Vorgehensweise bei der Risikoanalyse Automatisches Fahren

Approach for a Risk Analysis for Automated Train Operation

Jens Braband

Das vom Deutschen Zentrum für Schienenverkehrsforschung (DZSF) beauftragte Projekt ATO-RISK hat das Ziel, „Risikoakzeptanzkriterien für das automatisierte Fahren auf der Schiene" abzuleiten, allerdings unter den folgenden, im Untersuchungsrahmen abgesteckten Randbedingungen: R1 – der Auftrag bezieht sich auf Zugfahrten im Netz der Eisenbahnen des Bundes (EdB) mit automatisierten Systemen, schwerpunktmäßig in den Automatisierungsstufen GoA 3 und GoA 4; R2 – es werden keine speziellen Lösungsarchitekturen bewertet und keine Ableitung von Sicherheitszielen für technische Komponenten durchgeführt; R3 – als Ergebnisqualität, z. B. auch der Validierung, wird angestrebt, dass quantitative Ergebnisse (z. B. Tolerierbare Gefährdungsrate, Tolerable Hazard Rate – THR) in der Größenordnung übereinstimmen oder dass zumindest die Abweichungen zwischen verschiedenen Ergebnissen statistisch nicht signifikant ausfallen; R4 – alle Betrachtungen beziehen sich auf die Funktionale Sicherheit unter Bezug auf die CENELEC-Standards [14, 3]. Andere Sicherheitsaspekte, explizit Cybersicherheit, Arbeitsschutz, Brandschutz etc. sind nicht im Betrachtungsumfang enthalten; R5 – eine Untersuchung der Leistungsfähigkeit von Menschen in Bezug auf Sinneswahrnehmung und Verarbeitungsfähigkeit von Informationen ist nicht Bestandteil des Projekts. Diese erfolgt im Parallelprojekt ATO-SENSE. Schon bei anderen Risikoanalysen [2] hat es sich bewährt, zu Beginn eine fachliche Vorgehensweise abzustimmen, die die wesentlichen Arbeitsschritte und Methoden definiert und auf Plausibilität prüft.

1 Ansatz

Bei der Einführung des automatisierten Fahrens bei den EdB handelt es sich zweifellos um eine signifikante Änderung im Sinne der CSM-VO [5], zumindest wenn es um die fahrerlosen Varianten GOA 3 (Grade of Automation, GoA) oder GOA 4 geht. Automatic Train Operation (ATO) in GOA 2 kann dagegen schon als Stand der Technik angesehen werden, da es bereits einige zugelassene Implementierungen gibt, z. B. auch im Rahmen der Digitalen Schiene bei der S-Bahn Hamburg.

Daher ist insgesamt der in der CSM-VO definierte Prozess zu befolgen. Für viele der Gefährdungen wird voraussichtlich eine explizite Risikoanalyse notwendig sein, da es weder Regelwerke noch Referenzsysteme gibt. Die effektive und CSM-konforme Gestaltung der Risikoanalyse ist daher ein Kernpunkt der Vorgehensweise im Projekt ATO-RISK.

Aufgrund von R3 wird dafür ein semi-quantitativer Ansatz gewählt, da für eine quantitative Risikoanalyse in Deutschland nicht

The ATO-RISK project, which was commissioned by the German Centre for Rail Traffic Research (DZSF), has been given the goal of deriving "risk acceptance criteria for automated driving on railways", albeit under the following contractual boundary conditions: R1 – the task is related to train movements on normal train routes in the German Federal Railways (EdB) network using automation systems, but focussing on the GoA 3 and GoA 4 grades of automation; R2 – no special solution architectures will be evaluated and no safety objectives will be derived for technical components; R3 – the aim is to ensure that the quantitative results (e.g. Tolerable Hazard Rate – THR) match in their order of magnitude or that at least the deviations between the different results are not statistically significant in order to ensure the quality of the results, i.e. also for validation; R4 – all considerations relate to functional safety with reference to the CENELEC standards [14, 3]. No other safety aspects, explicitly cyber security, occupational safety, fire protection, etc. will be included in the scope of consideration; R5 – the project will not include an investigation into human performance in terms of sensory perception and the ability to process information. This will be performed in the parallel ATO-SENSE project. Other risk analyses [2] have already shown the benefits of coordinating a technical approach that defines the essential work steps and methods and checks them for plausibility right at the beginning.

1 The starting point

The introduction of automated driving on German Federal Railways is undoubtedly a significant change within the meaning of the CSM regulation [5], at least when it comes to the GOA 3 (Grade of Automation, GoA) or GOA 4 driverless variants. On the other hand, Automatic Train Operation (ATO) in GOA 2 can already be regarded as state of the art, as some approved implementations already exist, e.g. also within the context of the Digital Rail at the S-Bahn Hamburg.

Therefore, the process defined in the CSM regulation must generally be followed. An explicit risk analysis will probably be necessary for many of the hazards, as there are neither any codes of practice nor reference systems. The effective, CSM-compliant design of the risk analysis is therefore a key point of the procedure in the ATO-RISK project.

Based on R3, a semi-quantitative approach has been chosen for this, as there is not enough data available in Germany for a quantitative risk analysis to reliably estimate the numer-

ausreichend Daten vorliegen, um die zahlreichen benötigten Parameter verlässlich abzuschätzen. Dies hat u. a. die Risikoanalyse für den Funk-Fahrbetrieb (FFB) [2] gezeigt, und man darf davon ausgehen, dass ATO-RISK einen ähnlichen Umfang bzw. eine vergleichbare Komplexität hat.

DIN VDE V 0831-103 [12] ist seit 2014 Stand der Technik in Deutschland und wurde unter anerkannten Fachleuten, auch aus dem Nahverkehr, abgestimmt. Im September 2020 wurde sie auf den neuesten Stand der Gesetzgebung, insbesondere CSM-VO, und Normung, insbesondere DIN EN 50129 [15], aktualisiert. Sie erfüllt die Anforderungen der CSM-VO. Das in ihr abgebildete Risikoniveau entspricht für eine große Breite von Anwendungen der Leit- und Sicherheitstechnik, von Elektronischem Stellwerk (ESTW) über Bahnübergang (BÜ) bis zu European Train Control System (ETCS), dem heute im Fernverkehr in Deutschland akzeptierten Sicherheitsniveau [7]. Außerdem wurde sie gegenüber den Anforderungen der DIN VDE V 0831-101 [11] konstruiert und validiert, als bislang einzige semi-quantitative Methode.

Ein wesentlicher Vorteil der sog. Risk Score Matrix (RSM) nach DIN VDE V 0831-103 besteht darin, dass die Einschätzung des Schadensausmaßes qualitativ nach Unfallklassen, die durch typische Ereignisarten beschrieben sind, erfolgt, und dass diese Ereignisarten anhand der Unfall-Datenbank der Deutschen bahn AG (DB) validiert wurden [1]. Bei diesen Einstufungen wurde schon zur sicheren Seite hin abgeschätzt, d. h. es wurde nicht der Mittelwert benutzt, sondern ein schwereres, aber noch glaubwürdiges Schadensausmaß berücksichtigt.

Auch die einzige heute in Deutschland zugelassene fahrerlose U-Bahn in Nürnberg wurde mit einer semi-quantitativen Methode bewertet [8]. Die dort verwendete Methode wird allerdings im Fernverkehr nicht allgemein akzeptiert. Wenn die Randbedingungen aber vergleichbar sind, könnten durchaus realisierte und betriebsbewährte Systeme aus dem Nahverkehr als Referenzsysteme herangezogen werden.

2 Vorgehensweise

Nach DIN VDE V 0831-103 wird nun unter Berücksichtigung der Anforderungen der CSM-VO wie folgt vorgegangen (wobei die Aufgaben thematisch zusammengefasst wurden, Bild 1):

1. Systemdefinition: Die Funktionen, die im Untersuchungsrahmen liegen, werden identifiziert. Das Schutzziel der zu bewertenden Funktion und ihre Rahmenbedingungen werden kurz charakterisiert. Objekte, die durch die Funktion geschützt werden und die von einem Ausfall betroffen sind, werden bestimmt. Die relevanten betrieblichen Szenarien, in denen die Funktionen ausgeführt werden, werden identifiziert.
2. Gefährdungsidentifikation: Für jede relevante Ausfallart einer Funktion wird analysiert, welche Auswirkungen hieraus resultieren können.
3. Auswahl des Risikoakzeptanzkriteriums: In der Regel wird hier für GoA 3/4 explizite Risikoanalyse ausgewählt werden müssen. Wenn ausnahmsweise Regelwerk oder Referenzsystem ausgewählt werden können, so können die folgenden Schritte 4 und 5 entfallen und werden durch eine Bewertung des Referenzsystems ersetzt.
4. Ermittlung des Schadensausmaßes: Es wird die jeweils zutreffende Unfallklasse ermittelt.
5. Bewertung der Barrieren: Anschließend werden die möglichen Barrieren bestimmt und nach den vorgegebenen Tabellen bewertet. Bei mehreren Barrieren muss ggf. deren Abhängigkeit bewertet werden.

ous required parameters. This has been shown, among other things, by a risk analysis for radio based operations (FFB) [2] and it can be assumed that ATO-RISK has a similar scope or complexity.

DIN VDE V 0831-103 [12] has been a standard in Germany since 2014 and it has been coordinated by recognised experts, including from mass transit. In September 2020, it was updated to bring it in line with the latest legislation, in particular the CSM regulation, and standardisation, in particular DIN EN 50129 [15]. It meets the requirements of the CSM regulation. The risk level depicted in it for a wide range of applications in control and safety technology ranging from electronic interlocking (ESTW) to level crossing (LC) and on to European Train Control System (ETCS) corresponds to the safety level [7] accepted in mainline railways in Germany today. In addition, it has also been designed and validated against the requirements of DIN VDE V 0831-101 [11] as the only semi-quantitative method to date.

A major advantage of the so-called Risk Score Matrix (RSM) according to DIN VDE V 0831-103 is that the severity assessment is carried out qualitatively according to accident categories described by typical event types and these event types have been validated on the basis of Deutsche Bahn AG's (DB) accident database [1]. These classifications already erred on the side of caution, i.e. the mean value was not used, but a more conservative, yet still credible severity scope was taken into account.

The only driverless subway in Nuremberg that is now approved in Germany was also evaluated using a semi-quantitative method [8]. However, the method used there is not generally accepted in mainline railways. On the other hand, implemented and operationally proven systems from mass transit could be used as reference systems, provided the boundary conditions are comparable.

2 The approach

The following approach has been proposed in compliance with DIN VDE V 0831-103, while taking the requirements of the CSM regulation into account (the tasks have been summarised thematically; fig. 1):

1. The system definition: the functions that lie within the scope of the investigation are identified. The safety objective of the function that is to be evaluated and its framework conditions are briefly characterised. Objects that are protected by the function and that are affected by a failure are determined. The relevant operating scenarios where the functions are executed are identified.
2. The hazard identification: the potentially resulting effects are analysed for each relevant failure type of a function.
3. The selection of the risk acceptance principle (RAP): as a rule, explicit risk analyses will have to be selected for GoA 3/4. If a code of practice or reference systems can be exceptionally selected, the following steps 4 and 5 may be omitted and replaced with an assessment of the reference system.
4. The determination of severity: the applicable accident category is determined.
5. The evaluation of the barriers: the possible barriers are subsequently determined and evaluated according to the given tables. If there are several barriers, their dependence may have to be assessed.

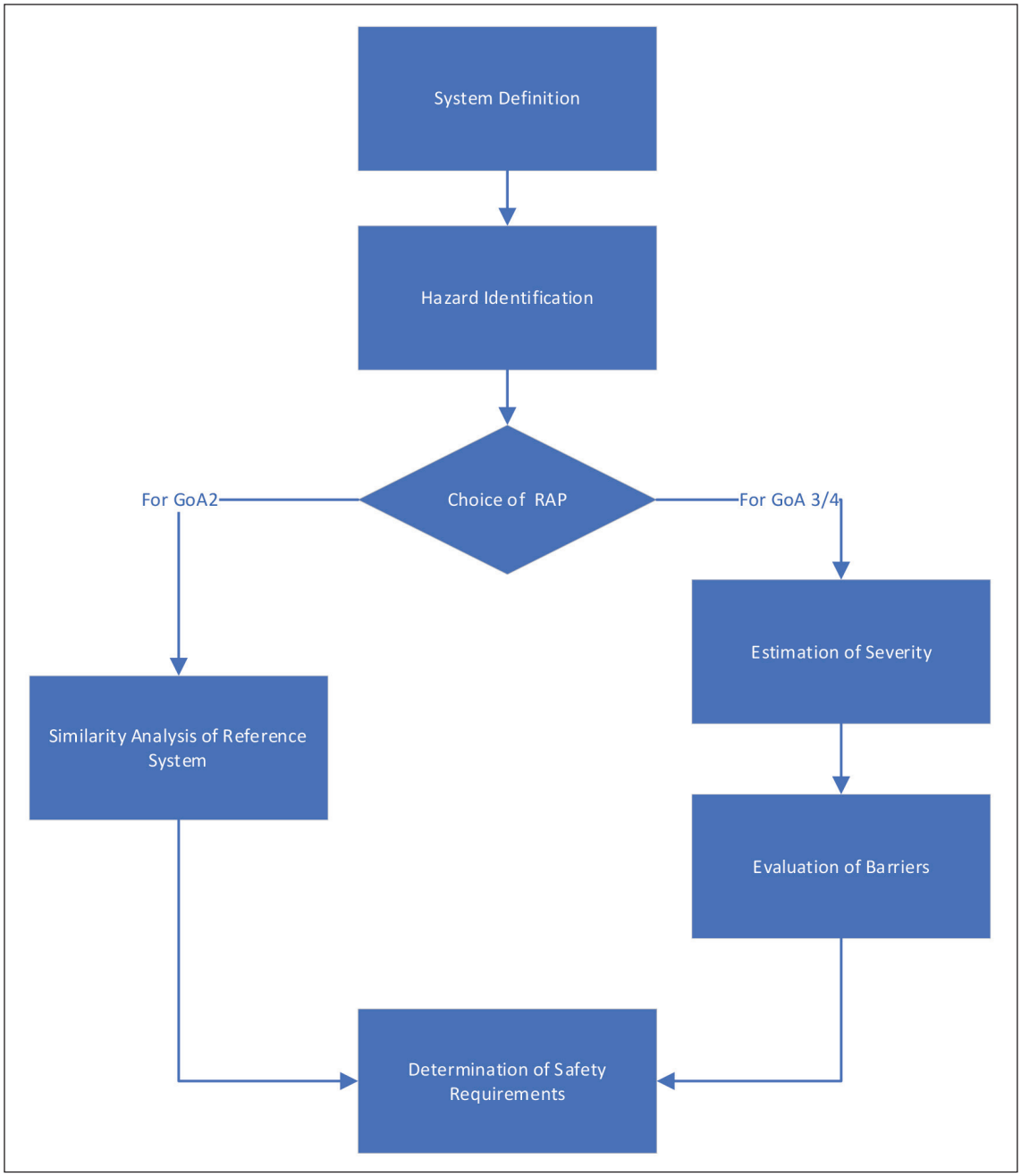

Bild 1: Vorgehensweise ATO-RISK
Fig. 1: The ATO-RISK approach
Quelle / *Source*: Siemens Mobility GmbH

6. Ermittlung der Sicherheitsanforderung: Für die jeweilige Ausfallart mittels Responsive Surface Methodology (RSM)

Dabei ist insbesondere die Koordination der Aufgaben mit ATO-SENSE wichtig, z. B., um Doppelarbeiten zu vermeiden. Diese ist aber durch R2 und R5 schon vorgezeichnet, denn ATO-RISK beschäftigt sich nur mit funktionalen Anforderungen, soweit sie zur Ableitung von Sicherheitsanforderungen notwendig sind. Die technische Realisierung (vgl. R2) oder die betrieblichen Randbedingungen an die Leistungsfähigkeit der technischen Lösung (vgl. R5) sind nicht Bestandteil der Untersuchung.

Das einfachere Beispiel der Gefahrraumfreimeldung am BÜ kann die Aufgabenteilung illustrieren: Hier würde ATO-SENSE die funktionalen Anforderungen definieren, z. B. welche Hindernisse erkannt werden müssen, und ATO-RISK würde die Integritätsanforderungen ableiten.

Um die Darstellung in Bild 1 möglichst einfach zu halten, wurden die begleitenden Verifikationsaufgaben sowie die abschließende unabhängige Validierung nicht explizit dargestellt.

6. The determination of the safety requirements: for each failure mode by means of the application of Responsive Surface Methodology (RSM)

The coordination of tasks with ATO-SENSE is particularly important, i.e. in order to avoid any duplication of work. However, this is already predetermined by R2 and R5, because ATO-RISK only deals with functional requirements to the extent that they are necessary for deriving safety requirements. The technical realisation (cf. R2) or the operating boundary conditions for the performance of the technical solution (cf. R5) do not constitute any part of the investigation.

The simpler example of obstacle detection at a full-barrier LC can illustrate the division of tasks: here, ATO-SENSE would define the functional requirements, e.g. which obstacles must be detected, and ATO-RISK would derive the integrity requirements.

Basisfunktionen des Fahrbetriebes		Fahren auf Sicht (Sichtfahrbetrieb)	Nicht automatischer Fahrbetrieb	Halbautomatischer Fahrbetrieb	Fahrerloser Fahrbetrieb	Unbegleiteter Fahrbetrieb
		GOA0	GOA1	GOA2	GOA3	GOA4
Sicherstellen sicherer Zugbewegungen	Sicherstellen einer sicheren Fahrstraße	x (Weichen stellen und überwachen im System)	System	System	System	System
	Sicherstellen der sicheren Abstandhaltung von Zügen	x	System	System	System	System
	Sicherstellen der sicheren Geschwindigkeit	x	x (teilweise überwacht durch System)	System	System	System
Fahren	Steuern und Überwachen von Beschleunigen und Bremsen	x	x	System	System	System
Überwachen des Fahrweges	Verhindern eines Zusammenstoßes mit Hindernissen	x	x	x	System	System
	Verhindern eines Zusammenstoßes mit Personen im Gleis	x	x	x	System	System
Überwachen des Fahrgastwechsels	Steuern und Überwachen der Fahrgastraumtüren	x	x	x	x	System
	Verhindern der Verletzung von Personen zwischen Wagen oder Bahnsteig und Zug	x	x	x	x	System
	Sicherstellen der sicheren Anfahrbedingungen	x	x	x	x	System
Betreiben eines Zuges	Einsetzen/Aussetzen	x	x	x	x	System
	Überwachung des Zugstatus	x	x	x	x	System
Sicherstellen des Erkennens und der Bewältigung von Notfallsituationen	Ausführen der Zugdiagnose, Erkennen von Feuer/Rauch und Entgleisung, Bemerken des Verlustes der Zugintegrität, Behandeln von Notfallsituationen (Ruf/Evakuierung/Überwachung)	x	x	x	x	System und/oder Personal in OCC
ANMERKUNG x = Verantwortlichkeit von Betriebspersonal (kann durch UGTMS-System realisiert werden)			System = muss durch UGTMS-System realisiert werden			

Tab. 1: Basisfunktionen nach DIN IEC 62290

Basic functions of train operation		On-sight train operation	Non-automated train operation	Semi automated train operation	Driverless train operation	Unattended train operation
		GOA0	GOA1	GOA2	GOA3	GOA4
Ensuring safe movement of trains	Ensure safe route	x (points command/control in System)	System	System	System	System
	Ensure safe separation of trains	x	System	System	System	System
	Ensure safe speed	x	x (partly supervised by System)	System	System	System
Driving	Control acceleration and braking	x	x	System	System	System
Supervising track	Prevent collision with obstacles	x	x	x	System	System
	Prevent collision with persons on track	x	x	x	System	System
Supervising passenger transfer	Control passenger doors	x	x	x	x	System
	Prevent person injuries between cars or between platform and train	x	x	x	x	System
	Ensure safe starting conditions	x	x	x	x	System
Operating a train	Set in/set off operation	x	x	x	x	System
	Supervise the status of the train	x	x	x	x	System
Ensuring detection and management of emergency situations	Perform train diagnostic, detect fire/smoke and detect derailment, handle emergency situations (call/evacuation, supervision)	x	x	x	x	System and/or staff in operation control centre
NOTE x = responsibility of operations staff (may be realised by Automation System)			System = shall be realised by Automation System			

Tab. 1: The basic functions according to DIN IEC 62290

3 Systemdefinition

In Anlehnung an [9] beschreibt der automatisierte Bahn- / Fahrbetrieb (ATO) eine Betriebsart, in der verschiedene Aufgaben des Bahnbetriebs entsprechend des aktuellen Automatisierungsgrades (GoA) automatisiert sind. Dies beinhaltet auch GoA 4, indem der Zug vollständig automatisch ohne Betriebspersonal an Bord gesteuert wird.
Welche Funktionen im Rahmen des jeweiligen Automatisierungsgrades automatisiert werden, findet sich in [14], Tab. 1.
Die Definition der Automatisierungsgrade stammt ursprünglich aus der für den Nahverkehr angewandten DIN IEC 62290, hat sich aber auch im Fernverkehr etabliert. So wurden die entsprechenden Definitionen aus DIN IEC 62290 leicht adaptiert auch im europäischen Förderprogramm für Innovationen im Schienenverkehr „Shift2Rail" bei der Erstellung der ATO over ETCS-Subsets mit redaktionellen Anpassungen übernommen [9].

In order to keep the representation in fig. 1 as simple as possible, the accompanying verification tasks, as well as the final independent validation, have not been explicitly displayed.

3 The system definition

Based on [9], ATO describes an operating mode in which various railway operations tasks are automated according to the current GoA. This also includes GoA 4 where the train is controlled completely automatically without any personnel on board.
The functions that are automated within the scope of the given GoA can be found in [14], tab. 1.
The definition of the GoA originally comes from IEC 62290 which is used for mass transit, but has also established itself in mainline railways. Thus, the corresponding definitions from DIN IEC 62290 have also been slightly adapted in the European "Shift2Rail" research program when creating the ATO over ETCS subsets with some editorial adjustments [9].

4 Funktionen

Weiterhin definiert die DIN IEC 62290 Basisfunktionen des Fahrbetriebs auf einer funktionalen Ebene, allerdings mit teilweise unterschiedlicher Terminologie, da diese für den Nahverkehr geschrieben wurde, z. B.:

- Überwachen des Fahrwegs
  - Verhindern des Zusammenstoßes mit Hindernissen
  - Verhindern des Zusammenstoßes mit Personen auf der Strecke
- Basisfunktionen der Betriebsführung und Überwachung
- …

Diese Basisfunktionen werden als Grundlage für die Betrachtung herangezogen.

Um Vollständigkeit zu erreichen, wird wie folgt vorgegangen

a. Die Funktionsliste aus der DIN IEC 62290 [14] wird als Grundlage genommen und es wird bewertet sowie begründet, warum diese zum System gehört oder nicht. Ggf. wird die Terminologie angepasst, wenn sie von der im Fernverkehr üblichen abweicht.
b. Ein Abgleich mit anderen Funktionslisten z. B. von S2R, DIN VDE V 0831-103 oder IEC 62267, wird durchgeführt.
c. Zusätzlich wird ein Quercheck mit den Netzzugangsbedingungen und Vorschriften wie RiL 408 durchgeführt.

Die Systemdefinition mit der Festlegung von Systemgrenzen, Schnittstellen, Funktionen und Systemumgebung hängt stets vom Standpunkt des Betrachters ab, Bild 2 [2].

Bei der RSM-Methode muss die Systemdefinition auf einer geeigneten funktionalen Ebene durchgeführt werden, die mit der CSM-VO kompatibel ist.

Dabei kommen für den automatisierten Fahrbetrieb GoA 3/4 u. a. folgende Schutzfunktionen in Betracht (aus der DIN VDE V 0831-103):

- Schutz vor Hindernissen im Fahrweg
- Automatisieren des Betriebes
- Überwachen des Betriebs
- …

Eine geeignete Systemdefinition ist auch deswegen wichtig, damit möglicherweise bereits bestehende technische Realisierungen von Subsystemen wie bei ETCS oder Punktförmiger Zugbeeinflussung (PZB), falls notwendig, als Systembestandteile behandelt werden können und z. B. schon existierende Sicherheitsziele für solche Systeme in der Ursachenanalyse als Vorgaben berücksichtigt werden können. Alternativ könnten sie auch als Barrieren außerhalb der Systemdefinition betrachtet werden. Es sollte nur vermieden werden, neue Sicherheitsanforderungen für bereits bestehende Systeme abzuleiten.

Diese Schutzfunktionen können in der Realisierung durchaus durch verschiedene Schutzeinrichtungen erbracht werden. Dies wird wegen R2 nicht weiter betrachtet.

Schutzziel und Rahmenbedingungen müssen charakterisiert werden, dazu gehören auch betriebliche Szenarien, in denen die Schutzfunktionen eingesetzt werden.

5 Szenarien

Die Funktionen werden hinsichtlich verschiedener veränderbarer betrieblicher Einflüsse betrachtet. Maßgebend ist hier das Szenario Zugfahrt bei EdB. Dabei muss u. a. nach Zugarten und Geschwindigkeiten unterschieden werden:

Zugarten:

1. Reisezüge – ggf. weitere Unterscheidung nach S-Bahn, Hochgeschwindigkeitszüge (Einfluss auf die Musterstrecken oder Szenarien – bauliche Unterschiede)

4 Functions

Furthermore, DIN IEC 62290 defines the basic train operation functions on a functional level, but with slightly different terminology, as this was written for mass transit, e.g..:

- track supervision
  - prevent collisions with obstacles
  - prevent collisions with people on the track
- Basic train operations and supervision functions
- …

These basic functions have been used as the basis for consideration.

The following steps have been followed in order to achieve completeness:

a. The function list from DIN IEC 62290 [14] has been taken as a basis and an evaluation and justification has been made as to whether or not it belongs to the system and why. Where necessary, the terminology has been adapted, if it deviates from that usually used in mainline railway.
b. A comparison with other function lists, e.g. from S2R, DIN VDE V 0831-103 or IEC 62267, is carried out.
c. In addition, a cross-check has been carried out with the German network access conditions and regulations such as RiL 408

The system definition with the defined system boundaries, interfaces, functions and system environment always depends on the point of view of the analyst; fig. 2 [2].

When using the RSM method, the system definition must be performed at an appropriate functional level that is compatible with the CSM VO.

The following safety functions are considered for automated GoA 3/4 operations (from DIN VDE V 0831-103):

- protection against track obstacles
- automation of operations
- supervision of operations
- …

A suitable system definition is also important so that possibly already existing technical realisations of subsystems such as ETCS or PZB system components can be dealt with, if necessary, and any already existing safety targets for these systems can be taken into account as specifications in the causal analysis. Alternatively, they could also be considered to constitute barriers outside the system definition. However, the derivation of new safety requirements for existing systems should be avoided.

Various protection devices can provide these safety functions in the implementation. This has not been further considered due to R2.

The safety objective and framework conditions must be characterised, including any operating scenarios where the protection functions have been used.

5 Scenarios

The functions are considered with regard to various changeable operating influences. The decisive thing here is the scenario for train movements on normal train routes at EdB. A distinction must be made, amongst other things, according to the train types and speeds:

Train types:

1. passenger trains –further distinctions may possibly be necessary, e.g. high-speed trains, S-Bahn…

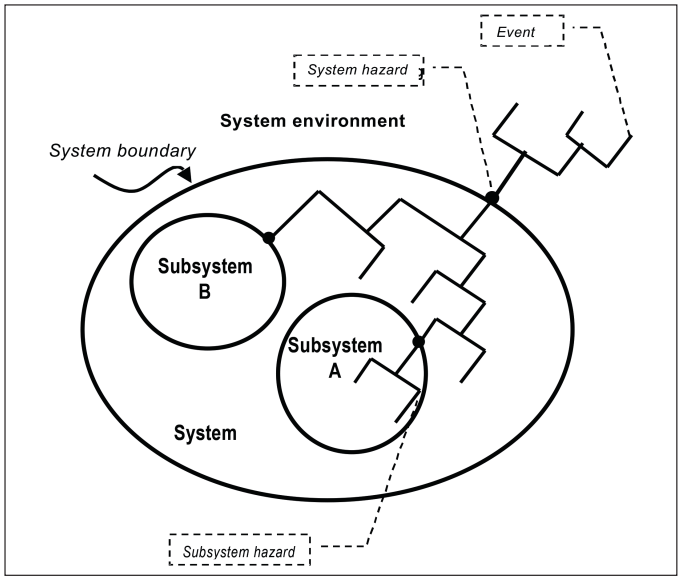

Bild 2: Bedeutung der Systemdefinition
Fig. 2: The importance of system definition Quelle / *Source*: Siemens Mobility GmbH

2. Güterzüge
Geschwindigkeiten:
- „Sehr hohe Geschwindigkeit" > 160 km/h – Obergrenze 250 km/h
- „Hohe Geschwindigkeit" > 80 km/h – 160 km/h
- „Mittlere Geschwindigkeit" > 40 km/h – 80 km/h
- „Niedrige Geschwindigkeit" <40 km/h

Gemäß DIN VDE V 0831-103 wird nur zwischen niedriger, mittlerer und hoher Geschwindigkeit unterschieden. Die EBO sieht aber streckenseitig besondere Ausnahmen bei Geschwindigkeiten über 160 km/h Bremsweg vor, z. B. dürfen keine BÜ vorhanden sein.
Darauf aufbauend können detailliertere Szenarien betrachtet werden, z. B.:
- Sicherung der Zugfahrt
  - Fahren auf Sicht
  - Fahren im Raumabstand
- Ausdehnung der betrachteten Zugbewegung
  - Fahrt auf freier Strecke
  - Fahrt in Bahnhöfen bzw. bei betrieblichen Halten

Nicht berücksichtigte Szenarien sind im Rahmen des Projekts ATO-RISK:
1. Züge bilden
2. Übergang von Rangier- in Zugfahrt und vice versa
3. Ändern des Zugstatus
4. Rangierfahrten
5. Abfertigung / Fahrgastwechsel
6. Übergänge vom Regelbetrieb zur Rückfallebene (und umgekehrt)

6 Musterstrecke

Um die statischen Infrastruktureigenschaften abzubilden, kann, falls notwendig, eine möglichst repräsentative Musterstrecke herangezogen werden. Mögliche relevante Elemente lassen sich aus der EBO bzw. der Fahrdienstvorschrift ableiten. Diese sind hinsichtlich ihrer Relevanz für die jeweiligen Szenarien zu bewerten.

7 Gefährdungsidentifikation

Alle maßgeblichen Versagensmöglichkeiten der betrachteten Schutzfunktionen müssen identifiziert werden. Dies kann strukturiert im Stil einer funktionalen Failure Mode Effect Analysis (FMEA) erfolgen.

2. freight trains
Train speeds:
- "Very high" > 160 km/h – 250 km/h (upper limit)
- "High" > 80 km/h – 160 km/h
- "Medium" > 40 km/h – 80 km/h
- "Low" <40 km/h

DIN VDE V 0831-103 only distinguishes between low, medium and high speed. However, the EBO has included special trackside exceptions for speeds above a 160 km/h braking distance, i.e. there must be no LC.
More detailed scenarios can be considered based on this, e.g.:
- train movement protection
  - on-sight operations
  - fixed block operations
- the type of train movement
  - tracks between stations
  - tracks inside stations

The following scenarios have not been covered in the ATO-RISK project:
1. train composition
2. the transition from shunting to regular train movements and vice versa
3. change of train status
4. shunting
5. dispatching / passenger exchange
6. the transition from regular operations to fallback mode and vice versa

6 The model track

A model track that is as representative as possible can be used, if necessary, to map the static infrastructure properties. Possible relevant elements can be derived from the EBO or other regulations. They must be evaluated with regard to their relevance to the respective scenarios.

7 Hazard identification

All the relevant failure modes of the considered protection functions must be identified. This can be achieved in a structured way in the style of a functional Failure Mode Effect Analysis (FMEA).
In addition, hazard identification results can also be compared with standards such as DIN EN 62267 [13] and project results. The combination of analytical and empirical approaches should be sufficient to justify the completeness at the chosen level of consideration.
A classification of hazards, possibly according to the CSM regulation, is not required with RSM. If necessary, however, any broadly justifiable risks can be identified and excluded from consideration. An essential assumption for the ATO system involves the fact that only functional safety is evaluated (cf. R4) and not any hazards based on sabotage, i.e. the wilful introduction of arbitrary obstacles onto the route.

8 Selecting the risk acceptance principle

As a rule, an explicit risk analysis will have to be performed for GOA 3/4 in accordance with DIN VDE V 0831-103, as there is currently no code of practice for automated operations for EdB, while automated operations in mass transit

Außerdem kann die Gefährdungsidentifikation mit Normen wie DIN EN 62267 [13] sowie Ergebnissen aus Projekten abgeglichen werden. Die Kombination aus analytischen und empirischen Ansätzen sollte auf der gewählten Betrachtungsebene ausreichen, um Vollständigkeit zu begründen.
Eine Klassifikation der Gefährdungen, wie nach der CSM-VO möglich, ist bei RSM nicht erforderlich. Falls notwendig, können aber allgemein vertretbare Risiken identifiziert und aus der Betrachtung ausgeschlossen werden. Für das System ATO besteht eine wesentliche Annahme darin, dass nur funktionale Sicherheit bewertet wird (vgl. R4) und nicht z. B. Gefährdungen aufgrund von Sabotage, z. B. mutwilliges Einbringen beliebiger Hindernisse auf der Strecke.

8 Auswahl des Risikoakzeptanzkriteriums

In der Regel wird bei GOA 3/4 eine explizite Risikoanalyse, entsprechend DIN VDE V 0831-103, durchgeführt werden müssen, da es bisher kein Regelwerk für automatisiertes Fahren bei EdB gibt und auch das automatische Fahren im Nahverkehr nur ausnahmsweise als Referenzsystem herangezogen werden kann. Dies muss im Einzelfall betrachtet werden.
Für GOA 2 können die heutigen Implementierungen als Referenzsysteme angesehen werden. Diese müssen analysiert bzw. bewertet werden, insbesondere unter Berücksichtigung der menschlichen Zuverlässigkeit. Wie komplex bzw. zielführend eine solche Analyse ist, wird sich erst im Lauf der Bearbeitung herausstellen. Alternativ könnte auch mit expliziter Risikoanalyse nach [12] vorgegangen werden.
Für einzelne Gefährdungen, für die Regelwerk existiert, z. B. Gefahrraumfreimeldung am BÜ, wird dies natürlich herangezogen.

9 Ermittlung des Schadensausmaßes

Bei der Ermittlung der maßgeblichen Unfallklasse kann es notwendig sein, die Betrachtung nach verschiedenen betrieblichen Szenarien hin zu unterscheiden.
Wichtig ist, dass die Begriffe in der Definition der Unfallklassen korrekt verwendet werden. Z. B. ist Auffahren auf ein Hindernis als „Fahren gegen ein Hindernis im Regellichtraum" definiert, wobei als Beispiele „Gleissperre, Baum, Hemmschuhe, Hakenkralle in der Oberleitung" explizit genannt werden. Dabei wird in DIN VDE V 0831-103 davon ausgegangen, dass das Hindernis *„sich nur in einem Teil des Regellichtraums (vorwiegend in dessen unteren Bereich) befindet, diesen jedoch nicht überwiegend oder vollständig belegt"*. Dies wird in der Regel bei vergessenen Einrichtungen oder zufällig einfallenden Hindernisse der Fall sein, jedoch nicht bei mutwillig eingebrachten Hindernissen oder Hindernissen, die sich aufgrund des Versagens anderer Schutzeinrichtungen dort befinden, z. B. Zügen oder Zugteilen nach Versagen der Gleisfreimeldung.
Weiter ist zu beachten, dass in den Unfallstatistiken relativ wenige Unfalldaten für Hochgeschwindigkeitsverkehr vorhanden sind. Die in DIN VDE V 0831-103 betrachteten typischen Geschwindigkeiten „niedrig", „mittel" sowie „hoch" beziehen sich auf Rangierfahrten, Regional- bzw. konventionellen Fernverkehr. Bei Geschwindigkeiten über 160 km/h ist eine gesonderte Argumentation zu führen und ggf. eine höhere Unfallklasse zu wählen.

10 Bewertung von Barrieren

Die Bewertung der Barrieren erfolgt nach den in DIN VDE V 0831-103 angegebenen Tabellen. Es besteht keine Notwendigkeit weiterer spezifischer Tabellen. Bei hohen Automatisierungsgraden

can only be used as a reference system in exceptional cases. This must be considered on a case-by-case basis.
The current implementations can be regarded as reference systems for GOA 2. These must be analysed or evaluated, while in particular taking human reliability into account. How complex or expedient such an analysis is will only become clear over the course of project. Alternately, an explicit risk analysis according to [12] could also be used.
Any regulations that exist for individual hazards, e.g. obstacle detection at the LC, are of course taken into account.

9 The estimation of severity

When determining the relevant accident categories, it may be necessary to differentiate the consideration according to different operational scenarios.
It is important that the terms in the accident category definitions are used correctly. For example, driving onto an obstacle is defined as "driving against an obstacle in the loading gauge", whereby "derailer, tree, brake shoes and, hook claw in the overhead line" are also explicitly mentioned as examples. In DIN VDE V 0831-103, it is assumed that an obstacle "*is only located in a part of the loading gauge (mainly in its lower area), but does not occupy it predominantly or completely*". This will usually be the case with forgotten devices or accidentally occurring obstacles, but not with intentionally introduced obstacles or obstacles that are located there due to the failure of any other safety functions, e.g. trains or train parts after a failure of the track clearance notification.
It should also be noted that there is relatively little accident data for high-speed traffic in the German accident statistics. The typical speeds "low", "medium" and "high" considered in DIN VDE V 0831-103 refer to shunting, regional or mainline railways. A separate argumentation must be made at speeds above 160 km/h and, if necessary, a higher accident category must be chosen.

10 The evaluation of barriers

The barriers are evaluated according to the tables specified in DIN VDE V 0831-103. There is no need for any further specific tables. High levels of automation mean that there should be few barriers and especially none due to human actions. When assessing the barriers, one can refer to the rich set of examples contained in Annex B of DIN VDE V 0831-103.
However, a special caveat must also be noted: in a few cases, DIN VDE V 0831-103 considers the personnel to constitute a risk-reducing factor, namely for existing functions that are not considered by ATO-RISK. In order for these risk analyses to continue to hold true, these barriers must be identified and the assumptions made there must be taken into account as additional safety requirements for the new automation functions. However, since the assumptions about such barriers have been made rather conservatively, it is not to be expected that this will result in any significant or additional requirements.

11 Analysis of the reference systems

Numerous projects have already been realised with GOA 2, so no risk analysis is necessary. However, it is necessary to show that the safety requirements derived from the risk analysis for GOA 3/4 do not lower the current achieved safety level [6]. This means that an analysis is only necessary for

sollten nur wenige Barrieren bestehen, insbesondere keine aufgrund von menschlichen Handlungen. Bei der Bewertung der Barrieren kann man sich an die reichhaltigen Beispiele in Anhang B der DIN VDE V 0831-103 anlehnen.
Dabei ist allerdings eine Besonderheit zu beachten: In wenigen Fällen wurde der Mensch in der DIN VDE V 0831-103 als risikoreduzierender Faktor angenommen, und zwar bei Bestandsfunktionen, die durch ATO-RISK nicht betrachtet werden. Damit diese Risikoanalysen weiter Bestand haben, müssen diese Barrieren identifiziert und die dort gemachten Annahmen als zusätzliche Sicherheitsanforderungen bei den neuen Automatisierungsfunktionen berücksichtigt werden. Da die Annahmen an solche Barrieren aber eher konservativ getroffen wurden, ist nicht zu erwarten, dass daraus wesentliche oder zusätzliche Anforderungen entstehen.

11 Analyse des Referenzsystems

Bei GOA 2 gibt es bereits zahlreiche realisierte Projekte, daher ist eigentlich keine Risikoanalyse notwendig. Es ist allerdings notwendig, zu zeigen, dass die durch die Risikoanalyse für GOA 3/4 abgeleiteten Sicherheitsanforderungen das heutige Sicherheitsniveau nicht senken [6]. D. h. eine Analyse ist nur notwendig für Funktionen, die verändert werden sollen oder bei denen der Mensch durch Technik ersetzt werden soll. Insbesondere wird keine Analyse für Funktionen durchgeführt, für die es schon Sicherheitsanforderungen gibt, wie z. B. PZB oder ETCS.
Für GOA 2 können Betriebserfahrungen qualitativ und / oder quantitativ ausgewertet werden. Dies kann über Bewertung von Referenzsystemen oder Auswertung betrieblicher Statistiken erfolgen. Ein wichtiger Aspekt ist hier in jedem Fall die Bewertung der menschlichen Zuverlässigkeit, die nach einem möglichst einfachen Schema, z. B. nach DIN VDE V 0831-103, vorgenommen werden soll. Das Ziel ist hier allerdings nicht, neue Sicherheitsanforderungen abzuleiten oder existierende Systeme neu zu bewerten, sondern sicherzustellen, dass das automatische Fahren in höheren Automatisierungsgraden mindestens die gleiche Sicherheit nach EBO bietet.
Allerdings muss hier evtl. die betriebliche Häufigkeit von gewissen Gefährdungsszenarien abgeschätzt werden. Dabei kann möglicherweise auf die Vorgehensweise nach DIN VDE V 0831-100 [10] zurückgegriffen werden, z. B. Abschätzung des Parameters für die Häufigkeit H. Zwar handelt es sich hier nicht um die Risikobeurteilung potenzieller Sicherheitsmängel, aber auch für die Beurteilung des betrieblichen Risikos einzelner Sicherheitsfunktionen könnte der Ansatz verwendet werden.

12 Ermittlung der Sicherheitsanforderungen

Auch die Ermittlung der Sicherheitsanforderungen in Form einer THR kann bei GOA 3/4 direkt nach DIN VDE V 0831-103 erfolgen (Bild 3). Diese Anforderungen müssen mit der heute erzielten Sicherheit bei GOA 2 verglichen werden.
Unter Umständen könnten auch die bei ATO unter GOA 2 erzielten Ergebnisse direkt in die RSM eingetragen werden. In der Regel sollten die Unfallklassen identisch sein, wenn die betrieblichen Randbedingungen ähnlich sind. D. h. es wäre im Vergleich interessant, welche Gefährdungsrate bei GOA 2 ermittelt wird.

13 Diskussion

Der Untersuchungsumfang von ATO-RISK ist aufgrund der Beauftragung auf Zugfahrten bei EdB beschränkt (R1). Eine Erweiterung z. B. auf Rangierfahrten stellt methodisch keine grundsätzliche Schwie-

any functions that are to be changed or where human actions are to be replaced by technology. In particular, no analysis is required for functions that already have safety requirements, such as PZB or ETCS.
The operating experience for GOA 2 can be evaluated qualitatively and / or quantitatively. This can be done by evaluating the reference systems or the operating statistics. In any case, an important aspect here involves the evaluation of human reliability, which should be carried out according to the simplest possible scheme, e.g. according to DIN VDE V 0831-103. However, the aim here is not to derive new safety requirements or to re-evaluate existing systems, but to ensure that automatic operations in higher degrees of automation offer at least the same degree of safety according to EBO. In any case, the operating frequency of certain hazard scenarios may have to be estimated here. It may be possible to use the procedure according to DIN VDE V 0831-100 [10], e.g. "Estimation of the parameters for the frequency H". While this is not a risk assessment of potential safety deficiencies, this approach could also be used to assess the operational risks of individual safety functions.

12 Determining the safety requirements

For GOA 3/4, the safety requirements in the form of a THR can also be determined directly in accordance with DIN VDE V 0831-103 (fig. 3). These requirements must be compared with the safety achieved today with GOA 2.
Under certain circumstances, the results obtained at ATO under GOA 2 could also be entered directly into the RSM. As a rule, the accident categories should be identical, if the operating boundary conditions are similar. This means that it would be interesting to compare which hazard rate is determined for GOA 2.

13 Discussion

The scope of the ATO-RISK analysis is limited to regular train movements at EdB based on the job order (R1). An extension e.g. to shunting, does not represent a fundamental methodological difficulty [1]. However, the transferability of the results to other operating conditions, e.g. in other countries, particularly depends on the acceptance of the RSM method. This is calibrated to the CSM regulation in terms of risk acceptance and thus a transfer within the scope of the CSM regulation should be possible in principle. But it could be that the accident categories would have to be adapted in other operating conditions or that other boundary conditions, e.g. fenced tracks, would lead to different risk assessments and thus safety requirements.
On the other hand, the function lists and hazard identification can be reused in any case, as these have been carried out at a fairly high functional level, as in mass transit, and have also been compared with all the relevant sources. Here, one could also think about whether these results can form the basis for standardisation, as is the case in mass transit.
Since ATO-RISK only deals with the derivation of functional safety requirements, almost all technical implementation questions play no role. This means that even such important questions as how to implement obstacle detection with the help of artificial intelligence (AI), for example, are completely irrelevant here, because the safety requirements are independent of the implementation and it does not matter whether the function is later realised using relay technology or AI. How-

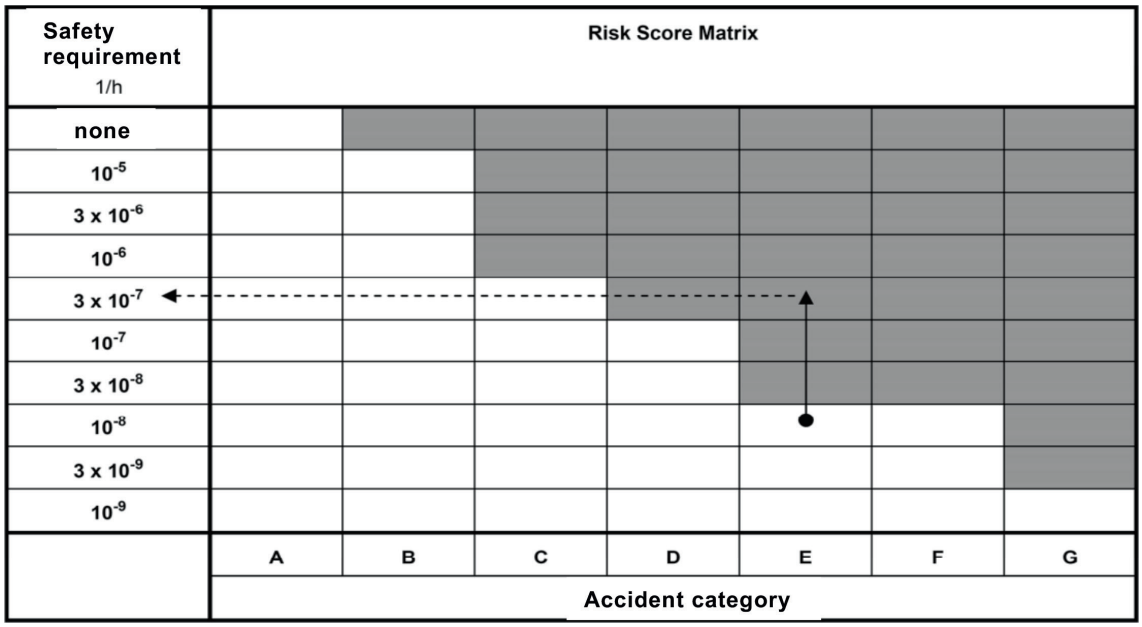

Bild 3: Ermittlung von Sicherheitsanforderungen nach DIN VDE V 0831-103
Fig. 3: Deriving the safety requirements according to DIN VDE V 0831-103

rigkeit dar [1]. Allerdings hängt die Übertragbarkeit der Ergebnisse auf andere Betriebsverhältnisse, z. B. in anderen Ländern, insbesondere von der Akzeptanz der RSM-Methode ab. Diese ist zwar von der Risikoakzeptanz her auf die CSM-VO kalibriert, und damit sollte eine Übertragung im Geltungsbereich der CSM-VO grundsätzlich möglich sein. Aber es könnte sein, dass bei anderen Betriebsverhältnissen die Unfallklassen angepasst werden müssten, oder dass es bei anderen Randbedingungen, z. B. eingezäunten Strecken, zu anderen Risikoabschätzungen und damit Sicherheitsanforderungen käme.
Dagegen können auf jeden Fall die Funktionslisten sowie die Gefährdungsidentifikation wiederverwendet werden, da diese wie im Nahverkehr auf einer recht hohen funktionalen Ebene erfolgt sind und diese mit allen relevanten Quellen abgeglichen werden. Hier könnte man auch darüber nachdenken, ob diese Ergebnisse wie im Nahverkehr die Grundlage einer Standardisierung bilden können.

ever, the same safety requirements must be met. The technical properties of an already implemented solution could only become relevant in an analysis of the reference systems.
For semi-quantitative methods such as RSM, DIN VDE V 0831-101 requires the estimates to be conservative. This could possibly lead to more demanding safety requirements than, for example, when using a quantitative method. Whether this argument holds true, however, is questionable, at least if one were to show the statistical uncertainty in the quantitative methods, instead of only working with averages, as is often the case. It has been shown [4] to statistically propagate so strongly even with only a few parameters, provided the uncertainty of the data has been correctly taken into account, that it exceeds an order of magnitude as a result, i.e. not even the derived Safety Integrity Level (SIL) can be clearly determined.

Da es hier nur um die Ableitung funktionaler Sicherheitsanforderungen geht, spielen fast alle Fragestellungen der technischen Realisierung keine Rollen. D. h. auch so wichtige Fragen, wie man z. B. eine Hinderniserkennung unter Zuhilfenahme von Künstlicher Intelligenz (KI) zulassen könnte, sind hier völlig irrelevant, denn die Sicherheitsanforderungen sind unabhängig von der Realisierung, und es ist völlig egal, ob die Funktion später mit Relaistechnik oder KI realisiert wird. Es sind aber dieselben Sicherheitsanforderungen zu erfüllen. Lediglich bei der Analyse von Referenzsystemen könnten technische Eigenschaften einer bereits realisierten Lösung relevant werden.

Bei semi-quantitativen Methoden wie der RSM wird nach DIN VDE V 0831-101 gefordert, dass die Abschätzungen konservativ sind. Dies könnte u. U. zu höheren Sicherheitsanforderungen führen als z. B. bei Anwendung einer quantitativen Methode. Ob dieses Argument allerdings stimmt, ist fraglich, zumindest wenn man bei quantitativen Methoden die statistische Unsicherheit ausweisen würde, anstatt, wie häufig üblich, nur mit Mittelwerten zu arbeiten. Es wurde gezeigt [4], dass sich schon bei wenigen Parametern die Unsicherheit der Daten statistisch so stark fortpflanzt, dass sie im Ergebnis eine Größenordnung übersteigt, d. h. nicht einmal der abgeleitete Safety Integrity Level (SIL) kann eindeutig bestimmt werden. Die Anzahl der bei ATO-RISK bei einem quantitativen Vorgehen abzuschätzenden Parameter wäre aber wesentlich höher. ■

However, the number of parameters to be estimated for ATO-RISK in a quantitative approach would be much higher. ■

LITERATUR | LITERATURE

[1] Beck, R.: Risikoanalyse mit Risk Score Matrix (RSM) und CSM-Design Targets (CSM-DT), Präsentation, 8. Workshops SiT – Safety in Transportation, 2015
[2] Braband, J.: Risikoanalysen in der Eisenbahn-Automatisierung, Eurailpress, 2005
[3] Braband, J.: Funktionale Sicherheit, in: Fendrich, L. (Hrsg.): Handbuch Eisenbahninfrastruktur, Springer Verlag, 2019, 583-638
[4] Braband, J.; Schäbe, H.: Propagation of uncertainty in railway signaling risk analysis, in: Safety and Reliability of Complex Engineered Systems – Podofillini et al. (Eds), Proc. ESREL 2015, Taylor & Francis Group, London, 2015, 2623-2626
[5] VO (EU) Nr. 402/2013, Durchführungsverordnung (EU) Nr. 402/2013 der Kommission vom 30. April 2013 über die gemeinsame Sicherheitsmethode für die Evaluierung und Bewertung von Risiken und zur Aufhebung der Verordnung (EU) Nr. 352/2009, Amtsblatt der Europäischen Union, ergänzt durch: VO (EU) Nr. 2015/1136, Durchführungsverordnung (EU) Nr. 2015/1136 der Kommission vom 13. Juli 2015 zur Änderung der Durchführungsverordnung (EU) Nr. 402/2013 über die gemeinsame Sicherheitsmethode für die Evaluierung und Bewertung von Risiken; deutsche Ausgabe berichtigt mit Amtsblatt der Europäischen Union L 70 vom 16. März 2016 L121/10 vom 03.05.2013
[6] EBO, Eisenbahn-Bau- und Betriebsordnung vom 8. Mai 1967 (BGBl. II S. 1563), zuletzt geändert durch Artikel 2 der Verordnung vom 5. April 2019 (BGBl. I S. 479)
[7] Projekt NeGSt: Projekt NeGSt (Neue Generation Signaltechnik): Teilbericht AP 2100 – Semi-quantitative Verfahren zur expliziten Risikoabschätzung, http://projekte.fir.de/negst/veroeffentlichungen
[8] Projekt SMARAGT: Abschlussbericht zum Technologieleitprojekt Automatisches Fahren U-Bahn (AGT), Geschäftszeichen Regierung Mittelfranken: 300-3043.1, 1999
[9] ATO OVER ETCS GLOSSARY Draft v1.5
[10] DIN VDE V 0831-100: Elektrische Bahn-Signalanlagen – Teil 100: Risikoorientierte Beurteilung von potenziellen Sicherheitsmängeln und risikoreduzierenden Maßnahmen, 2019
[11] DIN VDE V 0831-101: Elektrische Bahn-Signalanlagen – Teil 101: Semi-quantitative Verfahren zur Risikoanalyse technischer Funktionen in der Eisenbahnsignaltechnik
[12] DIN VDE V 0831-103: Elektrische Bahnsignalanlagen – Teil 103: Ermittlung von Sicherheitsanforderungen an technische Funktionen in der Eisenbahnsignaltechnik, 2020
[13] Bahnanwendungen – Automatischer städtischer schienengebundener Nahverkehr (AUGT) – Sicherheitsanforderungen, DIN EN 62267
[14] DIN IEC 62290-1: Bahnanwendungen – Betriebsleit- und Zugsicherungssysteme für den städtischen schienengebundenen Personennahverkehr – Teil 1: Systemgrundsätze und grundlegende Konzepte, 2014
[15] DIN EN 50129:2019: Bahnanwendungen – Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme – Sicherheitsbezogene elektronische Systeme für Signaltechnik, 2018

AUTOR | AUTHOR

Prof. Dr. Jens Braband
Principal Key Expert
Siemens Mobility GmbH
Anschrift /*Address*: Ackerstraße 22, D-38126 Braunschweig
E-Mail: jens.braband@siemens.com