Methoden

Andreas Dodinoiu*, Arne Geffert, Tianxiang Lan und Uwe Becker

Petrinetzbasierte Verlässlichkeitsanalyse einer sicherheitsrelevanten, bordautonomen Zugortung auf Grundlage von PROFUND

Petri net-based dependability analysis of a safety-relevant, autonomous train localization on the basis of PROFUND

https://doi.org/10.1515/auto-2020-0125
Empfangen 31. Juli 2020; angenommen 2. Dezember 2020

Zusammenfassung: Die bevorstehende Modernisierung des Schienenverkehrs wird sich auf die Zugsicherungs- und Signaltechnik auswirken, z. B. auf die Zugortung, die bordautonom und satellitenbasiert werden soll. Um schon in frühen Entwicklungsstadien Aussagen über die Verlässlichkeit eines solchen Systems treffen zu können, ist eine prospektive Risikoabschätzung auf funktionaler Ebene erforderlich. Durch Weiterentwicklung der PROFUND-Methode kann mithilfe einer petrinetzbasierten Modellierung und einer Monte-Carlo-Simulation eine quantitative Aussage über die Verlässlichkeit des Systems getroffen werden.

Schlagwörter: RAMS, Zuverlässigkeit, GNSS, Lokalisierung, Stanford-Diagramm

Abstract: The upcoming modernization of rail transport will affect the train control and signaling technology, for example the train localization which should become onboard and satellite-based. In order to determine the dependability of such a system at an early stage of development, a prospective risk assessment at functional level is necessary. By refining the PROFUND method, the dependability of the system can be evaluated quantitatively using Petri net-based modeling and Monte Carlo simulation.

Keywords: RAMS, reliability, GNSS, positioning, Stanford diagram

***Korrespondenzautor: Andreas Dodinoiu,** Technische Universität Braunschweig, Institut für Verkehrssicherheit und Automatisierungstechnik, Hermann-Blenk-Straße 42, 38108 Braunschweig, Deutschland, E-Mail: a.dodinoiu@tu-braunschweig.de, ORCID: https://orcid.org/0000-0002-8183-6816
Arne Geffert, Tianxiang Lan, Uwe Becker, Technische Universität Braunschweig, Institut für Verkehrssicherheit und Automatisierungstechnik, Hermann-Blenk-Straße 42, 38108 Braunschweig, Deutschland, E-Mails: a.geffert@tu-braunschweig.de, t.lan@tu-braunschweig.de, u.becker@tu-braunschweig.de, ORCID: https://orcid.org/0000-0001-5115-5908 (A. Geffert), https://orcid.org/0000-0002-3943-1401 (T. Lan)

1 Einleitung

Die Anbieter von Mobilitätsanwendungen der heutigen Zeit unterliegen den hohen gesellschaftlichen Erwartungen, die Sicherheit, den Umweltschutz und die Wirtschaftlichkeit ihrer Dienste zu verbessern. Dies ist nur durch eine stetige Modernisierung möglich und trifft insbesondere auf den Schienenverkehr zu. Gerade im Hinblick auf ein Fortbestehen des Schienenverkehrs ist eine Modernisierung, insbesondere des Eisenbahnverkehrsleitsystems, erforderlich. Für eine solche Modernisierung sind jedoch neue Ansätze für die Zugsteuerung und -ortung unerlässlich. Als eine mögliche Ortungstechnologie bietet sich ein multisensorielles System auf der Basis von Globalen Navigationssatellitensystemen (GNSS) an. Hierfür werden allerdings neue Ansätze zur Risikobewertung benötigt, für die im Folgenden eine neue Methode vorgestellt wird. Zu diesem Zweck werden im vorliegenden Beitrag zunächst die Verlässlichkeitskenngrößen des Schienenverkehrs und der GNSS-basierten Ortung ineinander überführt, anschließend werden nach der PROFUND-Methode die entsprechenden Prozesse auf funktionaler Ebene modelliert. Das auf Petrinetzen basierende Modell eignet sich für eine Risikoanalyse, welche mithilfe einer Monte-Carlo-Simulation durchgeführt wird. Der nachfolgend beschriebene Ansatz zeigt, wie sich – gemäß Anforderung aus der Bahn-Normung [1] – eine solche Analyse schon in einem frühen Stadium des Entwicklungsprozesses durchführen lässt. Dadurch kann das zu analysierende System bereits auf funktionaler Ebene modelliert werden. Gerätetechni-

sche Zuverlässigkeit, technologische Realisierungen o. ä. werden nicht betrachtet.

2 Betriebliche Betrachtung der Zugsteuerung

Im europäischen Schienenverkehr erfolgt die Umsetzung des Modernisierungsvorhabens (siehe Kapitel 1) durch die Einführung eines einheitlichen europäischen Eisenbahnverkehrsleitsystems ERTMS (European Rail Traffic Management System). Einen Bestandteil von ERTMS stellt dabei die Zugsteuerung ETCS (European Train Control System) dar. Der Ausbau von ETCS in Bestands- und Neubaustecken kann in drei Stufen erfolgen, jedoch sind nur ETCS Level 2 und 3 für den Einsatz von GNSS relevant, da hier teilweise bzw. vollständig auf streckenseitige Signaltechnik verzichtet werden kann. Nur bei einem überwiegenden oder vollständigen Verzicht auf die streckenseitige Signaltechnik ist der Einsatz einer sicherheitsrelevanten, fahrzeugseitigen Ortung aus betrieblichen und finanziellen Gesichtspunkten erstrebenswert, da hierdurch die Mehrkosten einer fahrzeugseitigen Ortung durch den Wegfall des Einbaus, des Betriebs und der Wartung der streckenseitigen Signaltechnik kompensiert werden können [2]. ETCS Level 2 und 3 unterscheiden sich vor allem dadurch, dass in Level 2 die Blockabschnitte durch eine Gleisfreimeldung im Gleis baulich fest vorgegeben sind. Dagegen wird bei ETCS Level 3 die Gleisfreimeldung – und damit verbunden die Zugvollständigkeitskontrolle – fahrzeugseitig realisiert. Die technische Umsetzung einer fahrzeugseitigen Gleisfreimeldung bzw. Zugvollständigkeitskontrolle hat nach aktuellem Stand von Wissenschaft und Technik noch einen großen Entwicklungsbedarf und wird deshalb in dieser Veröffentlichung nicht weiter betrachtet [3]. Im Hinblick auf die später dargestellte Modellierung sei angemerkt, dass auf die traditionelle Blocksicherung zurückgegriffen wird, d. h., dass sich innerhalb eines Blockabschnitts zu einem gegebenen Zeitpunkt in der Regel nur ein Schienenfahrzeug befinden darf, da sonst eine Gefährdung entsteht. Ausnahmen hiervon stellen z. B. das Rangieren und das Koppeln zweier Züge dar.

Die technische Umsetzung der Ortung eines Schienenfahrzeuges ist bei ETCS nicht fest vorgeschrieben. Es werden lediglich Funktionsumfang und Schnittstellen einer Ortungseinheit beschrieben, nicht jedoch die zu verwendende Sensorik oder Messprinzipien. Aus dieser Beschreibung geht hervor, dass sich das Schienenfahrzeug relativ mittels Odometrie kontinuierlich orten soll. Die hierbei

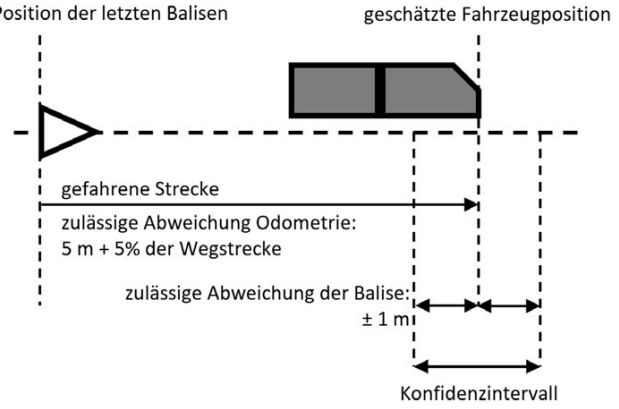

Abb. 1: Zulässige Abweichungen bei der Zugortung mit konventioneller ETCS-Streckenausrüstung [4].

entstehenden Messabweichungen sollen mithilfe von Balisen korrigiert werden. Balisen – fest im Gleiskörper verbaute, elektromagnetische Transponder – gewährleisten somit eine punktförmige Zugortung. Abb. 1 zeigt das beschriebene Verfahren mit den zulässigen Messabweichungen [4]. Die Datenübertragung erfolgt dadurch, dass das Fahrzeug die Baliseninformation bei der Überfahrt einer Balise mit einem entsprechenden Lesegerät ausliest. Um ein sicheres Auslesen einer Balise und damit eine verlässliche Ortung zu gewährleisten, werden diese nicht einzeln verlegt, sondern immer in Gruppen von zwei bis acht. Diese Balisengruppen werden dabei an Blockübergängen und an relevanten Streckenabschnitten, wie z. B. an Weichen, verlegt. Das Schienenfahrzeug meldet im Fall von ETCS dem Stellwerk seine Position über eine Funkschnittstelle und das Stellwerk gibt die weitere Fahrt des Zuges frei und stellt die Fahrstraße ein.

Aktuelle Bestrebungen gehen dahin, physische Balisen mithilfe einer fahrzeugseitigen Ortung auf Basis virtueller Balisen zu ersetzen, um so die Kosten auf weniger stark befahrenen Nebenstrecken zu senken [2]. Bei solchen virtuellen Balisen werden die zur verlässlichen Fahrzeugführung benötigten Ortungsinformationen durch eine alternative, fahrzeugseitige Ortungstechnologie ermittelt. Dies kann durch eine Vielzahl von Sensorik und Messprinzipien geschehen und ist Gegenstand anderer Forschungsarbeiten: Es können z. B. Kamerasysteme, Gleisradar, Wirbelstromsensoren, Inertialsensorik, terrestrische Funkortung oder satellitenbasierte Ortung eingesetzt werden [5]. Die Ergebnisse verschiedener Forschungsprojekte [2, 6] legen nahe, dass sich die schienenfahrzeugseitige Ortung vorteilhaft mithilfe satellitenbasierter Ortungssysteme realisieren lässt. Allerdings ist davon auszugehen, dass die verwendeten Sensoren nicht unabhängig voneinander

betrieben werden, sondern durch eine fehlertolerante Informationsverarbeitung zu einer Ortungslösung fusioniert werden. Dies bietet den Vorteil, dass durch die Beobachtung der Messqualität auf die Präzision der Messung geschlossen werden kann und eine Fehlereingrenzung möglich wird [7]. Dabei ist zu beachten, dass die häufig in anderen Domänen favorisierten, stochastischen Fusionsansätze (z. B. Kalman- oder Partikel-Filter) dem im Bahnbereich aus Gründen der Zulassungsfähigkeit angestrebten Determinismus zuwiderlaufen. Es gibt aber bereits Möglichkeiten und Ansätze, die Sensordaten sowohl deterministisch mit ausreichender Güte zu fusionieren [7] als auch zu plausibilisieren, letzteres z. B. mittels Voting [8].

Durch die Nutzung neuer Ortungstechnologien ergeben sich bei der Betrachtung der zulässigen Messabweichung neue Herausforderungen, da das Konfidenzintervall der Messabweichung nicht mit der klassischen Zugortung entsprechend den ETCS-Bestimmungen übereinstimmt (vgl. Abb. 2). Aus diesem Grund müssen bestehende Methoden weiterentwickelt werden, um die Messcharakteristik der verschiedenen Ortungstechnologien mit den Anforderungen aus dem Bahnbereich zu vereinheitlichen.

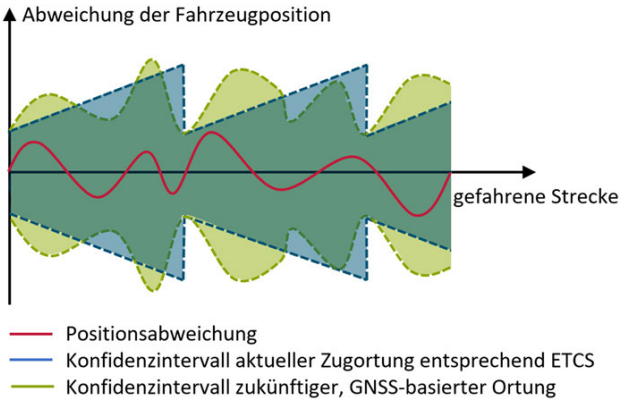

Abb. 2: Gegenüberstellung der Konfidenzintervalle von konventioneller und zukünftiger Zugortung [9].

3 Zulassung neuer Technologien im Bahnbereich

Für den Schienenverkehr muss nicht nur die Machbarkeit einer fahrzeugseitigen GNSS-Ortung untersucht, sondern auch die Verlässlichkeit eines solchen Systems nachgewiesen werden. Dies ist vor allem unter dem Gesichtspunkt sinnvoll, dass diese Technologie für den Einsatz im Eisenbahnbereich zugelassen werden muss.

Im Bahnbereich wird die Verlässlichkeit eines Systems durch die RAMS(S)-Kenngrößen charakterisiert [1]. Diese Kenngrößen sind die Zuverlässigkeit (reliablity), die Verfügbarkeit (availability), die Instandhaltbarkeit (maintainability) und die Sicherheit. Im Fall der Sicherheit ist die deutsche Sprache durch den polysemen Charakter dieses Terminus nicht eindeutig, da sowohl safety als auch security gemeint sein können. Während unter safety die Freiheit von inakzeptablen Risiken verstanden wird, die nach außen wirken (Schutz der Umwelt vor Gefährdungen durch das technische System), wird security als Schutz vor Eingriffen definiert, die von außen auf das System einwirken. Im weiteren Verlauf dieses Beitrags wird Sicherheit im Sinne von safety verstanden.

Der Terminus der Sicherheit stellt dabei historisch einen zentralen Bestandteil des Schienenverkehrs dar. Quantitativ lässt sich das mit dem Betrieb verbundene Risiko als Kombination aus Schadensschwere und Eintrittswahrscheinlichkeit des Schadens definieren. Ein System gilt als sicher, wenn das Risiko einen bestimmten Wert unterschreitet, das sogenannte Grenzrisiko [1]. Die Risikobeurteilung im Bahnbereich ist in den Common Safety Methods (CSM) [10] beschrieben und spaltet sich in drei Möglichkeiten auf (vgl. Abb. 3).

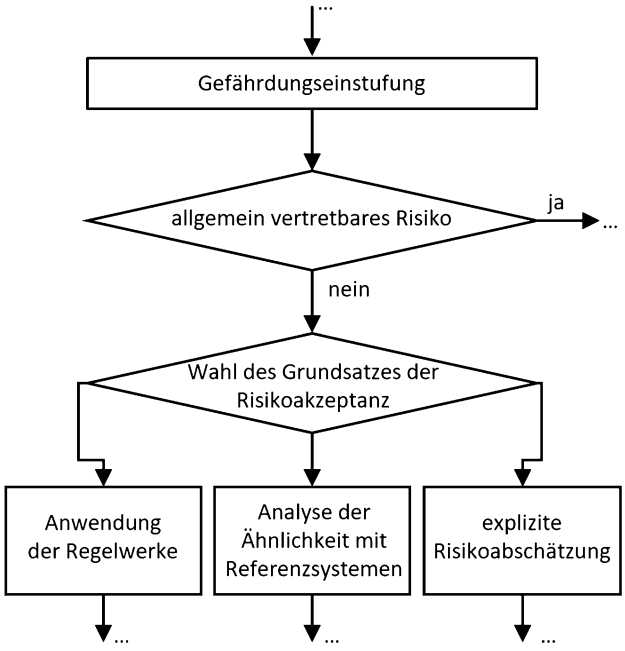

Abb. 3: Ablaufschema zur Risikobeurteilung – Ausschnitt aus der CSM-Verordnung [10].

Die Risikobeurteilung eines technischen Systems kann über bestehende Regelwerke, über einen Vergleich mit einem Referenzsystem oder über eine explizite Risikoabschätzung durchgeführt werden. Da es sich bei dem betrachteten System um eine noch im Forschungsstadium befindliche Ortungstechnologie handelt, kann zur Abschätzung auf keine bestehenden Regelwerke zurückgegriffen werden. Auch werden in diesem Beitrag keine ähnlichen Referenzsysteme analysiert, da es noch keinen vergleichbaren Einsatz von GNSS im Landverkehr gibt. Am ehesten vergleichbar wäre zwar (wegen ähnlicher Umgebungsbedingungen) der Automobilbereich, der momentan aber für sicherheitsrelevante Aufgaben der Fahrzeugführung größtenteils umfelderfassende Sensorik (z. B. Radar, Lidar, Kamera) statt GNSS einsetzt [11]. Darüber hinaus wird im Automobilbereich zurzeit noch diskutiert, wie die Absicherung der Sollfunktion erfolgen soll [12], unter die auch die in diesem Beitrag betrachtete Verlässlichkeit des Ortungssystems fällt. Daher ist es naheliegend, für den Bahnbereich eine explizite Risikoabschätzung durchzuführen. Der PROFUND-Ansatz wurde ausgewählt, da eine formale Risikoanalyse auf Basis von Petrinetzen in den CSM-Richtlinien [10] empfohlen wird. Dazu werden gemäß CSM-Methodik zunächst Szenarien und Sicherheitskriterien definiert. Anschließend wird das Risiko über die Bestimmung der Schadensschwere und -häufigkeit abgeschätzt. Insbesondere eignet sich dieser Ansatz im Hinblick auf eine spätere Zulassung für den Schienenverkehr, da hierfür aufgrund der durch die einschlägige Normung [1] vorgeschriebenen, analytischen Methoden zur Risikoermittlung eine reine Erprobung nicht ausreicht. Eine solche Erprobung kann jedoch ergänzend – zur abschließenden Demonstration der Sicherheit – erfolgen. Ferner wird in diesem Beitrag der Ansatz verfolgt, dass eine neue Technologie mindestens das gleiche Sicherheitsniveau erreichen muss wie die bestehende. Dafür werden die tolerierbaren Gefährdungsraten (THR) der bestehenden Technik (siehe Tab. 1) herangezogen.

Tab. 1: Gefährdungsraten einer Balise [9, 13].

Beschreibung der Gefährdung	Gefährdungsrate (THR)
Nichterkennung einer Balisengruppe (fahrzeugseitig)	$10^{-7}\ h^{-1}$
Erkennung Ausfall einer Balisengruppe (streckenseitig)	$10^{-9}\ h^{-1}$

4 Modellierung der Ortungsverlässlichkeit

Um die Ortungstechnologie bewerten zu können, müssen im Folgenden sowohl das Messumfeld als auch die Messqualität betrachtet werden. Der Einsatz einer GNSS-basierten Ortung für sicherheitsgerichtete Funktionen ist beispielsweise in der Luftfahrt bereits üblich. In diesem Umfeld sind verschiedene Methoden zur Überwachung sicherheitsrelevanter bzw. -bezogener Funktionen, wie z. B. RAIM, etabliert [2]. Der Eisenbahnbereich stellt jedoch durch seine Anforderungen in zweierlei Hinsicht eine Herausforderung für eine GNSS-basierte Ortung dar. Zum einen zeigen GNSS-Empfänger ein probabilistisches Verhalten [14], welches nur schwer mit den im Bahnbereich üblichen Absicherungsansätzen in Einklang zu bringen ist. Zum anderen ist das Gleisumfeld mit seiner Bebauung und mit seinen Tunneln ein weitestgehend neuer Anwendungsbereich für GNSS-basierte Ortungssysteme mit Sicherheitsverantwortung, da ein solches Umfeld in anderen Domänen, außer dem Landverkehr, kaum zu finden ist [15]. Hierbei sind vor allem Abschattungseffekte, Mehrwegeempfang und Nicht-Sichtverbindungen (NLOS) zu berücksichtigen (vgl. Abb. 4). Dies ist auf das Funktionsprinzip von GNSS zurückzuführen, welches eine direkte Sichtverbindung zu den Satelliten (LOS) benötigt, um eine genaue Positionslösung berechnen zu können.

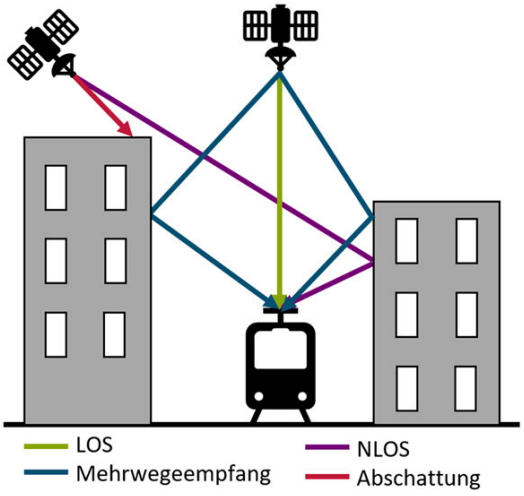

Abb. 4: Empfangswege GNSS (NLOS: es gibt nur einen Signalpfad ohne direkten Sichtkontakt zum jeweiligen Satelliten) [17].

Diese Effekte können – obwohl durch die ergänzende Sensorik (z. B. Odometer) abgemildert – sowohl die Messqualität in gefährdender Weise beeinträchtigen als auch

zu einer Funktionsunfähigkeit der Ortungseinheit führen. Die sich hieraus ergebenden Risiken sind dadurch charakterisiert, dass sie durch keine Fehlfunktion – also durch keinen *Defekt* im gerätetechnischen Sinne – ausgelöst werden. Das heißt, dass eine Gefährdung auftritt, obwohl das technische System – zumindest vordergründig – spezifikationsgemäß funktioniert. Daher werden Risiken dieser Art der Sollfunktion zugeordnet. Diese Risiken werden beispielsweise im Automobilbereich nicht durch die klassische funktionale Sicherheit abgedeckt, sodass sich für das automatisierte Fahren im Straßenverkehr gerade die SOTIF-Norm [16] (safety of the intended functionality, dt. Sicherheit der Sollfunktion) etabliert. Deren wesentliches Ziel besteht darin, eine möglichst hohe Anzahl an kritischen Situationen zu identifizieren (Abdeckung/Vollständigkeit), die im Anschluss abgesichert werden können. Demgegenüber muss bei der Modernisierung und Automatisierung des Schienenverkehrs die Absicherung im Rahmen bestehender Regelwerke erfolgen, die bedarfsgerecht zu erweitern und zu ergänzen sind.

Da im weiteren Verlauf nur auf die funktionalen Aspekte des GNSS-basierten Zugortungssystems eingegangen wird, werden nun dessen Messqualitätskenngrößen analog zu den im Bahnbereich etablierten RAMS(S)-Kenngrößen betrachtet [18]. Diese RAMS(S)-Kenngrößen werden in Abb. 5 den aus der Ortung bekannten Messqualitätskenngrößen Verfügbarkeit (availability), Integrität (integrity), Genauigkeit (accuracy) und Kontinuität (continuity) gegenübergestellt. Die Genauigkeit gibt an, wie weit die gemessene Position eines Messobjektes von seiner wahren Position – i. A. nicht bekannt – entfernt liegt. Eine Sicherheitsbetrachtung, ausgehend nur von der Verteilungsfunktion der Genauigkeit, ist im Bereich der GNSS-Ortung nicht ausreichend,

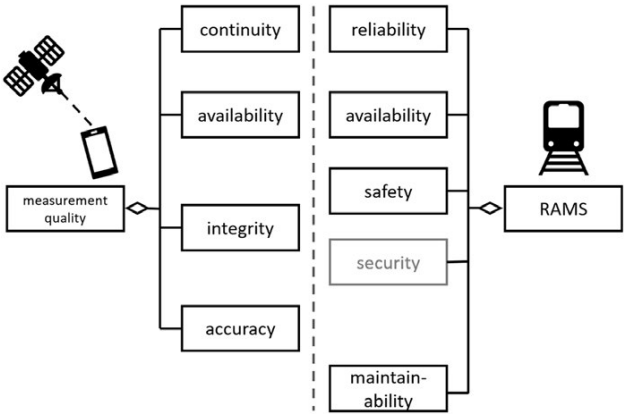

Abb. 5: Gegenüberstellung von GNSS-Messqualitätskenngrößen und RAMS(S)-Kenngrößen [18].

da die Verteilungsfunktion der Positionsabweichung wegen der lokalen, dynamischen Umgebungseinflüsse durch erhebliche Ausreißer, schwere Ränder, Asymmetrien etc. gekennzeichnet ist.

Deshalb wird mithilfe der Integrität – eine Überwachung – ein Maß für die Vertrauenswürdigkeit der Messwerte geschaffen. Diese Kenngröße stellt somit gerade im Hinblick auf sicherheitsrelevante Aufgaben ein besonders wichtiges Kriterium dar. Genauigkeit und Integrität interagieren dabei miteinander. Die Positionsabweichung (PE) in Abb. 6 zwischen der wahren und der gemessenen Position repräsentiert hierbei die Genauigkeit.

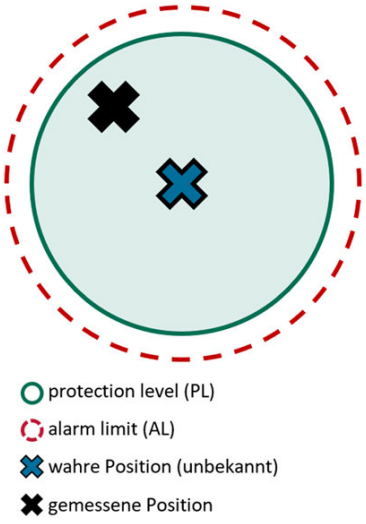

Abb. 6: Funktionsprinzip der Integritätsüberwachung [19].

Die Integritätsüberwachung bestimmt auf statistischer Basis ein Protection Level (PL) variabler Größe, welches einen geometrischen Bereich angibt, in dem mit hoher Wahrscheinlichkeit die wahre Position liegt. Für eine sichere Nutzung der Ortung muss das PL kleiner sein als das Alarm Limit (AL), das ein für eine Anwendung spezifisch ausgelegter Wert ist und – vereinfacht betrachtet – die maximal zulässige Streuung der Messabweichung für den jeweils betrachteten Einsatzfall angibt. Aus der Integrität lassen sich außerdem Verfügbarkeit und Kontinuität ableiten. Die Verfügbarkeit beschreibt die mittlere Wahrscheinlichkeit, dass ein Messwert ermittelt und genutzt werden kann. Demgegenüber ist die Kontinuität als Wahrscheinlichkeit definiert, dass Messwerte für einen bestimmten Zeitraum ununterbrochen ermittelt und genutzt werden können.

Die Integritätsüberwachung kann durch die komplexe Messumgebung im realen Betrieb fehlerhafte Entschei-

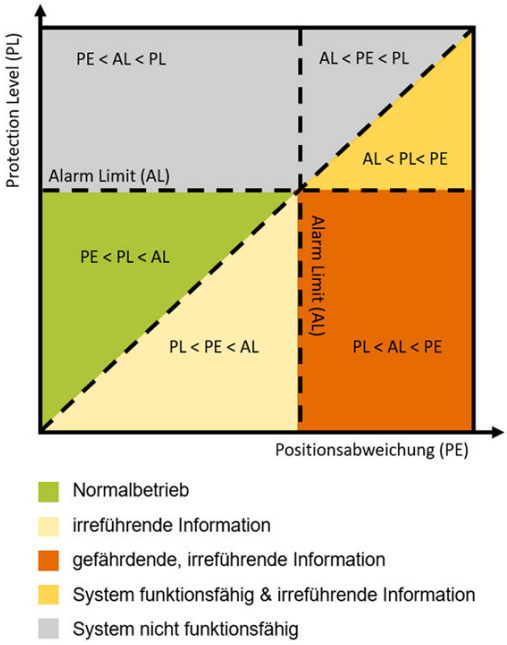

Abb. 7: Stanford-Diagramm [20], angepasst an die in dieser Veröffentlichung verwendete Terminologie.

Tab. 2: Notation der Petrinetzelemente.

Platz	Fusionsplatz	agglomerierter Platz	Kante
agglomerierte Kante	Testkante	Inhibitorkante	kausale Transition
zeitbewertete Transition	agglomerierte Transition	stochastische Transition (e-Verteilung)	

dungen treffen und somit nicht sichere Ortungsinformationen als sicher klassifizieren. Hierdurch entsteht eine Gefährdung. Die Zustände der Integritätsüberwachung, die sich aus dieser Betrachtung ergeben, können am Beispiel der Positionsinformation in einem so genannten Stanford-Diagramm (Abb. 7) veranschaulicht werden.

Bei dieser Darstellung werden die Größen PL und PE auf den Koordinatenachsen aufgetragen. Die fünf Zustände aus dem Standford-Diagramm müssen weiter aggregiert werden, um sie mit dem konservativen Sicherheitsverständnis des Schienenverkehrs in Einklang zu bringen. Aus diesem Grund wird das Verhalten des Ortungssystems mit den beiden Termini *Vertrauenswürdigkeit* und *Sicherheit* charakterisiert, welche auch für die spätere Modellierung genutzt werden [19]. Eine Positionsinformation ist vertrauenswürdig, wenn die Ortungseinheit einen verwendbaren Wert erzeugt (Positionslösung liegt vor, Integrität erzeugt keinen Alarm). Ist die Positionsinformation entsprechend dem Stanford-Diagramm nicht irreführend, wird diese als sicher klassifiziert. Zu beachten ist, dass die Zustandsgröße *Messwert sicher* im realen Betrieb nicht beobachtbar ist.

Die beschriebenen Zustände lassen sich in einem Petrinetz modellieren, um die Verlässlichkeit des Ortungssystems abzubilden. Die Notation der verwendeten Elemente ist in Tab. 2 aufgeführt. Eine Besonderheit stellen die Fusionsplätze dar, die eine Informationsverknüpfung zu anderen Plätzen abbilden. Modellierung und Analyse erfolgen mit dem π-Tool [21]. Dieses Tool ermöglicht es, die in der vorliegenden Publikation vorgestellten Petrinetzmodelle auf totale Verklemmungen zu überprüfen. Des Weiteren wurden partielle Verklemmungen durch eine manuelle Analyse der Petrinetze und durch eine gezielte Fehlerinjektion während des Markenspiels aufgezeigt und behoben. Daher kann davon ausgegangen werden, dass das hier vorgestellte Modell keine Verklemmungen mehr aufweist.

In dieser Publikation werden ausschließlich erweiterte generalisierte stochastische Petrinetze (EGSPN) verwendet. Diese stellen eine mehrfach erweiterte Form der Bedingungs-Ereignis-Netze dar, indem sie Gewichtungen und Prioritäten ermöglichen und die Transitionen um stochastische Verteilungen erweitern [22]. Durch die Verwendung von EGSPN können die meisten Herausforderungen bei der Modellierung adressiert werden: Das stochastische Verhalten der GNSS-Empfänger lässt sich modellieren und es kann auf eine umfangreiche Tool-Unterstützung zurückgegriffen werden. Jedoch ist dieses Beschreibungsmittel nicht imstande, gleichzeitig auftretende Ereignisse abzubilden, wodurch Teile des Ortungsprozesses, welche in der Realität parallel ablaufen, als serielle Prozesse approximiert werden müssen. Um darüber hinaus detaillierte Petrinetze übersichtlicher darstellen zu können, werden in der vorliegenden Publikation an geeigneter Stelle agglomerierte Netze verwendet. Diese Komponenten stellen eine Zusammenfassung hierarchisch darunterliegender Netze dar (Super-/Subsysteme) und können daher in komplexere Strukturen dekomponiert werden.

In Abb. 8 ist die Erfassung eines Messwerts über die Zustände *Messwert vertrauenswürdig* und *Messwert nicht vertrauenswürdig* sowie über die Zustände *Messwert sicher* und *Messwert gefährdend* dargestellt. Sie werden mithilfe des hierarchisch darüberliegenden Modells der Verläss-

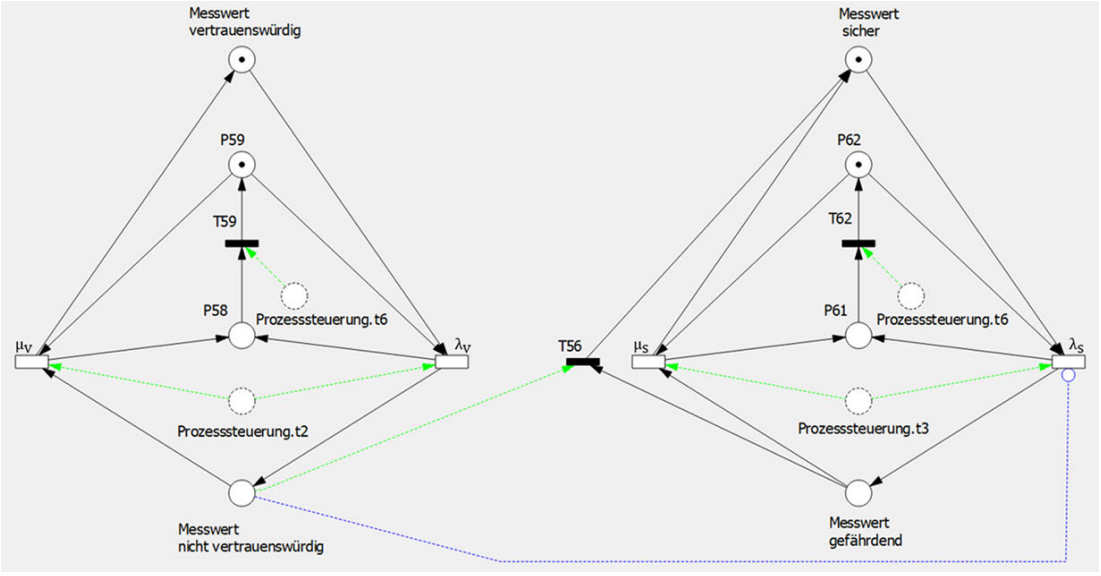

Abb. 8: Modelle der Messwerterfassung [19].

lichkeit der Ortung aggregiert, vgl. Abb. 9. Dieses Modell umfasst die folgenden Zustände:

- Positionsinformation sicher und funktionsfähig, wenn Messwert sicher und vertrauenswürdig
- Positionsinformation nicht funktionsfähig, wenn Messwert nicht vertrauenswürdig
- Positionsinformation nicht sicher, wenn Messwert gefährdend und vertrauenswürdig.

Zwischen den Zuständen *Positionsinformation nicht funktionsfähig* und *Positionsinformation nicht sicher* muss unterschieden werden, da im ersten Fall eine sicherheitsgerichtete Ausfallreaktion (fail-safe) ausgelöst wird. Diese Reaktion bewirkt vordergründig eine Verringerung der Verfügbarkeit. Im zweiten Fall kann jedoch ein Fehlzustand des Messwerts nicht erkannt werden (System funktionsfähig trotz fehlerhafter Positionsinformation), sodass eine Gefährdung entsteht, da eine eigentlich erforderliche Ausfallreaktion unterbleibt. Die theoretisch mögliche Zustandskombination aus *Messwert nicht vertrauenswürdig* und *Messwert gefährdend* (Abb. 8) wird nicht berücksichtigt, weil sie aus funktionaler Sicht nicht auftreten kann, da bei dem Zustand *Messwert nicht vertrauenswürdig* die Überwachung schon eine Integritätsverletzung erkannt hat.

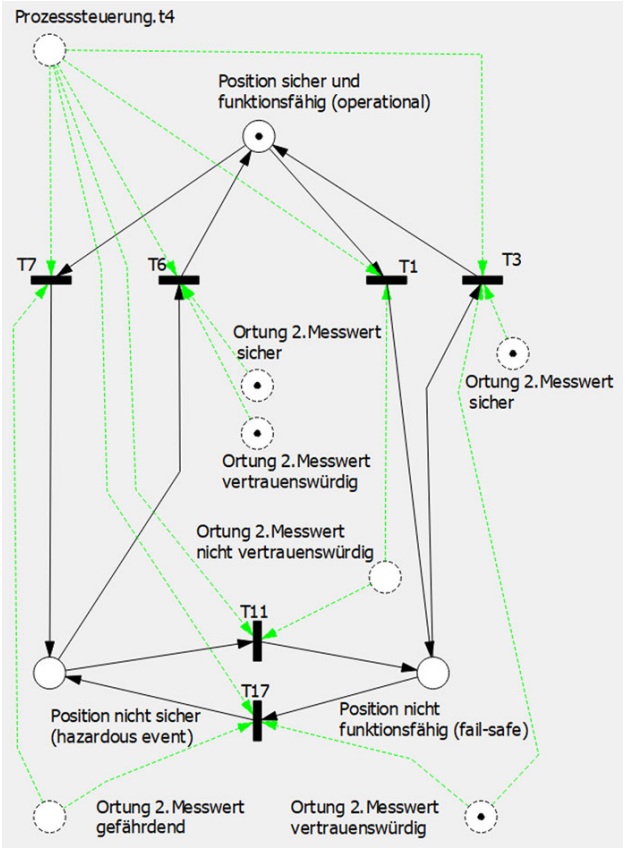

Abb. 9: Ortungsverlässlichkeit (Fusionsplätze mit der Beschriftung „Ortung 2.[...]“ beziehen sich auf die Zustände aus Abb. 8).

5 PROFUND-Modellierung des Schienenverkehrs

Der im Bahnbereich etablierte PROFUND-Ansatz [23] folgt dem Modell der Risikogenese nach Schnieder [24], vgl. Abb. 10. Nach diesem Modell kann ein Schadensfall nur dann (auf probabilistische Weise) eintreten, wenn sowohl ein exponiertes Rechtsgut als auch eine Gefährdung desselben vorliegen. Dieser Beitrag konzentriert sich auf den letzteren Bestandteil der Risikogenese, nämlich auf die verkehrliche Gefährdung ausgehend von der GNSS-basierten Ortung. Dazu werden bei der PROFUND-Methode der Prozess, die Funktion und die Verlässlichkeit (siehe Kapitel 3 und 4) des zu untersuchenden Systems modelliert. Auf diese Weise können Rückschlüsse auf die entscheidenden Kenngrößen der Verlässlichkeit – in diesem Beitrag auf die Sicherheit – gezogen werden.

Diesem Ansatz entsprechend werden im Folgenden der Verkehrsprozess, die Funktionen der Ortung und der Zugsicherung sowie die zugehörigen Verlässlichkeiten anhand eines Beispielszenarios modelliert. Als ein solches Szenario dient der Gegenfahrschutz, welcher im Betrieb verhindert, dass zwei Schienenfahrzeuge gemeinsam in einen Blockabschnitt einfahren können (vgl. Abb. 11). Dies wird durch die drei Funktionen der Zugortung, der zentralen Fahrwegsteuerung durch das Stellwerk und durch eine übergeordnete Routenplanung gewährleistet. Die Routenplanung ist hier nur der Vollständigkeit halber aufgeführt, da sie in der Regel keine Sicherheitsfunktionen erfüllt. Die Zugortung wird in diesem Beispiel durch eine GNSS-basierte Ortung (vgl. Abb. 8 und 9) gewährleistet und die Fahrwegsteuerung durch das Stellwerk sowie durch die entsprechenden Weicheneinheiten. Da die Verlässlichkeit des Stellwerks und die Verlässlichkeit der dazugehörigen Fahrwegsteuerung nicht im Fokus dieses Beitrags stehen, werden beide nur durch eine Ausfallrate entsprechend den Anforderungen nach dem Sicherheits-Integritätslevel (SIL) 4 mithilfe der stochastischen Transition „Z1 Einfahrt ohne sichere Fahrterlaubnis“ (bzw. mithilfe von „Z2 [...]“) modelliert (vgl. Abb. 13). Eine solche Vereinfachung wurde gewählt, da die Fahrwegsteuerung in ihrer Gesamtheit ein komplexes System aus verschiedenen Komponenten darstellt, welche je nach Komponente entweder nur auf den einzelnen Verkehrsteilnehmer wirken (Weichenlage) oder auf die Gesamtheit des Systems über die zentrale Steuerung im Stellwerk. Die daraus resultierende Gefährdungsrate müsste in einem eigenen, komplexen, dem PROFUND-Ansatz unterliegenden Petrinetz modelliert werden. Die damit verbundene Modellkomplexität stünde in einem Konflikt mit dem Ziel des vorliegenden Beitrags, eine *Methode* zur Absicherung einer sicherheitsrelevanten, bordautonomen Zugortung vorzustellen. Daher wird an dieser Stelle von einer detaillierten Modellierung der Fahrwegsteuerung abgesehen und stattdessen das Verhalten näherungsweise mit der bei SIL 4 zulässigen Gefährdungsrate von 10^{-9} pro Stunde beschrieben. Dabei wird vereinfachend davon ausgegangen, dass diese Gefährdungsrate nur am Gefahrenpunkt, also für 0,1 Sekunden pro Prozessdurchlauf, wirksam ist. Diese Annahme ist zwar diskussionswürdig, könnte aber in weiteren Arbeiten durch eine Skalierung der Ausfallrate (wegen des Exponentialansatzes problemlos möglich) auf einfache Weise angepasst werden. Ferner wird die Gefährdungsrate von 10^{-9} pro Stunde für die Transition „Z1 Einfahrt ohne sichere Fahrterlaubnis“ (bzw. für „Z2 [...]“) angenommen (vgl. Abb. 13), wohl wissend, dass es sich hierbei um eine konservative Abschätzung handelt.

Abb. 12 zeigt das Modell des Verkehrsprozesses in kondensierter Darstellung. Darin wird über eine regelmäßige Generierung von Schienenfahrzeugen ein Verkehr auf dem Gleis simuliert. Dabei tritt eine Gefährdung ein, wenn

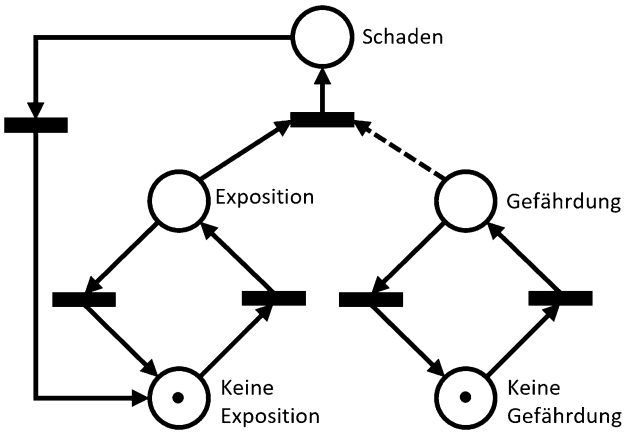

Abb. 10: Risikogenese nach Schnieder [24].

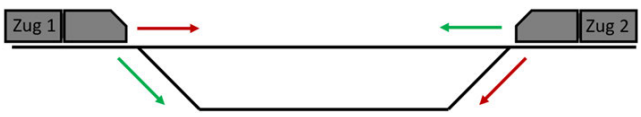

Abb. 11: Szenario des Gegenfahrschutzes: sicher gestellte Fahrstraße (grün), gefährdend gestellte Fahrstraße (rot).

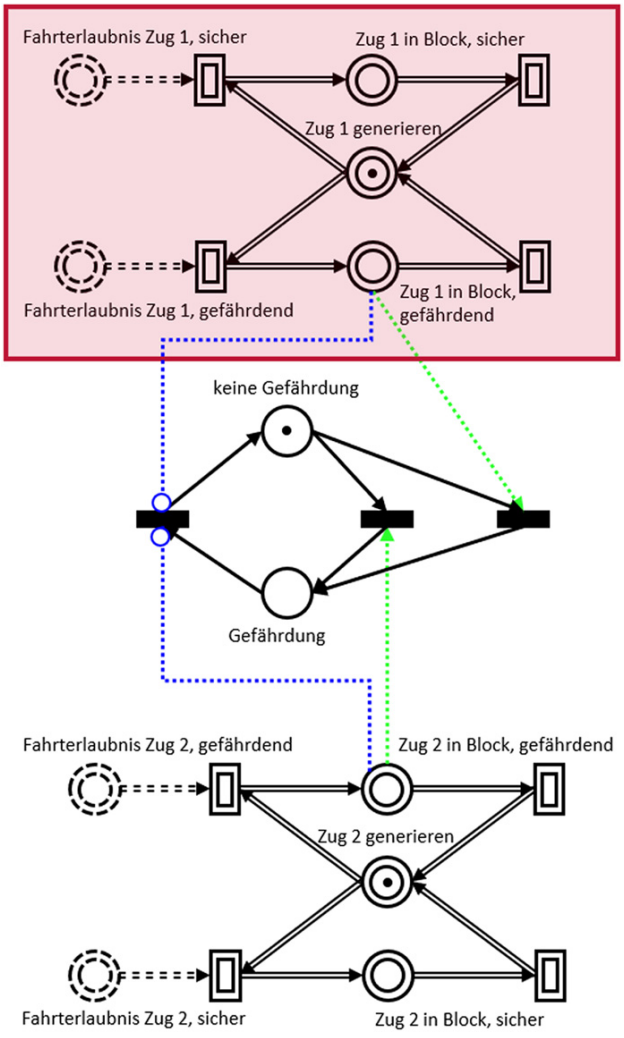

Abb. 12: Kondensiertes PROFUND-Modell des Verkehrsprozesses (rot umrahmter Bereich ist in Abb. 13 im Detail dargestellt).

eines der beiden Schienenfahrzeuge durch einen unsicheren Fahrbefehl, bedingt durch eine fehlerhafte Ortung oder Fahrwegsteuerung, ungewollt in den betrachteten Gleisabschnitt (Block) einfährt. Der eigentlich kontinuierlich wirkende Prozess der Ortung wurde bei dem gewählten Modellierungsansatz als eine diskrete Stützstelle am Gefahrenpunkt gewählt, da es sich bei der bestehenden Zugsicherungstechnik auch um eine diskrete Lokalisierung an den im Gleis eingelassenen Balisen handelt. Zwar wird durch diesen Ansatz vernachlässigt, dass die Positionslösung des Ortungssystems auch vor dem Gefahrenpunkt in einen gefährdenden Zustand wechseln kann, dieser bestehen bleibt und das Schienenfahrzeug in diesem Zustand in den Gefahrenpunkt einfährt, jedoch konnte so die Komplexität des Modells deutlich verringert werden. Dies ist auch dadurch bedingt, dass für die diskrete Betrachtung am Gefahrenpunkt ein gedächtnisloser Prozess innerhalb des Ortungsmodells näherungsweise ausreicht.

Abb. 13 zeigt ein detailliertes Modell dieses Prozesses für eines der beiden Schienenfahrzeuge (Zug 1 bzw. Z1). Mithilfe der Parametrierung der Prozesssteuerung (Abb. 14) wird eine geringe bis mittlere Streckenauslastung mit vier Zügen pro Stunde in beiden Richtungen modelliert, entsprechend einer Nebenstrecke. Ortung und Fahrwegsteuerung müssen sicherstellen, dass nicht zwei Schienenfahrzeuge gleichzeitig in einen Streckenblock fahren. Jedes Schienenfahrzeug besitzt jeweils ein eigenes, unabhängiges Ortungssystem identischer Modellierung und Parametrierung. Die Zug- bzw. Fahrwegsteuerung wird, wie bereits oben erwähnt, als ein zentrales System modelliert. Eine Gefährdung tritt ein, wenn entweder eine fehlerhafte Positionsinformation oder ein nicht detektierter Ausfall der Fahrwegsteuerung zu einer unzulässigen Fahrterlaubnis führen und es damit möglich ist, dass beide Züge gemeinsam in einen Blockabschnitt einfahren. Die auftretenden Risiken werden aufgrund des ereignisdiskreten Charakters der Petrinetze nicht kontinuierlich simuliert, sondern nur am Gefahrenpunkt der einmal pro Prozessdurchlauf stattfindenden Weichenüberfahrt bestimmt. Dies gilt sowohl für die mit der Fahrwegsteuerung als auch für die mit der GNSS-basierten Ortung verbundenen Risiken.

Im Rahmen der bestehenden Modellierung werden nur die komplementären Zustände *sicher* und *gefährdend* betrachtet. So führt ein sicherer Ausfall der Ortung im Verkehrsprozess zu einem Fail-Safe-Zustand und damit nicht zu einer Gefährdung. Dieser verkehrliche Fail-Safe-Zustand, welcher sich im Betrieb von einer Degradationsstufe bis hin zur Notbremsung des Schienenfahrzeuges offenbaren kann, wird im vorliegenden Beitrag nicht im Detail betrachtet, da ein solcher Detaillierungsgrad für die Erläuterung der (weiter-)entwickelten Absicherungsmethode nicht erforderlich ist. Vielmehr besteht das Ziel dieses Beitrags darin, die Forschungsergebnisse anhand eines verständlichen Beispiels zu erklären. Um ferner den zeitlichen Ablauf der Zug-Generierung, der Ortung und der Zugeinfahrt zu berücksichtigen, werden diese Prozesse über die Prozesssteuerung geführt (vgl. Abb. 14).

Durch die Prozesssteuerung und die dadurch vorgenommene Abstraktion des realen Prozesses werden Zustandsübergänge, welche in der Realität zeitlich simultan ablaufen, innerhalb des Modells seriell modelliert. Konkret werden in einem realen GNSS-Empfänger die Position und die Integrität quasi zeitgleich berechnet. Die Modellierung mithilfe ereignisdiskreter Petrinetze erlaubt die Abbildung dieser Parallelität jedoch nicht, sodass die Teilprozesse in der Simulation für jeweils 0,1 Sekunden

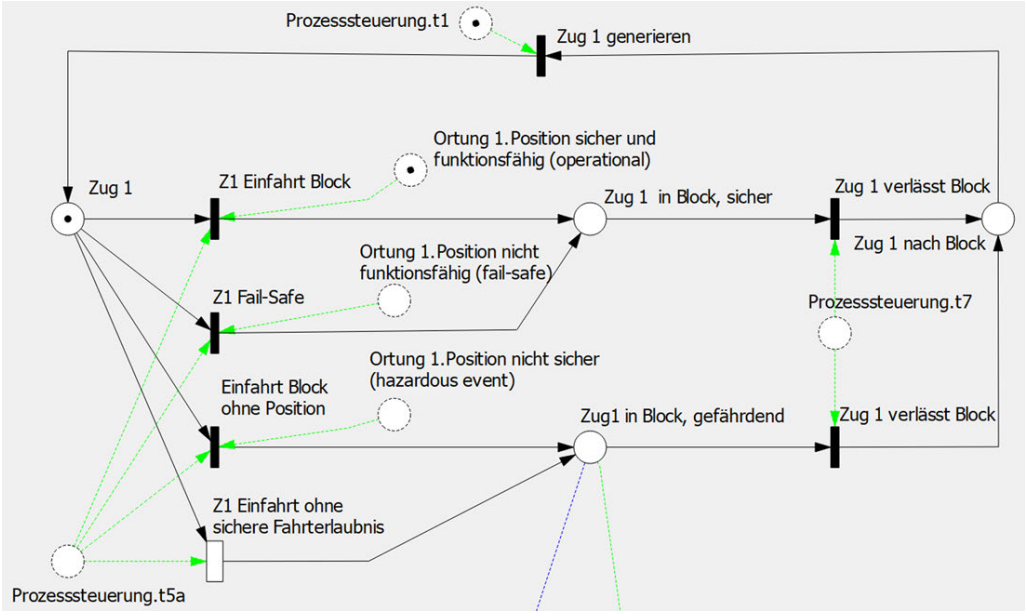

Abb. 13: Detaillierte Darstellung des Verkehrsprozesses für den Zug 1 (Z1). Fusionsplätze mit den Beschriftungen „Ortung 1.[...]“ und „Prozesssteuerung.[...]“ beziehen sich auf die Zustände aus Abb. 9 bzw. 14; Verkehrsprozess des Zuges 2 ist symmetrisch dazu.

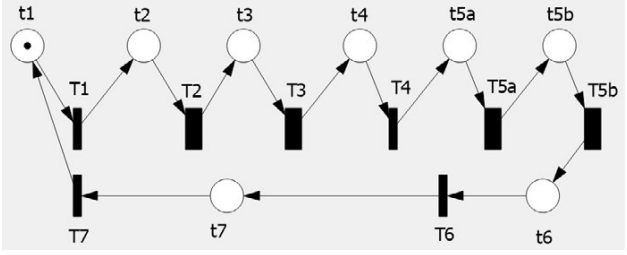

Abb. 14: Prozesssteuerung des Szenarios.

Tab. 3: Randbedingungen der Monte-Carlo-Simulation.

Simulationsumfang (samples)	10^9	
Signifikanz (p-Wert)	**0,1 %**	
Transition		
λ_S (Messwerterfassung)	10^{-1}–10^{-5} h^{-1}	neg. e-Verteilung
μ_S (Messwerterfassung)	36000 h^{-1}	neg. e-Verteilung
λ_V (Messwerterfassung)	10^{-0}–10^{-4} h^{-1}	neg. e-Verteilung
μ_V (Messwerterfassung)	36000 h^{-1}	neg. e-Verteilung
Z1 Einfahrt ohne sichere Fahrterlaubnis	10^{-9} h^{-1}	neg. e-Verteilung
Z2 Einfahrt ohne sichere Fahrterlaubnis	10^{-9} h^{-1}	neg. e-Verteilung
T2 (Prozesssteuerung)	0,1 s	determinist. Dauer
T3 (Prozesssteuerung)	0,1 s	determinist. Dauer
T5a (Prozesssteuerung)	0,1 s	determinist. Dauer
T5b (Prozesssteuerung)	0,1 s	determinist. Dauer

nacheinander ablaufen (entsprechend einer Messrate von 10 Hz). Um die mit der Simulation verbundene Rechenkomplexität zu verringern, wurde überdies angenommen, dass ein kompletter Zyklus des Prozesses in 0,4 Sekunden abläuft, wohingegen der reale Verkehrsprozess mit 4 Zügen pro Stunde (Dauer von 900 Sekunden pro Zug) vonstattengeht. Daher müssen die in der Simulation ermittelten Gefährdungsraten des Verkehrsprozesses durch einen konstanten Faktor von ca. 2250 dividiert werden. Der so modellierte Verkehrsprozess wird mithilfe eines Monte-Carlo-Ansatzes simuliert, und zwar mehrfach hintereinander mit variierten Parametern. Die gewählten Randbedingungen der Monte-Carlo-Simulation sind in Tab. 3 gesammelt aufgeführt. Da das verwendete Tool zur Durchführung der Monte-Carlo-Simulation keine Einsicht in die verwendeten Anfangsverteilungen ermöglicht, kann darüber keine Aussage getroffen werden. Die zugehörigen Ergebnisse befinden sich in Abb. 15.

In diesem Beitrag soll beispielhaft anhand der Übergangsraten λ_S und λ_V (vgl. Abb. 8 und 15) untersucht werden, wie sich die Qualität der GNSS-basierten Ortung auf die Gefährdungsrate des Verkehrsprozesses auswirkt. Dazu müssen die komplementären Parameter μ_S und μ_V (vgl. Abb. 8) heuristisch mit einer Rate von 10 pro Sekunde angenommen werden. Diese Werte sind sehr von der Messumgebung, vom verwendeten Empfänger sowie von dessen Integritätsalgorithmen abhängig und müssen daher vom Entwickler (z. B. auf Basis von Erfahrungswerten oder Sensorsimulationen) abgeschätzt werden. Um das Ver-

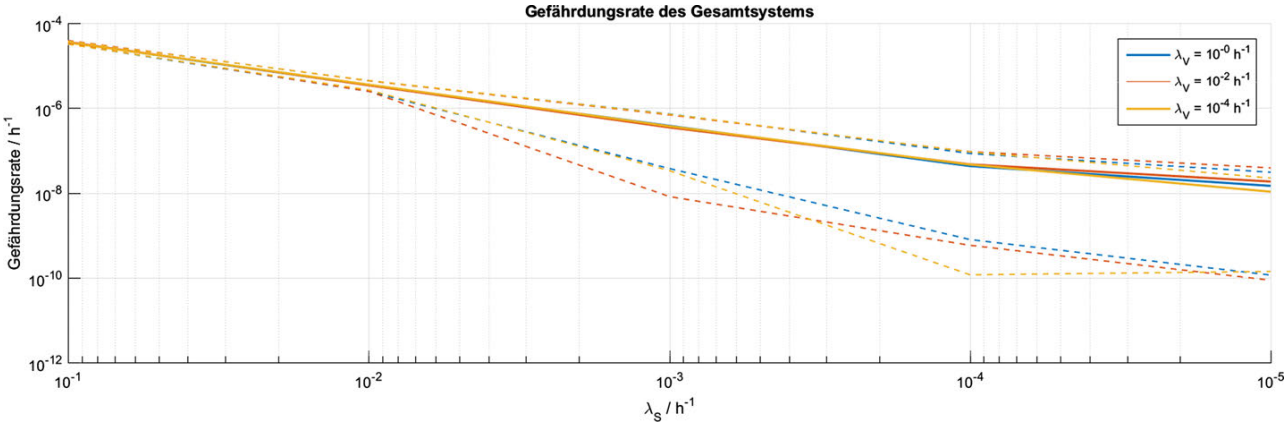

Abb. 15: Ergebnisse der Monte-Carlo-Simulation mit den dazugehörigen Konfidenzintervallen (99,9 % statistische Sicherheit, strichlierte Linien); simulierte Modelle, bestehend aus den Petrinetzen gemäß Abb. 8, 9, 12, 13 und 14.

halten des Modells analysieren zu können, werden anschließend die Parameter λ_V und λ_S variiert, da bei ihnen ein starker Einfluss auf die Verlässlichkeit der Ortung und damit auf die entstehende Gefährdung vermutet werden kann. Die Simulation kann nun wie folgt zur Systemauslegung genutzt werden: Sollten die simulierten Kenngrößen nicht mit den makroskopischen Anforderungen an das System übereinstimmen, können die Parameter λ_V und λ_S so lange variiert werden, bis die Simulationsergebnisse mit diesen Anforderungen übereinstimmen. Hieraus ergeben sich Anforderungen an das Ortungssystem.

Im Rahmen dieser beispielhaften Simulation ist die Gefährdungsrate die einzige Kenngröße für die Verlässlichkeit des Verkehrssystems. Es ist in Abb. 15 zu erkennen, dass die Variation von λ_S (Transition vom sicheren in den gefährdenden Lokalzustand des Ortungssystems) einen stärkeren Einfluss auf die Gefährdung des Verkehrsprozesses hat als die Variation von λ_V (Transition vom vertrauenswürdigen in den nicht vertrauenswürdigen Lokalzustand des Ortungssystems). Dieses Ergebnis erscheint plausibel, da ein häufiger Wechsel in den nicht vertrauenswürdigen Zustand technisch gleichbedeutend ist mit einer Erhöhung der Alarmhäufigkeit (Alarm mit dem Hinweis, den Messwert nicht zu nutzen). Bei gleichbleibender Entscheidungsgüte der Überwachung (λ_S) führt eine Erhöhung von λ_V lediglich zu einer höheren Eintrittswahrscheinlichkeit des Fail-Safe-Zustandes. Dieser Zustand verringert zwar die Verfügbarkeit des Systems und damit die Einsatzmöglichkeiten im Schienenverkehr, birgt aber für sich gesehen keine grundsätzlichen Gefahrenquellen. Dagegen führt eine nicht funktionsfähige Überwachung der Ortung – konservativ betrachtet – direkt zu einer Gefährdung. Um ein tieferes und damit weniger konservatives Verständnis des ausgehenden Risikos zu gewinnen, ist in weiteren Arbeiten eine Betrachtung der Schadensraten gemäß dem Risikogenesemodell (vgl. Abb. 10) notwendig.

Ein Vergleich mit der einschlägigen Normung [1] zeigt allerdings, dass die betrachteten Ausfallraten für λ_V und λ_S und damit die entstehenden Gefährdungsraten größer sind als die zulässigen (10^{-9} pro Stunde für SIL 4). Zwar war dies bereits vor der Simulation abzusehen, da die Ermittlung kleinerer Ausfallraten im Rahmen der vorliegenden Simulationsstudie nicht mit vertretbarem Rechenaufwand durchführbar war. Aber es ist davon auszugehen, dass die Gefährdungsrate aus Abb. 15 dem dargestellten Trend weiter folgt und gegen eine Sättigung konvergiert. Diese Sättigung ergibt sich aus der Gefährdungsrate der nach SIL 4 ausgelegten Fahrwegsteuerung.

Das Ziel der Simulation zur Ermittlung der Gefährdungsrate besteht darin, zu zeigen, dass sowohl ein gesellschaftlich als auch normativ akzeptables Risikoniveau erreicht werden kann. Dies kann über verschiedene Risikoakzeptanzkriterien erfolgen, wobei in dem betrachteten Beispiel das Prinzip der mindestens gleichen Sicherheit angewandt werden sollte, da in diesem Fall eine bestehende von einer neuen Technologie abgelöst werden soll. Die in der vorliegenden Publikation erfolgte Auslegung deckt jedoch nur die minimalen Anforderungen aus den gesetzlichen Vorgaben ab, welche von allen sicherheitskritischen Komponenten zusammen erfüllt werden müssen. Um die mindestens gleiche Sicherheit nachweisen zu können, muss zunächst das bestehende Risiko, das mit dem Betrieb der momentan im Einsatz befindlichen Technologie verbunden ist, anhand von Szenarien bestimmt werden.

6 Fazit und Ausblick

Die in diesem Beitrag vorgestellte Methode zeigt auf funktionaler Ebene einen neuen Ansatz zur Charakterisierung der Messqualität einer GNSS-basierten Ortungseinheit. Durch die Betrachtung des Verkehrs-, Ortungs- und Überwachungsprozesses können in einer frühen Phase des Entwicklungsprozesses sowohl Kenntnisse über die Verlässlichkeitskenngrößen des Schienenverkehrs gewonnen als auch Anforderungen an die Ortungseinheit präzisiert werden. Die in diesem Beitrag gezeigten Ergebnisse betonen die Bedeutung der Funktionsüberwachung gegenüber der Funktion und ebenso, wie durch eine Kombination dieser beiden komplementären Prinzipien die Verlässlichkeit des Gesamtsystems gesteigert werden kann. Dies ist insoweit für den Einsatz als sicherheitsrelevante Anwendung innerhalb des Schienenverkehrs wichtig, da eine satellitenbasierte Ortung – ohne Überwachungsfunktionen – auf absehbare Zeit nicht die erforderliche Verlässlichkeit erreichen können wird.

In weiteren Arbeiten muss der Einfluss des Simulationsumfangs (sample size) untersucht und der Prozessablauf optimiert werden, damit die mit der Monte-Carlo-Simulation ermittelten Konfidenzintervalle verringert und zugleich kleinere Gefährdungsraten ermittelt werden können – dies bei einem vertretbaren Rechenaufwand. Weiterhin müssen gemäß Risikogenesemodell – aufbauend auf den Gefährdungsraten – die Schadensraten bestimmt werden, um das entstehende Risiko umfassend beurteilen zu können. Eine umfassende Analyse der Verlässlichkeit erfordert zusätzlich die Betrachtung einer weiteren, zur Sicherheit orthogonalen Systemeigenschaft, nämlich der Verfügbarkeit. Hierzu sind die Modelle dahingehend zu erweitern, dass mittlere Aufenthaltswahrscheinlichkeiten von Zuständen ermittelt werden können. Überdies muss im Modell des Verkehrsprozesses zwischen gefährlichen und sicheren Ausfällen unterschieden werden. Die entwickelte Methode muss ferner durch reale Messdaten aus dem Schienenverkehr oder durch andere methodische Ansätze validiert werden.

Zum aktuellen Zeitpunkt setzt die vorgestellte Methode bei der manuellen Modellierung der Ortungs- und Verkehrsprozesse ein umfangreiches Fachwissen in den Bereichen Ortung, (Schienen-)Verkehr und Petrinetzmodellierung voraus. In weiteren Arbeiten muss deshalb der Modellierungsprozess weiter vereinheitlicht werden. Hierzu kann die der PROFUND-Methode zugrundeliegende Modularisierung der einzelnen Bestandteile genutzt werden, um eine teilautomatisierte Modellerstellung zu ermöglichen. So könnte der Einsatz bzw. die Bereitstellung vorgefertigter Module und Muster, z. B. für die Ortungseinheit, die Hürde für die Modellerstellung senken und damit zur Verbreitung der Methode beitragen. Jedoch stellt die immer weiterwachsende Komplexität der Netze eine Herausforderung für den Anwender und die Toolunterstützung dar. Sich anschließende Forschungsarbeiten müssen zeigen, an welchen Stellen eine Vereinfachung des Modells zulässig ist und inwieweit die hier verwendete Modellierungssoftware optimiert werden muss.

Danksagung: Wir danken Rasmus Rüdiger sowie Philipp Leder für die inhaltliche Unterstützung und Christian Frohn sowie Julia Rosenau für Korrektur und Formatierung dieses Beitrags.

Literatur

1. DIN EN 50126: Bahnanwendungen – Spezifikation und Nachweis von Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit und Sicherheit (RAMS) – Teil 1 & 2: DIN EN 50126:2018-10, Deutsche Fassung EN 50126:2018-10, 2018.
2. STARS: D5.4 EGNSS Services Evolution for railways and ETCS impacts. 2018, www.stars-rail.eu/wp-content/uploads/2019/08/D5.4_EGNSS_Services_Evolution_for_railways_and_ETCS_impacts.pdf, Stand: 01.10.2020.
3. smartrail 4.0 – Technologiebericht PoC GLAT, 2020, https://www.smartrail40.ch/service/download.asp?mem=0&path=/download/downloads/Anlage%20LCS_05%20-%20Technologiebericht-PoC_GLAT_v1.00.pdf, Stand: 14.01.2021.
4. STARS: D5.3 EGNSS Target Performances to meet railway safety requirements. 2018, http://www.stars-rail.eu/wp-content/uploads/2018/07/STR-WP5-D-ANS-034-07_-_D5.3_-_EGNSS_Target_Performances_to_meet_railway_safety_requirements_.pdf, Stand: 01.10.2020.
5. Grimm, M.; Hartwig, K.; Meyer zu Hörste, M.: Anforderungen an eine sicherheitsrelevante Ortung im Schienenverkehr. In: 20. Verkehrswissenschaftliche Tage, Grenzenloser Verkehr in einem Grenzenlosen Europa. 20. Verkehrswissenschaftliche Tage, Dresden, 2005.
6. GaLoROI: D8.3: Final Report. 2014, http://www.galoroi.eu/smart-railway-localisation/results/, Stand: 01.10.2020.
7. Kiriczi, S.: Signaltechnisch sichere Fehlergrenzen für die Erfassung der Bewegungszustände von Bahnen. Dissertation, Technische Universität Braunschweig, Institut für Regelungs- und Automatisierungstechnik, VDI Verlag Düsseldorf, 1996.
8. Lu, D.: GNSS for Train Localisation Performance Evaluation and Verification. Dissertation, Technische Universität Braunschweig, Braunschweig, Juni 2014, https://publikationsserver.tu-braunschweig.de/receive/dbbs_mods_00057180, Stand: 01.10.2020.
9. European Railway Agency: UNISIG SUBSET-036, FFFIS for Eurobalise, https://www.era.europa.eu/sites/default/files/filesystem/ertms/ccs_tsi_annex_a_-_mandatory_

specifications/set_of_specifications_3_etcs_b3_r2_gsm-r_b1/index009_-_subset-036_v310.pdf, Stand: 01.10.2020.
10. European Railway Agency: Guideline for the application of harmonized design targets (CSM DT) for technical systems as defined in (EU) Regulation 2015/1136 within the risk assessment process of Regulation 402/2013, 2017.
11. European GNSS Agency: Report on Road User Needs and Requirements, 2019, https://www.gsc-europa.eu/sites/default/files/sites/all/files/Report_on_User_Needs_and_Requirements_Road.pdf, Stand: 01.10.2020.
12. Schnieder, L.; Krumbach, P.: Positive Risikobilanzierung als ein Zulassungskriterium des hochautomatisierten Fahrens, in safe.tech 2019, München, 2019.
13. Beugin, J.; Legrand, C.; Marais, J.; Berbineau, M.; El-Miloudi, E.: Safety Appraisal of GNSS-Based Localization Systems Used in Train Spacing Control, In: IEEE Access. 1-1. 10.1109/ACCESS.2018.2807127.
14. Spiegel, D.; Geffert, A.; Schnieder, E.; Lu, D.: Stochastic behaviour quantification of GNSS receivers. Coordinates 11/16, S. 12-16, 2016, https://mycoordinates.org/pdf/nov16.pdf, Stand: 01.10.2020.
15. Dodinoiu, A.; Wagner, J.; Geffert, A.; Lu, D.; Becker, U.: Qualification of satellite-based localization systems for railway safety-related applications. In: 7th Transport Research Arena TRA 2018. Wien, 2018, DOI: 10.5281/zenodo.1440954.
16. ISO/PAS 21448:2019, Road vehicles — Safety of the intended functionality, 2019.
17. Geffert, A.; Dodinoiu, A.; Lan, T.; Rüdiger, R.; Becker, U.: Formalization of automation risks for dependability-based safeguarding of the nominal function, 9. Tagung Automatisiertes Fahren, 2019, TU München mit TÜV SÜD Akademie, https://mediatum.ub.tum.de/doc/1535147/1535147.pdf, Stand: 01.10.2020.
18. Geffert, A.; Dodinoiu, A.; Becker, U.: Multiperspektivischer Ansatz zur domänenübergreifenden Formalisierung von Verlässlichkeit am Beispiel der fahrzeugautonomen Ortung, safe.tech 2019, München, 2019.
19. Geffert, A.; Dodinoiu, A.; Lan, T.; Becker, U.: Towards an Integrity-Based GNSS Measurement Quality Model for an In-Depth Understanding of Localization Dependability. In: 2020 European Navigation Conference (ENC), Dresden, Germany, 2020, pp. 1–10. DOI: 10.23919/ENC48637.2020.9317430.
20. Walter, T.; Hansen, A.; Enge, P.: Validation of the WAAS MOPS Integrity Equation, http://web.stanford.edu/group/scpnt/gpslab/pubs/papers/Walter_IONAM_1999_WAAS_MOPS_Integrity_Validation.pdf, Stand: 01.10.2020.
21. Institute for Quality, Safety and Transportation, π-Tool, http://www.iqst.de/?page_id=24, Stand: 01.10.2020.
22. Schnieder, E.: Methoden der Automatisierung: Beschreibungsmittel, Modellkonzepte und Werkzeuge für Automatisierungssysteme. Vieweg+Teubner Verlag, 1999.
23. Slovák, R.: Methodische Modellierung und Analyse von Sicherungssystemen des Eisenbahnverkehrs. Dissertation, Technische Universität Braunschweig, 2006.
24. Schnieder, E.: (Verkehrs)sicherheit als regelungstechnische Aufgabe. at 12/14, S. 829–841, 2014, https://www.degruyter.com/downloadpdf/j/auto.2014.62.issue-12/auto-2014-1133/auto-2014-1133.pdf, Stand: 01.10.2020.

Autoreninformationen

Andreas Dodinoiu, M. Sc.
Technische Universität Braunschweig,
Institut für Verkehrssicherheit und Automatisierungstechnik,
Hermann-Blenk-Straße 42, 38108 Braunschweig, Deutschland
a.dodinoiu@tu-braunschweig.de

Andreas Dodinoiu studierte Maschinenbau mit der Vertiefungsrichtung Kraftfahrzeugtechnik an der Technischen Universität Braunschweig und erwarb anschließend im Jahr 2017 seinen Masterabschluss an derselben Universität. Seit 2017 ist er am Institut für Verkehrssicherheit und Automatisierungstechnik der Technischen Universität Braunschweig als wissenschaftlicher Mitarbeiter tätig und forscht an der Ortung auf Basis satellitengestützter Ortungssysteme im Bodenverkehr. Hierbei befasst er sich vor allem mit den Aspekten der Risikobeurteilung im Bereich der funktionalen Sicherheit mithilfe von formalen Beschreibungsmitteln und mit der Einbindung neuer Technologien in den Zulassungsprozess des Bahnbereichs.

Arne Geffert, M. Sc.
Technische Universität Braunschweig,
Institut für Verkehrssicherheit und Automatisierungstechnik,
Hermann-Blenk-Straße 42, 38108 Braunschweig, Deutschland
a.geffert@tu-braunschweig.de

Arne Geffert studierte Maschinenbau mit der Vertiefung Mechatronik. Seinen Bachelorabschluss erwarb er im Rahmen eines dualen Studiums an der Ostfalia Hochschule für angewandte Wissenschaften, seinen Masterabschluss an der Technischen Universität Braunschweig. Seit dem Jahr 2015 ist er wissenschaftlicher Mitarbeiter am Institut für Verkehrssicherheit und Automatisierungstechnik der Technischen Universität Braunschweig und beschäftigt sich mit Sicherheit und Verlässlichkeit für den automatisierten Verkehr. Seine Forschungsgebiete umfassen die Simulation GNSS-basierter Multi-Sensor-Ortungssysteme, das auf Petrinetzen basierende PROFUND-Modellkonzept sowie Ansätze zur sicherheitsgerichteten Entwicklung in frühen Phasen von Entwicklungsprozessen. Dabei befasst er sich sowohl mit dem Straßen- als auch mit dem Schienenverkehr und sucht stets nach Synergien zwischen beiden Verkehrsdomänen.

Tianxiang Lan, M. Sc.
Technische Universität Braunschweig,
Institut für Verkehrssicherheit und
Automatisierungstechnik,
Hermann-Blenk-Straße 42, 38108
Braunschweig, Deutschland
t.lan@tu-braunschweig.de

Tianxiang Lan erwarb im Jahr 2015 seinen Bachelor in Maschinenbau an der Chonqing Universität in China und 2018 seinen Master in Maschinenbau in der Vertiefungsrichtung Mechatronik an der Technischen Universität Braunschweig. Zurzeit ist er wissenschaftlicher Mitarbeiter am Institut für Verkehrssicherheit und Automatisierungstechnik und beschäftigt sich mit Datenfusion und Voting für satellitenbasierte, integrierte Ortungssysteme sowie mit der Charakterisierung satellitenbasierter Ortungssysteme für den Straßenverkehr mithilfe des maschinellen Lernens.

Dr.-Ing. Uwe Becker
Technische Universität Braunschweig,
Institut für Verkehrssicherheit und
Automatisierungstechnik,
Hermann-Blenk-Straße 42, 38108
Braunschweig, Deutschland
u.becker@tu-braunschweig.de

Uwe Becker studierte Maschinenbau und erhielt seinen Dipl.-Ing. im Jahr 1985 und seinen Dr.-Ing. im Jahr 2004, beide an der Technischen Universität Braunschweig. Vor seiner Pensionierung hatte er als kommissarischer Leiter des Instituts für Verkehrssicherheit und Automatisierungstechnik eine Verwaltungsprofessur inne. Er verfügt über vertiefte Kenntnisse der Systemtheorie, Automatisierungs- und Steuerungstechnik und hat langjährige Erfahrung in den Bereichen Verkehrssicherheit und formale Methoden.