Zugintegrität

Explizite Risikoabschätzung mittels Simulation

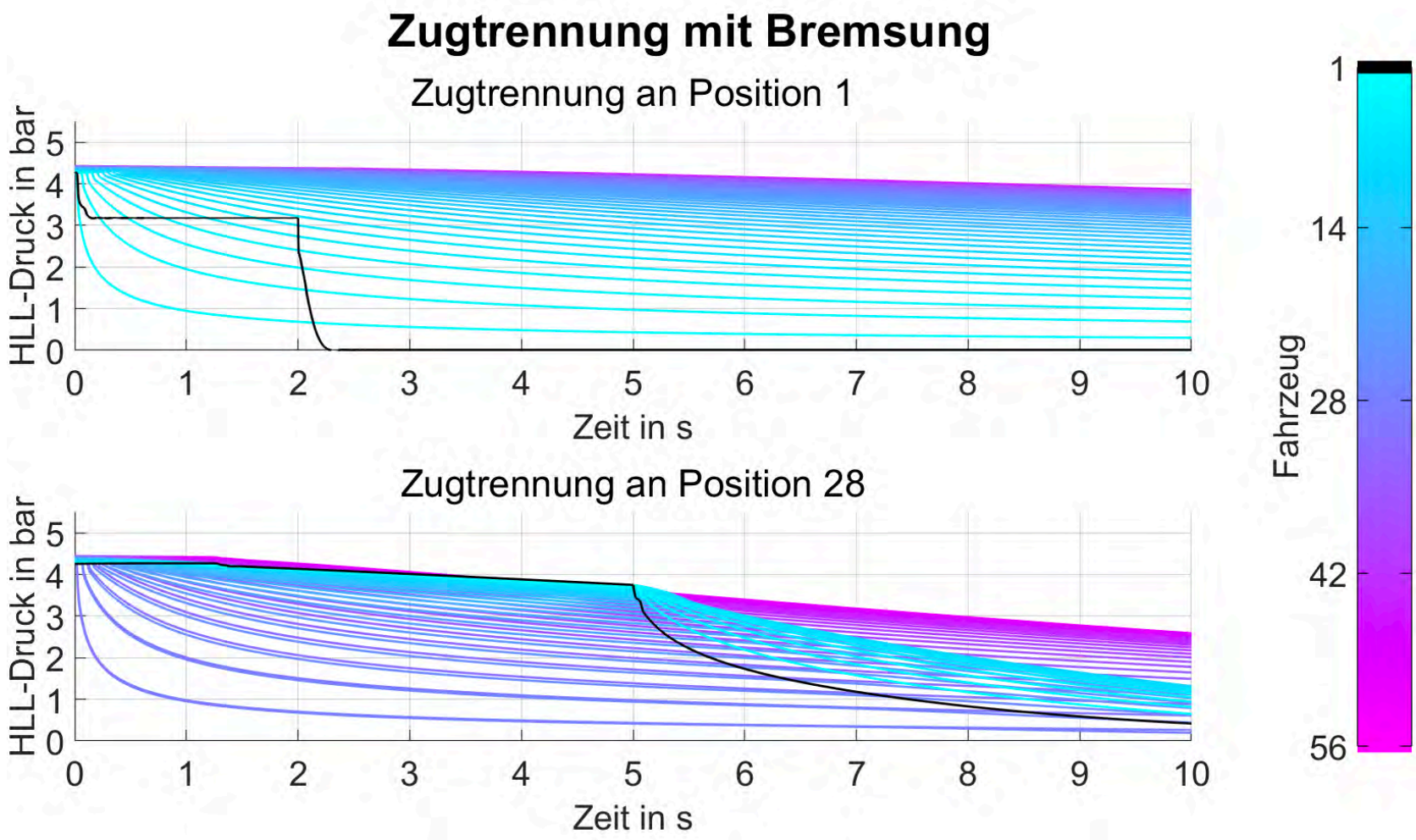






Zugintegrität

Explizite Risikoabschätzung mittels Simulation



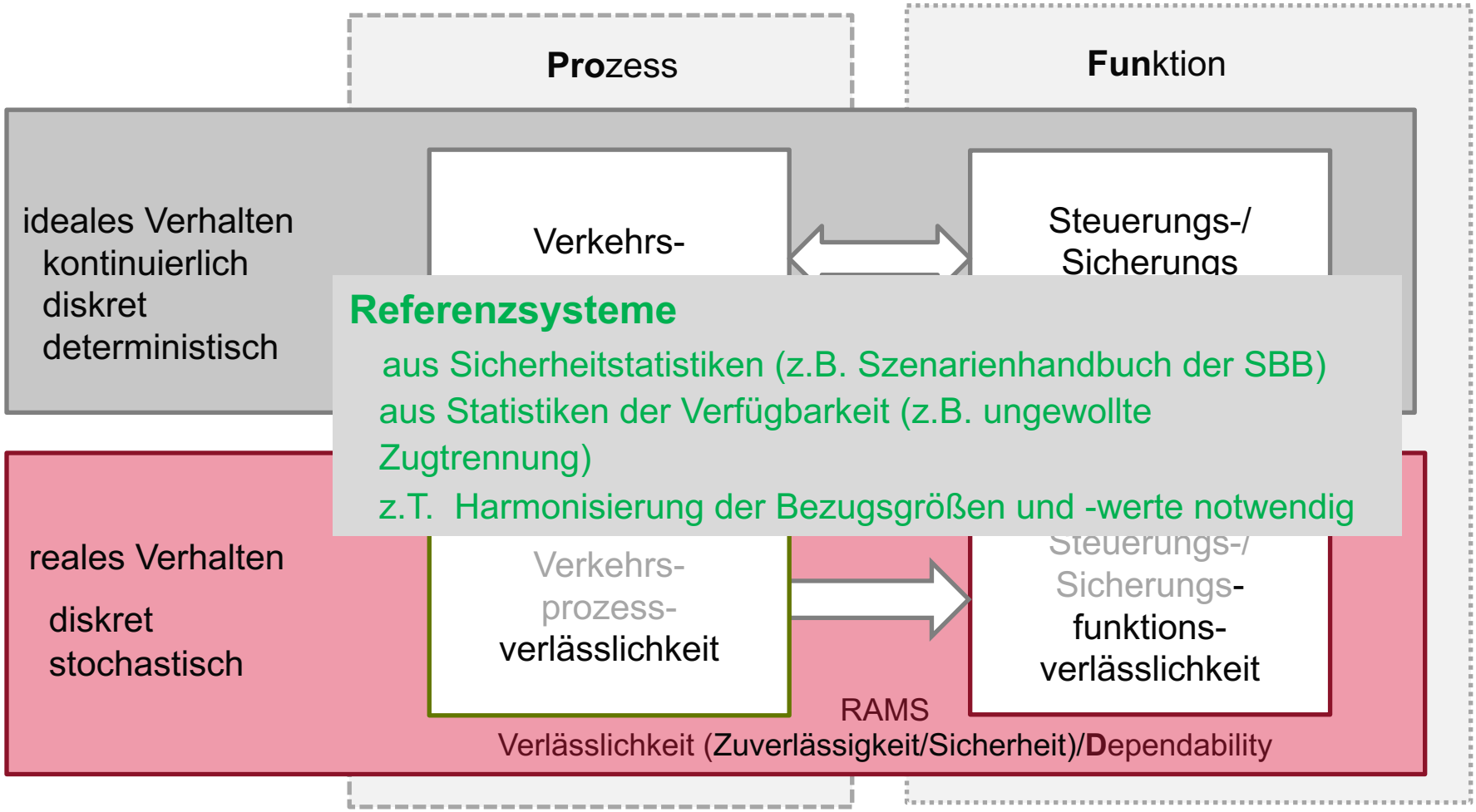
Zugintegrität

Explizite Risikoabschätzung mittels Simulation

- Die Studie untersucht durch Simulationen das Verhalten zweier Zugteile nach einer erfolgten Zugtrennung. Hierfür wird ein geprüftes Simulationsprogramm für Bremsverhalten erweitert und auf Plausibilität geprüft. Es wird eine Parametervariation von vier Parametern durchgeführt, woraus sich 150 Szenarien ergeben.
- In den 150 Szenarien entstehen Lückenlängen von bis zu 846 m. Mit 79 % führt der größte Anteil an Simulationen zu Lückenlängen zwischen 0 m und 25 m. Nur 10 der Szenarien führen zu Lücken mit einer Länge über 200 m. Als einflussreichster Parameter stellt sich die Position der Zugtrennung heraus.
- Es werden sowohl Trennungen hinter dem Triebfahrzeug als auch in der Mitte des Zuges simuliert, jedoch treten alle Lückenlängen deutlich über 100 m nur bei Trennung in der Mitte des Zuges auf. Zudem entstehen alle Lücken mit einer Länge über 200 m bei Simulationen aus Beharrungsfahrten mit 100 km/h oder 120 km/h. Als begünstigend für das Entstehen einer großen Lücke stellt sich eine Konzentration der ausgeschalteten Bremsen im vorderen Zugteil sowie ein vorne voll beladener und hinten leerer Zug heraus.
- Durch die Auswertung der Druckverläufe der Hauptluftleitung kann gezeigt werden, dass die Zeit zwischen Zugtrennung und dem zusätzlichen Einleiten der Schnellbremsung ein maßgeblicher Faktor ist. Bemerkt der Triebfahrzeugführer die Zugtrennung erst sehr spät, können durchaus größere Lücken als die simulierten entstehen. Je weiter die Trennstelle vom Triebfahrzeug entfernt ist, umso später ist es dem Triebfahrzeugführer möglich die Trennung zu erkennen.
- Die Simulationen zeigen, dass durch eine ungünstige Kombination verschiedener Faktoren so große Lückenlängen entstehen können, dass sich der Abstand von Zugspitze zum letzten Wagen gegenüber dem gekuppelten Zustand mehr als verdoppelt.

ProFunD Modellkonzept nach IEC 62551:2012

Herleitung von Anforderungen durch Referenzsysteme



Zugintegrität

Herleitung von Anforderungen – GAMAB Ansatz nach EN 50126-2

EN 50126-2:2017

Anhang A
(informativ)

ALARP, GAME, MEM

A.1 ALARP, GAME und MEM als als Verfahren für die Festlegung von Risikoakzeptanzkriterien

A.3 Globalement au Moins Equivalent (GAME)-Grundsatz

Der Grundsatz lautet:

– Jedes neu geführte öffentliche Transportsystem/-subsystem oder

– jede Änderung eines bestehenden Systems/Subsystems

sollte in der Gesamtsicht genauso sicher wie das bestehende, als Referenzsystem anerkannte System oder sicherer als dieses sein.

Zugintegrität

Herleitung von Anforderungen – Ermittlung der Gefährdungen nach EN 50126-2

EN 50126-2:2017

Anhang B
(informativ)

Anwendung von Ausfall- und Unfallstatistiken für die Ableitung einer THR

THR lassen sich nicht anhand von Unfallstatistiken berechnen, es sei denn, es stehen präzise erfasste Statistiken und Modelle zur Verfügung.

Ausschnitt aus der Liste der Systemgefährdungen (rote Schrift) der Anlage 1 der TeSiP Funktionsliste

Nr. System-gefährdung	Nr. Teil-gefäl	Beschreibung der Systemgefährdungen	Lok	Triebzug	Reisezug-wagen	Güterwagen
9	**Ungewollte Zugtrennung**					
	9a	Ungewollte Zugtrennung durch undefiniertes Traktionsverhalten, zu hohe, ruckartige Zugkräfte	X	X		
	9b	Ungewollte Zugtrennung bzw. Überpufferung durch undefiniertes Bremsverhalten (betriebliches Überbremsen)	X	X	X	X
	9c	Ungewollte Zugtrennung durch sonstige Ursachen (z.B. mechanischer Schaden)	X	X	X	X
	9d	Ungewollte Zugtrennung durch automatisches Entkuppeln		X		

Zugintegrität

Herleitung von Anforderungen – THR Ermittlung nach EN 50126-2

EN 50126-2:2017

Anhang B
(informativ)

Anwendung von Ausfall- und Unfallstatistiken für die Ableitung einer THR

THR lassen sich nicht anhand von Unfallstatistiken berechnen, es sei denn, es stehen präzise erfasste Statistiken und Modelle zur Verfügung.

Die **gefährliche Ausfallrate** pro Betriebsstunde für ein gegebenes Bahnsystem kann geschätzt werden durch:

$$\lambda_{Stunde} \text{ je Einheit} = n_{Jahr}/(\text{Stunden}_{Jahr} \times \text{Anzahl der Einheiten}).$$

Dabei ist n_{Jahr} die jährliche Anzahl von gefährlichen Ausfällen.

analog

Die **Ereignisrate** pro Betriebsstunde für ein gegebenes Bahnsystem kann geschätzt werden durch:

$$\lambda_{Stunde} \text{ je Einheit} = n_{Jahr}/(\text{Stunden}_{Jahr} \times \text{Anzahl der Einheiten}).$$

Dabei ist n_{Jahr} die jährliche Anzahl von Ereignissen

Statistik von Zugtrennungen im Netz der SBB

Ereignistabelle

Zugtrennungen ab 01.01.2016 bis 15.03.2018 / Auswertung aus Ereignistyp Level 4 "Zugtrennung" / Qu

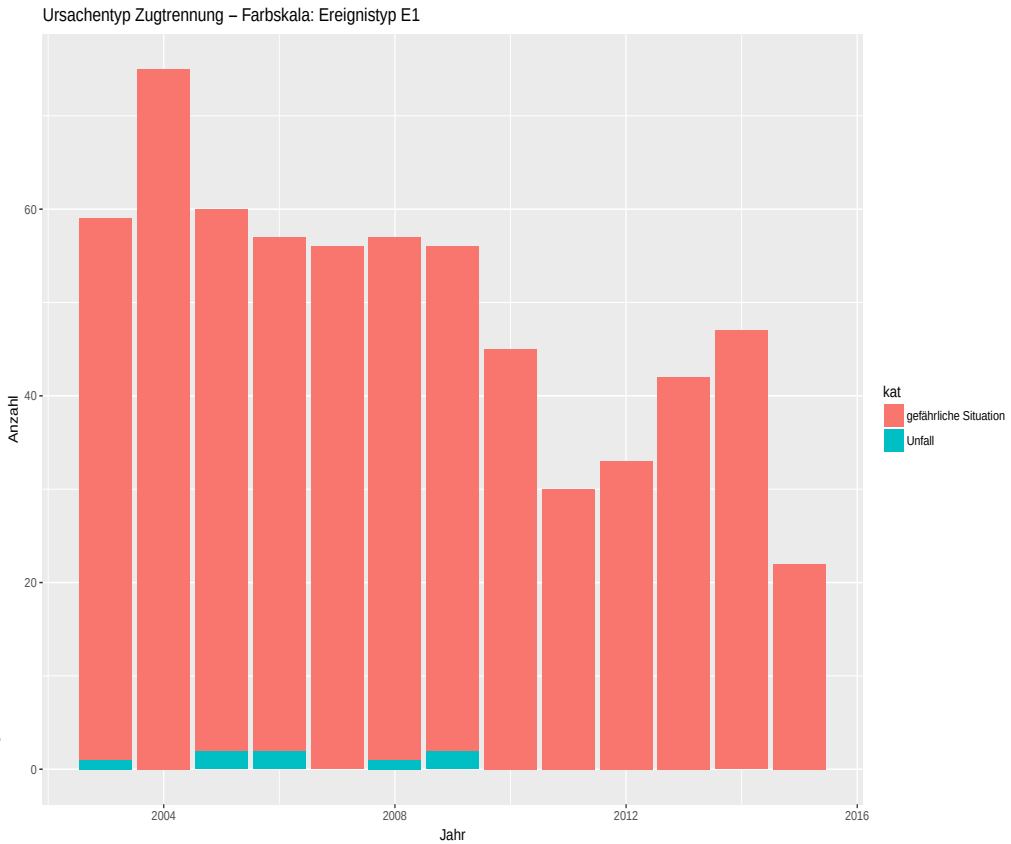
Ereignis Nummer	Datum Unregelm	Ereign	Zuggattung	Ursachentyp Lev	Ursachentyp Lev	Ursachentyp Level 4	Verurs. OE	Ereignis Beschreibung
ECUZYQ	10.02.2016	2016	Internationaler Güterzug	Störung Rollmater	Wagen	Zug- und Stossvorrichtung	G-PN-LPC-RNS-I	Treno 44681 annuncia una perdita d'
ECVYN8	22.04.2016	2016	Internationaler Kombizug	Zugtrennung	Anfahren / Beschle	Nicht zugeordnet	G-CINT	Zugstrennung Zug 41556 in Löchligu
ECX8QM	09.08.2016	2016	Internationaler Kombizug	Störung Rollmater	Triebfahrzeug / Tri	Zug- und Stossvorrichtung	G-CINT	Zugstrennung zwischen P-Lok und I
ECXJEK	01.09.2016	2016	Internationaler Güterzug	Fehlhandlung Fahr	Fahren	andere Ursache Fahren	#	Alla ripresa della corsa, una lok ha p
ECYAM6	07.11.2016	2016	Internationaler Schnellzug	Störung Rollmater	Wagen	Zug- und Stossvorrichtung	G-PN-LPC-ROT-I	Zwischen Einfahrvorsignal und Einfa
ECYCZR	17.11.2016	2016	Internationaler Schnellzug	Fehlhandlung Fahr	Fahren	andere Ursache Fahren	G-IN-CIN-CI-DO	Um 10.00 1.Verbindungsaufnahme r
ECYJAH	06.12.2016	2016	Cargo Express-Zug	Störung Rollmater	Wagen	Zug- und Stossvorrichtung	G-AM	Durante lo spostamento a cura del p
ECYPZP	16.12.2016	2016	InterRegio-Zug	Fehlhandlung Vorb	Kuppeln	Trennen / Kuppeln von Wag	P-OP-ZBS-ZUE	Zughaken zwischen Lok und erstem
ECYZUC	16.01.2017	2017	InterCity-Zug	Fehlhandlung Vorb	Reihung	Reihungsvorgabe nicht eing	G-PN-LPC-RWT-	Vor Einfahrt in Bahnhof Neuenburg h
ECZ2WA	18.01.2017	2017	Internationaler Kombizug	Störung Rollmater	Zugstrennung	Nicht zugeordnet	I-B-RSD	Il treno 41051 (con loc di spinta) si fe
ECZSCB	23.03.2017	2017	Internationaler Güterzug	Störung Rollmater	Zugstrennung	Nicht zugeordnet	#	Gemäss Lokführer hat in der Zugsm
ED2MDV	01.06.2017	2017	Internationaler Kombizug	Störung Rollmater	Zugstrennung	Nicht zugeordnet	#	Zugstrennung Zug 43559. Nachbarg
ED2ZFG	05.07.2017	2017	Internationaler Güterzug	Störung Rollmater	Zugstrennung	Nicht zugeordnet	G-PN-LPC-RWT-	Train 61097 de LT à Br, le singnal d'
ED3586	18.07.2017	2017	Internationaler Güterzug	Störung Rollmater	Zugstrennung	Nicht zugeordnet	G-PN-LPC-RWT-	En arrivant sur la voie 1 à Renens, j
ED42KK	10.10.2017	2017	Internationaler Güterzug	Zugtrennung	Anfahren / Beschle	Nicht zugeordnet	G-IN-CIN	Zug mit 3 Re 4/4. Während dem Auf
ED45P6	20.10.2017	2017	Leermaterialzug-(Reise)Extrazüge	Störung Rollmater	Triebfahrzeug / Tri	andere Ursachen Triebfahr:	#	Lf 28324 meldet, dass ihm auf seine
ED46HD	13.10.2017	2017	InterRegio-Zug	Störung Rollmater	Wagen	Zug- und Stossvorrichtung	P-OP-AM-FT-SU	Lors de mon freinage, me permettar
ED48AB	27.10.2017	2017	Internationaler Güterzug	Fehlhandlung Fahr	Fahren	andere Ursache Fahren	G-PN-LPC-RNS-I	Zugtrennung, nach Stillstandsüberw
ED4HHE	24.11.2017	2017	Internationaler Güterzug	Störung Rollmater	Wagen	Zug- und Stossvorrichtung	G-PN-LPC	Sul semplice binario nella galleria d
ED4QBS	13.12.2017	2017	InterRegio-Zug	Kommunikation	Andere Ursachen I	Nicht zugeordnet	G-PN	Zugtrennung zwischen Giubiasco ur
ED53WV	23.01.2018	2018	Internationaler Güterzug	Störung Rollmater	Wagen	Zug- und Stossvorrichtung	G-IN-CIN	Zur Zugstrennung kam es im Stillsta

Statistik von Zugtrennungen im Netz der SBB

Zeitreihe

Zugtrennungen ab 01.01.2016 bis 15.03.2018 / Auswertung aus Ereignistyp Level 4 "Zugtrennung" / Qu

Ereignis Nummer	Datum Unregelm	Ereign	Zuggattung	Ursachentyp Lev	Ursachentyp Lev	Ursachentyp Level 4	Verurs. OE	Ereignis Beschreibung
ECUZYQ	10.02.2016	2016	Internationaler Güterzug	Störung Rollmater	Wagen	Zug- und Stossvorrichtung	G-PN-LPC-RNS-I	Treno 44681 annuncia una perdita d'
ECVYN8						zugeordnet	G-CINT	Zugstrennung Zug 41556 in Löchligu
ECX8QM						nd Stossvorrichtung	G-CINT	Zugstrennung zwischen P-Lok und I
ECXJEK						e Ursache Fahren	#	Alla ripresa della corsa, una lok ha p
ECYAM6						nd Stossvorrichtung	G-PN-LPC-ROT-I	Zwischen Einfahrvorsignal und Einfa
ECYCZR						e Ursache Fahren	G-IN-CIN-CI-DO	Um 10.00 1.Verbindungsaufnahme r
ECYJAH						nd Stossvorrichtung	G-AM	Durante lo spostamento a cura del p
ECYPZP						en / Kuppeln von Wag	P-OP-ZBS-ZUE	Zughaken zwischen Lok und erstem
ECYZUC						ngsvorgabe nicht eing	G-PN-LPC-RWT-	Vor Einfahrt in Bahnhof Neuenburg h
ECZ2WA						zugeordnet	I-B-RSD	Il treno 41051 (con loc di spinta) si fe
ECZSCB						zugeordnet	#	Gemäss Lokführer hat in der Zugsm
ED2MDV						zugeordnet	#	Zugstrennung Zug 43559. Nachbarg
ED2ZFG						zugeordnet	G-PN-LPC-RWT-	Train 61097 de LT à Br, le singnal d'
ED3586						zugeordnet	G-PN-LPC-RWT-	En arrivant sur la voie 1 à Renens, j
ED42KK						zugeordnet	G-IN-CIN	Zug mit 3 Re 4/4. Während dem Auf
ED45P6						e Ursachen Triebfahr:	#	Lf 28324 meldet, dass ihm auf seine
ED46HD						nd Stossvorrichtung	P-OP-AM-FT-SU	Lors de mon freinage, me permettar
ED48AB						e Ursac		tillstandsüberw
ED4HHE						nd Sto		nella galleria d
ED4QBS						zugeor		en Giubiasco ur
ED53WV						nd Sto		am es im Stillsta



	Ursachen-typ E3	MTTF/h	n
1	Anfahren /Beschleunigen	19.296	234
2	Bremsen	56.454	78
3	übriges	14.1012	327

Zugintegrität

Berechnung der Ereignisrate ungewollter Zugtrennungen bei SBB und ÖBB

Die **Ereignisrate** pro Betriebsstunde für ein gegebenes Bahnsystem kann geschätzt werden durch:

λ_{Stunde} je Einheit = n_{Jahr}/($Stunden_{Jahr}$ × Anzahl der Einheiten).

für einen verfügbaren Zeitraum von etwa 12 Jahren sind für die SBB Cargo

Ereignise $n_{ESBBC} = 481 + 17 = 498$

Anzahl der Einheiten $N_{SBBC} = 340$

Betriebsdauer $T_{BC} = (10 + 2{,}08) \times 365 \times 24\ h = 12{,}08 \times 8760\ h = 105.820{,}8\ h$

Ereignisrate ungewollter Zugtrennungen für Güterzüge der SBB Cargo bzw. SBB Personenverkehr

$$\lambda_{ESBBC} = \frac{n}{N_{SBBC}\, T_b} = \frac{498}{340\ x\ 105820{,}8\ h} = \mathbf{1{,}38 \cdot 10^{-5}\ h^{-1}} \quad \gg \quad \lambda_{ESBBP} = \frac{n}{N_{ÖBBP}\, T_b} = \frac{40}{1008\ x\ 79.365{,}6\ h} = \mathbf{4{,}99 \cdot 10^{-7}\ h^{-1}}$$

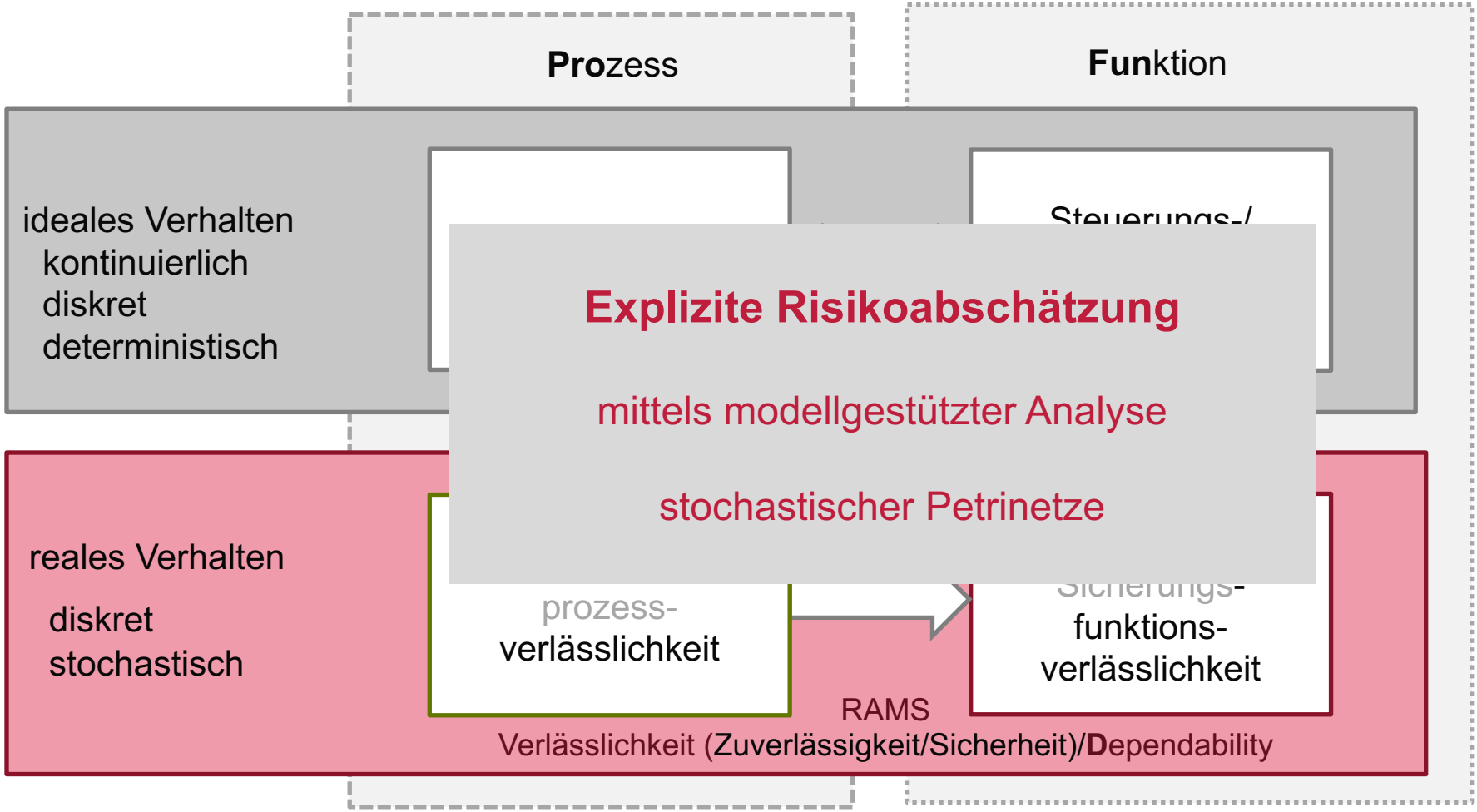
$n_{EÖBB} = 52{,}75$, $N_{ÖBB} = 388$, $T_{aC} = 365 \cdot 24\ h$

Ereignisrate ungewollter Zugtrennungen bei Zügen der ÖBB für den mittleren Zeitraum eines Jahres

$$\lambda_{EÖBB} = \frac{n_c}{N_{ÖBBC}\, T_{aC}} = \frac{52{,}75}{388 \cdot 365 \cdot 24} = \mathbf{1{,}55 \cdot 10^{-5}\ h^{-1}}$$

ProFunD Modellkonzept nach IEC 62551:2012

Herleitung von Anforderungen durch explizite Risikoabschätzung

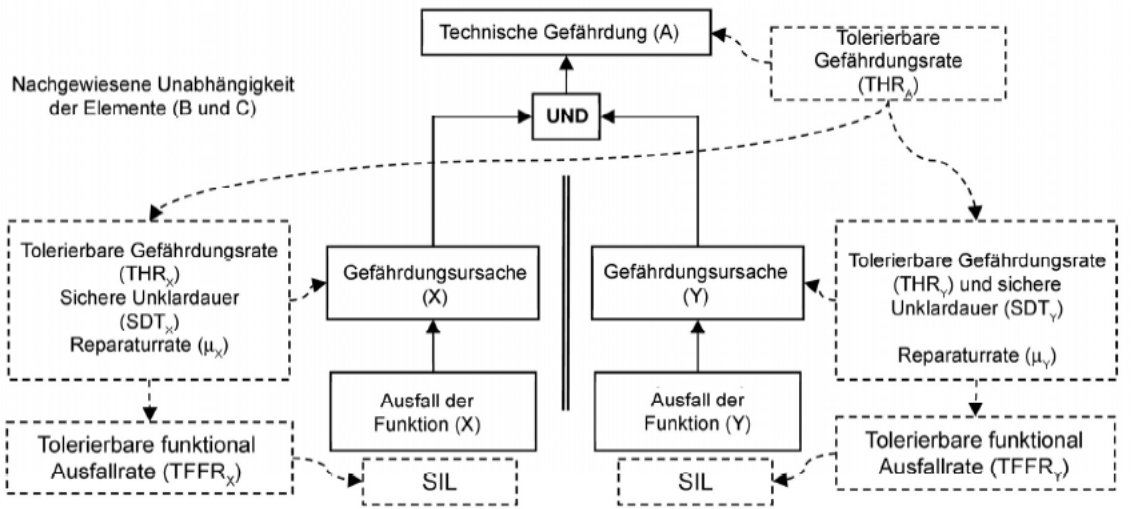


Zugintegrität

Berechnung der Gefährdungsrate ungewollter Zugtrennungen nach EN 50126-2

Gefährlicher Ausfall bei Zugtrennung
Gefährdungsrate
Postulat SIL = $10^{-9}\ h^{-1}$

$$THR_A \cong THR_X \times THR_Y \times \frac{\mu_X + \mu_Y}{\mu_X \times \mu_Y}$$

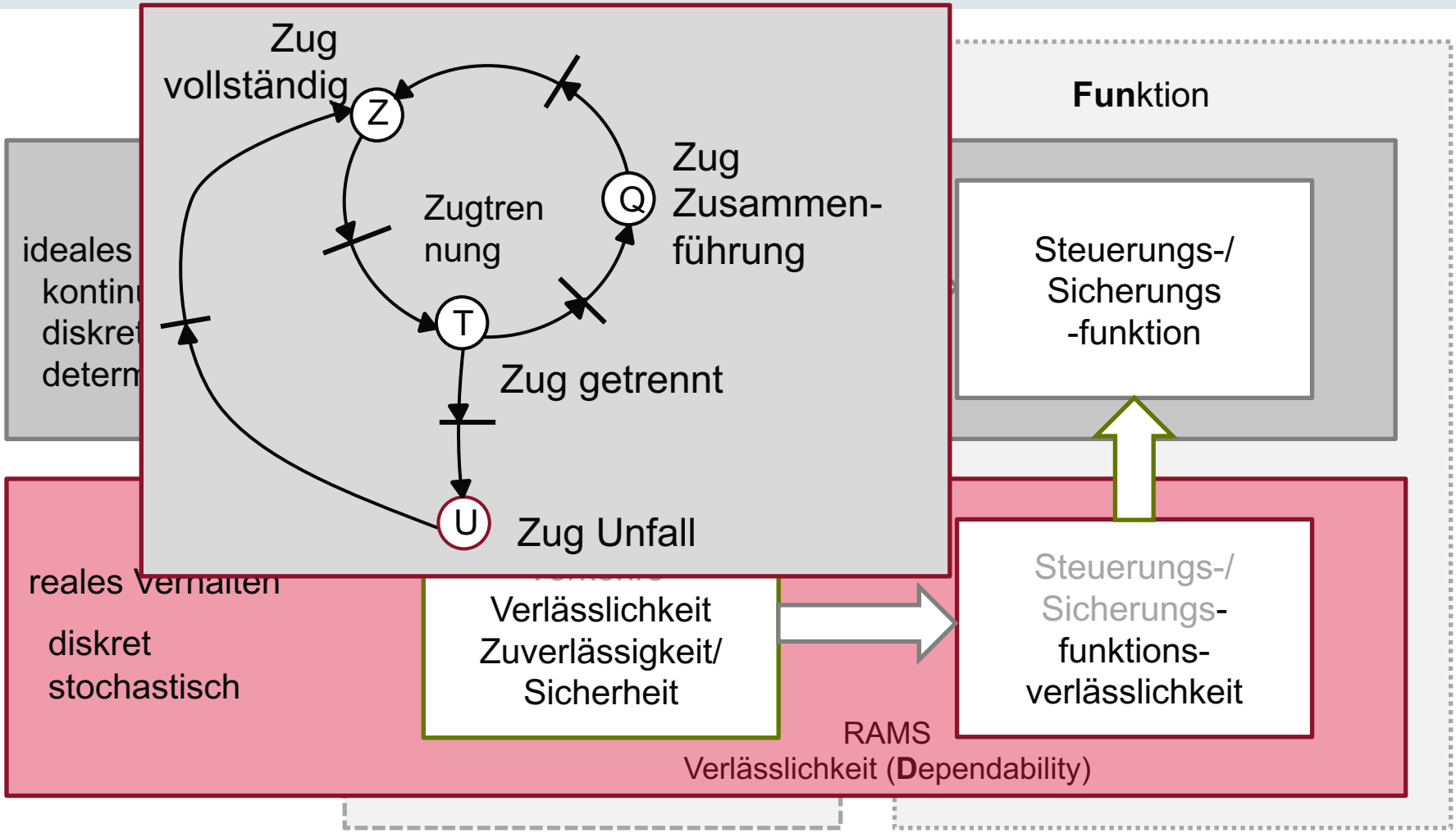


Ungewollte Zugtrennung
Ereignisrate vorhanden

Sicherung bei Ungewollter Zugtrennung
SIL gesucht

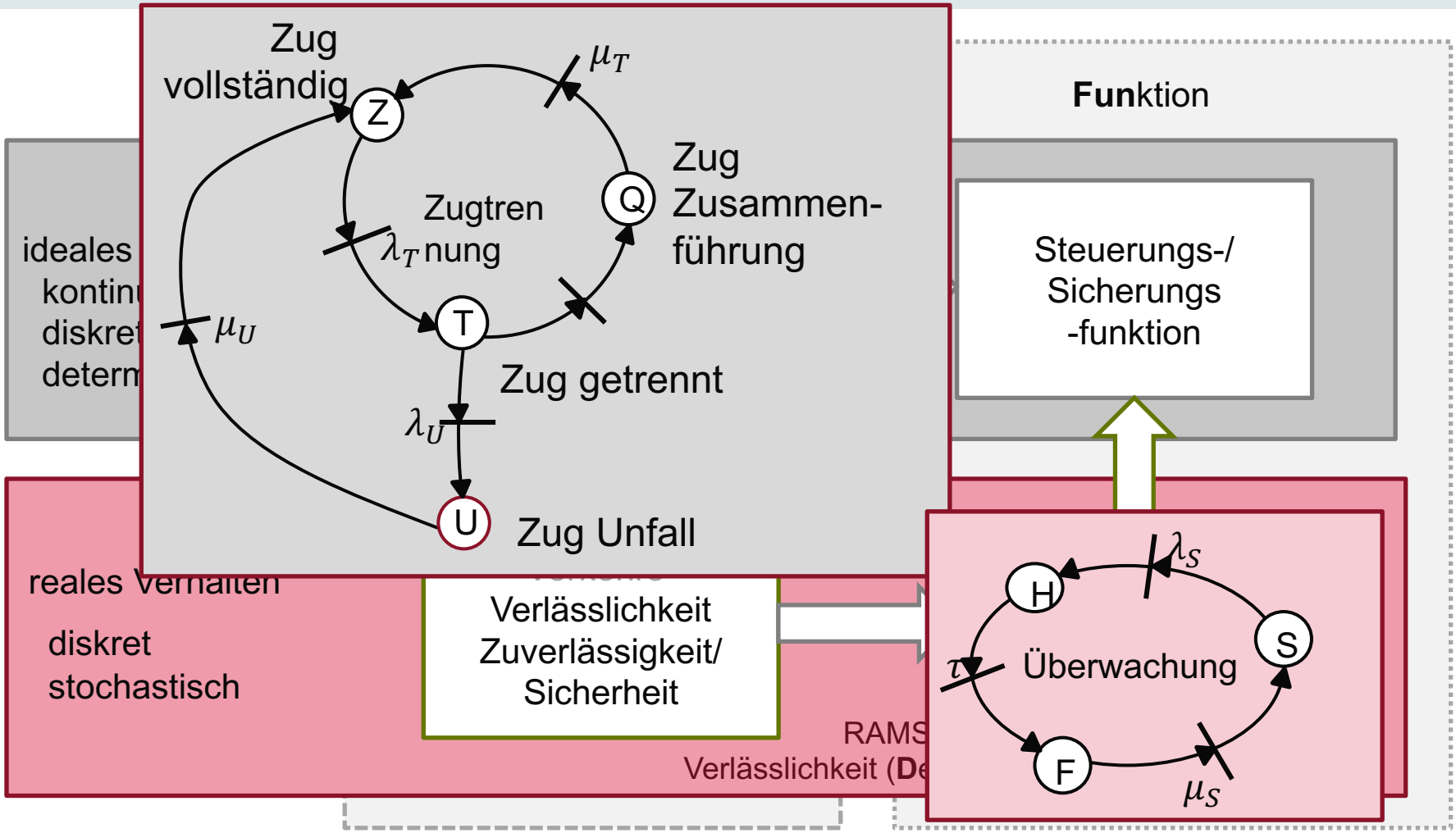
ProFunD Modellkonzept nach IEC 62551:2012

Risikoabschätzung: Prozessmodell als Petrinetz (nach EN 50128:2012 A17, D55)



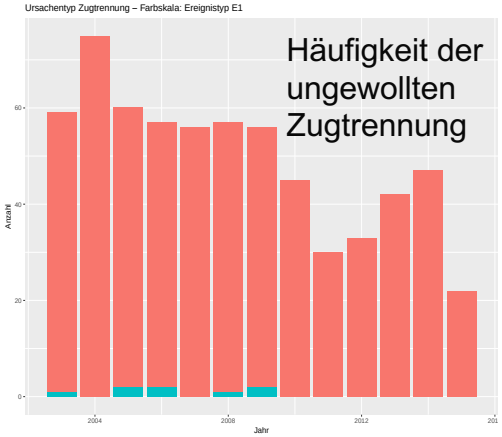
ProFunD Modellkonzept nach IEC 62551:2012

Risikoabschätzung: Prozessmodell und Überwachung



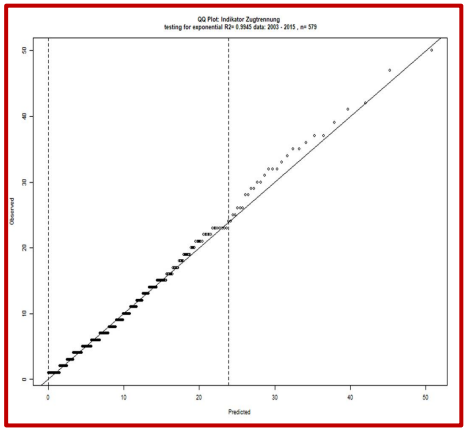
Modellgestützte Analyse der Zugtrennung

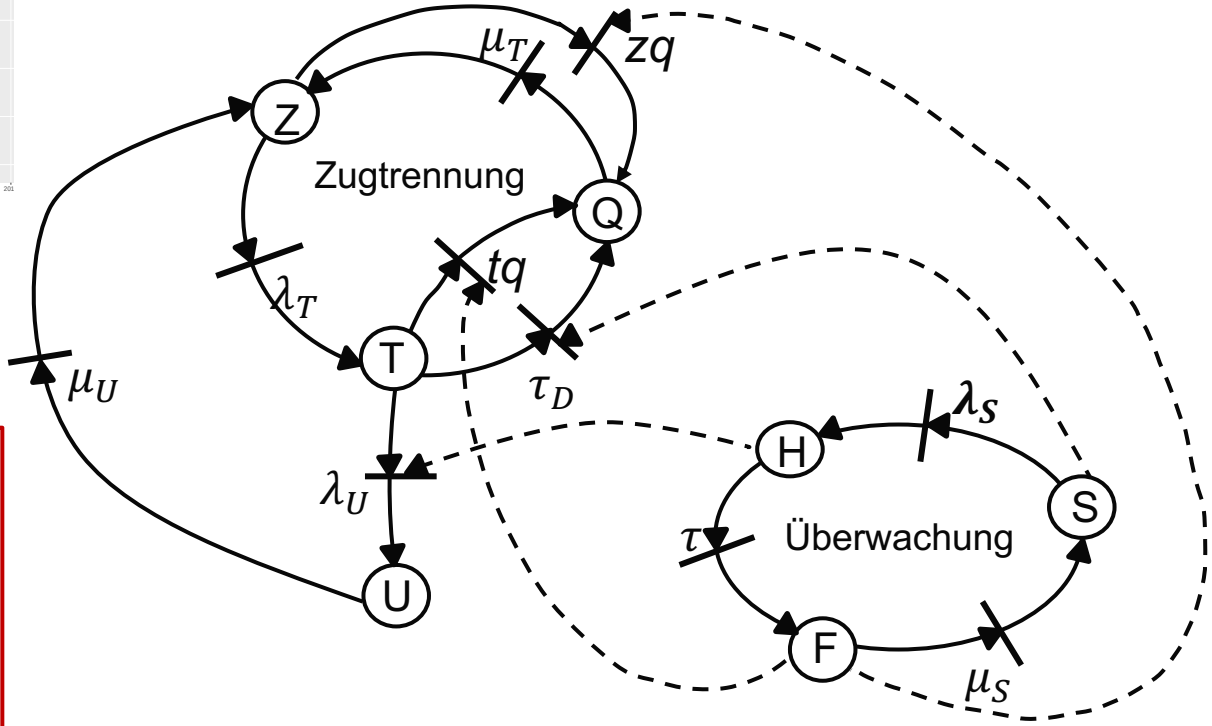
Verhalten einer Zugtrennung und sicherer Überwachung



$\lambda_T = 1{,}38 \cdot 10^{-5}$ bis $4{,}99 \cdot 10^{-7}\ h^{-1}$

Nachweis der negativ-Exponentialverteilung der zeitlichen Abstände $1/\lambda_T$ der Zugtrennung durch QQ-Plot



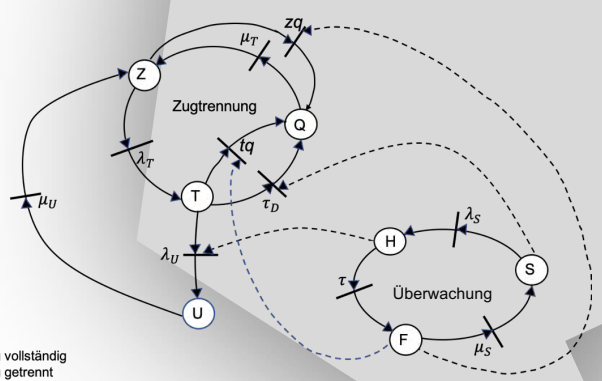


$\lambda_U = 1 \cdot 10^{-9} h^{-1} \Longrightarrow SIL\ 4$

Modellgestützte Analyse der Zugtrennung

Verhalten einer Zugtrennung und sicherer Überwachung

zeitbewertetes Petrinetzmodell



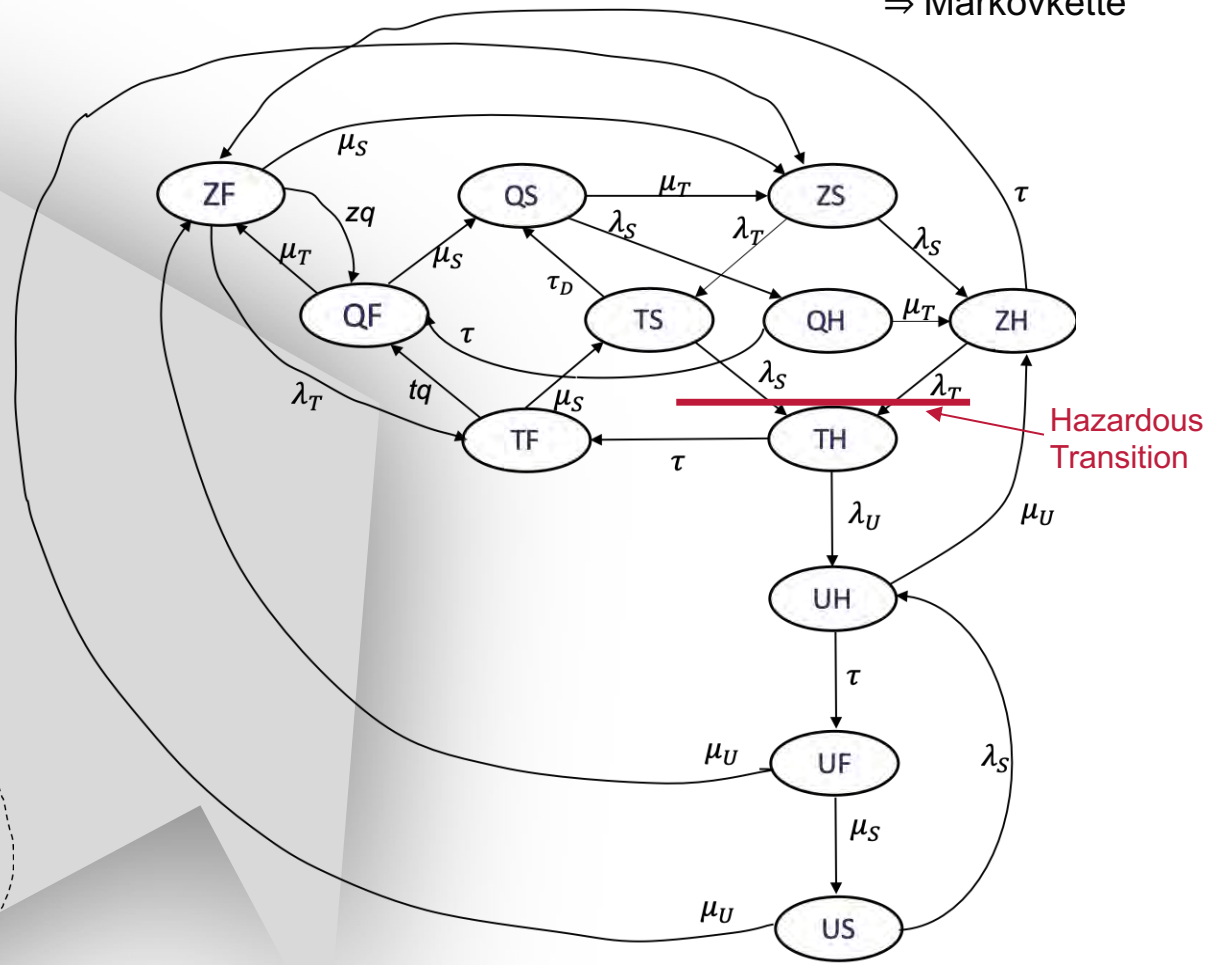
Z Zug vollständig
T Zug getrennt
Q Zug Zusammenführung
S Sensor und Überwachung sicher
H Überwachter Sensor im Fehlzustand
F Überwachter Sensor als fehlerhaft detektiert

Quelle / Bedeutung	Parameter	H. Robl (ehem. Technischer Betriebsinspektor, DB München)	ÖBB S. Rameder H. Dreossi	SBB A. Brand[1] J. Suter[2] ehem. Bahnhofsvorsteher)	Annahme Mittelwert Zielwert
Anzahl ungewollter Zugtrennungen	n	-	53/a	[1] 40/a	-
mittl. Dauer der Behebung der Zugtrennung	$1/\mu_T$	45 – 60 min	30 min – 4 h	[2] 60 min – 6 h	1/2 h^{-1}
Rate der Behebung der Zugtrennung	μ_T	1 h^{-1}- 1,33 h^{-1}	0,25h^{-1} - 2 h^{-1}	[2] 0,17h^{-1} - 1 h^{-1}	2h
Rate der Zugtrennung (Güterzüge, Personenzüge)	λ_T (SBB)	-	-	[1] 1,38 · 10^{-5} h^{-1} 4,99 · 10^{-7} h^{-1}	-
Ereignisrate der Unfälle infolge Zugtrennung	$1/\lambda_U$	0	0	[1] 0	SIL 4, 10^{-9} h^{-1}
Ereignisrate der Wiederherstellung der Überwachung	$1/\mu_S$		-	-	60 min =1h
Ereignisrate des Ausfalls der Überwachung	$1/\lambda_S$	-	-	-	? gesuchter Zielwert
Dauer der Offenbarung der fehlerhaften Überwachung	τ	-	-	-	1 min = 1/60 h = 0,017 h
Ereignisrate Offenbarung der fehlerhaften Überwachung	$1/\tau$	-	-	-	60 h^{-1}
Dauer der Detektionszeit einer Zugtrennung	τ_D	-	-	-	10 s

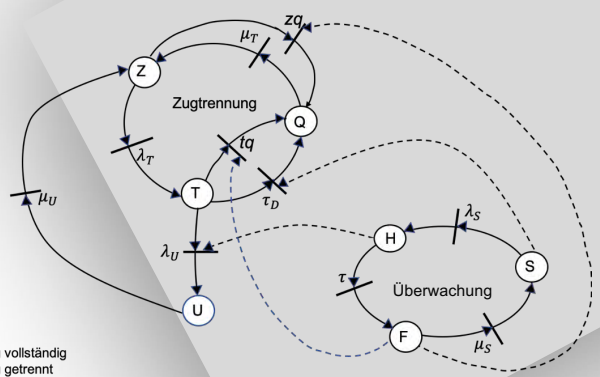
Modellgestützte Analyse der Zugtrennung

Verhalten einer Zugtrennung und sicherer Überwachung

Vollständiger Erreichbarkeitsgraph
⇒ Markovkette



zeitbewertetes Petrinetzmodell

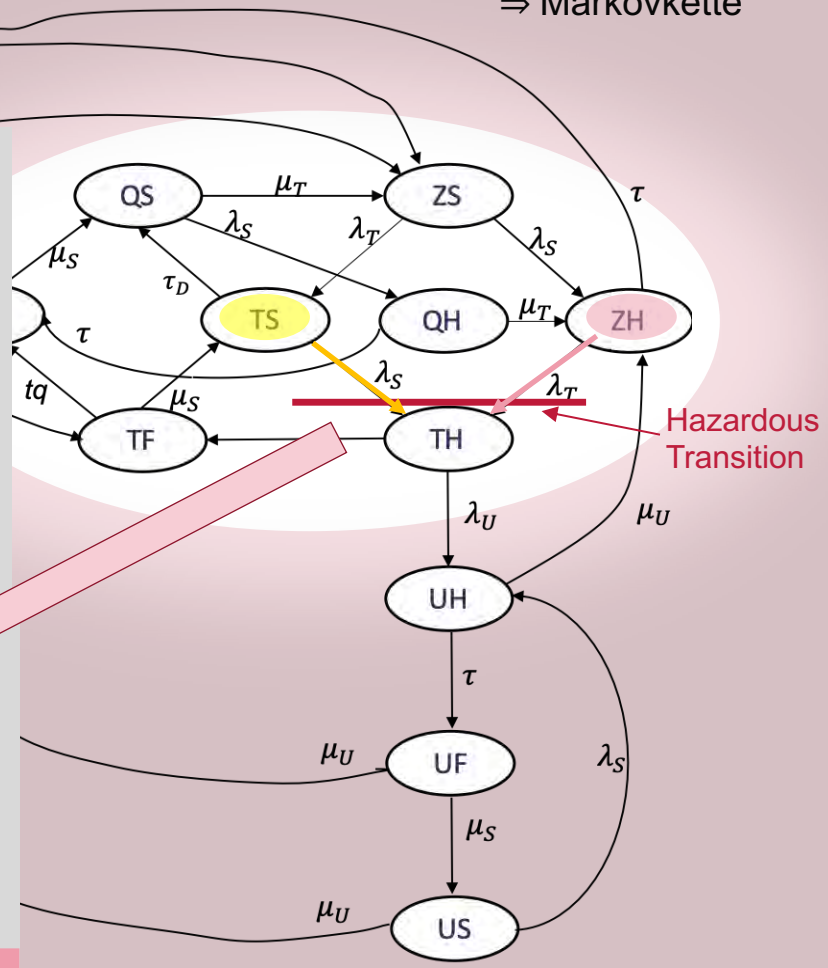


Z Zug vollständig
T Zug getrennt
Q Zug Zusammenführung
S Sensor und Überwachung sicher
H Überwachter Sensor im Fehlzustand
F Überwachter Sensor als fehlerhaft detektiert

Modellgestützte Analyse der Zugtrennung

Verhalten einer Zugtrennung und sicherer Überwachung

Vollständiger Erreichbarkeitsgraph
⇒ Markovkette



Mit stationärer Lösung der Chapman-Kolmogoroff-Gleichung aus der Markovkette und Näherung folgt

$$\lambda_H \approx \lambda_S P_{TS} + \lambda_T P_{ZH}$$

nach Zwischenrechnung und aufgelöst nach

$$\lambda_S \approx \frac{\lambda_H}{\lambda_T \left(\frac{1}{\mu_T} + \tau_D + \frac{1}{\mu_s} + \tau \right)}$$

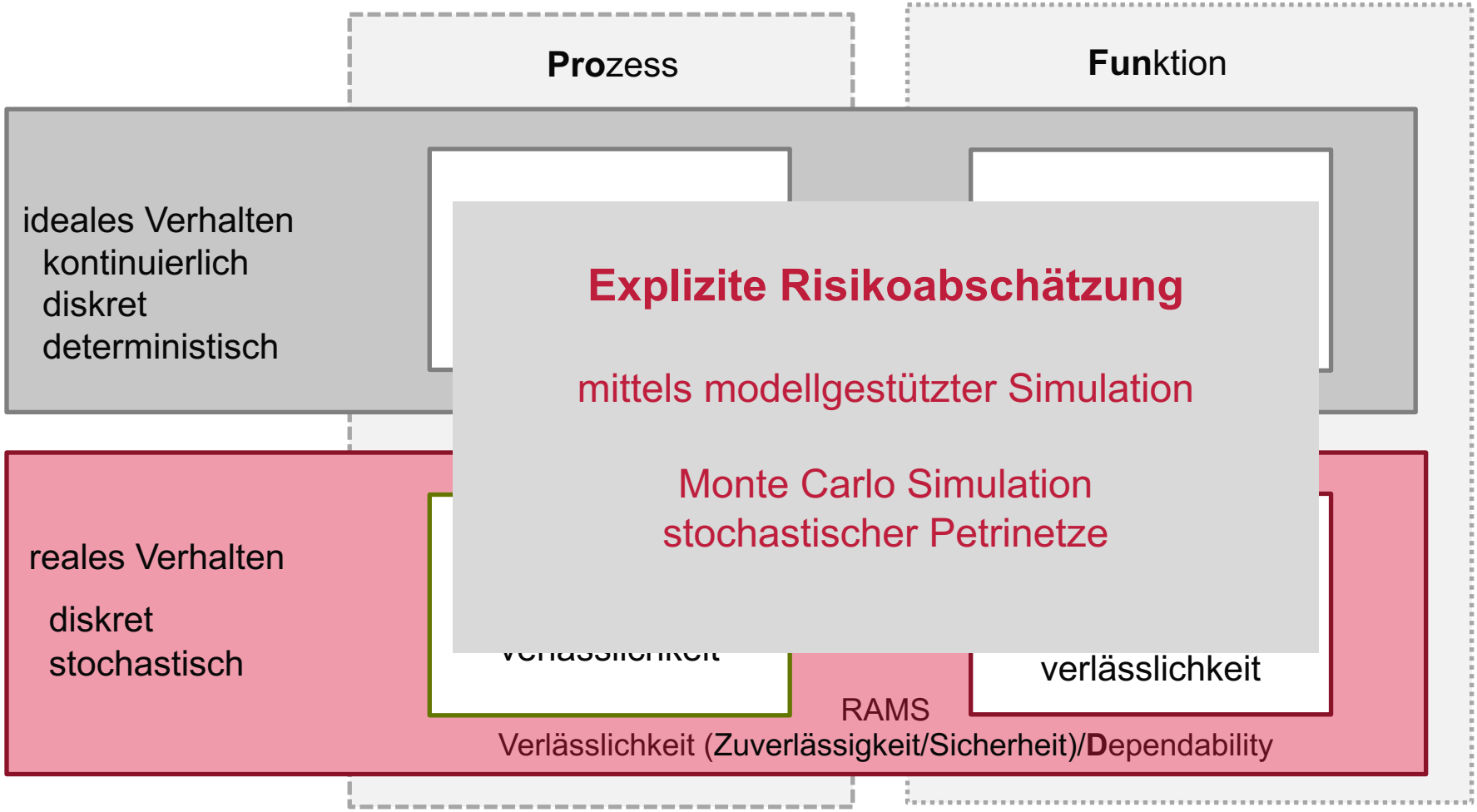
Werte eingesetzt

$$\lambda_S \approx 2{,}15 \cdot 10^{-5}\, h^{-1} / \mu_\Sigma$$

SIL Level	Intervall der Gefährdungsraten
4	1_{10}-8 - 1_{10}-9
3	1_{10}-7 - 1_{10}-8
2	1_{10}-6 - 1_{10}-7
1	1_{10}-5 - 1_{10}-6

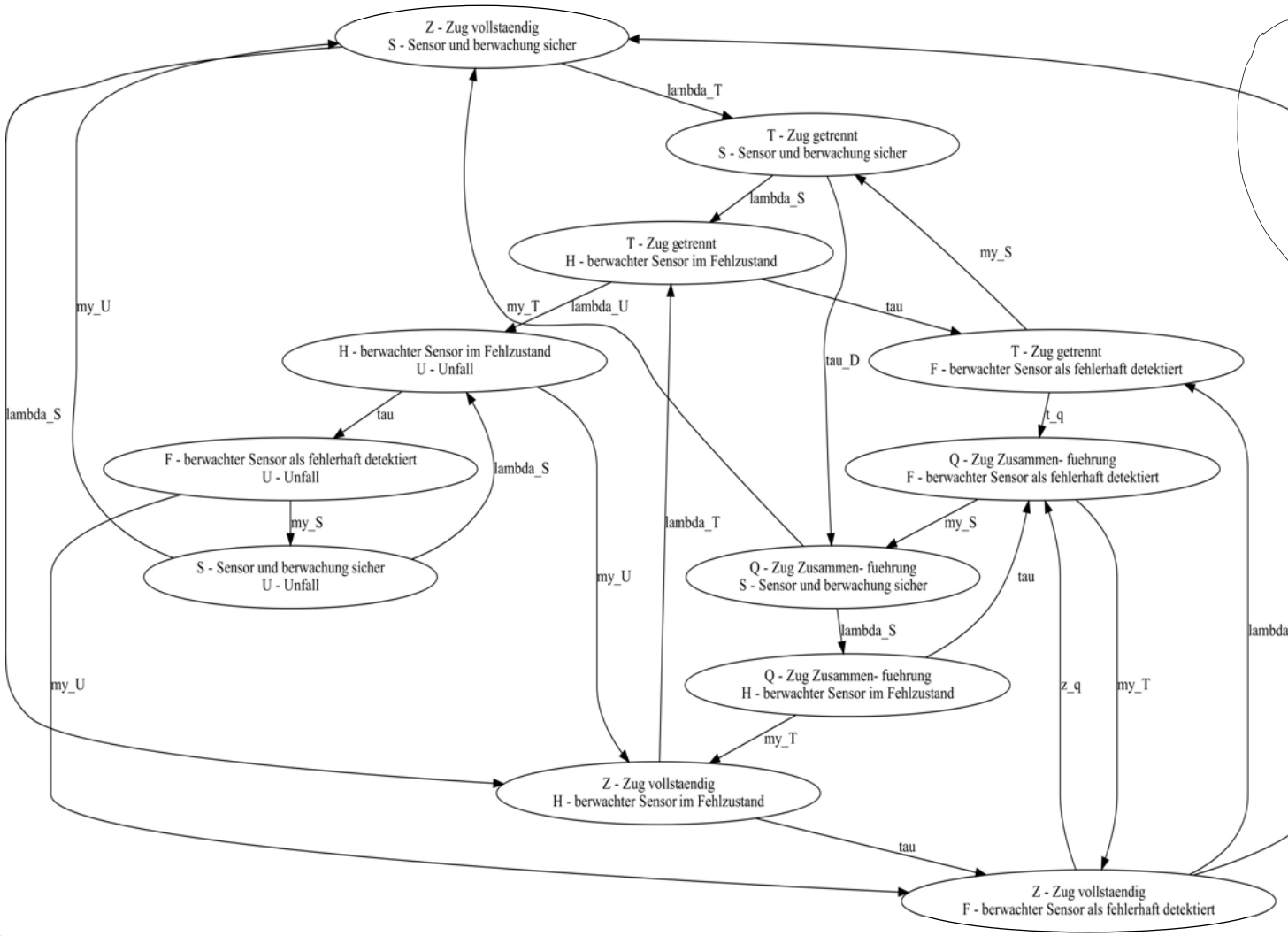
ProFunD Modellkonzept nach IEC 62551:2012

Herleitung von Anforderungen durch explizite Risikoabschätzung



Modellgestützte Analyse der Zugtrennung

Toolgestützte Verifikation: Vollständiger Erreichbarkeitsgraph mit π-Tool



Modellgestützte Analyse der Zugtrennung

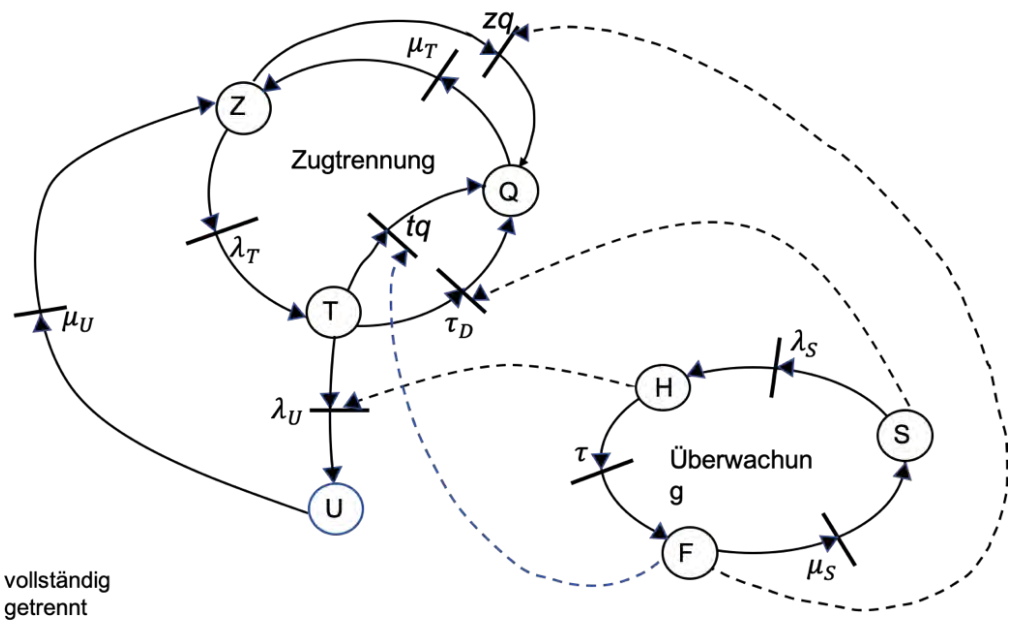
Ergebnisse der Monte Carlo Simulation des Petrinetzes mit π-Tool

Transition firing rates

Transition	Markovian rates	Sim rates
PN.tau_D	-1	1.37329e-05
PN.t_q	-1	< 4.47772e-09
PN.my_T	-1	0.00151432
PN.z_q	-1	0.00150059
PN.lambda_T	-1	1.37218e-05
PN.my_S	-1	0.00100086
PN.lambda_S	-1	0.00100086
PN.tau	-1	0.00100086
PN.lambda_U	-1	< 4.47772e-09
PN.my_U	-1	< 4.47772e-09

Place occupancy probability

Place	Markovian rates	Sim rates
PN.Z - Zug vollständig	-1	0.996976
PN.T - Zug getrennt	-1	3.80285e-08
PN.Q - Zug Zusammen-	-1	0.00302385
PN.H - Überwachter Sensor im Fehlzustand	-1	1.70145e-05
PN.S - Sensor und Überwachung sicher	-1	0.998983
PN.F - Überwachter Sensorals fehlerhaft det...	-1	0.00100022
PN.U - Unfall	-1	< 4.47772e-09

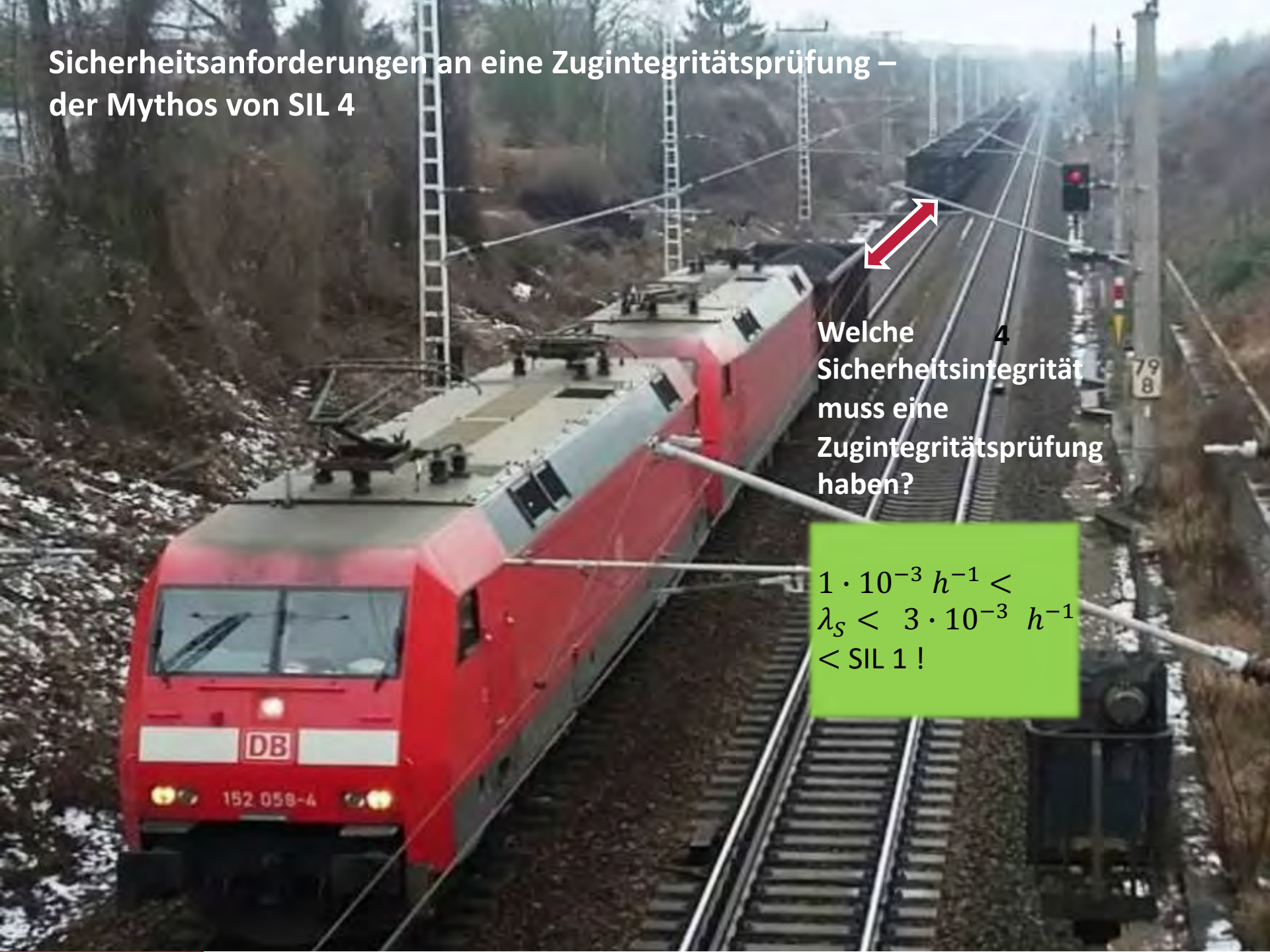


Z Zug vollständig
T Zug getrennt
Q Zug Zusammenführung
S Sensor und Überwachung sicher
H Überwachter Sensor im Fehlzustand
F Überwachter Sensor als fehlerhaft detektiert

SIL Level	Intervall der Gefährdungsraten
4	1_{10}-8 - 1_{10}-9
3	1_{10}-7 - 1_{10}-8
2	1_{10}-6 - 1_{10}-7
1	1_{10}-5 - 1_{10}-6

$$1 \cdot 10^{-3}\ h^{-1} < \lambda_S < \ 3 \cdot 10^{-3}\ \ h^{-1} < \text{SIL 1 !}$$

Sicherheitsanforderungen an eine Zugintegritätsprüfung – der Mythos von SIL 4



Welche 4 Sicherheitsintegrität muss eine Zugintegritätsprüfung haben?

$1 \cdot 10^{-3}\ h^{-1} < \lambda_S < 3 \cdot 10^{-3}\ h^{-1}$
< SIL 1 !

Zugintegrität

Gegenwärtige Maßnahmen zur Sicherung bei ungewollten Zugtrennungen

Für das sehr geringe Risiko ungewollter Zugtrennungen sind mehrere Sicherungsmaßnahmen verantwortlich, welche die gefährlichen Folgen nahezu ausschliessen.

Fahrzeugseitige Sicherung

1. Fail-safe automatische Bremsung durch Trennung der Hauptluftleitung
2. Wahrnehmung der Zugtrennung im Führerstand
3. Maßnahmen des Fahrzeugführers

4. Bestehende Gleisfreimeldeeinrichtungen
5. Fahrwegsicherung
6. Anzeige und Maßnahmen der Fahrdienstleitung.

Streckenseitige Sicherung

Diese Maßnahmen werden in der **sicheren Überwachung** zusammengefasst

Zugintegrität

Neue Maßnahmen zur Sicherung bei ungewollten Zugtrennungen

Für das sehr geringe Risiko ungewollter Zugtrennungen sind mehrere Sicherungsmaßnahmen verantwortlich, welche die gefährlichen Folgen nahezu ausschliessen. Neu ist die Detektion der Zugtrennung z.B. durch Druckabfallmessung

Fahrzeugseitige Sicherung

1. Fail-safe automatische Bremsung durch Trennung der Hauptluftleitung
2. Wahrnehmung der Zugtrennung im Führerstand
3. Maßnahmen des Fahrzeugführers
4. ETCS-Positions-, Zuglängen- und -trennungsmeldung an Fahrwegsicherung

5. Fahrwegsicherung
6. Anzeige und Maßnahmen der Fahrdienstleitung.

Streckenseitige Sicherung

Zugintegrität

Potenziale neuer Zugintegritätsfeststellung

Potenziale der Ausrüstung
Potenziale der Störungsvermeidung
Potenziale der Instandhaltung

<table>
<tr><th>Funktions-realisierung</th><th>Class B</th><th>ETCS L2</th><th>ETCS L2+ (Hybrid)</th><th>ETCS L3</th></tr>
<tr><td>Fahrzeug-lokalisierung</td><td rowspan="2">Achszähler/ Gleisstrom-kreise</td><td>Balise + Odometrie</td><td colspan="2" rowspan="2">Balise + Odometrie
GFM Emulation</td></tr>
<tr><td>Gleisfrei-meldung</td><td>Achszähler/ Gleisstrom-kreise</td></tr>
<tr><td>Zugintegritäts-feststellung</td><td>Maßnahmen
1 – 6
TF+HLL</td><td>Maßnahmen
1 – 6
TF+HLL</td><td colspan="2">Maßnahmen
1 – 3,5, 6
TF+HLL + Detekt.</td></tr>
<tr><td>Fahrweg-sicherung</td><td>STW</td><td>RBC
STW
FDL</td><td>RBC
STW
FDL</td><td>RBC
STW (MB)
FDL</td></tr>
</table>

Zugintegrität
Chancen durch Innovation

„Das Alte auf eine neue Weise tun - das ist Innovation.“

Joseph Schumpeter (1883-1950),
österreichisch-amerikanischer Ökonom

„Zugleich erleben wir täglich, wie sehr der digitale Fortschritt unser Leben in allen Bereichen verändert, natürlich auch unser Arbeitsleben. Darauf müssen wir neue Antworten finden. Denn wir wollen, dass alle Menschen Zugang zu der Bildung haben, die sie für diesen Wandel brauchen. Wir wollen, dass sie auch in Zukunft einen guten und sicheren Arbeitsplatz haben – und im Alter eine verlässliche Rente.

Dazu brauchen wir mehr denn je den Mut zu neuem Denken, die Kraft, bekannte Wege zu verlassen, die Bereitschaft, Neues zu wagen, und die Entschlossenheit, schneller zu handeln, in der Überzeugung, dass Ungewohntes gelingen kann – und gelingen muss, wenn es der Generation der heute jungen Menschen und ihren Nachkommen noch möglich sein soll, auf dieser Erde gut leben zu können.“

Neujahrsansprache 2020
von Bundeskanzlerin Dr. Angela Merkel
am 31. Dezember 2019

https://www.toonpool.com/cartoons/Angela%20Merkel_51563

Sicherheitsanforderungen an eine Zugintegritätsprüfung – der Mythos von SIL 4

Ergebnisse von Studien der M2C Expert Control GmbH
Im Auftrag der SBB und ÖBB

Eckehard Schnieder eckehardschnieder@hotmail.de
Jörg May Joerg.May@erc-gruppe.com
Jürg Suter j-suter@bluewin.ch
Florian Peche peche@tu-berlin.de
Andreas Dodinoiu a.dodinoiu@tu-braunschweig.de