Standortbestimmung des DZSF zum Thema ATO

Teil 1: Grundlagen und Sicherheitsanforderungen

KAI HOFMANN | RUSTAM TAGIEW | ROMAN TILLY | CHRISTIAN KLOTZ | MARKUS REINHARDT

Automatic Train Operation (ATO) – der automatisierte Bahnbetrieb – ist eines der großen Innovationsthemen im Sektor. Die Entwicklung entsprechender ATO-Systeme ist in erster Linie Aufgabe der Industrie. Das Deutsche Zentrum für Schienenverkehrsforschung (DZSF) befasst sich u. a. damit, wie ATO-Systeme genehmigt werden können. Dazu erarbeitet es im Austausch mit dem Sektor die Grundlagen, anhand derer Sicherheitsanforderungen und -nachweise für ATO im Eisenbahnbereich erbracht werden können. Ziel der Arbeit in Bezug auf ATO ist es, perspektivisch einen wissenschaftlich-technischen Konsens unter den relevanten Akteuren herbeizuführen. Dieser Beitrag gibt eine Übersicht, welche Forschungslücken in der Sicherheitsbewertung von ATO-Systemen bestehen, welche Ergebnisse bisher hervorgebracht wurden und welche Fragen in den nächsten Projekten untersucht werden. Das DZSF ist eine Ressortforschungseinrichtung des Bundesministeriums für Digitales und Verkehr (BMDV) und organisatorisch im Eisenbahn-Bundesamt (EBA) eingegliedert. Die hier dargestellte Perspektive ist dennoch diejenige der Forschung, nicht notwendigerweise die des Bundes und des EBA.

Grundlagen und Begriffe

Im Umfeld von ATO werden Begriffe oft unterschiedlich verwendet und ausgelegt. Daher erfolgt eine Beschreibung relevanter Begriffe für diesen Artikel, auf Grundlage der Verwendung im DZSF.

ATO und seine Automatisierungsstufen

Die Abgrenzung verschiedener Grade der Automatisierung (engl. „Grade of Automation" [GoA], unterteilt in GoA 0 bis 4) stammt aus dem Bereich des städtischen Schienenpersonennahverkehrs (Tab. 1). Sie gelten nur für unabhängige Bahnen, deren Fahrweg vom übrigen Verkehr baulich getrennt ist (§ 1 Abs. 2 Nr. 2 BOStrab), also U- und Hochbahnen. Auf Eisenbahnen nach Verständnis der europäischen Regulierung und der Eisenbahn-Bau- und Betriebsordnung (EBO) können diese Begriffe nicht unbesehen übertragen werden. Gemessen an dieser Definition, werden die Automatisierungsstufen in der Eisenbahn uneinheitlich verwendet. Der Stand der Technik in Europa ist „ATO over ETCS", das auf freier Strecke GoA 2 entspricht. Fahren diese Züge – wie in Hamburg – in der Abstellanlage ohne Triebfahrzeugführer (Tf), hebt das den Automatisierungsgrad nicht ohne Weiteres auf GoA 4. Entscheidend ist, wie sichergestellt wird, dass sich dort u. a. keine Personen im Gleis befinden. Beobachtet dazu eine Person die Gleise – nur von einem anderen Standort aus –, verbleibt die Aufgabe beim Menschen und der Automatisierungsstand bei GoA 2. Ein Fahrzeug ohne Tf an Bord führt nicht direkt zu einer Einstufung als GoA 4-System.

Ähnlich unklar sind Zwischenstufen wie z. B. ATO GoA 2.5, da mit solchen Verrechnungen der Stufen nur Verwirrung erzeugt wird. Verwendet wird das bei Konzepten, in denen die Hinderniserkennung von Menschen ohne Ausbildung als Tf übernommen wird, die bei Gefahr einen „Not-Aus Taster" bedienen [1], oder GoA 2+ für Systeme, die abschnittweise auch GoA 4 fahren können [2]. Im DZSF werden diese Beispiele in die vollständig erreichte Stufe GoA 2 eingeordnet. Unter GoA 3+ wird eine Zusammenfassung der Stufen 3 und 4 verstanden.

Sinnvoll erscheint es, die Einteilung der GoA-Stufen vom Tf zu lösen und danach vorzunehmen, welche Basisfunktionen noch vom Menschen – ob im Fahrzeug oder an anderer Stelle – abgedeckt werden müssen. Wie die im System realisierten Funktionen technisch umgesetzt werden, ist zweitrangig. Für die Einteilung in GoA-Stufen ist es unerheblich, ob z. B. die Signalerkennung über European Train Control System (ETCS) direkt oder per Kamera und Bilderkennung erfolgt.

Automatisiert, automatisch – autonom

Die Begriffe „automatisiert" und „automatisch" werden im DZSF für ATO synonym verwendet. Autonomie ist die Fähigkeit einer Instanz (z. B. eines Fahrzeugs mit allen Subsystemen), innerhalb eines definierten Aufgabenbereiches ohne aktive und notwendige Eingriffe anderer Instanzen zu operieren. Am Beispiel der Hinderniserkennung hieße das: Werden z. B. bahnfremde Objekte im Gleis wie in der Nürnberger U-Bahn durch Sensorik am Gleis erkannt und wird das Fahrzeug daraufhin gestoppt, fällt das unter automatisiert. Ein Fahrzeug, das hierfür selbst Sensorik verbaut hat und die Entscheidung an Bord trifft, bremst autonom.

Einsatz Künstlicher Intelligenz (KI) bei ATO

ATO erfordert, dass technische Systeme auf Basis von Eingabeparametern und Regeln Ergebnisse berechnen, aufgrund deren Basis Entscheidungen getroffen werden. Wenn Entscheidungen hinreichend komplex sind und die Systeme somit menschliche Entscheidungsfähigkeiten nachahmen, werden sie in der Regel als „Künstliche Intelligenz" (KI) bezeichnet.

Im Hinblick auf die Sicherheitsbewertung ist eine wesentliche Unterscheidung bei KI-Systemen, ob ihre berechneten Ergebnisse und Entscheidungen vor Inbetriebnahme voll-

Basisfunktionen des Fahrbetriebs	GoA 0	GoA 1	GoA 2	GoA 3	GoA 4	Umsetzung im Fahrzeug, vereinfacht
BF1: Zugbewegung absichern (systeminterne Gefahren)	Mensch	X	x	x	x	PZB, LZB, evtl. Bildverarbeitung im Rangierbetrieb
BF2: Zugbewegung steuern (Beschleunigen und Bremsen)	Mensch	Mensch	x	x	x	ETCS, evtl. Bildverarbeitung mit Signalerkennung
BF3: Fahrweg frei von ext. Hindernissen (z. B. Personen im Gleis)	Mensch	Mensch	Mensch	x	x	Bildverarbeitung zur Hinderniserkennung
BF4: Betreiben des Zugs (wie Türen, Bremsprobe, Notfälle)	Mensch	Mensch	Mensch	Mensch	x	Diverse Subsysteme

Tab. 1: GoA-Zuordnung der Basisfunktionen (BF), abstrahiert aus DIN EN 62267

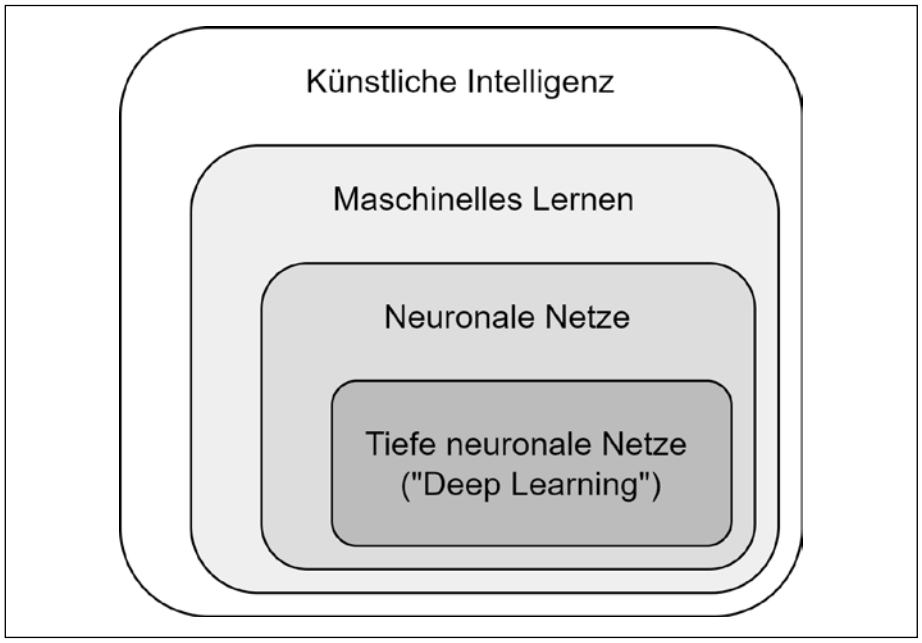

Abb. 1: Abgrenzung verschiedener KI-Implementierungen

ständig prüfbar sind. Vollständige Prüfbarkeit kann z. B. dadurch erreicht werden, dass die Entscheidungsregeln nachvollzogen werden können oder das Entscheidungsverhalten unter allen Eingabeparametern auf Korrektheit geprüft werden kann. Vollständige Prüfbarkeit ist aber gerade bei solchen KI-Systemen häufig nicht gegeben, deren Entscheidungsverhalten anhand von maschinellen Lernverfahren (ML) auf Basis von Trainingsdaten erlernt werden. Insbesondere sind hier KI-Implementierungen aus dem Bereich des Lernens mittels tiefer neuronaler Netze (engl. „Deep Learning", DL) zu nennen (Abb. 1). Diese haben sich als sehr leistungsfähig erwiesen (z. B. Bilderkennung, Textanalyse, Übersetzung), entziehen sich aber aufgrund der komplexen und umfangreichen Struktur einer vollständigen Prüfung.

Bei ML wird eine Abbildung zwischen Eingabeparametern und den zu ermittelnden Ergebnisgrößen durch Minimierung der Verlustfunktion erstellt, was als auch „Training" bezeichnet wird. Nach Abschluss des Trainings wird diese Abbildung im Betrieb verwendet, um für neue Eingabeparameter die unbekannten Ergebnisgrößen zu ermitteln. Die Abbildung ist für menschliche Entwickler kaum nachvollziehbar und kann nicht vollständig, sondern nur für eine Menge von Testfällen vor dem Einsatz getestet werden. Eine Erweiterung ist das Online-Lernen. Dabei wird die Abbildung im Betrieb weitertrainiert. Da damit Entscheidungsgrundlagen permanent verändert werden, kann Online-Lernen aus Sicherheitsgründen absehbar für ATO nicht zum Einsatz kommen [3]. Ein KI-System kann nur solche Situationen beherrschen und Aufgaben sicher erfüllen, die bereits in der Systemdefinition enthalten sind. Deshalb sollten auch für den Bahnbetrieb Operational Design Domains (ODD) wie im Automobilsektor definiert werden. Als Vorarbeit hierzu soll das geplante Projekt „Einsatzszenarien ATO" eine Systematik der Szenarien für ATO liefern, die für die Entwicklung und Zulassung von KI für ATO verwendet werden kann.

Bezogen auf ATO lassen sich Basisfunktionen (BF) für die Absicherung der Zugbewegung (BF1, Tab. 1) sowie die Steuerung der Zugbewegung (BF2) mit vollständig prüfbaren KI-Systemen (meistens einfach als Software bezeichnet) implementieren und sind im bestehenden rechtlichen Rahmen zulassungsfähig. Die Prüfung, ob der Fahrweg frei von externen Hindernissen ist (BF3), stellt allerdings an technische Systeme die Anforderung, das Zugumfeld zu überwachen und auf Hindernisse zu reagieren, wie es derzeit der Tf durch visuelle Prüfung und menschliche Intelligenz leistet. Die Umfeldüberwachung für BF3 umfasst mehrere Teilprobleme aus dem Bereich der Bildverarbeitung, darunter

- die Anwesenheit von Objekten zu erkennen,
- Objekte im Raum zu lokalisieren,
- Objekte zu klassifizieren,
- Objekte zu identifizieren,
- Objekte über mehrere Erfassungszeitpunkte zu verfolgen und
- das zukünftige Verhalten von Objekten zu prognostizieren.

Für BF4 kommen voraussichtlich kleinere Module zum Einsatz, die entweder ohne ML entwickelt werden können (z. B. Überwachung des Fahrgastwechsels) oder über Teleoperation gelöst werden müssen (z. B. Notfallsteuerung).

Sicherheitsanforderungen

Zur Sicherheit eines Systems ab GoA 3 existieren im Eisenbahnbereich noch keine Vorgaben in den europäischen TSI oder nationalen Vorschriften. Die Sicherheitsanforderungen müssen darum anhand des generischen Risikobewertungsverfahrens der CSM RA-VO (EU) 402/2013 ermittelt werden.

Der genaue Ablauf und der Detaillierungsgrad dieses iterativen Prozesses richten sich nach dem verwendeten Risikoakzeptanzgrundsatz (2.1.4. CSM RA, Abb. 2). In Ermangelung einschlägiger Regelwerke oder technischer Referenzsysteme muss hier explizit bewertet werden. Dazu werden die ermittelten Gefährdungen in Ausfallszenarien gegliedert und entsprechende Sicherheitsmaßnahmen festgelegt (2.1.6. CSM RA). Das durch die Sicherheitsmaßnahme beschränkte Risiko wird abgeschätzt (Risikoanalyse) und mit einem Risikoakzeptanzkriterium verglichen (Risikoevaluation). Bleibt das abgeschätzte innerhalb des akzeptierten Risikos, ist die Sicherheitswirkung der Maßnahme(n) ausreichend. Die innerhalb dieser Risikobeherrschung ausgewählten Sicherheitsmaßnahmen werden als Sicherheitsanforderungen in die Systemdefinition aufgenommen.

Systemdefinition

Untersuchungen zur Sicherheit und Funktion von ATO erfordern eine Beschreibung des Systems mit dem Anspruch auf Vollständigkeit und Abgrenzung. Je nach Betrachtungsgegenstand können unterschiedliche Aspekte im Fokus stehen.

In der Systemdefinition im Sinne der CENELEC-Normen oder der CSM RA wird der Gegenstand der Sicherheitsbewertung festgelegt. Es müssen Zweck, Grenzen und Umgebungsbedingungen des Systems definiert werden. Im Fokus steht der Bahnbetrieb mit seinen Grundfunktionen und Schutzzielen. Zunächst unabhängig davon, welche Aufgaben dabei an Fahrzeug oder Infrastruktur, LST und ATO fallen, müssen am Ende die Risiken beherrscht werden. Das DZSF-Projekt „ATO Risk" hat eine generische Systemdefinition auf Systemebene anhand DIN VDE V 0831-101 und DIN VDE V 0831-103 erstellt. Dieser Ansatz hat den Vorteil, bei weitgehender Unabhängigkeit von der technischen Umsetzung das System zu charakterisieren.

Im laufenden Projekt „ATO Sense" liegt der Fokus auf dem Vergleich automatisierter Funktionen mit den Leistungen des Tf. Auf Basis der Ril 408 entsteht eine Aufgabenliste für ATO-Systeme.

Als weiterer Bestandteil einer Systemdefinition ist zudem eine Beschreibung des Systems im technischen Sinne erforderlich. Hierzu zählen z. B. dessen Zusammensetzung aus Komponenten, interne und externe Schnittstellen sowie die Umsetzung in technischer Ausrüstung und Softwaremethoden. Hier gibt es noch kein umfassendes gemeinsames Verständnis im Sektor. Ansätze, v. A. für GoA 2, finden derzeit Eingang in die Neufassung der TSI CCS.

Was sich bei der Automatisierung durch Wegfall von Menschen an allgemeinen zivilen Hilfeleistungen des Zugpersonals, Verfehlungen und auch Verwundbarkeiten sich ändert, soll im laufenden Projekt „ATO Akzeptanz" untersucht werden.

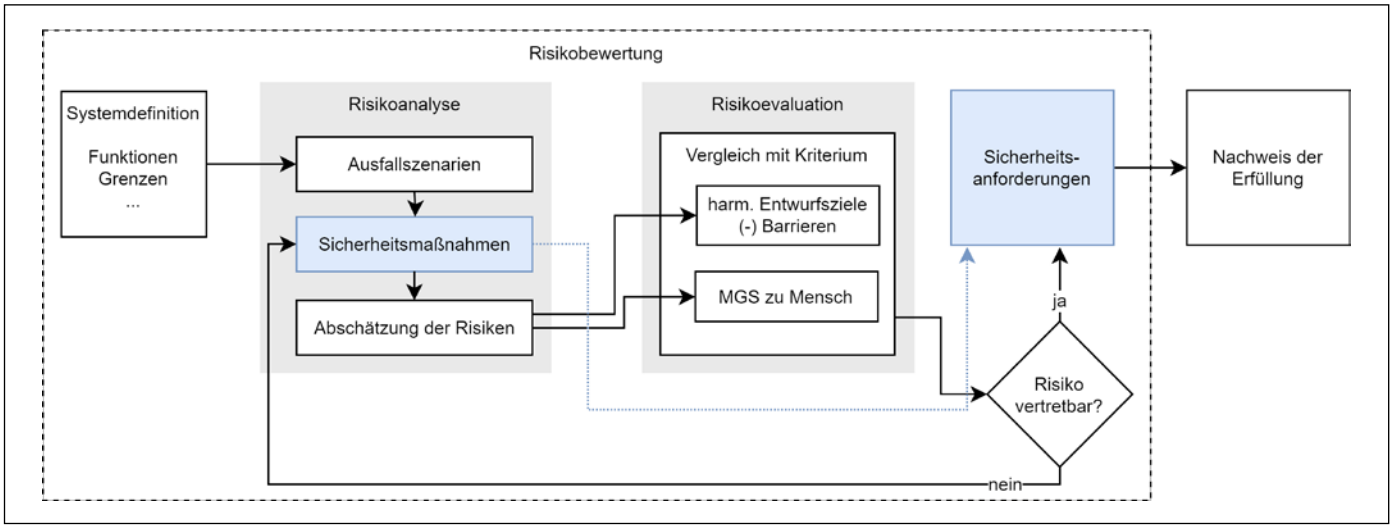

Abb. 2: Ablaufskizze der Risikobewertung

Risikoakzeptanz

Die Risikoabschätzung und -evaluierung richtet sich nach den Risikoakzeptanzkriterien aus 2.5.2. CSM RA für vertretbare Risiken. Die zwei Akzeptanzgrundsätze nach CSM RA sind: Mindestens die gleiche Sicherheit (MGS) wie das Referenzsystem sowie die harmonisierten Entwurfsziele. Die Risikoevaluierung erfolgt dabei separat für die einzelnen Funktionen laut Systemdefinition, sodass es möglich ist, je Funktion den Risikoakzeptanzgrundsatz zu variieren. Als Referenzsystem ab GoA 3 kommt ein durch einen Tf geführtes Fahrzeug (2.4.2. CSM RA) infrage. Weil ein Tf aber kein technisches System ist, können die Sicherheitsanforderungen nicht von den an Tf gestellten Anforderungen direkt abgeleitet werden (2.4.3. lit. b CSM RA). Stattdessen gilt es, die vom Tf beherrschten Risiken explizit zu analysieren. Dieses Sicherheitsniveau muss das zu bewertende System erreichen (2.4.4. CSM RA). Aus dem impliziten Risikogrundsatz wird so ein explizites Risikoakzeptanzkriterium. Das Projekt „ATO Sense" leitet aus dem Referenzsystem belastbare Anforderungen ab. Hier wird die menschliche Leistungsfähigkeit auf Basis theoretischer und experimenteller Vorarbeiten sowie Versuchen mit Tf in Fahrversuchen im Fahrsimulator ermittelt. Ziel ist es, ein Modell der menschlichen Leistungsfähigkeit abhängig von der Aufgabe sowie den inneren und äußeren Einflussfaktoren zu erstellen. Für die Zukunft beabsichtigt das DZSF im geplanten Projekt „ATO Fahrversuche", die dort gewonnenen Erkenntnisse experimentell im realen Bahnbetrieb oder auf Versuchsfahrten zu validieren und zu erweitern sowie durch Erfassung von Sensordaten die Leistungsfähigkeit direkt vergleichbar zu machen.

Die harmonisierten Entwurfsziele (2.5.5. CSM RA) sind quantitative Akzeptanzkriterien speziell für elektrische, elektronische und programmierbar elektronische technische Systeme (E/E/EP, 2.5.6. CSM RA). Funktionsausfällen eines technischen Systems – oder abgrenzbarer Teile davon (vgl. 3.2. CSM RA) – werden die ungünstigsten noch anzunehmenden Unfallfolgen („credible worst-case scenario", vgl. Art. 4 Abs. 2 lit. a CSM RA) zugeordnet. Führt der Ausfall unmittelbar zu einem katastrophalen Unfall (mit mehreren Toten, Art. 3 Nr. 23 CSM RA), gilt das Entwurfsziel einer Ausfallrate von höchstens 10^{-9} je Betriebsstunde (Art. 3 Nr. 36 CSM RA). Bei einem kritischen Unfall (mit einem Toten, Art. 3 Nr. 35 CSM RA) beträgt der Wert 10^{-7}. Führt der Ausfall – und das dürfte der Regelfall sein – nur mittelbar zum Unfall, können diese Entwurfsziele abgesenkt werden, sprich die akzeptierten Ausfallraten dürfen höher angesetzt werden. Dazu muss der Vorschlagende nachweisen, dass das gleiche Sicherheitsniveau mithilfe von Barrieren außerhalb des Systems erreicht wird. An dieser Stelle kommt vor allem die Sicherheitswirkung der LST zum Tragen.

E/E/EP-Systeme müssen nicht zwingend anhand der harmonisierten Entwurfsziele bewertet werden. Diese stellen nur die Obergrenze dar, die Mitgliedstaaten ohne Weiteres (vgl. 2.5.10. CSM RA) verlangen können. Andere Risikoakzeptanzkriterien sind weiterhin möglich, wenn sie sich aus gesetzlichen Anforderungen ableiten lassen oder darauf beruhen (2.5.2. CSM RA). Als Quellen kommen Rechtsakte der EU und nationale notifizierte Vorschriften in Betracht, einschließlich zumindest der zu ihrer Erfüllung für verbindlich erklärten Normen. Im Anhang A der DIN EN 50126-2 werden einige Risikoakzeptanzkriterien beschrieben (ALARP, GAMAB, MEM, MGS). Im DZSF-Projekt „ATO Risk" wurde die semi-qualitative Methode der Risk-Score-Matrix (RSM, aus der DIN VDE V 0831-103) verwendet. Welche Kriterien den Anforderungen in 2.5.2. CSM RA tatsächlich entsprechen, wird noch eingehend zu diskutieren sein.

Risikoanalyse und Risikoevaluation

In der Risikoanalyse werden die mit dem Einsatz des Systems einhergehenden Gefährdungen ermittelt und die zugehörigen Risiken abgeschätzt. Wie detailliert die Gefährdungen aufzuschlüsseln sind, hängt davon ab, welche Fälle die zu beurteilende Sicherheitsmaßnahme abdecken sollen (2.2.5 CSM RA). Die Art der Risikoabschätzung (qualitativ, quantitativ oder semi-quantitativ) bestimmt sich nach dem gewählten Risikoakzeptanzkriterium.

Für die explizite Risikoabschätzung werden die Gefährdungen in einzelne Szenarien gegliedert. Die Vorarbeiten dafür hat das DZSF-Projekt „ATO Risk" geleistet. Hier wurden die einzelnen Gefährdungen bezüglich der definierten Systemfunktionen erfasst. Eine genaue Szenarienbeschreibung beinhaltet neben der möglichen Gefährdung jedoch auch Betriebs- und Umgebungsbedingungen sowie weitere Konkretisierungen. Während im Automobilsektor hier bereits an einer Systematisierung gearbeitet wird, fehlt diese für das Bahnsystem bislang. Hier sieht das DZSF einen weiteren Schwerpunkt für die weitere Projektarbeit.

Die Risikoevaluation erfolgt zunächst für jede Systemfunktion einzeln. Ob die Leistungen in den dafür betrachteten Szenarien untereinander verrechnet werden dürfen, richtet sich nach dem gewählten Risikoakzeptanzgrundsatz (2.5.2. CSM RA). Neuartige Unfalltypen könnten demnach u. U. akzeptabel sein, solange insgesamt nicht mehr Unfälle geschehen und das Sicherheitsniveau gleichbleibt.

Am Referenzsystem wird die Wirkung der Sicherheitsmaßnahmen direkt der Leistungsfähigkeit des Menschen gegenübergestellt. Quantitative und semi-quantitative Risikoakzeptanzkriterien definieren das vertretbare Risiko anhand eines im Ergebnis zu erreichenden Sicherheitsniveaus. Um das akzeptierte Ausfallrisiko in den Szenarien zu bestimmen, muss der Vorschlagende auch ermitteln, wie oft das Gefährdungsszenario in der Realität vorkommt. Tritt eine unfallträchtige Situation nur selten auf oder wird durch andere Systeme (Barrieren) beherrscht, muss auch die Sicherheitsmaßnahme weniger leistungsfä-

hig sein. Das ist besonders für perspektivisch mit KI abzudeckende Gefährdungen relevant. Eine hinreichend genaue Abschätzung der Wahrscheinlichkeiten existiert bisher nicht. Es ist zu erwarten, dass die konkreten Gefährdungen auch von den Gegebenheiten an der Strecke abhängig sind und für eine ATO-Einführung risikomindernde Maßnahmen an der Infrastruktur notwendig sein können. Hierzu soll im geplanten Projekt „Performance Strecke" beispielhaft eine Strecke analysiert werden, um die konkreten Gefährdungen zu quantifizieren und so eine Risikobewertung streckenbezogen zu ermöglichen. Daraus sollen die technischen Anforderungen an die Leistungsfähigkeit einer ATO-Einheit für ein spezifisches ODD abgeleitet werden. ■

In Heft 2/2023 lesen Sie die Fortsetzung des Beitrags über die Nachweisführung für KI-Komponenten, Daten-Governance, die Rolle des Menschen und aktuelle Projekte des DZSF

QUELLEN

[1] Kawasaki, K.: Trend on Research and Development Activities Relating to Signalling and Telecommunication Systems in Railway Fields. Quarterly Report of RTRI 63.3 (2022), pp. 155-158

[2] Korf, W.; Grinwis, P.; Podt, T.: Rapportage audit projectbeheersing Noord/Zuidlijn Amsterdam voorjaar, 2010

[3] Tagiew, R.; Buder, T.; Hofmann, K.; Klotz, C.; Tilly, R. (2021): Towards Nucleation of GoA 3+ Approval Process. In 2021 5th High Performance Computing and Cluster Technologies Conference, pp. 41-47

Dr. Kai Hofmann
Wiss. Referent Recht
hofmannk@dzsf.bund.de

Dr. Rustam Tagiew
Wiss. Referent Künstliche Intelligenz
tagiewr@dzsf.bund.de

Dr. Roman Tilly
Wiss. Referent Data Science
tillyr@dzsf.bund.de

Dr.-Ing. Christian Klotz
Wiss. Referent Automatisierung
klotzc@dzsf.bund.de

Markus Reinhardt
Forschungsbereichsleiter
Digitalisierung und Automatisierung
reinhardtm@dzsf.bund.de

Alle Autoren:
Deutsches Zentrum für
Schienenverkehrsforschung (DZSF)
beim Eisenbahn-Bundesamt, Dresden