

Auszug aus

**Methode zur Sicherheitsnachweisführung einer
bordautonomen satellitenbasierten
Ortungseinheit für den Schienenverkehr**

Von der Fakultät für Maschinenbau
der Technischen Universität Carolo-Wilhelmina zu Braunschweig
zur Erlangung der Würde
eines Doktor-Ingenieurs (Dr.-Ing.)
genehmigte Dissertation

von: Dipl.-Ing. Hansjörg Manz
aus: Dresden

eingereicht am: 11.02.2016
mündliche Prüfung am: 04.05.2016

Gutachter: Prof. Dr.-Ing. Dr. h.c. mult. Eckehard Schnieder
Prof. Dr.-Ing. Jochen Trinckauf

Vorsitzender: Prof. Dr.-Ing. Peter Hecker

Kurzfassung

Mit dieser Arbeit wird ein Beitrag zur Steigerung der Attraktivität des Schienenverkehrs durch den Wechsel von traditioneller streckenseitiger auf satellitenbasierte fahrzeugseitige Ortung geleistet. Hierbei wird eine Grundlage für den Entwicklungsprozess für die Selbstortung des Schienenfahrzeugs ohne streckenseitige Einrichtungen oder Aktivitäten des Fahrers erstellt, um die Zertifizierung und Typzulassung einer bordautonomen, mit ETCS Level 3 konformen satellitenbasierten Ortungseinheit für den Schienenverkehr zu erreichen.

Anstelle der momentan im Schienenverkehr üblichen diskreten Zugortung können mit Einführung der satellitenbasierten kontinuierlichen Ortung eine Vielzahl an Vorteilen durch einen effizienteren Betrieb und den Verzicht auf streckenseitige Ortungskomponenten sowie Signalisierung ermöglicht und realisiert werden.

Die hier konzipierte Ortungseinheit muss für eine Zertifizierung entsprechend dem gültigen normativen Rahmen entwickelt werden. Dafür werden der normative Rahmen und dessen historische Entwicklung analysiert und die beteiligten Organisationen im Normerstellungsprozess sowie die Entwicklungsprozesse in Europa betrachtet. Um die Ergebnisse dieser Arbeit auch weltweit für Entwicklungsprozesse nutzen zu können, wird auch der internationale normative Rahmen fokussiert. Darauf aufbauend soll die Begutachtung und Zertifizierung der satellitenbasierten Ortungseinheit im Schienenverkehr durchgeführt und der Prozess nachvollzieh- und wiederholbar dargestellt werden. Die satellitenbasierte Zugortung soll in moderne Zugbeeinflussungssysteme eingebunden werden und ist somit nicht separat einsetzbar. Für die somit notwendige Integration wird hier die Grundlage gelegt, die Umsetzung erfolgt durch ein modulares Modellkonzept für die Schnittstellen.

Um eine klar strukturierte Darstellung zu ermöglichen, wird ein terminologisch konsistentes Vorgehen eingeführt und genutzt. Der Fokus liegt dabei auf für die Entwicklung und Zertifizierung relevanten Termini, was zum Verständnis und für eine konsistente Durchführung notwendig ist. Dies ist die Basis für die sichere Systementwicklung und die damit verknüpfte Zertifizierung für ein System mit eindeutigen Systemgrenzen. Diese werden hier eingeführt und sind notwendig, um festzulegen, für welche Teile die Sicherheitsanalyse zutreffend und anzuwenden ist. Dieses Vorgehen ermöglicht es, frühzeitig Probleme und Schwierigkeiten zu erkennen, adäquate Lösungen zu erarbeiten und diese in den Entwicklungsprozess einbinden zu können. Die dafür erforderlichen Prozesse werden zunächst allgemein dargestellt und darauf aufbauend auf die Zertifizierung angewandt, die der Nutzung der satellitenbasierten Ortung im Schienenverkehr zugrunde liegt.

Abstract

This thesis contributes to a more attractive railways by enhancing the change from traditional track side to satellite based vehicle self-localisation. The development process for the self-localisation of a rail vehicle without track side infrastructure and activities of the driver is created to reach the certification and type approval of a board autonomous localisation unit for railways compatible with ETCS level 3.

Instead of the currently used discrete localisation in railways the advantages of satellite based localisation can be used for a continuous localisation. This leads to various benefits by an efficient operation and the abandonment of track side localisation as well as signalling components.

The localisation unit designed in this thesis has to be developed for a certification according the normative background which is therefore analysed. Furthermore the historical background of the normative background is analysed and the participating organisations in the creation of a norm as well as the development process in Europe are focused. To use the results of this work for worldwide development processes, the international normative background is focused as well. On this basis, the certification and assessment of the satellite based localisation unit for railways is carried out with consistent and comprehensive process. The satellite based train localisation is integrated in modern train control system and can therefore not be used separately. For the necessary integration the fundamental work is done, the implementation is carried out by a modular model concept for the interfaces.

To enable a clear structured description, a terminologically consistent approach is introduced and used. The focus is on the terms relevant for development and certification to enhance the comprehensibility and for a consistent implementation. This work is the basis for a safe system development and the connected certification with a clearly structured system. These are introduced here and are necessary to know the relevant parts for the safety analysis. This approach enables to identify potential problems and difficulties early and to adopt adequate solutions to be included in the development process. The necessary processes are introduced in general and subsequently applied to the certification of the satellite based localisation in railways.

Inhaltsverzeichnis

Vorwort	III
Kurzfassung	V
Abstract	VI
Inhaltsverzeichnis	VII
Verzeichnis der Abkürzungen und Akronyme	XIII
Glossar	XVII
1 Einleitung.....	1
1.1 Herausforderungen im Schienenverkehr und mögliche Potenziale	1
1.1.1 Interoperabilität des Schienenverkehrs in Europa	1
1.1.2 Wirtschaftlicher Betrieb von Nebenstrecken	2
1.1.3 Verzicht auf streckenseitige Infrastruktur	2
1.1.4 Erhöhung der Streckenkapazität	3
1.1.5 ETCS als europäisches Zugbeeinflussungssystem	3
1.1.6 Ansatz, Problemstellung	4
1.2 Abgrenzung der Arbeit und Vorarbeiten.....	5
1.3 Ziele dieser Arbeit	6
1.3.1 Teilziel A: Konsistente Darstellung der Systemarchitektur.....	7
1.3.2 Teilziel B: Sicherheitsgerichteter Entwicklungsprozess.....	8
1.3.3 Teilziel C: Nachweis der sicheren Funktionalität	8
1.4 Struktur dieser Arbeit	9
2 Stand der Forschung und Technik in Zugbeeinflussung und Ortung	11
2.1 Leitsysteme zur Steuerung des Verkehrssystems Eisenbahn	11
2.1.1 Einführung Zugbeeinflussungssysteme	11
2.1.2 Gliederung der Zugbeeinflussungssysteme	12
2.1.3 Entwicklung und Anwendung der Zugbeeinflussung in Europa	12
2.1.4 Wandel zur europäischen Zugbeeinflussung	14
2.1.5 Technische Umsetzung von ETCS	14
2.1.6 Nutzung von ETCS in Europa	15
2.2 Migrationsprozesse im Schienenverkehr.....	16
2.2.1 Durchführung der Migration	16
2.2.2 Prozess der Migration	17
2.2.3 Besonderheiten der Migration von Zugbeeinflussungssystemen.....	18
2.2.4 Migration zwischen verschiedenen ETCS Leveln	19
2.3 Ortung im Schienenverkehr.....	20
2.3.1 Klassifikation von Ortungsmethoden.....	21
2.3.2 Fahrzeugseitige kontinuierliche Ortung.....	21
2.3.3 Strukturierung der zur Ortung verwendeten Sensoren.....	22
2.3.4 Fahrzeugseitige Sensoren und digitale Karte.....	23

2.3.5	Stand der Nutzung von GNSS im Schienenverkehr	24
2.3.6	In Betrieb befindliche satellitenbasierte Zugbeeinflussungssysteme....	25
2.3.7	Konzepte satellitenbasierter Zugbeeinflussungssysteme	26
2.4	Satellitenbasierte Sensorik	27
2.4.1	Satellitenbasierte Ortung.....	28
2.4.2	Funktionsweise und technische Aspekte der GNSS	29
2.4.3	Weltweite GNSS	30
2.4.4	Galileo.....	31
2.4.5	Erhöhung der Genauigkeit	32
2.4.6	Weltweite Ergänzungssysteme	33
2.4.7	Anwendungen der Luftfahrt.....	33
2.5	Integration und Zertifizierung der satellitenbasierten Ortung.....	35
2.5.1	Generische Zertifizierung satellitenbasierter Ortungssysteme	35
2.5.2	Domänenspezifische Zertifizierung satellitenbasierter Ortung.....	37
2.5.3	Zertifizierung industrieller Komponenten für den Schienenverkehr	37
3	Normativer Rahmen.....	39
3.1	Entwicklung normativer Dokumente	39
3.1.1	Beteiligte Organisationen am Normerstellungsprozess	40
3.1.2	Beteiligte Organisationen im Gesetzgebungsprozess	40
3.1.3	Beteiligte Interessenverbände	41
3.1.4	Wandel der europäischen Legislative	41
3.1.5	Wandel des sicherheitsgerichteten Entwicklungsprozesses.....	44
3.1.6	Einfluss des rechtlichen Wandels auf die Entwicklung und Zertifizierung	44
3.2	Zugrunde liegende Dokumente des normativen Rahmens.....	45
3.2.1	Allgemeine Industrienormen.....	46
3.2.2	Normen der Systemklassifikation	47
3.2.3	Grundlegende Normen des Schienenverkehrs	47
3.2.4	Grundlegende Spezifikationen des Schienenverkehrs	49
3.2.5	Dokumente des Herstellers und Betreibers	50
3.2.6	Internationale Dokumente der Entwicklung im Schienenverkehr	51
3.3	Sicherheitsnachweisführung.....	51
3.3.1	Begriffsdefinitionen	52
3.3.2	Sicherheitsnachweis in der Luftfahrt	54
3.3.3	Sicherheitsnachweis im Schienenverkehr in Europa	54
3.3.4	Einfluss der TSI auf Entwicklung und Zertifizierung.....	58
3.3.5	Sicherheitsnachweis im Schienenverkehr weltweit	58
3.3.6	Domänenübergreifender Ansatz	59
3.3.7	Strukturierung der Sicherheitsnachweisführung	60
3.3.8	Zusammenfassung der Ansätze.....	60
3.4	Normative Anforderungen im Schienenverkehr	61

3.4.1	Risikoakzeptanzkriterien im Schienenverkehr.....	62
3.4.2	Normative Anforderungen an Komponenten im Schienenverkehr.....	63
3.4.3	Normative Anforderungen an den Entwicklungsprozess.....	64
3.4.4	Normative Anforderungen an den Entwicklungsprozess (international).....	65
3.4.5	Durchführung der sicheren Systementwicklung	67
3.4.6	Nachweiskonzeption	68
3.4.7	Normkonforme entwicklungsbegleitende Dokumentation	71
3.4.8	Inbetriebnahmegenehmigung.....	72
4	Entwicklung sicherer Systeme und Systemstrukturierung	73
4.1	Entwicklung technischer Systeme im Schienenverkehr.....	73
4.1.1	Generischer sicherheitsgerichteter Entwicklungsprozess	74
4.1.2	Domänenunabhängige Verantwortlichkeiten.....	75
4.1.3	Personelle und institutionelle Unabhängigkeiten nach Sicherheitsstufe	76
4.1.4	Verantwortlichkeiten im Entwicklungsprozess	77
4.1.5	Verantwortlichkeiten während der Zertifizierung.....	79
4.2	Grundlagen der Strukturierung eines technischen Systems	81
4.2.1	Herausforderungen der Systemstrukturierung	82
4.2.2	Grundlegende Definitionen.....	82
4.2.3	Eigenschaften des Systembegriffs	83
4.2.4	Bedeutende Aspekte der Erstellung der Systemarchitektur	84
4.3	Ansätze zur Durchführung der Systemstrukturierung.....	84
4.3.1	Funktionsbezogene Struktur	85
4.3.2	Produktbezogene Struktur.....	87
4.3.3	Ortsbezogene Struktur.....	88
4.3.4	Integrierte Struktur	90
5	Strukturierung der Anforderungsspezifikationen	91
5.1	Anforderungen an Betrieb und Instandhaltung	91
5.1.1	Generische Darstellung der Anforderungen an Anwendungen	91
5.1.2	Strukturierung der Funktionen im Schienenverkehr	92
5.1.3	Zusammenfassung.....	95
5.2	Anforderungen an Stilllegung und Entsorgung.....	96
5.3	Anforderungen an Betrieb mit externen Einflüssen	96
6	Strukturierung der Sicherheitsanforderungsspezifikationen.....	97
6.1	Aufstellen der Sicherheitsanforderungen	98
6.1.1	Anforderungen an Systemkomponenten.....	99
6.1.2	Anforderungen entsprechend des Funktionsaspekts	100
6.1.3	Resultierende Anforderungen an die Ortungseinheit.....	102
6.1.4	Anforderungen an den Entwicklungsprozess.....	105
6.1.5	Anforderungen an durch Sensoren gelieferte Informationen.....	105

6.1.6	Technische Sicherheitsanforderungen	105
6.2	Anforderungen an Sicherheitsüberwachung im Betrieb	106
6.3	Anforderungen an Stilllegung und Entsorgung	106
6.4	Anforderungen an Sicherheitserprobung	106
7	Erstellung des Sicherheitsnachweises	109
7.1	Definition des Systems	110
7.1.1	Einleitung	111
7.1.2	Systemarchitektur	112
7.1.2.1	Beschreibung der Systemarchitektur	113
7.1.2.2	Definition der Schnittstellen	116
7.1.3	Sichere Systementwicklung	119
7.1.3.1	Zusammenfassung der technischen Sicherheitsprinzipien....	119
7.1.3.2	Projektierung von Teilsystemen und Systemaufbau	123
7.2	Allgemeine Informationen	124
7.2.1	Qualitätsmanagementbericht	124
7.2.2	Sicherheitsmanagementbericht	124
7.3	Technische Sicherheitsanalyse und Umsetzung	124
7.3.1	Einleitung	125
7.3.2	Betrieb mit externen Einflüssen	126
7.3.2.1	Klimatische Bedingungen	126
7.3.2.2	Mechanische Bedingungen	126
7.3.2.3	Höhe über Meeresspiegel	126
7.3.2.4	Elektrische Bedingungen (nicht auf Fahrzeugen)	127
7.3.2.5	Elektrische Bedingungen (auf Fahrzeugen)	127
7.3.2.6	Schutz vor unberechtigtem Zutritt	127
7.3.2.7	Erschwerte Bedingungen	127
7.3.3	Ausfallauswirkungen	127
7.3.3.1	Angabe der Fail-Safe-Prinzipien	128
7.3.3.2	Unabhängigkeit von Betrachtungseinheiten	129
7.3.3.3	Schutz gegen systematische Fehler	130
7.3.3.4	Auswirkung von Einzelausfällen	130
7.3.3.5	Auswirkung von Mehrfachausfällen	131
7.3.3.6	Offenbarung von (Einzel-)Ausfällen	132
7.3.3.7	Aktion nach Ausfalloffenbarung	132
7.3.4	Nachweis des korrekten funktionalen Verhaltens	132
7.3.4.1	Erfüllung der Sicherheitsanforderungen	133
7.3.4.2	Nachweis der korrekten Hardwarefunktionalität	135
7.3.4.3	Nachweis der korrekten Softwarefunktionalität	136
7.3.5	Sicherheitsbezogene Anwendungsbedingungen	137
7.3.5.1	Betrieb und Instandhaltung	138
7.3.5.2	Sicherheitsüberwachung im Betrieb	138

7.3.5.3	Stilllegung und Entsorgung.....	139
7.3.6	Sicherheitserprobung	139
7.3.6.1	Erfüllung der Systemanforderungen	139
7.3.6.2	Ergebnisse	140
7.4	Zusammenfassung und Schlussfolgerung	140
7.4.1	Beziehungen zu anderen Sicherheitsnachweisen	140
7.4.2	Zusammenfassung.....	141
8	Sicherheitsgutachten	143
8.1	Begutachtungsgegenstand	143
8.2	Unabhängigkeit des Gutachters	143
8.3	Durchführung der Begutachtung	144
8.4	Dokumentation der Begutachtung	145
8.5	Abweichungen gegenüber Sicherheitsanforderungen	147
8.6	Zulassung des betrachteten Systems	148
9	Zusammenfassung und Ausblick	149
9.1	Zusammenfassung und kritische Diskussion der Ergebnisse.....	149
9.2	Ausblick.....	150
Anhang 1:	Projekte zur satellitenbasierten Ortung im Schienenverkehr.....	151
Anhang 2:	Bekannte ETCS Ausrüstung in Europa	152
Anhang 3:	Normativer Rahmen der satellitenbasierten Ortung	153
Anhang 4:	Strukturierung der Funktionen in anderen Verkehrsdomänen.....	154
Anhang 5:	Anforderungen an Komponenten in Schienenfahrzeugen	155
Literaturverzeichnis		156
Abbildungsverzeichnis		169
Tabellenverzeichnis		172

9 Zusammenfassung und Ausblick

In dieser Arbeit wurde aufbauend auf den Grundlagen der satellitenbasierten Ortung und des Schienenverkehrs eine generische Methode zur Nachweisführung und zur Zertifizierung einer bordautonomen satellitenbasierten Ortungseinheit für den Schienenverkehr unter Nutzung externer Komponenten eingeführt und angewandt. In diesem abschließenden Kapitel werden in Abschnitt 9.1 die Ergebnisse dieser Arbeit zusammengefasst und in Abschnitt 9.2 ein Ausblick auf weiterführende und vertiefende Forschungsaktivitäten gegeben.

9.1 Zusammenfassung und kritische Diskussion der Ergebnisse

Die sichere Implementierung der satellitenbasierten fahrzeugseitigen Ortung wurde bereits in einer Vielzahl vorangegangener Projekte bearbeitet, woraus verschiedene Prototypen entstanden. Diese zeigten, dass eine satellitenbasierte, sichere Ortung im Schienenverkehr generell möglich ist und einen Beitrag zu einem effizienteren Betrieb im Schienenverkehr liefern kann. In den vergangenen Projekten wurde jedoch nicht die Zertifizierung selbst untersucht. Der dargestellte Entwicklungsprozess ist somit ein bedeutender Fortschritt dieser Arbeit gegenüber dem Stand der Technik.

Die Ergebnisse dieser Arbeit wurden mit Vorgehensweisen erreicht, die auch über diese Arbeit hinaus genutzt werden können. So wurde eine Methodik zur Strukturierung von Anwendungen im Verkehrsbereich erstellt und die Sicherheitsnachweisführung generisch betrachtet. Aufbauend auf einer terminologischen Strukturierung wurde die Systemarchitektur der zu entwickelnden Ortungseinheit erstellt. Für die Funktionen der Ortungseinheit werden im Wesentlichen die aus der Strukturierung der Anwendungen von GNSS resultierenden Eigenschaften genutzt. In diese Betrachtung floss außerdem die strukturierte Darstellung der relevanten Normen ein.

In dieser Arbeit konnte von den in Abschnitt 1.3 gestellten Zielen die Erstellung eines sicherheitsgerichteten Entwicklungsprozesses, die konsistente Darstellung der Systemarchitektur und der Nachweis der sicheren Funktionalität erreicht werden. Die erzielten Ergebnisse bilden eine wichtige Grundlage für die mögliche Einführung der satellitenbasierten fahrzeugseitigen Ortung mit SIL 3 auf Nebenstrecken, die keinen Aktivitäten des Fahrers bedarf. Durch den Entfall teurer streckenseitiger Einrichtungen wird eine Vielzahl von Vorteilen ermöglicht, wodurch die Wettbewerbsfähigkeit des Schienenverkehrs gestärkt werden kann. Die resultierenden Vorteile lassen sich in die Kategorien betrieblich, Sicherheit, Instandhaltung, wirtschaftlich und sozial untergliedern und sind in Tabelle 9-1 zusammengefasst.

Tabelle 9-1: Vorteile der Nutzung der satellitenbasierten Ortung im Schienenverkehr

Betriebliche Vorteile	Vorteile für Instandhaltung	Sicherheitsvorteile	Wirtschaftliche Vorteile	Soziale Vorteile
Kontinuierliche Zugortung	Geringere Schäden durch Vandalismus und bspw. Witterung	Erhöhung der Sicherheit	Marktuntersuchungen	Verkürzte Schließzeit von Bahnübergängen
Höhere Flexibilität in der Disposition	Geringerer Instandhaltungsaufwand	Geringeres Risiko menschlicher Fehler	Zielkostenrechnung für Umsetzungsstrategie	Exakter Halt der Züge an Bahnsteigen
Erhöhte Streckenkapazität	Exakte Ortung von zu reparierenden Streckenabschnitten		Kosteneffizienter Betrieb	Verbesserte Information der Fahrgäste
Kompatible Ortung als Basis für Interoperabilität			Umweltfreundliches Fahren durch präzises Beschleunigen und Bremsen	Reduzierung der Reisezeit
				Verbesserte Zuverlässigkeit des Betriebs

9.2 Ausblick

Gewisse Fernziele des Schienenverkehrs, wie bspw. das fahrerlose Fahren, sind durch eine Kombination der in der Anwendung des Funktionsaspekts dargestellten Subfunktionen der sicheren satellitenbasierten Ortung zu realisieren. Die damit verbundene Automatisierung des Schienenverkehrs würde noch viele weitere Vorteile mit sich bringen, bspw. die Reduzierung der Verantwortung des Betriebspersonals und vielfältige Kosteneinsparungen bspw. der Instandhaltungs- oder Betriebskosten, wofür jedoch hohe Anfangsinvestitionen zu tätigen sind.

Die europaweite Zertifizierung ohne nationale Besonderheiten bedarf möglicherweise über diese Arbeit hinausgehender administrativer Maßnahmen. Sie wäre jedoch hilfreich für die grenzüberschreitende, interoperable Durchführung des Schienenverkehrs. Somit wäre es wünschenswert, wenn – wie für 2016 geplant – eine europäische Behörde eine allgemein gültige Zertifizierung ausstellen könnte. Mit der 2004 gegründeten ERA sind die Voraussetzungen dafür geschaffen, jedoch liegen die entsprechenden Kompetenzen nach derzeitiger Rechtslage bei nationalen Behörden. Für eine allgemein gültige Zertifizierung in Europa wäre zunächst eine europaweite Harmonisierung der Regeln und Betriebsverfahren notwendig.