Scientific Railway Signalling Symposium 2018

Digital neue Wege fahren

13.06.2018

TECHNISCHE UNIVERSITÄT DARMSTADT

Institut für Bahnsysteme und Bahntechnik

Integrierter Galileo-Navigationsempfänger für Bahnanwendungen - Hochgenaue und robuste Lokalisierung durch inertiale Sensorfusion mit Galileo-basierten Navigationsdaten

René Zweigel, **Jan-Jöran Gehrt, Dirk Abel**

alle Institut für Regelungstechnik der RWTH Aachen University

1 Einleitung

Satellitennavigation (GNSS – Global Navigation Satellite System) liefert einen essentiellen Beitrag für generelle Automatisierungs- und Sicherungsfunktionen für Transportsysteme aller Art. Insbesondere für den Bahnsektor lassen sich damit effizientere Prozessabläufe realisieren, sowohl für sicherheitskritische als auch komfortsteigernde Anwendungen. Zusätzlich erlaubt eine satellitenbasierte Lokalisierung, die streckenseitige Sensor- und Geräteausstattung zu reduzieren und damit enorme Anschaffungs- und Instandhaltungskosten einzusparen. Notwendige Systemanforderungen hierfür sind beispielhaft eine gleisgenaue Positionsbestimmung, eine generelle Vernetzungsfähigkeit und ein flexibler, mobiler Datenaustausch. Diese drei wichtigen Themen werden durch das BMWi-Förderprojekt Galileo Online: GO![1][2] aufgegriffen, das die Entwicklung eines robusten und hochgenauen Satellitennavigationsempfängers speziell für Bahnanwendungen zum Ziel hat. Ein ganz zentrales Element der Empfängerentwicklung nimmt hierbei die Nutzbarmachung des neuen europäischen Satellitennavigationssystems Galileo ein.

Im aktuellen GNSS Market Report 2017 der European Global Navigation Satellite Systems Agency (GSA) wird der bahnseitige Anteil an allen satellitenbasierten Anwendungen auf gerade einmal 0,1 % abgeschätzt [1]. Der Bericht zeigt allerdings auch ein sehr hohes Einsatzpotential von GNSS-Anwendungen im Bahnbereich auf, sowohl bei sicherheitskritischen als auch bei Komfortanwendungen. Vor allem die Definition und Einführung von ETCS (European Train Control System) für Zugleitsysteme, das automatisierte Sicherungsfunktionen und eine permanente Zugkontrolle und Zugüberwachung übernehmen soll, wird der GNSS-Durchdringung im sicherheitskritischen Bahnbereich mittelfristig enormen Anschub verleihen.

Parallel dazu wird durch die Errichtung des europäischen Satellitennavigationssystems Galileo ein ziviles System aufgebaut, das Vorteile hinsichtlich Genauigkeit, Verfügbarkeit und Zuverlässigkeit gegenüber anderen Systemen bietet. Gerade im Hinblick auf sicherheitskritische Aspekte sind die Themen Verfügbarkeit und Integrität von besonderer Bedeutung. Dies trifft insbesondere auf den Bahnbereich mit seinen sehr hohen Anforderungen an die Zuglokalisierung zu.

Es gibt bereits aktuelle Forschungsvorhaben, die sich diesen Themen widmen. Beispielhaft kann das Projekt GaLoROI (Galileo Localisation for Railway Operation Innovation, Projektlaufzeit 2012-2014) genannt werden, das sich mit der Entwicklung einer on-board Lokalisierungseinheit zur Integration in das bestehende Zugsystem beschäftigt hat [2]. Im Vordergrund stand die Zertifizierungsfähigkeit der Lokalisierungseinheit [3]. Das Projekt konzentrierte sich auf die Kombination bestehender Technologien. In 3InSat (Train-Satellite, Projektlaufzeit 2012-2014) erfolgte die Entwicklung und Validierung einer neuen satellitenbasierten Lokalisierungs- und Kommunikationsplattform, die in bestehende ERTMS (European Rail Traffic Management System) Systeme integriert werden kann und SIL4-Anforderungen erfüllt [4], [5]. Die Projektergebnisse werden im Folgeprojekt ERSAT (ERTMS on Satellite, Projektbeginn 2015) validiert [6].

[1] Förderkennzeichen: 50NA1510 (Projektlaufzeit 04/2015 bis 06/2018)

[2] Homepage: www.go-galileo-online.de

Auch auf europäischer Ebene können diverse Projekte zur Integration von GNSS in Sicherungsfunktionen aufgeführt werden. Das Projekt RHINOS (Railway High Integrity Navigation Overlay System, Projektlaufzeit 2016-2017) hatte die Konzeptentwicklung einer überlagerten Integritätsarchitektur für GNSS-basierte Zuglokalisierung zum Ziel. Hierbei wurden bestehende Luftfahrtansätze adaptiert und bahnspezifisch erweitert. Im Projekt NGTC (Next Generation Train Control, Projektlaufzeit: 2013-2016) wurde eine Machbarkeitsstudie zu einem neuartigen Konzept einer GNSS-basierten virtuellen Balise in Kombination mit EGNOS (European Geostationary Navigation Overlay System) für ETCS-Level 3 erstellt, wobei ein Fokus zum Beispiel auf der länderübergreifenden Kompatibilität des Systems lag.

Allen genannten Vorhaben ist gemein, dass die konkrete Empfängerentwicklung in Kombination mit neuen Mobilfunktechnologien und zentraler Service-Plattform nicht Projektbestandteil ist.

Genau diese Themen sind Inhalt des hier vorgestellten Projekts Galileo Online: GO! In GO! wird ein für Bahnanwendungen maßgeschneiderter Navigationsempfänger entwickelt, in den modernste Kommunikationstechnik integriert ist und damit eine nahtlose Anbindung eines zentralen Servicesystems ermöglicht. Im Projekt wurde ein System aus der Synthese von optimierten Kommunikationswegen zur Datenerfassung und Datenbereitstellung sowie für Dienste basierend auf einer modularen Service-Architektur, den Zentralen Diensten, entworfen. Mittels moderner Navigations- und Kommunikationstechnologien können so neue Geschäftsmodelle mit Schwerpunkt auf Bahnanwendungen, wie z. B. dem vollautomatisierten Flachrangieren, geschaffen werden.

Die Kernaufgaben des entwickelten Empfängersystems inklusive seiner modularen und flexibel erweiterbaren Schnittstellen zu Sensorik, Datenübertragungskomponenten und Informationsplattformen sind in Abb. 1 schematisch dargestellt. Der Empfänger kann die hohen Sicherheitsanforderungen der Bahn erfüllen und eine robuste, gleisgenaue Zuglokalisierung sicherstellen. Hierbei kann die Stärke des Galileo-Systems und der Vorteil eines Multi-Konstellationsbetriebs (hier: gleichzeitige Nutzung von GPS und Galileo) für die robuste Positionsbestimmung gezeigt werden.

Projektpartner sind das Institut für Regelungstechnik der RWTH Aachen, die SCISYS Deutschland GmbH, die Vodafone GmbH, das Fraunhofer-Institut für Integrierte Schaltungen, die IMST GmbH und die innoZ GmbH.

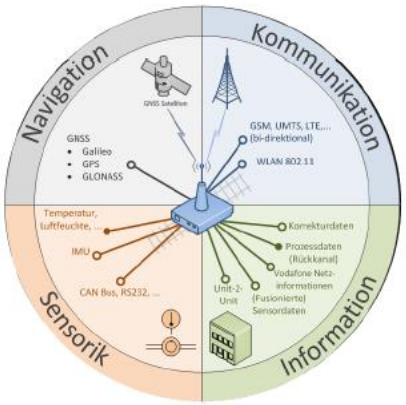

Abb. 1 Kernaufgaben des GO!-Empfängers
Quelle: [7]

2 Methoden

Im Projekt Galileo Online: GO! werden Mehrfrequenz- und Multikonstellationsverarbeitung (GPS L1, L2C, L5; Galileo E1, E5a, E5b, E5AltBOC) ebenso entwickelt wie eine Sensorfusion mit enger Kopplung auf Basis von Beschleunigungsinformationen und Satellitenrohdaten. Die Kombination verschiedener Satellitennavigationssysteme ist für eine durchgängigere Signalverfügbarkeit notwendig. Zusätzlich führen mehr verfügbare Satelliten zu einer besseren geometrischen Konstellation und damit zu einer besseren Genauigkeit. Die Verarbeitung mehrerer Frequenzen eines Satellitensystems erlaubt die Korrektur von Signallaufzeitfehlern und in Kombination mit Sensorfusionsansätzen eine genauere Lokalisierung mit hohen Abtastraten, die regelungstechnisch zur automatisierten Fahrzeugbewegung benötigt wird.

2.1 Das Navigationsmodul

Das Navigationsmodul wird in GO! vom Institut für Regelungstechnik der RWTH Aachen entwickelt und ist modular aufgebaut, siehe Abb. 2. Dadurch ist es leicht um weitere Satellitenrohdaten, Korrekturdaten aber auch um weitere bordeigene Sensordaten erweiterbar. Das Modul ermittelt die aktuellen Systemzustände auf Basis von relativen Messdaten einer Inertial Measurement Unit (IMU), die mit den absoluten Informationen des Satellitennavigationssystems fusioniert werden. Die generelle Struktur des Navigationsmoduls wurde erstmalig in [7] vorgestellt und seitdem ausgehend von GPS-Zweifrequenzbetrieb um einen Multi-Konstellationsbetrieb mit gleichzeitiger Verwendung von GPS und Galileo erweitert.

Die GNSS-Rohdaten kommen hierbei vom Basisband einer Empfängerentwicklungsplattform des Projektpartners Fraunhofer IIS. Die Rohdaten umfassen diverse Informationen wie z. B. Pseudo-Ranges, Dopplerverschiebungen, Ephemeriden und diverse Korrekturdaten.

Innerhalb der GNSS-Vorverarbeitung wird unter anderem die Augmentierung der GNSS-Beobachtungen durch differentielle Satellitennavigationsverfahren unterstützt. Außerdem enthält das Modul eine interne Logik, die eine automatische Umschaltung zwischen verschiedenen Navigations- und Korrekturmodi erlaubt. Somit wird Einschränkungen beim Satellitenempfang und Verlust von bodengebundenen differentiellen Korrekturdaten via Mobilfunk Rechnung getragen.

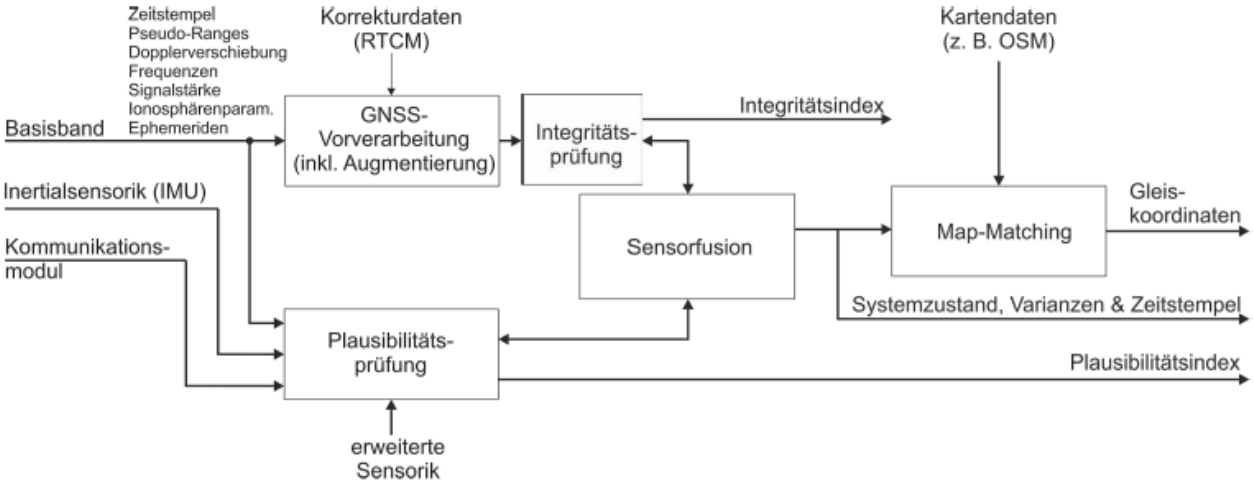

Abb. 2 Modularer Aufbau des Navigationsmoduls zur Sensorfusion von Inertialsensorik mit GNSS-Rohdaten
Quelle: [8]

Zur Fusion der Daten wird ein Kalman-Filter verwendet, der den jeweils aktuellen Systemzustand ermittelt, bestehend aus Position, Geschwindigkeit und Orientierung. Hierbei schätzt das Filter mit einer Rate von 100 Hz die aktuelle Eigenposition auf Basis von relativen Inertialmessdaten, die mit den absoluten Informationen des Satellitennavigationssystems fusioniert werden.

Der aktuelle Systemzustand wird einschließlich der vom Filter geschätzten Varianzen des Schätzfehlers und eines Zeitstempels an ein Data Gateway übermittelt und steht somit für die lokalen, regelungstechnischen Anwendungen und zusätzlich zur Übertragung an die zentrale Service-Plattform zur Verfügung.

Die Positionsinformation wird im geodätischen Referenzkoordinatensystem WGS84 ermittelt. Im Anwendungsfeld des Schienenverkehrs werden für die Bestimmung einer Zugposition jedoch Bahnkoordinaten gefordert, die Informationen zum Streckenabschnitt, der Streckenkilometrierung und Richtungsnummer enthalten. Daher ist eine Koordinatentransformation notwendig, die mittels Map-Matching-Ansätzen und Karteninformationen ermittelt wird. Das Map-Matching wird in GO! verwendet, um von einer (fehlerbehafteten) Positionsangabe auf eine bahnkonforme, schienenbezogene Kilometrierungsangabe zu kommen. Auch die wird fehlerbehaftet sein. Die aktuelle Berechnung ist lediglich vorwärtsgerichtet, soll aber zukünftig in das Navigationsfilter zurückgeführt werden. Da das vorhandene Kartenmaterial (hier OSM) allerdings eine geringe Genauigkeit aufweist, können damit lediglich Positionslösungen mit sehr schlechtem Satellitenempfang gestützt werden.

Die Module der Integritäts- und Plausibilitätsprüfung sind nicht Teil dieser Veröffentlichung.

2.2 Vorverarbeitung der Sensordaten

Die Satellitensignale werden je nach elektromagnetischer Aufladung der Ionosphäre und Wasserbeladung der Troposphäre unterschiedlich stark verzögert und abgelenkt. Allein die Positionsfehler, die durch Verzögerungen durch die Ionospährenaufladung verursacht sind, können bis zu 45 Meter betragen. Durch das bewährte Klobuchar-Korrekturmodell kann dieser Fehler bei Nutzung von GPS/L1 durchschnittlich um 50 % reduziert werden [9]. Der absolut verbleibende Messfehler nach Korrektur mit dem Klobuchar-Modell steigt allerdings mit kleiner werdendem Elevationswinkel der Satelliten.

Um insgesamt eine hochgenaue Zustandsbestimmung zu ermöglichen, wird die Augmentierung der GNSS-Beobachtungen durch differentielle Satellitennavigationsverfahren unterstützt. Hierbei werden externe Korrekturdatendienste genutzt, wie zum Beispiel der kostenpflichtige SAPOS-Dienst der Landesvermessungsämter. Als Datenformat für den Austausch wird der weitverbreitete RTCM-Standard verwendet. Diese Korrekturdaten müssen über Mobilfunk empfangen werden und sind meist kostenpflichtig.

Da die Mobilfunkverfügbarkeit im Bahnbereich nicht über die gesamte Fahrstrecke sichergestellt ist, wird die Kompensation der Ionosphärenfehler durch Nutzung mehrerer GNSS-Frequenzen bevorzugt, wodurch ein Großteil der dadurch entstehenden Fehler korrigiert werden kann [10].

2.3 Multi-Konstellationsbetrieb

Da der Satellitenempfang aufgrund von Abdeckung gerade im urbanen Bereich oder in bewaldeten Gebieten eingeschränkt ist, werden zur Erhöhung der Satellitenverfügbarkeit und zur Verbesserung der geometrischen Satellitenkonstellation gleichzeitig GPS- und Galileo-Satelliten mit jeweils zwei Frequenzen berücksichtigt. Der entsprechende Modus wird Multi-Konstellationsbetrieb genannt.

Die Herausforderung beim Multi-Konstellationsbetrieb im Vergleich zur Verarbeitung nur eines einzigen Satellitensystems besteht in der Berücksichtigung voneinander abweichender Systemzeiten. Dazu wird ein

System, in dieser Arbeit das GPS-System, als Referenzsystem definiert. Aus der Perspektive dieses Referenzsystems enthalten Laufzeitmessungen anderer Systeme lediglich eine weitere zu bestimmende Unbekannte. Die Bestimmung dieser Unbekannten erfolgt mittels eines Fehlermodells, für die mindestens fünf Satelliten zur Verfügung stehen müssen, um die insgesamt fünf Unbekannten schätzen zu können (x-, y- und z-Koordinaten, Uhrenfehler zwischen Satelliten und Rover, Zeitdifferenz zwischen GPS und Galileo).

2.4 Sensorfusion mittels Enger Kopplung

Das in dieser Arbeit umgesetzte Navigationsfilter ermittelt die aktuellen Systemzustände auf Basis von relativen Messdaten einer Inertial Measurement Unit (IMU), die mit den absoluten Informationen des Satellitennavigationssystems fusioniert werden. Es wird die Fusionsmethodik der engen Kopplung angewandt, bei der hochfrequente IMU-Daten mit 100 Hz Abtastrate und niederfrequente Beobachtungen eines Satellitenempfängers mit 10 Hz wiederum zu einer 100 Hz Navigationslösung fusioniert werden. Dahingegen bezeichnet das Verfahren der losen Kopplung eine Fusion von IMU-Daten mit zuvor separat ermittelter GNSS-Position und –Geschwindigkeit. Der Vorteil der engen Kopplung besteht darin, dass jedes Satellitensignal für sich korrigierbar ist und im Filter individuell bewertet und integriert werden kann. Die Gesamtnavigationslösung ist damit deutlich robuster und gewinnt an Genauigkeit. Einen detaillierten Überblick über das verwendete Navigationsfilter gibt die Veröffentlichung [7].

Das umgesetzte Navigationsfilter schätzt insgesamt 18 Systemzustände

$$X_k=[p^T v^n{}_{eb}{}^T q_{nb}{}^T b_a{}^T b_g{}^T c_b c_d]^T. \quad (1)$$

Teil des Zustandsvektors ist der Positionsvektor $\boldsymbol{p}$, der Geschwindigkeitsvektor $\boldsymbol{v}$, die Orientierung $\boldsymbol{q}$ als Quaternion, sowie die Messfehler der Beschleunigungsmessungen $\boldsymbol{b}_{\mathrm{a}}$ und die der Drehratenmessungen $\boldsymbol{b}_{\mathrm{g}}$. Darüber hinaus wird der Uhrenfehler des Satellitenempfängers in Form eines Offset c_{b} und Drift c_{d} berücksichtigt. Das Filter nutzt ein nichtlineares 6-DOF Modell

$$X_{k+1}=F_k(x_k)x_k+G_k(x_k)w_k \qquad w_k\sim N(0,Q_k) \quad (2)$$

$$z_k=H_k(x_k)x_k+v_k \qquad v_k\sim N(0,R_k) \quad (3)$$

wobei k der Zeitindex ist, $\boldsymbol{x}$ der Zustandsvektor, $\boldsymbol{w}$ das Prozessrauschen, $\boldsymbol{z}$ die Messgröße und $\boldsymbol{v}$ das Messrauschen. Die Vektoren $\boldsymbol{w}$ und $\boldsymbol{v}$ werden als normal verteilt und mittelwertfrei angenommen. $\boldsymbol{R}$ ist die Kovarianzmatrix des Messrauschens und $\boldsymbol{Q}$ die Kovarianzmatrix des Prozessrauschens. Die Matrizen $\boldsymbol{F}$, $\boldsymbol{G}$, und $\boldsymbol{H}$ werden als Transitionsmatrizen bezeichnet, wobei $\boldsymbol{H}$ auch Messmatrix genannt wird.

Das Filter bestimmt den kompletten Zustandsvektor mit einer Rate von 100 Hz. Die Satellitenrohdaten stehen lediglich mit einer Rate von 10 Hz zur Verfügung. Um die 100 Hz aufzufüllen, wird der Systemzustand bis zum nächsten Satellitensignal fortgeschrieben. Die Zustandsfortschreibung erfolgt über einen sogenannten Strap-Down-Mechanismus innerhalb des Navigationsfilters, das auch Signalunsicherheiten und Standardabweichungen der Sensordaten berücksichtigt [11].

3 Ergebnisse

Im Folgenden werden Lokalisierungsergebnisse präsentiert, die in realen Fahrversuchen sowohl straßen- als auch schienengebunden gewonnen wurden. Hierbei werden die erzielten Güten einer Standardlokalisierung mit GPS/L1 inklusive Klobuchar-Korrekturmodell, einer differentiell korrigierten GPS/L1-Lokalisierung und einer gleichzeitigen Nutzung von Galileo und GPS und jeweils zwei Frequenzen miteinander verglichen. Während der im Folgenden gezeigten Messungen wurde jeweils eine LORD MicroStrain 3DM-GX3-25 industrial-class IMU mit einer Abtastrate von 100 Hz verwendet. Für differenzielle Korrekturen wurden Korrekturdaten im RTCM-V3 Format über einen N-trip Caster per Mobilfunk empfangen. Als Referenzsystem wurde ein geodätischer Empfänger Septentrio AstRx3 HDC verwendet, der RTK-fähig (Real Time Kinematic) ist und mittels der empfangenen RTCM-Korrekturdaten eine zentimetergenaue Position mit einer Standardabweichung von 2 bis 8 Zentimeter ermittelt. Die Gültigkeit eines RTK-Systems als valide Referenz wurde in [12] nachgewiesen. Das Navigationsfilter wurde auf einem Rapid Control Prototyping (RCP) System mit einem 900 Hz Single-Core von dSPACE gerechnet.

3.1 Quasi-störungsfreie Umgebungsbedingungen

In der folgenden Untersuchung wurden Messfahrten in Aachen mit einem Audi A6 Avant durchgeführt. Es wurde eine Umgebung mit geringer Bebauung und Bewaldung gewählt. Um Störeinflüsse zu minimieren, wurde mit einer niedrigen Geschwindigkeit von ungefähr 10 km/h gefahren.

In Abb. 3 werden die entsprechenden Navigationslösungen aus der engen Kopplung präsentiert und verglichen. Die Ergebnisse für GPS/L1 inklusive Klobuchar-Korrekturmodell (rote Linie im oberen Ergebnisplot) liegen mit einem Positionsfehler zwischen 3 und 4 Meter im erwarteten Fehlerbereich. Im Multi-Konstellationsbetrieb mit jeweils zwei Frequenzen für GPS und Galileo (blaue Linie im oberen Ergebnisplot) und unter den hier vorherrschenden sehr guten Empfangsbedingungen konnte eine Genauigkeit deutlich unter 1 m erreicht werden. Hierfür wurden ausschließlich Satelliten mit zwei Frequenzen in der Navigationslösung berücksichtigt.

Es sei angemerkt, dass die hier erzielten Ergebnisse im Gütebereich von Differentiellem GPS (DGPS) liegen. Zur Umsetzung von DGPS wird allerdings eine permanente Internetverbindung zu entsprechenden, meist kostenpflichtigen Korrekturdiensten oder zur eigenen, kostenintensiven lokalen Basisstationen benötigt. Im Gegensatz dazu erlaubt der Multi-Konstellationsbetrieb mit jeweils zwei Frequenzen eine Internet-unabhängige Verwendung mit ebenfalls hoher Genauigkeit. Als Fazit kann formuliert werden, dass der DGPS-fähige GO!-Empfänger auch bei Problemen im Mobilfunkempfang eine sehr gute Positionsgenauigkeit durch Umschalten in den Multi-Konstellationsbetrieb mit jeweils zwei Frequenzen für GPS und Galileo ermittelt.

Diese Messkampagne hatte zum Ziel, zu zeigen, was im allerbesten Fall mit dem umgesetzten Filter möglich ist und diente als Orientierung für weitere Versuche und Evaluierungsfahrten.

3.2 Stark gestörte Empfangsbedingungen

Um die gewonnenen Erkenntnisse unter realen Bahnbedingungen mit bewaldeten Streckenteilen zu evaluieren, wurde eine Messkampagne auf einer 18 Kilometer langen Teststrecke im Chiemgau durchgeführt. Erschwerend kam hinzu, dass zur Zeit der Messfahrt Schnee lag, der auf den Bäumen zu einer erhöhten Signaldämpfung und auf vereisten Oberflächen zu einer erhöhten Mehrwegausbreitung der Satellitensignale führte, siehe Abb. 4. Aufgrund von eingeschränkter Mobilfunkversorgung während der Messfahrten war die Versorgung mit differentiellen Korrekturdaten meist gestört. Außerdem resultierten hochfrequente

Vibrationen aufgrund der Verwendung eines nahezu ungefederten Pritschenwagens und aufgrund starker Anregungen im kompletten Fahrzeugaufbau durch den Dieselmotor.

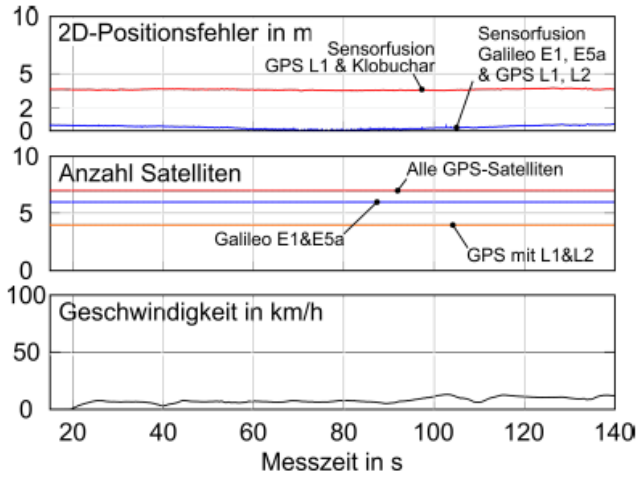

Abb. 3 Evaluierung der Verarbeitung von Multi-Konstellationssignalen unter quasi-störungsfreien Bedingungen: hohe Anzahl an Satelliten, langsame Geschwindigkeit, sehr geringe Signalabschwächung.
Quelle: [8]

Abb. 4 [links] 18 Kilometer lange Bahnstrecke durch den Chiemgau der Lokalbahn Obing-Bad Endorf LEO[3] und [rechts] Blick aus dem Messvehikel während der Messfahrt.
Quelle: [13], Map Data: ©2018 GeoBasis/BKG(©2009), Google

Abb. 5 stellt ausgewählte Ergebnisse aus der Chiemgau-Messfahrt vor. In dieser Auswertung werden drei verschiedene Lösungen des online-fähigen Navigationsfilters miteinander verglichen. Die entsprechenden 2D-Positionsfehler finden sich im oberen Teil der Abbildung. Die Fehler beziehen sich auf die ermittelte Position des Referenzsystems, dessen Modus aufgrund der schlechten Empfangsbedingungen von Korrekturdaten

[3] www.leo online.org, Chiemgauer Lokalbahn e.V., 2018

zwischen dem hochgenauen RTK-fix und dem genauen DGPS permanent wechselt. Dieses Verhalten des Referenzsystems weist auf gestörte Empfangsverhältnisse hin. Sprünge in den Auswertungen können unter anderem auf Modiwechsel des Referenzsystems zurückgeführt werden. Diese Wechsel sind im dritten Plot von oben dargestellt.

Die drei verschiedenen Filterlösungen in der Auswertung unterscheiden sich durch unterschiedliche Korrekturansätze im Fall von Multi-Konstellationsbetrieb mit jeweils zwei Frequenzen für GPS und Galileo (blaue Linie im oberen Ergebnisplot) und GPS/L1 mit differentiellen Korrekturen (grüne Linie im oberen Ergebnisplot). Außerdem wird eine nicht-fusionierte Lösung dargestellt (rote Linie im oberen Ergebnisplot). Die nicht-fusionierte Lösung basiert auf Auswertung aller korrigierten Pseudoranges von GPS und Galileo mit jeweils zwei Frequenzen und einer Positionsbestimmung nach der Methode der kleinsten Fehlerquadrate (Least Mean Squares).

Die jeweils verfügbaren/empfangenen Satelliten sind im zweiten Plot von oben aufgetragen. Hier kann beispielsweise die kurzzeitig stark reduzierte Anzahl von GPS und Galileo-Satelliten mit jeweils zwei Frequenzen (orangene und blaue Linie) nach Sekunde 2100 erkannt werden. Die Anzahl an verfügbaren Satelliten sinkt kurzzeitig auf drei Satelliten ab und bringt dadurch eine deutliche Verschlechterung der Positionsgenauigkeit für den Multi-Konstellationsbetrieb mit sich (blauer Datensatz im oberen Plot). Durch die Sensorfusion mit inertialen Sensordaten kann die Positionslösung gestützt werden, so dass die Abweichung kurzzeitig 10 Meter beträgt und nach kurzer Zeit wieder Gleisgenauigkeit mit einem Fehler unter 2 Metern aufweist.

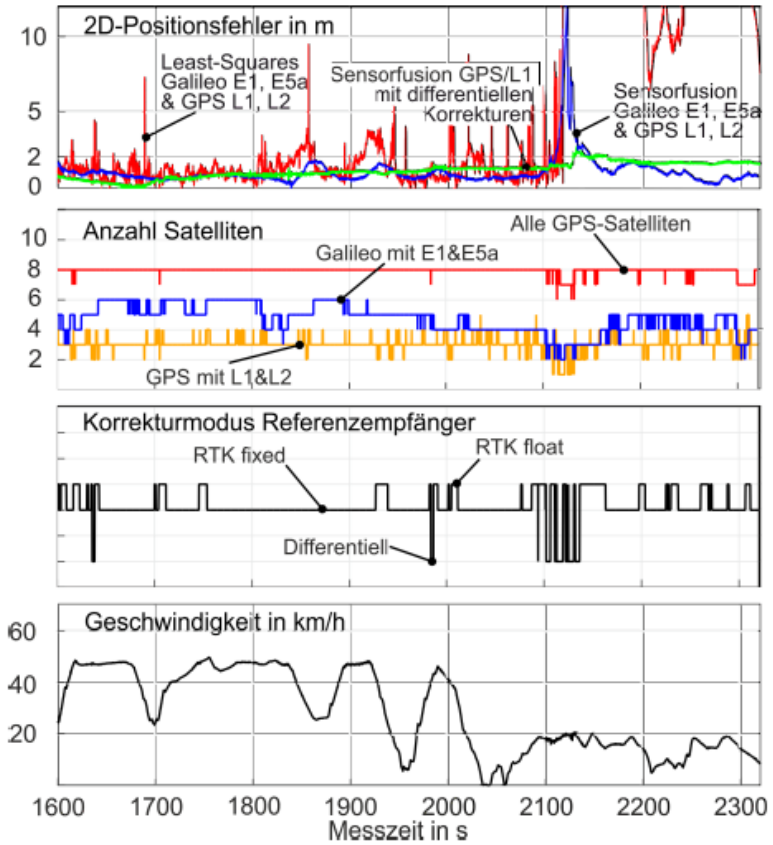

Abb. 5 Ergebnisauswertung für die Messfahrt im Chiemgau unter erschwerten Randbedingungen
Quelle: [13]

Vergleicht man dieses Ergebnis mit der nicht-fusionierten Lokalisierungslösung (roter Datensatz im oberen Plot), kann der Vorteil des Fusionsansatzes erkannt werden: bei der nicht-fusionierten Lösung erhöht sich die Positionsabweichung auf über 40 Meter und unterschreitet die 2 Meter Gleisgenauigkeit innerhalb des Messzeitraums nicht mehr.

Betrachtet man in Abb. 6 die aufgezeichneten Daten der Beschleunigungsmessung während der Chiemgau-Fahrt (links) und vergleicht diese mit einer ‚normalen' Fahrt mit ähnlicher Geschwindigkeit, dann ist zu erkennen, dass die Anregung der IMU in diesem Fall ungewöhnlich hoch war: Faktor 4 bis 5. Diese hochfrequenten Vibrationen resultierten durch den ungefederten Pritschenwagen und den antreibenden Dieselmotor. Im umgesetzten Navigationsfilter ist die verwendete IMU bezüglich ihres normalen Rauschverhaltens und Signaldrifts modelliert. Im Fall der Chiemgau-Messfahrt war das Rauschen deutlich erhöht, so dass das dadurch resultierende IMU-Verhalten nicht genau durch das hinterlegte Modell abgebildet werden konnte. Das führte während der Messfahrt zu einem verringerten Stützeffekt im Fall von eingeschränkten Satellitenempfang: siehe Zeitpunkt in Abb. 5 mit lediglich drei Satelliten.

Die Verfügbarkeit von GPS-Satelliten mit lediglich der Frequenz L1 bleibt währenddessen weiterhin hoch, so dass die Auswirkungen auf die beiden GPS/L1-basierten Ansätze geringer ausfallen. Durch den noch andauernden Ausbau des Galileo-Systems und die beginnende Erneuerung der GPS-Satelliten werden solche Ereignisse zukünftig seltener auftreten. Verglichen mit den Ergebnissen aus dem vorherigen Unterkapitel fällt die 2D-Genauigkeit aller Filterlösungen geringer aus. Die fusionierte Filterlösung mit GPS/L1 inklusive Klobuchar weißt permanent eine Genauigkeit größer 2 Meter auf. Bis auf den erwähnten kurzen Zeitraum mit wenigen Zweifrequenzsatelliten liegt die Genauigkeit der Multi-Konstellationslösung im Durchschnitt bei unter 1 Meter mit stellweise höherer Genauigkeit als DGPS.

Damit konnte auch unter sehr schlechten Umgebungs- und Empfangsbedingungen nachgewiesen werden, dass der Multi-Konstellationsbetrieb mit jeweils zwei Frequenzen für GPS und Galileo im Gütebereich von DGPS liegt und eine mobilfunkunabhängige und gleisgenaue Lokalisierung im Bahnbereich ermöglicht.

4 Zusammenfassung

In der vorliegenden Arbeit wird das Projekt Galileo Online: GO! vorgestellt und seine bahnspezifischen Ziele motiviert. In GO! wird ein für Bahnanwendungen maßgeschneiderter Navigationsempfänger entwickelt, der flexibel erweitert werden kann und eine gleisgenaue Lokalisierung ermöglicht. Über den aktuellen Stand und die entsprechenden Empfängerentwicklungen im Projekt informiert diese Publikation. Hierbei kann die Stärke des Galileo-Systems und der Vorteil eines Multi-Konstellationsbetriebs mit jeweils zwei Frequenzen für GPS und Galileo für die Positionsbestimmung gezeigt werden. Der Nachweis erfolgte in einer quasi-störungsfreien Umgebung und auf einer Bahnstrecke mit stark gestörten Empfangsbedingungen. Um zukünftig die Potentiale des GO!-Empfängers gegen die hohen Sicherheitsanforderungen der Bahn abgleichen zu können, sind breit angelegte Evaluationen und Dauertests notwendig.

Danksagung

Das Projekt Galileo Online: GO! wird durch das Bundesministerium für Wirtschaft und Energie (BMWi) gefördert und unter der Fördernummer 50NA1510 geführt. Grundlage für die Förderung ist ein Beschluss des Deutschen Bundestages. Die Autoren danken des Weiteren den Kollegen Michael Breuer, Thomas Konrad, Jiaying Lin, Andreas Trzuskowsky und Matthias Wehr für das wissenschaftliche Zuarbeiten.

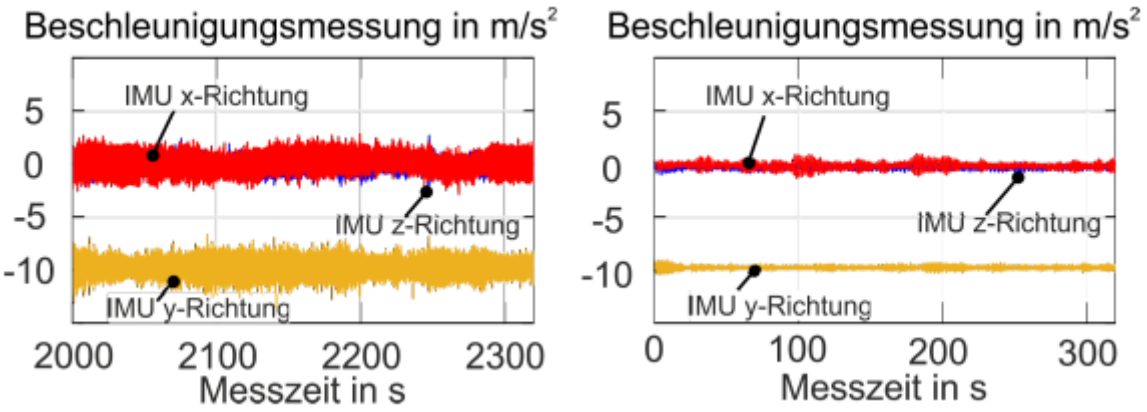

Abb. 6 Vergleich der bordeigenen Beschleunigungsdaten während der Chiemgau-Messfahrt (links) und einer ‚normalen' Fahrt mit einem Versuchsträger

5 Literaturübersicht

[1] GSA: European Global Navigation Satellite Systems (2017): *GNSS Market Report*.

[2] Nguyen et al. (2013): *Dependability evaluation of a GNSS and ECS based localisation unit for railway vehicles*, 13th IEEE International Conference on TIS Telecommunicatgions (ITST), pp. 474-479.

[3] Manz et al. (2014): *Approach to Certification of Satellite Based Localisation Unit in Railways*, Transport Research Arena, pp. 1-10, 2014.

[4] Senesi (2012): *Satellite application for train control systems: The Test Site in Sardinia*, Journal of Rail Transport Planning & Management, Bd. 2, pp. 73-78, 2012.

[5] Rispoli et al. (2013): *Recent Progress in Application of GNSS and Advanced Communications for Railway Signaling*, 23th Conference Radioelektronika, pp. 13-22.

[6] Facchinetti et al. (2015): *Trends in GNSS Italian Application Scenarios in transportation*, 2015 International Association of Institutes of Navigation World Congress, pp. 1-8.

[7] M. Breuer, T. Konrad und D. Abel (2016): *High Precision Localisation in Customised GNSS Receiver for Railway Applications*, Proceedings of the 29th International Technical Meeting of the ION Satellite Division, ION GNSS+ 2016, Portland, Oregon, pp. 779-787.

[8] R. Zweigel, J. Gehrt und D. Abel (2017): *Galileo Online: GO! - Development of a High-Precision, Satellite-based Navigation Receiver with Integrated Communication Solutions Particularly for Railway Applications*, Proc. of IRSA 2017 - International Rail Symposium Aachen (IRSA), pp. 344-359.

[9] E. Kaplan und C. Hegarty (2016): *Understanding GPS: principles and applications*, ARTECH HOUSE, Inc..

[10] S. Kedar, G. Hajj, B. Wilson und M. Heflin (2003): *The effect of the second order GPS ionospheric correction on receiver positions*, Proc. of Geophysical Research Letters, Vol. 30, No. 16, pp. 1-4.

[11] P. Zarchan und H. Musoff (2015): *Fundamentals of Kalman Filtering*, American Institut of Aeronautics and Astronautics.

[12] T. Konrad, M. Breuer, T. Engelhardt und D. Abel (2017): *State Estimation for a Multirotor using Tight-Coupling of GNSS and Inertial Navigation*, Proceedings of the 20th IFAC World Congress, pp. 12180-12185.

[13] J. Gehrt, R. Zweigel, T. Konrad und D. Abel (2018): *How the Parallel Use of GPS and Galileo Benefits Railway Applications*, Inside GNSS GPS, Galileo, GLONASS, Beidou, pp. 40-47.

Welches Potential hat smarte Infrastruktur? – ETCS für Ballungsgebiete am Beispiel der Stuttgarter S-Bahn

Peter Reinhart[1], Sven Wanstrath[2]

beide DB Projekt Stuttgart-Ulm GmbH

1 Einleitung

Die S-Bahn Stuttgart stößt an ihre Leistungsgrenzen. 2017 wurden werktäglich rund 420.000 Fahrgäste gezählt – 5 % mehr als im Vorjahr. Eine stufenweise Ausdehnung der Hauptverkehrszeiten (HVZ) von rund 2x3 Stunden (morgens/abends) auf zukünftig durchgehend 14,5 Stunden pro Tag wurde 2016 beschlossen und wird bis 2021 schrittweise umgesetzt.

Im Kern des Systems liegt die Stammstrecke, zwischen Hauptbahnhof (tief) und Schwabstraße, die zur HVZ von sechs jeweils im 15-Minuten-Takt verkehrenden Linien befahren wird. Damit ergibt sich eine Leistungsanforderung von 24 Zügen pro Stunde und Richtung bzw. einer mittleren Zugfolgezeit im Fahrplan von 2 ½ Minuten. Mit Langzügen, die den Betrieb in den Spitzenstunden dominieren, werden mit der heutigen konventionellen Leit- und Sicherungstechnik (H/V, PZB) Mindestzugfolgezeiten von 2 ¼ Minuten realisiert. Die dabei geplanten Haltezeiten von 30 Sekunden werden vielfach überschritten, HVZ-Haltezeiten von mehr als 60 Sekunden Alltag. Während die Fahrgastzahlen stetig weiter steigen, werden die Pünktlichkeitsziele regelmäßig verfehlt.

Seit 2015 wird in Stuttgart über die Einführung von ETCS Level 2 auf der S-Bahn-Stammstrecke diskutiert, zumal das bestehende Relaisstellwerk der Strecke im Rahmen von Stuttgart 21 ohnehin zurückgebaut und durch ein Elektronisches Stellwerk ersetzt wird (Abb. 1). Die Grundvoraussetzung für ETCS Level 2 wäre damit geschaffen. Zwischenzeitlich wurde eine ETCS-Entwurfsplanung erstellt und eine begleitende Untersuchung in die Wege geleitet, die noch bis September 2018 läuft. Über die Umsetzung ist anschließend zu entscheiden.

Eine Ausrüstung mit Linienzugbeeinflussung (LZB), wie sie seit 2004 auf der S-Bahn-Stammstrecke München im Hochleistungsbetrieb eingesetzt wird, wurde seit den späten 1990er Jahren wiederholt vorgeschlagen. Diese Überlegungen wurden nicht mehr weiterverfolgt, da die LZB durch die Industrie abgekündigt ist, bis ca. 2030 ohnehin durch ETCS abgelöst werden soll und im Zuge von Stuttgart 21 ohnehin weite Teile des Knotens auch mit ETCS (neben Ks/PZB) ausgerüstet werden. Nicht zuletzt lässt ETCS Level 2 bei genauerer Betrachtung mehr Potentialansätze für die Verbesserung von Betriebsqualität und Leistungsfähigkeit erkennen.

Wie weit reicht also das Potential smarter Infrastruktur?

[1] Peter.Reinhart@deutschebahn.com

[2] Sven.Wanstrath@deutschebahn.com

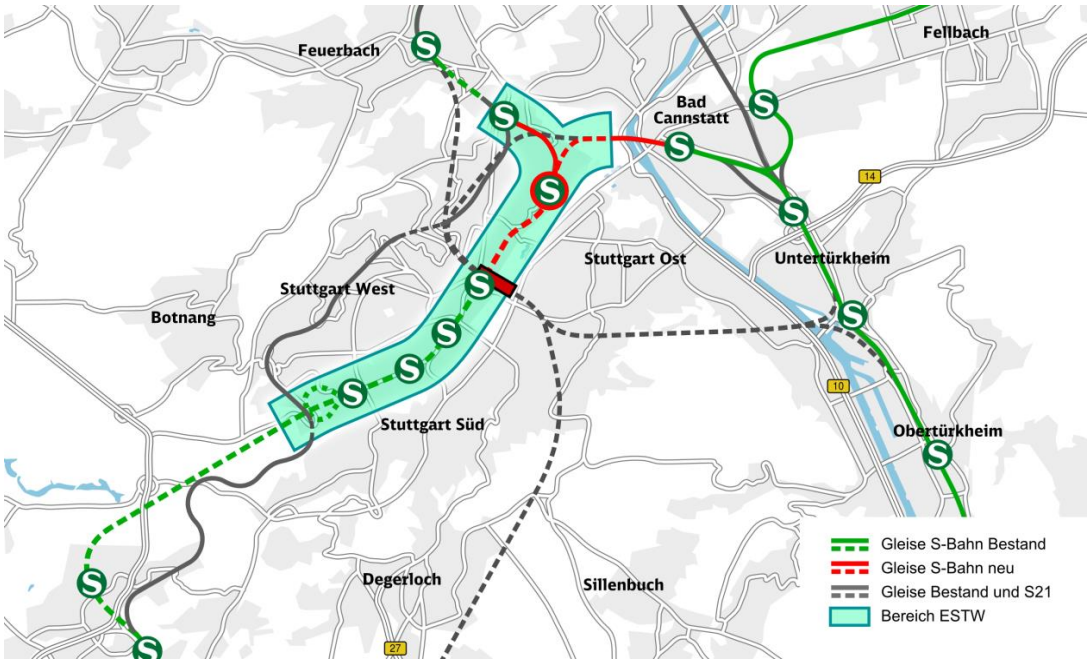

Abb. 1 Erweiterte S-Bahn-Stammstrecke, mit neuer Station Mittnachtstraße und ESTW-Bereich

2 Typischer Betriebsablauf

Um ein System zu optimieren, ist es unabdingbar, die tatsächlichen betrieblichen Abläufe zu beobachten und zu analysieren. Maßgebend für die Leistungsfähigkeit des Gesamtsystems der S-Bahn-Stammstrecke ist die Zugfolge im Bereich der Stationen, wo Züge regelmäßig halten.

Der planmäßige Betriebsablauf in konventioneller Leit- und Sicherungstechnik lässt sich in vier Phasen unterteilen und für Langzüge vereinfacht wie folgt beschreiben:

- 30 s Halt am Bahnsteig (planmäßig, in der Praxis meist länger)
- 22+3s Räumung des Bahnsteigs+Durchrutschweg[3] (annähernd konstante Beschleunigung mit 1 m/s² auf 60 km/h)
- ca. 45s Annäherung des nachfolgenden Zuges (Fahrstraßenbilde- und -auflösezeiten, Sichtzeit zum Vorsignal, Fahrt bis zum Bahnsteiganfang mit 60 km/h)
- ca. 30s Zielbremsung entlang des Bahnsteigs, mit einer gemessenen mittleren Bremsverzögerung von rund 0,6 m/s².

Der räumliche Mindestabstand zweier unbehindert fahrender Züge, wie er in der Fahrplankonstruktion zu Grunde gelegt wird, beträgt dabei nicht weniger als einen Kilometer (Abb. 2).

[3] Vereinfachend wird der Begriff „Durchrutschweg" für die Schutzstrecke hinter Hauptsignalen/Blockkennzeichen verwendet, auch wenn im Einzelfall „Gefahrpunktabstand" gemeint ist.

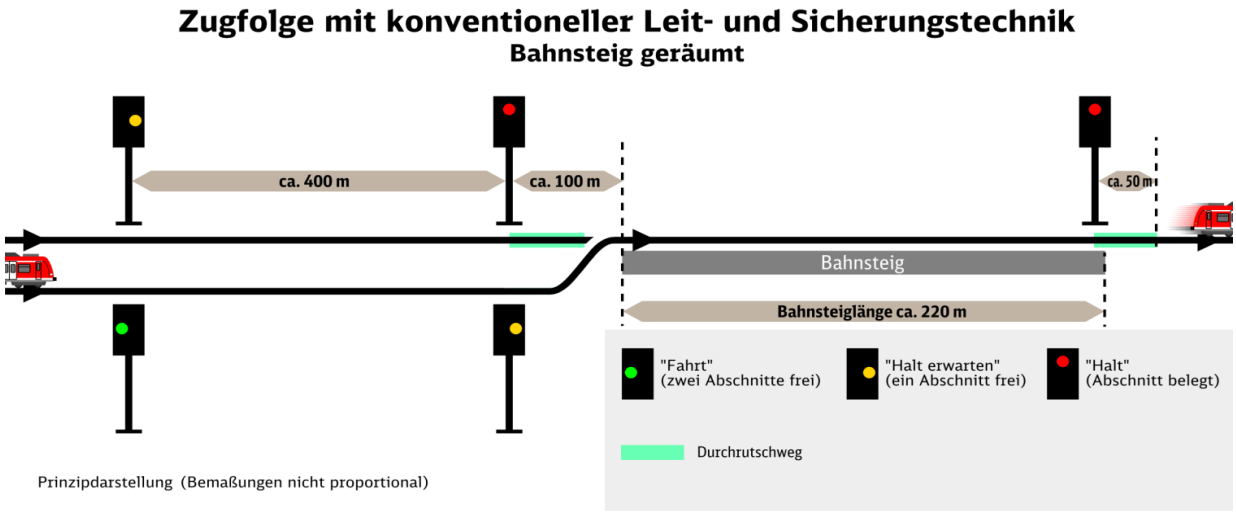

Abb. 2 Mindestabstand zweier unbehindert fahrender Züge in konventioneller Leit- und Sicherungstechnik

3 Potentiale

Angesichts von Kosten von mehr als 200 Mio. Euro je Kilometer, die mit dem Bau neuer S-Bahn-Strecken in dichtbesiedelten Ballungsräumen einhergehen, rückt eine effizientere Nutzung bestehender Nahverkehrsinfrastruktur mit ETCS zunehmend in den Fokus. Teilweise werden Mindestzugfolgezeiten von 60 bis 90 Sekunden als Ziel genannt. [1]

Bei der Victoria Line, einer U-Bahn-Linie in London, werden – mit einem CBTC-System – bereits seit 2017 planmäßig 36 Züge pro Stunde mit 40 Sekunden Halte- und 10 Sekunden Pufferzeit gefahren. Auf der Thameslink-Stammstrecke in London wurde im März 2018 mit dem Hochlauf von ETCS Level 2 und ATO im Fahrgastbetrieb begonnen – bei nicht optimalen Randbedingungen sollen ab Ende 2019 24 Züge pro Stunde und Richtung bei 45 Sekunden Planhaltezeit und wenigstens 15 Sekunden Pufferzeit gefahren werden. Unter geringeren Leistungsanforderungen fahren S-Bahnen mit ETCS u. a. bereits am Genfer See, Danzig, und Madrid.

Wesentliche Potentialansätze zur Verkürzung der Mindestzugfolgezeit liegen insbesondere in der Blockteilung, den Laufzeiten, dem Bremsmodell, dem Beschleunigungs- und Bremsvermögen sowie im automatisierten, vorausschauenden Fahren.

Wie viel Leistungsfähigkeit und Betriebsqualität lässt ein unter diesen Gesichtspunkten durchoptimiertes S-Bahn-System mit ETCS Level 2 also erwarten? Um sich dieser Frage zu nähern, bietet es sich an, das „optimale System“ zunächst vom Ende zu Ende zu denken. Was wäre, wenn

- die laufenden Positions- und Geschwindigkeitsdaten eines nach Halt abfahrenden Zuges genutzt werden, um den nachfolgenden Zug optimal – knapp unter seiner Zwangsbremseinsatzkurve – nachzuführen, wobei exakte Erwartungen an die Freimeldung einzelner Gleisfreimeldeabschnitte bestünden?
- die Reaktionszeit der Leit- und Sicherungstechnik null wäre?
- keine Durchrutschwege erforderlich wären?

- im automatisierten Betrieb mit Triebfahrzeugführer (ATO GoA 2) genauso straff an den Bahnsteig herangebremst wie beschleunigt werden könnte (1 m/s²)?

Wenn der notwendige Schnellbremsweg des nachfolgenden Zuges ungefähr der Bahnsteiglänge entspricht, ergäbe sich der in Abb. 2 dargestellte Betriebsablauf. Nach 30-sekündigem Halt und 22-sekündiger Räumung würde die Zielbremsung am Bahnsteig weitere 22 Sekunden in Anspruch nehmen. Eine Mindestzugfolgezeit von 1 ¼ Minuten wäre die Folge – eine Minute kürzer als mit konventioneller Leit- und Sicherungstechnik.

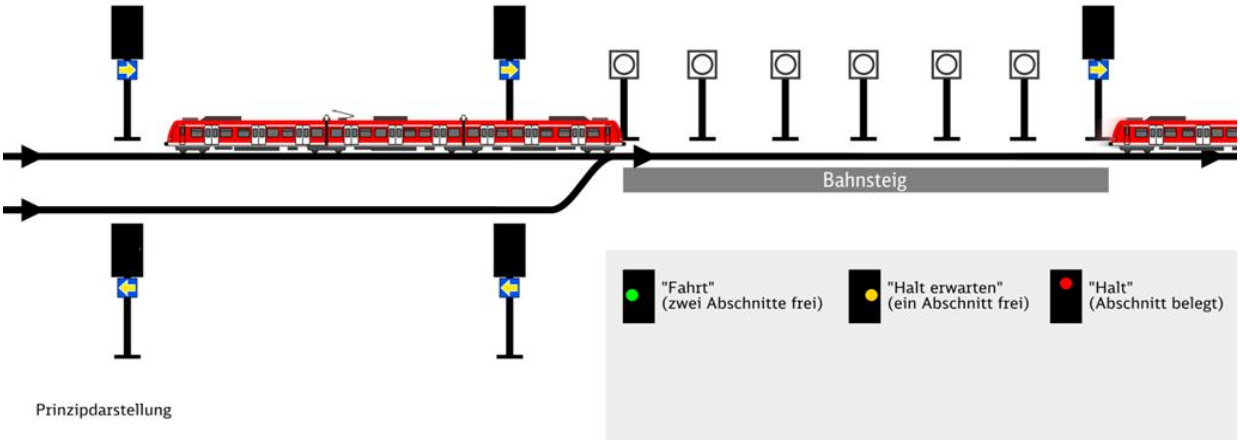

Abb. 3 Mindestabstand zweier unbehindert fahrender Züge im „optimalen System“ (Gedankenmodell)

Dieses *theoretische* Gedankenmodell lässt sich technisch offensichtlich nicht ohne weiteres in die Praxis umsetzen, beispielsweise aufgrund notwendiger Laufzeiten. In der Praxis wären Abstand und Zugfolgezeit entsprechend größer. Doch wie weit reicht das tatsächliche Potential von ETCS in einem durchoptimierten System bei homogenem Betrieb *unter Praxisbedingungen*?

Dazu bietet es sich an, fünf Optimierungslinien genauer zu betrachten:

3.1 Hochleistungsblock

Weit verbreitet ist die Erkenntnis, dass die Bildung nahezu beliebig kurzer Zugfolgeabschnitte (Hochleistungsblock) maßgeblich zu erheblichen Leistungs- bzw. Qualitätssteigerungen führen kann. Auf der S-Bahn-Stammstrecke München trägt die Teilung des Bahnsteigbereichs in vier Teilblöcke (Abb. 4) maßgeblich zur Erfüllung der hohen Leistungsanforderungen bei.

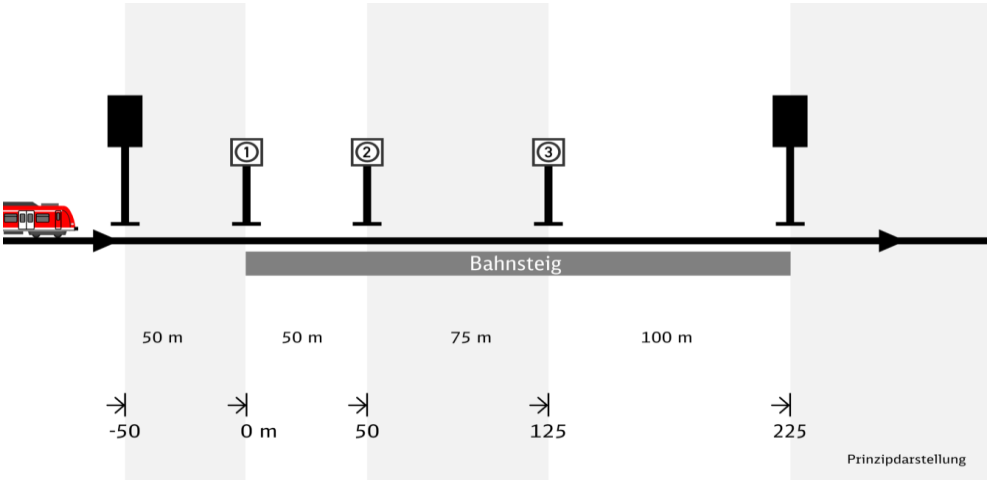

Abb. 4 Typische Bahnsteig-Blockteilung auf der S-Bahn-Stammstrecke München

ETCS kann grundsätzlich ebenfalls mit sehr kurzen Zugfolgeabschnitten und Durchrutschwegen umgehen. Restriktionen können sich gleichwohl insbesondere aus der Mindestlänge von Gleisfreimeldeabschnitten sowie Verarbeitungsgeschwindigkeiten ergeben. Abseits von ATO spielen auch menschliche Auffassungsgrenzen eine Rolle.

3.2 Laufzeiten

Im Gegensatz zum erdachten „optimalen“ System benötigt die Leit- und Sicherungstechnik einen gewissen Zeitbedarf, der sich aus einem Teil für das Stellwerk und einem Teil für ETCS (Streckenzentrale + GSM-R + Fahrzeuggerät + Schnittstellen) zusammensetzt. In Betriebssimulationen der DB werden für Fahrstraßenbildung und -auflösung – ohne Weichen, ohne ETCS – insgesamt üblicherweise 8 Sekunden zu Grunde gelegt; Messungen in der Praxis an heutigen S-Bahn-Stellwerken bestätigen diese Größenordnung. Für den ETCS-Teil – von der Meldung an das RBC über die Verarbeitung, die Übermittlung der Fahrterlaubnis per GSM-R und die Verarbeitung im Fahrzeug – zeigen u. a. Beobachtungen bei Thameslink, dass diese 3-4 Sekunden umfassen, ungefähr entsprechend den beobachteten Reaktionszeiten der LZB bei der S-Bahn München.

Für die Gesamtlaufzeit – vom Freifahren der Fahrstraßenzugsschlussstelle bis zur verarbeiteten Fahrterlaubnis auf dem folgenden Zug – sind beispielsweise in der Schweiz Ende-zu-Ende-Laufzeiten von etwa acht Sekunden dokumentiert. Diese Beispiele lassen sich nicht ohne weiteres auf die Bedingungen in Deutschland übertragen.

Optimierungsansätze liegen insbesondere im Stellwerk und beim Funk: Muss beispielsweise für das Nachrücken am Bahnsteig stets ein (zyklischer) Stellanstoß für jede Teilfahrstraße abgewartet werden oder könnte dies durch einen Selbststellbetrieb beschleunigt werden? Potentiale ergeben sich zudem aus technischer Weiterentwicklung, auch dem GSM-R-Nachfolgesystem (FRMCS).

3.3 Automatisierter Bahnbetrieb (ATO), vorausschauendes Fahren

Ein wesentlicher Schlüssel zur Leistungssteigerung liegt im automatisierten Bahnbetrieb mit Triebfahrzeugführer (ATO GoA 2), wie er bereits auf der Thameslink-Stammstrecke in London zur Anwendung kommt. Allein durch ein Fahren knapp unterhalb der Zwangsbremseinsatzkurve (EBI) können gegenüber

konventioneller, an der Indication-Bremskurve orientierter Betriebsführung bis zu rund 12 Sekunden Zugfolgezeit eingespart werden.

Ein weiterer wichtiger Schlüssel zur Optimierung liegt dabei im Fahren mit genauen Erwartungen an die Freimeldung nachfolgender Abschnitte, wozu auch Positions- und Geschwindigkeitsdaten vorausfahrender Züge in einem Verkehrsleitsystem (TMS) verarbeitet werden können. Theoretisch können mit ATO, ETCS und TMS nachfolgende Züge – in Abhängigkeit von der tatsächlichen Haltezeit des vorausfahrenden Zuges – stets optimal an den Bahnsteig herangeführt werden. Der Praxisbeweis steht gleichwohl noch aus.

Während im konventionellen Betrieb eine möglichst dichte Teilung am Bahnsteiganfang geboten ist – im Extremfall sollen vor dem Bahnsteiganfang stehende Züge so schnell wie möglich mit dem Nachrücken beginnen können –, kommen mit ATO/ETCS/TMS für die Optimierung der Leistungsfähigkeit kritische Punkte in den Fokus. An diesen Punkten ist die Geschwindigkeit der beiden Züge kurzzeitig gleich, der Abstand zwischen dem räumenden und dem nachfolgenden Zug minimal, eine besonders dichte Blockteilung in diesem Bereich damit geboten. Im Vergleich zum „manuellen“ Betrieb verschiebt sich der maßgebende Punkt – in Abhängigkeit vom Beschleunigungs- und Bremsvermögen der Fahrzeuge – beispielsweise in die Bahnsteigmitte (Abb. 5). Vor dem kritischen Punkt ist der Abstand – zum vorausfahrenden Zug und zur Zwangsbremskurve – noch nicht minimal. Nach dem kritischen Punkt nimmt der Abstand zwischen den beiden Zügen wieder zu, während der nachfolgende Zug mit der Zielbremsung zum Bahnsteig beginnt, sodass in beiden Bereichen auf eine sehr enge Blockteilung verzichtet werden kann.

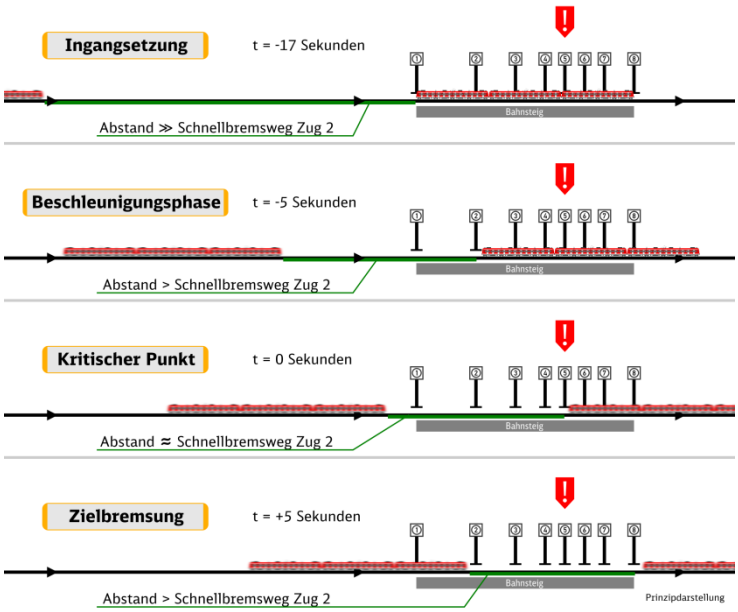

Abb. 5 Betriebsablauf und Abschnittsteilung bei automatisiertem, vorausschauendem Fahren, fokussiert auf einen kritischen Punkt (Prinzipdarstellung!)

Zusätzlich eröffnet ATO den Weg für planbar straffere, aber harmonische Betriebsbremsungen. Würde beispielsweise mit der größtmöglichen Betriebsbremsverzögerung der heutigen Fahrzeuge (rund 1 m/s²) statt der heute im Mittel gemessenen rund 0,6 m/s² gebremst werden, wäre eine weitere Verkürzung der Mindestzugfolgezeit um mehr als eine Zehntelminute die Folge.

3.4 Bremsmodell

Weitere Potentialansätze liegen auch im Bremsmodell selbst. ETCS (Baseline 3) bietet dabei neben dem klassischen Bremshundertstel-Modell (Lambda-Modell) für Triebzüge die Möglichkeit einer feineren Modellierung mittels Gamma-Modell: Eine in Bremsversuchen ermittelte und nach Geschwindigkeitsstufen differenzierbare Schnellbrems-Momentanverzögerung (z. B. 1,0 m/s² bis 60 km/h) wird dabei mit einem Sicherheitsfaktor (k_dry) multipliziert. Dieser auf dem Fahrzeug hinterlegte Faktor bildet die Wahrscheinlichkeit ab, dass aufgrund von Versagen einzelner Komponenten der sichere Bremsweg überschritten wird. Er wird anhand eines von der Strecke an das Fahrzeug übermittelten Konfidenzlevels ausgewählt. Je größer die von der Strecke geforderte Bremswegsicherheit (in Deutschland 99,9999 %), desto kleiner k_dry und desto geringer die zulässige Verzögerung, womit sich Bremsweg und damit die Mindestzugfolgezeit verlängern.

Daraus ergeben sich mehrere Potentialansätze, beispielsweise:

- „Bessere“ Bremsverzögerungen durch gezielte Bremsversuche aus den auf der Stammstrecke üblichen Bremsausgangsgeschwindigkeiten von 60 bzw. 80 km/h, an Stelle einer einheitlichen Verzögerung aus 120 oder 140 km/h.
- Differenzierung des Sicherheitsfaktors k_dry nach Zuglänge: Der seltene Ausfall einzelner Komponenten kann auf einem Langzug offensichtlich besser abgefedert werden als auf einem Kurzzug. Bessere k_dry-Werte für die – betrieblich besonders kritischen – Langzüge könnten die Folge sein.
- Differenzierung des Konfidenzlevels nach Betriebsfällen: Für Folgefahrten könnte ein anderes Sicherheitsziel gelten als für drohende Flanken- und Gegenfahrten. Ein niedrigerer Konfidenzlevel führt zu größerem k_dry und verkürzt wiederum Bremswege und Mindestzugfolgezeiten.

Darüber hinaus bestehen Potentialansätze in dem spezifizierten ETCS-Bremsmodell selbst, das für die gesamte Zuglänge das größte Gefälle selbst dann ansetzt, wenn nur ein kleiner Teil des Zuges darinsteht. Liegt vor einem ebenen Bahnsteig ein erhebliches Gefälle, können sich dadurch Bremswege und letztlich Mindestzugfolgezeiten um mehrere Sekunden verlängern. Eine entsprechende Weiterentwicklung der ETCS-Spezifikation ist geplant („Game Changer“-Bremskurven).

3.5 Optimierungen an Fahrzeugen

Nicht zuletzt bestehen weitere Potentialansätze im Bereich der Fahrzeuge.

Eine Beschleunigung mit beispielsweise 1,2 statt 1 m/s² hätte eine rund 3 Sekunden frühere Räumung des Bahnsteigs zur Folge, eine Schnellbremsverzögerung von 2 statt 1 m/s² würde eine um eine Zehntelminute dichteres Nachfahren ermöglichen. Eine weitere Erhöhung der Betriebsbremsverzögerung könnte die Zielbremsphase verkürzen und damit zu einem noch früheren Beginn des Fahrgastwechsels führen.

Während bei Straßen- und Stadtbahnen solche Werte längst üblich sind, stellt sich im Kern die Frage: Was ist einem S-Bahn-Fahrgast eigentlich zuzumuten?

4 Schluss

Der Nutzen von ETCS reicht über eine Erhöhung der Leistungsfähigkeit bzw. eine Verbesserung der Betriebsqualität hinaus. So wurden und werden international Lichtsignale an ETCS-Strecken zurückgebaut, da sich ETCS gegenüber der konventionellen Signalisierung als robuster erwiesen hat – bei neuen Strecken werden vielfach gar keine Lichtsignale mehr aufgebaut. Ebenfalls eröffnet die genaue Kenntnis von Standort und Geschwindigkeit von Zügen die Möglichkeit, Kundeninformation sehr viel präziser als heute zu gestalten.

In Diskussionen wird dabei häufig gegen die Nutzung von ETCS Level 2 eingewandt, die Funkkanalkapazität sei nicht ausreichend, die Übertragung störanfällig oder nicht ausreichend robust. Dabei bieten gerade unterirdische Strecken insgesamt hervorragende Rahmenbedingungen für eine qualitativ hochwertige Funkversorgung. Auf und im Umfeld der Stammstrecke Stuttgart besteht dabei schon heute in weiten Teilen eine Versorgung durch mehrere Funkzellen (Abb. 6), mit weitgehend deutlich über den Anforderungen liegenden Pegeln.

Schließlich wird eingewandt, die Unterteilung des Bahnsteigs in viele Gleisfreimeldeabschnitte sei übertrieben, im Übrigen der Einsatz von ETCS Level 3 – mit einem Verzicht auf streckenseitige Gleisfreimeldung – das Mittel der Wahl. Ungeachtet der fehlenden Serienreife wird dabei vergessen, dass die Laufzeit einer solchen virtuellen Gleisfreimeldung – von der zyklischen Integritätsmeldung des Fahrzeugs, dem zyklischen Position Report, der Übertragung per GSM-R, der Verarbeitung im RBC und der Verarbeitung im Stellwerk – wesentlich länger als bei konventionellen Achszählsystemen ist. Die aufgrund von Ortungseffekten gegenüber der physischen Zuglänge größere virtuelle Zuglänge trägt ein Übriges zu einer späteren Gleisfreimeldung bei. Besonders kurze Gleisfreimeldeabschnitte sind in einem optimierten System dabei nur an einigen wenigen kritischen Punkten erforderlich, beispielsweise an Weichen und in Bereichen, in denen der vorausfahrende Zug noch langsam anfährt (z. B. am Bahnsteiganfang).

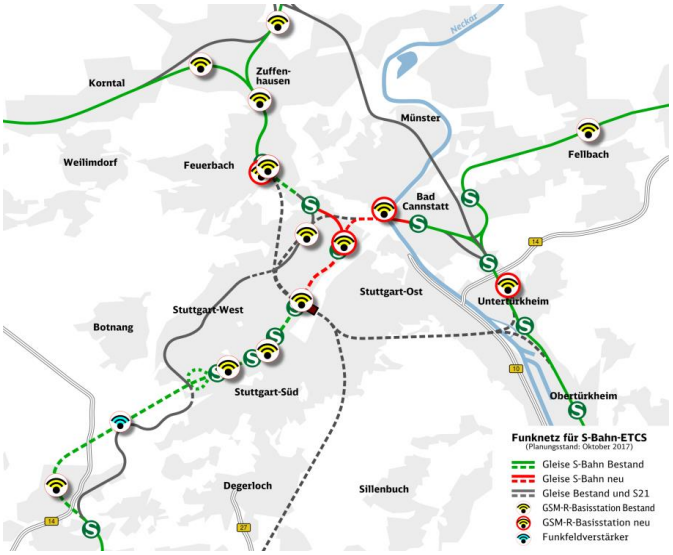

Abb. 6 Funknetz für S-Bahn-ETCS (Bestand & geplanter Neubau, Stand Oktober 2017)

Weltweit wird die Zahl der ETCS-Projekte, die unter sehr hohen Leistungsanforderungen betrieben werden, in den kommenden Jahren wachsen. Dazu zählen neben Thameslink beispielsweise S-Bahn-ETCS-Stammstrecken in Brisbane, Brüssel, Sydney und Wien, die italienischen Großknoten Florenz, Mailand und Rom, aber auch die Lötschberg- und Gotthard-Basistunnel sowie die NBS Mattstetten—Rothrist. Auch in dem im Rahmen von

Stuttgart 21 entstehenden neuen Fern- und Regionalverkehrsknoten leistet ETCS einen wesentlichen Beitrag für mehr Leistungsfähigkeit und Betriebsqualität. Wurde ETCS bislang vor allen Dingen unter dem Gesichtspunkt der Interoperabilität gedacht, zeigen sich bei genauerer Betrachtung eine Reihe von möglichen Hebeln für Kapazität und Qualität.

Die Suche und Fundierung von Potentialansätzen geht weiter. Die Jagd nach jeder Sekunde – sie hat gerade erst begonnen!

5 Literaturverzeichnis

[1] Uwe Arnecke, Kay (2018): *Für mehr Intelligenz in der Infrastruktur*, in *Der Nahverkehr* 1+2/2018, Düsseldorf.

Alle Grafiken: DB PSU

Modellierung des Steuerungsprozesses der Rückfallebenen im Schienenverkehr als Grundlage für die Automatisierung

M.Sc. Bilal Üyümez

Technische Universität Darmstadt

Institut für Bahnsysteme und Bahntechnik

1 Einleitung

Im Zuge der Digitalisierung und getrieben durch die Entwicklungen im Straßenverkehr dreht sich im Schienenverkehr seit längerer Zeit alles um Automatisierung und Vernetzung. Die Besonderheit des Schienenverkehrs gegenüber dem Straßenverkehr liegt darin, dass er aufgrund der Spurführung ein wesentlich automatisierungsfreundlicheres System ist. So existieren z.B. im Metro-Bereich bereits automatisierte, fahrerlose Systeme. Um von dem ökologischen und ökonomischen Nutzen des automatisierten Fahrens auch bei Nah- und Fernverkehr zu profitieren, werden Forschungen und Entwicklungen in dieser Hinsicht betrieben. Die technische Machbarkeit des automatisierten Schienenverkehrs ist durch den bewährten Einsatz im Metro-Bereich in wesentlichen Zügen nachgewiesen. Die große Herausforderung ist nun, neue Betriebsverfahren zu entwickeln, damit das automatisierte Fahren auf der komplexen Infrastruktur der Vollbahnen möglich wird.

Der sichere Bahnbetrieb stützt sich auf die drei Säulen Mensch, Regelwerke und Technik. Regelwerke leisten einen Beitrag zum Erhalt des hohen Sicherheitsstandards und beschreiben u.a. das komplexe Zusammenspiel von Mensch und Technik. In diesem gehört zur Komponente „Mensch“ das Betriebspersonal, genauer der Fahrdienstleiter, der Disponent und der Triebfahrzeugführer. Der Fahrdienstleiter ist für die sichere Durchführung von Zugfahrten zuständig, während der Triebfahrzeugführer den Zug fährt. Neben der Steuerung hat der Triebfahrzeugführer auch die Aufgabe, den Fahrweg zu beobachten und bei gefahrdrohenden Situationen entsprechend in seiner Verantwortung zu handeln. Der Disponent überwacht den Betrieb und greift bei kleineren und größeren Störungen in den Betriebsablauf ein, um ggf. auftretende Fahrplanabweichungen möglichst gering zu halten. Treten Störungen auf, so agieren die genannten Akteure im Betrieb alleinig in ihrer Verantwortung und halten den Betrieb mit verminderter Betriebsqualität durch Anwendung von Ersatzverfahren aufrecht. Dieser Prozess wird als Rückfallebene bezeichnet.

Bei der Entwicklung eines automatisierten, fahrerlosen Systems (Automatic Train Operation, ATO), das die vorher manuell durchgeführten Aktionen des Triebfahrzeugführers automatisch ausführen soll, ist es notwendig, das Verhalten des Triebfahrzeugführers sowohl im Regelbetrieb als auch in der Rückfallebene vollständig abzubilden. Die Gestaltung von Rückfallebenen, die eine Teilmenge des Betriebs darstellen, stellt hierbei die größte Herausforderung dar, da diese heute schon die „Hohe Schule“ beim Design der Regelwerke und Betriebsverfahren eines Bahnsystems darstellt (vgl. in [1]). In diesem Zusammenhang beschäftigt sich das Institut für Bahnsysteme und Bahntechnik der TU Darmstadt im Rahmen der gemeinsamen Innovationsallianz mit der Deutschen Bahn AG im Projekt „Automatisiertes, fahrerloses Fahren bei Abweichungen vom Regelbetrieb“ mit der Entwicklung von Lösungsansätzen für ein automatisiertes, fahrerloses Fahren in der Rückfallebene. Das Projekt ist Bestandteil der Arbeitsgruppe Signalling, in deren Rahmen in einem interdisziplinären Team an verschiedenen Herausforderungen der digitalen Leit- und Sicherungstechnik gearbeitet wird.

In diesem Artikel wird der gegenwärtige Steuerungsprozess der Rückfallebenen allgemeingültig modelliert. Das generische Modell soll die Grundlage dafür bilden, die funktionale Architektur für das ATO-System abzuleiten und in Zukunft neue Betriebsverfahren für die Rückfallebenen im ATO-Betrieb zu konzipieren.

2 Modellierung des heutigen Steuerungsprozesses der Rückfallebenen im Bahnbetrieb

Ziel der Modellbildung ist die Erstellung eines vereinfachten Abbildes der Realität durch Formulierungen geeigneter Größen und ihrer Zusammenhänge. Abgesehen von Bauarbeiten und Langsamfahrstellen sind die Ursachen für die Störungsereignisse im Betrieb vielfältig und nicht deterministisch. Für die allgemeine Einteilung der Ursachen wird auf [6] verwiesen.

Der Prozess der Rückfallebene hingegen ist in Abhängigkeit des Störungsereignisses durch verbindlich definierte Verfahrensregeln geprägt (vgl. in [2]). Das Interesse der Modellbildung in dieser Arbeit liegt daher auf der allgemeingültigen Beschreibung der logischen Ablauffolgen von Funktionen innerhalb des Prozesses.

2.1 Vorgehen bei der Erstellung des Modells

Die Modellbildung ist ein strukturierter Prozess aufeinander folgender Phasen. Der Entwicklung des Modells geht in einer ersten Phase eine Prozessanalyse voraus. Ausgangspunkt der ersten Phase ist eine Analyse der heutigen natürlich-sprachlich formulierten Rückfallebenen. Die Analyse erfolgt in drei Schritten.

Der erste Schritt umfasst die Erfassung von den bisher aufgetretenen Störungsfällen im Eisenbahnbetrieb in Deutschland. Hierfür werden die Richtlinien (Ril) 408, 418 und 420 der Deutschen Bahn AG als Datengrundlage herangezogen. Nach der Datenerhebung werden im nächsten Schritt mithilfe der selben Quellen die zugehörigen Rückfallebenen identifiziert und alle Aktionen innerhalb dieser Rückfallebenen ausgearbeitet. Hierbei werden aus den natürlich-sprachlich formulierten Abläufen die Aktionen und die zugehörigen verantwortlichen Akteure extrahiert. Im letzten Schritt werden die Verantwortlichkeiten der Akteure zusammen mit den Störungsereignissen in tabellarischer Form dargestellt. Für eine klare Darstellung der Ablauffolgen werden die ausgearbeiteten Aktionen sequentiell zusammengefasst. In der Tabelle 1 ist ein Ausschnitt aus der erstellten Störungsmatrix zu sehen.

Tab. 1 Ausschnitt aus der erstellten Störungsmatrix

Störungsart	1. Aktion	2. Aktion	3. Aktion	4. Aktion	5. Aktion
Hauptsignal gestört	Sofort am gestörten Signal anhalten	Die Situation dem Fahrdienstleiter melden	Befehl 2 zur Weiterfahrt erteilen	Befehlsvordruck ausfüllen	Weiterfahrt mit Befehl 2

Legende: Die rot markierten Zellen sind die Aktionen des Triebfahrzeugführers, während die grün markierte Zelle die Aktion des Fahrdienstleiters enthält. Die Gelbe Zelle enthält eine Aktion, die von beiden Akteuren ausgeführt wird

In der zweiten Phase werden die identifizierten Aktionen der Betriebskonstituenten analysiert und nach dem Ansatz des menschlichen Informationsverarbeitungsmodells (engl. Human Information Processing Model) (vgl. in [9]) zu logisch zusammenhängenden Funktionsblöcke aggregiert und zu einer Prozesskette verschaltet.

2.2 Generisches Modell der heutigen Rückfallebenen als Funktionsflussdiagramm

Der operative Bahnbetrieb lässt sich in drei Zustände unterteilen. Der erste Zustand ist der Regelbetrieb, bei dem der Transportprozess reibungslos stattfindet. Tritt eine Störung ein, die sich betriebshemmend auswirkt, so wechselt der Regelbetrieb in den Störungszustand. Diese vorliegende Störungssituation wird von entsprechendem Betriebspersonal wahrgenommen und es wird adäquat drauf reagiert. Im anschließenden Rückfallebenenzustand werden Maßnahmen und Handlungsweisen festgelegt. Dies geschieht heute durch Zuhilfenahme von Regelwerken. Die festgelegte Handlungsweise wird dann im letzten Schritt ausgeführt.

Diese Prozessschritte, die in logischer Abfolge durch die Betriebskonstituenten abgearbeitet werden, können als Funktionsflussdiagramm modelliert werden. Das Funktionsflussdiagramm (engl. Functional Flow Block Diagram, FFBD) ist ein sehr bekanntes Werkzeug des Systemingenieurs. Der Zweck des Funktionsflussdiagramms ist es, die Ablauflogik eines Prozesses durch Konzentration auf die wesentlichen Elemente transparent zu beschreiben. Es wird ebenfalls zur Definition von Systemanforderungen in funktionaler Hinsicht eingesetzt (vgl. in [8]). Die Grundelemente des FFBD sind Funktionsblöcke, deren Verbindungspfeile mit Verbindungsrichtung und die logischen Verknüpfungen *UND, ODER und XOR (Exklusiv Oder)*. Funktionen stellen Aktivitäten dar und können auf verschiedenen Detaillierungsstufen beschrieben werden, weshalb eine entsprechende Nummerierung der Funktionsblöcke vorgesehen ist. Die Modellierung des Steuerungsprozesses der Rückfallebenen erfolgt in diesem Beitrag auf dem Top- Level. Das bedeutet, dass jeder Funktionsblock in weitere Subfunktionen unterteilt werden kann, bis die elementare Funktion erreicht ist. Durch die logischen Verknüpfungsoperatoren wird beschrieben, wie Funktionen miteinander verknüpft werden.

Die UND- Verknüpfung beschreibt eine parallele Ausführung von Funktionen und setzt voraus, dass alle Bedingungen in dem Pfad erfüllt sein müssen, damit der Prozess fortgesetzt werden kann. Die ODER-Verknüpfung wird verwendet, um anzuzeigen, dass auch eine Funktion im alternativen Pfad zum Fortfahren des Prozesses genügt. Die XOR-Verknüpfung beschreibt, dass nur eines der verknüpften Ereignisse eintreten darf, um die über das XOR verbundene Funktion auszulösen.

An dieser Stelle ist anzumerken, dass aufgrund des Ergebnisses der Prozessanalyse die Sequenzierung der Aktivitäten innerhalb des Prozesses ausschließlich in ODER-Verknüpfung abgebildet wird. Die aus der Prozessanalyse hergeleiteten logischen Funktionsblöcke werden in der nachfolgenden Tabelle festgehalten und die modellierte Prozesskette wird in der Abbildung 1 dargestellt.

Tab. 2 Elemente des Funktionsflussdiagramms für den Rückfallebenenprozess

Funktionsnummer	Funktionsblock
1.1	Wahrnehmung
1.2	Störungsoffenbarung
1.3	Sicheren Zustand erreichen
1.4	Maßnahme und Handlungsweise festgelegen
1.5	Kommunikationsaufbau
1.6	Handlung ausführen

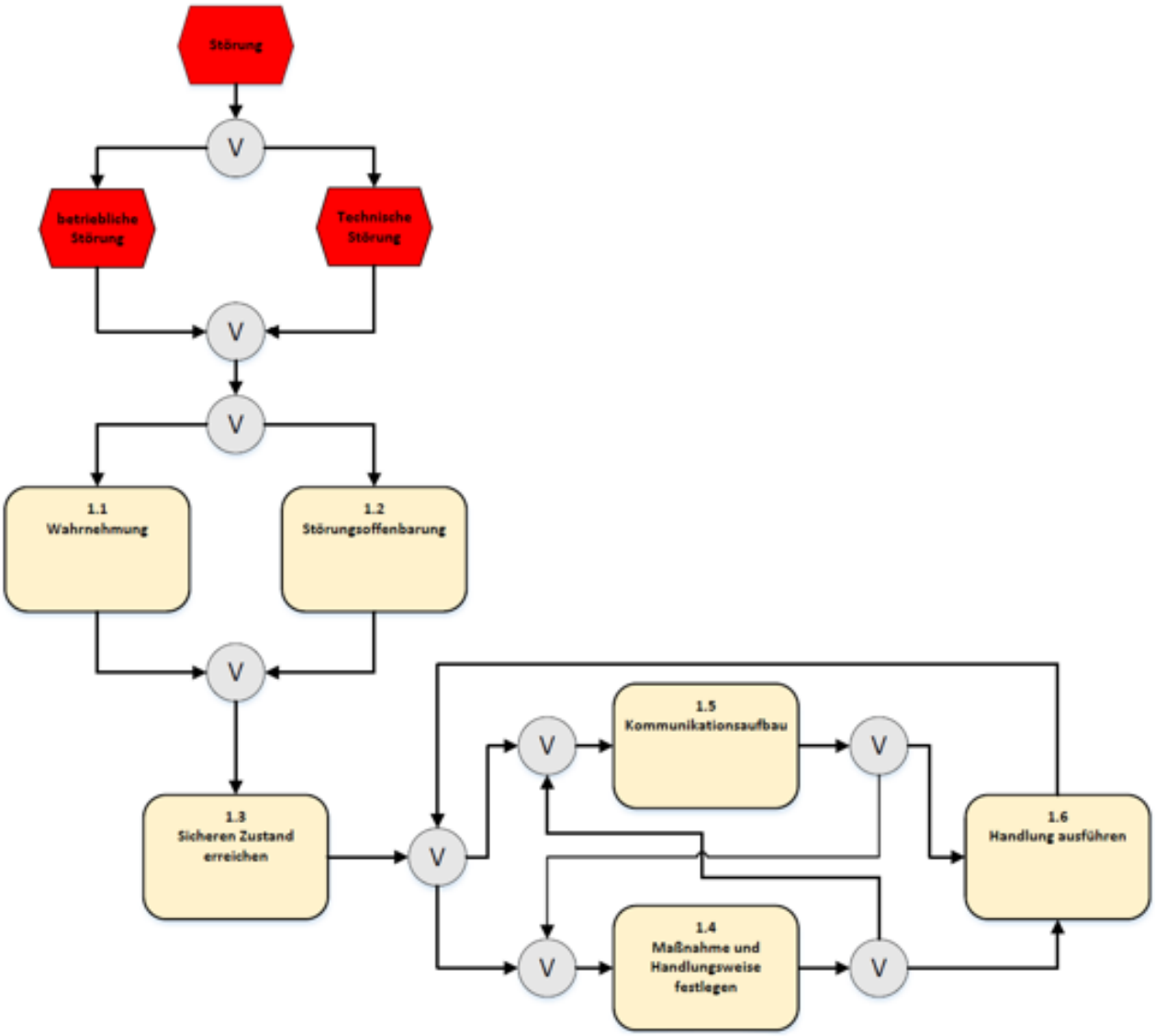

Abb. 1 generisches Funktionsflussdiagramm für die Steuerung der Rückfallebenen

Aus der Abbildung 1 ist ersichtlich, dass die Prozesskette durch ein Störungsereignis angestoßen wird. Dabei ist es möglich, dass entweder eine technische Störung, eine betriebliche Störung oder eine Kombination aus beidem vorliegen kann. Hierbei ist anzumerken, dass in dieser Arbeit die naturbedingten Störungen der Kategorie betriebliche Störungen zugeordnet sind.

Die vorliegende Störung wird entweder durch ein Betriebspersonal (Triebfahrzeugführer) wahrgenommen, welche durch den Funktionsblock 1.1 abgebildet wird, oder es erfolgt eine automatische Störungsoffenbarung durch das ausgefallene System selbst (Funktionsblock 1.2). Letztere leitet sich aus der Norm EN 50129 ab. Diese Norm besagt, dass sicherheitsrelevante Systeme nach dem Fail-Safe-Prinzip entworfen werden müssen, das heißt, dass bei Eintreten einer Fehlfunktion diese innerhalb einer genügend kurzen Zeit offenbart werden und ein sicherer Zustand eingenommen und beibehalten werden muss (vgl. in [5]). Diese Sequenzierung wird beim Vorliegen von technischen Störungen durchlaufen. Bei betrieblichen Störungen wie zum Beispiel einer Fehlleitung, wird der Zug manuell durch den Triebfahrzeugführer sofort angehalten, also zum sicheren

Zustand überführt. Dies ist im Funktionsflussdiagramm durch die Sequenzierung der Funktionen 1.1 und 1.3 dargestellt.

Erreicht das System den sicheren Zustand, so erfolgt daraufhin eine Entscheidungsfindungsphase, die den Kern des Prozesses darstellt und auf interpersoneller Kommunikation und auf der Planungsfähigkeit des Menschen basiert. In dieser Phase werden Maßnahmen und Handlungsweisen ausgewählt, die am besten zur aktuellen Situation passen. Das wird in dem Modell durch die Funktion 1.4 (Maßnahme und Handlungsweise festlegen) abgebildet. Der Funktionsblock 1.5 (Kommunikationsaufbau) ist notwendig, da jede Störung, die Auswirkungen auf den Betrieb hat, dem vorgesehenen Betriebspersonal kommuniziert werden muss. Nach Ausführung der Funktion 1.3 sind unterschiedliche Abfolgen möglich, um den Kern des Prozesses abzuarbeiten und eine anschließende Handlung auszuführen. Diese möglichen Abfolgen sind wie folgt:

1. mögliche Abfolge: Kommunikation mit dem entsprechenden Betriebspersonal aufbauen, danach gemeinsam eine zu der Situation passende Maßnahme und Handlungsweise planen und diese im letzten Schritt ausführen.

2. mögliche Abfolge: eine zu der Situation passende erste Maßnahme und Handlungsweise planen, diese ausführen (z.B. Abschalten eines Systems im Fahrzeug), dann die Situation dem entsprechenden Betriebspersonal melden, danach gemeinsam weitere gegebenenfalls notwendige Maßnahmen und Handlungsweisen planen und diese im letzten Schritt ausführen.

3. mögliche Abfolge: eine zu der Situation passende erste Maßnahme und Handlungsweise planen, diese dann dem entsprechenden Betriebspersonal melden, danach gemeinsam weitere gegebenenfalls notwendige Maßnahmen und Handlungsweisen festlegen und diese im letzten Schritt ausführen.

4. mögliche Abfolge: durch den ODER-Verknüpfungsoperator nach der Funktion 1.3 wird impliziert, dass die Ausführung der Funktionen 1.4 und 1.5 auch simultan erfolgen kann. Dieser Sachverhalt spiegelt die Realität mehr wieder und erfordert höchste Konzentration des entsprechenden Betriebspersonals.

Die Betrachtung der aufgeführten Abfolgen erfolgt hier aus Sicht des Triebfahrzeugführers. Diese Abfolgen gelten ebenfalls für die anderen beteiligten Betriebskonstituenten. Die mögliche Abfolge 2 ist damit zu erklären, dass der Triebfahrzeugführer, der mit betrieblichem Wissen ausgestattet ist, seine Handlungsweisen nicht jedes Mal mit einem anderen Betriebspersonal neu planen muss, sondern im Falle einer bekannten Störung auf einen vorbereiteten Plan oder ein vorbereitetes Verfahren zurückgreift und diesen ausführt. Diese vorbereiteten Verfahren sind in den Regelwerken niedergeschrieben, die er während der Fahrt mitführen muss.

3 Nutzen des entwickelten Modells bei der Entwicklung eines ATO-Systems

Modellbasierte Methoden werden immer häufiger im Entwicklungsprozess technischer Systeme eingesetzt, welche den Systementwurf unterstützen (vgl. in [7]). Das in dieser Arbeit entwickelte Modell beschreibt den Steuerungsprozess der Rückfallebenen generisch und in halbformaler Weise. Während der informalen Phase der Entwicklung wurden die beteiligten Akteure in den entsprechenden Rückfallebenen identifiziert und ihnen die Aktionen zugeordnet, für die sie verantwortlich sind. Mithilfe dieses Modells können die Aktionen aller beteiligten Betriebskonstituenten in logischen Funktionsblöcken gruppiert werden.

Für den Entwurf einer ATO- Systemarchitektur bedeutet das, dass die in dem Modell aufgeführten Funktionalitäten modularisiert werden können. Das hat den Vorteil, dass die unterschiedlichen Funktionskomponenten klar voneinander getrennt entwickelt, getestet und wieder miteinander zu einer

Gesamtsystemarchitektur verbunden werden können. Außerdem können weitere Funktionskomponente hinzugefügt und die logisch gruppierten Funktionsblöcke mit einem geeigneten Top-Down Ansatz zu Teilfunktionen oder Elementarfunktionen zerlegt werden. Ein besonderer Nutzen des Modells liegt darin, dass zukünftige Rückfallebenen- Szenarien für den automatisierten Betrieb definiert und simuliert werden können. Grundlagen für die Szenarien stellt dabei die formale Definition der Systemeingänge und erwarteten Ausgaben an entsprechenden Schnittstellen, welche durch Experten bestimmt werden können. Diese formal beschriebenen Systemeingänge und die erwarteten Ausgänge können in einem weiteren Schritt hinsichtlich der funktionalen Sicherheit nachgewiesen werden. Die Verwendung formaler Methoden werden in Normen wie z.B. der EN 50128 von Systemen mit Sicherheitsintegritätslevel (SIL) 1 und 2 empfohlen sowie für Systeme mit SIL 3 und 4 sogar dringend empfohlen (vgl. in [4] und [5]). Nicht zuletzt eignet sich das Modell auch für eine technikunabhängige Erklärung der Vorgänge in den Rückfallebenen und überwindet die Sprachbarriere zwischen Anwender und Systemingenieuren (vgl. in [3]).

4 Fazit und Ausblick

In diesem Artikel wurde der Steuerungsprozess der Rückfallebenen nach dem systemtheoretischen Ansatz modelliert. Die zu Beginn durchgeführte Prozessanalyse ergab, dass die heute eingesetzten Rückfallebenen zum einen sehr unterschiedlich sind und zum anderen auf Erfahrungen und Expertenwissen basieren. Trotz der existierenden Diversität, konnte anhand des entwickelten Modells eine generische Steuerung konzipiert werden. Basierend auf diesem Modell, können in Zukunft neue Ersatzbetriebsverfahren für den automatisierten Betrieb entworfen und vor dem realen Einsatz ausgeführt und formal verifiziert werden. Die verständliche Notation des Modells überwindet die Sprachbarriere zwischen Anwender und Systemingenieuren.

Für eine vollständige Validierung des Modells ist es notwendig, einen formalen Nachweis für die Richtigkeit des Prozesses durchzuführen. Dieses Modell wird in Zukunft für eine strukturierte Entwicklung der funktionalen Architektur des ATO-Systems eingesetzt. Dabei werden die einzelnen Funktionskomponenten weiter in Subfunktionen zerlegt und formal beschrieben.

5 Literaturverzeichnis

[1] Pachl, Jörn (2017): *„Betriebliche Randbedingungen für autonomes Fahren auf der Schiene“*, Deine Bahn, 09/2017

[2] Mühleck, Karl-Heinz; Küpper, Jonannes (2010): *Betriebliche Regeln für Triebfahrzeugführer*, Deine Bahn, 10/2010

[3] Haase. H, Volkmar (1988): *Modelle zur Spezifikation von Prozesslenkungssystemen*, Institut für Informationsverarbeitung Technische Universität Graz, Graz

[4] CENELEC EN 50128 (2012): *Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme: Software für Eisenbahnsteuerungs- und Überwachungssysteme*, Berlin

[5] CENELEC EN 50129 (2003): *Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme: Sicherheitsrelevante elektronische Systeme für Signaltechnik*, Berlin

[6] DB AG (2002): *Richtlinie 420.01 der Betriebszentralen DB Netz AG, V 420.9001 00- Kodierliste von Verspätungsursachen*, Frankfurt am Main.

[7] Friedmann Bitsch et al. (2017): *Effiziente Sicherheitsnachweisführung mithilfe modellbasierter Systemanalyse*, Signal + Draht, 06/2017

[8] Defense Acquisition University Press (2001): *Systems Engineering Fundamentals*, Virginia

[9] Skybrary (2016): *Information Processing*, auf www.skybrary.aero/index.php/Information_Processing, abgerufen am 26.02.18

The Future Use Cases of Formal Methods in Railways

Sebastian Schön[1], Eduard Kamburjan[2], Reiner Hähnle[2]

[1] Institut für Bahnsysteme und Bahntechnik TU Darmstadt

[2] Software Engineering Group TU Darmstadt

1 Abstract

Formale Methoden sind nicht einheitlich und unterschiedliche Formalismen werden an verschiedenen Stellen für unterschiedliche Zwecke in der Eisenbahnindustrie verwendet. Diese reichen von etablierten Simulationswerkzeugen über halbformale Ansätze in der Modellierung wie UML und die vollständige formale Spezifikation kritischer Komponenten in Event-B bis hin zu einheitlichen Ansätzen für die Modellierung von Eisenbahnbetrieb in ABS.

Dieses Positionspapier fasst den aktuellen Stand der Branchendurchdringung formaler Methoden zusammen und zeigt die Perspektiven für formale Methoden auf: Hierzu gibt dieses Paper einen Überblick über die verwendeten Formalismen und ihre Anwendungsfälle in der Eisenbahnindustrie, einen Überblick über die erfolgreiche Anwendung formaler Methoden in anderen Ingenieurdisziplinen, eine Analyse welche Aspekte in diesen Bereichen die erfolgreiche Anwendung formaler Methoden ermöglichten und ob sie in der Eisenbahntechnik auftreten sowie eine abschließende Schlussfolgerung, wo formale Methoden ähnliche Auswirkungen auf das Eisenbahnwesen haben werden oder wo im Eisenbahnwesen einzigartige Aspekte zu neuen Anwendungsfällen formaler Methoden führen.

Während es für diese Arbeit nicht möglich ist, eine repräsentative Nutzerstudie oder einen vollständigen Überblick über die formalen Methoden im Schienenverkehr zu geben, bietet unsere Übersicht Hinweise auf aktuelle Übersichtsartikel und Studien.

2 Ausgangssituation

Das System Bahn ist stärker reglementiert als andere Verkehrsträger. Zahlreiche Regelwerke mit betrieblichen Regeln sowie Planungs-, Bau- und Instandhaltungsvorschriften zum Teil mit Sicherheitsrelevanz sind einzuhalten. Die Erstellung dieser Regelwerke ist derzeit Handarbeit, getrieben von Expertenwissen und teilweise gebunden an Einzelpersonen.

Trotz ständiger Pflege durch Aktualisierungen können die natürlichsprachlich festgehaltenen Vorgaben Widersprüche enthalten oder vom Nutzer widersprüchlich ausgelegt werden. Die Aktualisierung von Regelwerken ist aufwendig und derzeit rein durch Experten so weit wie möglich abgesichert.

Automatisch verarbeitbare betriebliche Regelwerke gibt es bisher nicht, in Deutschland gibt es lediglich erste Versuche für automatisch verarbeitbare Planungsvorschriften im Projekt PlanPro der DB Netz [35]. Auch Simulationsmöglichkeiten sind vor allem für betriebliche Abläufe im Störungsfall kaum vorhanden, bestehende Ansätze konzentrieren sich auf Simulationen für z. B. Kapazitätsuntersuchungen.

Eine automatisierte Kontrolle von Regelwerken auf Safetyeigenschaften sowie Über- und Unterspezifizierung existiert nicht, nur eine testfallbasierte Kontrolle, z.B. für Stellwerksplanungen, wobei eine vollständige Abdeckung nicht garantiert ist.

3 Motivation

Wir zeigen, dass aus Bereichen, die ähnlich stark reglementiert oder deren Prozesse vergleichbar mit dem System Bahn sind, aus erfolgreichen Projekten Lehren gezogen werden können um für das System Bahn Folgendes zu erschließen:

- Nutzung von Simulationen von Betriebsprozessen in der Entwicklung zur frühzeitigen Fehleraufdeckung
- Automatische Kontrolle auf Fehlerfreiheit während und am Ende des Entwicklungsprozesses von Regelwerken
- Eine automatisierte Kontrolle auf Safetyeigenschaften sowie Über- und Unterspezifizierung

4 Verwendete Formalismen und ihre Anwendungsfälle in der Eisenbahnindustrie

Im Bahnsektor werden formale Methoden zum einen im Entwicklungsprozess vor allem für Software eingesetzt, aber zum anderen auch zur Modellierung von Prozessen und Logiken. Wenige Anwendungsfälle gehen jedoch über die Nutzung eines formalen Prozesses zur Dokumentation z. B. in Algorithmen hinaus. Auch erreichen bisher nur sehr wenige Anwendungsfälle den praktischen Einsatz.

Betriebsprozesse

Diese Arbeiten setzen zur generischen Beschreibung von Eisenbahnbetriebsprozessen standardisierte UML Diagramme ein. Solche Diagramme werden ebenfalls von der DB Netz bei der Dokumentation aller hauseigenen Prozesse von Vertrieb über Betrieb bis Infrastrukturmanagement eingesetzt. Diese Dokumentation wird als DB-Prozessmodell bezeichnet. Vorarbeiten hierzu lieferte unter anderem die Entwicklung einer Methode zur Stammdatenintegration [12] im Jahr 2010 an der Universität St. Gallen.

In Arbeiten an der TU Braunschweig wurde ein eigenes generisches Referenzsystem für Betriebsverfahren spurgeführter Verkehrssysteme entwickelt [13]. Ein ähnliches Referenzsystem mit formalen Steckbriefen nutzt die DB Netz zur Beschreibung der geschäftlichen Anwendungsfälle für die Leitung und Sicherung des Bahnbetriebs (kurz: GAF) sowie im Lastenheft zu den betrieblich-technischen Systemfunktionen (kurz: BTSF).

Für die Nachweise der unter ETCS geltenden betrieblichen Regeln sind vor allem zwei Ansätze nennenswert. In Real-Time Maude wurde für einfache Betriebsverhältnisse auf der Strecke der Nachweis für ETCS Level 2 in einer Arbeit der Swansea University erbracht. Das Forschungsinstitut INRETS erarbeitet derzeit einen ERTMS Simulator mit dem Ziel, die Betriebsprozesse vollumfänglich darzustellen.

Planung der Ausrüstung mit LST Komponenten

Sowohl theoretische Vorarbeiten zur regelbasierten Konsistenzprüfung von Infrastrukturplanungen [4] als auch erste praktische Anwendungen sind bekannt [5].

Entwicklungsprozess

Im Entwicklungsprozess von Leit- und Sicherungstechnik werden entsprechend des V-Modells Spezifikationen und Testfälle zur Verifikation eingesetzt. Im industriellen Einsatz befinden sich bei den Signalbauunternehmen formale Verfahren und Methoden zur Sammlung von Stellwerksanforderungen. [1]

Zur Sammlung und Anwendung von Testfällen befinden sich Softwarelösungen zur Validierung von ETCS-Planungen, z.B. im Projekt SAT-valid [2], sowie mehrere Produkte zur Zertifizierung von Stellwerksplanungen

u.a. die Software Prover-Certifier im unmittelbaren praktischen Einsatz [9]. In den letzten Jahren sind theoretische Arbeiten zum Testen gegen formal festgehaltene Spezifikationen u.a. zur Verifizierung von fahrzeug- oder infrastrukturseitigen Komponenten des ETCS-Level 2 [3] aufgekommen.

Lasten- und Pflichtenheft für Stellwerksplanungen

Neben dem Einsatz bei der Sammlung von Spezifikationen und Testfällen ist ein Einsatz formaler Methoden bei der Modellierung von Stellwerkslogik naheliegend sowie bei der Modellierung von Betriebsverfahren in Einzelfällen versucht worden.
Zahlreiche Arbeiten aus Dänemark zeigen ein Verfahren zur Modellierung und zur formalen Überprüfung von Stellwerkslogiken [6]. Diese Logiken sind in Form von Verschlusstabellen festgehalten und werden mit dem SMT Solver der SONOLAR-Software verifiziert [7].
Eine ähnliche Verifizierung wird im laufenden EUR-Interlocking Projekt (Nachfolgeprojekt von INESS) angestrebt, eine endgültige Wahl des Verfahrens steht zum derzeitigen Zeitpunkt aus (Stand Ende 2017).
Weitere theoretische Ansätze zur formalen Modellierung lieferten Arbeiten an der ETH Zürich zur Modellierung und Gewährleistung von Abhängigkeiten in Eisenbahnsicherungsanlagen [10]. Ebenfalls an der ETH Zürich existieren theoretische Vorarbeiten zur Modellierung von Betriebsverfahren mit formalen Methoden [11].

Anlagenspezifische Stellwerksplanungen

Die Open-Source Software Werkzeugumgebung OnTrack generiert aus erstellten sicherungstechnischen Lageplänen Verschlusstabellen und in einem weiteren automatischen Schritt formale Modelle zur späteren Verifikation mit CSP||B [8].

Die Software Solver wurde kürzlich eingesetzt, um nach Umbaumaßnehmen einen bestehenden formalen Nachweis unter Nutzung der Sprache B für den CBTC-Rechnerkern der fahrerlosen U-Bahnlinie 14 in Paris zu erneuern [9].

Im industriellen Einsatz befindet sich in diesem Bereich die SCADE Suite, sowie die Software Solver. Beide Produkte können für die Modellierung und die Verifikation von Stellwerksprojektierungen, projektierten Bahnübergangssicherungsanlagen und den beiden Systemen zugrundeliegenden Achszählkreisen genutzt werden. Darüber hinaus wurde die SCADE Suite im Projekt OpenETCS zur Modellierung und Verifizierung der im Projekt entwickelten On-Board-Unit-Software genutzt und ist in großem Umfang für die Verifizierung von Avionikkomponenten in der Luftfahrtindustrie im Einsatz.

Eisenbahnbetriebswissenschaften

Auch in anderen Bereichen des Eisenbahnwesens wie der Instandhaltung [14] und den Eisenbahnbetriebswissenschaften wurden formale Methoden testweise eingesetzt. Bei den Eisenbahnbetriebswissenschaften zeigt eine Arbeit den Nutzen für eine Deadlock-freie Fahrplanerstellung [15] unter Nutzung einer Softwareumgebung zur Modellüberprüfung, die auf der Software UMC basiert.

In den hier genannten Arbeiten zur Modellierung von Stellwerkslogik und Betriebsverfahren wird neben der Einführung neuer Ansätze zunehmend auf bewährte standardisierte formale Ansätze zurückgegriffen.

5 Einsatz in anderen Industriebereichen

Im Folgenden soll ein Blick in andere Industriebereiche für Hinweise zu den Rahmenbedingungen für einen erfolgreichen Einsatz formaler Methoden genutzt werden. Hierzu werden zunächst andere Verkehrsträger sowie erfolgreiche Beispiele aus der Softwareentwicklung herangezogen.

5.1 Andere Verkehrsträger

Avionik

Im Bereich der Software von Avionikkomponenten oder der Programmierung von Mikroprozessoren für Avionikkomponenten wurden bereits früh formale Nachweise geführt. Die Unterstützung bei der Fehlersuche ist bis heute die häufigste Verwendung von formalen Verifikationswerkzeugen unter Nutzung von Modellprüfsoftwarewerkzeugen zum Nachweis von Eigenschaften. Anstatt zu versuchen, zu beweisen, dass die Avionikkomponente für alle Eigenschaften zu jeder Zeit korrekt reagiert, wird diese Technik verwendet, um begrenzte Eigenschaften unter eingeschränkten Bedingungen nachzuweisen. Dies kann die Begrenzung der Tiefe der Zustandsraumsuche oder die Verwendung von Simulationen zum Erreichen eines bestimmten Zustands und die anschließende Analyse des Zustandsraums mit formalen Methoden beinhalten.

Als frühes Beispiel sei hier die Untersuchung des Traffic Alert and Collision Avoidance System (TCAS II) Mitte der 1980er Jahre genannt. Hierbei wurde jedoch kein automatisiertes Tool eingesetzt, sondern die formalen Spezifikationen wurden in Zustandsdiagrammen [16] aufgezeichnet, in denen die Logiken der Software in tabellarischer Form gesetzt und präsentiert werden.

Später wurde zunehmend auf automatische Tool-Unterstützung zurückgegriffen: So zum Beispiel durch das Langley Research Center zum Nachweis der Uhrsynchronisation für Avionikanwendungen [17] oder zur Spezifikation und Modellierung der Software für den Flight Warning Computer (FWC) der Airbus-Baureihen A330 und A340 unter Nutzung der LOTOS Sprache und anhängigen Softwarewerkzeugen. Auf diesen Erfolgen aufbauend wurde bei Airbus bei der Neuentwicklung der kompletten Avioniksoftware für die Baureihe A380 [18] auf formale Methoden und Nachweise zurückgegriffen.

Airbus ist aber nicht der einzige Hersteller, bei dem die formale Verifikation als kostengünstige Alternative zum Testen bereits frühzeitig erfolgreich eingesetzt werden konnte. Weiterhin ist Dassault-Aviation zu nennen und Rockwell Collins hat die Modellprüfung zur Validierung von Anforderungen eingesetzt [19].

Anforderungen an den Zertifizierungsprozess für Software für Verkehrsflugzeuge sind seit 2011 im DO-178B Standard, Softwareüberlegungen bei der Zertifizierung von luftgestützten Systemen und Geräten, festgehalten. Der Standard DO-178C erlaubt den Ersatz von bestimmten Formen der Prüfung durch formale Verifikation [20].

Einige dieser in die Standards aufgenommenen Regelungen sind auch auf die Forschungsaktivitäten der amerikanischen Luft-und Raumfahrtagentur NASA zurückzuführen. NASA begann bereits Mitte der 1990er Jahre damit die Anwendung formaler Methoden zur Zertifizierung kritischer Systeme zu erforschen [21] und erforscht deren Einsatz weiterhin mit zwei Gruppen (Robust Software engineering at Ames, Langley; Formal methods, Laboratory for Reliable Software at JPL).

Neben der industriellen Anwendung zur Verifizierung von Avionikbausteinen existieren weitere Studien zum Einsatz von Event-B bei der Planung von unbemannten Raumfahrtmissionen und Produktion der genutzten Raumsonden [22].

In der Luftfahrbranche werden formale Methoden aber nicht nur zum Nachweis von Avionikbausteinen und -software eingesetzt. Verschiedene, derzeit noch rein theoretische Forschungsvorhaben ohne industrielle Anwendung haben den Nachweis von Prozeduren während des Betriebs zum Ziel. So erstellte das DLR in Braunschweig eine eigene domänenspezifische Sprache zur Formalen Verifikation von Simulationsszenarios in der Luftfahrt: Aviation Scenario Definition Language (ASDL) [23].

Eine weitere Studie zu Prozeduren im Luftbetrieb zerlegte die Schritte das Abflugverfahren auf einem Beispielflughafen bis zum Start in einen Graphen und modellierte diesen Graphen mittels der Vienna Development Method Specification Language (VDM-SL). Zusätzlich wurden die Infrastrukturen des Flughafens wie Taxiways und Start- und Landebahn ebenfalls in einen Graphen zerlegt. Vergleichbar mit einer Stellwerksprojektierung wurden Blöcke definiert, wobei die Graphenknoten mit Warteschleifen ausgestattet sind, an denen sich mehr als nur ein Flugzeug im Abflugverfahren anmelden kann. Die Erfüllung der Anforderungen, dass Flugzeuge bis zum Start schlussendlich eine sinnhafte Abfolge von Graphenknoten durchlaufen und alle Warteschleifen verlassen haben, wurde mit der VDM-SL-Toolbox analysiert und nachgewiesen.

Ein weiteres Beispiel zur Untersuchung von Prozeduren in Luftverkehrssystemen ist die formale Analyse des Betriebskonzepts für das Kleinflugzeugtransportsystem (Small Aircraft Transportation System, kurz: SATS). Das SATS-Betriebskonzept wird mit nicht-deterministischen, asynchronen Transitionssystemen modelliert, die dann formal mit Hilfe von Zustandserkundungstechniken analysiert werden [24].

5.2 Andere Verkehrsträger: Automatisches Fahren im Straßenverkehr

Im High-Assurance Cyber Military Systems (HACMS) Project der Darpa wurden zum einen testweise formale Methoden für die Entwicklung von Systemen für den unmittelbaren militärischen Einsatz eingesetzt, aber zum anderen auch auf Bereiche, die für eine zivile Nutzung denkbar sind. So wurden unter anderem formale Methoden bei der testweisen Entwicklung von Satelliten und im Convoy fahrenden selbstfahrenden LKW angewendet. Alle diese Anwendungsfälle kamen laut der veröffentlichten Berichte bei der Darpa bisher nicht über den Planspiel- oder Prototypen-Status hinaus.

Weitere theoretische Vorarbeiten nutzten Risikostrukturen als Modell für die Entwicklung von High-Level-Controllern, die in der Lage sind, die Risiken zur Laufzeit zu minimieren, d. h. die sichersten Zustände in einer gegebenen Betriebssituation aufrechtzuerhalten oder zu erreichen. Die bisher veröffentlichten Arbeiten skizzieren einen inkrementellen Ansatz zur Entwicklung von Strategien zur Eindämmung der Risiken beim automatischen Fahren im Straßenverkehr [25].

5.3 Software Engineering

Weitere Felder aus dem Bereich der Ingenieurwissenschaften setzen ebenfalls formale Methoden bei der Entwicklung von Software ein. Besonders hier sind Erfolge zu benennen und ein Vergleich mit dem möglichen Einsatz im Eisenbahnwesen lohnend. Als besonders sicherheitskritischer Bereich seien im Folgenden die durchgeführten Projekte zu Modellüberprüfung und Anwendung formaler Methoden bei der Verifizierung von Steuerungssoftware für Atomkraftwerke aufgeführt.

5.3.1 Software Engineering für sicherheitskritische Ingenieurswissenschaften

Eine der ersten Anwendungen von formalen Methoden in diesem Kontext betraf die Systemsoftware bei der Reaktorabschaltung des Darlington Atomkraftwerks in Kanada. Im Planungsprozess für die Software wurde

eine tabellarische Notation verwendet, um sowohl die Anforderungen als auch das Design zu beschreiben und um die Richtigkeit des Entwurfs mit einem Theorembeweiser überprüfen zu können.

In Ungarn wurde die Software zur Kontrolle auf Leckage eines Reaktors mittels eines Colored Petri Net (CPN) Formalismus versuchsweise modelliert. Die korrekte Funktion wurde mittels Zustandsraumanalyse und expliziter Zustandsmodellprüfung nachgewiesen. Über den reinen Einsatz von formalen Nachweisen hinaus wurde zusätzlich die Primärkreisdynamik mit CPN modelliert und die Zusammensetzung dieses Modells und der Abschaltprozedur bei Leckage durch Simulation analysiert.

Formale Methoden und Modellprüfung wurden in Korea intensiv im Rahmen von Forschungsprojekten zur Kernkraftwerksautomatisierung genutzt. Die Erlebnisberichte beschreiben einen rechnergestützten Werkzeugsatz, der die Entwicklung von SPS-basierten Systemen (Speicherprogrammierbare Steuerung) unterstützt [26]. Dieser Werkzeugsatz umfasst Werkzeuge zur Pflege und Erstellung von formalen Pflichtenheften, zum Systemdesign und für eine automatische Übersetzung in C-Programme.

Eine formale Sprache, die einerseits auf tabellarischen Notationen und andererseits auf Zustandsautomaten basiert, wird für die Anforderungsspezifikation verwendet. Hieraus kann automatisch Code generiert werden. Im Nachgang werden nach weiteren nötigen Zwischenarbeitsschritten Modellprüfung und Theoremprüfung zur Überprüfung der Korrektheit eingesetzt. Hierzu muss der Code zunächst in Verilog (eine gebräuchliche Hardwarebeschreibungssprache) übersetzt werden. Die Verilog-Programme werden dann automatisch in die Eingabesprache des Cadence SMV-Modellprüfers übersetzt.

Grenzwerte für zeitlich kritische Prozessdauern wurden von den Forschern in Zusammenarbeit mit Experten ermittelt und in das Modell eingepflegt. Schlussendlich wurden mehrere Fehler gefunden, die bei manuellen Inspektionen nicht bemerkt wurden. Die Einbindung von Expertenwissen war essentiell für den Projekterfolg und sollte Basis für weitere Versuche im Eisenbahnwesen sein.

5.3.2 Software Engineering in verteilten Systemen

Verteilte Systeme sind eine Menge interagierender Prozesse (oder Prozessoren), die über keinen gemeinsamen Speicher verfügen und daher über Nachrichten miteinander kommunizieren müssen [27]. Aufgrund der überproportional steigenden Anforderungen bei der Programmierung von verteilten Systemen wird besonders hier versucht, formale Methoden anzuwenden, um Fehler aufzudecken.

Zahlreiche Forschungsarbeiten nutzen formale Methoden zur Verifizierung von in Software modellierten Prozessen verteilter Systeme: So wurde ein Bug im Prozess des mittels des Needham-Schroeder public-key authentication Protokoll durchgeführten Schlüsselaustauschs zur Authentifizierung in großen Computernetzwerken gefunden, nachdem dieses System bereits 17 Jahre im Einsatz war [28]. Weiter wurde mit KeY, einem Softwareverifikationswerkzeug für in Java geschriebene Programme, ein Bug in der Java Standard library gefunden [29].

Im industriellen Einsatz finden sich unter anderem Beispiele auch bei IBM, Microsoft, Amazon und Facebook, die im Folgenden kurz aufgelistet sind:

- IBM: Einsatz bei neuen Releases seines Transaktionsverarbeitungssystems CICS [30]
- Microsoft: Verifizierung von HTTPS im Projekt Everest [31]
- Amazon: Einsatz von TLA+ zur Verifizierung von Algorithmen für Backups, Konsistenzprüfung von Backups und weiteren Funktionen von verteilten Systemen und Web-Services, die Kunden zur Verfügung gestellt werden [32]
- Facebook: Integration eines auf statischer Analyse basierenden Verifikationstools in den Software-Entwicklungszyklus [33]

5.3.3 Weitere Beispiele aus dem Software Engineering

Neben den genannten Beispielen für die Nutzung von formalen Methoden in der Spezifizierung, Entwicklung und Verifizierung z. B. von Avionik-Bausteinen sind auch andere Beispiele aus der Softwareentwicklung zu nennen. Diese umfassen zahlreiche Softwarearten, zum Beispiel hardwarenahe Software für Mikroprozessoren oder für Programmalgorithmen, die in einer High-Level-Language wie z. B. Java geschrieben wurden.

Hardwarenah wurden beispielsweise formale Methoden durch den Halbleiterhersteller Inmos bei der Entwicklung einer Floating Point Unit für den T800 Transputer eingesetzt. Für die Medizintechnik wird durch Phillips Healthcare der Analytical Software Design Ansatz verfolgt um unter anderem für Bildgebungsgeräte wie Röntgen oder CT und Elektronenmikroskope die Kontrollsoftware zu erstellen und zu verifizieren. Hierbei wird zur frühzeitigen Aufdeckung von Fehlern Uppaal eingesetzt, eine integrierte Softwarewerkzeugumgebung zur Modellierung, Validierung und Verifikation von Systemen, die als Netzwerke von zeitgesteuerten Automaten modelliert sind. Die Wahl fiel auf Uppaal wegen seiner ansprechenden und verständlichen Benutzeroberfläche und den Simulationsmöglichkeiten, die für industrielle Anwender attraktiv sind [34].

6 Nutzen

In Anlehnung an den Entwicklungsprozess nach dem V-Modell können folgende Lebenszyklusschritte mit mehreren Unterschritten identifiziert werden: Planungsphase, Erstellungsphase und Betriebsphase.

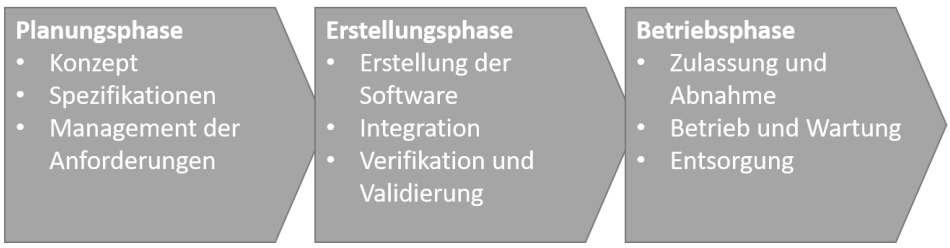

Abb. 1 Lebenszyklusschritte eines Softwareproduktes

Beispiele aus der Industrie zeigen, dass eine Nutzung von formalen Methoden während möglichst vieler der oben genannten Schritte während der Planungs- und Erstellungsphase des Entwicklungsprozesses zum Projekterfolg beitragen. So wurde beim koreanischen Atomprogramm eine durchgängige Werkzeugkette

geschaffen, um sowohl die Spezifikationen zu erfassen und deren Erfüllung zu verifizieren als auch bei der Erstellung der Softwaren die Fehleraufdeckung zu unterstützen.

Die Einbindung von Experten zur Definition von Grenzwerten und Testfällen ist unabdingbar.

Die Gesamtqualität des Produktes und die Entwicklungskosten konnten durch eine frühe Fehlererkennung in der Erstellungsphase auf einfache Weise reduziert werden. Weiter gilt es, die Verbindung mit eingesetzten Methoden aus der Planungsphase herzustellen, um weitere Verifizierungsschritte gegen die gesammelten Spezifikationen zu automatisieren. Eine höhere Automatisierung trägt an dieser Stelle auch zur Beschleunigung der Entwicklung und zur Kostensenkung bei. Am Ende der Erstellungsphase kann direkt aus dem formalen Design heraus ein Programmcode generiert werden.

Steht für die automatische Generierung des Programmcodes aus dem formalen Modell sogar ein verifizierter Compiler zur Verfügung, können auch einzelne Zulassungstests wegfallen. Der Wegfall möglichst vieler Zulassungsschritte durch die durchgängige Nutzung verifizierter Werkzeuge, die formale Methoden nutzen, ist denkbar und anzustreben.

Die erfolgreiche Anwendung in der Medizintechnik durch Philips zeigt auch die Bedeutung eines guten User-Interfaces, um den Zugang zur Nutzung von formalen Methoden für größere Bereiche der Ingenieurwissenschaften über die Informatik hinaus zu erleichtern.

7 Ergebnisse

Wir erwarten den Anstieg der Nutzung von formalen Methoden in der Eisenbahntechnik in folgenden Bereichen:

(1) Als Mittel zur Kommunikation und Vereinheitlichung – Anwendungsfälle im Software Engineering zeigen, dass der positive Effekt der Formalisierung eines Produkts nicht zwingend der Gebrauch des entstandenen Modells ist, sondern, dass eine eindeutige Definition der Schlüsselkonzepte und Schnittstellen erzeugt wurde. Diese erlauben es den intern Beteiligten aber auch internationalen Teams schneller ein klares gemeinsames Verständnis zu finden und dieses effizienter zu nutzen. Dies erfordert auch zu Beginn keine globale Anerkennung: Ein einzelnes Team kann seinen Bereich formalisieren und ihn zur Kommunikation mit Außenstehenden nutzen. Beispielsweise erwarten wir die Nutzung von formalen Methoden in der Lehre und Weiterbildung.

(2) Als Mittel zur Unterstützung neuer Entwürfe in kritischen Projektphasen – aktuelle formale Methoden schaffen es Modelle zu analysieren, aber es fehlt ihnen an Präzision oder Effizienz bei bereits vollständig entwickelten Modellen. Es hilft an dieser Stelle das System Bahn als verteiltes System zu verstehen. Für diese Systeme stehen bereits formale Methoden und Werkzeuge zur Verfügung. Die erfolgreiche Nutzbarmachung dieser vorhandenen Werkzeuge konnte mit den ersten Case-Studies im Projekt FormbaR gezeigt werden. Aufbauend auf dem ersten Punkt erwarten wir, dass Probleme und Streitpunkte unter formellen Bedingungen übermittelt und analysiert werden können, zusätzlich zur informellen Beschreibung.

(3) Als Mittel zur Unterstützung der Zertifizierung. Die zwei bereits genannten Punkte ermöglichen eine Kommunikation speziell von sicherheitskritischen Gestaltungsentscheidungen gegenüber zertifizierenden Behörden.

Wir erwarten nicht, dass formale Methoden große Schritte in der Planung von Eisenbahnprojekten vollständig automatisieren. Stattdessen sehen wir sie als weiteres Hilfsmittel zur Unterstützung der bereits genutzten

Systeme. Dennoch erwarten wir, dass formale Methoden ein wichtiges Instrument zur Gestaltung und Zertifizierung von (wahrscheinlich autonomen) Prozessen sein werden.

8 Literaturverzeichnis

[1] Hon, Yuen Man (2009): *Ein ingenieurgerechtes formales Verfahren für die Spezifikation von Stellwerksanforderungen*, Dissertation an der TU Braunschweig, Braunschweig

[2] Wenzel, Benedikt; Wolf, Alexander; Schütte, Jörg; Jurtz, Steffen (2012): *SAT.VALID – A new data validation tool for communication based train control system (such as ETCS)*, Konferenzbeitrag auf der ASPECT 2012, London

[3] Sango, Marc; Gransart, Christophe; Duchien, Laurence (2014): *Safety component-based approach and its application to ERTMS/ETCS on-board train control system*. Konferenzbeitrag auf der TRA2014 Transport Research Arena 2014, Paris

[4] Luteberget, Bjørnar; Johansen, Christian (2018): *Efficient verification of railway infrastructure designs against standard regulations*, in Journal for Formal Methods in System Design 52: 1. https://doi.org/10.1007/s10703-017-0281-z

[5] Klaus, Christoph; Buder, Jens; Brödel, Reiner (2015): *Neue Werkzeuge in der LST-Planung mit PlanPro*, in EI – Der Eisenbahningenieur 07/2015, Hamburg

[6] Gjaldbaek, Torben; Haxthausen, Anne E. (2003): *Modelling and verification of interlocking systems for railway lines*, in IFAC Proceedings Volume (36) 14

[7] Haxthausen, Anne E. (2013): *Applied Bounded Model Checking for Interlocking System Designs*, in Software Engineering and Formal Methods: SEFM 2013, Madrid

[8] James, Philip; Trumble, Matthew; Treharne, Helen; Roggenbach, Markus; Schneider, Steve (2013): *OnTrack: An Open Tooling Environment for Railway Verification*. In: Brat G., Rungta N., Venet A. (eds) NASA Formal Methods. NFM 2013. Lecture Notes in Computer Science, vol 7871. Springer, Berlin, Heidelberg

[9] Prover (2017): *White Paper – Interlocking Design Automation – The Process*

[10] Montigel, Markus (1994): *Modellierung und Gewährleistung von Abhängigkeiten in Eisenbahnsicherungsanlagen*, Doctoral Thesis, Institut für Verkehrsplanung, Transporttechnik, Strassen- und Eisenbahnbau (IVT), ETH Zürich, Zürich.

[11] Höppner, Silko (2015): *Generische Beschreibung von Eisenbahnbetriebsprozessen*, Doctoral Thesis, Institut für Verkehrsplanung und Transportsysteme (IVT), ETH Zürich, Zürich.

[12] Schmidt, Alexander (2010): *Entwicklung einer Methode zur Stammdatenintegration*, Dissertation der Universität St. Gallen, St. Gallen

[13] Bosse, Gunnar (2010): *Grundlagen für ein generisches Referenzsystem für die Betriebsverfahren spurgeführter Verkehrssysteme*, Dissertation an der TU Braunschweig, Braunschweig

[14] Ruijters E., Stoelinga M. (2016): *Better Railway Engineering Through Statistical Model Checking*. In: Margaria T., Steffen B. (eds) Leveraging Applications of Formal Methods, Verification and Validation: Foundational Techniques. ISoLA 2016. Lecture Notes in Computer Science, vol 9952. Springer, Cham

[15] Mazzanti F., Spagnolo G.O., Ferrari A. (2014): *Designing a Deadlock-Free Train Scheduler*: A Model Checking Approach. In: Badger J.M., Rozier K.Y. (eds) NASA Formal Methods. NFM 2014. Lecture Notes in Computer Science, vol 8430. Springer, Cham

[16] D.R. Harris (1986): *A Hybrid Object and Constraint Representation Language*, AAAI-86, Philadelphia, Pennsylvania

[17] Rush, John; von Henke, Friedrich (1993): *Formal verification of algorithms for critical systems*. IEEE Transactions on Software Engineering, 19(1):13

[18] Souyris, J.; Wiels, V.; Delmas, D.; Delseny, H. (2009): *Formal Verification of Avionics Software Products*. Formal Methods 2009 sowie: DELMAS, D.; SOUYRIS, J. (2007): *Astrée: From Research to Industry*. SAS 2007: 437-451

[19] Millers, S.; Tribble, A.; Whalen, M.; Heimdahl, M. (2006): *Proving the Shalls: Early Validation of Requirements through Formal Methods*. Software Tools for Technology Transfer, volume 8, number 4. sowie: Miller, S.; Whalen, M.; Cofer, D. (2010): *Software Model Checking Takes off*. Communications of the ACM, Volume 53, N° 2. 2010

[20] Moy, Yannick; Ledinot, Emmanuel; Delseney, Hervé, Wiels, Virginie; Monate, Benjamin (2013): *Testing or Formal Verification: DO-178C Alternatives and Industrial Experience*, in IEEE Software (Volume: 30, Issue: 3)

[21] J. RUSHBY (1995): *Formal Methods and their Role in the Certification of Critical Systems*. Technical Report CSL-95-1,

[22] Salehi Fathabadi A., Rezazadeh A., Butler M. (2011): *Applying Atomicity and Model Decomposition to a Space Craft System in Event-B*. In: Bobaru M., Havelund K., Holzmann G.J., Joshi R. (eds) NASA Formal Methods. NFM 2011. Lecture Notes in Computer Science, vol 6617. Springer, Berlin, Heidelberg

[23] Chhaya, Bharvi und Jafer, Shafagh und Durak, Umut (2018): *Formal Verification of Simulation Scenarios in Aviation Scenario Definition Language (ASDL).* Aerospace. Multidisciplinary Digital Publishing Institute (MDPI)

[24] Muñoz C., Carreño V., Dowek G. (2006): *Formal Analysis of the Operational Concept for the Small Aircraft Transportation System*. In: Butler M., Jones C.B., Romanovsky A., Troubitsyna E. (eds) Rigorous Development of Complex Fault-Tolerant Systems. Lecture Notes in Computer Science, vol 4157. Springer, Berlin, Heidelberg

[25] Gleirscher M., Kugele S. (2017): *From Hazard Analysis to Hazard Mitigation Planning: The Automated Driving Case*. In: Barrett C., Davies M., Kahsai T. (eds) NASA Formal Methods. NFM 2017. Lecture Notes in Computer Science, vol 10227. Springer, Cham

[26] Seo-Ryong Koo, Poong Hyun Seong, JunBeom Yoo, Sung Deok Cha, Cheong Youn, and Hyun-Chul Han. NuSEE (2006): *An integrated environment of software specification and V&V for PLC based safety-critical systems*. Nuclear Engineering and Technology, 38(3)

[27] Löhr, Peter (2001): *Verteilte Systeme*, auf www.inf.fu-berlin.de/lehre/WS01/VS/Lectures/vs1.pdf, abgerufen am 15.5.2018

[28] Lowe, Gavin (1995): *An attack on the Needham-Schroeder public-key authentication protocol*, Information Processing Letters (Volume 56, Issue 3)

[29] de Gouw, S., de Boer, F.S., Bubel, R. et al. (2016): *Verifying OpenJDK's Sort Method for Generic Collections,* J Autom Reasoning. https://doi.org/10.1007/s10817-017-9426-4

[30] Hoare J., Dick J., Neilson D., Sørensen I. (1996): *Applying the B technologies to CICS.* In: Gaudel MC., Woodcock J. (eds) FME'96: Industrial Benefit and Advances in Formal Methods. FME 1996. Lecture Notes in Computer Science, vol 1051. Springer, Berlin, Heidelberg

[31] Microsoft (2016): *Project Everest – Verified Secure Implementations of the HTTPS Ecosystem*, auf https://www.microsoft.com/en-us/research/project/project-everest-verified-secure-implementations-https-ecosystem/, abgerufen am 15.5.2018

[32] Chris Newcombe, Tim Rath, Fan Zhang, Bogdan Munteanu, Marc Brooker, Michael Deardeuff (2015): *How Amazon Web Services Uses Formal Methods*, Communications of the ACM, Vol. 58 No. 4

[33] Calcagno C. et al. (2015): *Moving Fast with Software Verification*. In: Havelund K., Holzmann G., Joshi R. (eds) NASA Formal Methods. NFM 2015. Lecture Notes in Computer Science, vol 9058. Springer, Cham

[34] Hooman, Jozef (2016): *Industrial Application of Formal Models Generated from Domain Specific Languages*, *Theory and Practice of Formal Methods - de Boer Festschrift, LNCS 9660*

[35] Gerke, Carsten; Bleidiesel, Joachim; Lodemann, Michael; Luttenberger, Norbert (2012): *XML-Schemata zum Datenaustausch im Planungsprozess von elektronischen Stellwerken*, ETR, Nr. 3, März 2012