NeGSt

Neue Generation Signaltechnik

Sektorweite Initiative zur Sicherung der Zukunftsfähigkeit der Leit- und Sicherungstechnik

Teilbericht

AP 2100 – Semi-quantitative Verfahren zur expliziten Risikoabschätzung

06.08.2013

Gefördert durch:

Bundesministerium für Wirtschaft und Technologie

aufgrund eines Beschlusses des Deutschen Bundestages

Laufzeit: 01.09.2011 – 31.08.2013

Projektträger: TÜV Rheinland Consulting GmbH

Änderungsverfolgung

Datum	Bearbeiter	Version	Inhalt
15.03.2013	Beck (DB Netz AG)	V01	Erstellung
29.04.2013	Beck (DB Netz AG)	V02	Red. Änderungen
30.04.2013	Beck (DB Netz AG)	V03	Ergänzung Beispiel »Temporäre Langsamfahr-stellen einrichten«
16.07.2013	Notter (Thales) Beck (DB Netz AG)	V04	Ergänzung nach Review in AG2
06.08.2013	Beck (DB Netz AG)	V1.0	Finale Abstimmung in AG2

Inhaltsverzeichnis

1 Einleitung

Mit dem in Anhang I, Ziffer 2.5.4 der VO (EG) Nr. 352/2009 (»CSM VO«) genannten Kriterium für die Entwicklung technischer Systeme (»Risikoakzeptanzkriterium für technische Systeme – RAC-TS«) steht erstmals ein harmonisiertes Kriterium zur Verfügung, dass auch zur »Kalibrierung« semi-quantitativer Methoden zur expliziten Risikoabschätzung Verwendung finden kann.

In diesem Dokument soll daher – neben einer kurzen grundlegenden Einführung zu semi-quantitativen Methoden – anhand des Entwurfes der Vornorm E DIN VDE V 0831-103 und ausgewählter Beispiele gezeigt werden, wie eine derartige Kalibrierung erfolgen kann. Außerdem soll ein Ausblick dazu gegeben werden, wie sich die derzeitigen Tendenzen zur Weiterentwicklung des Kriteriums RAC-TS auswirken bzw. welche Empfehlungen zur Weiterentwicklung gegeben werden können.

Vorab soll noch folgende grundsätzliche Erläuterung gegeben werden: In den einschlägigen Normen wird in der Regel nur zwischen »qualitativen oder quantitativen Methoden der Gefährdungs- und Risikoanalyse« unterschieden (siehe z.B. Abschn. 7.4.2.8 in DIN EN 61508-1). Im Sinne dieses Berichtes wird jedoch für alle Methoden, die sowohl qualitative als auch quantitative Aspekte enthalten und mit denen sich Sicherheitsanforderungen in Form einer zulässigen Ausfall- / Gefährdungsrate bzw. einer Sicherheitsanforderungsstufe (SIL) ermitteln lassen der Begriff »semi-quantitativ« verwendet.

2 Vorgaben der CSM VO

2.1 Ausgangslage

In der aktuell gültigen Fassung der CSM VO findet sich für das Kriterium RAC-TS folgende Vorgabe:

2.5.4. Wenn sich aus Ausfällen technischer Systeme Gefährdungen ergeben, die nicht von den anerkannten Regeln der Technik oder der Verwendung eines Referenzsystems abgedeckt werden, gilt für die Planung des technischen Systems folgendes Risikoakzeptanzkriterium:

Bei technischen Systemen, bei denen im Falle eines funktionellen Ausfalls von unmittelbaren katastrophalen Folgen auszugehen ist, muss das damit verbundene Risiko nicht weiter eingedämmt werden, wenn die Ausfallrate pro Betriebsstunde **kleiner oder gleich 10^{-9}** ist.

2.2 Vorschläge zur Weiterentwicklung des Kriteriums RAC-TS

In den Jahren 2007 – 2011 wurde von der hiermit beauftragten Arbeitsgruppe der ERA (»RAC Task Force«) ein erster Vorschlag zur Weiterentwicklung des Kriteriums RAC-TS erarbeitet und in [7] veröffentlicht (s. Abbildung 1).

Severity of the estimated consequences	Acceptable rate of occurrence (R) of the analysed unwanted direct consequence (e.g. of an accident with catastrophic consequences)
multiple fatalities	$R \leq 10^{-9}/h$
single fatality and/or multiple serious injuries	$10^{-9}/h < R \leq 10^{-8}/h$
single serious injury and/or multiple light injuries	$10^{-8}/h < R \leq 3x10^{-7}/h$
single light injury	$3x10^{-7}/h < R \leq 10^{-5}/h$
non safety related consequence	not applicable

Abbildung 1: Vorschlag für weitere Kategorien des Kriteriums RAC-TS

Zu diesem Vorschlag wurde von der ERA initiiert, eine Auswirkungsanalyse durchzuführen, in der die Beteiligten vor Allem Fragestellungen zu bisherigen Erfahrungen mit der Festlegung von Anforderungen an Ausfallraten technischer Funktionen (insbesondere in Verträgen) und Erwartungen an die Harmonisierung von Risikoakzeptanzkriterien sowie deren Auswirkungen auf Produkte beantworten sollten.

Mit [2] legte die CER der ERA ein Positionspapier hierzu vor, in dem auch ein Textvorschlag für die Weiterentwicklung des Kriteriums RAC-TS enthalten ist:

2.5.4. The following design targets shall apply to failures of functions of technical systems for which a suitable probabilistic approach applies:

(a) For a failure that has a credible potential to lead directly to those types of events that have the expectation to affect a group of people and result in collective fatalities, the frequency of the failure of the function does not have to be reduced further if it is demonstrated to lie **within the range 1 x 10^{-9} to 1 x 10^{-8}** failures per operating hour appropriate to the assessed function.

(b) For a failure that has a credible potential to lead directly to those types of events that have the expectation to affect individual people and may result in individual fatality, or those events that may result in collective serious injuries, the frequency of the failure of the function does not have to be reduced further if it is demonstrated to be **less than 1x 10^{-7}** failures per operating hour appropriate to the assessed function.

(c) For a failure that has a credible potential to lead directly to those types of events that have the expectation to affect individual people and may result in a serious injury, but not fatality, the frequency of the failure of the function does not have to be reduced further if it is demonstrated to be **less than 1 x 10^{-6}** failures per operating hour appropriate to the assessed function.

These design requirements shall be referred to as harmonised risk acceptance criteria for technical systems. The achievement of these design targets results in acceptable levels of safety when the safe integration of the technical system into the railway system has been demonstrated.

In (a) to (c) above, the term 'directly' means that no consideration is given to barriers external to the technical system that can reduce the frequency of occurrence of the failure, or mitigate the severity of its consequence.

The harmonised RAC represent the most demanding design criteria that can be required. The harmonised RAC are required to be used only where mutual recognition is being sought, or an AB or NSA can demonstrate that the harmonised RAC are necessary to meet a national safety level. An AB or NSA shall not require a proposer to meet the harmonised RAC in any other cases.

Nach verschiedenen Zwischenschritten und Diskussionen wurde in einem Treffen zwischen ERA und den beteiligten Sektororganisationen folgender Text vorabgestimmt, der im Wesentlichen auf einem zwischen CER und UNIFE abgestimmten Vorschlag beruht (englischer Originaltext aus [2]):

2.5.4. The following design targets shall apply to failures of functions of technical systems for which probabilistic targets can be demonstrated:

(a) For a failure that has a typical credible potential to lead directly to an accident affecting a group of people and resulting in fatalities, the frequency of the failure of the function does not have to be reduced further if it is demonstrated to be **less than 10^{-8}** failures per operating hour appropriate to the assessed function.

(b) For a failure that has a typical credible potential to lead directly to an accident affecting an individual person and resulting in fatality, or affecting a group of people and resulting in serious injuries, the frequency of the failure of the function does not have to be reduced further if it is demonstrated to be **less than 10^{-7}** failures per operating hour appropriate to the assessed function.

(c) For a failure that has a typical credible potential to lead directly an accident affecting an individual person and resulting in a serious injury, but not fatality, the frequency of the failure of the function does not have to be reduced further if it is demonstrated to be **less than 10^{-6}** failures per operating hour appropriate to the assessed function.

These design requirements shall be referred to as harmonised risk acceptance criteria for technical systems. The achievement of these design targets results in acceptable levels of safety when the safe integration of the technical system into the railway system has been demonstrated.

In (a) to (c) above, the term 'directly' means that no consideration is given to barriers external to the technical system that can reduce the frequency of the failure, or mitigate the severity of its consequence.

Letztlich konnte jedoch im anschließenden Review dieses Vorschlages keine Einigung zwischen allen Beteiligten über den finalen Text erzielt werden. Maßgebend hierfür war u.a., dass sich bereits bei vorangegangenen Versuchen zur Validierung des Ansatzes gezeigt hatte, dass hierfür bei den Beteiligten zu wenige aussagekräftige Daten zur Verfügung standen und somit eine belastbare Aussage über die Auswirkungen des weiterentwickelten Kriteriums nicht möglich war. Somit konnte

auch die Befürchtung einiger Beteiligter, dass die Weiterentwicklung zu einer Erhöhung der Sicherheitsanforderungen gegenüber bestehenden Analysen / Realisierungen führen wird (somit »zu konservativ« ist) nicht ausgeräumt werden. Andererseits wurde gleichzeitig auch von einigen Aufsichtsbehörden die Meinung vertreten, dass sie diesen Vorschlag eher als Absenkung der Sicherheitsanforderungen ansehen, zumal der Textvorschlag in (a) formal die Absenkung um eine Zehnerpotenz vorgesehen hat.

Infolgedessen konnte die ERA für die 1. Revision zur CSM VO bis zum vorgesehenen Termin keinen abgestimmten Textvorschlag für die Weiterentwicklung des Kriteriums RAC-TS unterbreiten. Nähere Informationen zu den Aktivitäten und Diskussionen können [4] entnommen werden.

Basierend auf den bisherigen Erfahrungen hat die ERA in [5] mittlerweile einen neuen Vorschlag zur Weiterentwicklung von RAC-TS erarbeitet, der nachfolgend wiedergegeben ist.

2.5.4. The following design targets shall apply to failures of functions of technical systems:

(a) For a failure that has a typical credible potential to lead directly to an accident affecting a group of people and resulting in fatalities and/or severe injuries and/or major damages to the environment, the frequency of the failure of the function does not have to be reduced further if it is demonstrated to be **less than or equal to 10^{-9}** failures per operating hour.

(b) For a failure that has a typical credible potential to lead directly to an accident affecting an individual person and resulting in fatality and/or severe injury, the frequency of the failure of the function does not have to be reduced further if it is demonstrated to be **less than or equal to 10^{-7}** failures per operating hour.

(c) For a failure that has a typical credible potential to lead directly to an accident resulting in one or more light injuries, the frequency of the failure of the function does not have to be reduced further if it is demonstrated to be **less than 10^{-5}** failures per operating hour.

These design requirements shall be referred to as harmonised risk acceptance criteria for technical systems. The achievement of these design targets results in acceptable levels of safety when the safe integration of the technical system into the railway system has been demonstrated.

In (a) to (c) above, the term 'directly' means that no consideration is given to barriers external to the technical system that can reduce the frequency of the failure, or mitigate the severity of its consequence.

Zielstellung in den nächsten Monaten ist es, dass der Vorschlag von den betroffenen Organisationen (Eisenbahnunternehmen, Hersteller, Sicherheitsbehörden, Sektororganisationen) validiert wird. Die Regeln hierzu will die ERA in Kürze bekanntgeben. Weiterhin soll es möglich sein, alternative Vorschläge zu unterbreiten, die jedoch nach den gleichen Regeln zu validieren sind.

3 Semi-quantitative Methoden

3.1 Allgemeines

Semi-quantitative Methoden zur expliziten Risikoabschätzung / Risikoanalyse lassen sich, von wenigen Ausnahmen abgesehen, prinzipiell als Kombination einer Risikomatrix (oder eines Risikographen, der sich jedoch auf eine Risikomatrix zurückführen lässt) und Tabellen zur Bewertung von Barrieren darstellen. Sie werden seit etlichen Jahren in verschiedenen Industriezweigen erfolgreich angewendet und sind in den hierfür geltenden einschlägigen Normen genannt. Beispiele hierfür sind:

- DIN EN 61508-5 für sicherheitsbezogene elektrische/elektronischer/programmierbare elektronische Systeme (Risikograph und »Matrix des Ausmaßes des gefährlichen Vorfalls«),
- DIN EN 13849-1 für Sicherheit von Maschinen (Risikograph).

Hierbei ist darauf hinzuweisen, dass die Methoden in den genannten Normen als Beispiele beschrieben sind und demzufolge der Anwender in der Regel in Abhängigkeit vom Anwendungsfall noch eine weitergehende Anpassung bzw. Kalibrierung durchführen muss.

Der Vorteil bei der Anwendung semi-quantitativer Methoden besteht darin, dass sich gegenüber rein quantitativen Methoden viele Schritte standardisieren lassen. Dies führt zu einer Vereinfachung, Wiederverwendbarkeit und Effizienzsteigerung bei der Durchführung von Risikoanalysen.

Ein wesentlicher Nachteil der bekannten Methoden ist jedoch, dass derzeit für keine Methode eine Begründung für die Konstruktion bzw. ein Hinweis auf das zu Grunde liegende Risikoakzeptanzkriterium veröffentlicht ist. Wohl zumindest mit aus diesem Grund haben diese Methoden bei Bahnanwendungen in der Vergangenheit überwiegend keine Anwendung gefunden bzw. wurde auch die Anwendung von der Aufsichtsbehörde abgelehnt.

Eine weitere Schwäche liegt darin, dass die Methoden oftmals zu konservative Ergebnisse liefern – auch wenn dies aus sicherheitstechnischer Sicht zunächst nicht als Nachteil angesehen werden muss. Dieser Effekt wird vielfach noch dadurch verstärkt, dass Anwender im Zweifel eher zu »worst case« Einschätzungen tendieren, um auf der »sicheren Seite« zu liegen. In [1] finden sich nähere Ausführungen zu dieser Thematik. In [8] wird darüber hinaus am Beispiel des Risikographen nach VDV-Schrift 332 für die punktförmige Zugbeeinflussung gezeigt, dass die hiermit ermittelten Ergebnisse offensichtlich zu konservativ sind.

3.2 Anforderungen an semi-quantitative Methoden nach DIN V VDE V 0831-101

Mit der Vornorm DIN V VDE V 0831-101 wurden für den Anwendungsbereich »Elektrische Bahn-Signalanlagen« erstmals Anforderungen an die verlässliche Konstruktion und Anwendung semi-quantitativer Methoden zur Risikoanalyse aufgestellt. Die Vornorm gibt Anleitung, wie diese Methoden konstruiert und angewandt werden können, um Sicherheitsanforderungen für technische Systeme für Bahn-Signalanlagen abzuleiten, indem

- grundlegende Prinzipien erklärt werden,
- die notwendigen Verfahrensschritte zur Durchführung der Risikoanalyse bereitgestellt werden,
- geeignete Benennungen, Voraussetzungen, Maßgrößen für die Beurteilung der maßgeblichen Parameter wie Schadensausmaß oder Wirksamkeit von Barrieren bereitgestellt werden,
- Beispiele für die notwendigen Arbeitsblätter oder andere Tabellenformen bereitgestellt werden.

Die DIN V VDE V 0831-101 definiert insgesamt 28 Anforderungen an die Konstruktion und / oder Anwendung einer semi-quantitativen Methoden, auf die – sofern für diesen Bericht relevant – nachfolgend noch näher eingegangen wird.

3.3 Die semi-quantitative Methode RSM nach E DIN VDE V 0831-103

Als Anforderung A4 in DIN V VDE V 0831-101 ist gefordert, dass für jede semi-quantitative Methode ein Anwender-Handbuch erstellt werden muss, das Definitionen, Erläuterungen und Beispielanwendungen enthält. Ausgehend von dieser Anforderung wurde mit dem Entwurf der Vornorm E DIN VDE V 0831-103 ein derartiges Handbuch für die Methode »Risk Score Matrix« (RSM) erarbeitet. Hierin wird eine Anleitung für die Anwendung dieser Methode gegeben, indem

- der Aufbau der Methode beschrieben wird,
- die notwendigen Parameter festgelegt werden,
- eine Systemdefinition für generische Funktionen der Eisenbahnsignaltechnik durchgeführt wird (in Anhang A),

- für diese Funktionen mittels der gewählten Methode exemplarisch Sicherheitsanforderungen – unter Berücksichtigung relevanter Randbedingungen – abgeleitet werden,
- die Erfüllung der Anforderungen an die Konstruktion und Anwendung semi-quantitativer Methoden nach DIN V VDE V 0831-101 nachgewiesen wird (in Anhang C).

Insbesondere wurde darauf Wert gelegt, die Konstruktion der Methode ausreichend zu begründen. Wesentlicher Bestandteil der Methode ist hierbei die Kalibrierung anhand des Kriteriums RAC-TS. Die nähere Beschreibung der Methode erfolgt nachfolgend im Abschnitt 4.

4 Methodik nach E DIN VDE V 0831-103

4.1 Aufbau und Kalibrierung der RSM

Aufbau und Kalibrierung der RSM sind in Abbildung 2 dargestellt:

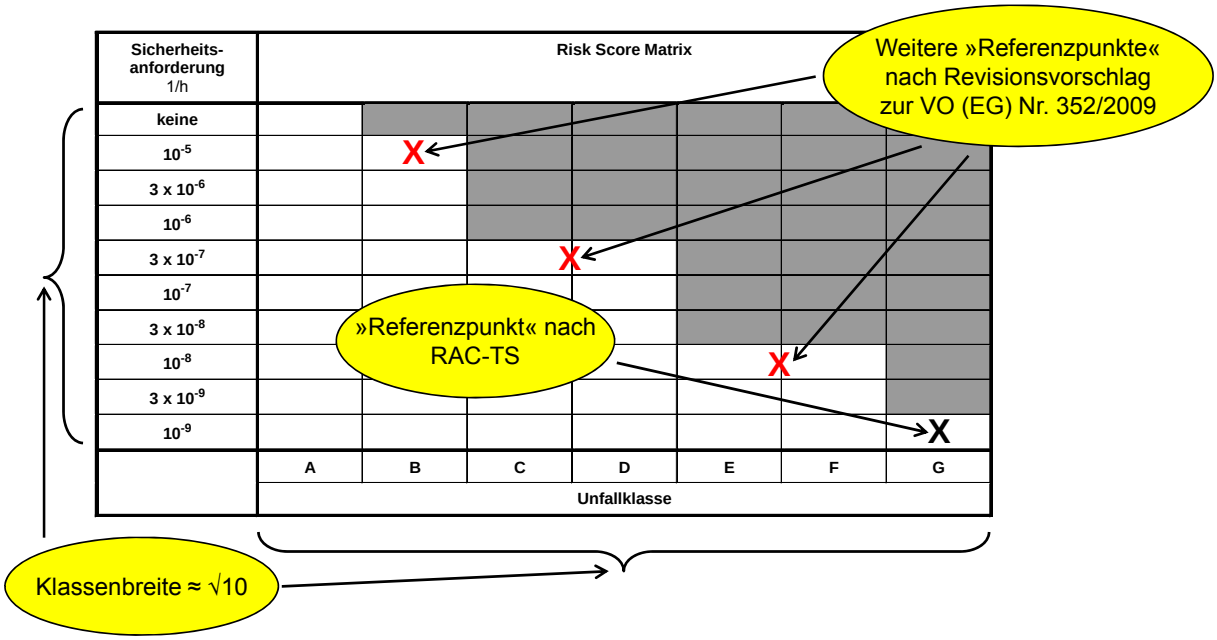

Abbildung 2: Risk Score Matrix nach E DIN VDE V 0831-103

In der Risk Score Matrix sind horizontal die Unfallklassen und vertikal die Sicherheitsanforderungen eingetragen. Die Grenze des tolerierbaren Risikos wird hierbei durch die jeweils oberste weiße Zelle in der jeweiligen Spalte – als Verbindung zwischen Unfallklasse und angegebener Sicherheitsanforderung – repräsentiert.

Die Klasseneinteilung – sowohl für die Unfallklassen als auch für die Sicherheitsanforderungen – ist dabei so gewählt, dass sich eine Klasse um angenähert den Faktor √10 von der benachbarten Klasse unterscheidet. Hiermit wird einerseits Anforderung A3 (Granularität) aus DIN V VDE V 0831-101 erfüllt und andererseits eine darüber hinausgehende bessere Granularität erreicht und somit auch Anforderung A26 (Sensitivität) unterstützt.

Die Zelle im Schnittpunkt zwischen Unfallklasse G und der Sicherheitsanforderung 10^{-9}/h bildet den Referenzpunkt zur Kalibrierung entsprechend des Risikoakzeptanzkriteriums RAC-TS nach CSM VO.

Die Zellen im Schnittpunkt zwischen

- Unfallklassen E/F und Sicherheitsanforderung 10^{-8}/h,
- Unfallklassen C/D und Sicherheitsanforderung 3×10^{-7}/h,

- Unfallklasse B und Sicherheitsanforderung 10^{-5}/h

bilden Referenzpunkte zur Kalibrierung entsprechend des Vorschlages der ERA [7] zur Revision der CSM VO.

Die aufgeführten Sicherheitsanforderungen sind hierbei als diejenigen zu verstehen, die sich ohne Berücksichtigung von Barrieren ergeben. Für die Unfallklassen C/D bzw. E/F gelten hierbei die gleichen Sicherheitsanforderungen, da in der RSM aus dem oben genannten Grund eine feinere Granularität gewählt wurde als bei der Definition des (weiterentwickelten) Kriteriums RAC-TS. Zu den daraus zu gewinnenden Erkenntnissen erfolgen in diesem Bericht an anderer Stelle noch detailliertere Ausführungen.

4.2 Anwendung der Methodik

Die Anwendung der RSM auf definierte Funktionen / Ausfälle erfolgt nach dem nachfolgend beschriebenen Schema:

Für jede Ausfallart wird zunächst analysiert, welche Ereignisart(en) hieraus resultieren können und die jeweils zutreffende Unfallklasse ermittelt. Anschließend werden die möglichen Barrieren bestimmt und anhand von Tabellen mit Punkten bewertet. Danach wird geprüft, ob bei einer Barriere eine Abhängigkeit zu anderen Barrieren oder der Unfallklasse besteht und die Punktzahl dieser Barriere ggf. reduziert. Die Sicherheitsanforderung ergibt sich, indem in der Spalte mit der Unfallklasse – ausgehend von der jeweils obersten weißen Zelle – für jeden Bewertungspunkt einer Barriere jeweils eine Zelle nach oben gegangen wird und dann der in der gleichen Zeile äußerst links stehende Wert abgelesen wird. Sofern bei einer Ausfallart mehrere Gefährdungsszenarien möglich sind, ergibt sich die Sicherheitsanforderung für diese Ausfallart als Minimalwert aus den Sicherheitsanforderungen für die jeweiligen Szenarien.

4.3 Die Tabelle der Unfallklassen in E DIN VDE V 0831-103

Eine »zentrale Vorgabe« in E DIN VDE V 0831-103 (da als Ausgangspunkt für die Ermittlung von Sicherheitsanforderungen und Nachweis für die Kalibrierung der Methode gegen ein Risikoakzeptanzkriterium dienend) stellt die Tabelle der Unfallklassen dar, wie sie in Tabelle 1 dargestellt ist.

Unfallklasse	Ereignisart	»maßgebendes« Schadensausmaß
A	Aufprall auf Gleissperre Aufprall einer Rangierfahrt auf Gegenstand Unzeitige Zwangsbremsung	Kein Personenschaden; geringer Sachschaden
B	Person stürzt beim Aussteigen Person oder Fahrzeug wird von Schrankenbaum getroffen Aufprall eines Reisezuges auf Gegenstand bei niedriger Geschwindigkeit Aufprall eines Güterzuges auf Gegenstand Entgleisung einer Rangierfahrt Zusammenstoß von Rangierfahrten	Ein Leichtverletzter; mittlerer Sachschaden
C	Aufprall eines Reisezuges auf Gleisabschluss Aufprall eines Reisezuges auf Gegenstand bei mittlerer Geschwindigkeit Entgleisung eines Reisezuges bei niedriger Geschwindigkeit	Mehrere Leichtverletzte
D	Zusammenstoß mit einem Reisezug bei niedriger Geschwindigkeit Entgleisung eines Güterzuges Zusammenstoß zwischen Güterzügen Aufprall eines Reisezuges auf Gegenstand bei hoher Geschwindigkeit	Ein Schwerverletzter oder viele Leichtverletzte; hoher Sachschaden
E	Entgleisung eines Reisezuges bei mittlerer Geschwindigkeit Zusammenprall mit nicht führendem Eisenbahnfahrzeug	Mehrere Schwerverletzte
F	Zusammenprall mit führendem Eisenbahnfahrzeug Personenunfall an höhengleichem Bahnsteigzugang Personenunfall in einer Arbeitsstelle Zusammenstoß mit einem Reisezug bei mittlerer Geschwindigkeit	Ein Todesfall oder viele Schwerverletzte; beträchtlicher Sachschaden
G	Entgleisung eines Reisezugs bei hoher Geschwindigkeit Zusammenstoß mit einem Reisezug bei hoher Geschwindigkeit	Mehrere Todesfälle

Tabelle 1: Unfallklassen nach E DIN VDE V 0831-103

Obwohl dies für den Anwender prinzipiell als entbehrlich angesehen werden könnte, wurde in der Tabelle die Spalte »maßgebendes Schadensausmaß« eingefügt, da hiermit einerseits eine Begründung für die Kalibrierung gegen ein Risikoakzeptanzkriterium direkt ersichtlich ist und andererseits bei Bedarf die Einstufung von anderen – nicht in der Tabelle genannten – Ereignissen erleichtert

wird. Das »maßgebende Schadensausmaß« ist hierbei dasjenige, welches überwiegend – d.h. bei konservativer Abschätzung – bei einem Ereignis der jeweiligen Ereignisart nicht überschritten wird. Zur Gewährleistung der Kompatibilität zwischen den Klasseneinteilungen für die Unfallklassen und für die Sicherheitsanforderungen ist hierbei der Begriff »mehrere« im Sinne von »ca. 3« und »viele« im Sinne von »ca. 10« aufzufassen.

Zur Einordnung der Ereignisarten erfolgte ein Abgleich unter Zuhilfenahme statistischer Daten, bei dem geprüft wurde, dass Ereignisarten mindestens in diejenige Unfallklasse eingeordnet sind, die von 90 % aller Ereignisse der jeweiligen Ereignisart nicht überschritten wird. Mindestens bedeutet hierbei, dass im Zweifel (z. B. auch bei zu geringer Aussagekraft der statistischen Daten im Einzelfall) konservative Annahmen getroffen wurden – auch um die Einordnung im Gesamtzusammenhang (z. B. unterschiedliche Unfallklassen bei unterschiedlichen Geschwindigkeiten) plausibel zu halten. Dies ist auch notwendig, da schwere Eisenbahnunfälle glücklicherweise sehr selten sind und bei ausschließlicher Betrachtung statistischer Daten daher Ereignisse mit potenziell schwerem Ausmaß möglicherweise in eine »zu niedrige« Unfallklasse eingestuft würden.

Insgesamt erfolgte die Einstufung der Ereignisse daher als Kombination aus Auswertung statistischer Daten und Experteneinschätzungen. Hierbei wurde auch auf die Vorarbeiten der ERA zurückgegriffen, indem die Beispiele in [6] berücksichtigt wurden. So ist als Ereignisart, die in die höchste (»kritischste«) Unfallklasse fällt, hiernach die Entgleisung eines Reisezuges bei hoher Geschwindigkeit aufgeführt. Ebenfalls entsprechend des Beispiels in [6] sind die Entgleisung eines Reisezuges bei mittlerer und bei niedriger Geschwindigkeit sowie die Entgleisung einer Rangierfahrt eingeordnet. Für Aufpralle eines Reisezuges auf Gegenstände (außer auf einen Gleisabschluss, da hierfür aussagekräftige statistische Daten vorliegen) wird insgesamt eine konservative Einordnung vorgenommen.

4.4 Barrierenmodell in E DIN VDE V 0831-103

Für die Bestimmung von Barrieren sieht E DIN VDE insgesamt 4 Tabellen vor:

- Bewertung menschlicher Handlungen,
- Bewertung von der Betriebsdichte abhängiger Barrieren,
- Bewertung der Anforderungsrate mit Ausfalloffenbarung,
- Bewertung weiterer Barrieren.

Außerdem beschreibt eine gesonderte Tabelle die Bewertung der Abhängigkeit zwischen Barriere und anderen Barrieren bzw. Unfallklasse. In den Tabellen werden für die einzelnen Barrieren Wirksamkeitsklassen gebildet, die in Bezug auf ihre Risikoreduktion mit Punkten bewertet werden. Grundsatz für die Bewertung von Barrieren ist, dass entsprechend der gewählten Klasseneinteilung für die Unfallklassen und Sicherheitsanforderungen eine Punktzahl von 2 einer Risikoreduktion durch die Barriere in Höhe von 0,1 (Faktor 10) entspricht. Durch die Tabelle zur Bewertung weiterer Barrieren besteht auch die Möglichkeit der Kombination der Methode mit anderen Verfahren (z.B. ETA, FTA), mit denen eine Quantifizierung der Wirksamkeit von Barrieren möglich ist.

5 Validierung der Methode nach E DIN VDE V 0831-103 anhand weiterer Beispiele

In diesem Abschnitt soll gezeigt werden, dass sich die Methode RSM nach E DIN VDE V 0831-103 grundsätzlich auch dafür eignet, für andere Systeme / Funktionen als diejenigen, die im Anhang B des Vornormentwurfes genannt sind, Sicherheitsanforderungen abzuleiten. Hierzu werden entsprechende Beispiele beschrieben. Es ist darauf hinzuweisen, dass diese Beispiele im Rahmen des Forschungsvorhabens NeGSt nicht den Anspruch einer vollständigen Risikobewertung erfüllen können. Insbesondere dient die jeweilige Systemdefinition nur dem im Rahmen dieses Berichtes erforderlichen allgemeinen Verständnis. Die Form der Bewertung von Funktionen entspricht hierbei dem Muster in E DIN VDE V 0831-103.

5.1 Tunnelbegegnungsverbot

5.1.1 Systemdefinition

Die im Bau befindliche Neubaustrecke Ebensfeld – Erfurt soll von TSI-konformen Reisezügen und Güterzügen im Mischbetrieb befahren werden. Auf dieser Strecke sind zweigleisige, einröhrige Tunnel vorhanden. Um bei Fahrgeschwindigkeiten bis 300 km/h für Reisezüge die Sicherheit im Sinne EBA-Richtlinie [3] sowie in Bezug auf aerodynamische Einwirkungen sicherstellen zu können, sind neben einem fahrplanmäßigen Begegnungsausschluss wirksame Maßnahmen notwendig, um auch bei Abweichungen vom Fahrplan Begegnungen in Tunneln zuverlässig zu vermeiden. Hierzu sollen in definierten Tunnelbereichen mit Hilfe eines technischen Systems (TBV-System) im Zusammenwirken mit der Stellwerkstechnik Begegnungen/Überholungen zwischen Reise- und Güterzügen ausgeschlossen werden.

Das TBV-System stellt im Wesentlichen die folgenden Funktionen auf definierten tunnelreichen Streckenabschnitten (= Tunnelbereichen) sicher:

- Über Sensoren (z. B. zur Achsmustererkennung) sowie mittels weiterer im Stellwerk bzw. im RBC verfügbarer Daten wird die Zugart aller sich dem Tunnelbereich nähernden Züge ermittelt (Zugarterkennung).
- Das TBV-System überwacht nach erfolgter Zugarterkennung jederzeit die Standorte aller im Überwachungsbereich befindlichen Züge (Zuglaufverfolgung).
- In Abhängigkeit der aktuellen Belegung eines Tunnelbereichs auf dem jeweils anderen Gleis wird einem sich nähernden Zug über eine geeignete Verarbeitungslogik eine Fahrerlaubnis ohne Restriktion, eine solche mit Restriktion (Geschwindigkeitsbeschränkung) oder ein Haltbefehl zugeordnet. Das TBV-System übermittelt diese Information an dasjenige Stellwerk, welches das zugeordnete Signal vor dem Tunnelbereich steuert.

5.1.2 Ableitung von Sicherheitsanforderungen entsprechend E DIN VDE V 0831-103

Schutzziel:

– Ausschließen von unzulässigen Begegnungen/Überholungen von Reise- und Güterzügen in Tunnelbereichen

Randbedingungen:

Die Betrachtung beschränkt sich auf Risiken infolge von möglichen Ereignissen in Tunneln, die in einem unmittelbaren Zusammenhang mit unzulässigen Begegnungen/Überholungen zwischen Reise- und Güterzügen und damit mit der Sicherheit des geplanten TBV-Systems stehen.

Ausfallarten der Funktion:

a) Unzulässige Begegnung/Überholung in Tunnelbereich nicht ausgeschlossen

Auswirkungen einschließlich ggf. auslösender Bedingungen:

a1) Wenn unmittelbar vor der Begegnung/Überholung ein Güterzug entgleist bzw. in Brand gerät, kann es im Moment der Begegnung/Überholung zu einer Eskalation mit entsprechend höheren Sach- und Personenschäden kommen, wenn die Begegnung/Überholung nicht durch Intervention des Fahrdienstleiters (Abgabe eines Nothaltauftrages) noch verhindert werden kann. Als konservative Abschätzung des zu erwartenden weiteren Schadensverlaufes muss davon ausgegangen werden, dass die Auswirkungen vergleichbar sind mit denjenigen bei Entgleisung eines Reisezuges oder Zusammenstoß mit einem Reisezug – jeweils bei hoher Geschwindigkeit entsprechend der zulässigen Geschwindigkeit in Tunnelbereichen (= **Unfallklasse G**) – auch wenn diese Ereignisse streng genommen lediglich Folgeereignisse von Entgleisung bzw. Brand eines Güterzuges sind und hierfür das diesbezügliche Schadensausmaß angesetzt werden müsste.

Anmerkung: Da der Fokus des Entwurfs E DIN VDE V 0831-103 auf Funktionen/Ausfällen der LST liegt, findet sich in der Tabelle der Unfallklassen das Ereignis Brand nicht wieder, sodass hier die Auswirkungen anhand eines Vergleiches mit Auswirkungen anderer Ereignisse ermittelt wurden.

a2) Auf Grund aerodynamischer Lasten bei Begegnung mit/Überholung von Zügen mit Pkw-Transportwagen oder Zügen der »Rollenden Landstraße«: Beschädigung/Verlust von Anbauteilen von Straßenfahrzeugen oder Einrichtungen zum Schutz der Ladung (z.B. Planen) (= **Unfallklasse A**, da nur Sachschaden zu erwarten ist)

a3) Auf Grund aerodynamischer Lasten bei Begegnung mit Zügen mit Schiebewandwagen bzw. Wagen mit beweglichen Seitenwänden/Türen: Abreißen von Schiebewänden, Seitenwänden oder Türen und in Folge davon Aufprall eines Reisezuges auf diese Teile. Prinzipiell wäre bei Anwendung der Tabelle der Unfallklassen nach E DIN VDE V 0831-103 hierfür Unfallklasse D entsprechend eines Aufpralls eines Reisezuges auf einen Gegenstand bei hoher Geschwindigkeit zu wählen. Das angenommene Ausmaß dieses Ereignisses wird hierbei jedoch auch davon beeinflusst, dass der Aufprall typischerweise mit der Zugspitze erfolgt und das Schadensausmaß durch geeignete Gestaltung der Fahrzeuge (Bahnräumer, Einrichtungen zur Gewährleistung der Crashsicherheit) beeinflusst wird. In dem hier betrachteten Gefährdungsszenario kann der Aufprall jedoch auch seitlich erfolgen (z.B. in Fensterhöhe), sodass von kritischeren Auswirkungen auszugehen ist. Andererseits erscheint auch die Wahl der höchsten Unfallklasse nicht gerechtfertigt, sodass hier als konservative Annahme **Unfallklasse F** angenommen wird.

a4) Auf Grund aerodynamischer Lasten bei Überholung von Zügen mit Schiebewandwagen bzw. Wagen mit beweglichen Seitenwänden/Türen: wie a3) – **Unfallklasse F**.

Auf Grund von Erkenntnissen aus vorangegangenen Analysen zu aerodynamischen Einwirkungen bei Begegnung/Überholung zwischen Reise- und Güterzügen in Tunneln (die beginnend bereits vor Aufnahme des Hochgeschwindigkeitsverkehrs auf den Strecken Mannheim – Stuttgart und Hannover – Würzburg) durchgeführt wurden) wird das Gefährdungsszenario »Verlust einer schweren Ladung infolge von aerodynamischen Einwirkungen« nicht als maßgebend angesehen und daher nicht betrachtet.

Schutzobjekt:

a) Reisende, Mitarbeiter, Fahrzeuge, Ladung

Bewertung von Barrieren:

a1) Entgleisung bzw. Brand eines Güterzuges unter der zusätzlichen Bedingung, dass dies unmittelbar vor einer Begegnung/Überholung mit einem Reisezug in einem Tunnelbereich stattgefunden hat, sind seltene bis sehr seltene Ereignisse. Andererseits erfolgt eine Ausfalloffenbarung des TBV-Systems häufig bis dauernd, da auf Grund des vorgesehenen Betriebspro-

grammes ständig Möglichkeiten zur Begegnung zwischen Reise- und Güterzügen bestehen und insofern ein Versagen des TBV-Systems vom Fahrdienstleiter erkannt werden kann. Bei Anwendung von Tabelle 7 aus E DIN VDE V 0831-103 ergibt sich hieraus die **Punktzahl 6**.

a2) Da mit Unfallklasse A bereits die niedrigste Unfallklasse angenommen wurde, wird auf die Bewertung von Barrieren verzichtet.

a3) Es darf davon ausgegangen werden, dass nicht jede unzulässige Begegnung zu einem Abreißen von Schiebewänden oder anderen größeren beweglichen Teilen von Güterwagen führt. Dies ist einerseits darin begründet, dass bei hier anzunehmender unveränderter Konstruktion der Güterwagen derzeit bei Begegnungen ein definiertes Drucklastniveau ertragbar ist, ohne dass hieraus entsprechenden Beschädigungen an Güterwagen resultieren und auch bei den veränderten Randbedingungen, wie sie der Risikobewertung zu Grunde liegen, eine gewisse Anzahl an Belastungen verkraftbar ist, bevor Beschädigungen eintreten. Auch unter Berücksichtigung der Tatsache, das sich in einem Zug mehrere »gefährdete« Güterwagen befinden können und somit die Wahrscheinlichkeit – bezogen auf die Begegnung mit einem Zug – entsprechend steigt, kann insgesamt zumindest von einer mittleren Risikoreduktion ausgegangen werden. Dies entspricht der Annahme, dass es bei ca. 10 unzulässigen Begegnungen einmal zu einem Abreißen einer Schiebewand oder anderen beweglichen Teilen kommt. Bei Anwendung von Tabelle 9 aus E DIN 0831-103 resultiert hieraus die **Punktzahl 2**.

a4) Aus Versuchen sei als bekannt vorausgesetzt, dass aus Überholungen ungünstigere aerodynamische Bedingungen resultieren können, sodass die entsprechende Drucklast ansteigt. Somit steigt auch die Wahrscheinlichkeit des Abreißens einer Schiebewand oder anderer beweglicher Teile. Wird hier davon ausgegangen, dass die Wahrscheinlichkeit konservativ betrachtet um den Faktor 2 ansteigt, so ergibt sich bei Anwendung von Tabelle 9 aus E DIN 0831-103 die Punktzahl 1. Andererseits darf jedoch berücksichtigt werden, dass das Szenario Überholung auf Grund von Infrastruktur und Betriebslage (Überholung eines Güterzuges in einem Tunnelbereich ist nur möglich, wenn diese die Fahrt eines Zuges auf dem Gegengleis über einen längeren Abschnitt zulässt) wesentlich seltener ist als das Szenario Begegnung. Unter Anwendung von Tabelle 6 aus E DIN 0831-103 kann dieses Szenario als »unterdurchschnittliche Betriebsdichte« gegenüber dem Szenario Begegnung eingestuft werden, woraus sich die Punktzahl 2 ergibt. Dies entspricht der Annahme, dass Begegnung und Überholung im Verhältnis ca. 10 : 1 stehen. Insgesamt ergibt sich somit die **Punktzahl 3**.

Anmerkung: Auf Basis umfassender Analysen der aerodynamischen Zusammenhänge und daraus resultierender Auswirkungen wurde rechnerisch ermittelt, dass die Wahrscheinlichkeit für ein Abreißen von Schiebewänden oder anderer beweglicher Teilen tatsächlich geringer ist als die bei vorstehender Betrachtung angenommene Wahrscheinlichkeit. Da diese Analysen jedoch nicht öffentlich verfügbar sind (und somit die Werte nicht einfach übernommen werden können), in diesem Bericht nur die generelle Anwendbarkeit der Methode RSM untersucht wird und semi-quantitative Methoden im Zweifelsfall durchaus konservativere Resultaten liefern dürfen, wird hierin kein Widerspruch gesehen.

Darstellung der RSM:

Tabelle 2 stellt die entsprechende RSM dar.

Sicherheits-anforderung 1/h	Risk Score Matrix						
keine	● a2)						
10^{-5}							
3×10^{-6}							
10^{-6}							
3×10^{-7}							
10^{-7}							
3×10^{-8}							
10^{-8}						a3) ● a4)	
3×10^{-9}							
10^{-9}							● a1)
	A	B	C	D	E	F	G
	Unfallklasse						

Tabelle 2: RSM für »Tunnelbegegnungsverbot«

Sicherheitsanforderung:

1×10^{-7}/h

5.2 Rechnergestützter Zugleitbetrieb (RZL) am Beispiel des Projektes SATLOC

5.2.1 Systemdefinition

Das System stellt eine technische Unterstützung für den Zugleitbetrieb auf schwach befahrenen Strecken (UIC Kategorie E, max. 2 Züge pro Stunde) bereit. Die wichtigsten Eigenschaften:

- Streckenzentrale und Fahrzeuge stehen kontinuierlich über eine hochverfügbare Funkverbindung in Kontakt.
- Die Fahrzeuge ermitteln ca. einmal pro Sekunde ihre Position und übermitteln diese an die Streckenzentrale, die die Position plausibilisiert.
- Die Fahraufträge werden von der Streckenzentrale erzeugt und vom Zugleiter plausibilisiert und freigegeben.
- Der Triebfahrzeugführer plausibilisiert den Fahrauftrag, bevor er ihn annimmt.
- Das Fahrzeuggerät überwacht die Ausführung des Fahrauftrags kontinuierlich, bei Verstoß wird automatisch die Notbremse aktiviert. Ohne Fahrauftrag schützt das System gegen unberechtigtes Anfahren.
- Streckenseitige Ausrüstung z. B. Stellwerke, sind nicht Teil des RZL. Es wird davon ausgegangen, dass die Weichen korrekt gestellt sind, z. B. Rückfallweichen.

Prinzipielle Zusammenhänge sind in Abbildung 5 dargestellt. Weitere Informationen können http://satloc.uic.org/Project-summary entnommen werden.

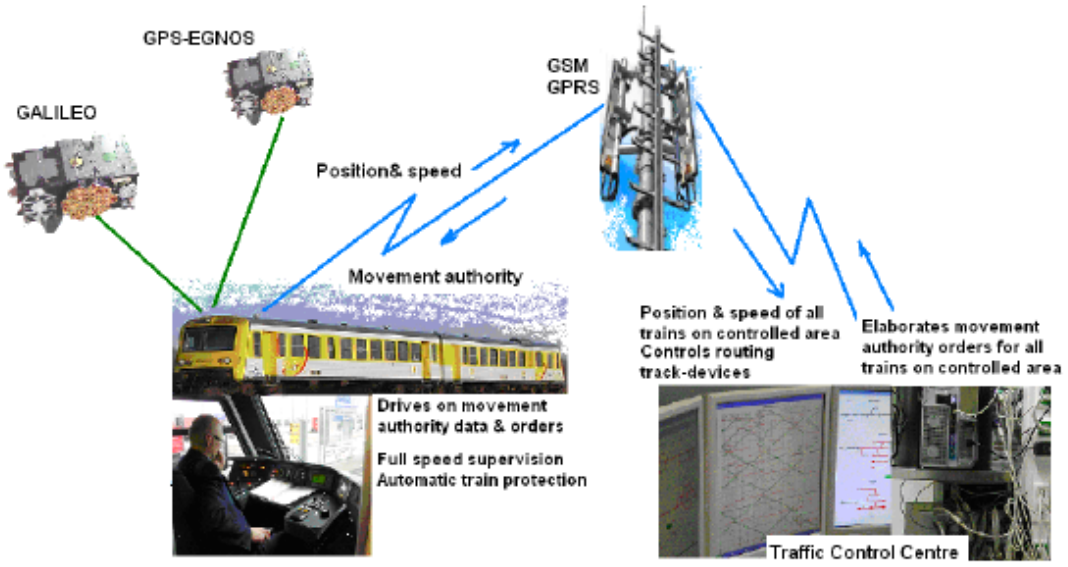

Abbildung 3: Ausführungs-Beispiel: SATLOC-Projekt

Die wichtigsten Funktionen sind:

1. Bereitstellung des Fahrauftrags (MA)
2. Überwachung des Fahrauftrags (TC)

Diese Funktionen entsprechen nach E DIN VDE V 0831-103:

1. MA=Überwachungsgrößen bereitstellen (B5.17)
2. TC=Zugbewegung überwachen (B5.19)

5.2.2 Ableitung von Sicherheitsanforderungen entsprechend E DIN VDE V 0831-103

<u>Überwachungsgrößen bereitstellen (MA)</u>

Schutzziel:

– Umsetzung der Informationen von der streckenseitigen Signaltechnik für die fahrzeugseitige Zugsicherungsausrüstung, d. h. Bereitstellung eines konfliktfreien Fahrauftrags

– Übertragung von Informationen / Anweisungen an die fahrzeugseitige Zugsicherungsausrüstung

Randbedingungen:

– die Anzeige von Überwachungsgrößen befreit den Triebfahrzeugführer nicht von der Beobachtung der Strecke und der Signale am Fahrweg

– der Zugleiter plausibilisiert den Fahrauftrag anhand seines Lagebildes

– der Triebfahrzeugführer plausibilisiert den Fahrauftrag anhand seines betrieblichen Auftrags, z. B. Fahrplan

Ausfallarten der Funktion:

a) weniger restriktive Überwachungsgrößen an fahrzeugseitige Zugsicherungsausrüstung übertragen

b) restriktivere Überwachungsgrößen an fahrzeugseitige Zugsicherungsausrüstung übertragen

Auswirkungen einschließlich ggf. auslösender Bedingungen:

a1) Entgleisung durch Überschreitung der für den Fahrtverlauf zulässigen Geschwindigkeit bei mittlerer Geschwindigkeit (= **Unfallklasse F**)

a2) Frontal-Zusammenstoß mit anderen Fahrzeugen durch Unterschreitung der Mindestabstände (= **Unfallklasse G**)

Bei höheren zulässigen Geschwindigkeiten werden die betreffenden Strecken in der Regel mit automatischen Zugsteuerungssystemen ausgerüstet. Als konservative Annahme wird jedoch trotzdem davon ausgegangen, dass bei einer eingleisigen Strecke in der Regel zwei Reisezüge mit mittlerer Geschwindigkeit betroffen sind, so dass sich eine hohe Geschwindigkeit beim Zusammenstoß ergeben kann.

b) durch Widerspruch zwischen Ortung bzw. Geschwindigkeitsmessung auf dem Zug und übertragenen Überwachungsgrößen: Person stürzt auf Grund unzeitiger Zwangsbremsung (= **Unfallklasse A**)

Schutzobjekt:

a) Reisende, Mitarbeiter, Fahrzeuge, Ladung

Bewertung von Barrieren:

a1) Der Triebfahrzeugführer muss den Fahrauftrag plausibilisieren, bevor er ihn akzeptiert. Er kann Fehler erkennen, allerdings nur relativ offensichtliche. Da sich bei einfachen Betriebsverhältnissen die Aufträge häufig wiederholen und auch Fahrzeug- und Streckeneigenschaften sich nur selten ändern, werden die Fahraufträge in der Regel identisch sein und der Triebfahrzeugführer kann Abweichungen davon leicht erkennen. Dies kann als regelbasierte Handlung ohne Stress (da das Beachten von Fahraufträgen bei mittlerer Geschwindigkeit an sich keine Stresssituation darstellt) unter guten Bedingungen angesehen werden, d. h. 4 Punkte. Auch der Zugleiter hat die Möglichkeit, fehlerhafte Fahraufträge zu erkennen, allerdings wohl nur, wenn der Fehler ziemlich offensichtlich ist. Wir stufen diese Handlung als wissensbasiert ein, allerdings unter normalem Stress und guten Bedingungen, d. h. 2 Punkte. Da es Fehler geben könnte, die sowohl vom Triebfahrzeugführer als auch vom Zugleiter schwer zu erkennen sind, ist die Unabhängigkeit der Prüfungen nicht vollständig (1 Punkt Abzug). Hieraus ergibt sich die **Punktzahl 5**.

a2) Wie a1): **Punktzahl 5**

b) Der Triebfahrzeugführer kann fehlerhaft übertragene Überwachungsgrößen oder fehlerhafte Ortungsinformationen, die im Widerspruch, nicht erkennen und eine Zwangsbremsung nicht verhindern. Insofern kann **keine wirksame Barriere** identifiziert werden.

Darstellung der RSM:

Tabelle 3 stellt die entsprechende RSM dar.

Sicherheits-anforderung 1/h	Risk Score Matrix						
keine	b) ●						
10^{-5}							
3×10^{-6}							
10^{-6}							
3×10^{-7}							
10^{-7}							
3×10^{-8}							
10^{-8}						a1) ●	
3×10^{-9}							
10^{-9}							a2) ●
	A	B	C	D	E	F	G
	Unfallklasse						

Tabelle 3: RSM für »Überwachungsgrößen bereitstellen (MA)«

Sicherheitsanforderung:

3×10^{-7}/h (für Ausfallart »weniger restriktive Überwachungsgrößen an fahrzeugseitige Zugsicherungsausrüstung übertragen«)

keine (für Ausfallart »restriktivere Überwachungsgrößen an fahrzeugseitige Zugsicherungsausrüstung übertragen«)

<u>Zugbewegung überwachen (TC)</u>

Schutzziel:

– gewährleisten, dass der Zug selbsttätig zum Halten gebracht werden kann, wenn die Fahrweise des Triebfahrzeugführers im Hinblick auf die Geschwindigkeit (entsprechend der Überwachungsgrößen) unzulässig ist

Randbedingungen:

– die Anzeige von Überwachungsgrößen befreit den Triebfahrzeugführer nicht von der Beobachtung der Strecke und der Signale am Fahrweg

Ausfallarten der Funktion:

a) keine Zwangsbremsung ausgelöst bei Überschreitung von Überwachungsgrößen

b) unzeitige Zwangsbremsung ausgelöst

Auswirkungen einschließlich ggf. auslösender Bedingungen:

a1) Wie a1) oben: **Unfallklasse F**

a2) Wie a2) oben: **Unfallklasse G**

b) Person stürzt auf Grund unzeitiger Zwangsbremsung (= **Unfallklasse A**)

Schutzobjekt:

a) Reisende, Mitarbeiter, Fahrzeuge, Ladung

Bewertung von Barrieren:

a1) Der Triebfahrzeugführer hat trotz vorhandener Zugsicherungsausrüstung die Signale (bei einfachen Strecken die Tafeln) am Fahrweg sowie die Anzeigen auf seinem Führerstandsdisplay zu beachten. Dies kann als fertigkeitsbasierte Handlung ohne Stress (da das Beachten von Signalen bzw. Führerstandsdisplay an sich keine Stresssituation darstellt) und bei schlechten Bedingungen angesehen werden (Tafeln sind weniger auffällig als Signale) – **Punktzahl 5**.

a2) Evtl. hat der Triebfahrzeugführer noch die Möglichkeit, den entgegenkommenden Zug zu erkennen, aber schon bei mittleren Geschwindigkeiten keine Möglichkeit mehr, den Zusammenstoß zu vermeiden. Wie a1) **Punktzahl 5**

b) Wie b) oben keine wirksame Barriere

Darstellung der RSM:

Tabelle 4 stellt die entsprechende RSM dar.

Sicherheits-anforderung 1/h	**Risk Score Matrix**						
keine	b) ●						
10^{-5}							
3×10^{-6}							
10^{-6}							
3×10^{-7}							
10^{-7}							
3×10^{-8}							
10^{-8}						a1) ●	
3×10^{-9}							
10^{-9}							a2) ●
	A	**B**	**C**	**D**	**E**	**F**	**G**
	Unfallklasse						

Tabelle 4: RSM für »Zugbewegung überwachen (TC)«

Sicherheitsanforderung:

3×10^{-7}/h (für Ausfallart »keine Zwangsbremsung ausgelöst bei Überschreitung von Überwachungsgrößen«)

keine (für Ausfallart »unzeitige Zwangsbremsung ausgelöst«)

5.3 Temporäre Langsamfahrstellen einrichten

5.3.1 Systemdefinition

Derzeit erfolgt bei den Zugsicherungssystemen LZB und ETCS Level 2 die Interaktion zwischen Bediener und der »Streckenzentrale« der Systeme (LZB-Zentrale bzw. RBC) über ein separates Bediensystem. Im Zusammenhang mit der Zielstellung einer einheitlichen Bedienphilosophie für integrierte Bedienungen von LST-Systemen, Dispositionssystemen und Telekommunikationsanlagen soll künftig die Bedienung des RBC über ein integriertes Bediensystem zusammen mit der Bedienung des Stellwerks erfolgen.

E DIN V 0831-103 beinhaltet bei der Ableitung von Sicherheitsanforderungen für das System »Bedienung und Anzeige« nur diejenigen Bedienungen und Anzeigen , die derzeit in einem ESTW möglich sind (s. Abschn. B.7.1 in E DIN V 0831-103). Deshalb wird im Folgenden – exemplarisch für das Einrichten temporärer Langsamfahrstellen – gezeigt, wie sich für ETCS Level 2 Sicherheitsanforderungen für Bedienung und Anzeige im RBC ableiten lassen.

5.3.2 Ableitung von Sicherheitsanforderungen entsprechend E DIN VDE V 0831-103

Temporäre Langsamfahrstellen erfassen und übertragen

Schutzziel:

- gewährleisten, dass Eingaben, Änderungen oder Löschungen von Temporären Langsamfahrstellen nur wirksam werden, wenn das entsprechende Eingabekommando vom Fahrdienstleiter eingegeben und freigegeben wurde
- gewährleisten, dass Langsamfahrstellen korrekt entsprechend der Eingabe wirksam werden
- gewährleisten, dass Langsamfahrstellen-Eingaben nur einmalig im unmittelbaren zeitlichen Zusammenhang mit der Bedienhandlung wirksam werden

Randbedingungen:

- Temporäre Langsamfahrstellen dienen der sicheren Betriebsführung in Sondersituationen (Baustellen etc.). Die permanenten Geschwindigkeitsvorgaben werden der Streckeneinrichtung der Zugsicherung auf andere Weise mitgeteilt (Projektierung).
- Die vorliegende Ableitung von Sicherheitszielen bezieht sich nur auf die Erfassung und Übertragung von Temporären Langsamfahrstellen. Es wird davon ausgegangen, dass die Temporären Langsamfahrstellen nach Bestätigung durch den Bediener im Zugsicherungssystem sicher verwaltet werden.
- Es wird davon ausgegangen, dass vor erstmaliger Fahrtfreigabe auf einen Bereich mit Temporären Langsamfahrstellen durch den für die Fahrtfreigabe Verantwortlichen geprüft wird, ob die erforderlichen Temporären Langsamfahrstellen im System registriert sind.
- Dabei wird angenommen, dass eine TSR-Eingabe nur dann als wirksam angezeigt wird, wenn sie auch wirksam geworden ist.
- Temporäre Langsamfahrstellen werden erst beim nächsten folgenden Zug aktiv, d.h. es kommt in keinem Fall zu Zwangsbremsungen.
- Bezüglich der Eingabe Temporärer Langsamfahrstellen bei ETCS wird davon ausgegangen, dass es zulässig ist, externe Barrieren zu berücksichtigen, soweit sie allgemeiner Natur sind und keine spezifischen SACs abgeleitet werden.

Ausfallarten der Funktion:

a) »Temporäre Langsamfahrstelle erfassen und übertragen« wird mit verfälschter Funktion wirksam (inkl. Änderung, Löschung)

b) »Temporäre Langsamfahrstelle erfassen und übertragen« wird zur Unzeit wirksam (inkl. Änderung, Löschung)

c) »Temporäre Langsamfahrstelle erfassen und übertragen« wird nicht wirksam

Auswirkungen einschließlich ggf. auslösender Bedingungen:

a1) Ohne weitere Einschränkung der Randbedingungen muss davon ausgegangen werden, dass eine unerkannt fehlerhaft eingegebene Temporäre Langsamfahrstelle unmittelbar gefährlich auswirken kann, wenn die Änderung weniger restriktiv ist. Als Folgen hieraus kann sich im Worst Case die Entgleisung eines Reisezuges durch überhöhte Geschwindigkeit im oberen Geschwindigkeitsbereich ergeben (= **Unfallklasse G**).

a2) Wie a1), jedoch bei Regionalstrecken (= **Unfallklasse E**, da in diesem Fall von mittlerer Geschwindigkeit des betroffenen Zuges ausgegangen werden darf).

b1) Wie a1)

b2) Wie a2)

c1) Wie a1)

c2) Wie a2)

Schutzobjekt:

a), b), c) Reisende, Mitarbeiter, Fahrzeuge, Ladung

Bewertung von Barrieren:

a1) Die Notwendigkeit zum Ausführen einer Eingabe, Löschung oder Änderung einer temporären Langsamfahrstelle ergibt sich nur in Sondersituationen und ist somit ein *öfter, aber nicht ständig auftretendes* Ereignis (öftere Exposition eines Zuges mit Änderungen oder Löschungen von Langsamfahrstellen). Es kann von einer mittleren Risikoreduktion ausgegangen werden. Bei Anwendung von Tabelle 9 aus E DIN VDE V 0831-103 ergibt sich hieraus konservativ die Punktzahl 2 (eine von 10 Betriebsstunden).

Bei fälschlichen Änderungen an bereits eingegebenen Temporären Langsamfahrstellen tritt eine Gefährdung nur auf, wenn die Geschwindigkeit am relevanten Ort weniger restriktiv vorliegt als erforderlich. Eine zu wenig restriktiv oder nicht vorliegende Temporäre Langsamfahrstelle führt nicht zwangsläufig zu einem Unfall, da bei temporären Langsamfahrstellen häufig ein weiteres Ereignis hinzukommen muss, um einen Unfall auszulösen (z.B. im Baustellenbereich ein unvorsichtiges Verhalten von Arbeitern). Es kann von einer geringen Risikoreduktion ausgegangen werden. Dies trifft nicht zu in Fällen, in denen eine zu hohe Geschwindigkeit direkt zur Gefährdung der Zugfahrt führt (z.B. bei einer Temporären Langsamfahrstelle wegen Schienenbruchs). Da beide Barrieren nicht in allen Fällen wirksam sind, werden sie kombiniert betrachtet. Aus der Abschätzung, dass wenigstens eine von beiden in 1 von 2 Fällen wirksam sind, ergibt sich bei Anwendung von Tabelle 9 aus E DIN VDE V 0831-103 Punktzahl 1.

Es kann davon ausgegangen werden, dass Triebfahrzeugführer über temporäre Langsamfahrstellen in vielen Fällen noch auf anderen Wegen informiert werden. Somit kann zumindest von einer geringen Risikoreduktion ausgegangen werden und es ergibt sich die Punktzahl 1 (Tabelle 5 in E DIN VDE V 0831-103, wissensbasiert, gute Bedingungen, Stress). Dies gilt nicht für Temporäre Langsamfahrstellen mit Geschwindigkeiten über 160 km/h, für die es keine weiteren Informationswege gibt. Alternativ kann für diese aber angenommen werden, dass

sie im Regelfall innerhalb der Sicherheitsreserven des Systems Bahn liegen (jedenfalls bei Streckenhöchstgeschwindigkeiten bis 250 km/h). Es kann bei Anwendung von Tabelle 9 aus E DIN VDE V 0831-103 konservativ von einer geringen Risikoreduktion ausgegangen werden, womit sich auch hier die Punktzahl 1 ergibt. Insgesamt resultiert für alle Geschwindigkeitsbereiche die Punktzahl 1.

Der für die Fahrtfreigabe im Bereich der Temporären Langsamfahrstelle Verantwortlichekann eine fehlerhaft ausgeführte Eingabe einer Temporären Langsamfahrstelle in der Regel an der rückgemeldeten Statusinformation erkennen und die Fahrtfreigabe auf den zu sichernden Bereich verhindern (das beinhaltet nicht die unmittelbare Eingabeprüfung, diese wäre ggf. als zusätzliche Barriere oder innerhalb der Bewertung des Eingabeverfahrens selber anzusetzen). Es wird konservativ von einer regelbasierten Handlung unter guten Arbeitsbedingungen, aber nicht optimalem Stressniveau ausgegangen, da es je nach konkreter Situation auch zu Unterforderung durch seltene Nutzung der Funktion kommen kann, oder zur Überforderung in Notfallsituationen, die Temporäre Langsamfahrstellen erfordern. Nach Tabelle 5 aus E DIN VDE V 0831-103 ergibt sich hieraus die Punktzahl 3. Da eine Abhängigkeit zwischen Eingabe und Prüfung nicht vollständig ausgeschlossen werden kann (CCF), wird konservativ die Punktzahl 2 angesetzt.

Insgesamt ergibt sich somit die **Punktzahl 6**.

a2) Wie a1) **Punktzahl 6**

b1) Wie bei a1) ohne die letztgenannte Barriere (Überprüfung durch Bediener): **Punktzahl 4**

b2) Wie b1): **Punktzahl 4**

c1) Wie a1), jedoch ohne die Barriere, dass nur weniger restriktive Änderungen gefährlich werden: **Punktzahl 5**

c2) Wie c1): **Punktzahl 5**

Darstellung der RSM:

Tabelle 5 stellt die entsprechende RSM dar.

Sicherheits-anforderung 1/h	Risk Score Matrix						
Keine							
10^{-5}							
3×10^{-6}							
10^{-6}							
3×10^{-7}							
10^{-7}							
3×10^{-8}							
10^{-8}				a2)	b2) c2)		
3×10^{-9}							
10^{-9}						a1)	b1) c1)
	A	B	C	D	E	F	G
	Unfallklasse						

Tabelle 5: RSM für »Temporäre Langsamfahrstellen erfassen und übertragen «

Sicherheitsanforderung:

1×10^{-6}/h (für Ausfallart »Temporäre Langsamfahrstelle erfassen und übertragen« wird mit verfälschter Funktion wirksam (inkl. Änderung, Löschung) – allgemein)

1×10^{-5}/h (für Ausfallart »Temporäre Langsamfahrstelle erfassen und übertragen« wird mit verfälschter Funktion wirksam (inkl. Änderung, Löschung) – bei Regionalstrecken)

1×10^{-7}/h (für Ausfallart »Temporäre Langsamfahrstelle erfassen und übertragen« wird zur Unzeit wirksam (inkl. Änderung, Löschung) – allgemein)

1×10^{-6}/h (für Ausfallart »Temporäre Langsamfahrstelle erfassen und übertragen« wird zur Unzeit wirksam (inkl. Änderung, Löschung) – bei Regionalstrecken)

3×10^{-7}/h (für Ausfallart »Temporäre Langsamfahrstelle erfassen und übertragen« wird nicht wirksam – allgemein)

3×10^{-6}/h (für Ausfallart »Temporäre Langsamfahrstelle erfassen und übertragen« wird nicht wirksam – bei Regionalstrecken)

Temporäre Langsamfahrstellen anzeigen

Schutzziel:

– gewährleisten, dass betriebliche Maßnahmen nur eingeleitet werden, wenn die für die betrieblichen Maßnahmen erforderlichen temporären Langsamfahrstellen in der Zugsicherungseinrichtung umgesetzt sind

Randbedingungen:

– betriebliche Maßnahmen, die Temporäre Langsamfahrstellen erfordern, werden ohne gesonderte Buchführung über die Eingabe und Löschung von Langsamfahrstellen aufgrund der Anzeige von Temporäre Langsamfahrstellen im Meldebild eingeleitet

– vor Einleitung der betrieblichen Maßnahmen überzeugt sich der Bediener, dass die angezeigten Temporären Langsamfahrstellen den erforderlichen in Position und Geschwindigkeit entsprechen

Ausfallarten der Funktion:

a) Es wird eine Temporäre Langsamfahrstelle angezeigt, obwohl im System keine hinterlegt ist, oder sie wird mit falscher Position oder Geschwindigkeit angezeigt.

Auswirkungen einschließlich ggf. auslösender Bedingungen:

a1) Die Auswirkung einer versehentlich angezeigten, aber nicht vorhandenen Temporären Langsamfahrstelle entspricht der einer versehentlich unerkannt gelöschten Temporären Langsamfahrstelle aus »Temporäre Langsamfahrstellen erfassen und übertragen«. Gleiche Auswirkungen kann auch eine mit falscher Position oder Geschwindigkeit angezeigte Temporäre Langsamfahrstelle haben. Damit wird auch hier konservativ von **Unfallklasse G** ausgegangen.

a2) Wie a1) bei Regionalstrecken (= **Unfallklasse E**, da in diesem Fall von einer mittleren Geschwindigkeit des betroffenen Zuges ausgegangen werden darf).

Schutzobjekt:

a) Reisende, Mitarbeiter, Fahrzeuge, Ladung

Bewertung von Barrieren:

a1) Eine fälschlich oder falsch angezeigte Temporäre Langsamfahrstelle entspricht bei Auswertung des Meldebildes im Worst Case einer unerkannt gelöschten Temporären Langsamfahrstelle aus »Temporäre Langsamfahrstellen erfassen und übertragen«, jedoch ohne die dort letztgenannte Barriere (Überprüfung der Temporären Langsamfahrstelle durch den Bediener: hierfür ist die vorliegende Funktion Voraussetzung, weshalb diese Barriere nicht angesetzt werden kann). Aus den ansetzbaren Barrieren aus a1) bei »Temporäre Langsamfahrstellen erfassen und übertragen« ergibt sich die Punktzahl 4.

Hinzu kommt noch, dass die fälschlich oder falsch angezeigte Temporäre Langsamfahrstelle in Position und Geschwindigkeit genau der für die betrieblichen Maßnahmen erforderlichen Temporären Langsamfahrstelle entsprechen muss, um zu einer Gefährdung zu führen. Für die resultierende Risikoreduktion wird von einer mittleren Wirksamkeit ausgegangen. Hieraus ergibt sich bei Anwendung der Tabelle 9 aus E DIN VDE V 0831-103 die Punktzahl 2.

Insgesamt ergibt sich somit die **Punktzahl 6**.

a2) Wie a1): **Punktzahl 6**

Darstellung der RSM:

Tabelle 6 stellt die entsprechende RSM dar.

Sicherheits-anforderung 1/h	Risk Score Matrix						
Keine							
10^{-5}							
3×10^{-6}							
10^{-6}							
3×10^{-7}							
10^{-7}							
3×10^{-8}							
10^{-8}						a2)	
3×10^{-9}							
10^{-9}							a1)
	A	**B**	**C**	**D**	**E**	**F**	**G**
	Unfallklasse						

Tabelle 6: RSM für »Temporäre Langsamfahrstellen anzeigen «

Sicherheitsanforderung:

1×10^{-6}/h (allgemein)

1×10^{-5}/h (bei Regionalstrecken)

5.4 Kransicherung

5.4.1 Systemdefinition

Für ein neues Betriebsprogramm in Terminals des Kombinierten Verkehrs (KV) ist es erforderlich, dass parallel zu Kranungen in den nicht betroffenen Gleisen Ein- und Ausfahrten von Zügen erfolgen können. Hierdurch werden Stillstandszeiten gegenüber herkömmlichen Umschlaganlagen, bei denen der Kranbetrieb während der Ein- und Ausfahrt von Zügen eingestellt wird, deutlich minimiert. Es muss sichergestellt werden, dass der für eine Zugfahrt freizuhaltende Lichtraum nicht durch Kranungen verletzt wird. Schutzziel hierbei ist, eine Kollision zwischen Zug und Kran / kranenden Lasten zu verhindern. Dies soll durch eine technische Abhängigkeit zwischen den Krananlagen und der LST in Form des neuen Systems »Kransicherung« gewährleistet werden. Weitere Randbedingungen sind:

- Es ist vor Zulassen einer Zugfahrt zu prüfen, dass sich keine Teile der Krananlage oder Ladungen im Lichtraum befinden.
- Über das Freisein des Lichtraumes erfolgt eine Meldung an die LST.
- Mit Abgabe der Meldung ist sicherzustellen, dass Bewegungen der Krananlage (einschließlich ggf. aufgenommener Lasten größter anzunehmender Abmessungen) in das / die betroffene(n) Gleis(e) nicht mehr möglich sind.
- Während der Zugfahrten müssen die nicht von diesen Fahrten betroffenen Gleise und die Sortieranlage mittels Kran bedienbar sein.
- Eine Gefährdung von Zugfahrten durch Pendeln der Last wird durch (veränderten) mechanischen Aufbau der Krananlagen ausgeschlossen.
- Fahrgeschwindigkeit der Züge: 60 km/h

Eine schematische Darstellung enthält *Abbildung 4*.

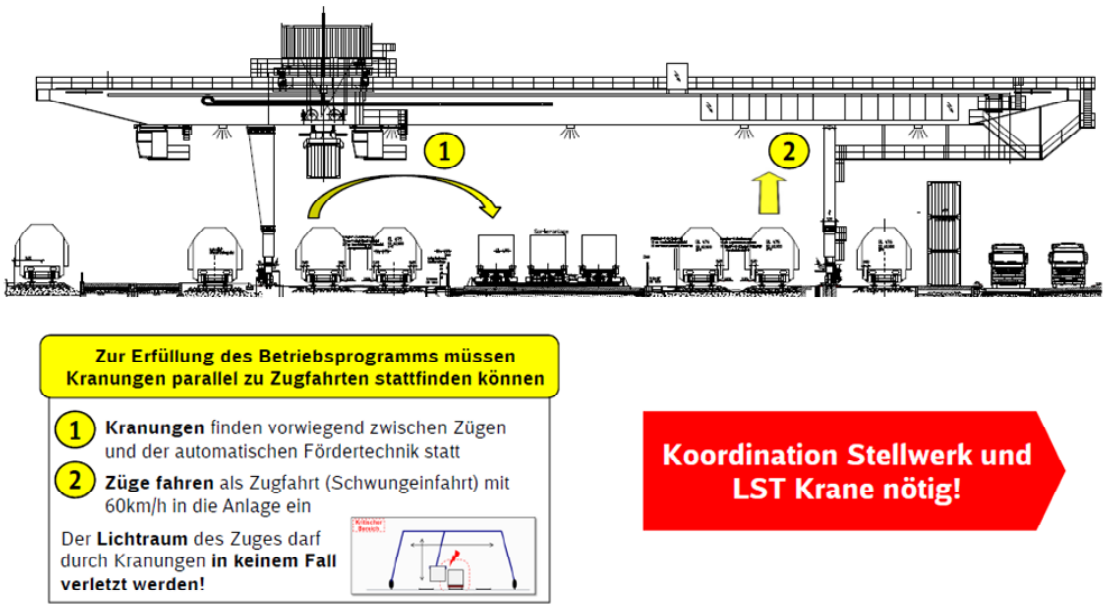

Abbildung 4: Neues Betriebsprogramm für KV-Terminal

5.4.2 Ableitung von Sicherheitsanforderungen entsprechend E DIN VDE V 0831-103

Schutzziel:

– prüfen, dass sich keine Teile der Krananlage oder Teile von Ladungen im Lichtraum befinden

– gewährleisten, dass während der Zugfahrten die Kranbewegungen für das jeweilige Start- oder Zielgleis gesperrt sind.

Randbedingungen:

keine

Ausfallarten der Funktion:

a) Hindernis im Lichtraum wird nicht erkannt

b) Kranbewegung nicht gesperrt oder Sperrung vorzeitig aufgehoben

Auswirkungen einschließlich ggf. auslösender Bedingungen:

a) Das Ereignis stellt einen Aufprall dar (= Unfallklasse B); als konservative Annahme wird jedoch **Unfallklasse D** (entsprechend eines Zusammenstoßes zwischen Güterzügen) angenommen, da die Auswirkungen beim anzunehmenden Aufprall auf Container oder Wechselauflieger vergleichbar mit einem Zusammenstoß sind.

b) Wie a)

Schutzobjekt:

a) und b) Mitarbeiter, Fahrzeuge, Ladung

Bewertung von Barrieren:

a) Der Triebfahrzeugführer kann ggf. auf Grund der niedrigen Geschwindigkeit ein im Lichtraum befindliches Hindernis erkennen. Andererseits wird er auf das Freisein des Fahrweges vertrauen und kann auf Grund der in Umschlaganlagen herrschenden Sichtverhältnisse auch nicht in jedem Fall rechtzeitig erkennen, ob sich ein Hindernis noch im Fahrweg oder ggf. bereits im benachbarten Bereich befindet. Als konservative Annahme wird daher hierfür keine Risikoreduktion angenommen.

   Der Kranführer darf Kranbewegungen in für Zugfahrten benötigten Gleisen nicht durchführen. Während er bei Senkbewegungen relativ einfach erkennen kann, welcher Bereich betroffen ist, gilt dies für Dreh- und Schwenkbewegungen nicht ohne Weiteres. Insofern muss hier konservativ von einer regelbasierten Handlung bei eher schlechten Bedingungen (Sichtverhältnisse) und unter Stress (Kranungen müssen auch bei Zugein- / - ausfahrten erfolgen, um die Umschlagkapazität zu gewährleisten) ausgegangen werden. Insofern ergibt sich die **Punktzahl 2**.

b) Wie a) – **Punktzahl 2**. Als konservative Annahme wird hierbei davon ausgegangen, dass der betroffene Bereich noch nicht von einer Zugfahrt besetzt ist, da ansonsten der Kranführer die Fahrzeuge des einfahrenden Zuges erkennen und entsprechend reagieren kann.

Darstellung der RSM:

Tabelle 7 stellt die entsprechende RSM dar.

Sicherheits-anforderung 1/h	Risk Score Matrix						
keine							
10^{-5}							
3×10^{-6}							
10^{-6}							
3×10^{-7}				a), b)			
10^{-7}							
3×10^{-8}							
10^{-8}							
3×10^{-9}							
10^{-9}							
	A	B	C	D	E	F	G
	Unfallklasse						

Tabelle 7: RSM für »Kransicherung«

Sicherheitsanforderung:

3×10^{-6}/h

5.5 Schlussfolgerungen

Anhand der Beispiele lässt sich zeigen, dass sich mit der Methodik nach E DIN VDE V 0831-103 grundsätzlich auch andere sicherheitsbezogene Funktionen analysieren lassen und hierfür Sicherheitsanforderungen abgeleitet werden können. Nach Ansicht der Arbeitsgruppe erscheinen hierbei – in Verbindung mit der ohnehin erforderlichen nachvollziehbaren Begründung für die Wahl der jeweiligen Parameter – die abgeleiteten Sicherheitsanforderungen ausreichend plausibel in Bezug auf Erfahrungen mit der Realisierung vergleichbarer technischer Systeme und daraus folgenden erreichbaren Sicherheitskennwerten. Dies zeigt damit, dass sowohl die Konstruktion der Methode als auch die gewählte Vorgehensweise für die Kalibrierung auf Basis von RAC-TS grundsätzlich dafür geeignet ist, die Anforderungen an semi-quantitative Methoden zu erfüllen und Nachteile, die sich teilweise bei anderen Methoden gezeigt haben, zu vermeiden.

6 Analyse der Systematik der RSM

6.1 Aufbau

Bei der Konstruktion der RSM nach E DIN VDE V 0831-103 fällt auf, dass bezüglich der »Risikoakzeptanz«, d.h. den Schnittpunkten zwischen Unfallklassen und Sicherheitsanforderungen, eine ungleichmäßige Abstufung besteht. Dies ist der Tatsache geschuldet, dass die Abstufung der Unfallklassen feiner ist als die Abstufung von Anforderungen aus dem (weiterentwickelten) Kriterium RAC-TS nach [7], da hierbei die Auswirkungen von Unfällen teilweise zusammengefasst sind (entsprechend den Unfallklassen C/D bzw. D/E) und außerdem hierbei eine Unterscheidung zwischen »viele« und »mehrere« nicht vorgenommen wurde.

Im »Idealfall« müsste diese Abstufung diagonal durch die Tabelle verlaufen. Dass dies nicht möglich ist, ergibt sich jedoch bereits aus der Tatsache, dass ausgehend von Unfallklasse G als »kritischste Klasse« (wobei davon ausgegangen wird, dass diese Klasse den Ausgangspunkt der Kalibrierung darstellt und somit unverändert bleiben muss) in der Matrix 9 weitere Zeilen aber nur 6 weitere Spalten zur Verfügung stehen. Somit sind »Sprünge« in der Abstufung zwangsläufig zu akzeptieren, da bei einer Veränderung der Matrix durch Zusammenfassung bestehender Klassen ggf. Anforderung A3 aus DIN V VDE V 0831-101 (Granularität) nicht mehr erfüllt werden könnte.

6.2 Wertebereiche und Grenzen

Bereits in [4] wird darauf hingewiesen, dass – ausgehend vom ersten Vorschlag zur Weiterentwicklung von RAC-TS (s. Abschn. 2.2) – eine lebhafte Diskussion darüber geführt wurde, ob für die Kriterien besser Wertebereiche oder konkrete Werte festgelegt werden sollte. Hierbei wurde auch auf die Problematik der geforderten Präzision der Nachweisführung eingegangen. Für die Kalibrierung semi-quantitativer Methoden ist die gewählte Vorgehensweise zunächst grundsätzlich egal, da bereits als Anforderung A27 (Ermittlung von Sicherheitsanforderungen) in DIN V VDE V 0831-101 ausgesagt wird, dass in der jeweiligen Methode festzulegen ist, welche konkrete THR nachzuweisen ist, wenn in der Methode Intervalle für die Sicherheitsanforderungen ermittelt werden. Vor dem Hintergrund der mit der Festlegung harmonisierter Risikoakzeptanzkriterien beabsichtigten gegenseitigen Anerkennung wäre aber zumindest ein direkter Hinweis bei den Risikoakzeptanzkriterien zum erforderlichen Nachweis hilfreich. Sofern hierzu keine Aussage getroffen ist, erscheint im Zusammenhang mit einem möglicherweise abzuleitenden Rechtsanspruch zur gegenseitigen Anerkennung nur zielführend, hierbei die jeweils obere Grenze (geringste Anforderung aus dem Wertebereich) zu akzeptieren – auch wenn die derzeitige Praxis in vergleichbaren Fällen eine andere Vorgehensweise gängig erscheinen lässt. In diesem Sinne wurden auch in E DIN VDE V 0831-103 die »Kalibrierungspunkte« festgelegt.

Weiterhin gilt für die Kalibrierung semi-quantitativer Methoden zu beachten, dass der auf den ersten Blick vernachlässigbar erscheinende Unterschied, ob ein Wertebereich mit »kleiner« oder »kleiner gleich« begrenzt wird, wesentlichen Einfluss auf die Festlegung von Klassen hat. Bei Verwendung von »kleiner« muss demnach immer die nächste Klasse, bei der dieses Kriterium erfüllt ist, gewählt werden, was in Abhängigkeit von der Granularität zu erheblichen Sprüngen führen kann und teilweise auch die Erfüllung der Anforderung A26 aus DIN V VDE V 0831-101 (Sensitivität) erschwert. Zum Umgehen potenzieller Schwierigkeiten wurden in der RSM nach E DIN VDE V 0831-103 für die Sicherheitsanforderungen konkrete Werte und keine Wertebereiche festgelegt.

6.3 Unfallklassen

In E DIN VDE V 0831-103 ist die Zahl der Unfallklassen zwangsläufig dadurch vorgegeben, dass die höchste (»kritischste«) Unfallklasse anhand des Kriteriums RAC-TS in der derzeit gültigen Fassung

der CSM VO kalibriert ist und eine Abstufung der Unfallklassen entsprechend der Bandbreite für die Sicherheitsanforderungen gewählt wurde. Eine Zusammenfassung von Unfallklassen erscheint daher für semi-quantitative Methoden nur dann zweckmäßig, wenn auch die Klassen für die Sicherheitsanforderungen zusammengefasst werden. Da üblicherweise (s. die einschlägigen Normen) hierfür vier Klassen gebildet werden, sollten jedoch auch mindestens vier Unfallklassen gebildet werden.

6.4 Beziehung zu DIN EN 50129

Tabelle A.1 der DIN EN 50129 (SIL-Tabelle) enthält vier Wertebereiche für Sicherheitsanforderungen. Die Matrix sollte daher kompatibel hierzu sein, d.h. den gesamten Wertebereich abdecken – jedoch gleichzeitig auch nicht darüber hinausgehen. Dies wird in der RSM nach E DIN VDE V 0831-103 beispielsweise dadurch erreicht, dass die Sicherheitsanforderung 10^{-9}/h die letzte Klasse bildet, obwohl bei strenger Auslegung des als Kalibrierung gewählten Kriteriums RAC-TS, welches den Wertebereich mit **≤** 10^{-9}/h abgrenzt, noch eine weitere Klasse folgen müsste. Ein Verzicht hierauf ist jedoch auch deshalb sinnvoll, da ansonsten die Grenze dieser (neuen) Klasse nicht klar wäre.

Anmerkung: Es muss jedoch auch darauf hingewiesen werden, dass die DIN EN 50129 davon ausgeht, dass es grundsätzlich auch denkbar ist, dass an eine Funktion eine strengere quantitative Anforderung als 10^{-9}/h gestellt wird, da unterhalb von Tabelle A.1 entsprechende Hinweise zum Umgang mit dieser Situation gegeben werden. Insofern kann auch der Bereich ≤ 10^{-9}/h als kompatibel zu den Klassen der DIN EN 50129 angesehen werden – nicht jedoch, falls explizit ein kleinerer Wert vorgegeben würde.

6.5 Konservativität

Anforderung A2 in DIN V VDE V 0831-101 fordert, dass die Konstruktion semi-quantitativer Methoden im Grundsatz konservativ sein muss. Dies ist in E DIN VDE V 0831-103 insofern berücksichtigt, dass der ursprüngliche Vorschlag zur Weiterentwicklung des Kriteriums RAC-TS für die Kalibrierung verwendet wurde und dieser Vorschlag im Verlauf der Diskussionen von einigen Beteiligten als zu konservativ angesehen wurde. Daher soll im Folgenden auch betrachtet werden, welche denkbaren Varianten der RSM zu weniger konservativeren Anforderungen führen.

7 Möglichkeiten zur Weiterentwicklung der RSM

Ausgehend von der Analyse in Abschn. 6 soll in diesem Abschnitt untersucht werden, welche grundsätzlichen Möglichkeiten zur Weiterentwicklung der RSM denkbar sind, in denen die Anforderungen aus Abschn. 6 ggf. besser erfüllt werden können.

7.1 Variante 1

Abbildung 5 zeigt eine veränderte RSM im Vergleich zu den Wertebereichen nach Tabelle A.1 der DIN EN 50129.

Sicherheits-anforderung 1/h	Risk Score Matrix						
keine							
10^{-5}							
3×10^{-6}							
10^{-6}							
3×10^{-7}							
10^{-7}							
3×10^{-8}							
10^{-8}							
3×10^{-9}							
10^{-9}							
	A	B	C	D	E	F	G
	Unfallklasse						
THR/h		$<10^{-5}$	$<10^{-6}$	$<10^{-6}$	$<10^{-7}$	$<10^{-7}$	$<10^{-8}$
SIL		SIL 1	SIL 2	SIL 2	SIL 3	SIL 3	SIL 4

Abbildung 5: RSM und Wertebereiche nach DIN EN 50129

Hierbei zeigt sich, dass in drei Fällen Alternativen bestehen: in den Spalten mit gelb markierten Zellen erfüllen sowohl diese Zellen als auch die jeweils darunter liegenden (weißen) Zellen die Vorgabe (Wert entsprechend des Wertes für die THR nach DIN EN 50129). Im Sinne einer konservativen Konstruktion der Methode entsprechend Anforderung A2 aus DIN V VDE V 0831-101 wären in den betreffenden Unfallklassen jeweils die strengeren Anforderungen zu wählen. Für die Unfallklasse F erscheint dies in jedem Fall zweckmäßig, da ansonsten ein zu großer Sprung zur nächsten Unfallklasse entsteht. Für Unfallklasse D ergibt sich damit jedoch eine höhere Anforderung.

Darüber hinaus ergibt sich für Unfallklasse B eine höhere Anforderung auf Grund der Abgrenzung des Wertebereiches in DIN EN 50129 (< 10^{-5}). Für Unfallklasse E ergibt sich eine geringere Sicherheitsanforderung.

Ein Vorteil dieser Variante wäre, dass keine Unterscheidung zwischen der Sicherheitsanforderung 10^{-5}/h und keiner Sicherheitsanforderung notwendig wäre, die beide keine Entsprechung in Tabelle A.1 der DIN EN 50129 haben.

7.2 Variante 2

Die Erfüllung der Anforderung »möglichst gleichmäßige Abstufung« ist z.B. durch eine Variante entsprechend Abbildung 6 möglich.

Sicherheits-anforderung 1/h	Risk Score Matrix						
keine							
10^{-5}							
3×10^{-6}							
10^{-6}							
3×10^{-7}							
10^{-7}							
3×10^{-8}							
10^{-8}							
3×10^{-9}							
10^{-9}							
	A	B	C	D	E	F	G
	Unfallklasse						

Abbildung 6: RSM mit gleichmäßiger Abstufung

Diese Variante enthält zwar Sprünge zwischen den Klassen, ist jedoch insgesamt gleichmäßig abgestuft. Außerdem sind alle Wertebereiche aus DIN EN 50129 (einschließlich »SIL 0«) berücksichtigt. Es ergeben sich in keiner Unfallklasse höhere Anforderungen als in der Version nach E DIN VDE V 0831-103.

7.3 Variante 3

Zu Vergleichszwecken werden nachfolgend auch die aus Variante 2 abgeleiteten Versionen einer RSM mit weniger konservativeren Anforderungen (s. Abbildung 7) bzw. konservativeren Anforderungen (s. Abbildung 8) mit dargestellt.

Sicherheits-anforderung 1/h	Risk Score Matrix						
keine							
10^{-5}							
3×10^{-6}							
10^{-6}							
3×10^{-7}							
10^{-7}							
3×10^{-8}							
10^{-8}							
3×10^{-9}							
10^{-9}							
	A	B	C	D	E	F	G
	Unfallklasse						

Abbildung 7: RSM mit weniger konservativer Konstruktion

Nachteil dieser Variante ist vor Allem der relativ große Sprung zwischen den Anforderungen für Unfallklasse E und Unfallfallklasse G. Im Sinne vor Anforderung A2 aus DIN V VDE V 0831-101 ist diese Variante daher eher nicht empfehlenswert. Außerdem ergibt sich keine gleichmäßige Abstufung mehr.

7.4 Variante 4

In Abbildung 8 ist auch die konservativere aus Variante 2 abgeleitete RSM dargestellt.

Sicherheits-anforderung 1/h	Risk Score Matrix						
keine							
10^{-5}							
3×10^{-6}							
10^{-6}							
3×10^{-7}							
10^{-7}							
3×10^{-8}							
10^{-8}							
3×10^{-9}							
10^{-9}							
	A	B	C	D	E	F	G
	Unfallklasse						

Abbildung 8: RSM mit konservativerer Konstruktion

Auch hier ergibt sich keine gleichmäßige Abstufung.

8 Bewertung der Vorschläge zur Weiterentwicklung des Kriteriums RAC-TS

8.1 Zielstellung

In diesem Abschnitt soll – auf Basis der RSM nach E DIN VDE V 0831-103 – analysiert werden, wie sich die verschiedenen Vorschläge zur Weiterentwicklung des Kriteriums RAC-TS (s. Abschn. 0) möglicherweise auf die Kalibrierung der RSM auswirken. Außerdem wird untersucht, welche Auswirkungen auf Sicherheitsanforderungen zu erwarten sind. Dies erfolgt entsprechend der Aufgabenstellung für diesen Bericht auf theoretischer Basis anhand eines Vergleiches der in Anhang B in E DIN VDE V 0831-103 exemplarisch abgeleiteten Sicherheitsanforderungen mit denjenigen Sicherheitsanforderungen die sich – bei im Übrigen unverändert bleibenden Annahmen – aus einer veränderten Kalibrierung der RSM ergeben würden.

Vorangestellt werden muss hierbei, dass sich die verschiedenen Ansätze zur Weiterentwicklung des Kriteriums RAC-TS sowohl in den Wertebereichen als auch in der Klassifizierung der Auswirkungen unterscheiden, was eine »Abbildung« auf die Systematik der RSM nicht in allen Fällen einfach macht. Für die Abbildung in der RSM wird daher nachfolgend so verfahren, dass bei Wertebereichen immer der höchste Wert verwendet wird, der in den jeweiligen Bereich passt. Die möglichen Auswirkungen auf Grund der Unterscheidung zwischen »Personengruppe« oder »Einzelperson« werden zunächst nicht näher analysiert, sondern es wird davon ausgegangen, dass z.B. »Tod einer Einzelperson« dem »maßgebenden Schadensausmaß« (s. Tabelle 1) »Ein Todesfall« entspricht. In den nachfolgenden Abbildungen sind die »Referenzpunkte zur Kalibrierung« entsprechend der jeweiligen Vorschläge mit rotem Kreuz **X** markiert.

8.2 Vorschlag der CER

Die Abbildung des ursprünglichen Vorschlages der CER nach [2] in Form der RSM zeigt *Abbildung 9*.

Sicherheits-anforderung 1/h	Risk Score Matrix						
keine							
10^{-5}							
3×10^{-6}							
10^{-6}							
3×10^{-7}				X			
10^{-7}							
3×10^{-8}					X		
10^{-8}							X
3×10^{-9}							
10^{-9}							
	A	B	C	D	E	F	G
	Unfallklasse						

Abbildung 9: RSM und Vorschlag der CER

Bei diesem Vorschlag finden die Unfallklassen B und C keine Entsprechung mehr in den Sicherheitsanforderungen. Auch wenn dadurch Befürchtungen, der Vorschlag sei für Unfälle geringeren Ausmaßes geeigneter, da keine zu konservativen Anforderungen festgelegt würden, vorgebeugt wird, erscheint dies für die Kalibrierung semi-quantitativer Methoden nicht geeignet, da für Ereignisse, die sich überwiegend in Bereichen ohne Reisendenverkehr und bei niedrigen Geschwindigkeiten (z.B. insbesondere Rangierbetrieb) ereignen können, somit i.d.R. keine Sicherheitsanforderungen ergeben.

Weiterhin ist der Unterschied zwischen den Sicherheitsanforderungen, die sich für Unfallklasse E/F und G ergeben sehr gering, da eine ungünstige Abgrenzung zwischen den Kategorien vorgenommen wurde (einmal Wertebereich mit eingeschlossenen Werten an der Grenze und einmal Wertebereich mit nicht eingeschlossenem Wert an der Grenze (»kleiner als«)).

8.3 Letzter Vorschlag für 1. Revision der CSM VO

Die Abbildung des im Treffen zwischen ERA und den beteiligten Sektororganisationen vorabgestimmten Vorschlages zeigt Abbildung 10.

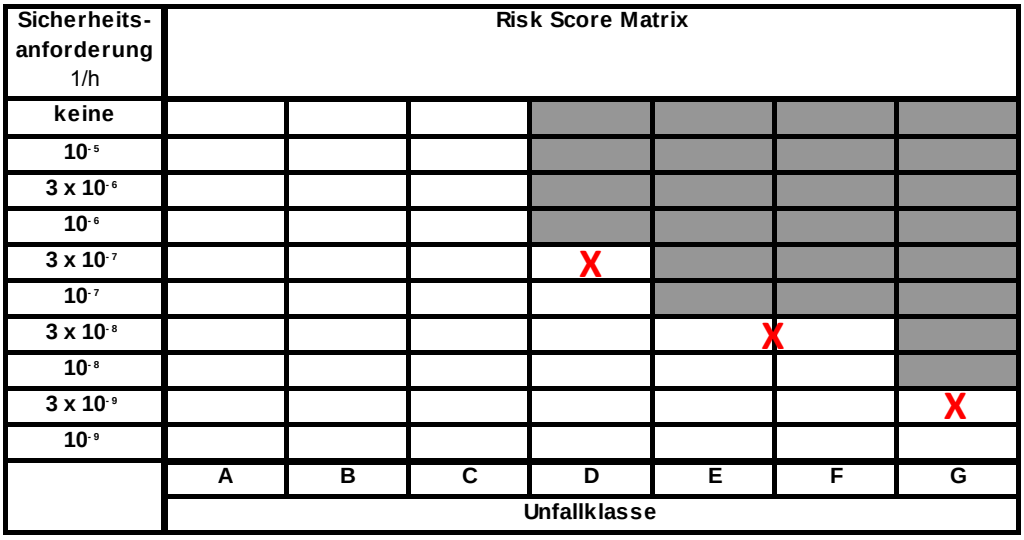

Abbildung 10: RSM und vorabgestimmter Vorschlag

Im Vergleich zum Vorschlag der CER zeigt sich nur bei Unfallklasse G ein Unterschied, da die Variante mit einem Wertebereich wieder verlassen wurde. Die übrigen Anmerkungen zum Vorschlag der CER sind auch bei diesem Vorschlag zutreffend.

8.4 Aktueller Vorschlag der ERA

Die Abbildung des aktuellen Vorschlages der ERA nach [5] in Form der RSM zeigt Abbildung 11.

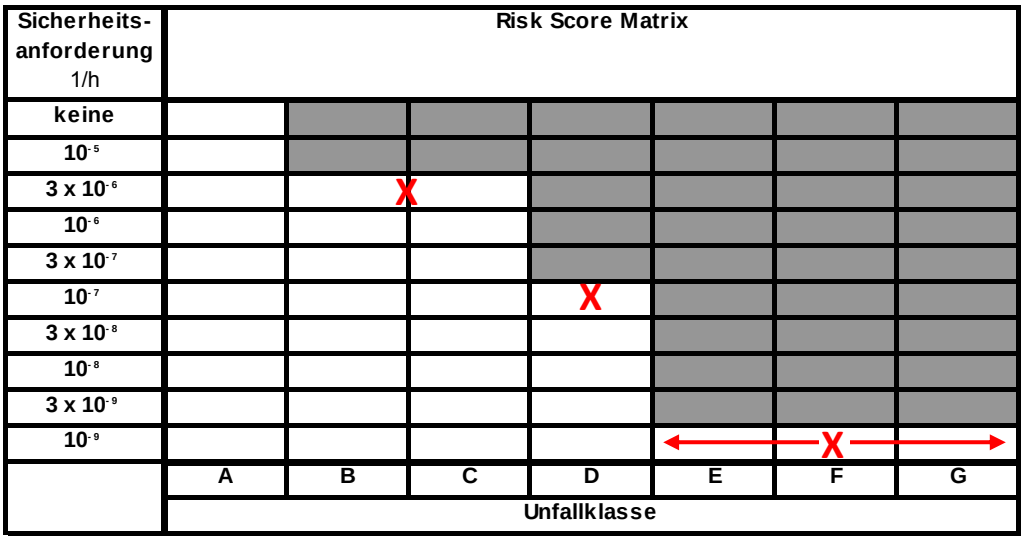

Abbildung 11: RSM und aktueller Vorschlag ERA

Es ergibt sich eine relativ grobe Abstufung, da vor Allem dadurch bedingt ist, dass nur drei Kategorien vorgeschlagen sind. Mit Ausnahme der Unfallklasse G sind die Anforderungen für alle Unfallklassen erhöht. Dies ist dadurch bedingt, das auch alle Ereignisarten, die zu Schwerverletzten führen

können, in die höchste Kategorie (hier durch den Doppelpfeil ausgedrückt) einzuordnen sind und die Unfallklasse dementsprechend zu kalibrieren ist. Für die Unfallklassen B und C ergeben sich höhere Anforderungen, da hier im Gegensatz zum ursprünglichen Vorschlag der Wertebereich mit »kleiner als« begrenzt ist und somit in der RSM die nächstniedrigere Klasse für die Sicherheitsanforderung zu wählen ist.

Problematisch erscheint bei diesem Vorschlag vor Allem die gegenüber den anderen Vorschlägen unterschiedliche Handhabung der Unterscheidung zwischen Personengruppe und Einzelperson. So ist es bereits nicht nachvollziehbar, wie ein Unfall, der eine Einzelperson betrifft zu Tod **und**/oder schwerer Verletzung dieser Person führen kann. Darüber hinaus wird in diesem Vorschlag der Ansatz der vergleichbaren Kritikalität zwischen Tod einer Einzelperson und vielen Schwerverletzten verlassen und der Tod einer Einzelperson geringer gewichtet. Im Sinne einer gleichmäßigen Klassenbreite zwischen den Unfallklassen müsste daher möglicherweise für die Unfallklasse D die gleiche Anforderung wie für die Unfallklassen E bis G gelten, sodass die Anforderungen weiter erhöht würden.

8.5 Vergleich mit Risikoakzeptanzkriterien aus der Luftfahrt

Nähere Ausführungen zu Sicherheitsanforderungen in der Luftfahrt und deren Nachweis finden sich insbesondere in dem von der EASA herausgegebenen Standard CS-25, der Anforderungen für die Zertifizierung großer Passagierflugzeuge festlegt.

In Abschn. CS 25.1309 der CS 25 wird als generelle Designregel für alle Systeme und Komponenten des Flugzeugs gefordert, dass diese für sich betrachtet und im Zusammenwirken mit anderen Systemen so beschaffen sein müssen, dass

- jeder katastrophale Fehlzustand äußerst unwahrscheinlich ist und nicht aus einem Einzelfehler resultieren kann,
- jeder gefährliche Fehlzustand äußerst selten ist und
- jeder größere Fehlzustand selten ist.

Nähere Ausführungen zu grundsätzlichen Zusammenhängen und zum Nachweis dieser Designvorgabe sind in Abschn. AMC 25.1309 der CS 25 gegeben. Hier wird zusätzlich definiert, dass

- kleinere Fehlzustände wahrscheinlich sein (d.h. auftreten) dürfen und
- für Fehlzustände, die keinen Einfluss auf die Sicherheit haben, bestehen keine Anforderungen bezüglich deren Auftretenswahrscheinlichkeit.

Für Fehlzustände ist in Abschn. AMC 25.1309 der CS 25 definiert:

- Katastrophal: Fehlzustände, die zu vielen Todesfällen führen können – üblicherweise verbunden mit einem Verlust des Flugzeuges (früher definiert mit: Fehlzustände, die einen sicheren Flug oder eine sichere Landung verhindern)
- Gefährlich: Fehlzustände, welche die Leistungsfähigkeit des Flugzeuges oder die Fähigkeit der Flugbesatzung, schwierige Betriebsbedingungen zu beherrschen, einschränken mit der Folge
  - einer großen Reduzierung von Sicherheitsmargen oder der Funktionstüchtigkeit,
  - körperlicher Beeinträchtigung oder erhöhter Arbeitsbelastung für die Flugbesatzung, sodass nicht sichergestellt ist, dass diese ihre Aufgeben richtig oder vollständig ausführt,
  - schwerer oder tödlicher Verletzung einer relativ kleinen Zahl der Insassen (außer Flugbesatzung)

- Größer: Gefährlich: Fehlzustände, welche die Leistungsfähigkeit des Flugzeuges oder die Fähigkeit des Bordpersonals, schwierige Betriebsbedingungen zu beherrschen, einschränken mit der Folge beispielsweise
  - einer signifikanten Reduzierung von Sicherheitsmargen oder der Funktionstüchtigkeit,
  - einer signifikanten Erhöhung der Arbeitsbelastung für das Bordpersonal oder von Bedingungen, welche die Leistungsfähigkeit des Bordpersonals beeinträchtigen,
  - von Komforteinschränkungen für die Flugbesatzung,
  - von körperlicher Beeinträchtigung für Passagiere oder das Kabinenpersonal bis hin zu möglichen Verletzungen.

Weiterhin wird für die Quantifizierung von Wahrscheinlichkeiten von Fehlzuständen definiert:

- Wahrscheinlich: durchschnittliche Wahrscheinlichkeit pro Flugstunde > 10^{-5}.
- Selten: durchschnittliche Wahrscheinlichkeit pro Flugstunde < 10^{-5}, jedoch > 10^{-7}.
- Äußerst selten: durchschnittliche Wahrscheinlichkeit pro Flugstunde < 10^{-7}, jedoch > 10^{-9}.
- Äußerst unwahrscheinlich: durchschnittliche Wahrscheinlichkeit pro Flugstunde ≤ 10^{-9}.

Der bildlich dargestellte Zusammenhang zwischen Sicherheitszielen und Fehlzuständen aus Abschn. AMC 25.1309 / Bild 2 ist in Abbildung 12 wiedergegeben.

Effect on Aeroplane	No effect on operational capabilities or safety	Slight reduction in functional capabilities or safety margins	Significant reduction in functional capabilities or safety margins	Large reduction in functional capabilities or safety margins	Normally with hull loss
Effect on Occupants excluding Flight Crew	Inconvenience	Physical discomfort	Physical distress, possibly including injuries	Serious or fatal injury to a small number of passengers or cabin crew	Multiple fatalities
Effect on Flight Crew	No effect on flight crew	Slight increase in workload	Physical discomfort or a significant increase in workload	Physical distress or excessive workload impairs ability to perform tasks	Fatalities or incapacitation
Allowable Qualitative Probability	No Probability Requirement	<---Probable---->	<----Remote---->	Extremely <----------> Remote	Extremely Improbable
Allowable Quantitative Probability: Average Probability per Flight Hour on the Order of:	No Probability Requirement	<----------> $<10^{-3}$ Note 1	<----------> $<10^{-5}$	<----------> $<10^{-7}$	$<10^{-9}$
Classification of Failure Conditions	No Safety Effect	<-----Minor------>	<-----Major------>	<--Hazardous-->	Catastrophic
Note 1: A numerical probability range is provided here as a reference. The applicant is not required to perform a quantitative analysis, nor substantiate by such an analysis, that this numerical criteria has been met for Minor Failure Conditions. Current transport category aeroplane products are regarded as meeting this standard simply by using current commonly-accepted industry practice.					

Abbildung 12: Zusammenhang zwischen Sicherheitszielen und Fehlzuständen nach CS-25

Zu beachten ist hierbei, dass die Wertebereiche für quantitative Wahrscheinlichkeiten abweichend vom Text mit »<« wiedergegeben sind und der Wertebereich < 10^{-3} gemäß Anmerkung nur als »Referenz« dient.

Hinweis: Eine ähnliche Begründung wie in Anmerkung 1 der vorstehenden Tabelle findet sich in E DIN VDE V 0831-103 zur Erläuterung der Vorgabe »keine Sicherheitsanforderung«:

> »Keine Sicherheitsanforderung« bedeutet an dieser Stelle, dass keine quantitative Anforderung an die Sicherheit gestellt wird. An die im Anwendungsbereich dieser Vornorm liegenden Systeme der Eisenbahnsignaltechnik werden üblicherweise hohe Zuverlässigkeitsanforderungen gestellt, da ein Ausfall dieser Systeme erhebliche Auswirkungen auf den Eisenbahnbetrieb hat. Bei Erfüllung dieser Zuverlässigkeitsanforderungen darf davon ausgegangen werden, dass auch für Systeme mit einer weniger strengen Sicherheitsanforderung als 10-5/h ein sicherheitsbezogener Ausfall hinreichend selten ist und kein Sicherheitsnachweis nach EN 50129 erforderlich ist.

In Abschn. AMC 25.1309 der CS 25 werden außerdem Hintergrundinformationen zum Zustandekommen des »Referenzwertes« 1 x 10^{-9} gegeben. Diesem liegt die Annahme zu Grunde, dass

- gemäß Auswertung von Daten aus der Vergangenheit die Wahrscheinlichkeit eines schweren Flugunfalles ungefähr 1 : 1 Million Flugstunden beträgt,

- ungefähr 10 % davon durch Fehlzustände des Flugzeugs verursacht sind,
- für neu zu bauende Flugzeuge keine höhere Wahrscheinlichkeit zulässig sein sollte,
- somit die Wahrscheinlichkeit eines durch einen solchen Fehlzustand bedingten schweren Flugunfalles nicht größer sein darf als 1×10^{-7} pro Flugstunde,
- ohne nähere Begründung angenommen wird, dass ungefähr 100 potenzielle Fehlzustände, die zu einem katastrophalen Ausfall führen können, in einem Flugzeug möglich sind,
- unter gleichmäßiger Aufteilung der zulässigen Wahrscheinlichkeit von 1×10^{-7} pro Flugstunde sich für jeden Fehlzustand eine zulässige Wahrscheinlichkeit von 1×10^{-9} pro Flugstunde ergibt.

Die in der Luftfahrt etablierten Kategorien für Sicherheitsziele sind auf den ersten Blick identisch mit dem aktuellen Vorschlag der ERA zu RAC-TS. Dies gilt jedoch nur für die Wertebereiche. Bezüglich der Auswirkungen bestehen gravierende Unterschiede. So wäre die Kategorie »Multiple fatalities« schon eher als weitere Abstufung anzusehen, die keine Entsprechung im ERA-Vorschlag findet. Außerdem wird für die Kategorie »wenige Tote« ein wesentlich geringeres Sicherheitsziel gefordert als im ERA-Vorschlag, bei dem hierfür das höchste Sicherheitsziel angesetzt werden müsste.

Weiterhin gilt zu beachten, dass die Ableitung der Sicherheitsziele in der Luftfahrt keine direkte Entsprechung im Eisenbahnwesen hat, da kein Bezug zwischen Unfalldaten und zulässigen Versagensraten hergestellt wurde – allein schon deshalb, weil es derzeit keine Begründung für eine anzunehmende Zahl von zu berücksichtigenden Funktionen gibt. Hierfür müsste zunächst eine Liste erstellt werden, welche die Funktionen auf einer geeigneten Ebene benennt (z.B. analog der Funktionsliste für LST-Anlagen in E DIN VDE V 0831-103). Problematisch hierbei könnte allerdings sein, dass diese Annahmen bei Notwendigkeit neuer Funktionen keinen Bestand mehr haben. Da sich in der Vergangenheit gezeigt hat, dass dies für Bahnanwendungen durchaus erforderlich ist, wäre insofern auch von einer derartigen Herleitung eher abzuraten. Weiterhin besteht der Unterschied dass es zum angenommen Unfallverlauf »Verlust des Flugzeuges« (d.h. i.d.R. Tod aller bzw. der überwiegenden Zahl der Insassen) aus der Luftfahrt keine direkte Entsprechung im Eisenbahnwesen gibt, da bereits Unfälle mit mehr als 10 Toten die absolute Ausnahme darstellen.

Aus dem Vergleich ergibt sich folgende Schlussfolgerung:

Das derzeitige Sicherheitsziel von 10^{-9} funktionellen Ausfällen pro Betriebsstunde in der CSM VO hat prinzipiell eine Entsprechung in der Luftfahrt – ist vor dem Hintergrund der betrachteten Auswirkungen jedoch bereits eher als konservativ anzusehen. Der aktuelle Vorschlag der ERA zur Weiterentwicklung von RAC TS ist im Vergleich zu den Sicherheitszielen in der Luftfahrt wesentlich restriktiver.

8.6 Bewertung

Ausgehend von der Analyse der Systematik der RSM nach E DIN VDE V 0831-103 in Abschn. 6 sollten Risikoakzeptanzkriterien folgende Kriterien erfüllen, um die Kalibrierung semi-quantitativer Methoden zu unterstützen:

- gleichmäßige Abstufung
- mindestens 4 Kategorien
- Abgrenzung der Wertebereiche unter Einschluss des jeweiligen Wertes (»kleiner gleich«)
- »Abdeckung« des Wertebereiches nach DIN EN 50129 bzw. Kompatibilität hierzu.

In Tabelle 8 ist zusammengestellt, inwieweit diese Anforderungen bei den einzelnen Vorschlägen erfüllt sind. Außerdem ist dargestellt, ob diese Vorschläge im Vergleich zum Vorschlag der RAC Task Force der ERA weniger konservativ sind.

Vorschlag	gleichmäßige Abstufung	Anzahl Kategorien	Abgrenzung Wertebereiche	kompatibel zu DIN EN 50129	weniger konservativ
Vorschlag RAC Task Force der ERA	-	+	+	+	n.a.
Vorschlag der CER	-	-	-	-	+
Vorschlag für Revision der CSM VO	+	-	-	-	+
aktueller Vorschlag ERA	+	-	-	+	--
RSM nach E DIN V VDE 0831-103	-	+	+	+	n.a.
RSM - Variante 1	-	++	+	++	-
RSM - Variante 2	+	++	+	++	+
RSM - Variante 3	-	++	+	+	++
RSM - Variante 4	-	++	+	+	--

Tabelle 8: Qualitative Bewertung von Vorschlägen

Erläuterung: ++ = sehr gut erfüllt, + = erfüllt, - = nicht erfüllt, -- = sehr schlecht erfüllt, n.a. = nicht anwendbar

Eine quantitative Bewertung der Auswirkungen verschiedener Vorschläge ist grundsätzlich auf Basis der in E DIN VDE V 0831-103 für die exemplarisch genannten Funktionen / Ausfälle genannten Sicherheitsanforderungen möglich. In Tabelle 9 ist daher dargestellt, für wie viele Sicherheitsanforderungen sich bei den jeweiligen Vorschlägen im Vergleich restriktivere, gleiche bzw. weniger restriktive Werte ergeben.

Vorschlag	Anzahl Werte		
	restriktiver	**gleich**	**weniger restriktiv**
Vorschlag RAC Task Force der ERA	(entspricht RSM aus E DIN VDE V 0831-103)		
Vorschlag der CER	0	31	104
Vorschlag für Revision der CSM VO	0	31	104
aktueller Vorschlag ERA	69	64	2
RSM nach E DIN V VDE 0831-103	(Referenz)		
RSM - Variante 1	23	96	16
RSM - Variante 2	0	117	18
RSM - Variante 3	0	115	20
RSM - Variante 4	32	101	2

Tabelle 9: Quantitative Bewertung von Vorschlägen

Es zeigt sich, dass der aktuelle Vorschlag der ERA zu wesentlich restriktiveren Werten führt als alle anderen Vorschläge. Gleichzeitig zeigt sich, dass die Varianten 2 und 3 in diesem Vergleich prinzipiell gleichwertig sind.

8.7 Schlussfolgerungen

Aus der qualitativen Bewertung nach Tabelle 2 ergibt sich, dass lediglich Variante 2 alle Anforderungen erfüllt und im Übrigen der Vorschlag der RAC Task Force die qualitativen Anforderungen besser erfüllt als spätere Vorschläge.

9 Aus der Analyse zu gewinnende Erkenntnisse für die Weiterentwicklung des Kriterium RAC-TS

Abgeleitet aus der Analyse in Abschnitt 8 soll in diesem Abschnitt ein Vorschlag diskutiert werden, wie auf Basis der weiterentwickelten RSM nach Variante 2 Risikoakzeptanzkriterien zu definieren wären, damit sie hierzu kompatibel sind. Es sei jedoch darauf hingewiesen, dass dies ein rein methodisch-theoretischer Vorschlag ist, der insbesondere aus den Erkenntnissen zum Zusammenhang von RAC-TS und der Kalibrierung semi-quantitativen Methoden zur Risikobewertung begründet ist.

Für den weiteren Vorschlag wird von folgenden Prämissen ausgegangen:

- Für das Kriterium RAC-TS wird eine Granularität wie in der RSM nicht benötigt bzw. ist ggf. auch nicht zweckmäßig.
- Daher wird daher davon ausgegangen, dass 4 Klassen erforderlich werden – wie im Vorschlag der RAC Task Force.

- Zweckmäßig erscheint eine – durch Beschränkung auf 4 Klassen zwangsläufig erforderliche – Zusammenfassung der Auswirkungen entsprechend den Unfallklassen C/D aus der RSM einerseits und den Unfallklassen E/F aus der RSM andererseits.
- Als höchste Anforderung bleibt »≤ 10^{-9}/h« für die höchsten zu erwartenden Auswirkungen bestehen.
- Die geringste Anforderung sollte im Bereich von 10^{-5}/h liegen, da dies eine Grenze in Tabelle A.1 der DIN EN 50129 darstellt.

In Abbildung 13 ist dargestellt, wie eine Zuordnung von Klassen für ein weiterentwickeltes Kriterium RAC-TS auf Basis der RSM nach Variante 2 aussehen könnte.

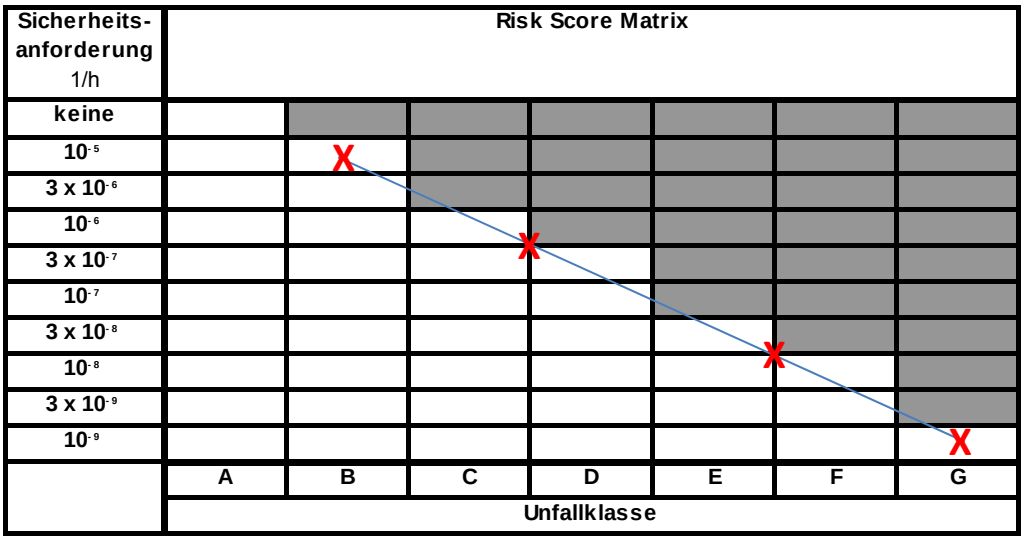

Abbildung 13: RSM und Kalibrierung für RAC-TS

Entsprechend der in Abschn. 8 gewählten Darstellung bilden die roten Kreuze auch hier die »Kalibrierungspunkte«. Die mittleren Punkte sind jeweils an der Grenze zwischen zwei Unfallklassen und zwei Klassen für die Sicherheitsanforderungen dargestellt, um zu zeigen, dass hier prinzipiell ein Wertebereich abgedeckt werden muss. Anhand der blauen Linie, welche die Verbindung zwischen den Punkten für die niedrigste und die höchste Anforderung darstellt, ist ersichtlich, dass die mittleren Punkte genau auf dieser Gerade liegen und somit das Kriterium »gleichmäßige Abstufung« erfüllt ist.

Um von dieser Darstellung zu einem Textvorschlag für die Definition eines weiterentwickelten Kriteriums RAC-TS bzw. zu einer Darstellung analog der für den Vorschlag der RAC Task Force (s. Abbildung 1) zu gelangen sind weitere Randbedingungen zu definieren:

Auf Grund der »Zusammenfassung« der Unfallklassen C/D bzw. E/F gibt es prinzipiell folgende Varianten für die Festlegung von Werten für diese beiden Bereiche:

1. oberster (d.h. weniger restriktiver) Wert, im Beispiel: 10^{-6}/h entsprechend des Wertes für Unfallklasse C und 3 x 10^{-8}/h entsprechend des Wertes für Unfallklasse E,
2. unterster (d.h. restriktiverer) Wert, im Beispiel: 3 x 10^{-7}/h entsprechend des Wertes für Unfallklasse D und 10^{-8}/h entsprechend des Wertes für Unfallklasse F,
3. Wertebereich, der beide Werte einschließt, im Beispiel: 3 x 10^{-7}/h ≤ R ≤ 10^{-6}/h und 10^{-8}/h ≤ R ≤ 3 x 10^{-8}/h; in diesem Fall schließen die Werte der Wertebereiche nicht aneinander an, wie es sonst in vergleichbaren Tabellen üblich ist (z.B. Tabelle A.1 in DIN EN 50129).

4. Wertebereich, der erst an der Grenze (d.h. unter Ausschluss des jeweiligen Wertes) zur nächsten Klasse endet, im Beispiel: 3×10^{-8}/h < R ≤ 10^{-6}/h und 10^{-9}/h < R ≤ 3×10^{-8}/h.

Bezüglich der Wertebereiche gelten die Ausführungen in Abschn. 6.2. Für die dort angesprochene wünschenswerte Festlegung, welcher Wert konkret nachzuweisen ist (analog Anforderung A27 in DIN V VDE V 0831-101) gelten folgende Überlegungen:

Vor dem Hintergrund einer gegenseitigen Anerkennung müssten immer die restriktivsten Werte für den Nachweis vorgeschrieben werden, da es dann für den Fall, dass diese Anerkennung nicht angestrebt wird, immer noch möglich ist, in den einzelnen Mitgliedsstaaten andere Werte, die innerhalb dieses Bereiches liegen, zu verwenden. Würde der weniger restriktivere Wert für die gegenseitige Anerkennung akzeptiert, könnten national strengere Werte festgelegt werden, was dem Ansatz einer gegenseitigen Anerkennung zuwiderlaufen würde. Würde national wiederum hierauf verzichtet, wäre ein Wertebereich sinnlos, da diese Variante dann der Variante 2 entspricht.

Bei Variante 4 ist es im Vergleich zu Variante 3 schwieriger, einen Wert für den Nachweis festzulegen, da der restriktivste Wert im Prinzip bereits dem Wert der nächsten Klasse entspricht. Grundsätzlich möglich wäre jedoch, einen »Mittelwert« festzulegen, der innerhalb des Wertebereiches der jeweiligen Klasse liegt. Für das Beispiel wäre das dann 3×10^{-7}/h und 10^{-8}/h; diese Werte entsprechen gleichzeitig den Werten aus Variante 2.

Insgesamt erscheint Variante 3 in Verbindung mit einer zu treffenden Festlegung, welcher Wert für die gegenseitige Anerkennung nachzuweisen ist, am besten geeignet.

Unter Berücksichtigung der vorstehenden Ausführungen und unter Anlehnung an die tabellarische Darstellung der RAC Task Force (s. Abbildung 1) können die Erkenntnisse in folgender Darstellung zusammengefasst werden:

Typischerweise erwartete Auswirkungen des unerwünschten Ereignisses	**Akzeptierte Häufigkeit (R) des unerwünschten Ereignisses**
Mehrere Todesfälle	R ≤ 10^{-9}/h
Ein Todesfall und/oder mehrere Schwerverletzte	R ≤ 10^{-8}/h für gegenseitige Anerkennung, ansonsten R ≤ 3×10^{-8}/h
Ein Schwerverletzter und/oder mehrere Leichtverletzte	R ≤ 3×10^{-7}/h für gegenseitige Anerkennung, ansonsten R ≤ 10^{-6}/h
Ein Leichtverletzter	R ≤ 10^{-5}/h

Tabelle 10: Möglichkeit für weiterentwickeltes Kriterium RAC-TS

Aus der Darstellung ist ersichtlich, dass im Prinzip die Aspekte aller Varianten hierbei berücksichtigt sind. Außerdem zeigt sich, dass die seinerzeit von der RAC Task Force vorgeschlagenen Werte durchaus plausibel sind, da sie sich auch aus dieser Darstellung ergeben.

10 Zusammenfassung

In diesem Bericht wurde anhand des Beispiels der RSM aus E DIN VDE V 0831-103 gezeigt, wie sich semi-quantitative Methoden zur Risikoanalyse mittels des Kriteriums RAC-TS kalibrieren lassen, um für Funktionen technischer Systeme nachvollziehbar Sicherheitsanforderungen ableiten zu können. Insofern wird auch die Notwendigkeit einheitlicher Risikoakzeptanzkriterien für technische Systeme aus dieser Sicht bestätigt.

Weiterhin wurde ergänzend gezeigt, wie sich aus Anforderungen an semi-quantitative Methoden Erkenntnisse für die Weiterentwicklung des Kriteriums RAC-TS ableiten lassen.

11 Anhang

11.1 Referenzen

a) Rechtliche und normative Grundlagen

CSM VO	VERORDNUNG (EG) Nr. 352/2009 DER KOMMISSION vom 24. April 2009 über die Festlegung einer gemeinsamen Sicherheitsmethode für die Evaluierung und Bewertung von Risiken gemäß Artikel 6 Absatz 3 Buchstabe a der Richtlinie 2004/49/EG des Europäischen Parlaments und des Rates, Amtsblatt der Europäischen Union, L 108/4, 29.4.2009
DIN EN 13849-1	Sicherheit von Maschinen - Sicherheitsbezogene Teile von Steuerungen - Teil 1: Allgemeine Gestaltungsleitsätze, Ausgabedatum 2008-12
DIN EN 50 129	Bahnanwendungen – Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme – Sicherheitsrelevante elektronische Systeme für Signaltechnik, Ausgabedatum 2003-12
DIN EN 61508-1	Funktionale Sicherheit sicherheitsbezogener elektrischer/ elektronischer/programmierbarer elektronischer Systeme Teil 1: Allgemeine Anforderungen, Ausgabedatum 2011-02
DIN EN 61508-5	Funktionale Sicherheit sicherheitsbezogener elektrischer/ elektronischer/programmierbarer elektronischer Systeme Teil 5: Beispiele zur Ermittlung der Stufe der Sicherheitsintegrität (safety integrity level), Ausgabedatum 2011-02
E DIN VDE V 0831-103	Elektrische Bahn-Signalanlagen – Ermittlung von Sicherheitsanforderungen an technische Funktionen in der Eisenbahnsignaltechnik, Entwurf 2013-04
CS-25	Certification Specifications for Large Aeroplanes, Amendment 9 vom 05.08.2010
VDV-Schrift 332	Sicherheitsintegritätsanforderungen für Bahnsignalanlagen bei Nichtbundeseigenen Eisenbahnen (NE)

b) Weiterführende Literatur

[1] Bepperling, Sonja-Lara: Validierung eines semi-quantitativen Ansatzes zur Risikobeurteilung in der Eisenbahntechnik, Dissertation 2008

[2] CER: POSITION PAPER covering the results of the CER –UIC 'Application Exercise' concerning the RAC 'design criteria' values presented in ERA draft revision recommendation for regulation 352/2009, 15.12.2011

[3] EBA: Anforderungen des Brand- und Katastrophenschutzes an den Bau und den Betrieb von Eisenbahntunneln, Stand vom 15.08.2001.

[4] ERA Safety Unit – CSM Team: Agency report on the experience with the existing regulation (EC) No 352/2009 on a common safety method on risk evaluation and assessment an on the revision of that regulation, Version 1.0 vom 13.07.2012

[5] ERA Safety Unit, Management System Sector: Information note about ERA's plan for the way forward for the DEVELOPMENT OF EXPLICIT HARMONISED RISK ACCEPTANCE CRITERIA FOR FAILURES OF FUNCTIONS OF TECHNICAL SYSTEMS, Version 0.1 vom 16.01.2013

[6] ERA Safety Unit – RAC Task Force: Definition of RAC for failures of functions of technical systems, which are covered entirely by a technical solution, Version 3.0 vom 23.05.2011

[7] ERA Safety Unit, Safety Assessment Sector: Proposal for Risk Acceptance Criteria to be included in the Scope of the Revision of Regulation 352/2009/EC, Executive Summary, Version 2.0 vom 28.06.2011

[8] Milius, Birgit: Konstruktion eines semi-qualitativen Risikographen für das Eisenbahnwesen, Dissertation 2009

11.2 Abkürzungen

Abk.	Langform / Erläuterung
CCF	Common Cause Failure (Ausfall auf Grund einer gemeinsamen Ursache)
CER	Community of European Railway and Infrastructure Companies (Gemeinschaft der europäischen Bahnen und Infrastrukturgesellschaften)
CSM	Common Safety Method
EASA	European Aviation Safety Agency (Europäische Agentur für Flugsicherheit)
ERA	European Railway Agency
ESTW	Elektronisches Stellwerk
ETA	Ereignisbaumanalyse (Event Tree Analysis)
ETCS	European Train Control System (Europäisches Zugsteuerungs- und Zugbeeinflussungssystem)
FTA	Fault Tree Analysis (Fehlzustandsbaumanalyse)
KV	Kombinierter Verkehr
LST	Leit- und Sicherungstechnik
LZB	Linienzugbeeinflussung
MA	Bereitstellung des Fahrauftrags (Funktionalität)
RAC	Risk Acceptance Criteria (Risikoakzeptanzkriterien)
RAC-TS	Risk Acceptance Criterion for Technical Systems (Risikoakzaptanzkriterium für technische Systeme)
RBC	Radio Block Center (ETCS-Streckenzentrale)
RSM	Risk Score Matrix
RZL	Rechnergestützter Zugleitbetrieb
SAC	Safety-related Application Condition (Sicherheitsbezogene Anwendungsbedingung)
SATLOC	Satellite based operation and management of local low traffic lines
SIL	Safety Integrity Level (Sicherheitsanforderungsstufe)
TBV	Tunnelbegegnungsverbot
TC	Überwachung des Fahrauftrags (Funktionalität)
THR	Tolerable Hazard Rate (tolerierbare Gefährdungsrate)
TSI	Technische Spezifikation Interoperabilität
UIC	Union internationale des chemins de fer (Internationaler Eisenbahnverband)
UNIFE	Union des Industries Ferroviaires Européennes (Verband der europäischen Eisenbahnindustrie)
VDV	Verband Deutscher Verkehrsunternehmen