

Anwendungsbeispiel eines Leitfadens zur ATO-Risikoanalyse

Example of an application for an ATO-risk analysis user guide

Frederik-Alexander Adebahr | Bernhard Evers | Christian Klotz | Franziska Rexin | Hendrik Schäbe

Im Projekt „Risikoakzeptanzkriterien für das automatisierte Fahren auf der Schiene“ (ATO-RISK) [6] wurden Grundlagen für die Ableitung von Anforderungen an die Sicherheitsintegrität zukünftiger automatisierter Funktionen im Vollbahnbereich entwickelt. Der Einfluss des betrieblichen Kontextes auf die daraus resultierenden Anforderungen an die Sicherheitsintegrität wurde untersucht und mithilfe eines Anwenderleitfadens dokumentiert. In diesem Beitrag wird dessen Anwendbarkeit anhand des Beispiels „Fahrerlose Bereitstellung von Zügen zwischen einem Betriebshof oder Abstellgleis und einem Bahnhof und umgekehrt“ demonstriert. Relevante Aspekte eines Betriebskonzeptes für dieses im Vergleich zum Fahrgastbetrieb einfachere beherrschbare Szenario werden dargelegt und mit den generischen Annahmen in ATO-RISK verglichen. Die Anforderungen an die Sicherheitsintegrität werden mit der in [6] angegebenen Methodik unter Berücksichtigung der oben genannten Betriebsbedingungen abgeleitet.

1 Einführung

Die einzelnen Schritte des Anwenderleitfadens werden kurz beschrieben. Anschließend werden relevante Aspekte eines Betriebskonzeptes für das vorgegebene Szenario dargestellt und mit den generischen Annahmen aus [6] verglichen. Der Schwerpunkt liegt dabei auf den Funktionen zur Vermeidung eines Zusammenstoßes mit Gegenständen oder Personen auf freier Strecke und im Bahnsteigbereich. Die Anforderungen an die Sicherheitsintegrität dieser Funktionen werden mit der in [6] beschriebenen Methodik abgeleitet. Zusätzlich werden diese Funktionen unter dem Gesichtspunkt der menschlichen Zuverlässigkeit bewertet, beide Ergebnisse werden verglichen und validiert. Abschließend werden die Ergebnisse zusammengefasst und diskutiert.

2 Anwenderleitfaden

2.1 Allgemeine Beschreibung (Einleitung)

Wie in Bild 1 dargestellt, ist es notwendig, eine konsolidierte Liste der zu automatisierenden Funktionen durch Analyse des Betriebskonzeptes zu erstellen. Anschließend wird die neu erstellte Liste mit der bereits vorhandenen, auf ATO-RISK basierenden Funktionsliste abgeglichen, um die Vollständigkeit der Analyse zu gewährleisten. Nach einer detaillierten Analyse werden die Randbedingungen (z. B. Vorhandensein eines eingezäunten Gleisbereichs) festgelegt. Stimmen die Funktionen einschließlich der Randbedingungen mit den bereits in ATO-RISK analysierten überein, können die Sicherheitsanforderungen aus ATO-RISK übernommen werden. Anderenfalls müssen diese neu abgeleitet werden.

The principles used for deriving the safety integrity requirements of future automated functions on mainline railways have been developed in the “Risk Acceptance Criteria for Automated Driving on Rail” project (ATO-RISK) [6]. The influence of the operating context on the resulting safety integrity requirements has been emphasised and substantiated by means of a user guide. This article demonstrates its applicability based on the example of the “driverless provision of trains from a depot or siding to a station and vice versa”. The relevant aspects of this scenario’s operating concept, which is a more controllable environment than passenger operations, have been stated and compared with the generic assumptions made in ATO-RISK. The safety integrity requirements have been derived using the methodology stated in [6] while taking the aforementioned operating conditions into consideration.

1 Introduction

The individual steps in the user guide are briefly described. The relevant aspects of the operating concept for the given scenario are then stated and compared with the generic assumptions made in [6]. The main focus is on those functions that prevent collisions with objects or people on the track and platform areas. The safety integrity requirements for these functions have been derived using the methodology found in [6]. These functions have likewise been additionally evaluated from the perspective of human reliability and both the results have then been compared and validated. The results have been summarised and discussed at the end.

2 The user guide

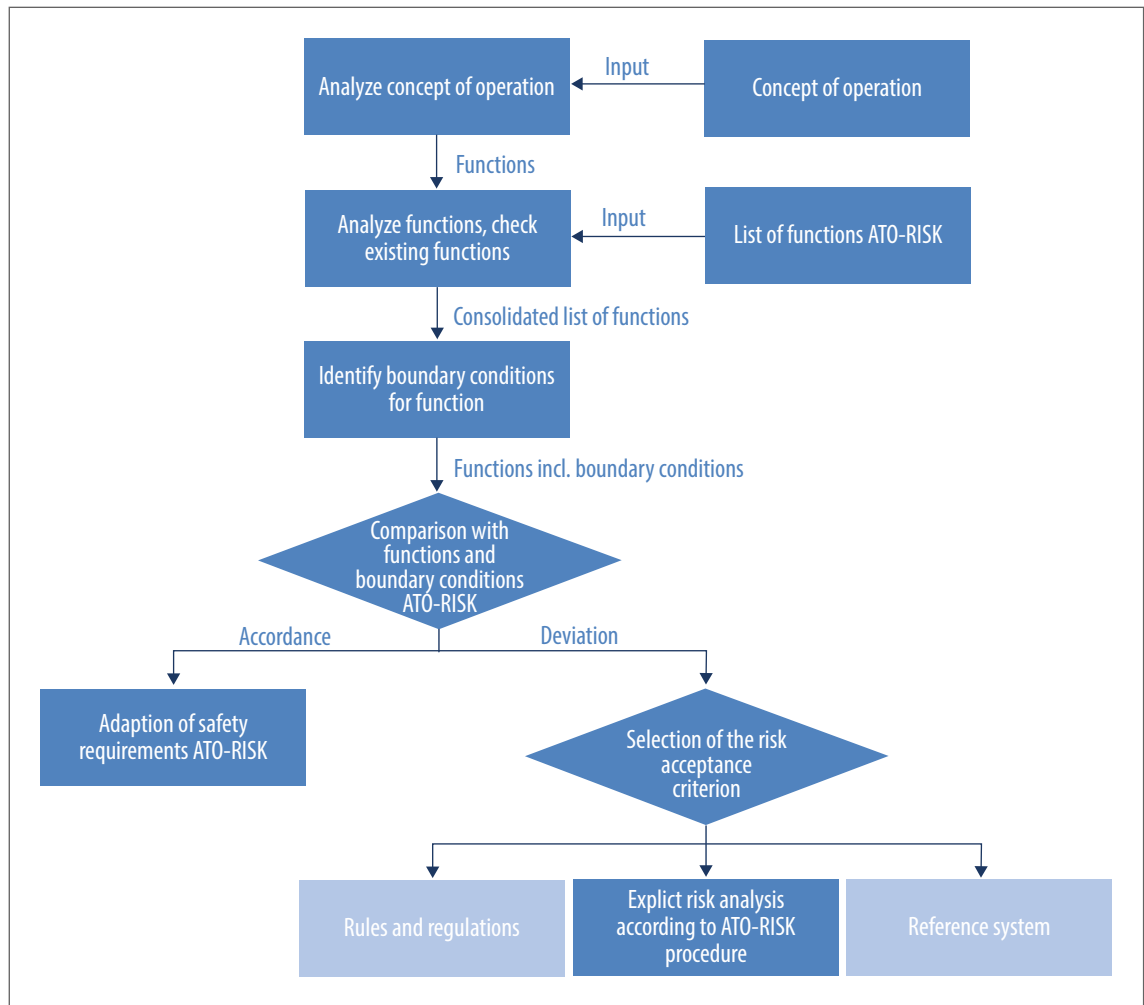
2.1 A general description (Introduction)

As shown in fig. 1, it is necessary to derive a consolidated list of the functions that are to be automated. The list is created by analysing the operating concept. It is then crosschecked with the already existing function list based on ATO-RISK to ensure that it is complete.

The boundary conditions (eg. the existence of a fenced track area) are defined after the detailed analysis.

The derived functions, including the boundary conditions, are compared with the functions/boundary conditions already analysed in ATO-RISK. If there is a match, the safety requirements from ATO-RISK can be adopted. Otherwise, the risk acceptance criterion must be newly derived.

Bild 1: Ablauf innerhalb des Anwenderleitfadens
Fig. 1: The user guide process



2.2 Betriebskonzept

Basis für diesen Beitrag ist das folgende Betriebskonzept für die automatische Bereitstellung von Zügen ohne Fahrgäste oder Personal von einem Bahnsteigbereich zu einem Depot oder Abstellgleis und umgekehrt. Es umfasst keine Durchfahrten an Bahnhöfen oder Bahnsteigbereichen. Vorgesehen ist ein Mischbetrieb von automatischen und manuell gesteuerten Zügen. Diese Analyse konzentriert sich auf die automatischen Züge. Für dieses Betriebskonzept wird eine maximale Zuggeschwindigkeit von 40 km/h oder 80 km/h angenommen. Güterwagen, z.B. mit Gefahrgut, und andere Sondervorschriften sind ausgeschlossen. Darüber hinaus wird angenommen, dass die technische Sicherung des Betriebs ohne Triebfahrzeugführer hinreichend sicher ist, einschließlich des Flankenschutzes, des Schutzes gegen nachfolgende und entgegenkommende Züge, der Absicherung des Zugabstandes und der Geschwindigkeit. Im Falle von Bauarbeiten in dem angenommenen Bereich finden keine automatischen Fahrten statt. Der Bereich kann wie folgt charakterisiert werden:

- Es sind keine Bahnübergänge vorhanden.
- Tunnel und Brücken sind mit Sicherheitsmaßnahmen ausgestattet, die das Risiko von Gegenständen oder Personen an diesen Stellen hinreichend mitigieren.
- Fußwege oder Abkürzungen werden überprüft und z.B. durch bauliche Maßnahmen gesichert.
- Gleisbereich am Bahnsteig: Bei der automatischen Einfahrt in einen Bahnhof können sich Fahrgäste im Bahnsteigbereich aufhalten. Die Züge fahren nur mit langsamer Geschwindigkeit (maximal 40 km/h) ein, eine Bahnsteigdurchfahrt ist nicht vorgesehen. Nach dem Anhalt

2.2 The operating concept

This article is based on the following operating concept that covers the automated provision of trains without any passengers or staff from a platform area to a depot or a siding and vice versa. It does not include the passage through any stations or platform areas. Mixed operations with automatic and manually driven trains are foreseen in the assumed area. This analysis focuses on the automated trains. The maximum train speed for this operating concept can be assumed to be either up to 40 km/h or up to 80 km/h respectively. Freight wagons, eg. with hazardous materials or other items subject to special handling rules, have been excluded. Moreover, the technical protection of the train's movement without a driver is assumed to be sufficiently safe, including the flank protection, the protection against any following and opposing trains, the protection of the distance between trains and the speed protection. No automated trips will take place during any construction work in the anticipated area. The area can be characterised as follows:

- there are no level crossings.
- the tunnels and bridges have been equipped with supplementary measures that cover the risk of any objects or people occurring at these points.
- the footpaths and shortcuts have been checked and secured, e.g. with structural measures.
- the platform track area: any passengers on the platform area need to be considered as present for automated station en-

ten ist keine Türentriegelung oder Türöffnung vorgesehen. Vor der automatischen Ausfahrt aus einem Bahnhof steht das Fahrzeug am Bahnsteig, ohne dass sich Fahrgäste an Bord befinden. Es fährt mit langsamer Geschwindigkeit (weniger als 40 km/h) ab. Im Allgemeinen ist auf dem Bahnsteig kein Personal anwesend.

- Gleisbereich auf dem Betriebshof: Hier befindet sich ein eingezäunter Bereich, d.h. es besteht kein Zutritt für betriebsfremde Personen. Eingewiesenes Betriebspersonal ist anwesend. Ein Anhalten des automatischen Zuges ist möglich, wenn sich Personen in der Nähe befinden. Fahrten finden mit langsamer Geschwindigkeit (maximal 25 km/h) statt.
- Abstellgleis: Dies ist ein eingezäunter Bereich, der den Zugang für betriebsfremde Personen ausschließt und in dem sich unterwiesenes Betriebspersonal aufhalten kann.
- Gleisbereich im Übergang vom/ zum Abstellgleis bzw. Depot: Dieser Bereich ist für Externe schwer zugänglich und kann nur vorsätzlich betreten werden. Die Anwesenheit von Betriebspersonal ist nicht vorgesehen.

2.3 Funktionsliste

Der Schwerpunkt dieses Beitrags liegt auf den Funktionen, die einen Zusammenstoß mit Personen oder Hindernissen verhindern sollen. Weitere betriebliche Aspekte im Zusammenhang mit Funktionen, die außerhalb des Geltungsbereichs liegen, werden nicht berücksichtigt und nicht beschrieben.

Tab. 1 listet die übergeordneten Funktionsblöcke aus [6] und [2] auf, die in diesem Beitrag behandelt werden.

2.4 Randbedingungen für die Funktion „Hinderniserkennung“

Für die Funktion „Verhindern des Zusammenstoßes mit Hindernissen und Personen“ kann man feststellen, dass die meisten Aspekte aus [6] wiederverwendet werden können. So wird analog zu [6] eine Unterscheidung in drei Hinderniskategorien vorgenommen:

1. absichtlich platzierte Hindernisse,
2. Hindernisse aufgrund von vorhersehbarem Missbrauch von Bahnanlagen und
3. zufällig auftretende Hindernisse.

Ein Unfall ist – mit der in diesem Beitrag zu bestimmenden tolerierbaren Gefährdungsrate (Tolerable Hazard Rate – THR) – durch geeignete Maßnahmen, z. B. Bremsen und / oder Warnen, zu verhindern.

3 Beispielhafte Risikoanalyse „Verhindern des Zusammenstoßes mit Personen“

Die Funktion dient dem Erkennen von versehentlich oder ungewollt auf dem Gleis befindlichen Personen. Die Auswertung bezieht sich auf folgende Gleisbereiche des Betriebskonzepts: Gleisbereich im Depot, Abstellgleisbereich, Gleisbereich im Übergang vom/ zum Abstellgleis und Gleisbereich im Übergang vom/ zum Depot. Im Gegensatz zu [6] bezieht sich diese Analyse nicht auf die freie Strecke.

Funktionsblock	Im Beitrag betrachtet
Zugbewegung überwachen	Nein
Fahren	Nein
Beobachtung der Bahnstrecke	
- Verhindern des Zusammenstoßes mit Hindernissen und Personen	Nein
- Überwachen der Gleisintegrität	Nein
Überwachen des Fahrgastwechsels / der Fahrgasttüren	Nein
Züge fahren	Nein
Erkennen und Bewältigen von Notfallsituationen	Nein

Tab. 1: Funktionsblöcke

try. The trains only move at slow speeds (up to a maximum of 40 km/h) to stop at the station; no platform passing is foreseen. No door release or door opening is provided after stopping. The vehicle at the platform has no passengers on board prior to its automated departure from the station. It departs at a slow speed (less than 40 km/h). Generally, there is no staff attendance on the platform.

- the track area in the depot: a fenced area, i.e. no access for unauthorised personnel. The automatic train can be immobilised if anybody is in the vicinity. Movement at slow speeds (max. 25 km/h).
- sidings: there is a fenced area that excludes access for unauthorised personnel and where instructed operating personnel can be present.
- the track area in the transition from/to the siding or depot: this area is difficult to access for external individuals and can only be reached with a purpose. It is not foreseen that any operating personnel will be present.

2.3 The function list

This article focuses on the function that prevents collisions with obstacles and people on the track and in the platform area for demonstration purposes. No further operating aspects related to the functions above and beyond this scope have been considered or described.

Tab. 1 includes the superordinate function blocks from [6] and [2] that are covered by this article.

2.4 The boundary conditions for the “Obstacle detection” function

It can be concluded that most of the aspects from [6] can be reused for the “prevention of collisions with obstacles and people” function. As such, distinctions are made between three obstacle categories in line with [6]:

1. intentionally placed obstacles
2. obstacles occurring due to the foreseeable misuse of rail-road facilities
3. randomly occurring obstacles

The defined accident must be prevented (in line with the Tolerable Hazard Rate (THR) determined in this article) by adequate means, e. g. by braking and/ or a warning.

3 An example of a “prevention of collisions with people” risk analysis

This function is used to detect the presence of any people accidentally or unintentionally located on the track. The analysis refers to the following track areas in the operating concept: the track area in the depot, the siding, the track area in the transition from/ to the siding, the track area in the transi-

Function block	Covered in the article
Ensure safe train movement	No
Driving	No
Observation of the track	
- Preventing collisions with obstacles and people	Yes
- Monitoring track integrity	No
Monitoring the passenger exchange / passenger doors	No
Train operation	No
Detecting / managing emergency situations	No

Tab. 1: The functional scope of the article

3.1 Schutzziel und allgemeine Bedingungen

Primäres Schutzziel ist das Erkennen von Personen, die sich unabsichtlich im Regellichtraum oder im Sogbereich des Zuges aufhalten. Im Folgenden werden diese Personengruppen als zu schützende Personen bezeichnet. Da es sich um eine Leerfahrt handelt, sind Fahrgäste im Falle eines Zusammenstoßes nicht betroffen. Folglich werden nur der Zug und die Person im Gleisbereich als Schutzobjekte betrachtet. Es wird davon ausgegangen, dass eine Person, die mit geringer Geschwindigkeit erfasst wird, ebenfalls tödlich verletzt wird. Weiterhin ist zu erwarten, dass einige der betrachteten Personen noch auf den mit geringer Geschwindigkeit herannahenden Zug reagieren können. Bei mittlerer Geschwindigkeit wird davon ausgegangen, dass keine Reaktion der betrachteten gefährdeten Personengruppen möglich ist. Es werden die folgenden zwei Szenarien betrachtet:

1. mittlere Geschwindigkeit (≤ 80 km/h) und
2. niedrige Geschwindigkeit (≤ 40 km/h).

3.2 Versagensarten

Die zu schützenden Personen werden nicht oder zu spät erkannt. Es wird nicht zwischen den Fehlerarten „nicht erkannt“ und „zu spät erkannt“ unterschieden, da eine zu späte Erkennung bedeutet, dass die Bremsung oder Warnung nicht wirksam ist.

3.3 Auswirkungen und Unfallklassen

Die Person wird vom Zug erfasst und erleidet tödliche Verletzungen (Unfallklasse F).

3.4 Zu schützende Objekte

Zu schützende Personen sind ungewollt anwesende Personen. Zu diesen Personen gehören auch Kinder und beeinträchtigte Personen.

3.5 Bewertung der Barrieren

Für diese Funktion kann eine Barriere abgeleitet werden, indem die Anforderungsrate zusammen mit der Fehleroffenbarung nach Tab. 5 [1] bewertet wird. Es wird ein jährliches Prüfintervall und damit eine Ausfallhäufigkeit von „gelegentlich bis selten“ angenommen. Die Eintrittshäufigkeit des Ereignisses „eine Person aus dem definierten Personenkreis befindet sich im Lichtraumprofil oder im Sogbereich des Zuges“ wird nach den Angaben der „Bundesstelle für Eisenbahnunfalluntersuchung“ als sehr selten eingestuft. Daraus ergibt sich nach Tab. 5 [1] eine Barriere, die mit drei Punkten bewertet wird.

Bei niedrigen Geschwindigkeiten (Szenario 2) existiert auch eine Barriere durch die mögliche Reaktion der Person im Lichtraumprofil des Zuges. Fällt die Hinderniserkennung aus, wird zwar keine automatische Reaktion durch Bremsen oder Warnen ausgelöst. Aufgrund des allgemeinen Gefahrenbewusstseins an Bahngleisen sowie der geringen Geschwindigkeit des herannahenden Zuges in Szenario 2 wird dennoch in vielen Fällen eine Reaktion der Person, auch trotz der Beeinträchtigungen innerhalb des Personenkreises, erwartet. Es wird daher davon ausgegangen, dass die Personen auch ohne zugehörige Bremsung oder Warnung in ca. 50 % der Fälle auf einen herannahenden Zug reagieren und so einen Zusammenstoß vermeiden können. Daher wird diese zusätzliche Barriere mit einem Punkt gemäß Tab. 8 [1] für Szenario 2 bewertet.

Daraus ergeben sich drei Punkte für die Barrieren in Szenario 1 (mittlere Geschwindigkeit) und vier Punkte für die Barrieren in Szenario 2 (niedrige Geschwindigkeit).

3.6 Abhängigkeit zwischen den Barrieren

Die angewendeten Barrieren sind voneinander unabhängig und werden daher als voll wirksam angenommen.

tion from/ to the depot. In contrast to [6], this analysis does not refer to the open line, since it is either inaccessible or restricted.

3.1 The protection objective and the general conditions

The primary objective involves the detection of any people unintentionally occurring in the clearance area or in the train's suction area. These groups of people are subsequently referred to as the people to be protected. Since this is an empty run, no passengers will be affected in the event of a collision. Consequently, only the train and the people in the track area are considered to be objects of protection. It is assumed that a person hit at low speeds will also be fatally injured. However, it is to be expected that some of the people under consideration will still be able to react to a train approaching at low speeds. It is assumed that vulnerable groups of people under consideration will be unable to react at medium speeds.

Therefore, the following two scenarios have been considered:

1. medium speed (≤ 80 km/h) and
2. low speed (≤ 40 km/h).

3.2 Failure modes

The people to be protected are either not detected or are detected too late. No distinction is made between the “not detected” and “detected too late” failure types, since detection too late implies that the braking or warning has not been effective.

3.3 Effects and accident classes

The person is hit by the train and suffers fatal injuries (accident class F).

3.4 The objects to be protected:

People to be protected occur unintentionally. These people include children and impaired people.

3.5 The evaluation of barriers

A barrier can be derived for this function by evaluating the demand rate with the failure detection according to tab. 5 [1]. An annual proof test interval and thus a failure frequency of “occasional to infrequent” has been assumed. According to the data from the “Federal Authority for Railway Accident Investigations”, the frequency of an event involving “a person who can be assigned to the defined group of people on the track in the train's clearance or suction area” is classified as very rare. Thus, this results in a barrier of three points in line with tab. 5 [1].

At low speeds (scenario 2), a barrier is also applied by means of the possible reaction of the person within the train's clearance. If the obstacle detection fails, no braking or warning reaction will be triggered. In addition, a limited reaction capability has been assumed, since the group of people under consideration involves mentally or physically impaired people or people who have been involved in an accident. A reaction is nevertheless expected from the person in many cases due to the general awareness of danger near railroad tracks, as well as the slow speed of the approaching train in scenario 2. It is therefore assumed that the people can still react to an approaching train at low train speeds in approximately 50 % of the cases, even without the train braking or giving a warning, and thus avoid a collision. As such, the barrier is one point for scenario 2 (slow speed) according to tab. 8 [1].

Sicherheitsanforderung 1/h	Risiko-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							

Tab. 2: Risiko-Score-Matrix „Erkennung von Personen“ nach [1]

3.7 Bestimmung der Sicherheitsanforderungen

Die tolerierbaren funktionalen Ausfallraten (Tolerable Functional Failure Rate – TFFR) werden aus der Risiko-Score-Matrix abgeleitet (Tab. 2).

3.8 Sicherheitsanforderung (bei jährlichem Proof-Test)

- TFFR von $3 \times 10^{-7}/h$ für die Fehlerart „Person wird nicht oder zu spät erkannt“ (bei mittlerer Geschwindigkeit ≤ 80 km/h)
- TFFR von $10^{-6}/h$ für die Fehlerart „Person wird nicht oder zu spät erkannt“ (bei niedriger Geschwindigkeit ≤ 40 km/h).

Wenn ausgeschlossen werden kann, dass sich Personen unbeabsichtigt im Gleisbereich aufhalten, treten die genannten Gefährdungen nicht auf, sodass die resultierenden TFFR keine Bemessungsgrundlage für diese Funktion darstellen.

3.9 Überblick über die Ergebnisse der Risikoanalyse

Die für das vorliegende Betriebskonzept und die oben genannten Funktionen abgeleiteten Sicherheitsintegritätsanforderungen nach [1], [8] und [6] sind in Tab. 3 zu finden. Hervorzuheben ist, dass der Zusammenstoß mit Objekten im Gleis nur zu Sachschäden führen kann, weshalb keine Sicherheitsanforderung gestellt wird.

4 Die Human-Factors-Methode nach ATO-RISK

Zur Bewertung der menschlichen Fehlerwahrscheinlichkeit eines Triebfahrzeugführers wird die modifizierte Human-Factors-Methode aus [6] nach RARA [4] herangezogen. „Railway Action Reliability Assessment“, abgekürzt RARA, beinhaltet eine Klassifizierung menschlicher Handlungen, die in acht generische Aufgabentypen (Generic Task Types – GTT) und 27 Einflussfaktoren (Error Producing Conditions – EPC) unterteilt sind. Die Methode ist flexibler und aktueller als die in Deutschland üblicherweise verwendete Methode nach Hinzen [5]. In [6] wird die Methode RARA an die Erfordernisse einer generischen Betrachtung der menschlichen Fehlerwahrscheinlichkeit angepasst.

4.1 Verwendung der Funktionen von ATO-RISK

Für die Funktionen des generischen Anwendungsfalls in ATO-RISK wurden die GTT und EPC in einem Workshop nach [4] ermittelt, siehe Bild 2 für die hier relevanten Funktionen.

Safety requirement 1/h	Risk Score Matrix						
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
Accident class							

Tab. 2: The “Obstacle detection of People” Risk Score Matrix according to [1]

This results in a total barrier of three points for scenario 1 (medium speed) and a barrier of four points for scenario 2 (low speed).

3.6 The dependency between the barriers

The applied barriers are consequently independent of each other and can be assumed to be fully effective.

3.7 Determining the safety requirements

The Tolerable Functional Failure Rates (TFFR) are derived from the Risk Score Matrix (tab. 2).

3.8 The safety requirement (with an annual proof test)

- a TFFR of $3 \times 10^{-7}/h$ for the “person is not detected or detected too late” failure mode (at medium speeds ≤ 80 km/h),
- a TFFR of $10^{-6}/h$ for the “person is not detected or detected too late” failure mode (at low speeds ≤ 40 km/h).

If people can be excluded from unintentionally entering the track area, the aforementioned hazards will not occur, meaning that the resulting TFFR do not constitute a dimensioning basis for this function.

3.9 An overview of the results of the risk analysis

The safety integrity requirements derived for the selected functions according to [1], [8] and [6] under the given operating concept can be found in tab. 3. It is worth highlighting the fact that the failed prevention of a collision with objects on the track can only lead to property damage, which is why no safety requirement has been assigned.

4 The Human Factors Method according to ATO-RISK

The modified Human Factors Method according to “RARA” [4] from [6] is considered when evaluating a train driver’s probability of human error. The “Railway Action Reliability Assessment”, abbreviated as RARA, includes a classification of human actions divided into eight generic task types (GTT) and 27 error producing conditions (EPC). The method is more flexible and more up to date than the method according to Hinzen [5], which is usually used in Germany. [6] has adapted the RARA method to the requirements of a generic consideration of the human error probability.

Ereignis	TFFR
Erkennen von Personen im Gleisbereich auf freier Strecke (≤ 80 km/h) mittlere Geschwindigkeit (≤ 40 km/h) niedrige Geschwindigkeit	$3 \cdot 10^{-7}/h$ $10^{-6}/h$
Erkennen von Objekten im Gleichbereich auf freier Strecke	Keine Anforderung an die Sicherheitsintegrität
Erkennen von Personen am Bahnsteig	$10^{-5}/h$

Tab. 3: Ergebnisse der semiquantitativen Risikoanalyse

4.2 Auswertung und Ergebnisse der Human-Factors-Methode für das Betriebskonzept

Für das in Abschnitt 2.2 vorgestellte Betriebskonzept werden die in ATO-RISK gewählten Parameter überprüft. Die GTT ändern sich nicht, da der grundlegende Charakter der Aufgabe gleichbleibt. EPC T2 wird bei Fahrten bis zu 40 km/h nicht angewendet, da aufgrund der geringen Geschwindigkeit mehr Zeit für die Hinderniserkennung zur Verfügung steht. Gemäß Abschnitt 2.2 gilt diese Geschwindigkeitsbegrenzung für alle Bahnsteiggleisbereiche. EPC T6 wird für das Fahren in Bahnsteiggleisbereichen nicht angewendet. EPC P2 ist von der Konkretisierung auf Bereitstellungsfahrten nicht betroffen und wird angewendet. Tab. 4 zeigt gemäß der Human-Factors-Methode in [6] Kapitel 4 die Berechnungsergebnisse für die fahrerlose Bereitstellung von Zügen, die vom Depot oder Abstellgleis in einen Bahnhof und umgekehrt fahren.

Bild 2: GTT und EPC der ausgewählten Funktionen in [6]

Fig. 2: The GTT and EPC for the selected functions in [6]

Functions tailored for RARA	Selected GTT in ATO-RISK workshop	Selected EPC in ATO-RISK workshop
1: Dealing with obstacles on the open track if they are clearly identifiable as obstacles.	R3	T2, T6, P2
2: Dealing with obstacles on the open track if it is not immediately clear whether an object is a relevant obstacle.	R7	T2, T6, P2
5: Monitor and respond of faults on constantly existing infrastructure elements.	R5	T6, P2
6: Monitor and respond to faults in punctual infrastructure elements.	R3 (Conservative, smallest possible GTT of selection in [R23] tab. 21)	T6, P2
GTT R3: “simple response to a dedicated alarm and execution of actions covered in procedures, keyword: simplicity“ GTT R5: “fairly simple task performed rapidly or given insufficient or inadequate attention“ GTT R7: “identification of situation requiring interpretation of alarm/indication patterns“ EPC T2: “a shortage of time available for error detection and correction“ EPC T6: “little or no independent checking or testing of output“ EPC P2: “fatigue from shift and work patterns“		

Event	TFFR
Obstacle detection of people in the track area (≤ 80 km/h) medium speed (≤ 40 km/h) low speed	$3 \cdot 10^{-7}/h$ $10^{-6}/h$
Detection of objects on the track	No safety integrity requirement
Obstacle detection of people on the platform	$10^{-5}/h$

Tab. 3: The results of the semi-quantitative risk analysis

4.1 Using the functions from ATO-RISK

GTTs and EPCs have been determined for the generic use case in ATO-RISK in a workshop conforming to [4]: see fig. 2 for the relevant functions.

4.2 The evaluation and results of the Human Factors Method for the operating concept

The selected ATO-RISK parameters have been reviewed for the operating concept presented in Section 2.2. The GTT's do not change, because the basic character of the task remains the same. EPC T2 is not applied to driving at speeds of up to 40 km/h, as more time is available for the obstacle detection due to the slow speed. According to Section 2.2, this speed limitation applies to all platform track areas. EPC T6 is not applied to driving in the platform track areas. EPC P2 is not affected by the concretisation of the provisioning trips and therefore remains in place. Tab. 4

Funktionen nach [6] zugeschnitten auf RARA	Bahnsteigbereich, 40 km/h	40 km/h	80 km/h
1: Umgang mit Hindernissen auf freier Strecke, wenn diese deutlich als Hindernisse erkennbar sind.	gewähltes GTT: R3 gewähltes EPC: P2 untere Grenze: 5,60E-04 obere Grenze: 7,20E-04	gewähltes GTT: R3 gewählte EPC: T6, P2 untere Grenze: 8,40E-04 obere Grenze: 1,44E-03	gewähltes GTT: R3 gewählte EPC: T2, T6, P2 untere Grenze: 2,94E-03 obere Grenze: 8,64E-03
2: Umgang mit Hindernissen auf freier Strecke, wenn nicht sofort klar ist, ob ein Objekt ein relevantes Hindernis ist.	gewähltes GTT: R7 gewähltes EPC: P2 untere Grenze: 9,80E-02 obere Grenze: 1,26E-01	gewähltes GTT: R7 gewählte EPC: T6, P2 untere Grenze: 1,47E-01 obere Grenze: 2,52E-01	gewähltes GTT: R7 gewählte EPC: T2, T6, P2 untere Grenze: 5,15E-01 obere Grenze: 1

„untere Grenze“: bezieht sich auf die untere Intervallgrenze der Methode mit einer Gewichtung aller EPC von 25 %
 „obere Grenze“: bezieht sich auf die obere Intervallgrenze der Methode mit einer Gewichtung aller EPC von 50 %.

Tab. 4: Verwendete GTT, EPC und Ergebnisse

Functions according to [6] tailored to RARA	Platform track area, 40 km/h	40 km/h	80 km/h
1: Dealing with obstacles on the open track if they are clearly identifiable as obstacles.	selected GTT: R3 selected EPC: P2 lower limit: 5.60E-04 upper limit: 7.20E-04	selected GTT: R3 selected EPC: T6, P2 lower limit: 8.40E-04 upper limit: 1.44E-03	selected GTT: R3 selected EPC: T2, T6, P2 lower limit: 2.94E-03 upper limit: 8.64E-03
2: Dealing with obstacles on the open track if it is not immediately clear whether an object is a relevant obstacle.	selected GTT: R7 selected EPC: P2 lower limit: 9.80E-02 upper limit: 1.26E-01	selected GTT: R7 selected EPC: T6, P2 lower limit: 1.47E-01 upper limit: 252E-01	selected GTT: R7 selected EPC: T2, T6, P2 lower limit: 5.15E-01 upper limit: 1

“lower limit”: refers to the lower interval limit of the method with a 25 %weighting of all the EPC
 “upper limit”: refers to the upper interval limit of the method with a 50 %weighting of all the EPC

Tab. 4: The used GTT, EPC and the results

5 Validierung

Eine umfassende Erläuterung des methodischen Ansatzes von ATO-RISK ist in [3] oder im Abschlussbericht [6] dokumentiert.

Für das Beispiel, welches im vorliegenden Beitrag erörtert wird, wurden die nachfolgend dargestellten Prüfungen durchgeführt. Es wurden nur die Ereignisse analysiert, für die ein quantitatives Ergebnis ermittelt wurde. Darüber hinaus wurde die Wahrscheinlichkeit menschlichen Versagens unter Verwendung einer Anforderungsrate von 1/8760 h gemäß [7] in eine TFFR umgerechnet. Die Ergebnisse sind in der folgenden Tab. 5 dargestellt.

Für das erste Ereignis liegen beide Methoden nahe beieinander. Die Berücksichtigung der menschlichen Zuverlässigkeit führt zu etwas größeren TFFR-Werten als die Methode aus Kapitel 3.

shows the calculation results for the driverless provision of trains moving from a depot or a siding to the station and vice versa according to the Human Factors Method in Chapter 4 of [6].

5 Validation

Please refer to [3] or the final report of [6] for a comprehensive explanation of the methodological approach of ATO-RISK.

The following cross-check has been carried out for this specific example, as discussed in the article. Therefore, only those events with a derived quantitative result have been analysed. Furthermore, the human error probability has been converted to a TFFR using a demand rate of 1/8760 h according to [7]. The results are presented in the following tab. 5.

Ereignis	TFFR; Kapitel 3 [1/h]	Wahrscheinlichkeit menschlichen Versagens; Kapitel 4, untere Grenze	Wahrscheinlichkeit menschlichen Versagens; Kapitel 4, obere Grenze	TFFR; Kapitel 4, untere Grenze [1/h]	TFFR; Kapitel 4, obere Grenze [1/h]
Erkennen von Personen im Gleisbereich auf freier Strecke (<= 80 km/h) mittlere Geschwindigkeit	3.00E-07	2.94E-03	8.64E-03	3.36E-07	9.86E-07
Erkennen von Personen im Gleisbereich auf freier Strecke (<= 40 km/h) niedrige Geschwindigkeit	1.00E-06	8.40E-04	1.44E-03	9.59E-08	1.64E-07
Erkennen von Personen am Bahnsteig	1.00E-05	5.60E-04	7.20E-04	6.39E-08	8.22E-08

Tab. 5: Vergleich der Ergebnisse von Kapitel 3 und 4

Event	TFFR; Chapter 3 [1/h]	Probability of human error; Chapter 4, lower boundary	Probability of human error; Chapter 4, upper boundary	TFFR; Chapter 4, lower boundary [1/h]	TFFR; Chapter 4, upper boundary [1/h]
Person is not detected or detected too late (<= 80 km/h) medium speed	3.00E-07	2.94E-03	8.64E-03	3.36E-07	9.86E-07
Person is not detected or detected too late (<= 40 km/h) low speed	1.00E-06	8.40E-04	1.44E-03	9.59E-08	1.64E-07
Obstacle detection of people at the platform	1.00E-05	5.60E-04	7.20E-04	6.39E-08	8.22E-08

Tab. 5: A comparison of the results for Chapters 3 and 4

Für die beiden anderen Ereignisse, die für den Triebfahrzeugführer einfacher sind, d.h. das Erkennen eines Hindernisses bei niedriger Geschwindigkeit oder an einem Bahnsteig, wurden in Kapitel 3 deutlich höhere TFFR-Werte ermittelt als in Kapitel 4. Dies ist nachvollziehbar, da der Mensch auf Situationen bei geringer Geschwindigkeit sehr gut reagieren kann, sodass er die Situation besser bewältigt, als es notwendig wäre. Dies ist eine direkte Folge der unterschiedlichen Ansätze von Kapitel 3 und 4. In Kapitel 3 wird eine Sicherheitsanforderung für eine Funktion erarbeitet, um eine TFFR abzuleiten, während die Methode in Kapitel 4 die Frage beantwortet, wie gut ein Mensch in der vorgegebenen Situation agieren kann. Dieser Unterschied wurde auch in [6] diskutiert, und die Unterschiede wurden erklärt.

Es kann somit festgestellt werden, dass die explizite Risikoanalyse nach DIN VDE V 0831- 103 [1] grundsätzlich geeignet ist, Risikoakzeptanzkriterien für ATO-Projekte abzuleiten. Insgesamt kann festgestellt werden, dass sich der Ansatz der Risikoanalyse nach der CSM-Verordnung (Common Safety Methods) als sehr vorteilhaft erwiesen hat, da bei der Anwendung der Risikoakzeptanzprinzipien „Regelwerk“ oder „Referenzsystem“ bestehende Vorgaben übernommen werden können. Darüber hinaus wurde der Vorteil einer semiquantitativen Risikoanalyse in Anlehnung an DIN VDE V 0831-103 [1] für diejenigen Teilfunktionen aufgezeigt, für die weder ein Regelwerk noch ein Referenzsystem existiert.

Both methods are close for the first result. The human reliability consideration is giving slightly larger TFFR values than the method from Chapter 3.

Chapter 3 has derived much larger TFFR values than Chapter 4 for the other two events that are less demanding, i.e. detect an obstacle at low speeds or at a platform. This is understandable given that humans can handle situations at low speeds very well, so that a human performs better than would be necessary. This is a direct result of the different approaches of Chapters 3 and 4. Chapter 3 asks for a safety requirement for a function to derive a TFFR, whereas the method in Chapter 4 answers the question of how well a human being might perform in the given situation. This difference has also been discussed in [6] and the differences have been explained.

It can therefore be stated that the explicit risk analysis according to DIN VDE V 0831- 103 [1] is in principle suitable for deriving the risk acceptance criteria for ATO projects. It can generally be stated that the risk analysis approach in accordance with the CSM (Common Safety Methods) Regulation has proved to be very advantageous, as it has proved possible to adopt the existing specifications when using the “rules and regulations” or “reference system” risk acceptance principles. In addition, the advantage of a semi-quantitative risk analysis based on DIN VDE V 0831-103 [1] has been demonstrated for those sub-functions, for which neither a set of rules nor a reference system existed.

Steuern, stellen, sichern.



Scheidt & Bachmann – innovative Sicherheitstechnologie seit 1872.

- Betriebsleittechnik
- Stellwerkstechnik
- Bahnübergangstechnik

6 Diskussion und Schlussfolgerung

Die Anforderungen an die Sicherheitsintegrität der Funktionen können mittels der Methodik von [1] und [6] abgeleitet werden. Zum Abgleich erfolgte die Bewertung dieser Funktionen aus der Perspektive menschlicher Zuverlässigkeit auf der Grundlage der Methode RARA, die auf die verschiedenen Betriebsszenarien einschließlich Geschwindigkeitsbegrenzungen zugeschnitten wurde. Beide Ergebnisse wurden miteinander verglichen und validiert.

Der Anwenderleitfaden ist eine geeignete Methode für die Bewertung von Funktionen oder Randbedingungen, die nicht bereits in [6] behandelt wurden. Alle Unterschiede zwischen den Ergebnissen der semiquantitativen Risikoanalyse einerseits und der menschlichen Zuverlässigkeit andererseits sind erklärbar.

Für die Funktion „Erkennen von Objekten im Gleisbereich auf freier Strecke“ sind unter den gegebenen Randbedingungen aufgrund des geringen zu erwartenden Schadensausmaßes keine Sicherheitsintegritätsanforderungen zu definieren. Einige Anforderungen, wie z. B. das Erkennen von Personen auf Bahnsteiggleisen, können direkt aus ATO-RISK übernommen werden.

Es lässt sich feststellen, dass zur Ableitung von Risikoakzeptanzkriterien für ATO-Funktionen die Risikoanalyse nach [6] geeignet ist. Es können mit vertretbarem Aufwand verlässliche Ergebnisse erzielt werden. Aufgrund geringerer Sicherheitsanforderungen und besser beherrschbarer Umgebungsbedingungen könnte das skizzierte Betriebskonzept der Bereitstellungsfahrten ein sinnvoller erster Anwendungsfall für die Einführung von ATO sein. ■

LITERATUR | LITERATURE

- [1] DIN VDE V 0831-103: Elektrische Bahnsignalanlagen – Teil 103: Ermittlung von Sicherheitsanforderungen an technische Funktionen in der Eisenbahnsignaltechnik, 2020
- [2] DIN EN 62290-1: Bahnanwendungen – Betriebsleit- und Zugsicherungssysteme für den städtischen schienengebundenen Personennahverkehr – Teil 1: Systemgrundsätze und grundlegende Konzepte, 2014
- [3] Braband, J.: Ansatz zur Risikoanalyse beim automatischen Fahren, SIGNAL+DRAHT 10/2021, S. 25-34
- [4] Gibson, H.: Railway Action Reliability Assessment user manual: A technique for the quantification of human error (T270 Manual), London: Rail Safety and Standards Board Ltd (RSSB), 2012
- [5] Hinzen, A.: Der Einfluss menschlichen Fehlverhaltens auf die Eisenbahnsicherheit, Dissertation, RWTH Aachen, 1993
- [6] Braband, J.; Evers, B.; Kinas, M.; Lindner, L.; Milhailescu-Stoica, D.; Regin, F.; Adebahr, F.; Milius, B.; Schäbe, H.: Abschlussbericht ATO-RISK, Risikoakzeptanzkriterien für das automatisierte Fahren auf der Schiene, Berichte des Deutschen Zentrums für Schienenverkehrsforschung, Projektnummer 2020-19-S-1202, 2023
- [7] Adebahr F.; Schäbe H.: Wahrscheinlichkeit menschlicher Fehler und Ausfallraten technischer ATO-Systeme, SIGNAL+DRAHT 3/2023, S. 21-29
- [8] VDV: Anforderungen an Einrichtungen zur Gewährleistung der Fahrgastsicherheit in Haltestellen bei Fahrbetrieb ohne Fahrzeugführer, VDV-Schrift 399, Oktober 2000

6 Discussion and conclusion

The safety integrity requirements for the functions have been derived using the methodologies of [1] and [6]. In addition, these functions have also been evaluated from the perspective of human reliability based on the RARA methodology, which has been tailored to the different operating scenarios, including the speed limits. Both results have been compared and validated.

The user guide is a suitable method for evaluating any functions or conditions that have not already been covered in [6]. All the differences between the results derived using the semi-quantitative risk analysis on the one hand side and human reliability on the other hand are explicable.

No safety integrity requirements have to be defined for the “detection of objects on the track” function under the given boundary conditions due to the low extent of damage to be expected. Some requirements, such as the detection of people on platform tracks, can be taken directly from ATO-RISK.

A risk analysis according to [6] is suitable for deriving the risk acceptance criteria for ATO functions. Credible results can be achieved with a reasonable effort. The lower safety requirements and better controllable environment mean that the present use case could constitute a sensible migration path for the introduction of ATO. ■

AUTOREN | AUTHORS

Frederik-Alexander Adebahr

Scientific Assistant

TU Berlin

Adresse / Address: Salzufer 17-19, D-10587 Berlin

E-Mail: f.adebahr@tu-berlin.de

Bernhard Evers

System Architect, Research and Development

Siemens Mobility GmbH

Adresse / Address: Siemens Mobility, Ackerstraße 22, D-38126 Braunschweig

E-Mail: bernhard.evers@siemens.com

Christian Klotz

Research area cross-sectional topics digitalization, automation, migration and law

Deutsches Zentrum für Schienenverkehrsforschung (DZSF)

beim Eisenbahn-Bundesamt

Adresse / Address: August-Bebel-Straße 10, D-01219 Dresden

E-Mail: klotzc@dzsf.bund.de

Franziska Regin

System Management ERTMS/ATO

Siemens Mobility GmbH

Adresse / Address: Kieffholzstraße 44, D-12435 Berlin

E-Mail: franziska.regin@siemens.com

Hendrik Schäbe

Principal Assessor RAMS

TÜV Rheinland InterTraffic GmbH

Adresse / Address: Am Grauen Stein, D-51105 Köln

E-Mail: schaebe@de.tuv.com