

Risikoanalyse für das Automatisierte Fahren – Validierung und Erkenntnisse

Risk analysis for automated driving – validation and findings

Jens Braband | Hendrik Schäbe

Das vom Deutschen Zentrum für Schienenverkehrsforschung (DZSF) beauftragte Projekt ATO-RISK hatte das Ziel, „Risikoakzeptanzkriterien für das automatisierte Fahren auf der Schiene“ abzuleiten. Ein wichtiger Aspekt dabei ist die Validierung der Ergebnisse. Außerdem sind während der Bearbeitung zahlreiche Erkenntnisse gewonnen worden, die auch für andere Anwendungen interessant sind. Dazu werden nach einer kurzen Zusammenfassung des grundsätzlichen Vorgehens des ATO-RISK-Projekts zunächst die Ergebnisse der Validierung erläutert und anschließend am wichtigen Beispiel der Hinderniserkennung diskutiert. Abschließend werden übergreifende Erkenntnisse präsentiert und diskutiert. Die Risikoanalyse sollte nicht mit der Sicherheitsanalyse verwechselt oder vermischt werden, insbesondere werden im Rahmen der Risikoanalyse keine speziellen Lösungsarchitekturen bewertet, und es wird 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 etc. sind nicht Betrachtungsgegenstand. Weiterhin 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 [9] sowie der DIN VDE V 0831-103 [13] als gewählte Methode für explizite Risikoanalyse kompatibel ist.

Wie in der Vorgehensweise [7] beschrieben, wird als Risikoakzeptanzkriterium je nach Funktion eine explizite Risikoanalyse durchgeführt oder auf existierende Regelwerke oder Referenzsysteme zurückgegriffen. Für die explizite Risikoanalyse wird die CSM-VO konforme Norm DIN VDE V 0831-103 [13] angewendet. Die Bewertung verschiedener Szenarien erfolgt nach diesem semiquantitativen Ansatz mithilfe einer Risk Score Matrix (RSM), die das erwartete Schadensausmaß qualitativ nach Unfallklassen differenziert. Für eine detailliertere Darstellung sei auf [4] verwiesen.

Zur Absicherung der Ergebnisse wird eine Untersuchung der menschlichen Zuverlässigkeit im heutigen Betrieb nach GoA 2 durchgeführt (Bild 1). Diese Analyse wurde in [2] umfassend dargestellt.

The ATO-RISK project commissioned by the German Centre for Rail Transport Research (DZSF) aimed to derive “risk acceptance criteria for automated driving on rail”. An important aspect of this is the validation of the results. In addition, numerous findings have been obtained during the work that are also of interest for other applications. Therefore, after a short summary of the basic approach of the ATO-RISK project, the results of the validation are initially explained and then discussed using the important example of obstacle detection. Finally, overarching findings are presented and discussed. Risk analysis should not be confused or mixed with safety analysis; in particular, risk analysis does not evaluate specific solution architectures or derive safety objectives for technical components. All considerations refer to Functional Safety with reference to the CENELEC standards. Other safety aspects, explicitly cyber security, occupational health and safety, etc., are not the subject of consideration. Furthermore, an investigation of the performance of humans in terms of sensory perception and information processing ability is not part of the project. This is being carried out in the parallel project ATO-SENSE.

1 Approach of the ATO-RISK project

Within the framework of the ATO-RISK project, a system for automated rail / driving operation with automation level (GoA) 3 (driverless operation) as well as GoA 4 (without operating personnel on board) is first defined. 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 Regulation [9] and DIN VDE V 0831-103 [13] as the selected method for explicit risk analysis.

As described in the procedure [7], an explicit risk analysis is carried out as a risk acceptance criterion (RAC), depending on the function, or existing regulations or reference systems are used. For the explicit risk analysis, the CSM Regulation compliant standard DIN VDE V 0831-103 [13] is applied. The evaluation of different scenarios is carried out according to this semi-quantitative approach with the aid of a Risk Score Matrix (RSM), which qualitatively differentiates the expected extent of damage according to accident classes. For a more detailed presentation, please refer to [4].

To validate the results, an analysis of human reliability in today's operation is performed according to GoA 2, compare

Ein entscheidender Punkt ist die Zusammenführung sowie die abschließende Validierung der Ergebnisse, die den Schwerpunkt dieses Beitrags bildet.

Im Vergleich zu anderen Ansätzen [1] erkennt man an Bild 1 insbesondere den erweiterten Umfang und den umfassenden Abgleich aller Aspekte zur Ermittlung der Sicherheitsintegritätsanforderungen. Man kann die Vorgehensweise auch in Analogie zur bekannten Watchdog-Architektur (d.h. einen Spezialfall eines zweikanaligen Systems mit einem Vergleich im Sinn der reaktiven Ausfallsicherheit nach [14]) interpretieren: Die beiden Analysen werden auf der gemeinsamen Systemdefinition weitgehend unabhängig durchgeführt. Ein unabhängiger Vergleich (Validierung) plausibilisiert die Ergebnisse der Risikoanalyse, wo möglich und sinnvoll, mit den Ergebnissen der menschlichen Zuverlässigkeitsanalyse. Für eine umfangreichere Erläuterung des methodischen Vorgehens von ATO-RISK soll auf [7] oder den Abschlussbericht [1] verwiesen werden.

2 Ergebnisse der Validierung

Die Validierung wurde in vier Schritten durchgeführt:

- Review (Verifizierung) der Ergebnisse der drei Arbeitspakete
- Validierung der Endergebnisse durch Vergleich der Arbeitsergebnisse zum Status quo GoA 2 sowie Risikoakzeptanz GoA 3/4

fig. 1. This analysis has been comprehensively presented in [2].

A crucial point is the consolidation as well as the final validation of the results, which is the focus of this article.

Compared to other approaches [1], one can see from fig. 1 in particular the extended scope and the comprehensive comparison of all aspects for determining the safety integrity requirements. One can also interpret the approach in analogy to the well-known watchdog architecture (i.e. a special case of a two channel System with comparator in the sense of reactive fail-safety according to [14]): the two analyses are performed largely independently based on the common system definition. An independent comparator (validation) makes the results of the risk analysis plausible, where possible and reasonable, with the results of the human reliability analysis.

For a more comprehensive explanation of the methodological approach of ATO-RISK, please refer to [7] or the final report [1].

2 Results of the validation

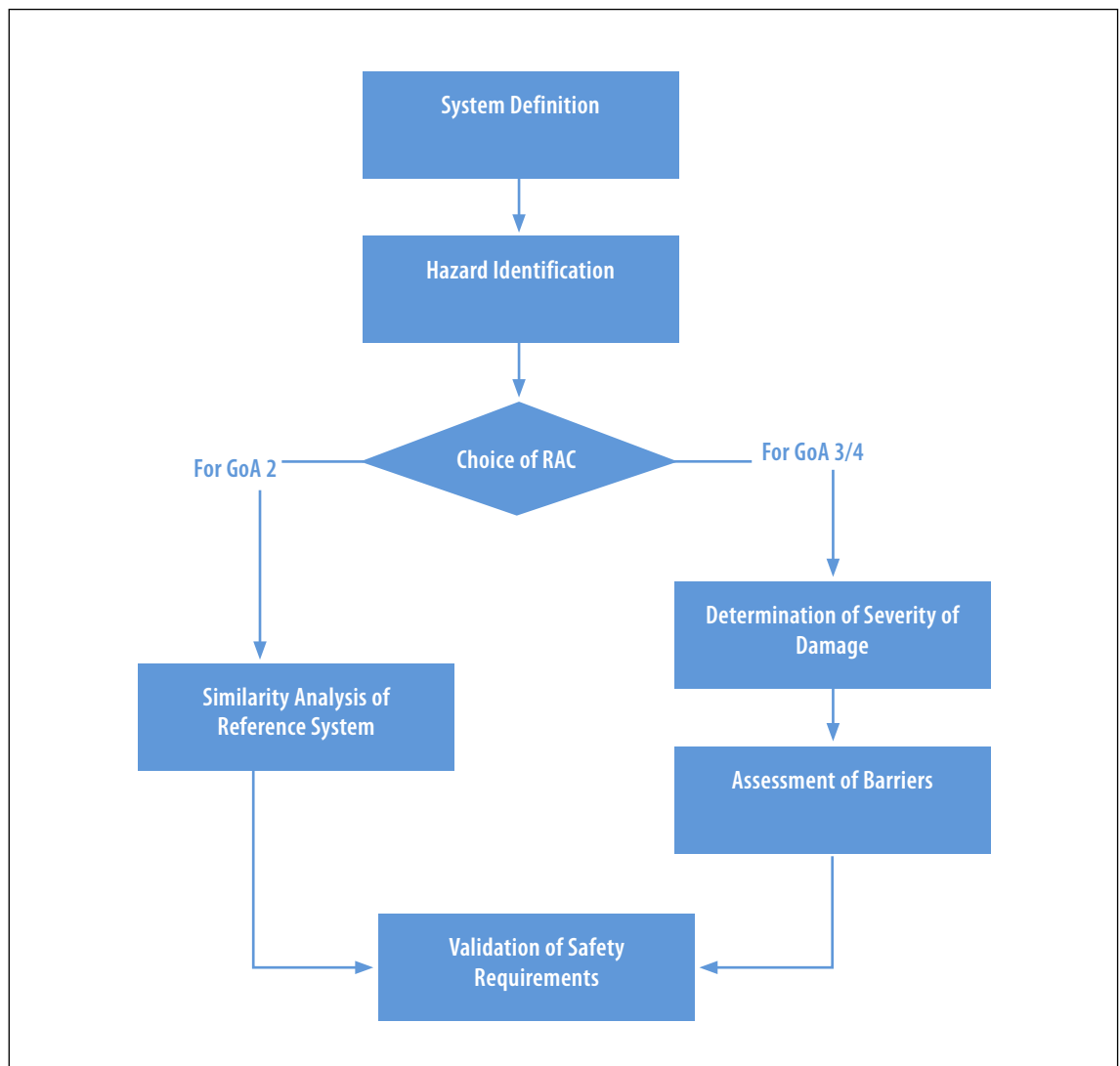
The validation was carried out in four steps:

- Review (verification) of the results of the three work packages

Bild 1: Vorgehensweise ATO-RISK

Fig. 1: Procedure ATO-RISK

Quelle / Source: Siemens Mobility



- Ableitung wesentlicher Ergebnisse mit einem unabhängigen Verfahren
 - Diskussion der Auswirkungen der getroffenen Aussagen zur Risikoakzeptanz auf den Bahnbetrieb nach Einführung von GoA 3 bzw. 4.
- Die Verifizierung der Ergebnisse der Arbeitspakete fand in Form eines Reviews statt. Das Review fand in zwei Phasen statt. Zum einen war der TÜV Rheinland bei der Präsentation und Diskussion der Zwischenergebnisse anwesend. Hierbei wurde in Diskussionen bereits besprochen, ob die Arbeiten in die richtige Richtung gehen. Diese Arbeiten fanden vor der Erstellung der relevanten Berichte statt. Die in Diskussionen geäußerten Aspekte wurden berücksichtigt. Der Validierer hat hierbei seine Meinung geäußert, aber trotzdem genügend Freiraum gelassen, sodass dem Projektteam keine Entscheidung vorgegeben wurde. Eine derartige Arbeitsweise ist wichtig, um zum einen frühestmöglich auf Probleme hinzuweisen – andererseits aber auch, um die Unabhängigkeit des Validierers nicht zu gefährden.

Im Rahmen des Reviews wurden keine methodischen Mängel festgestellt. Die Quellen für die Funktionsliste sind korrekt gewählt. Es kann davon ausgegangen werden, dass die Funktionsliste korrekt und vollständig ist. Auch bei den weiteren Vorbereitungen bezüglich der Schwereklassifikation von Unfällen und der Effizienz von Barrieren wurden keine Mängel entdeckt.

Die Bestimmung von menschlichen Fehlerwahrscheinlichkeiten wurde nach gängigen und im Bahnbereich anwendbaren Verfahren durchgeführt [2]. Dasselbe trifft auf die Ableitung von TFFR-Werten für technische Systeme zu, die den Triebfahrzeugführer (Tf) ersetzen sollen [4].

Die Validierung der Endergebnisse wurde in zwei Schritten durchgeführt. Im ersten Schritt wurde eine Kreuzvalidierung der Ergebnisse durchgeführt. Im zweiten Schritt wurde eine Validierung der Ergebnisse gegenüber anderen Quellen für menschliche Fehler durchgeführt. Im Rahmen der Validierung der Ergebnisse wurden unabhängige Berechnungen und Betrachtungen durchgeführt, insbesondere mit

- Validation of the final results by comparing the work results to the status quo GoA 2 as well as risk acceptance GoA 3/4
- Derivation of significant results using an independent method
- Discussion of the effects of the statements made on risk acceptance on rail operations after the introduction of GoA 3/4.

The validation of the results of the work packages took place in the form of a review. The review took place in two phases. Firstly, TÜV Rheinland as the validator was present during the presentation and discussion of the interim results. Here, discussions were held to determine whether the work was going into the right direction. This work took place before the relevant reports were prepared. The aspects expressed in discussions were taken into account. The validator expressed his opinion here, but still left enough room for manoeuvre so that no decision was imposed on the project team. Such a way of working is important, on the one hand, in order to point out problems as early as possible but also, on the other, in order not to endanger the independence of the validator.

No methodological deficiencies were identified during the review. The sources for the function list have been chosen correctly. It can be assumed that the functional list is correct and complete. No deficiencies were found in the further preparations regarding the severity classification of accidents nor the efficiency of barriers.

The determination of human error probabilities was carried out according to common procedures applicable in the railway sector [2]. The same applies to the derivation of TFFR values for technical systems that are to replace the driver [4]. The validation of the final results was performed in two steps. In the first step, a cross-validation of the results was performed. In the second step, a validation of the results against other sources of human error was performed.

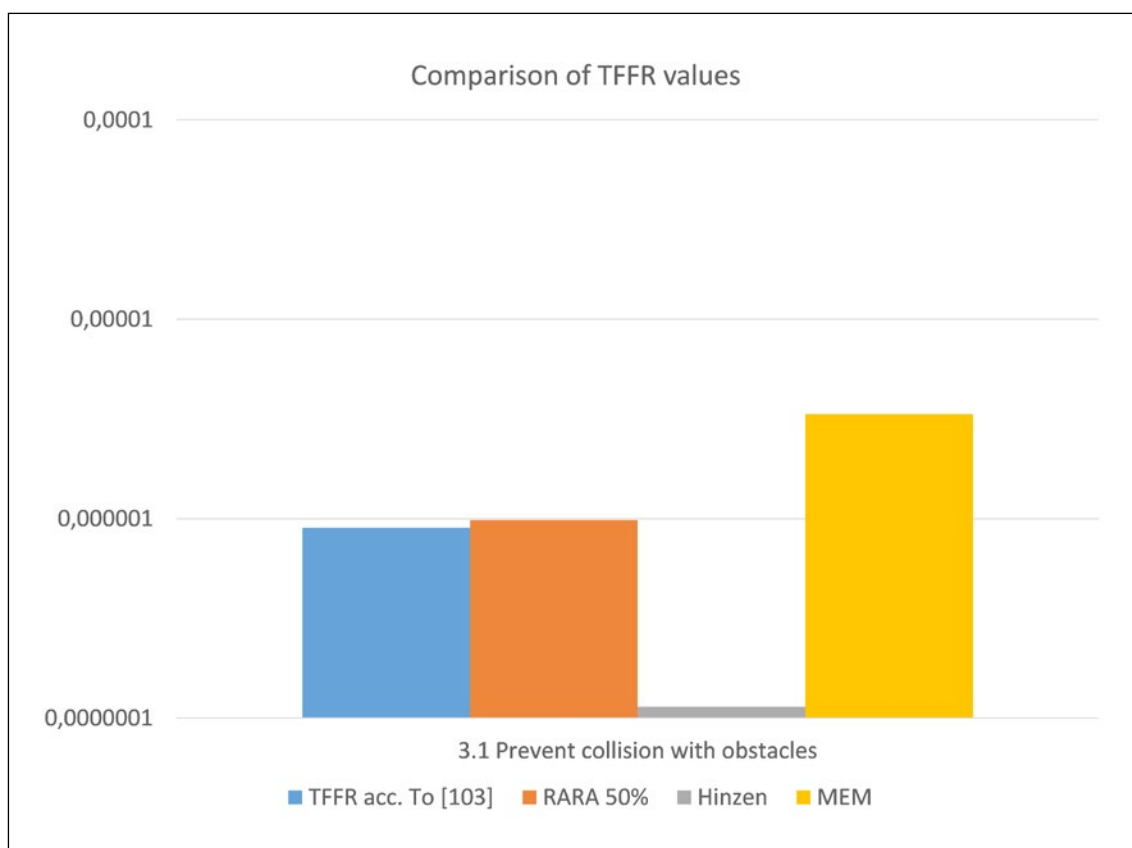


Bild 2: Beispiel für den Vergleich von Ergebnissen

Fig. 2: Example of comparison of results
Quelle / Source: TÜV Rheinland

dem MEM-Prinzip und dem Vergleich mit Unfallstatistiken. Dabei konnten die Ergebnisse vom Prinzip her bestätigt werden, jedenfalls soweit man das bei vier unterschiedlichen (semi-) quantitativen Verfahren erwarten kann (siehe Bild 2 für ein Beispiel).

Allerdings ergeben sich gerade im Vergleich mit der klassischen Bewertungsmethode nach Hinzen [12] erhebliche Abweichungen, die untersucht werden müssen.

3 Diskussion der Ergebnisse

Die Abstimmung der Ergebnisse mit den Ergebnissen zur Analyse des Referenzsystems GoA 2 war nur bei Funktionen möglich, für die eine explizite Risikoanalyse durchgeführt wurde, aber dies umfasste insbesondere die wichtige Funktionsgruppe der Hinderniserkennung. Hier konnte zumindest gezeigt und durch die Validierung bestätigt werden, dass aus Sicht des Status quo bei GoA 2 keine Widersprüche zu den Ergebnissen der expliziten Risikoanalyse bestehen. Ein detaillierter Vergleich war hier nicht sinnvoll, da einerseits schon die Ergebnisse der etablierten Methoden der menschlichen Zuverlässigkeitsanalyse teilweise erhebliche Unterschiede aufwiesen [2], andererseits aber auch die menschlichen Zuverlässigkeitsanalysen eines anderen Zuschnitts der Funktionsliste bedurften als bei der technischen Realisierung [1]. Dabei muss erwähnt werden, dass auch keine bessere Ergebnisqualität gefordert bzw. erwartet worden war, sondern quantitative Ergebnisse sollten in der Größenordnung übereinstimmen. Dies ist in allen Fällen erreicht worden.

Man kann die Ergebnisqualität mit den Ergebnissen und Erfahrungen von Hinzen [12] vergleichen, der Ergebnisse von Modellrechnungen gegenüber Unfallstatistiken validiert hat: Z.B. für Zusammenstöße von Zügen ergab sich statistisch ein Mittelwert von $3,3 \times 10^{-8}$ (die Einheiten und andere Parameter sollen hier zur Vereinfachung vernachlässigt werden), während sich auf Basis der Modellrechnung $1,2 \times 10^{-7}$ ergab, d.h. der numerische Unterschied betrug etwa Faktor 3,6 (wobei das Modell konservativer war als die Betriebsstatistik, d.h. die Hinzen-Methode lieferte pessimistischere Ergebnisse). Wäre der numerische Unterschied 10 gewesen, so wäre die statistische Sicherheit zwar geringer, aber bei solch komplexen Modellen immer noch akzeptabel.

Um die Ergebnisse besser interpretieren zu können, sollte man allerdings reflektieren, woher die teilweise deutlichen Unterschiede, z.B. in Bild 2 dargestellt, kommen. Da ist zunächst der offensichtliche Unterschied der beiden Bewertungsmethoden der menschlichen Zuverlässigkeit, der Hinzen-Methode und RARA (auf die Diskussion von Varianten wird hier verzichtet). Dazu ist es sinnvoll, sich zu vergegenwärtigen, dass sich die Fehlerwahrscheinlichkeit p einer menschlichen Handlung in erster Näherung wie folgt zusammensetzt

$$p \approx p_w + p_v + p_r$$

Dabei stehen die Indizes für Wahrnehmung (w), Verarbeitung (v) und Reaktion (r), in Analogie zu Automatisierungssystemen (Sensorik, Verarbeitung, Aktorik). Die Hinzen-Methode wurde Ende der 1980er Jahre entwickelt und mit betrieblichen Daten validiert. Allerdings stand damals die Verarbeitung der Information im Vordergrund und war für die Ergebnisse maßgeblich, die Wahrnehmung und die Reaktion waren eher untergeordnet. Dies entsprach auch der Technik und dem Betrieb dieser Zeit, wo sich die Wahrnehmung z.B. auf die Erkennung von Signalen oder Ausleuchtungen am Stellisch im Relaisstellwerk bezog und die Reaktion auf das Drücken von Tasten oder Ziehen von Hebeln. Man konnte also davon ausgehen,

As part of the validation of the results, independent calculations and observations were carried out, in particular using the MEM principle and comparison with accident statistics. In doing so, the results could be confirmed in principle, at least as far as can be expected with four different (semi-)quantitative methods (see fig. 2 for an example).

However, especially in comparison with the classical evaluation method according to Hinzen [12] there are considerable deviations, which have to be investigated.

3 Discussion of the results

The reconciliation of the results with the results for the analysis of the reference system GoA 2 was only possible for functions for which an explicit risk analysis was carried out, but this included in particular the important function group of obstacle detection. Here it could at least be shown and confirmed by the validation that from the point of view of the status quo in GoA 2 there are no contradictions with the results of the explicit risk analysis. A more detailed comparison was not meaningful here, since on the one hand the results of the established methods of human reliability analysis already showed partly considerable differences [2], but on the other hand the human reliability analyses also required a different cutting of the function list than in the technical realisation [1]. In this context it also has to be mentioned that no better result quality was demanded or expected, but quantitative results should agree in the order of magnitude. This has been achieved in all cases.

The quality of the results can be compared with the results and experiences of Hinzen [12], who validated the results of model calculations against accident statistics: e.g. for collisions of trains, the statistical mean value was 3.3×10^{-8} (the units and other parameters are neglected here for sake of simplicity), whereas on the basis of the model calculation, the mean value was 1.2×10^{-7} , i.e., the numerical difference was about a factor of 3.6 (where the model was more conservative than the operational statistics, i.e., Hinzen's method gave more pessimistic results). If the numerical difference had been 10, the statistical confidence would have been lower, but still acceptable for such complex models.

However, in order to be able to better interpret the results one should reflect on where the partly significant differences, e.g., shown in fig. 2, come from. First of all, there is the obvious difference between the two evaluation methods of human reliability, the Hinzen method and RARA (we will refrain from discussing variants here). To this end, it is useful to remember that the error probability p of a human action is composed as follows in a first approximation

$$p \approx p_w + p_v + p_r$$

Here, the indices stand for perception (w), processing (v) and reaction (r), in analogy to automation systems (sensors, processing, actuators). The Hinzen method was developed in the late 1980s and validated with operational data. At that time, however, the processing of the information was the main focus and was decisive for the results, while perception and reaction were rather subordinate. This was also consistent with the technology and operations of the time, where perception was related to, for example, detecting signals or illuminations at the control desk in

dass die Informationsverarbeitung hier den maßgeblichen Anteil darstellt

$$p_{\text{Hinzen}} \approx p_v, \text{ da } p_r, p_w \ll p_v$$

Dies wird auch in [12] eindeutig festgestellt: „Die drei Verhaltensebenen im Modell sind durch folgende Schwierigkeitsniveaus der Informationsverarbeitung charakterisiert: Fertigungs-basierendes Verhalten [...], Regel-basierendes Verhalten [...], Wissens-basierendes Verhalten [...]“. Dies erklärt, warum man mit der Hinzen-Methode oft zu sehr konservativen, von den anderen Methoden abweichenden Ergebnissen gelangt, da bei vielen Handlungen nicht die Informationsverarbeitung, sondern die Wahrnehmung maßgeblich ist [1] und deshalb hier gilt

$$p_{\text{Hinzen}} \approx p_v \ll p_w \approx p$$

Bei der RARA-Methode sieht es, auch in der bei ATO-RISK verwendeten Variante, ähnlich aus: Grundsätzlich folgt RARA derselben Aufteilung der Handlungen wie Hinzen, d. h. auch hier wird die Verarbeitung als „führender Faktor“ betrachtet, aber die Einteilung erfolgt differenzierter und eisenbahnspezifisch von R1 bis R8, wobei alleine die ersten fünf Aufgabentypen (sog. GTT, vgl. [2]) im Kern fertigungs-basiert sind und nur R8 wissensbasiert. Insbesondere die weiteren Faktoren (sog. EPC, [2]), die berücksichtigt werden können, können es ermöglichen, auch Probleme der Wahrnehmung und Reaktion mit zu berücksichtigen. Daher ist das Modell bei RARA grob wie folgt:

$$p_{\text{RARA}} \approx p_v \times f_1 \times \dots \times f_n$$

D. h. RARA verwendet ein multiplikatives Modell, wobei die zusätzlichen Faktoren größer als Eins sind. Um jetzt Fehler bei der Wahrnehmung angemessen zu berücksichtigen, braucht es also adäquate Faktoren, und die müssen auch verwendet werden. Hier kommen z. B. T2 (Zeitmangel zur Fehlererkennung und -korrektur), In1 (geringer Signal-Rausch-Abstand, d. h. schlechte Erkennbarkeit aufgrund von Umgebungsbedingungen) oder P2 (Einfluss des Schichtdienstes) in Frage, aber dies sind eher zur Verarbeitung beitragende denn eigenständige Faktoren, die sich auf die Wahrnehmung beziehen [1]. D. h. auch hier kann man annehmen, dass die Abschätzung eher konservativ ist, allerdings nicht so stark wie bei Hinzen:

$$p_{\text{RARA}} \approx p_v \times f_1 \times \dots \times f_n < p_w \approx p$$

Dabei wurde weiterhin nicht berücksichtigt, dass die RARA-Methode, geschweige denn die Anpassungen, bisher nicht für den deutschen Eisenbahnverkehr validiert wurde, sondern nur im Vereinigten Königreich und dass eventuell bestehende Unterschiede in den Eisenbahnbetrieben auch noch die Ergebnisse verzerren können. Dies bedeutet, dass derzeit eine Risiko- oder Sicherheitsanalyse für ATO GoA 3 oder 4, die sich allein auf Methoden der menschlichen Zuverlässigkeitsanalyse stützt, nicht zielführend ist, sondern nur einen unterstützenden Charakter haben kann. Entweder müssten Methoden angewendet werden, die die Aspekte der Wahrnehmung besser abbilden (und diese müssten auch noch validiert werden), oder es müssen sehr spezifische Analysen wie z. B. in ATO-SENSE erfolgen, die sich nur mit der Wahrnehmung beschäftigen. Hier besteht u. U. noch weiterer Forschungsbedarf, insbesondere, da die Hinzen-Methode und auch RARA sich strukturell in ihren Ansätzen

the relay interlocking, and reaction was related to pressing buttons or pulling levers. One can therefore assume that the information processing represents the decisive part here

$$p_{\text{Hinzen}} \approx p_v, \text{ da } p_r, p_w \ll p_v$$

This is also clearly stated in [12]: “The three levels of behaviour in the model are characterised by the following difficulty levels of information processing: Skill-based behaviour [...], Rule-based behaviour [...], Knowledge-based behaviour [...]”. This explains why the Hinzen method often leads to very conservative results that deviate from the other methods, since in many actions it is not information processing, but perception that is decisive [1] and therefore the following applies here

$$p_{\text{Hinzen}} \approx p_v \ll p_w \approx p$$

The RARA method looks similar, also in the variant used in ATO-RISK: basically, RARA follows the same division of actions as Hinzen, i. e., processing is also considered as the “leading factor” here, but the division is more differentiated and railway-specific from R1 to R8, where alone the first five task types (so-called GTT, cf. [2]) are skill-based in the core and only R8 is knowledge-based. In particular, the additional factors (so-called EPC, cf. [2]) that can be taken into account may allow problems of perception and response to be included. Therefore, the model in RARA is roughly as follows:

$$p_{\text{RARA}} \approx p_v \times f_1 \times \dots \times f_n$$

I. e. RARA uses a multiplicative model, where the factors are greater than one. So now to adequately account for errors in perception, adequate factors are needed and must be used. Here, for example, T2 (lack of time to detect and correct errors), In1 (low signal-to-noise ratio, i. e., poor detectability due to environmental conditions) or P2 (influence of shift work) come into play, but these are factors contributing to processing rather than independent factors relating to perception [1]. It can be assumed again that the estimate is rather conservative, but not as strong as Hinzen’s:

$$p_{\text{RARA}} \approx p_v \times f_1 \times \dots \times f_n < p_w \approx p$$

Furthermore, it was not taken into account that the RARA method, let alone the adaptations, has not yet been validated for German rail transport but only in the United Kingdom, and that differences may exist in the railway undertakings that may also distort the results. This means that a risk or safety analysis for ATO GoA 3 or 4 that is based solely on methods of human reliability analysis would currently not be useful, but could be of a supporting nature. Either methods that better represent the aspects of perception would have to be applied (and these would also have to be validated), or very specific analyses such as in ATO-SENSE would have to be carried out that only deal with perception. There may be a need for further research here, especially as the Hinzen method and also RARA are structurally different in their approaches to the requirements (multiplicative model compared to the additive model required).

zen von den Anforderungen unterscheiden (multiplikatives Modell im Vergleich zum benötigten additiven Modell).

4 Zusammenfassung

Zusammenfassend lässt sich damit feststellen, dass die explizite Risikoanalyse nach DIN VDE V 0831-103 prinzipiell geeignet ist, um Risikoakzeptanzkriterien für ATO-Projekte abzuleiten. Die Methode nach Hinzen führt teilweise zu schärferen Anforderungen, dies ist jedoch in der Konstruktion bzw. Anwendung der Methode begründet, die nicht für alle betrachteten Funktionen geeignet ist.

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 semi-quantitativen Risikoanalyse auf Grundlage von DIN VDE V 0831-103 gezeigt.

Die EBO [10] fordert die Anwendung „Anerkannter Regeln der Technik“, dies ist etwas strenger als der Grundsatz der Risikoakzeptanz „Anwendung von Regelwerken“ der CSM-VO [9], da nicht alle Regelwerke zugleich auch anerkannte Regeln der Technik sind, siehe [9] Abschnitt 2.3.2 zu den Kriterien, welches Dokument als Regelwerk

4 Summary

In summary, it can thus be stated that the explicit risk analysis according to DIN VDE V 0831-103 is in principle suitable for deriving risk acceptance criteria for ATO projects. The method according to Hinzen leads in part to stricter requirements, but this is due to the construction or application of the method, which is not suitable for all functions considered.

Overall, it can be stated that the approach of risk analysis in accordance with the CSM Regulation proved to be very advantageous, as it was possible to adopt existing specifications when using the risk acceptance principles of “codes of practice” or “reference system”. The rules and regulations used as codes of practice included, in particular, building regulations, regulations on fire protection or regulations on the transport of hazardous goods. In addition, the advantage of a semi-quantitative risk analysis based on DIN VDE V 0831-103 was demonstrated for those sub-functions for which neither a set of rules nor a reference system existed.

The EBO [10] requires the application of recognised rules of technology, which is somewhat stricter than the “application of codes of practice” principle of risk acceptance of the CSM Regulation [9], since not all rules and regulations are also recognised codes of practice, see [9] Section 2.3.2 on the criteria as to which document can be regarded as a set of codes of practice. If safety cannot be demonstrated by means of the



THE FUTURE OF COMMUNICATION BY RAIL

Future-proof your railway operations with us

Funkwerk develops, produces & sells professional communication solutions for railways. We continue to set new technical standards: We have a fixed eye on the future train radio standard FRMCS & are actively involved in its development.

- » supplement our modular MESA® product family with powerful 5G radio modules
- » we secure your investment with multi-mode train radios “Made in Germany”
- » contact us now!

betrachtet werden kann. Wenn man die Sicherheit nicht mithilfe der Regeln der Technik nachweisen kann, so eröffnet die EBO [10] in Ziffer (2) die Möglichkeit eines Nachweises der gleichen Sicherheit, z. B. über ein Referenzsystem.

Ein Nachweis gleicher Sicherheit kann nun darüber geführt werden, dass zum einen in einem ersten Schritt hinreichende Sicherheitsanforderungen gestellt werden und in einem weiteren Schritt die Erfüllung derselben nachgewiesen wird. Mit dem Forschungsprojekt ATO-RISK ist nun der erste Schritt erfolgt.

Dies bedeutet letztendlich, dass ATO-RISK derartige Sicherheitsanforderungen abzuleiten hat, dass auf keinen Fall ein niedrigeres Sicherheitsniveau erreicht wird als vor dem Ersetzen des Tf durch technische Systeme.

Es kann davon ausgegangen werden, dass aufgrund des konservativen Ansatzes bei der Ableitung der Anforderungen an technische Systeme eher mit einem höheren Sicherheitsniveau nach dem Ersetzen des Tf durch technische Systeme zu rechnen ist, vorausgesetzt, bei der Entwicklung und Implementierung der Systeme werden die relevanten Normen und Regelwerke beachtet. ■

recognised rules of technology, the EBO [10] opens up the possibility of demonstrating the same safety in clause (2), e.g., by means of a reference system.

Proof of the same level of safety can now be provided by setting adequate safety requirements in a first step and proving that these requirements are met in a further step. The first step has now been taken with the ATO-RISK research project. This ultimately means that ATO-RISK has to derive such safety requirements that in no case can a lower safety level be achieved than before the replacement of the driver by technical systems.

It can be assumed that, due to the conservative approach taken in deriving the requirements for technical systems, a higher level of safety can be expected after the replacement of the driver by technical systems provided that the relevant standards and regulations are observed in the development and implementation of the systems. ■

LITERATUR | LITERATURE

- [1] Deutsches Zentrum für Schienenverkehrsforschung: Risikoakzeptanzkriterien für das automatisierte Fahren auf der Schiene (ATO-RISK), Abschlussbericht, 2023
- [2] Adebahr, F.; Schäbe, H.: Die Wahrscheinlichkeit menschlicher Fehler und Ausfallraten technischer ATO-Systeme, SIGNAL+DRAHT 03/2023, pp. 21 – 29
- [3] Voigt: Auswertung Unfalldatenbank der Bundesstelle für Eisenbahnunfalluntersuchung (BEU) (01.01.2017 bis 26.04.2021), ausgewertet am 18.05.2021
- [4] Braband, J.; Lindner, L.; Rexin, F.: Risikoanalyse für die Hinderniserkennung beim Automatischen Fahren, SIGNAL+DRAHT 03/2023, pp. 12 – 20
- [5] Braband, J.: Risikoanalysen in der Eisenbahn-Automatisierung, Eurailpress, 2005
- [6] Braband, J.: Funktionale Sicherheit, in: Fendrich, L. (Hrsg.): Handbuch Eisenbahninfrastruktur, Springer Verlag, 2019, S. 583-638
- [7] Braband, J.: Vorgehensweise bei der Risikoanalyse Automatisches Fahren, SIGNAL+DRAHT 10/2021, S. 25-34
- [8] Braband, J.; Schäbe, H.: Propagation of uncertainty in railway signaling risk analysis, in: Safety and Reliability of Complex Engineered Systems – Podofilini et al. (Eds), Proc. ESREL 2015, Taylor & Francis Group, London, 2015, 2623-2626
- [9] 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
- [10] 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)
- [11] Report on Railway Safety and Interoperability in the EU, 2020
- [12] Hinzen, A.: Der Einfluss des menschlichen Fehlers auf die Sicherheit der Eisenbahn, Dissertation, RWTH Aachen, 1993
- [13] DIN VDE V 0831-103: Elektrische Bahnsignalanlagen – Teil 103: Ermittlung von Sicherheitsanforderungen an technische Funktionen in der Eisenbahnsignaltechnik, 2020
- [14] DIN EN 50129:2019: Bahnanwendungen – Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme – Sicherheitsbezogene elektronische Systeme für Signaltechnik, 2018

AUTOREN | AUTHORS

Prof. Jens Braband

Principal Key Expert

Siemens Mobility GmbH

Anschrift / Address: Ackerstraße 22, D-38126 Braunschweig

E-Mail: jens.braband@siemens.com

Dr. Hendrik Schäbe

Principal Assessor RAMS

TÜV Rheinland Intertraffic GmbH

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

E-Mail: schaebe@de.tuv.com