Bundesministerium
für Verkehr und
digitale Infrastruktur

Forschungsprojekt

Autonomes Fahren im Schienenverkehr

Kurzbericht vom Oktober 2018 (Schlussbericht auf Anfrage)

BMVI-Auftragsforschung: FE-Nr. 97.370/2016

Erstellt durch:

IVE – Ingenieurgesellschaft für Verkehrs- und Eisenbahnwesen mbH (IVE mbH) mit den Unterauftragnehmern IFS, RWTH Aachen; IVE TU Braunschweig und Prof. Hermes

Forschungsvorhaben 97.370/2016

Autonomes Fahren

Bewertung der Potentiale, Analyse bestehender Sicherheitsanforderungen und Prüfung der Übertragbarkeit auf das deutsche Eisenbahnsystem

Kurzfassung

In den letzten Jahrzehnten wurden verschiedene Ansätze für eine weitere Automatisierung des Fahrens im Schienenverkehr bis hin zum autonomen Fahren ohne Triebfahrzeugführer entwickelt und getestet. Das Eisenbahn-Bundesamt als Aufsichtsbehörde steht vor der Aufgabe, für eine weitere Automatisierung des Fahrens die Rahmenbedingungen aus rechtlicher Sicht sowie unter Sicherheitsaspekten zu definieren. In der gültigen EBO ist die Pflicht enthalten, arbeitende Triebfahrzeuge mit einem Triebfahrzeugführer zu besetzen. Neben der Überprüfung des rechtlichen Rahmens werden damit auch die erforderlichen Vorschläge für eine Anpassung erarbeitet, sodass eine weitergehende Automatisierung im Eisenbahnwesen ermöglicht wird.

Das Forschungsvorhaben gliedert sich in vier aufeinander aufbauende Untersuchungen:

Kategorisierung vorhandener Ansätze für eine weitere Automatisierung des Fahrens

Aufgrund einer Recherche werden die vorhandenen Ansätze für eine weitere Automatisierung wie folgt unterschieden:

- Abgeschlossene Schienenbahnsysteme
- Zugbeeinflussungssysteme
- Projekte und Realisierungsmaßnahmen bei der Vollbahn
- ATO over ETCS

Bestehende, automatisierte Metrosysteme sind nicht ohne weiteres auf die Eisenbahn in Deutschland übertragbar: Die automatisierten Systeme sind abgeschlossen, sodass die freien Strecken von außen nicht zugänglich sind. Das Freihalten von Gefahrenbereichen auf Bahnsteigen und des Lichtraumprofils der Strecke kann einfach überwacht werden. Eine hierfür erforderliche Kommunikation über Kabel oder WLAN-Netze auf allen Eisenbahnstrecken ist dagegen unwirtschaftlich.

...

Allerdings können Systeme für die Bahnsteigüberwachung von den Metrosystemen für die Eisenbahn übernommen werden.

Die bisherigen Projekte bei der Vollbahn zeigen die prinzipielle Machbarkeit einer weiteren Automatisierung des Fahrens bis hin zum autonomen Fahren. Systeme für die Überwachung von Bahnübergängen stehen heute am Markt zur Verfügung. Die Nutzung des entstehenden einheitlichen ETCS als Streckendatenübermittler eines ATO Systems ist in Simulationen auf PC und auf Simulationen mit bestehender Hardware möglich.

Bewertung der Potenziale und Auswirkungen einer weiteren Automatisierung des Eisenbahnverkehrs in Deutschland

Folgende wesentliche Potenziale können aufgrund einer weiteren Automatisierung im Eisenbahnverkehr in Deutschland angegeben werden:

- Optimierte Brems- und Beschleunigungsvorgänge und dadurch eine mögliche Erhöhung der Energieeffizienz – soweit eine Gesamtsystemübersicht z. B. durch einen zentralen Steuerrechner vorhanden ist.
- Steigerung der Sicherheit durch Fehlervermeidung von Menschen
- Beim fahrerlosen Fahren (GoA 3) würde die Reaktionszeiten des Triebfahrzeugführers entfallen.
- In abgeschlossenen Personennahverkehrssystemen wie S-Bahnen: Verdichtete Zugfolgetakte und ad hoc-Einsatz von zusätzlichen Zügen – in der Folge für den einzelnen Reisenden daher häufigere Verkehrszeiten und eine Steigerung der Pünktlichkeit ohne größeren Personaleinsatz.
- Für den Güterverkehr scheinen sich wesentliche Vorteile aufgrund einer möglichen Flexibilisierung und längerer möglicher Laufwege zu ergeben.

Den Potenzialen müssen aber folgende Nachteile gegenübergestellt werden:

- Mit einer weiteren Automatisierung steigert sich der Bedarf an Sicherungstechnik und Sicherheitsmaßnahmen an Infrastruktur, Fahrzeugen und IT.
- Derzeit sind die Reichweiten der Sensoren für das Erkennen von Hindernissen im Gleisbereich immer noch sehr begrenzt.
- Bisher unbekannte Verzögerungszeiten für die Steuerung der automatisierten Systeme können eventuell höher sein, als die Reaktionszeiten der Triebfahrzeugführer.

...

- Neben den technischen Aspekten kann auch die Akzeptanz der Reisenden gegenüber fahrerlosen oder autonomen Personenverkehrssystemen insbesondere im Hochgeschwindigkeitsverkehr fraglich sein.

Aufgrund der derzeit vorhandenen technischen Ausrüstung von Infrastruktur und Fahrzeugen – insbesondere aber der Leit- und Sicherungstechnik können folgende Quervergleiche angegeben werden:

- Einer möglichst flächendeckenden Ertüchtigung eines halbautomatischen Fahrbetriebs (GoA 2) wird im Vergleich zum fahrerlosen Fahrbetrieb (GoA 3) ein höheres Potenzial zugeordnet. Halbautomatischer Fahrbetrieb ist mit schon vorhandener und bewährter Technik möglich, bietet Vereinfachungen für den Triebfahrzeugführer und damit einen Sicherheitsgewinn. Demgegenüber steht der hohe technische Aufwand für einen fahrerlosen Fahrbetrieb bzw. der wesentlich höhere technische Aufwand für einen unbegleiteten Fahrbetrieb.
- Im Fernverkehr – Personen- wie auch Güterverkehr – wird einem fahrerlosen Fahrbetrieb (GoA 3) ein höheres Potenzial zugeordnet als einem unbegleiteten Fahrbetrieb (GoA 4). Die Einsparung aufgrund des Verzichts von Personal im Zug wird gegenüber dem wesentlich höheren technischen Aufwand für einen unbegleiteten Fahrbetrieb als gering eingeschätzt. Hinzu kommt insbesondere im Hochgeschwindigkeitsverkehr eine eventuell mangelnde Akzeptanz der Reisenden gegenüber unbegleiteten Zügen.
- Damit ergeben sich Potenziale für einen unbegleiteten Fahrbetrieb (GoA 4) aus derzeitiger Sicht ausschließlich in abgeschlossenen Zugsystemen mit hohen Taktfolgen – und damit in entsprechenden Nahverkehrs oder S-Bahn-Systemen. Auch denkbar wären kleine selbstfahrende Gütereinheiten auf begrenzten Strecken z. B. auf Anschlussgleisen.

Analyse der Sicherheitsanforderungen, Identifizierung von Sicherheitsproblemen

Für die Analyse der Sicherheitsanforderungen wird ein Risikomanagementverfahren in Anlehnung an die CSM-Verordnung durchgeführt:

- Im Fokus des Risikomanagementverfahrens steht zunächst die funktionale Sicherheit. Sicherheitsanforderungen werden in Form von Safety Integrity Levels mittels der semi-quantitativen Methode „Risk Score Matrix“ (RSM) abgeleitet.
  Entsprechend dem Schadensausmaß – das mit dem Ausfall oder Versagen einer Funktion verbunden werden kann – ergibt sich für Komponenten der Eisenbahnsignaltechnik in der

...

Regel die höchste Sicherheitsanforderung SIL 4. Diese kann bei geeigneten vorhandenen Barrieren wieder reduziert werden.
Gleichzeitig wird berücksichtigt, dass Fehlhandlungen von Triebfahrzeugführern oder von weiteren Zugpersonalen immer Einfluss auf die Wahrscheinlichkeit bzw. auf die Ausfallrate haben. Das Schadensausmaß bei Versagen einer Funktion bleibt unabhängig vom Automatisierungsgrad immer gleich.

- Anschließend werden Resilienz und Vulnerabilität der (neuen) Automatisierungssysteme gegenüber nicht-technischen Gefahren bzw. gegenüber böswilligen Angriffen untersucht. Alle Komponenten der unterschiedlichen Teilsysteme werden sogenannten Conduits zugeordnet innerhalb denen die dieselben Security-Anforderungen gelten. Die Anforderungen werden in Form von Security-Levels (SL) angegeben, die die Stärke eines Angreifers bzw. für einen erfolgreichen Angriff beschreiben.

Bei Erhöhung auf den Automatisierung GoA 2 ergibt sich auch für die Basisfunktion Steuern und Überwachen von Bremsen und Beschleunigen mit SIL 4 die höchste Sicherheitsanforderung. Diese Sicherheitsanforderung betrifft zudem nicht nur die direkten Steuersysteme, sondern auch das Datenkommunikationssystem und den Systementwurf mit z. B. der Festlegung von Überwachungskurven.

Für das Conduit Datenkommunikationssystem kann zudem beispielhaft ein Security-Level-Target von SL-T 3 abgeleitet werden. Eine Reduzierung auf SL-T 2 ist nur möglich, soweit z. B. der Ort des Angriffs als nah bewerten werden kann. Diese für das Datenkommunikationssystem abgeleitete Security-Anforderung kann auf weitere Systeme bzw. Komponenten, für die SIL 4 auch bei den weiteren Automatisierungsgraden gefordert wird, übertragen werden.

Ab einen Automatisierungsgrad GoA 3 ist ein Triebfahrzeugführer in einem Zug nicht mehr vorgesehen. Mit Ausnahme des Erkennens von Stör- oder Notfällen werden alle Basisfunktionen durch technische Systeme erfüllt. Für die Basisfunktionen Fahrgastwechsel überwachen und Fahrweg überwachen insbesondere mit den Schutzfunktionen ergeben sich Sicherheitsanforderungen zwischen SIL 2 und SIL 3. Für die weiteren Basisfunktionen ergeben sich mit SIL 4 wieder die höchsten Sicherheitsanforderungen. Hierzu gehören insbesondere die Schutzfunktionen hinsichtlich der Fahrzeugortung und der Datenkommunikation.

Im höchsten Automatisierungsgrad GoA 4 soll die Basisfunktion Stör- oder Notfall erkennen (Überwachen des Betriebes) durch technische Systeme erfüllt werden. Entsprechend dem derzeitigen Stand können zwar technische Einzelentwicklungen als Realisierungsmög-

...

lichkeiten angegeben werden, nicht aber wie eine Zusammenstellung technischer Systeme für eine vollständige Automatisierung. Aufgrund einer bisher fehlenden Differenzierung ergibt sich allgemein zunächst eine Sicherheitsforderung von SIL 4.

Prüfung der Eignung der rechtlichen Rahmenbedingungen in Deutschland mit Vorschlägen für Anpassungen des geltenden Rechtsrahmens

Der aktuelle Bestand an Rechtsnormen wird erfasst. Dabei zeigt sich, dass im Recht der Eisenbahnsicherheit sowohl auf europäischer (Interoperabilitätsrichtlinie mit TSI „Verkehrsbetrieb und Verkehrssteuerung“) als auch auf nationaler Ebene (hier allerdings nur auf Verordnungsebene: § 45 EBO) dem Triebfahrzeugführer eine zentrale Rolle zukommt. Dabei unterscheidet das Recht der Eisenbahnsicherheit, soweit es um den Schutz von Leben, Gesundheit und Sachgütern geht, nicht zwischen funktionaler Sicherheit („safety“) und Schutz vor nichttechnischen Gefahren („security“), sondern deckt beide Gefahrenquellen ab.

Soll in der Bundesrepublik Deutschland zukünftig automatisiertes Fahren auf der Schiene zugelassen werden, so besteht jedenfalls ab der Stufe GoA 3 rechtlicher Anpassungsbedarf: Das nationale Eisenbahnsicherheitsrechts müsste auf die obligatorische Besetzung arbeitender Triebfahrzeuge mit einem Tf verzichten und für GoA 2 zulassen, dass einzelne bislang vom Tf (und weiterem Zugbegleitpersonal, dem Sicherheitsfunktionen zugewiesen sind) wahrgenommene Funktionen durch technische Ersatzsysteme erfüllt werden. Dazu bedarf es einer Anpassung der EBO (§ 45). Hinsichtlich des Rechtsregimes der „Cybersicherheit in Kritischen Infrastrukturen“ (NIS-Richtlinie, BSI-Gesetz, Kritisverordnung) ist ein Anpassungsbedarf nicht ersichtlich.

Fortgeschrittene Stufen automatisierten Fahrens auf der Schiene, die auf den Tf verzichten, kann das nationale Recht nur für Strecken und Netze zulassen, die nicht in den Anwendungsbereich der Interoperabilitätsrichtlinie fallen. Das europäische Eisenbahnrecht der Interoperabilität enthält (noch) keine Öffnungs- oder Ausnahmeklausel, die automatisiertes Fahren auf der Schiene ohne Tf ermöglicht. Aus verfassungsrechtlichen Gründen könnte die Zulassung automatisierten Fahrens auf der Schiene eine parlamentsgesetzliche Legitimationsgrundlage (Änderung des AEG) erfordern.

Auf der Basis der Annahme, dass die Einführung automatisierten Fahrens auf der Schiene keine parlamentarische Entscheidung durch Gesetz erforderlich macht, wird ein Vorschlag für eine Ergänzung der EBO (§ 46 neu) gemacht, der

...

- sich an der Straßenbahn-Bau- und Betriebsordnung (BOStrab) orientiert, die in § 53 Abs. 2 eine Ausnahme von der Pflicht normiert, jeden Zug während der Fahrt mit einem streckenkundigen Fahrzeugführer zu besetzen,
- eine Ausnahme von allen in § 45 EBO enthaltenen Pflichten zu, die sich auf das erforderliche Zugpersonal beziehen,
- einen klarstellenden Vorbehalt zugunsten des vorrangigen Eisenbahnrechts der EU enthält,
- mit dem Maßstab „nach dem Stand von Wissenschaft und Technik“ angesichts des Gefährdungspotentials das höchste der im technischen Sicherheitsrecht zur Verfügung stehenden Anforderungsniveaus enthält,
- für alle Stufen des automatisierten Fahrens auf der Schiene (nur) die „gleiche Sicherheit“ wie die durch das konventionelle Eisenbahnsystem erreichte bzw. erreichbare Sicherheit fordert,
- neben einer Generalklausel einzelne Sicherheitsanforderungen konkretisiert, die sich an den funktionalen Sicherheitsanforderungen anhand der Basisfunktionen orientiert, wie sie in den Anhängen D und E systematisiert und konkretisiert werden,
- nur eine schrittweise (für einzelne Strecken) und rückholbare (Widerruflichkeit der Ausnahme) Einführung der Automatisierung im Wege von Ausnahmegenehmigungen zulässt,
- eine Kooperationspflicht zwischen Infrastrukturbetreiber und Eisenbahnverkehrsunternehmen zur Gewährleistung der Funktionsfähigkeit sicherer technischer Ersatzsysteme enthält.

Forschungsvorhaben 97.370/2016

Autonomes Fahren

Bewertung der Potentiale, Analyse bestehender Sicherheitsanforderungen und Prüfung der Übertragbarkeit auf das deutsche Eisenbahnsystem

Automatic Train Operation

Assessment of potentials, analyse of safety and security requirements, verification of transferability to the German railway system

Abstract

Today the automation is one of the key words in the technical discussion of road traffic and of railway transport as well. For train operation, it is usually to differentiate between five Grades of Automation (GoA) – from GoA 0 with no automation and on-sight operation up to GoA 4 with unattended train operation without a driver even in case of disruption or accident. However, in the European railway networks, also in the German railway network, the train protection is automated – according to GoA 1.

In the past decades, different approaches for a further automation have been developed and tested. Nevertheless, in Germany a driver in the working power car is necessary in accordance to the current legal framework. Therefore, the responsible Federal Ministry of Transport and Digital Infrastructure and the Federal Railway Authority – the National Safety Authority – have to develop and propose safety requirements and legal conditions.

The research project is divided in four analyses:

Categorisation of existing approaches for further automation of train driving and operation

On basis of a literature research, the existing approaches are summerised in profile letters. In a first step the following categories are differentiated:

- Closed railway systems
- Automatic train control systems

...

- Projects and first implementations in conventional railway systems
- ATO over ETCS

Existing automatic metro systems are not applicable to the German railway system directly. Most of the automatic systems are closed. An unauthorised access to tracks and infrastructure gauge is not possible. Tracks and platforms can be monitored easily. In contrast, the German railway network is an open system. In addition, the required data communication via cable or Wi-Fi network on all railway lines will be cost intensive.

First implementations in conventional railway systems show that automatic train operation even up to unattended train operation is possible. In addition, in some projects solutions for an ATO over ETCS are developed. Here ETCS can be used as a homogeneous basis for the required data communication.

Assessment of potentials and effects of further automation of train operation in the German railway network

The following significant potentials of a further automation of train operation are identified:

- Optimisation of braking and acceleration processes and so increase of energy efficiency – if the system includes a complete system overview or a central control and managing unit
- Increase safety by avoiding human failure – the driver's reaction times would eliminate in driverless train operation (GoA 3).
- Possibility of ad hoc use of additional trains in closed passengers transport systems
- Possibility of longer routes in rail freight transport

In contrast, the following disadvantages have to consider:

- Further automation increases the need for safety and security technology on infrastructure, vehicles and IT.
- Today, the sensor’s range for obstacle detection is limited.
- The resulting delay times in ATO systems are unknown.
- The passenger’s acceptance of unattended train operation, especially in high-speed traffic, is questionable.

Analyse of safety and security requirements

Safety and security requirements are analysed on basis of the Regulation (EU) N°402/2013 (CSM) – the harmonised framework for risk assessment:

...

- The first part of an overall risk management process is focussed on safety functions of train operation. Safety integrity Levels (SIL) are set for the safety functions by using the semi-qualitative method “Risk Score Matrix” in accordance to the German pre-standard DIN VDE V 0831-103.
  For the signal system, the highest level SIL 4 is required. It is possible to reduce the level for a separate safety function, if safety barriers effected to a separate safety function are determined. In addition, human errors of the driver or other train staff have influence on the failure rate. However, in a railway system the consequences of a malfunction are independent of the grade of automation.
- The second part of the risk management process is focussed on security requirements. Generally, automated control and operation systems use information technology that increase the opportunity for cyber-attacks against control system hardware and software. All devices and subsystems of an automated train operation system are allocated to conduits and zones. One conduit or zone shares common security requirements. On basis of the framework specified in IEC 62443 for each conduit or zone a target security level (SL-T) from SL-T 0 to SL-T 4 is set, that summarise detailed technical control system requirements associated to seven foundational requirements.
  By example for the communication system a target security level of SL-T 3 is set, because an attacker needs advanced security knowledge, advanced domain knowledge and advanced knowledge of the train operation system.

Review of the legal framework, suitability of existing rules and proposal of modification the work rules

The existing – European as well as national – legal framework for railway interoperability and safety is based on the train drivers’ function. This concerns both the “safety” in terms of correct functioning of the rail system and the “security” in terms of protection against attacks by third parties. In the context of Union law

- the Directive (EU) 2016/797 on the interoperability of the rail system within the European Union (recast) and
- the Commission Regulation (EU) 2015/995 amending Decision 2012/757/EU concerning the technical specification for interoperability relating to the ‘operation and traffic management’ subsystem of the rail system in the European Union

...

is relevant. In the German national context is relevant the "Railway Construction and Operation Act" (EBO, regulation issued by the Federal Ministry of Transport). According to § 45 EBO the use of train drivers is compulsory.

Consequently, German legislation has to be adapted to allow the implementation of automatic train operation up to unattended train operation introducing the possibility to replace train drivers' function by technical systems. In contrast, the new legal regime concerning cyber-security of critical infrastructures does not have to be adapted.

Advanced automatic train operation can be allowed by German national legislation only in so far as European rail interoperability legislation is not applicable (networks that are functionally separate from the rest of the Union rail system and intended only for the operation of local, urban or suburban passenger services). The Directive (EU) 2016/797 does not currently contain an exception, which would allow the renunciation of the use of train drivers. The question that remains unanswered is to what extend the decision in favor of advanced automatic train operation is "essential" in the sense that as a result of the national constitutional law the legislation could remain reserved to German Parliament.

A model of a new provision (§ 46 EBO) that could be adopted is proposed as part of this research project. This proposal

- is inspired by the regulation issued by the Federal Ministry of Transport concerning automatic metro systems,
- includes a clarifying reservation as regards prior-ranking Union railway law,
- includes high level using the formula "according to the state of the art in science and technology",
- requires the same level of safety/security which is required for the conventional railway system,
- requests proof of safety/security related to the basic safety functions – following the analysis of safety and security requirements in this research project,
- only allows automatic train operation as an exception (only specific cases, step-by-step-strategy, revocability),
- includes compulsory cooperation between railway undertakings and infrastructure managers in order to ensure an adequate level of safety/security).