

Risikoanalyse für die Hinderniserkennung beim Automatischen Fahren

Risk analyses for obstacle detection in automatic driving

Jens Braband | Luisa Lindner | Franziska Rexin

Das vom Deutschen Zentrum für Schienenverkehrsforschung (DZSF) beauftragte Projekt ATO-RISK hat das Ziel, „Risikoakzeptanzkriterien für das automatisierte Fahren auf der Schiene“ abzuleiten. Dabei liegt der Fokus in diesem Beitrag auf der Risikoanalyse zum Funktionsblock „Verhindern des Zusammenstoßes mit Gegenständen oder Personen bei automatisierten Systemen“. Dazu werden nach einer kurzen Zusammenfassung des grundsätzlichen Vorgehens des ATO-RISK Projekts zunächst die funktionale Gliederung dieses Funktionsblocks erläutert und anschließend die Besonderheiten der Risikoanalyse nach der Methodik der DIN VDE V 0831-103 herausgearbeitet. Abschließend wird eine Übersicht der Ergebnisse aus der Risikoanalyse präsentiert und diskutiert. Die Risikoanalyse sollte nicht mit der Sicherheitsanalyse verwechselt oder vermischt werden, insbesondere werden keine speziellen Lösungsarchitekturen bewertet und keine Ableitung von Sicherheitszielen für technische Komponenten durchgeführt. Alle Betrachtungen beziehen sich auf die Funktionale Sicherheit unter Bezug auf die CENELEC-Normen. Andere Sicherheitsaspekte, explizit Cybersicherheit, Arbeitsschutz und dergleichen sind nicht Betrachtungsgegenstand. Weiter ist eine Untersuchung der Leistungsfähigkeit von Menschen in Bezug auf Sinneswahrnehmung und Verarbeitungsfähigkeit von Informationen nicht Bestandteil des Projekts. Diese erfolgt im Parallelprojekt ATO-SENSE.

1 Ansatz des ATO-RISK-Projekts

Im Rahmen des ATO-RISK-Projekts wird zunächst ein System für den automatisierten Bahn-/Fahrbetrieb mit Automatisierungsgrad (GoA) 3 (fahrerloser Betrieb) sowie GoA 4 (ohne Betriebspersonal an Bord) definiert. Grundlage der Systemdefinition bildet eine vollständige Funktionsliste, die die Gesamtfunktionalität unter den abgesteckten Randbedingungen festhält. Dabei muss die Systemdefinition auf einer geeigneten funktionalen Ebene durchgeführt werden, die mit der CSM-VO [7] sowie der DIN VDE V 0831-103 [10] als gewählte Methode für explizite Risikoanalyse kompatibel ist. Je nach Anwendungsfall sind die angenommenen Randbedingungen zu prüfen und unter Umständen neu zu bewerten, hierzu liefert ATO-RISK einen Anwenderleitfaden. Mit dem Rückgriff auf bewährte Nahverkehrsnormen und der Ergänzung aus bestehenden Betriebsvorschriften oder Normen wird ein systematischer Ansatz verfolgt, der sowohl eine Vollständigkeit für die in ATO-RISK genannten Funktionsumfänge als auch die Kompatibilität mit Bestandstechniken gewährleistet [1].

Wie in der Vorgehensweise [5] beschrieben, wird für die explizite Risikoanalyse die CSM-VO-konforme Norm DIN VDE V 0831-103 [10] angewendet. Die Bewertung verschiedener Szenarien er-

The ATO-RISK project, commissioned by the German Centre for Rail Traffic Research (DZSF), aims to derive “risk acceptance criteria for automated driving on railways”. This article focuses on the risk analysis for the “preventing collisions with objects or people in automated systems” function block. After a short summary of the ATO-RISK project’s basic approach, this function block’s functional structure is first explained and the special risk analysis features according to the DIN VDE V 0831-103 methodology are then elaborated. Finally, an overview of the risk analysis results is presented and discussed. Risk analysis should not be confused or mixed up with safety analysis. In particular, no special solution architectures are evaluated and no safety targets are derived for technical components. All the considerations refer to functional safety with reference to the CENELEC-standards. Other safety aspects, explicitly cyber security, occupational health and safety, etc. are likewise not the subject of consideration. Furthermore, an investigation into the performance of humans in terms of their sensory perception and information processing ability is not part of the project and is being carried out in the parallel ATO-SENSE project.

1 The ATO-RISK project’s approach

A system for automated railways/driving with Grade of Automation (GoA) 3 (driverless operations) or GoA 4 (without staff on board) has been initially defined as part of the ATO-RISK project. The system definition is based on a complete function list that specifies the overall functionality under the defined boundary conditions. The system definition must be carried out at a suitable functional level that is compatible with the CSM-VO [7] and DIN VDE V 0831-103 [10] as the selected methods for explicit risk analysis. The assumed boundary conditions must be checked and possibly re-evaluated depending on the application and ATO-RISK provides a user guide for doing so. A systematic approach that ensures both completeness for the functional scope specified in ATO-RISK and compatibility with the existing technologies [1] is pursued with recourse to the proven local transport standards and supplementation from existing operating regulations or standards.

As described in the procedure [5], the CSM-VO compliant standard DIN VDE V 0831-103 [10] is used for the explicit risk analysis. This semi-quantitative approach means that the evaluation of different scenarios is carried out using a Risk

Sicherheitsanforderung 1/h Safety requirement 1/h	Risk Score Matrix Risk Score Matrix						
keine none							
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 Accident class						

Tab. 1: Beispiel für eine Risk Score Matrix nach DIN VDE V 0831-103

Tab. 1: An example of a Risk Score Matrix according to DIN VDE V 0831-103

Quelle / Source: [10]

folgt nach diesem semiquantitativen Ansatz mithilfe einer Risk Score Matrix (RSM), die das erwartete Schadensausmaß qualitativ nach Unfallklassen differenziert. Als Risikoakzeptanzkriterium wird je nach Funktion eine explizite Risikoanalyse durchgeführt oder auf existierende Regelwerke oder Referenzsysteme zurückgegriffen. Aufgrund des frühen Entwicklungsstadiums des automatischen Fahrens im Regional- und Fernverkehr ist die Verfügbarkeit von Regelwerk sowie geeigneter Referenzsysteme jedoch eingeschränkt. Nach Prüfung der Anwendbarkeit kann für einzelne Funktionen das automatische Fahren im Nahverkehr als Referenzsystem herangezogen werden. Für eine umfangreichere Erläuterung des methodischen Vorgehens von ATO-RISK soll auf [5] verwiesen werden.

Im Folgenden wird die Anwendung des beschriebenen Vorgehens beispielhaft an dem Funktionsblock „Verhindern des Zusammenstoßes mit Hindernissen und Personen“ gezeigt. Im Rahmen der funktionalen Systemdefinition werden in Übereinstimmung mit [10] die Hindernisdetektion, die Ableitung einer angemessenen Reaktion und schließlich die Auslösung dieser Reaktion getrennt betrachtet. Entsprechend ist der übergeordnete Funktionsblock Verhindern des Zusammenstoßes mit Hindernissen und Personen unter Berücksichtigung der funktionalen Basiselemente weiter untergliedert in Unterfunktionen (Bild 1). Ziele der Aufteilung sind eine schärfer differenzierte Anforderungsableitung und Analyse der zugehörigen Barrieren anhand von Szenarien und Schadensausmaß.

Gegenstand der Betrachtung sind Netze, bei denen keine durchgängige Umzäunung der freien Strecke vorausgesetzt wird. Allerdings wird eine bauliche Abgrenzung oder infrastrukturelle Sicherung an ausgewählten Gefahrpunkten angenommen, an denen die Wahrscheinlichkeit von kreuzenden Personen erhöht ist. Im Rahmen von ATO-RISK ist ein Gefahrpunkt definiert als ein Punkt entlang der Strecke, an dem Hindernisse mit erhöhter Wahrscheinlichkeit oder systematisch auftauchen, wie z.B. bekannte „Trampelpfade“ oder Brücken. Zudem ist an Gefahrpunkten neben der erhöhten Auftrittswahrscheinlichkeit teilweise mit besonders gefährlichen Hindernissen zu rechnen, z.B. mit einem Baufahrzeug an einer Baustelle oder einem eingeschlossenen Fahrzeug an einem Bahnübergang. Die Gefahrpunkte Bahnsteig und Bahnübergang werden von ATO-RISK in separaten Unterfunktionen betrachtet (Bild 1). Bei der Betrachtung der (frei-

Score Matrix (RSM), which qualitatively differentiates the expected extent of damage according to the accident classes. Either an explicit risk analysis is performed or existing sets of rules and regulations or reference systems are used as the risk acceptance criteria depending on the function. However, the availability of rules and regulations as well as suitable reference systems is limited due to the early stage of automated driving development in regional and long-distance traffic. Automatic driving in local traffic can be used as a reference system for individual functions once its applicability has been checked. Reference should be made to [5] for a more comprehensive explanation of the ATO-RISK methodological approach.

The application of the described procedure is exemplified by the preventing collisions with obstacles and people function block in the following. Obstacle detection, the derivation of the appropriate reaction and finally the triggering of this reaction are considered separately within the framework of the functional system definition in accordance with [10]. Accordingly, the superordinate function block preventing collisions with obstacles and people is further subdivided into sub-functions that take into consideration the basic functional elements (fig. 1). The objective of this subdivision is a more sharply differentiated requirement derivation and analysis of the associated barriers based on scenarios and the extent of damage.

The object under consideration is networks where no continuous fencing of the free route is assumed. However, structural fencing or infrastructural protection is assumed at selected danger points where the probability of people crossing is higher. A danger point is defined within the context of ATO-RISK as a point along the route where obstacles are more likely or systematic to occur, such as known trails or bridges. Moreover, particularly dangerous obstacles are sometimes to be expected at danger points in addition to the increased probability of occurrence, for example a construction vehicle at a construction site or a trapped vehicle at a railroad crossing. ATO-RISK considers the platform and level crossing danger points in separate sub-functions (fig. 1). When considering a (free) track, the assumption is that the occurrence of any obstacles is random to a first approximation. It is assumed that the rail-

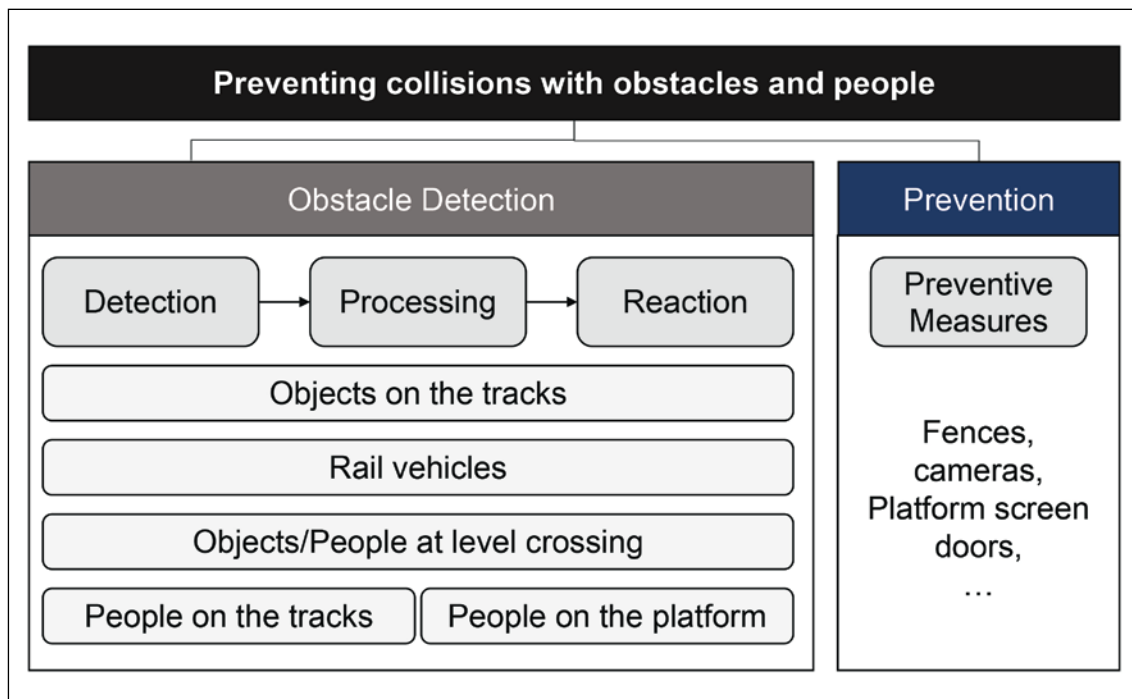


Bild 1: Gliederung des Funktionsblocks 3 Fahrwegbeobachtung zur Verhinderung des Zusammenstoßes mit Hindernissen und Personen

Fig. 1: The structure of the track monitoring to prevent collisions with obstacles and people function block 3

Quelle / Source: [1]

en) Strecke gilt die Annahme, dass das Auftreten der Hindernisse in erster Näherung zufällig ist.

Es wird davon ausgegangen, dass die Bahninfrastruktur, angrenzende Bauwerke sowie die Fahrzeuge des Bahnbetriebs gemäß baulichen Verordnungen und Konstruktionsregeln errichtet wurden und ordnungsgemäß nach Regelwerk gewartet werden.

Für die Bewertung der Hindernisdetektion werden die folgenden Hinderniskategorien als Unterscheidungs- und Klassifizierungsansätze definiert:

1. Absichtlich platzierte Hindernisse: Security im Sinne von Schutz vor Sabotage ist nicht Betrachtungsgegenstand von ATO-RISK. Aufgrund möglicher Auswirkungen von Sabotage auf den Bahnbetrieb wie auch möglicher Schäden ist die Detektion von Objekten dieser Klasse sinnvoll und sollte auch bestmöglich ausgeführt werden. Eine Auslegung der Sicherheitsanforderung der Hindernisdetektion auf diese Vorfälle ist jedoch nicht sinnvoll bzw. gar nicht möglich. Ergänzend dazu ist zu beachten, dass auch Suizide außerhalb des Betrachtungsumfangs liegen und nicht zur Ableitung der Sicherheitsanforderungen herangezogen werden, da absichtlich herbeigeführte Personenschäden in den Umfang der Security fallen.
2. Vorhersehbarer Missbrauch der Eisenbahnanlagen: Sicherheitsnormen wie [11] verlangen, vernünftigerweise vorhersehbare Fehlanwendungen zu betrachten, d.h. die missbräuchliche Nutzung muss vorhersehbar sein und einen irgendwie gearteten Nutzen versprechen, z.B. Abkürzung eines Weges durch missbräuchliches Betreten von Bahnanlagen. Weitere Beispiele könnten sein: unbefugtes Eindringen, Eisenbahnsurfen, Werfen von Gegenständen von Brücken auf die Strecke. Die Detektion entsprechender Objekte bzw. Personen ist nach [9] notwendig und sollte auch bestmöglich ausgeführt werden, allerdings um die Verfügbarkeit des Betriebs zu erhöhen. Eine Auslegung der Sicherheitsanforderung der Hindernisdetektion auf diese Vorfälle ist ebenfalls nicht sinnvoll, sondern es wird erwartet, dass die Detektion solcher Hindernisse durch die Anforderungen zur Detektion anderer Hindernisse ausreichend mit abgedeckt wird.

road infrastructure, adjacent structures, as well as the railroad vehicles have been built in accordance with the building regulations and design rules and have been properly maintained in accordance with the rules and regulations.

The following obstacle categories have been defined as differentiation and classification approaches for obstacle detection evaluation:

1. Intentionally placed obstacles: Security in the sense of protection against sabotage is not a subject of ATO-RISK. The detection of this class of objects is reasonable and should also be executed in the best way possible. However, designing an obstacle detection safety requirement for these incidents is not reasonable or even possible. In addition, it should be noted that suicides also fall outside the scope of consideration and are not used to derive the safety requirements, since deliberately caused personal injuries fall within the scope of security.
2. Foreseeable misuse of railroad facilities: Safety standards such as [11] require reasonably foreseeable misuses to be considered. The misuse must be foreseeable and promise some type of benefit, e.g. shortening a route through the misuse of rail facilities. Other examples could include: trespassing, railroad surfing or throwing objects from bridges onto the track. According to [9], the detection of corresponding objects or people is necessary and should also be carried out as best as possible, but in a manner that increases the availability of operations. It is also not reasonable to design an obstacle detection safety requirement for these incidents, but it is expected that the detection of any such obstacles has been sufficiently covered by the requirements for the detection of other obstacles.
3. Unintentional obstacles:
 - a. Environmental impacts: rock falls, landslide, avalanches, floods, etc.: The detection of the relevant objects is reasonable and should also be carried out in the best way possible. In addition, it is advisable to provide supplementary measures at discrete danger points, e.g. by means of isolated structural boundaries or technical monitoring. Technical monitoring devices already exist for special cas-

3. Unbeabsichtigt auftretende Hindernisse:

- a. Umwelteinflüsse: Steinschlag, Erdbeben, Lawinen, Hochwasser etc.: Die Detektion entsprechender Objekte ist sinnvoll und sollte auch bestmöglich ausgeführt werden. Zusätzlich ist es empfehlenswert, ergänzende Maßnahmen an diskreten Gefahrpunkten, z. B. durch vereinzelte bauliche Abgrenzungen oder durch technische Überwachung, vorzusehen. So existieren bereits technische Überwachungseinrichtungen für spezielle Fälle, z. B. Lawinen etc. Die Sicherheitsanforderungen der Hindernisdetektion ergeben sich daher aus den in diesen Fällen anzuwendenden Regelwerken.
- b. Gegenstände: Die folgenden Gegenstände sind laut Auswertung der Unfallereignisdatenbank zu erwarten [2]:
 - I. Tiere (einzeln bzw. Herde)
 - II. Fahrzeuge (Autos, Bagger, Fahrräder etc.)
 - III. Sonstige Objekte (z. B. Steine, Eisabwurf)
- c. Systeminterne Objekte: Hemmschuh, Schienenfahrzeuge Gleissperre etc.
- d. Menschen, z. B. Bauarbeiter; aufgrund von Fehlverhalten (Abgrenzung zu vorhersehbarem Missbrauch).

Hindernisse / Objekte gemäß Kategorie 3 b, c und d dienen als Auslegungsgrundlage für die Bewertung der Hinderniserkennung.

Im Rahmen des ATO-RISK-Projekts wurde für die Bewertung von Funktionen für den automatischen Bahnbetrieb (GoA 3/4) ein allgemeiner Anwenderleitfaden entwickelt (vgl. ATO-RISK-Abschlussbericht [1]). Dieser schildert das grundsätzliche Vorgehen bei der Risikoanalyse entsprechender Funktionen und kann für zukünftige Bewertungen herangezogen werden. Dabei ist unter anderem die Anwendbarkeit der Methodik der [10] für die zu bewertenden Funktionen zu prüfen. Für den in diesem Beitrag betrachteten Funktionsblock „Verhindern des Zusammenstoßes mit Objekten und Personen“ wird primär die explizite Risikoanalyse nach der Methodik der DIN VDE V 0831-103 [10] als Risikoakzeptanzkriterium herangezogen.

Bild 2 stellt die Schritte zur Ableitung von Sicherheitsanforderungen auf Basis der Methode nach DIN VDE V 0831-103 [10] dar. Zusätzlich werden die jeweiligen Besonderheiten zur Anwendbarkeit der Methodik im Kontext von ATO-RISK für Anwendungsfälle von höheren Automatisierungsgraden adressiert, welche in den Abschnitten 2–6 näher erläutert werden.

2 Funktion und Schutzziel

Im ersten Schritt müssen die Funktion und das Schutzziel klar definiert werden. Schutzobjekte sind beispielsweise Zug, Reisende, externe Personen oder Betriebspersonal (bei GoA 3 Zugpersonal). Für die Funktion "Verhindern des Zusammenstoßes mit Personen" wird davon ausgegangen, dass primär die externen Personen im Lichtraumprofil (außerhalb) des Zuges zu schützen sind, da die wirkenden Kräfte für Reisende im Zug bei einem Aufprall vernachlässigbar klein angenommen werden.

3 Randbedingungen und Einschränkungen

Zusätzlich sollten für die Funktionen entsprechende Randbedingungen definiert sein, damit die Ableitung der Barriere und die Anwendbarkeit der Unfallklassen der DIN VDE V 0831-103 [10] begründet werden können. Beispielsweise ist im Fall, dass ein Betreiber eine Umzäunung der Strecke vorsieht, zu prüfen, ob es sich bei der Umzäunung um eine Risikoreduktion oder einen vollständigen Schutz handelt.

es, e.g. avalanches, etc. The obstacle detection safety requirements are therefore derived from the rules and regulations to be applied in these cases.

- b. Objects: The following objects are to be expected according to the evaluation of the accident event database [2]:
 - I. animals (single or herd)
 - II. vehicles (cars, excavators, bicycles, etc.)
 - III. other objects (i.e. stones, falling ice)
- c. Internal system objects: stop block, rail vehicles, track lock etc.
- d. People, e.g. construction workers; due to misconduct (a differentiation from foreseeable misuse).

The obstacles / objects according to categories 3 b, c and d serve as the design basis for the evaluation of obstacle detection.

A general user guide has been developed for the assessment of functions for automatic railroad operations (GoA 3/4) as part of the ATO-RISK project (cf. ATO-RISK final report [1]). It describes the basic risk analysis procedures for corresponding functions and can be used for future assessments. The applicability of the methodology of [10] to the functions under assessment must be checked, amongst other things. The explicit risk analysis for the preventing collisions with objects and people function block considered in this article is primarily used as a risk acceptance criterion according to the methodology of DIN VDE V 0831-103 [10].

Fig. 2 shows the steps for deriving the safety requirements based on the method according to DIN VDE V 0831-103 [10]. In addition, the respective special features for the applicability of the methodology within the context of ATO-RISK for use cases at higher grades of automation have also been addressed, as explained in more detail in the sections 2–6.

2 Function and protection goal

The function and the protection goal must be clearly defined in the first step. The objects of protection are, for example, the train, the passengers, other people or the operating personnel (train personnel for GoA 3). The preventing collisions with people function primarily assumes that any other people in the train's loading gauge (outside) are to be protected, since the forces acting on the passengers in the train in the event of a collision are negligible.

3 The boundary conditions and restrictions

In addition, appropriate boundary conditions should also be defined for the functions so that the derivation of the barrier and the applicability of the accident classes from DIN VDE V 0831-103 [10] can be justified. For example, in the case where an operator provides fencing on the line, a check must be made to see whether the fencing in question constitutes risk reduction or complete protection.

4 Typical scenarios

When defining boundary conditions, it makes sense to perform a functional subdivision into different scenarios. A differentiation should be made between freight and passenger trains. In many cases, different accident classes result for these two train classes since there are no people on board a freight train to be endangered in GoA 3 or GoA 4 operations. If both train class-

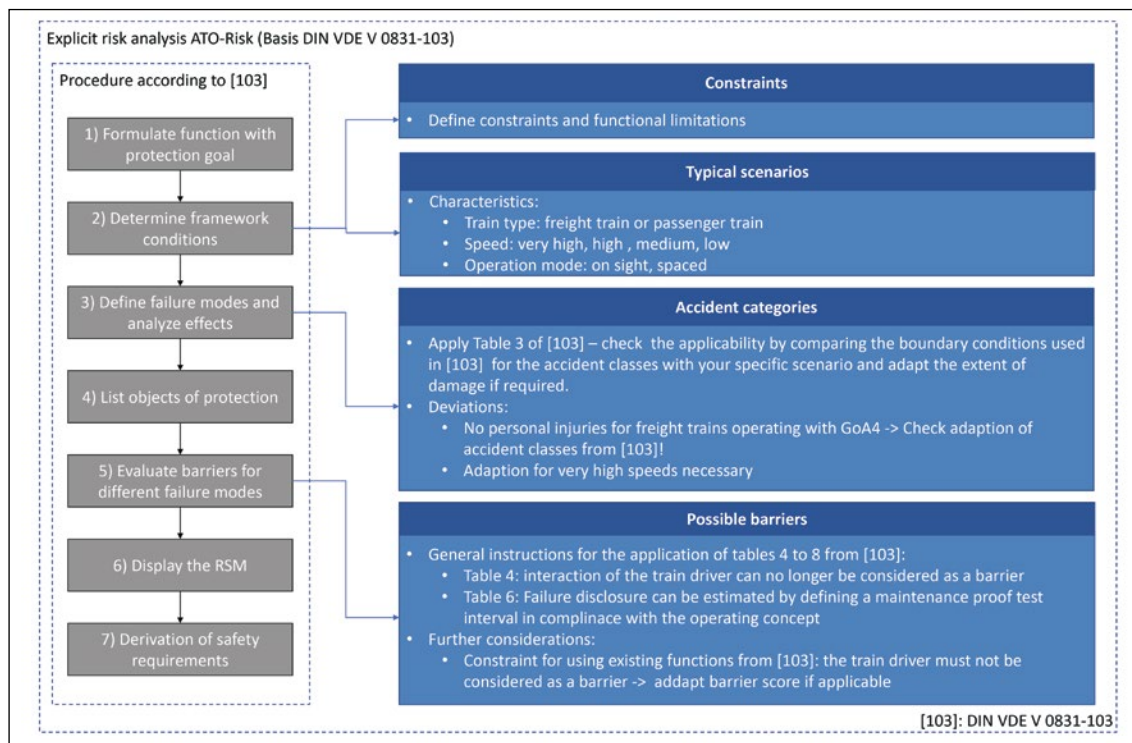


Bild 2: Explizite Risikoanalyse ATO-RISK

Fig. 2: The ATO-RISK explicit risk analysis

Quelle / Source: [1]

4 Typische Szenarien

Bei der Definition von Randbedingungen ist es sinnvoll, eine funktionale Unterteilung in verschiedene Szenarien durchzuführen. Differenziert werden sollte dabei zwischen Güter- und Reisezügen. Für diese beiden Zugklassen ergeben sich in vielen Fällen unterschiedliche Unfallklassen, da im GoA 3- bzw. GoA 4-Betrieb keine Personen an Bord eines Güterzuges gefährdet werden können. Würde man beide Zugklassen somit gemeinsam bewerten, würden zu strenge Sicherheitsanforderungen an Güterzüge entstehen.

Darüber hinaus ist es sinnvoll, in der Funktionsbewertung verschiedene Geschwindigkeitskategorien zu unterscheiden. I.d.R. gelten für hohe oder sehr hohe Geschwindigkeiten die strengsten Sicherheitsanforderungen. Sollte jedoch in einem zukünftigen Betriebsfall vorgesehen sein, nur niedrige oder mittlere Geschwindigkeiten zu fahren (beispielsweise im Fall von S-Bahnnetzen), würden durch die pauschale Annahme hoher bzw. sehr hoher Geschwindigkeiten überdimensionierte Sicherheitsanforderungen für den vorliegenden Anwendungsfall entstehen. Um die Anwendbarkeit der Unfallklassen der DIN VDE V 0831-103 zu gewährleisten, müssen die gleichen Geschwindigkeitskategorien wie in [10] verwendet werden.

Die Festlegung der getrennt zu bewertenden Geschwindigkeitsklassen ist zudem an das Schutzobjekt anzupassen. Bei der Erkennung von Personen im Gleisbereich kann beispielsweise argumentiert werden, dass bei der entsprechenden Person unabhängig von der Geschwindigkeit tödliche Verletzungen angenommen werden müssen. Somit muss in derartigen Einzelfällen eine feingliedrige Unterteilung in Geschwindigkeitsklassen nicht zielführend sein. Dies ist im jeweiligen Einzelfall zu prüfen.

Eine weitere Unterscheidung nach dem Verfahren der Zugfolgesicherung bei Fahren auf Sicht bzw. Fahren im Raumabstand ist zusätzlich sinnvoll, um an die Betriebsart angepasste Barrieren heranziehen zu können. Beispielsweise kann somit bei der Hindernisdetektion von Schienenfahrzeugen auf der Strecke bei einem Fahren im Raumabstand die Gleisfreimeldung als Barriere heran-

es were assessed together, this would result in excessively strict safety requirements for freight trains.

In addition, it makes sense to subdivide the different speed categories in the function evaluation. Usually, the strictest safety requirements apply to high or very high speeds. However, if a future operating case plans to run at only low or medium speeds (for example in the case of urban rail networks), the assumption of high or very high speeds would result in overdimensioned safety requirements for the present application. The same speed categories as in [10] must be used in order to ensure the applicability of the DIN VDE V 0831-103 accident classes. The determination of the speed classes to be separately evaluated must also be adapted to the object of protection. When detecting people in the track area, for example, it can be argued that fatal injuries must be assumed for the given person regardless of the speed. Thus, a fine-grained subdivision into speed classes may not be expedient in such individual cases. This must be examined in each individual case.

A further differentiation according to the train detection method for driving on sight or driving at a distance is also useful in order to enable the use of barriers adapted to the operating mode. For example, in the case of obstacle detection involving rail vehicles on the track, the track clearance message can be used as a barrier when driving at a distance, which means that the safety requirements for the obstacle detection systems can be relaxed.

5 Accident classes

When defining the types of failure and analysing the corresponding effects, the matching accident classes are assigned to the event types using the methodology from the [10] standard. The assignment of accident classes to driverless or unaccompanied train operations must be adapted here since the [10] methodology refers to operations with a driver and there could be fewer personal injuries in GoA 4 in particular.

gezogen werden, wodurch die Sicherheitsanforderungen an die Systeme zur Hinderniserkennung gelockert werden können.

5 Unfallklassen

Bei der Definition der Ausfallarten und Analyse der entsprechenden Auswirkungen werden bei Anwendung der Methodik aus der Norm [10] den Ereignisarten entsprechende Unfallklassen zugewiesen. Dabei ist die Zuweisung der Unfallklassen an den fahrerlosen bzw. unbegleiteten Zugbetrieb anzupassen, da sich die Methodik der [10] auf den Fahrbetrieb mit Triebfahrzeugführer bezieht und es insbesondere in GoA 4 weniger Personenschäden geben könnte.

Für neuartige Antriebstechnologien, wie beispielsweise Batterie- oder Wasserstoffantriebe, hat eine separate Prüfung zu erfolgen, ob die Zuordnung der typischen Ereignisarten zu den maßgeblichen Schadensausmaßen bzw. Unfallklassen gemäß [10] weiterhin zulässig ist. Dies liegt daran, dass neuartige Technologien nicht in die Erstellung der Unfallklassen in [10] eingeflossen sind.

6 Barrieren

Für die Bewertung von Barrieren können die Tab. 4 bis 8 aus [10] herangezogen werden.

Bei der Bewertung menschlicher Handlungen (Tab. 4 aus [10]) ist anzumerken, dass der Triebfahrzeugführer in GoA 3 und GoA 4

A separate examination must be carried out for new types of drive technologies, such as battery or hydrogen drives, in order to determine whether the assignment of the typical event types to the relevant damage dimensions or accident classes is still permissible according to [10]. This is due to the fact that novel technologies have not been included in the accident classes created in [10].

6 Barriers

Tab. 4 to 8 from [10] can be used for the evaluation of barriers. When evaluating human actions (tab. 4 from [10]), it should be noted that the train driver can no longer act as a barrier in GoA 3 and GoA 4. However, this table can be used, for example, for outside people who can react to an approaching train and, if necessary, take evasive action.

Furthermore, a demand rate with a failure revelation as a barrier can be evaluated based on tab. 6 in [10]. In this case, a proof test interval must be defined depending on the operator's operating concept. Given the scope of the proof tests, it makes sense for them to coincide with more extensive maintenance work. A maximum proof test interval of once a year is assumed under ATO-RISK. Tab. 1 shows the analysis for two different scenarios for the detection of groups of people (category 3d) depending on the speed and the possibility of the people avoiding the accident if warned.

Systems for Automatic Train operation Drive SWing DRS-10 ATO over ETCS

- Interoperable and connected
- Following latest ERTMS / ETCS specifications
- Ready for freight trains
- Increasing traffic density and functionality
- Energy and CO2 emission savings 10-30%
- Ready for ETCS Level 3
- ATO GoA4 capability

AŽD Praha - leader in ATO for railways
ATO GoA2 in operation for 25 years, @300+ vehicles



www.azd.cz



nicht mehr als Barriere wirken kann. Herangezogen werden kann diese Tabelle jedoch beispielsweise für außenstehende Personen, welche z.B. auf einen sich annähernden Zug reagieren und ggf. entsprechend ausweichen können.

Weiterhin ist auf Basis der Tab. 6 in [10] die Bewertung der Anforderungsrate mit Ausfalloffenbarung als Barriere möglich. Dabei ist ein Proof-Test-Intervall abhängig vom Betriebskonzept des Betreibers zu definieren. Wegen des Umfangs der Proof-Tests ist es sinnvoll, dass diese mit umfangreicheren Wartungsarbeiten zusammenfallen. Im Rahmen von ATO-RISK wird ein Proof-Test-Intervall von maximal einmal jährlich angenommen. Tab. 1 zeigt eine Analyse für zwei verschiedene Szenarien bei der Erkennung von Personengruppen (Kategorie 3d) in Abhängigkeiten von Geschwindigkeit und der Möglichkeit der Personen, bei Erkennung den Unfall noch zu vermeiden.

Das beschriebene Vorgehen des Anwenderleitfadens wurde im Rahmen des ATO-RISK-Projekts für alle geeigneten Funktionen des erläuterten Funktionsblocks „Verhindern des Zusammenstoßes mit Objekten und Personen“ durchgeführt [1]. Eine Übersicht der Ergebnisse dieser Analysen wird im folgenden Abschnitt dargestellt.

7 Ergebnisübersicht

Aus Gründen der besseren Übersichtlichkeit werden nicht alle Ergebnisvarianten, welche sich aus den verschiedenen Szenarien ergeben, einbezogen. Zudem werden nur die wichtigsten Randbedingungen angegeben. Die vollständigen Ergebnisse finden sich in [1].

Außerdem wird auch eine informative SIL-Einstufung abgegeben, da diese von Anwendern häufig als erste Orientierung gewünscht wird. Diese Einstufung setzt voraus, dass die betroffenen Funktionen komplett und ohne weitere SIL-Zuteilung nach diesen Sicher-

Nummer	Funktion	Randbedingungen	Sicherheitsanforderung	SIL-Stufe (informativ)
3.1.1.1	Hindernisdetektion von Gegenständen auf der Strecke	Reisezug (hohe Geschwindigkeit) Proof-Test 1 Jahr	$3 \times 10^{-6}/h$	SIL1
		Güterzug (hohe Geschwindigkeit) Proof-Test 1 Jahr	Keine quantitative Vorgabe	Basisintegrität
		Güterzug (hohe Geschwindigkeit)	$10^{-5}/h$	SIL1
3.1.1.2	Hindernisdetektion von Schienenfahrzeugen auf der Strecke	Reisezug (Fahren auf Sicht)	$3 \times 10^{-7}/h$	SIL2
3.1.1.3	Hindernisdetektion im Kreuzungsbereich Straße/Schiene	Nur bis 160 km/h zulässig	$10^{-7}/h$	SIL3
3.1.1.4.1	Hindernisdetektion von Personen im Gleisbereich	Mittlere und hohe Geschwindigkeit Proof-Test 1 Jahr	$3 \times 10^{-7}/h$	SIL2
3.1.1.4.2	Hindernisdetektion von Personen im Bahnsteiggleisbereich	Niedrige Geschwindigkeit Keine Durchfahrten	$10^{-5}/h$	SIL1
		Mit Durchfahrten	$10^{-6}/h$	SIL2
3.2.1	Überwachen von Infrastrukturelementen		Einhaltung Technischer Regelwerke	-
3.2.1	Überwachen von Umwelteinflüssen		Ggf. spezifische Detektionssysteme an Gefahrpunkten	-

Tab. 2: Zusammenstellung der essenziellen Ergebnisse

The user guide's described procedure has been carried out for all the suitable functions of the explained "preventing collision with objects and people" function block [1] within the ATO-RISK project. An overview of the results of these analyses is presented in the following section.

7 An overview of the results

Not all the outcome variants resulting from the different scenarios have been included in tab. 2 for the sake of clarity. In addition, only the most important boundary conditions have been given. The complete results can be found in [1].

Additionally, an informative SIL classification has also been provided, as this is often requested by users as a first orientation. This classification assumes that the affected functions would be developed completely and without any further SIL assignment according to these safety requirements, i.e. that there is no redundancy or diversity with other functions or within the function [11].

8 Summary and discussion

This article has been able to demonstrate the fundamental suitability of the [10] methodology for the risk analysis of a GoA 3/4 using the example of the preventing collisions with obstacles and people function. Furthermore, the presented evaluation has clarified the high importance of individual boundary condition analyses for the individual functions. As a result, safety requirements are obtained for many variants of obstacle detection which fall in the range from SIL1 to SIL2 and even up to SIL3 in exceptional cases, such as the danger zone clearance at a level crossing.

Number	Function	Boundary condition	Safety Requirement	SIL-Level (informative)
3.1.1.1	Obstacle detection of objects on the track	Passenger train (high speed) Proof-test 1 year	$3 \times 10^{-6}/h$	SIL1
		Freight train (high speed) Proof-test 1 year	No quantitative target	Basic integrity
		Freight train (high speed)	$10^{-5}/h$	SIL1
3.1.1.2	Obstacle detection of rail vehicles on the track	Passenger train (driving on sight)	$3 \times 10^{-7}/h$	SIL2
3.1.1.3	Obstacle detection in the road/rail intersection area	Only permitted up to 160 km/h	$10^{-7}/h$	SIL3
3.1.1.4.1	Obstacle detection of people in the track area	Medium and high speed Proof-test 1 year	$3 \times 10^{-7}/h$	SIL2
3.1.1.4.2	Obstacle detection of people in the platform track area	Low speed No passes	$10^{-5}/h$	SIL1
		With passes	$10^{-6}/h$	SIL2
3.2.1	Monitoring of infrastructure elements		Compliance with technical regulations	-
3.2.1	Monitoring environmental influences		If necessary, specific detection systems at danger points	-

Tab. 2: The compilation of the essential results

heitsanforderungen entwickelt würden, d. h., dass es keine Redundanz oder Diversität mit anderen Funktionen oder innerhalb der Funktion gibt [11].

8 Zusammenfassung und Diskussion

Am Beispiel der Funktion „Vermeiden des Zusammenstoßes mit Hindernissen und Personen“ konnte im Rahmen dieses Beitrags die grundsätzliche Eignung der Methodik nach [10] für die Risikoanalyse eines GoA 3/4 gezeigt werden. Des Weiteren hat die dargestellte Bewertung den hohen Stellenwert der individuellen Analyse der Randbedingungen für die einzelnen Funktionen verdeutlicht. Im Ergebnis erhält man für viele Varianten der Hinderniserkennung Sicherheitsanforderungen, die sich im Bereich von SIL1 bis SIL2 bewegen, in Ausnahmefällen, wie der Gefahrenraumfreimeldung am Bahnübergang, auch bis zu SIL3 reichen. Insgesamt kann festgestellt werden, dass der Ansatz der Risikoanalyse nach CSM-VO sich als sehr vorteilhaft herausgestellt hat, da bei Verwendung der Risikoakzeptanzprinzipien „Regelwerk“ bzw. „Referenzsystem“ bestehende Vorgaben übernommen werden konnten. Zu den Regelwerken zählten insbesondere auch Bauvorschriften, Vorschriften zum Brandschutz oder zum Gefahrguttransport. Außerdem wurde bei den Teilfunktionen, für die weder ein Regelwerk vorlag noch ein Referenzsystem existierte, der Vorteil einer semiquantitativen Risikoanalyse auf Grundlage von DIN VDE V 0831-103 gezeigt.

Overall, it can be stated that the approach to risk analysis according to CSM-VO has turned out to be very advantageous, since existing specifications can be adopted when using the “rules and regulations” or “reference system” risk acceptance principles. The rules and regulations particularly included the building regulations, fire protection regulations or regulations on the transportation of hazardous goods. In addition, the advantage of a semi-quantitative risk analysis based on DIN VDE V 0831-103 has also been demonstrated for those sub-functions, for which neither a set of rules nor a reference system existed.

Semi-quantitative methods require the estimates to be conservative. This could possibly lead to higher safety requirements than, for example, when a quantitative method is used. However, it is questionable whether this argument is true or at least if one would show the statistical uncertainty in quantitative methods instead of the more commonly use processing of mean values. It has been shown [6] that, provided the data uncertainty has been taken into account correctly, it propagates statistically to such an extent that it exceeds an order of magnitude in the result even with a just few parameters, i.e. not even the derived SIL can be unambiguously determined. However, the number of parameters to be estimated in ATO-RISK in a quantitative approach would be much higher. In addition, the results could become route or location dependent. However, this contradicts the approach practiced in Germany

RAILWAY DIAGNOSTIC AND MONITORING CONFERENCE 2023

20TH - 21ST APRIL 2023

CONTINENTAL PARK HOTEL, LUCERNE 

**REGISTER
NOW**



REGISTER NOW AT:
WWW.EURAILPRESS.DE/EVENTS



Bei semiquantitativen Methoden wird 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 [6], dass sich schon bei wenigen Parametern bei korrekter Berücksichtigung die Unsicherheit der Daten statistisch so stark fortpflanzt, dass sie im Ergebnis eine Größenordnung übersteigt, d. h. nicht einmal der abgeleitete SIL kann eindeutig bestimmt werden. Die Anzahl der bei ATO-RISK bei einem quantitativen Vorgehen abzuschätzenden Parameter wäre aber wesentlich höher. Außerdem könnten die Ergebnisse strecken- oder ortsabhängig werden. Dies widerspricht aber dem in Deutschland praktizierten Ansatz, dass die Ergebnisse von Risikoanalysen generisch sein sollten, um in der betrieblichen Umsetzung möglichst viel Flexibilität zu gewinnen.

Wenn sich die Randbedingungen eines Projekts stark von den in dieser Analyse getroffenen Anforderungen unterscheiden, z. B., weil Gefahrenpunkte eingezäunt sind oder die Randbedingungen gar nicht explizit betrachtet wurden, z. B. Rangierbetrieb oder Abstellanlage, so ist zu empfehlen, die Risikoanalyse unter Beachtung des Anwenderleitfadens anzupassen. So können angepasste, in der Regel schwächere, Sicherheitsintegritätsanforderungen abgeleitet werden. ■

where the results of any risk analyses should be generic in order to gain as much flexibility as possible in their operational implementation.

If the boundary conditions of a project differ greatly from the requirements made in this analysis, e.g. because the danger points have been fenced off or the boundary conditions have not been explicitly considered, e.g. shunting operations or stabling facilities, it is recommended that the risk analysis be adapted in compliance with the user guide. In this way, adapted (usually weaker) safety integrity requirements can be derived. ■

AUTOREN | AUTHORS

Jens Braband

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

Luisa Lindner

Systems Engineer Railway Automation
Siemens Mobility GmbH
Anschrift / Address: Ackerstraße 22, D-38126 Braunschweig
E-Mail: luisa.lindner@siemens.com

Franziska Rixin

Systemmanagement ERTMS/ATO
Siemens Mobility GmbH
Anschrift / Address: Kieffholzstraße 44, D-12435 Berlin
E-Mail: franziska.rixin@siemens.com

LITERATUR | LITERATURE

- [1] Deutsches Zentrum für Schienenverkehrsforschung: Risikoakzeptanzkriterien für das automatisierte Fahren auf der Schiene (ATO-RISK), Abschlussbericht, 2023
- [2] Voigt: Auswertung Unfalldatenbank der Bundesstelle für Eisenbahnunfalluntersuchung (BEU) (01.01.2017 bis 26.04.2021), ausgewertet am 18.05.2021
- [3] Braband, J.: Risikoanalysen in der Eisenbahn-Automatisierung, Eurailpress, 2005
- [4] Braband, J.: Funktionale Sicherheit, in: Fendrich, L. (Hrsg.): Handbuch Eisenbahninfrastruktur, Springer Verlag, 2019, S. 583-638
- [5] Braband, J.: Vorgehensweise bei der Risikoanalyse Automatisches Fahren, SIGNAL+DRAHT, 10/2021, S. 25-34
- [6] 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
- [7] 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
- [8] 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)
- [9] Report on Railway Safety and Interoperability in the EU, 2020
- [10] DIN VDE V 0831-103: Elektrische Bahnsignalanlagen – Teil 103: Ermittlung von Sicherheitsanforderungen an technische Funktionen in der Eisenbahnsignaltechnik, 2020
- [11] DIN EN 50129:2019: Bahnanwendungen – Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme – Sicherheitsbezogene elektronische Systeme für Signaltechnik, 2018