Technische Universität Dresden
Fakultät Verkehrswissenschaften „Friedrich List“
Institut für Luftfahrt und Logistik
Professur Technologie und Logistik des Luftverkehrs

Diplomarbeit

Intermodaler Vergleich des Methodenspektrums im Rahmen von Zulassungsverfahren der jeweiligen Verkehrsmittel

eingereicht von Claudia Bätz

geb. am 24. Oktober in Dresden

Betreuer:
Prof. Dr.-Ing. habil. Hartmut Fricke
Franziska Dieke-Meier
Stefanie Schwartz (Institut für Verkehrssystemtechnik, DLR e. V.)

Dresden, den 31. Januar 2008

Bibliographischer Nachweis

Claudia Bätz
Intermodaler Vergleich des Methodenspektrums im Rahmen von Zulassungsverfahren der jeweiligen Verkehrsmittel
- 2008 - 98 Seiten, 21 Abbildungen, 8 Tabellen

Technische Universität Dresden

Diplomarbeit

Autorenreferat:
Die vorliegende Arbeit untersucht die Zulassungsverfahren und die angewandten Methoden zum Nachweis der Anforderungserfüllung von Luft- und Schienenverkehrsmitteln. In diesem Zusammenhang wird die Übertragbarkeit der Methoden auf andere Verkehrsdomänen untersucht. Letztendlich werden Gestaltungsvorschläge für das Zulassungsverfahren von Schienenfahrzeugen sowie für ein domänenübergreifendes Verfahren aufgezeigt.

Thesen zur Diplomarbeit

- Luftfahrzeuge werden von der Europäischen Luftfahrtagentur (EASA) zugelassen. Diese Zulassung wird von allen Mitgliedstaaten der Europäischen Union anerkannt.
- Schienenfahrzeuge werden von dem deutschen Eisenbahn-Bundesamt (EBA) zugelassen. Sollen die Fahrzeuge grenzüberschreitend eingesetzt werden, muss die Einhaltung der Anforderungen der Technischen Spezifikationen für Interoperabilität (TSI) nachgewiesen werden. Das erfolgt durch eine EG-Prüferklärung einer benannten Stelle.
- Zum Nachweis der Anforderungserfüllung werden verschiedene Methoden eingesetzt. Im Luftverkehr wird den Anwendern ein beispielhaftes Verfahren zur Verfügung gestellt. Im Schienenverkehr ist die Auswahl der Methoden den Herstellern überlassen.
- Für die Zulassung von Luftfahrzeugen wird ein Risikoakzeptanzkriterium vorgegeben, das aus statistischen Unfallauswertungen bestimmt wurde. Für den Schienenverkehr wird kein Risikoakzeptanzprinzip festgelegt. Die Anwender müssen selbst eines auswählen. Es gibt Bestrebungen, ein einheitliches Kriterium für den Schienenverkehr zu entwickeln.
- Die meisten angewendeten Methoden werden nicht nur in den untersuchten Verkehrsdomänen eingesetzt sondern auch in vielen anderen Bereichen. Im Luftverkehr werden drei spezielle Methoden genutzt: das Functional Hazard Assessment (FHA), Preliminary System Safety Assessment (PSSA) und System Safety Assessment (SSA). Zumindest die Übertragung des FHA und des PSSA auf den Schienenverkehr ist denkbar.

Inhaltsverzeichnis

Tabellenverzeichnis

Abbildungsverzeichnis

Abkürzungsverzeichnis

AEG Allgemeines Eisenbahngesetz

ALARP As Low As Reasonably Practicable – So niedrig wie vernünftigerweise anwendbar

AMC Acceptable Means of Compliance – Annehmbare Nachweisverfahren

ARP Aerospace Recommended Practice – Luftfahrtstandards der Society of Automotive Engineers (SAE)

BEGebV Verordnung über die Gebühren und Auslagen für Amtshandlungen der Eisenbahnverkehrsverwaltung des Bundes

BMVBS Bundesministerium für Verkehr, Bau und Stadtentwicklung

CCA Common Cause Analysis

CCFA Common Cause Failure Analysis

CEN Europäisches Komitee für Normung

CENELEC Europäisches Komitee für Elektrotechnische Normung

CMA Common Mode Analysis

COTIF Übereinkommen über den internationalen Eisenbahnverkehr

CS Certification Specification – Zulassungsspezifikation

CTM Cause Tree Method – Fehlerbaumanalyse

DAL Development Assurance Level – Entwicklungsabsicherungsstufe

DIN Deutsches Institut für Normung

DOA Design Organisation Approval – Zulassung als Entwicklungsbetrieb

EASA European Aviation Safety Agency – Europäische Luftfahrtagentur

Abkürzungsverzeichnis

EBA Eisenbahn-Bundesamt

EBC Eisenbahn-Cert – Benannte Stelle Interoperabilität beim Eisenbahn-Bundesamt

EBO Eisenbahn-Bau- und Betriebsordnung

ECAC European Civil Aviation Conference – Europäische Zivilluftfahrtkonferenz

EdB Eisenbahnen des Bundes

EG Vertrag zur Gründung der Europäischen Gemeinschaft

ERA European Railway Agency – Europäische Eisenbahnagentur

ERTMS European Rail Traffic Management System – Europäisches System der Zugsteuerung und Zugsicherung

ETA Event Tree Analysis – Ereignisbaumanalyse

ETCS European Train Control System – Europäisches Zugkontrollsystem

EU Europäische Union

EUROCAE European Organisation for Civil Aviation Equipment

FAA Federal Aviation Administration – Luftfahrtbehörde der USA

FAR Federal Aviation Requirement – Standard der FAA

FHA Functional Hazard Assessment

FMEA Failure Mode and Effects Analysis – Fehler-Möglichkeits- und Einfluss-Analyse

FMECA Failure Mode and Effects and Criticality Analysis – Fehler-Möglichkeits-, Einfluss- und Kritikalitäts-Analyse

FTA Fault Tree Analysis – Fehlerbaumanalyse

GAMAB Globalement Au Moins Aussi Bon – Insgesamt mindestens genauso gut

GSM-R Global System for Mobile Communications - Rail – Eisenbahnfunksystem

H Hazard Rate – Gefährdungsrate

HAZOP Hazards and Operability Study – Gefahren- und Operabilitätsstudie

ICAO International Civil Aviation Organization – Internationale Zivilluftfahrtorganisation

IEC Internationale Elektrotechnische Kommission

IK Interoperabilitätskomponente

ISO International Organization for Standardization – Internationale Normungsorganisation

JAA Joint Aviation Authorities – Vereinigung europäischer Luftfahrtbehörden

JAR Joint Aviation Requirement – Standard der JAA

LBA Luftfahrt-Bundesamt

LuftVG Luftverkehrsgesetz

MEM Minimum Endogenous Mortality – Minimale Endogene Sterblichkeit

MGS Mindestens gleiche Sicherheit

OTIF Zwischenstaatliche Organisation für den internationalen Eisenbahnverkehr

PHA Preliminary Hazard Analysis – Vorbereitende Gefährdungsanalyse

Pkw Personenkraftwagen

PRA Particular Risk Assessment

PSSA Preliminary System Safety Assessment

RAC-TS Risk Acceptance Criterion for Technical Systems – Risikoakzeptanzkriterium für technische Systeme

RAMS Reliability, Availability, Maintainability and Safety – Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit und Sicherheit

RPZ Risikoprioritätszahl

RTCA Radio Technical Commission for Aeronautics - US-amerikanische Normungsorganisation

SAE Society of Automotive Engineers – Normungsorganisation für Verkehrsbereiche

Abkürzungsverzeichnis

SESAR Single European Sky Air Traffic Management Research

SIL Sicherheitsintegritätslevel

SSA System Safety Assessment

TCDS Type-certificate Data Sheet – Datenblatt der Musterzulassung

TEIV Transeuropäische-Eisenbahn-Interoperabilitätsverordnung

THR Tolerable Hazard Rate – Tolerierbare Gefährdungsrate

TSI Technische Spezifikationen für Interoperabilität

UIC Internationaler Eisenbahnverband

UNIFE Verband europäischer Eisenbahnhersteller

VwV Abnahme § 32 Verwaltungsvorschrift für die Abnahme von Eisenbahnfahrzeugen gemäß § 32 Abs. 1 EBO im Zuständigkeitsbereich des Eisenbahn-Bundesamt

ZSA Zonal Safety Analysis

Glossar

Anerkannte Regeln der Technik

„technische Festlegung die von einer Mehrheit repräsentativer Fachleute als Wiedergabe des Standes der Technik angesehen wird“ [11]

Ausfall infolge gemeinsamer Ursachen (Common Cause Failure)

Der Ausfall mehrerer, als voneinander unabhängig betrachteten Komponenten, aufgrund einer gemeinsamen Ursache.

Norm

„Dokument, das mit Konsens erstellt und von einer anerkannten Institution angenommen wurde und das für die allgemeine und wiederkehrende Anwendung Regeln, Leitlinien oder Merkmale für Tätigkeiten oder deren Ergebnisse festlegt, wobei ein optimaler Ordnungsgrad in einem gegebenen Zusammenhang angestrebt wird“ [11]

Risiko

„Komination aus Häufigkeit oder Wahrscheinlichkeit und den Folgen eines spezifizierten gefährlichen Ereignisses.“ [14]

Stand der Technik

„entwickeltes Stadium der technischen Möglichkeiten zu einem bestimmten Zeitpunkt, soweit Produkte, Prozesse und Dienstleistungen betroffen sind, basierend auf entsprechenden gesicherten Erkenntnissen von Wissenschaft, Technik und Erfahrung“ [11]

1 Einleitung

1.1 Motivation

Bevor Verkehrsmittel eingesetzt werden können, müssen die Hersteller in einem Zulassungsverfahren den Behörden nachweisen, dass alle Anforderungen erfüllt wurden und dass die Fahrzeuge für den sicheren Betrieb geeignet sind. Besonders bei grenzüberschreitendem Verkehr oder Verkauf in verschiedene Staaten bedeutet das für die Hersteller Mehraufwand in wirtschaftlicher und organisatorischer Hinsicht, falls für jedes Land eine eigene Zulassung erlangt werden muss.

Je später Fehler im Fahrzeugentwurf entdeckt werden, umso schwieriger und teurer wird ihre Beseitigung. Das kann außerdem mit zeitlichen Verzögerungen verbunden sein. Die Hersteller von Verkehrsmitteln wenden deshalb frühzeitig Verfahren an, um die Einhaltung der Anforderungen zu überprüfen. Mit zunehmender Komplexität der Systeme werden diese Nachweise immer schwieriger. Beim Bau des Airbus A380 mussten die Flügel verstärkt werden, nachdem sie im Test der erforderlichen Belastung nicht standhalten konnten[35].

Im Schienenverkehr wurden in den letzten Jahren Technische Spezifikationen für Interoperabilität (TSI) eingeführt, die einen einheitlichen Mindeststandard für den Eisenbahnverkehr in der Europäischen Union gewährleisten sollen. Die diesbezüglich veröffentlichten Normen und Richtlinien enthalten jedoch keine speziellen Vorgaben, wie diese Ziele erreicht werden sollen. Deswegen sollen andere Zulassungsverfahren untersucht und die Übertragbarkeit der verwendeten Methoden untersucht werden.

1.2 Zielstellung

In dieser Arbeit sollen die verwendeten Methoden zum Nachweis der Aufgabenerfüllung während der Zulassungsverfahren von Verkehrsmitteln untersucht werden. Dazu werden

zuerst die Eigenschaften und besonderen Merkmale der einzelnen Verkehrsmittel betrachtet. Anschließend erfolgt eine Untersuchung der anzuwendenden Gesetze und Regelwerke für die Zulassungsverfahren. Danach werden die Verfahren untersucht und verglichen. Der Schwerpunkt liegt auf den Methoden zum Nachweis der Erfüllung der Anforderungen. Dabei soll die Übertragbarkeit der Methoden auf den Schienenverkehr bewertet werden. Zum Schluß sollen Gestaltungsvorschläge für das Zulassungsverfahren von Schienenfahrzeugen sowie ein domänenübergreifendes Verfahren gegeben werden.

2 Besondere Merkmale und technische Anforderungen der Verkehrsmittel

Verkehr kann unterteilt werden in einen zivilen und einen militärischen Sektor. Der zivile Bereich setzt sich aus dem kommerziellen sowie nicht-kommerziellen Verkehr zusammen. Zu ersterem gehört der öffentliche Verkehr, der Privatverkehr hingegen zum nicht-gewerblichen Verkehr. Diese Differenzierung ist wichtig für die Betrachtung der Risikoakzeptanz, welche mit selbsteingegangenen und beeinflussbaren Risiken steigt. Der Vergleich des motorisierten Individualverkehrs mit dem öffentlichen Personenverkehr macht diese unterschiedliche Bewertung besonders deutlich. Dem hohen Unfallrisiko auf der Straße wird eine viel geringere Rolle beigemessen als dem niedrigeren Unfallrisiko im Luft- und Schienenverkehr. In diesen Bereichen erhalten seltene Ereignisse mit vielen Toten in der Öffentlichkeit eine sehr große Aufmerksamkeit, während die häufigen Verkehrsunfälle im Individualverkehr auf der Straße (PKW, Motorrad, Fahrrad, Fußgänger) mit wenigen Opfern kaum noch wahrgenommen werden. Deshalb erwartet die Bevölkerung für öffentliche Verkehrsmittel einen besonders hohen Sicherheitsstandard, der mittels Zulassungsverfahren erreicht werden soll. Zum Verständnis der Hintergründe und Probleme ist es aus diesem Grund wichtig, die besonderen Merkmale und technischen Anforderungen der unterschiedlichen Verkehrsmittel zu kennen. Das folgende Kapitel wird auf diese Punkte für den Luft-, Schienen- und Straßenverkehrs genauer eingehen.

2.1 Luftverkehr

Nach den ersten motorisierten Flugversuchen Anfang des 20. Jahrhunderts hat sich der Luftverkehr nach dem Zweiten Weltkrieg aufgrund des enormen Fortschritts der Technik zu einem Massenverkehrsmittel entwickelt. Besonders durch die Einführung von Strahltriebwerken konnten die Reisegeschwindigkeiten, die erreichbaren Entfernungen sowie die Zuladung erhöht werden. Der Luftverkehr hat damit bei der Beförderung von Personen und Fracht besonders international an Bedeutung gewonnen. Für einen reibungslosen grenzüberschreitenden Flugverkehr sind deshalb einheitliche Anforderungen an die Infrastruktur, die Flughäfen und Flugsicherungseinrichtungen, notwendig. Aufgrund der geringen Anzahl an Verkehrsflugzeugherstellern werden die gleichen Typen in vielen verschiedenen Ländern betrieben. Die Luftfahrt kann in einen militärischen und einen zivilen Bereich mit der Verkehrsluftfahrt und der allgemeinen Luftfahrt unterteilt werden. Die Anforderungen der Verkehrsfliegerei sind hierbei höher als die der allgemeinen Luftfahrt.

Sowohl Luftverkehrsgesellschaften als Betreiber, als auch Luftfahrzeugführer, Fluglotsen und technisches Personal benötigen spezielle Lizenzen. Für die Koordinierung und Überwachung des sicheren Flugbetriebs ist die Flugsicherung zuständig. Ein Luftfahrzeug verfügt bei seiner Bewegung in der Luft über sechs Freiheitsgrade. Der Luftfahrzeugführer ist somit in der Lage, Hindernissen bei rechtzeitiger Erkennung auszuweichen, es ist ihm aber nicht möglich, einfach anzuhalten. Zusätzlich verkehren Zivilflugzeuge in für Menschen lebensfeindlichen Höhen von bis zu 11 Kilometern. Die Geschwindigkeiten erreichen bereits beim Start 300 $^{km}/_{h}$ und im Reiseflug können sie auch 900 $^{km}/_{h}$ übersteigen. Bei Problemen muss das Flugzeug bis zur Landung in einem sicheren Zustand gehalten oder wieder versetzt werden. Bei einem Absturz sind sowohl Verluste von Menschenleben als auch hoher materieller Schaden zu erwarten. Dies gilt nicht nur für das Flugzeug und seine Insassen sondern auch für Personen und Einrichtungen am Boden.

Der europäische Luftraum wird durch eine Vielzahl nationaler Flugsicherungen kontrolliert, mit unterschiedlichen Strukturen und Technik. Um den Anforderungen des wachsenden europäischen Luftverkehrs gerecht zu werden, soll in dem Projekt Single European Sky Air Traffic Management Research (SESAR) ein gemeinsames Flugsicherungsprogramm implementiert werden. Zu diesem Zweck haben sich zivile und militärische Flugsicherungen, Gesetzgeber, Industrie, Betreiber sowie Nutzer zusammengeschlossen.[19]

2.2 Schienenverkehr

Die erste Zugverbindung wurde bereits 1835 in Deutschland in Betrieb genommen. Seit dieser Zeit hat sich der Schienenverkehr sehr stark auf nationaler Ebene weiterentwickelt, infolgedessen jeder Staat heute eine eigene Infrastruktur hat, die unter anderem gekennzeichnet ist durch verschiedene Spurweiten, Lichtraumprofile, Stromversorgungssysteme und Zugsicherungstechnik. Dies erschwerte in der Vergangenheit oftmals den grenzüberschreitenden Verkehr. Aufgrund der Harmonisierungsbestrebungen der Europäischen Union hinsichtlich der Verkehrsnetze für eine Förderung des Binnenmarkts hat sich diese Situation mittlerweile positiv entwickelt[1]. In diesem Kontext erließ die Europäische Union (EU) Interoperabilitätsrichtlinien und Technische Spezifikationen für Interoperabilität (TSI). Es soll z. B. ein gemeinsames europäisches Zugsicherungs- und Zugkontrollsystem (ERTMS) aufgebaut werden, das aus dem Zugkontrollsystem (ETCS) und dem Eisenbahnfunksystem (GSM-R) besteht.

Die Nutzung des Schienenverkehrs erfolgt nur im kommerziellen Bereich. Triebfahrzeugführer, Sicherungspersonal und Betreiber benötigen für die Ausübung ihrer Tätigkeiten spezielle Lizenzen. Die Fahrzeuge müssen in Bezug auf die vorhandene Infrastruktur zugelassen sein. Auf Grund der schienengebundenen Spurführung erfolgt die Bewegung auf einer Linie. Es sind keine Steuermöglichkeiten für den Triebfahrzeugführer vorhanden. Der Fahrweg wird durch die Weichenstellung bestimmt. Bedingt durch die niedrige Reibung zwischen Schiene und Rad, der hohen Massen und Geschwindigkeiten sind Bremswege von einem Kilometer vorhanden. Folglich ist es nicht möglich, Hindernissen auf der Strecke auszuweichen oder unmittelbar zu stoppen. Der Weg muss deshalb vorher gesichert und freigegeben werden. Dies erfolgt durch die Fahrdienstleiter in den Stellwerken oder Betriebszentralen. Bei einem Unfall können mehrere hundert Insassen und Menschen in der Umgebung betroffen sein. Meistens ist damit ein großer materieller Schaden verbunden.

2.3 Straßenverkehr

Wir alle sind Teilnehmer am Straßenverkehr, ob selbst als Fahrer, Insasse oder Fußgänger. Im Jahr 2004 lag der Motorisierungsgrad in Deutschland bei 550 Personenkraftwagen (Pkw)

[1] vgl. EG [16], Art. 154

pro 1000 Einwohner [34]. Damit hat statistisch betrachtet mehr als jeder zweite Deutsche ein eigenes Auto. Die Straße wird zur Beförderung von Personen wie auch Fracht genutzt. Das gilt für den zivilen und militärischen Bereich.

Die grenzüberschreitende Pkw-Fahrt ist aus technischer Sicht kein Problem. Gleichwohl müssen verschiedene Verkehrsregeln im Ausland beachtet werden. Das gravierendste Beispiel in diesem Zusammenhang ist der Links- und Rechtsverkehr. Die Fahrbewegung verläuft in der Fläche. Bei rechtzeitiger Erkennung von Hindernissen kann der Fahrer zur Seite ausweichen oder bremsen, um Schäden zu vermeiden oder zu reduzieren. Bei einem Unfall mit einem Pkw sind nur wenige Personen betroffen, bei einem Bus können es auch mehrere Dutzend sein. Oft sind aber zusätzlich andere Verkehrsteilnehmer, wie z. B. Radfahrer oder Fußgänger beteiligt.

Tabelle 2.1: Vergleich der Eigenschaften der Verkehrsmittel des Luft-, Schienen- und Straßenverkehrs

Eigenschaft	Verkehrsdomäne		
	Luftverkehr	Schienenverkehr	Straßenverkehr
Verkehrsmittel	Luftfahrzeug	Schienenfahrzeug	Automobil
Bewegung	im Raum (3-D)	Linie (1-D)	in der Fläche (2-D)
Infrastruktur	Flugplatz, Flugsicherungsanlagen	Schienennetz, Bahnhof, Zugsicherungsanlagen	Straßen, Lichtsignalanlagen
Fahrzeugführer Sicherungspersonal	Pilot Fluglotse	Triebfahrzeugführer Fahrdienstleiter, Betriebsleiter	Fahrer keines
Bremsweg	in Luft nicht möglich, am Boden bis zu Landebahnlänge	bis zu 1 Kilometer	relativ kurz
Umweltbedingung	lebensfeindlich (Höhe) normal (Bodennähe)	normal	normal

2.4 Zusammenfassung

Luft- und Schienenverkehr zählen zum öffentlichen Verkehr. Der Straßenverkehr hingegen gehört zum Individualverkehr. Dadurch ergeben sich Unterschiede in der Risikowahrnehmung und -akzeptanz und daraus folgend in den Anforderungen an die Sicherheit der Verkehrsmittel.

Bei dem Unfall eines Flugzeugs oder Zuges sind die Schäden beträchtlich größer und mehr Menschen betroffen als bei einem Autounfall. Es gibt auch weitere Ähnlichkeiten zwischen dem Luft- und Schienenverkehr. In beiden Bereichen können die Verkehrsmittel bei Problemen nicht schnell stoppen, sondern das System muss bis zum nächstmöglichen Halt in einen sicheren Zustand versetzt werden. Tabelle 2.1 führt die wichtigsten Eigenschaften eines Flugzeugs, Schienenfahrzeugs und Automobils auf. Im Rahmen dieser Arbeit werden die Zulassungsverfahren im Luft- und Schienenverkehr genauer untersucht.

3 Rahmenbedingungen für die Zulassung

Für die Zulassung von Verkehrsmitteln wichtige Regelwerke sind Gesetze, Verordnungen, Richtlinien, Empfehlungen und Standards. Diese unterscheiden sich jeweils in ihrer Verbindlichkeit, was in Abbildung 3.1 dargestellt ist. An oberster Stelle stehen die Gesetze. Da sie meist nur allgemeine Angaben liefern, gehen die Verordnungen weiter ins Detail. Eine Stufe tiefer stehen Durchführungsverordnungen und Verwaltungsvorschriften. Die Basis bilden Normen, Standards und branchenspezifische Richtlinien. Die Verbindlichkeiten für europäische Veröffentlichungen sind im *Vertrag zur Gründung der Europäischen Gemeinschaft (EG)* festgelegt. Danach sind europäische Verordnungen in den Mitgliedstaaten verbindlich und unmittelbar gültig[1].

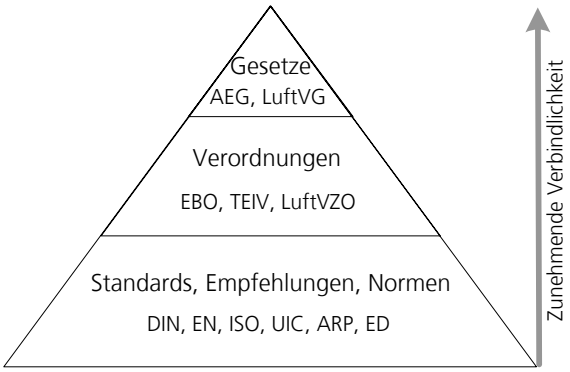

Abbildung 3.1: Verbindlichkeit der unterschiedlichen Regelwerke

Für den Betrieb eines Verkehrsmittels ist eine vorherige Zulassung erforderlich. Sowohl im Luft- als auch im Schienenverkehr wurde das Verfahren zweigeteilt. Es ist zu unterscheiden zwischen einer Zulassung für die Musterbauart, welche die Einhaltung der rechtlichen

[1] vgl. EG [16], Art. 249

Vorgaben bescheinigt sowie einer Betriebszulassung für die einzelnen Fahrzeuge, die einem zugelassenen Typ entsprechen. In der vorliegenden Arbeit wird der Begriff Zulassung auf die Musterzulassung von Flugzeugen und Eisenbahnen bezogen, wenn es nichts anderes angegeben ist.

Das folgende Kapitel beschreibt die wichtigsten internationalen, europäischen (EU) und nationalen zulassungsrelevanten Vorschriften sowie Normen. Zusätzlich zu den hier aufgeführten Bestimmungen gelten noch viele weitere, z. B. für den Arbeits-, Brand- und Umweltschutz, die ebenfalls eingehalten werden müssen. Eine Beschreibung der Zulassungsverfahren folgt in Kapitel 4.

3.1 Luftverkehr

Die Zulassung für einen bestimmten Flugzeugtyp heißt Musterzulassung. Sie wird dem Entwicklungsbetrieb, der meistens auch der Hersteller ist, erteilt. Für der operativen Einsatz benötigt der Betreiber zudem eine Lufttüchtigkeits- bzw. Verkehrszulassung. Abbildung 3.2 liefert eine Zusammenfassung der wichtigsten anzuwendenden Gesetze und Verordnungen.

3.1.1 Gesetzgebung

International

Die größte Bedeutung auf internationaler Ebene hat die 1944 gegründete Internationale Zivilluftfahrtorganisation (ICAO) mit dem *Abkommen über die internationale Zivilluftfahrt (Chicagoer Abkommen)*. Der heutigen Unterorganisation der Vereinten Nationen gehören derzeit 190 Staaten an[2]. Sie hat es sich unter anderem zum Ziel gesetzt, „die Grundsätze und die Technik der internationalen Luftfahrt zu entwickeln sowie die Planung und Entwicklung des internationalen Luftverkehrs zu fördern“ [25, Art. 44]. Dies umfasst u. a. die Bereiche Technik, Betrieb und Personal. Für eine größtmögliche Einheit auf diesen Gebieten veröffentlicht die ICAO Richtlinien, Empfehlungen und Verfahren, die Mindestanforderungen in den behandelten Bereichen darstellen, in 18 Anhängen (Annexe) zum Chicagoer Abkommen. Davon sind für die Zulassung von Luftfahrzeugen besonders die Annexe 8 *Airworthiness of Aircraft* und 16 *Environmental Protection* von Bedeutung.

[2] `http://www.icao.int/cgi/statesDB4.pl?en`, Abruf:11.09.2007

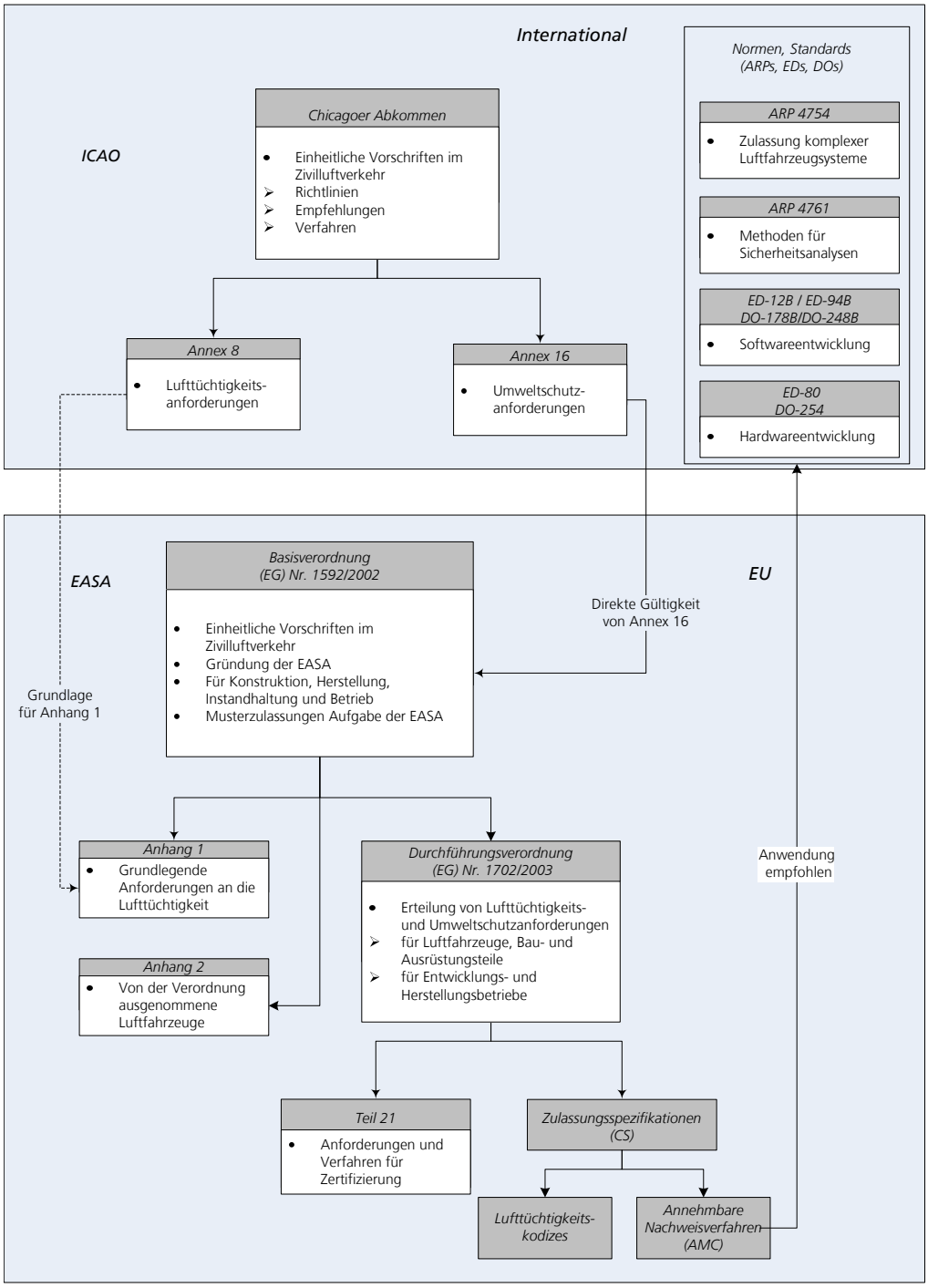

Abbildung 3.2: Darstellung der wichtigsten rechtlichen Grundlagen für die Musterzulassung von Verkehrsflugzeugen

Die Inkraftsetzung der durch die ICAO erlassenen Dokumente erfordert eine separate Umsetzung in das nationale Recht der Mitgliedstaaten, wozu diese sich mit der Unterzeichnung des Chicagoer Abkommens verpflichtet haben. Eine Abänderung oder Nichteinhaltung muss der ICAO innerhalb 60 Tagen angezeigt werden[3]. Die Vorgaben stellen dabei lediglich grundlegende Anforderungen für einen wirtschaftlichen und sicheren Flugbetrieb dar, die in sehr vielen verschiedenen nationalen Umsetzungen resultieren. Auf Basis des Abkommens erteilte Lufttüchtigkeitszeugnisse müssen von allen Mitgliedsländern anerkannt werden[4]. Für Musterzulassungen existiert derzeit noch keine derartige Regelung. Aufgrund wirtschaftlichen und organisatorischen Mehraufwandes drängen die Hersteller jedoch schon seit langem auf ein einheitliches und gegenseitig anerkanntes Verfahren. Aus diesem Grund begannen die Federal Aviation Administration (FAA) und die Joint Aviation Authorities (JAA), ihre Anforderungen und Verfahren, die in den meisten Staaten direkt angewandt werden oder als Grundlage dienen, zu prüfen und anzugleichen[5]. Dieser Prozess wurde nach Gründung der Europäischen Luftfahrtagentur (EASA) von dieser fortgesetzt.

Europa

Als sich mehrere europäische Staaten zum Bau des gemeinsamen Verkehrsflugzeuges Airbus zusammenschlossen, bildete die Europäische Zivilluftfahrtkonferenz (ECAC) 1970 eine Arbeitsgruppe für die Erstellung einheitlicher Bauvorschriften. 20 Jahre später entstand daraus die Joint Aviation Authorities (JAA), welche sich aus mehreren nationalen europäischen Luftfahrtbehörden zusammensetzte. Der ECAC und JAA gehören derzeit 42 Mitgliedstaaten an[6]. Mit der Veröffentlichung der Joint Aviation Requirements (JARs) sollten vergleichbare Vorgaben für den Luftverkehr geschaffen werden. Die fehlende Gesetzgebungsbefugnis der JAA machte eine Umsetzung in nationales Recht notwendig. Dabei konnten die Staaten einzelne Änderungen vornehmen. Das Ergebnis waren diverse Fassungen der einzelnen JARs. [30]

Für die Gewährleistung eines hohen und einheitlichen Sicherheitsniveaus in der Zivilluftfahrt entschloss sich die Europäische Union (EU) im Zuge des Subsidaritätsprinzips tätig

[3] vgl. ICAO [25], Art. 38

[4] vgl. ICAO [25], Art. 33

[5] vgl. Weber u. Holderbach [47]

[6] ECAC `http://www.ecac-ceac.org/index.php?content=lstsmember&idMenu=1&idSMenu=10`, Abruf: 13.08.2007, JAA, `http://www.jaat.eu/introduction/introduction.html`, Abruf: 13.08.2007

zu werden. Damit ist es der EU gestattet, auf Gemeinschaftsebene tätig zu werden, sollten Ziele des EU-Vertrags nicht auf Ebene der Mitgliedstaaten durchgesetzt werden können[7]. Zu diesem Zweck erließ das Europäische Parlament die *Verordnung (EG) Nr. 1592/2002 zur Festlegung gemeinsamer Vorschriften für die Zivilluftfahrt und zur Errichtung einer Europäischen Agentur für Flugsicherheit* (EASA). Diese sowie weitere EU-Verordnungen gelten aufgrund des europäischen Rechts unmittelbar und in der vorliegenden Form in allen Mitgliedstaaten. Damit wurde eine einheitliche Rechtsgrundlage in der gesamten Gemeinschaft geschaffen. Die neugegründete Europäische Luftfahrtagentur (EASA) nimmt auf dem Gebiet der Musterzulassungen „im Namen der Mitgliedstaaten die Funktionen und Aufgaben des Entwurfs-, Herstellungs- oder Eintragungsstaats wahr" [42, Art. 15, Satz 1]. Die EASA kann sich bei diesen Aufgaben der Hilfe der nationalen Luftfahrtbehörden oder qualifizierter Prüfstellen bedienen[8]. Als Vorlage für die von der EASA veröffentlichen Regelungen dienten die JARs, die als Anhänge zu den neuen Verordnungen in oftmals nur leicht abgewandelter Form veröffentlicht wurden. Obwohl die EASA eine EU-Organisation ist, können auch andere europäische Nicht-EU-Mitgliedstaaten die Regelungen entsprechend spezieller Vereinbarungen übernehmen[9]. Neben den 27 EU-Staaten gehören ihr noch Island, Liechtenstein, Norwegen und die Schweiz an[10]. Die beiden wichtigsten Verordnungen für die Luftfahrtgerätezulassung sind die VO 1592/2002 [42] sowie ihre Durchführungsverordnung VO 1702/2003 [43] mit dem Anhang Teil 21. Die *Verordnung (EG) Nr. 1592/2002 des Europäischen Parlaments und des Rates vom 15. Juli 2002 zur Festlegung gemeinsamer Vorschriften und zur Errichtung einer Europäischen Agentur für Flugsicherheit* soll einen hohen Sicherheitsstand in der Zivilluftfahrt gewährleisten[11]. Ihr Geltungsbereich wird in Artikel 1a wie folgt beschrieben:

> „die Konstruktion, die Herstellung, die Instandhaltung und den Betrieb von luftfahrttechnischen Erzeugnissen, Teilen und Ausrüstungen sowie für Personen und Organisationen, die mit der Konstruktion, Herstellung und Instandhaltung dieser Erzeugnisse, Teile und Ausrüstungen befasst sind". [42, Art. 1a]

Sie gilt nicht für die Bereiche Polizei, Zoll und Militär sowie die in Anhang II aufgeführten

[7] vgl. EG [16], Art. 5
[8] vgl. VO 1592/2002 [42], Art. 15, Satz 1
[9] vgl. VO 1592/2002 [42], Art. 55
[10] Banal [5]
[11] vgl. VO 1592/2002 [42], Gründe

Luftfahrzeuge, z. B. Forschungsflugzeuge, historische Luftfahrzeuge und Einzelstücke[12]. Neben technischen Aspekten werden auch die des Umweltschutzes berücksichtigt. Durch die Vereinheitlichung der Regelungen sollen die erteilten Musterzulassungen von allen Mitgliedstaaten anerkannt werden, wodurch doppelte Verfahren vermieden werden[13]. Die für den Betrieb von Luftfahrzeugen notwendigen Verkehrszulassungen obliegen weiter dem Zuständigkeitsbereich der nationalen Luftfahrtbehörden. Der in diesem Zusammenhang wichtige Begriff *Zulassung* wird dabei definiert als:

> „jede Form der Anerkennung, dass ein Erzeugnis oder eine Ausrüstung, eine Organisation oder eine Person die geltenden Vorschriften, einschließlich der Bestimmungen dieser Verordnung und ihrer Durchführungsverordnungen, erfüllt, sowie die Ausstellung des entsprechenden Zeugnisses, mit dem diese Übereinstimmung bescheinigt wird". [42, Art. 3e]

Die Musterzulassung gilt als Nachweis der Erfüllung der Lufttüchtigkeitsanforderungen, welche in Anhang I aufgeführt werden. Neben den Luftfahrzeugen und einzelnen Komponenten bedürfen auch die beteiligten Entwicklungs- und Herstellungsbetriebe einer Zulassung.

Die erlassenen Durchführungsbestimmungen sollen

> „a) dem Stand der Technik und den bestbewährten Verfahren auf dem Gebiet der Lufttüchtigkeit entsprechen;
>
> b) den weltweiten Erfahrungen im Luftfahrtbetrieb sowie dem wissenschaftlichen und technischen Fortschritt Rechnung tragen;
>
> c) eine unmittelbare Reaktion auf erwiesene Ursachen von Unfällen und ernsten Zwischenfällen ermöglichen." [42, Art. 5, Satz (5)]

Damit soll ein hohes Sicherheitsniveau gewährleistet werden. Während die Lufttüchtigkeitsanforderungen des ICAO-Annex 8 die Grundlage für die in Anhang 1 aufgelisteten Punkte darstellt, wird bezüglich des Umweltschutzes direkt auf den Annex 16 des Chicagoer Abkommens verwiesen, der zu erfüllen ist[14].

Die *VERORDNUNG (EG) Nr. 1702/2003 DER KOMMISSION vom 24. September 2003 zur Festlegung der Durchführungsbestimmungen für die Erteilung von Lufttüchtigkeits-*

[12] vgl. VO 1592/2002 [42], Art. 1, Satz 2; Art. 4, Satz 2
[13] vgl. VO 1592/2002 [42], Art. 2
[14] vgl. VO 1592/2002 [42], Art. 6

und Umweltzeugnissen für Luftfahrzeuge und zugehörige Erzeugnisse, Teile und Ausrüstungen sowie für die Zulassung von Entwicklungs- und Herstellungsbetrieben enthält „die gemeinsamen technischen Anforderungen und Verwaltungsverfahren für die Erteilung von Lufttüchtigkeits- und Umweltzeugnissen für Erzeugnisse, Teile und Ausrüstungen“ [43, Art. 1, Satz (1)]. Dazu gehört auch der Anhang *Teil 21 - Zertifizierung von Luftfahrzeugen und zugehörigen Produkten, Bau- und Ausrüstungsteilen und von Entwicklungs- und Herstellungsbetrieben*, der die entsprechenden Anforderungen und Verfahren enthält[15]. Abschnitt B des Teils 21 beschäftigt sich mit den Musterzulassungen. Für die Zulassung durch die EASA muss der Entwickler nachweisen, dass er die vorgegebenen Anforderungen und Umweltschutzbestimmungen erfüllt hat[16]. Der Inhaber der Musterzulassung ist verpflichtet, einen sicheren Betrieb seitens der Technik zu ermöglichen. Dazu muss er u. a. Handbücher und Instandhaltungsanweisungen erstellen sowie bei später auftretenden Problemen Anweisungen zur Behebung bereitstellen[17]. Genauere Vorgaben veröffentlicht die EASA in Zulassungsspezifikationen (CS), die aus zwei Teilen bestehen, den *Lufttüchtigkeitskodizes (Airworthiness Codes)* und den *Acceptable Means of Compliance (AMC)* . Die AMCs enthalten Angaben zur Erfüllung der im ersten Teil benannten Anforderungen an das Luftfahrtgerät. Die wichtigsten Zulassungsspezifikationen für die Verkehrsflugzeugzulassung sind die *Certification Specifications for Large Aeroplanes (CS-25)* sowie die *General Acceptable Means of Compliance for Airworthiness of Products, Parts and Appliances (AMC-20)*. Es gibt außerdem noch viele andere Zulassungsspezifikationen, z. B. die *CS-36 Aircraft Noise*, *CS-AWO - All Weather Operations* und *CS-Definitions*. In Zusammenarbeit mit der Federal Aviation Administration (FAA) wurden die entsprechenden Werke untereinander angepasst. In den AMCs wird auf gültige Normen verwiesen. Laut der CS-25 [9] steht es den Antragstellern frei, den in den Zulassungsspezifikationen veröffentlichten Verfahren zu folgen. Bei korrekter Anwendung werden diese durch die Behörden anerkannt. Für andere Wege muss der Nachweis der Nutzbarkeit erbracht werden.

Deutschland

Im Geltungsbereich der Verordnung (EG) Nr. 1592/2002 übernimmt die EASA die Aufgaben der nationalen Luftfahrtbehörden. Die deutsche Luftfahrtbehörde, das Luftfahrt-Bundesamt

[15] vgl. VO 1702/2003 [43], Art. 1
[16] vgl. VO 1702/2003 [43], 21A.20
[17] vgl. VO 1702/2003 [43]

(LBA) unterstützt die Agentur bei dieser Aufgabe[18]. Für den nicht von der oben genannten Verordnung abgedeckten Bereich gilt das deutsche Recht. Weil die in dieser Arbeit betrachtete Musterzulassung von Verkehrsflugzeugen in den Zuständigkeitsbereich der EASA fällt, soll an dieser Stelle nicht weiter auf das deutsche Luftverkehrsgesetz (LuftVG) und seine Verordnungen eingegangen werden.

3.1.2 Wichtige Normen und Standards

Neben den gesetzlichen Vorgaben existieren zusätzlich branchenspezifische Standards. Die wichtigsten sind in Abbildung 3.2 dargestellt. Bedeutende Organisationen für die Erstellung von Luftfahrtnormen sind die:

- Society of Automotive Engineers (SAE) International,
- European Organisation for Civil Aviation Equipment (EUROCAE).

Die EUROCAE beschäftigt sich vorrangig mit Standards für technische Flugzeugsysteme [18]. Dabei arbeitet sie stellenweise eng mit ihrem amerikanischen Gegenstück, der Radio Technical Commission for Aeronautics (RTCA) zusammen, was in der Veröffentlichung vergleichbarer Empfehlungen beider Organisationen deutlich wird. Besonders zu erwähnen sind die beiden Dokumente

- *ED-12B Software Considerations in Airborne Systems and Equipment Certification* (DO-178B der RTCA) und
- *ED-80 Design Assurance Guidance for Airborne Electronic Hardware* (DO-254 der RTCA).

Als Zusatz zur ED-12B/DO-178B wurde die ED-94B/DO-248B veröffentlicht. Sie klärt Fragen und Unklarheiten, die sich aus der DO-178B ergeben.

Die Normen der SAE werden als Aerospace Recommended Practices (ARP) veröffentlicht. Für die Luftfahrzeugzulassung ist besonders die *ARP 4754 Certification considerations for Highly Integrated or Complex Aircraft Systems* wichtig. Sie basiert auf den Anforderungen der Federal Aviation Requirement (FAR) und AMC 25.1309. Der Schwerpunkt liegt auf komplexen elektronischen Systemen. Dabei wird der komplette Systemlebenszyklus

[18] vgl. LBA [28]

in Betracht gezogen. Für detailliertere Angaben zur Software und Hardware wird auf die ED-12B und ED-80 verwiesen. Methoden für den Sicherheitsnachweis werden in der *APR 4761 Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment* vorgestellt. [4]

3.1.3 Zusammenfassung

Der Luftverkehr unterscheidet zwischen einer Musterzulassung für jeden Flugzeugtyp, die die Voraussetzung für die Serienproduktion darstellt und dem Lufttüchtigkeitszeugnis, welches bestätigt, dass das Luftfahrzeug dem der Musterzulassung entspricht. Bereits heute gibt es durch die ICAO viele einheitliche Standards und Empfehlungen auf internationaler Ebene. Dennoch werden diese weltweit verschieden umgesetzt. Im Gegensatz zu den Lufttüchtigkeitszeugnissen gibt es für Musterzulassungen keinen einheitlichen Grundsatz der gegenseitigen Anerkennung. Damit muss der Entwicklungsbetrieb für Flugzeuge in jedem Staat, in dem sie später registriert werden sollen, eine Musterzulassung erwerben. Die EU regelt in der Verordnung VO 1592/2002, dass Mitglieder der EASA von ihr ausgestellte Zertifikate akzeptieren müssen. Zugleich wird eng mit der amerikanischen FAA die Harmonisierung der Zulassungsverfahren, die bereits mit der JAA begonnen wurde, fortgesetzt. Dabei wurden Verfahren angepasst und vereinheitlicht. Die Entwicklungsbetriebe können sich explizit über Unterschiede informieren. Ein kurzer Überblick der wichtigsten Vorschriften für die Musterzulassung von Verkehrsflugzeugen liefert die Abbildung 3.2. Die Bundesrepublik Deutschland hat sich sowohl der ICAO als auch der EU gegenüber verpflichtet, deren Standards und Richtlinien anzuerkennen und umzusetzen. Damit spielen das deutsche LuftVG und die dazugehörigen Verordnungen für die Musterzulassung nur noch eine untergeordnete Rolle.

3.2 Schienenverkehr

Für Schienenverkehrsmittel existiert, ebenso wie beim Luftverkehr, eine Zweiteilung der Zulassung. Es wird unterschieden zwischen einer Bauartzulassung für ein Fahrzeugmuster und der Inbetriebnahmegenehmigung für das einzelne Fahrzeug. Die in diesem Zusammenhang wichtigsten Organisationen und Regelungen werden hier kurz vorgestellt und in Abbildung 3.3 zusammenfassend dargestellt.

3.2.1 Gesetzgebung

International

Der 1922 gegründete Internationale Eisenbahnverband (UIC) vereint derzeit 171 Mitglieder[19] weltweit, unter anderem Eisenbahnverkehrsunternehmen, Eisenbahninfrastrukturbetreiber und Bahndienstleister. Der UIC hat es sich zum Ziel gesetzt, einheitliche Standards zu erstellen sowie den Bau und Betrieb von Eisenbahnen zu fördern. Dabei soll ebenfalls den heutigen wirtschaftlichen Verhältnissen Rechnung getragen werden. Dies will der UIC durch die Veröffentlichung von Richtlinien und Empfehlungen erreichen, welche jedoch nicht verpflichtend sind. Dabei arbeitet er auch mit anderen Verbänden, Organisationen und Normgebungsinstituten zusammen.[40]

Eine weitere wichtige internationale Vereinigung ist die Zwischenstaatliche Organisation für den internationalen Eisenbahnverkehr (OTIF), die einen grenzüberschreitenden einheitlichen Personen- und Güterverkehr in Europa und Asien verwirklichen will. Derzeit gehören ihr 42 Staaten[20] an, allen voran aus Europa aber auch aus Nordafrika sowie dem Nahen und Mittleren Osten. Bei der Überarbeitung des *Übereinkommens über den internationalen Eisenbahnverkehr (COTIF)* , das für alle Unterzeichner verpflichtend ist, wurde besonders Wert auf den technischen Bereich gelegt. Eine Harmonisierung sollte durch die Erklärung der Verbindlichkeit anzuwendender Normen und einem gemeinsamen Verfahren für die Zulassung von Eisenbahnmaterial und deren gegenseitige Anerkennung (Cross Acceptance) erreicht werden. Diese Punkte wurden in den Anhängen APTU[21] und

[19] UIC `http://www.uic.asso.fr/apropos/article.php3?id_article=209`, Abruf: 13.08.2007

[20] OTIF `http://www.otif.org/html/d/pres_info_generales.php`, Abruf: 23.07.2007

[21] Einheitliche Rechtsvorschriften für die Verbindlicherklärung technischer Normen und für die Annahme einheitlicher technischer Vorschriften für Eisenbahnmaterial, das zur Verwendung im internationalen Verkehr bestimmt ist

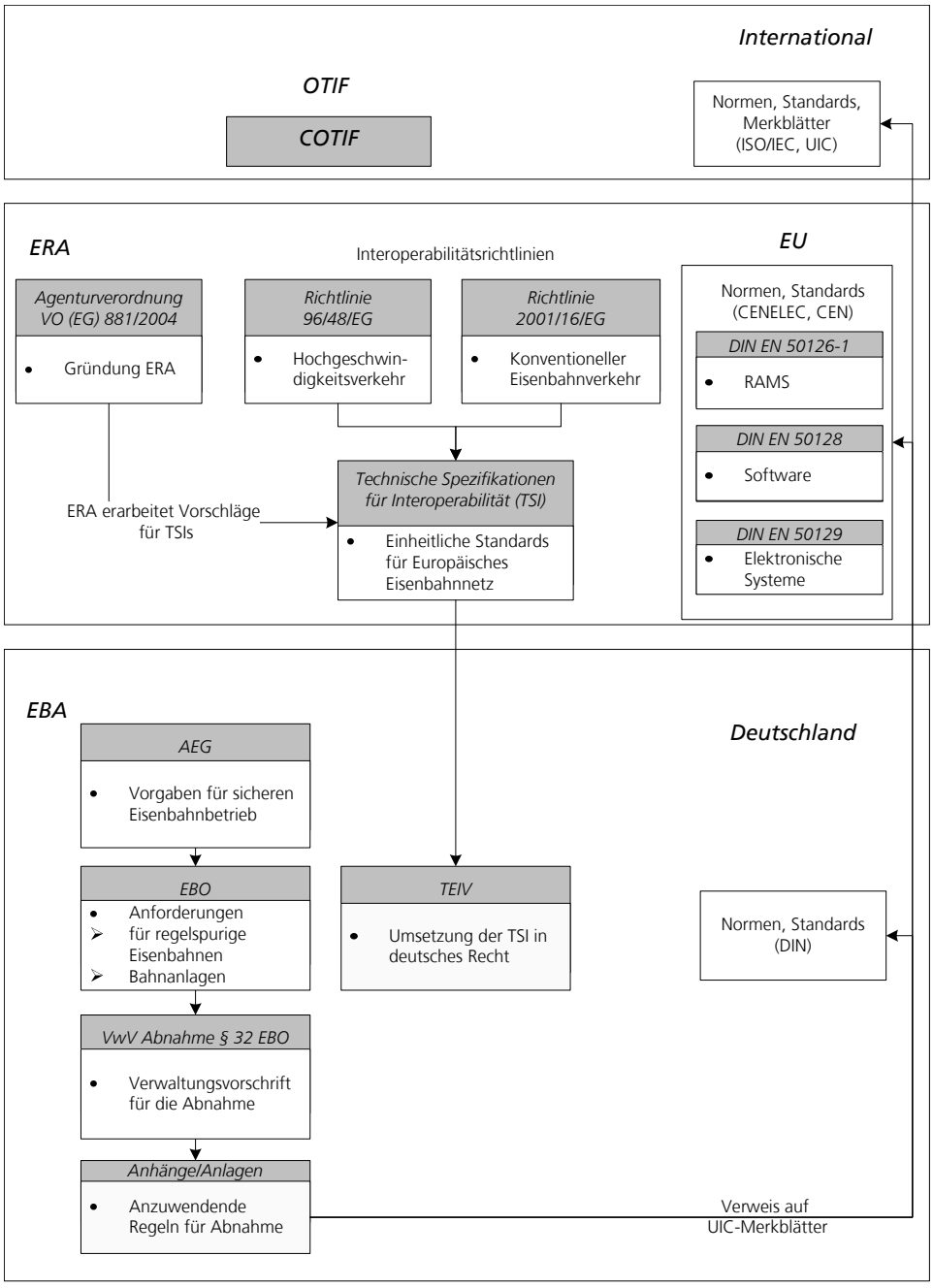

Abbildung 3.3: Darstellung der wichtigsten rechtlichen Grundlagen für die Musterzulassung von Schienenfahrzeugen

ATMF[22] festgeschrieben. Da sie jedoch teilweise im Widerspruch zu den Regelungen der EU liegen, haben deren Mitgliedstaaten das Abkommen von 1999 nur ohne die kontroversen Stellen angenommen. Derzeit laufen Verhandlungen über einen Beitritt der EU als Organisation zur OTIF und eine Anpassung der beiden Anhänge. [29]

Europa

Der *Vertrag zur Gründung der Europäischen Gemeinschaft (EG)* benennt eine gemeinsame Verkehrspolitik als eines der Tätigkeitsfelder zur Erreichung ihrer Ziele, zu denen u. a. eine Förderung des Wirtschaftslebens durch einen barrierefreien Binnenmarkt gehört[23]. Der Rat kann gemäß dem Vertrag „Maßnahmen zur Verbesserung der Verkehrssicherheit" [16, Art. 71 d] sowie „alle sonstigen zweckdienlichen Vorschriften erlassen." [16, Art. 71 d]

Aufgrund der geschichtlich bedingten teilweise stark voneinander abweichenden Infrastrukturen und Betriebsverfahren ist die Harmonisierung auf europäischer Ebene bisher jedoch noch nicht weit fortgeschritten. Zur Verbesserung der Kompatibilität veröffentlichte die EU die Richtlinien 96/48/EG für den Hochgeschwindigkeitsverkehr [32] und 2001/16/EG für den konventionellen Eisenbahnverkehr [31], die das Eisenbahnsystem in acht Teilsysteme gliedert:

- Fahrzeuge,
- Infrastruktur,
- Zugsteuerung, Zugsicherung und Signalgebung,
- Energieversorgung,
- Betrieb,
- Instandhaltung,
- Umwelt,
- Fahrgäste.

[22] Einheitliche Rechtsvorschriften für die technische Zulassung von Eisenbahnmaterial, das im internationalen Verkehr verwendet wird

[23] vgl. EG [16], Art. 2, Art. 3

Die Teilsysteme bestehen wiederum aus mehreren Interoperabilitätskomponenten (z. B. Bauteile oder Bauteilgruppen). Jedes Teilsystem muss in einer Technischen Spezifikation für Interoperabilität (TSI) abgehandelt werden. Die darin enthaltenen Mindestanforderungen und Eckwerte sollen die Kompatibilität in der Gemeinschaft sicherstellen. Dazu gehört eine Auflistung mit Normen und anderen Richtlinien (z. B. UIC-Merkblätter), die zwingend eingehalten werden müssen. Diese Regelungen gelten für Schienenverkehrsmittel, die grenzüberschreitend auf dem transeuropäischen Netz betrieben werden sollen. Für solche Fahrzeuge muss in einem Zertifizierungsverfahren die Konformität mit den Technischen Spezifikationen für Interoperabilität (TSI) nachgewiesen werden. Dies ist Voraussetzung für eine anschließende Zulassung durch das Eisenbahn-Bundesamt (EBA).[24]

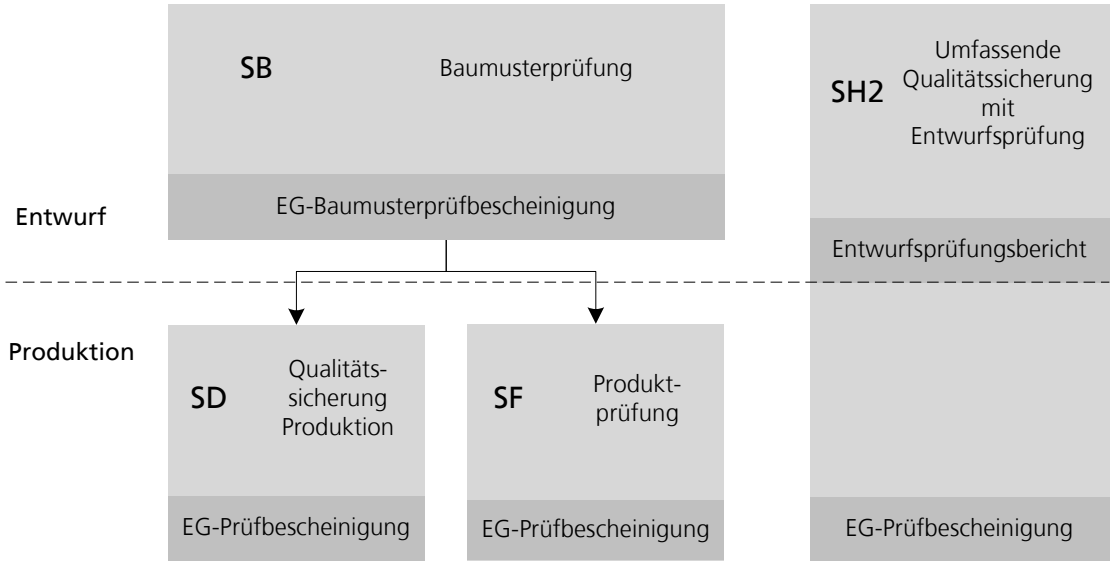

Abbildung 3.4: Module für die Zertifizierung von Schienenfahrzeugen mit den Prüfbescheinigungen gemäß den Richtlinien RL 96/48 [32] und RL 2001/16 [31]

Das EU-Prüfverfahren im Eisenbahnverkehr basiert auf dem Konformitätsbewertungsverfahren des Beschlusses 93/465/EWG[25]. Es besteht aus mehreren Modulen, die für den Eisenbahnverkehr angepasst wurden (Abb. 3.4). Der Antragsteller kann sich entscheiden, welche Module er anwendet. Dabei kann er wählen zwischen einer Baumusterprüfung

[24] vgl. TEIV [38], § 6 (3)

[25] 93/465/EWG: Beschluß des Rates vom 22. Juli 1993 über die in den technischen Harmonisierungsrichtlinien zu verwendenden Module für die verschiedenen Phasen der Konformitätsbewertungsverfahren und die Regeln für die Anbringung und Verwendung der CE- Konformitätskennzeichnung

(SB) und einer Prüfung der Produktion (SD oder SF) oder einer umfassenden Qualitätsplanung und Entwurfssicherung (SH2). Die Prüfungen und Zertifizierung erfolgt durch eine *benannte Stelle*, in Deutschland das *Eisenbahn-Cert (EBC)* . Zusätzlich zur Zertifizierung ist eine Bauartzulassung durch das Eisenbahn-Bundesamt (EBA) erforderlich, welche auf maximal fünf Jahre begrenzt wird[26]. [27, 39]

Auf dem europäischen Netz wurde die Einführung des europäischen Zugkontrollsystems (ETCS) beschlossen, was den grenzüberschreitenden Verkehr ermöglichen soll, ohne alle jeweiligen nationalen Sicherungstechniken an Bord der Fahrzeuge installieren zu müssen.

Für die Fortschreibung der TSI und Interoperabilitätsverfahren wurde durch die *Verordnung (EG) Nr. 881/2004* die Europäische Eisenbahnagentur (ERA) als Gemeinschaftsagentur gegründet. Diese dient vorrangig der Datensammlung und Auswertung sowie dem Erstellen von Vorschlägen für weitere Harmonisierungen für die Europäische Kommission. In diesem Punkt ähnelt sie der EASA, jedoch hat sie keine Befugnisse für die Zulassung von Fahrzeugen. [23]

Deutschland

Die Umsetzung der europäischen Richtlinien 96/48/EG und 2001/16/EG in deutsches Recht erfolgt in der *Verordnung über die Interoperabilität des transeuropäischen Eisenbahnsystems (Transeuropäische-EisenBahn-Interoperabilitätsverordnung – TEIV).* Neben den europäischen Verordnungen liegt die Gesetzgebung für Eisenbahnen des Bundes (EdB) in Deutschland beim Staat.[27] Es gilt das *Allgemeine Eisenbahngesetz (AEG)* , welches „der Gewährleistung eines sicheren Betriebs der Eisenbahn“ [1, § 1 Abs. 1] dient. „Die Eisenbahnen sind verpflichtet, [...] Fahrzeuge und Zubehör sicher zu bauen [...].“ [1, § 4 Abs. 2] Für EdB ist das EBA die zuständige Behörde für Prüfungen und Zulassungen.[28] Dies betrifft die Bauartzulassung sowie die Inbetriebnahmegenehmigung.

Die *Eisenbahn-Bau- und Betriebsordnung (EBO)* ist im Bereich regelspuriger Eisenbahnen mit einer Spurweite von 1 435 mm anzuwenden[29]. Sie fordert für Fahrzeuge die Gewährleistung von Sicherheit und Ordnung. Dafür müssen Angaben dieser Verordnung erfüllt oder, falls keine genauen Vorgaben enthalten sind, den *anerkannten Regeln der*

[26] vgl. TEIV [38], § 7 (2)
[27] vgl. GG [24], Art. 73 (1)6a
[28] vgl. AEG [1], § 4 Abs. 2
[29] vgl. EBO [15], § 1 (1), § 5

Technik entsprochen werden. Bei einer Abweichung muss „mindestens die gleiche Sicherheit wie bei Beachtung dieser Regeln nachgewiesen“ [15, § 2 Abs. 1 Satz 2] werden. Der zweite Abschnitt der EBO beschäftigt sich mit Bahnanlagen. Angaben über die Fahrzeuge werden im dritten Abschnitt behandelt. Die an dieser Stelle aufgeführten Vorschriften gelten für Regelfahrzeuge.[30] Die folgenden Paragraphen enthalten Angaben über die Radsatzlasten, Räder, Fahrzeugbegrenzungen, Bremsen, Zug- und Stoßeinrichtungen sowie erforderliche Ausrüstungen[31]. Vor Inbetriebnahme müssen Fahrzeuge zuerst nach § 32 EBO zugelassen werden. Dieses Verfahren wird in der *Verwaltungsvorschrift für die Abnahme von Eisenbahnfahrzeugen gemäß § 32 Abs. 1 EBO im Zuständigkeitsbereich des Eisenbahn-Bundesamt (VwV Abnahme § 32)* näher beschrieben. Sie enthält die Voraussetzungen und den Ablauf der Fahrzeugabnahme. Dabei wird der Hersteller verpflichtet, eine Betriebs- und Instandhaltungsdokumentation für seine Produkte zu erstellen und solange er der Halter der Zulassung ist, diese zu pflegen.[32] Die Anhänge und Anlagen zur VwV Abnahme § 32 enthalten Listen mit Anforderungen für die Abnahme gemäß § 32 EBO und den jeweiligen Gesetzen, Verordnungen, Richtlinien, UIC-Merkblättern und Normen, die zu erfüllen sind.

3.2.2 Wichtige Normen und Standards

Für den Schienenfahrzeugbau und die -zulassung gelten verschiedene Normen. Die wichtigsten Normungsorganisationen in diesem Bereich sind:

- International Organization for Standardization (ISO),
- Internationale Elektrotechnische Kommission (IEC),
- Europäisches Komitee für Normung (CEN),
- Europäisches Komitee für Elektrotechnische Normung (CENELEC),
- Deutsches Institut für Normung (DIN).

Daneben existieren noch viele Richtlinien und Empfehlungen, z. B. der Deutschen Bahn (DB) oder des UIC. Eine genaue Aufstellung kann den TSI oder der VwV Abnahme § 32

[30] vgl. EBO [15], § 18 (1)
[31] vgl. EBO [15], §§ 19ff.
[32] vgl. VwV Abnahme § 32 [46], Kapitel 2

entnommen werden. Die wichtigsten Normen in diesem Bereich sind die drei folgenden der CENELEC (s. Abb. 3.3):

- DIN EN 50126-1 Bahnanwendungen - Spezifikation und Nachweis der Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit, Sicherheit (RAMS) - Teil 1: Grundlegende Anforderungen und genereller Prozess,
- DIN EN 50128 Bahnanwendungen - Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme - Software für Eisenbahnsteuerungs- und Überwachungssysteme,
- DIN EN 50129 Bahnanwendungen - Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme - Sicherheitsrelevante elektronische Systeme für Signaltechnik.

Diese drei Normen basieren auf der *IEC 61508 Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme.*[33] Sie enthält allgemeine Angaben für den behandelten Bereich. Diese Norm kann entweder direkt angewandt oder für spezielle Branchen angepasst werden. Von der CENELEC wurde der zweite Weg gewählt, der in den oben genannten Standards resultierte. [34]

Die *DIN EN 50126-1* beschäftigt sich mit den Grundlagen der Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit und Sicherheit (RAMS). Sie definiert damit verbundene wichtige Begriffe und enthält Angaben über den System-Lebenszyklus sowie Verfahren und Prozesse. Damit soll den Eisenbahnunternehmen und der Industrie eine gemeinsame Grundlage und Verständnis geboten werden.[12] Die *DIN EN 50129* enthält Anforderungen für die Zulassung sicherheitskritischer Systeme eisenbahnsignaltechnischer Anlagen. Die Vorgaben gelten für generische Teilsysteme sowie anwendungsspezifische Systeme. Sie beschäftigt sich mit den Vorgaben, angefangen von der Spezifikation über Entwicklung und Konstruktion bis zu Änderungen und Erweiterungen.[14] Softwarespezifikationen werden in der *DIN EN 50128* genauer beschrieben.[13]

[33] vgl. DIN EN 50129 [14]
[34] vgl. Ständer u. Becker [37]

3.2.3 Zusammenfassung

International veröffentlicht der UIC bereits seit längerem Richtlinien, die zu einheitlichen Standards im Schienenverkehr führen sollen. Auf diese Merkblätter wird auch im Anhang der deutschen VwV Abnahme § 32 verwiesen. Die OTIF, deren Mitglieder im Gegensatz zum UIC Staaten sind, hat sich die Harmonisierung innerhalb des von ihr vertretenen Raums zum Ziel gesetzt. Die diesbezüglichen Regelungen der 2006 in Kraft getretenen überarbeiteten Fassung des COTIF kollidieren in einigen Bereichen jedoch mit dem EU-Recht, weshalb diese Teile in Deutschland derzeit keine Anwendung finden. Die EU selbst hat sich in den letzten Jahren dem Ziel der Harmonisierung verschrieben und in einigen Bereichen bereits Erfolge erreicht. Dafür wurden die TSI erstellt, die die Interoperabilität auf dem transeuropäischen Netz gewährleisten sollen. Diese sind für Fahrzeuge im europäischen Verkehrsnetz anzuwenden. Die Umsetzung der EU-Vorgaben in deutsches Recht wurde durch die Transeuropäische-Eisenbahn-Interoperabilitätsverordnung (TEIV) vollzogen. Eine EG-Prüfbescheinigung durch eine benannte Stelle ist Voraussetzung für die Erteilung einer Bauartzulassung durch das EBA. Im nationalen Bereich sind besonders das AEG und die untergeordnete EBO von Bedeutung. Die Fahrzeugzulassung wird in der VwV Abnahme § 32 detaillierter beschrieben. Die Zulassung von Eisenbahnen wird zwischen einem Baumuster und einem einzelnen Fahrzeug getrennt behandelt. Die Bauartzulassung gemäß der TEIV ist nur befristet gültig, ansonsten unbefristet. Die Zulassung für einzelne Fahrzeuge ist sowohl auf europäischer als auch nationaler Ebene unbegrenzt gültig.

Abbildung 3.3 soll einen kurzen Überblick über die wichtigsten Regelwerke für die Schienenfahrzeugzulassung geben. Dabei ist im Vergleich zum Luftverkehr ersichtlich, dass der Schwerpunkt auf der deutschen Gesetzgebung liegt.

3.3 Vergleich der Rahmenbedingungen der Verkehrsdomänen

Die rechtlichen Rahmenbedingungen der Verkehrsmittelzulassung der beiden Domänen haben sowohl Gemeinsamkeiten als auch Unterschiede (Tabelle 3.1). In beiden Bereichen gibt es bereits seit Jahren Bestrebungen, die Zulassung auf internationaler Ebene zu regeln. Dieses Vorhaben war bisher nur begrenzt erfolgreich. Internationale Verbände

versuchen durch Vorgaben einheitliche Mindestanforderungen zu erstellen. Obwohl diese Organisationen keine Gesetzgebungsbefugnis besitzen, verpflichten sich ihre Mitglieder mit Unterzeichnung der Verträge sich an die Vorgaben zu halten. Dies betrifft die ICAO für den Luftverkehr und die OTIF im Eisenbahnverkehr.

Tabelle 3.1: Vergleich der rechtlichen Rahmenbedingungen für die Zulassung von Luft- und Schienenfahrzeugen

Eigenschaft	**Luftverkehr**	**Eisenbahnverkehr**
Internationale Organisationen	ICAO	UIC, OTIF
zuständige Stellen (EU)	EASA	EBA
zuständige Stellen (D)	LBA	EBA
nationale Zuständigkeit	Bund	Bund
Ministerium	BMVBS	BMVBS
Zulassungen		
für Fahrzeugmuster	Musterzulassung	Baumusterzulassung
für Betrieb	Verkehrszulassung	Inbetriebnahmegenehmigung
Gültigkeit Zulassungen		
für Fahrzeugmuster	unbegrenzt	unbegrenzt (D) begrenzt (EU)
für Betrieb	unbegrenzt	unbegrenzt

Zur Verbesserung der wirtschaftlichen Bedingungen hat die EU Verordnungen und Richtlinien zur Vereinheitlichung erlassen, u. a. für die Fahrzeugzulassung. Im Luftverkehr wurde mit der Verordnung VO 1592/2002 [42] die EASA gegründet, die für die Musterzulassungen zuständig ist. Für den Eisenbahnverkehr wurde die ERA durch die Verordnung VO 881/2004 [45] gegründet. Diese hat im Gegensatz zur EASA keine so weit reichenden Befugnisse. Für die Zertifizierung der Fahrzeuge, die das transeuropäische Netz benutzen sollen und unter die Richlinien RL 96/48 [32] und RL 2001/16 [31] fallen, ist eine benannte Stelle zuständig. Die Baumusterzulassung wird durch das Eisenbahn-Bundesamt (EBA) erteilt. Die Gültigkeit der Zulassung auf Grundlage der EG-Zertifizierung ist auf maximal fünf Jahre begrenzt, ansonsten ist sie ebenso wie die Flugzeugmusterzulassung unbegrenzt.

In Deutschland fallen der Luft- und Schienenverkehr in den Zuständigkeitsbereich des Bundes. Sie unterstehen dem Bundesministerium für Verkehr, Bau und Stadtentwicklung (BMVBS), dem die Behörden Luftfahrt-Bundesamt (LBA) und Eisenbahn-Bundesamt (EBA) untergeordnet sind. Die nationale Zuständigkeit erstreckt sich vor allem auf die Zulassungen für den Betrieb der Fahrzeuge.

Neben den Gesetzen existieren noch unzählige Normen, Standards und Richtlinien. Diese umfassen besonders den Bereich komplexer elektronischer Systeme. Auch in diesem Bereich sind Bestrebungen zur weiteren internationalen Harmonisierung ersichtlich.

4 Darstellung der Zulassungsverfahren

4.1 Ablauf des Zulassungsprozesses für Luftfahrzeuge

Der Zulassungprozess seitens des Antragstellers wird in Artikel 15 der Verordnung (EG) Nr. 1592/2002 [42] und in der Verordnung (EG) Nr. 1702/2003 [43] geregelt. Die Europäische Luftfahrtagentur (EASA) hat außerdem die *Internal Working Procedure Type Certification (TCP)* [17] im Internet veröffentlicht, die den Ablauf seitens der Agentur beschreibt. Die nachstehenden Erläuterungen zum Zulassungsprozess sind in Abbildung 4.1 dargestellt.

Der Antrag an die EASA für eine Musterzulassung eines Luftfahrzeugs muss durch einen zugelassenen Entwicklungsbetrieb gestellt werden.

Gemäß 21A.15 der VO 1702/2003 [43] muss der Antrag enthalten:

- eine dreidimensionale Luftfahrzeugzeichnung sowie
- die geplanten Basisdaten mit vorgesehenen Beschränkungen und Betriebskenndaten.

Aktuelle Angaben über das richtige Format, die Adresse und Gebühren sind der EASA-Homepage zu entnehmen. Die Verantwortung für die technische Prüfung kann durch die EASA selbst oder durch eine angeschlossene nationale Luftfahrtbehörde, z. B. das Luftfahrt-Bundesamt (LBA), durchgeführt werden. Der Einführung in das Projekt dient ein erstes Treffen zwischen den zuständigen Mitarbeitern der Behörde und des Antragstellers. Der weitere Zulassungsverlauf kann in vier Phasen unterteilt werden:

1. Technische Einarbeitung und Erarbeitung der Musterzulassungsgrundlage,
2. Festlegung des Zulassungsprogramms,

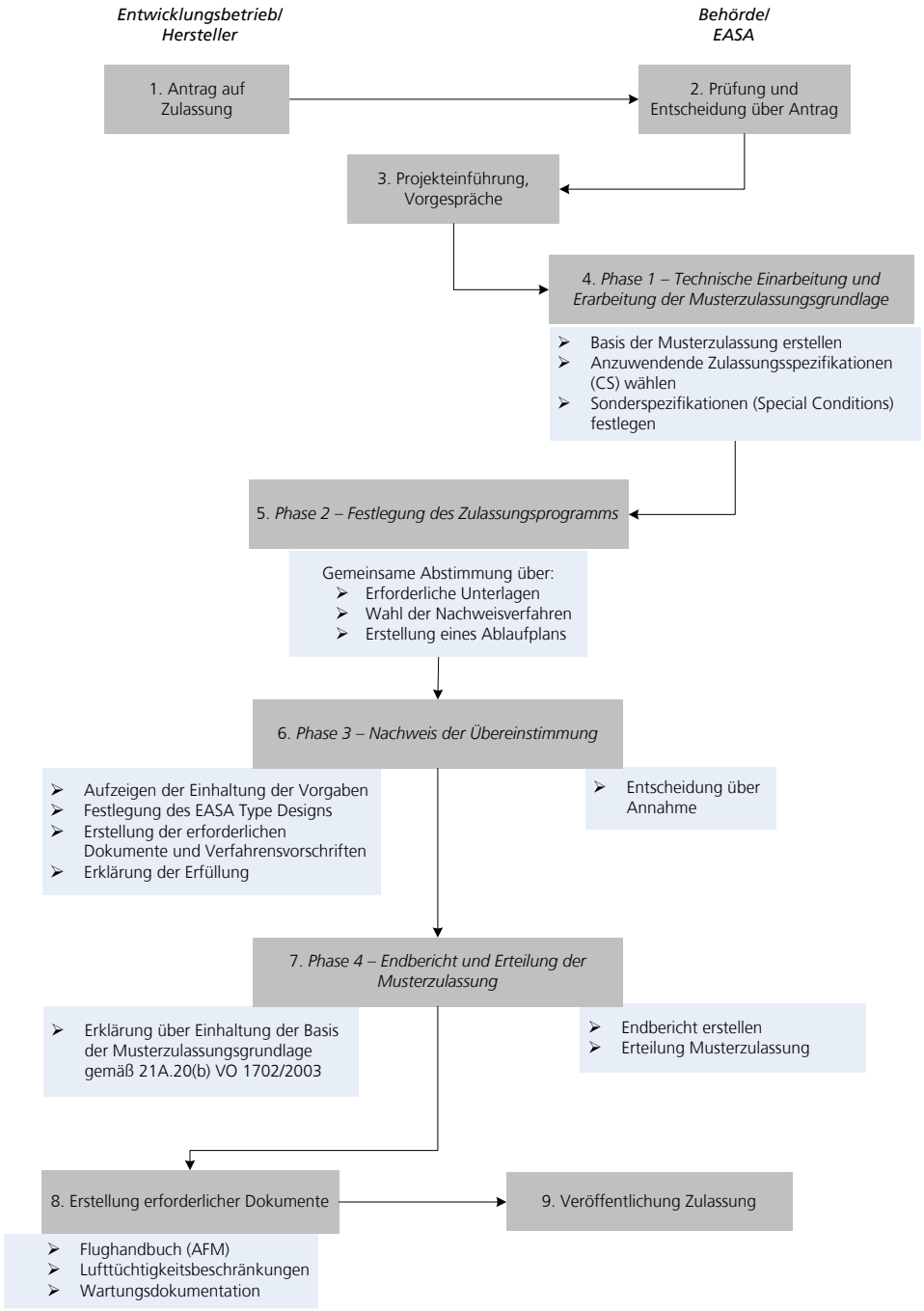

Abbildung 4.1: Graphische Darstellung des Zulassungsprozesses für Luftfahrzeuge

3. Nachweis der Übereinstimmung mit den Anforderungen,

4. Endbericht und Erteilung der Musterzulassung.

In der ersten Phase, der technischen Einarbeitung und Erarbeitung der Musterzulassungsgrundlage, finden mehrere Treffen zwischen beiden Seiten statt. Dies dient dem besseren Verständnis des geplanten Entwurfs und neuer Technologien. Daraufhin wird durch die EASA eine Musterzulassungsgrundlage erstellt. Diese enthält die anzuwendenden Zulassungsspezifikationen sowie besondere technische Einzelspezifikationen. Sie kann auch vom Antragsteller gewünschte Änderungen enthalten. Die Musterzulassungsgrundlage, die für jedes zulassungspflichtige Erzeugnis, z. B. ein Flugzeug oder Triebwerk, erstellt werden muss, kann während des Zulassungsprozesses, wenn erforderlich, angepasst werden. Der *Antrag auf Musterzulassung* hat eine Gültigkeit von drei Jahren, für große Luftfahrzeuge von fünf Jahren. Bei Nachweis eines längeren Zeitraums kann dieser von der EASA genehmigt werden. Falls das Verfahren innerhalb der gegebenen Zeit nicht abgeschlossen werden kann, muss eine Verlängerung beantragt oder ein neuer Antrag gestellt werden. Sollten sich dabei die anzuwendenden Lufttüchtigkeitszulassungen ändern, sind die neuen gültig. Ferner müssen die Anforderungen an den Umweltschutz (Lärm und Emissionen) nach Annex 16 des Chicagoer Abkommens sowie die gültigen EASA-Zulassungsspezifikationen (CS) berücksichtigt werden.

Die Festlegung des Zulassungsprogramms erfolgt in Phase zwei. In Absprache zwischen den Beteiligten wird entschieden über:

- Erforderliche Unterlagen,
- Wahl der Nachweisverfahren und
- Erstellung eines Ablaufplans.

In der dritten Phase muss die EASA über die Annahme des Nachweises der Übereinstimmung entscheiden. Die Aufgaben des Entwicklers an dieser Stelle sind:

- Aufzeigen der Einhaltung der Anforderungen in jedem Punkt,
- Festlegung der Musterbauart,
- Erstellung der erforderlichen Dokumente und Verfahrensvorschriften sowie

- Erklärung der Erfüllung gemäß 21A.44 (VO 1702/2003).

Können einzelne Lufttüchtigkeitsvorgaben nicht eingehalten werden, muss aufgezeigt werden, dass die Sicherheit durch kompensierende Faktoren das erforderliche Niveau erreicht. Die Erklärung der Erfüllung gemäß 21A.44 [43] beinhaltet die Bereitschaft des Antragstellers, die Aufrechterhaltung der Lufttüchtigkeit zu gewährleisten, Handbücher zu erstellen und zu pflegen sowie seinen Aufzeichnungspflichten nachzukommen.

Zuletzt folgt die vierte Phase, Endbericht und Erteilung der Musterzulassung. Der Antragsteller muss eine Erklärung über die Einhaltung der einschlägigen Anforderungen der Musterzulassungsgrundlage und des Umweltschutzes gemäß 21A.20(b) [43] abgeben. Ferner muss die EASA die Erfüllung der Auflagen bestätigen. Nach Erstellung und Bestätigung des Abschlussberichts erteilt der zuständige EASA-Verantwortliche die Musterzulassung mit dem Type-certificate Data Sheet (TCDS). Die Bekanntmachung erfolgt auf der Internetseite der Agentur. Die Musterzulassung kann Einschränkungen hinsichtlich der Betriebsbedingungen enthalten, die nach späteren Tests entfallen können. Die Zulassung bleibt solange gültig, bis sie zurückgegeben oder widerrufen wird.

Die Gebührensätze für die Zulassung von Luftfahrzeugen werden in der Verordnung (EG) Nr. 593/2007 festgeschrieben. Für die Musterzulassung eines Flugzeugs zwischen 50 t bis 150 t müssen z. B. 1.330.000 € gezahlt werden.[44]

4.2 Ablauf des Zulassungsprozesses für Schienenfahrzeuge

Bei der Zulassung von Schienenfahrzeugen muss nach den geplanten Einsatzgebieten unterschieden werden. Fahrzeuge, die nur in Deutschland verkehren sollen, benötigen die Zulassung durch das Eisenbahn-Bundesamt (EBA) nach der VwV Abnahme § 32 [46]. Für einen angestrebten grenzüberschreitenden Verkehr auf dem transeuropäischen Netz ist vor der deutschen Bauartzulassung eine Zerifizierung durch die benannte Stelle, das Eisenbahn-Cert (EBC), zu erlangen. Dabei muss die Einhaltung der Vorgaben der Richtlinien RL 96/48 [32] für den Hochgeschwindigkeitsverkehr oder der RL 2001/16 [31] für den konventionellen Verkehr nachgewiesen werden.

4.2.1 Zulassungsverfahren nach VwV Abnahme § 32

Die VwV Abnahme § 32 [46] enthält Angaben zum Verfahren der Behörde. Sie wird den Antragstellern als Hilfe im Internet zur Verfügung gestellt. Das Verfahren ist in Abbildung 4.2 graphisch dargestellt.

Für die Abnahme eines Schienenfahrzeugs müssen zuerst drei Voraussetzungen erfüllt sein:

- Nachweis eines Qualitätssicherungssystems beim Hersteller,
- Erklärung des Antragstellers über die Einhaltung der anerkannten Regeln der Technik,
- Erstellung fahrzeugbezogener Unterlagen.

Die Anhänge der Vorschrift enthalten die erforderlichen Unterlagen und eine Auflistung der anzuwendenden Regelwerke. Die vorzulegenden Unterlagen sollen eine Plausibilitätsprüfung der Sicherheitsbewertungen hinsichtlich der Einhaltung der Anforderungen gewährleisten. Abnahmeanträge sollten bereits während der Entwurfsphasse beim EBA eingereicht werden. Am Anfang des Zulassungsverfahrens werden der Zeitplan, die anzuwendenden Vorschriften, die durchzuführenden Nachweise zur Erfüllung der Anforderungen sowie der Behörde vorzulegende Dokumente festgelegt. Die in den Anhängen zur Verwaltungsvorschrift für die Abnahme von Eisenbahnfahrzeugen gemäß § 32 Abs. 1 EBO im Zuständigkeitsbereich des Eisenbahn-Bundesamt (VwV Abnahme § 32) festgelegten Anforderungen werden dem Projekt entsprechend angepasst. Darüber hinaus müssen weitere Untersuchungen durchgeführt werden, deren Ergebnisse dem EBA jedoch nur auf Anforderung vorgelegt werden müssen. Wird von den anerkannten Regeln der Technik abgewichen, zum Beispiel bei neuartigen Verfahren, dann ist ein Nachweis für mindestens die gleiche Sicherheit wie bei Anwendung der anerkannten Regeln der Technik vorzulegen. Der Hersteller muss dem Betreiber Unterlagen zum Betrieb und der Instandhaltung zur Verfügung stellen. Für die Zulassung wird die Rechtslage am Tag der Abnahme zugrundegelegt. Als Planungssicherheit für den Hersteller kann auf Antrag eine Zusicherung genehmigt werden. In dem Fall erfolgt die Abnahme gemäß einer Checkliste auf Basis des Pflichtenheftes. Die Gültigkeit der Zusicherung ist auf drei Jahre begrenzt. Für nicht im

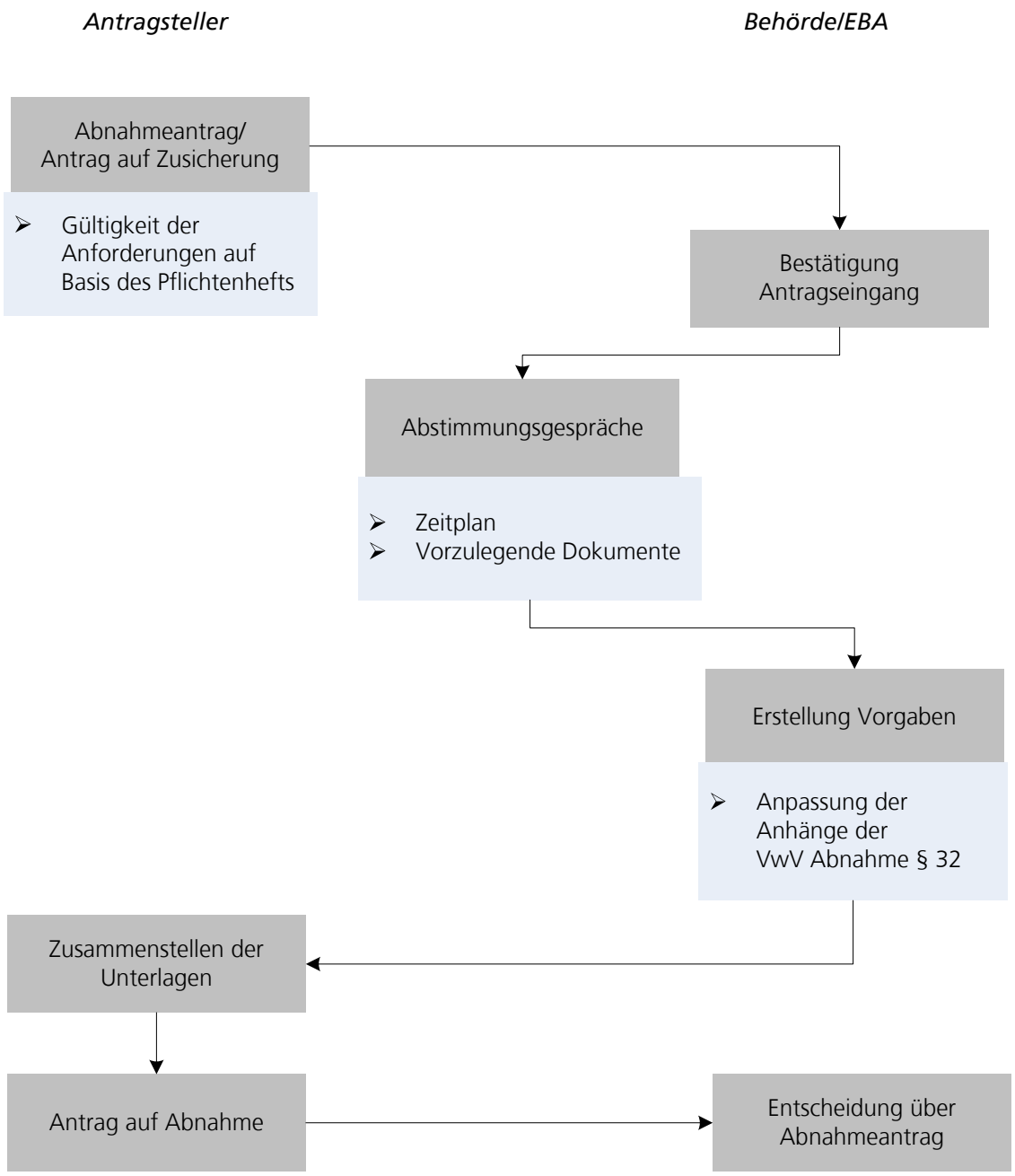

Abbildung 4.2: Graphische Darstellung des Zulassungsprozesses für Schienenfahrzeuge nach der VwV Abnahme § 32

Pflichtenheft definierte Anforderungen gilt der Stand der Regelungen vom Tag der Abnahme. Für das Bauartmuster muss die Erfüllung der EBA-Anforderungen nachgewiesen werden. Nach Eingang der erforderlichen Unterlagen wird der Antrag auf Abnahme innerhalb von acht Wochen entschieden. Für überwachungsbedürftige Anlagen ist ebenfalls eine Bauartzulassung erforderlich. Für Zugsicherungs- und Zugfunksysteme gelten zusätzlich Vorgaben des entsprechenden Referats. Für einzelne Komponenten kann ein *Vorgriff auf die Abnahme* durch eine Teilabnahme erfolgen. Prüfstellen für eisenbahntypische Prüfungen und Gutachter können, nach Anerkennung ihrer Eignung, das EBA bei seiner Aufgabe unterstützen. Eine entsprechende Liste ist auf der Internetseite des EBA veröffentlicht. Der Abnahmebescheid ist solange gültig, bis er zurückgegeben oder widerrufen wird. Die Verwaltungskosten richten sich nach der Verordnung über die Gebühren und Auslagen für Amtshandlungen der Eisenbahnverkehrsverwaltung des Bundes (BEGebV). [46]

4.2.2 Zulassungsverfahren nach EU-Richtlinien

Für Schienenfahrzeuge, die auf dem transeuropäischen Netz grenzüberschreitend verkehren sollen, ist eine Zertifizierung durch eine benannte Stelle, z. B. Eisenbahn-Cert (EBC), erforderlich. Damit wird die Konformität mit den Anforderungen der Technischen Spezifikationen für Interoperabilität (TSI) bescheinigt. Anschließend muss eine Bauartzulassung des EBA erworben werden. Das Verfahren ist in den Abbildungen 4.3 bis 4.7 dargestellt.

Die Zertifizierung nach europäischem Recht basiert auf dem modularen Prüfverfahren des Beschlusses 93/465/EWG[1] für Konformitätsbewertungsverfahren. Die Module dieses Beschlusses wurden für die Verwendung im Eisenbahnverkehr leicht angepasst (Abb. 3.4). In dem Verfahren müssen die Konformität des Baumusters mit den Vorgaben und ein Qualitätssystem nachgewiesen werden. Der Zulassungsprozess wird in dem Leitfaden zur Richtlinie 96/48/EG für den Hochgeschwindigkeitsverkehr [27] sowie in Thomasch [39] beschrieben.

Der Antragsteller muss sich als erstes für die anzuwendenden Module entscheiden (Abb. 4.3). Das sollte bereits am Anfang der Entwicklung in Absprache mit der benannten Stelle geschehen. Es stehen die drei in Tabelle 4.1 benannten Alternativen zur Auswahl.

[1] 93/465/EWG: Beschluß des Rates vom 22. Juli 1993 über die in den technischen Harmonisierungsrichtlinien zu verwendenden Module für die verschiedenen Phasen der Konformitätsbewertungsverfahren und die Regeln für die Anbringung und Verwendung der CE- Konformitätskennzeichnung

Tabelle 4.1: Module für die Fahrzeugzulassung nach dem EU-Prüfverfahren (nach [39])

Phase	Alternativen		
	1	2	3
Entwurf	SB	SB	SH2
Bauartprüfung	SB	SB	
Qualitätssicherung	SD		SH2
Produktprüfung		SF	

Bei den ersten beiden Möglichkeiten wird eine Baumusterprüfung (SB) sowie eine Prüfung der Produktion (SD oder SF) durchgeführt, wobei das Modul SD nur für Teilsysteme angewandt werden kann, wenn alle beteiligten Hersteller über ein von der benannten Stelle zugelassenes Qualitätssicherungssystem verfügen. Eine Alternative stellt das Modul SH2 dar. In diesem Fall bewertet die benannte Stelle das Qualitätssystem des Entwicklungsbetriebs während der Entwurfsphase und prüft den Entwurf. Das Ergebnis ist eine zeitlich befristete EG-Entwurfsprüfbescheinigung. Das Qualitätssystem der Hersteller wird während der Produktion wie auch beim Modul SD überwacht. Die Module sind alle ähnlich aufgebaut. Der Auftraggeber beantragt eine EG-Prüfung durch die benannte Stelle und erstellt die technische Dokumentation sowie weitere Unterlagen. Die benannte Stelle erteilt zum Schluss jedes Moduls eine EG-Prüfbescheinigung. Daraufhin erstellt der Antragsteller eine EG-Prüferklärung.

Im *Modul SB* (Abb. 4.4) beantragt der Auftraggeber eine EG-Prüfung während einer Baumusterprüfung. Dazu muss er für den Entwurf des Teilsystems Fahrzeug eine technische Dokumentation und Unterlagen erstellen, die u. a. eine Auflistung aller verwendeten Interoperabilitätskomponenten (IK) sowie der Hersteller enthalten müssen. Falls erforderlich, muss der benannten Stelle ein repräsentatives Muster bereitgestellt werden. Die benannte Stelle prüft sowohl die technischen Unterlagen als auch die EG-Erklärungen aller verwendeten Interoperabilitätskomponenten. Des Weiteren führt sie ein Design-Review durch, in dem alle Verfahren, Werkzeuge und Ergebnisse des Entwurfs untersucht werden. Es werden alle Prüfungen durchgeführt, die die TSI vorschreiben. Zuletzt erstellt die benannte Stelle eine technische Akte und die EG-Baumusterprüfbescheinigung.

Das *Modul SD* (Abb. 4.5) wird auf die Qualitätssicherung in der Produktion angewandt. Der Auftraggeber beantragt die EG-Prüfung. Alle beteiligten Hersteller müssen über

ein durch die benannte Stelle zugelassenes Qualitätssicherungssystem in der Produktion verfügen. Der Auftraggeber hat die technische Dokumentation und eine EG-Prüferklärung zu erstellen. Die benannte Stelle muss die Qualitätssicherungssysteme prüfen, zulassen und überwachen. Außerdem erstellt sie die technische Akte sowie die EG-Prüfbescheinigung für das Teilsystem.

Haben nicht alle Hersteller ein zugelassenes Qualitätssicherungssystem, kann das *Modul SF* (Abb. 4.6) angewandt werden. Der Auftraggeber beantragt die EG-Prüfung und erstellt die technische Dokumentation sowie die EG-Prüferklärung. Die benannte Stelle führt an dem montierten Teilsystem Konformitätsprüfungen durch und erstellt die technische Akte sowie eine EG-Prüfbescheinigung.

Wird alternativ das *Modul SH2* (Abb. 4.7), umfassende Qualitätssicherung mit Entwurfsprüfung, gewählt, erfolgt keine explizite Baumusterprüfung durch das Eisenbahn-Cert (EBC). Der Auftraggeber wiederum hat die EG-Prüfung zu beantragen und sicherzustellen, dass alle Hersteller ein Qualitätssicherungssystem betreiben. Ferner hat er technische Unterlagen, wie in Modul SB zu erstellen und Baumusterprüfungen durchzuführen, soweit diese erforderlich sind. Der Auftraggeber muss der benannten Stelle nachweisen, dass alle von der TSI gestellten Anforderungen an das Teilsystem erfüllt sind. Zuletzt erstellt er eine EG-Prüferklärung. Die Aufgaben der benannte Stelle liegen in der Beurteilung, Zulassung und Überwachung des Qualitätssicherungssystems sowie der Prüfung der Anträge und EG-Erklärungen. Ferner hat sie einen Entwurfsprüfungsbericht, die technische Akte und die EG-Prüfbescheinigung zu erstellen.

Die Gültigkeit der europäischen Baumuster- bzw. Entwurfsprüfbescheinigungen ist zeitlich befristet. Bei weiterer Produktion nach Ablauf dieses Zeitraums muss der Entwurf dem Stand der Technik angepasst werden.

Das Ergebnis dieses Verfahrens ist eine Konformitätsbescheinigung der benannten Stelle zur Einhaltung der Anforderungen der TSI. Anschließend muss noch eine Bauartzulassung durch das EBA erlangt werden. Das Verfahren ähnelt dem in Abschnitt 4.2.1 vorgestellten Verfahren. Dabei wird die EG-Prüferklärung des Antragstellers anerkannt. Zusätzlich müssen aber noch nationale Anforderungen erfüllt werden, die durch die TSI nicht abgedeckt sind. [38]

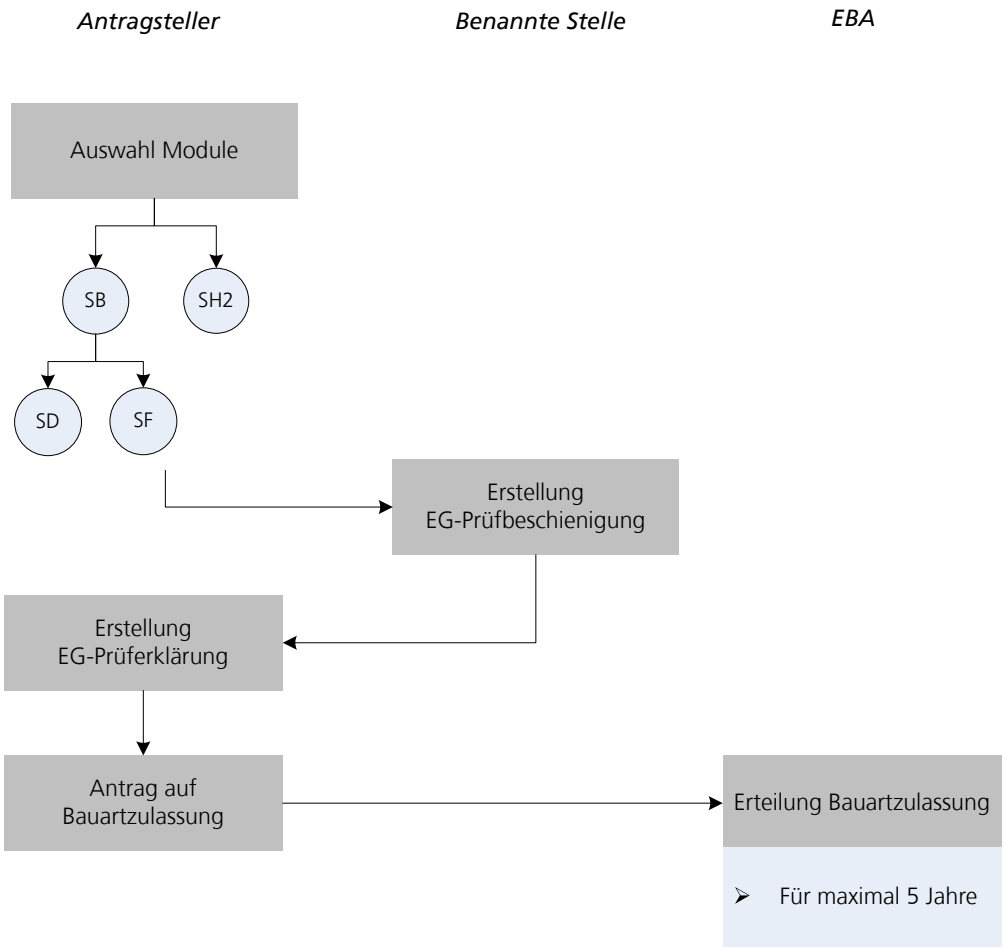

Abbildung 4.3: Graphische Darstellung des Zulassungsprozesses für Schienenfahrzeuge nach den Richtlinien 96/48/EG und 2001/16/EG - Teil 1 Modulauswahl

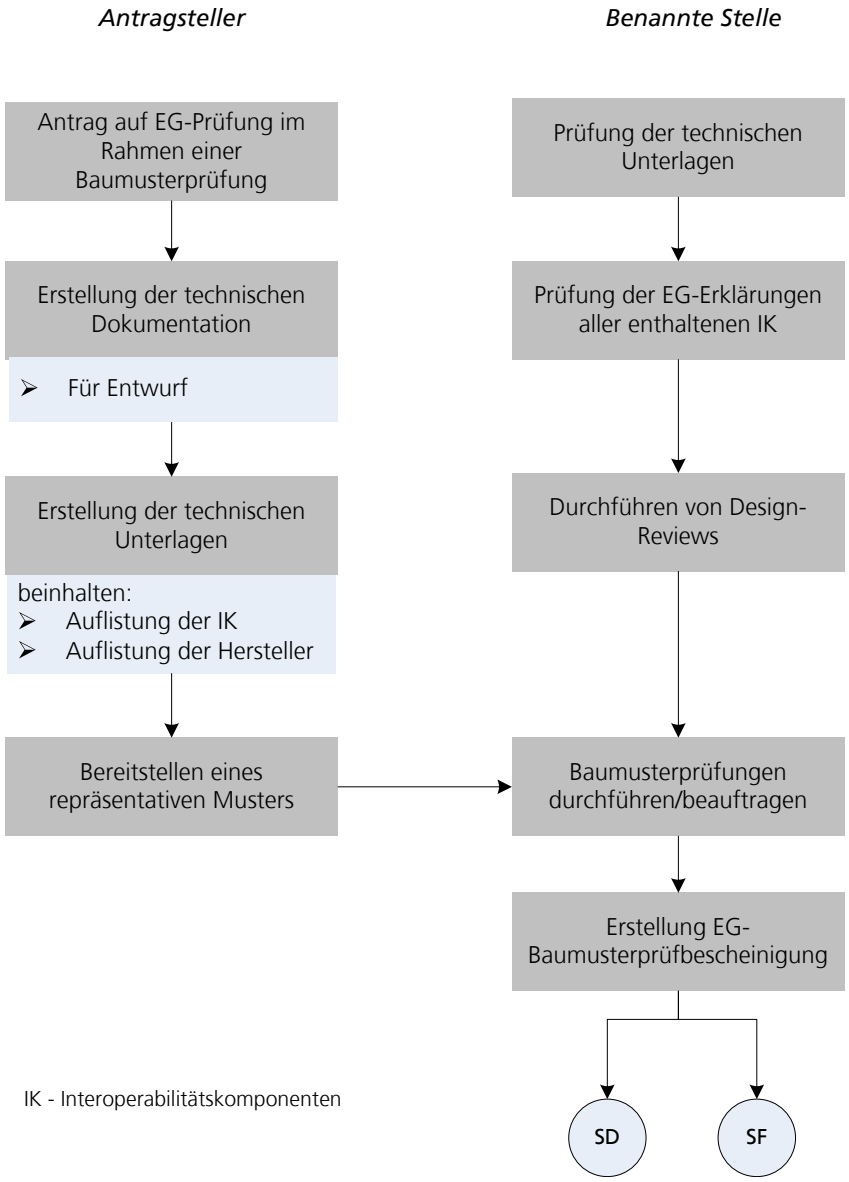

Abbildung 4.4: Graphische Darstellung des Zulassungsprozesses für Schienenfahrzeuge nach den Richtlinien 96/48/EG und 2001/16/EG - Teil 2 Modul SB

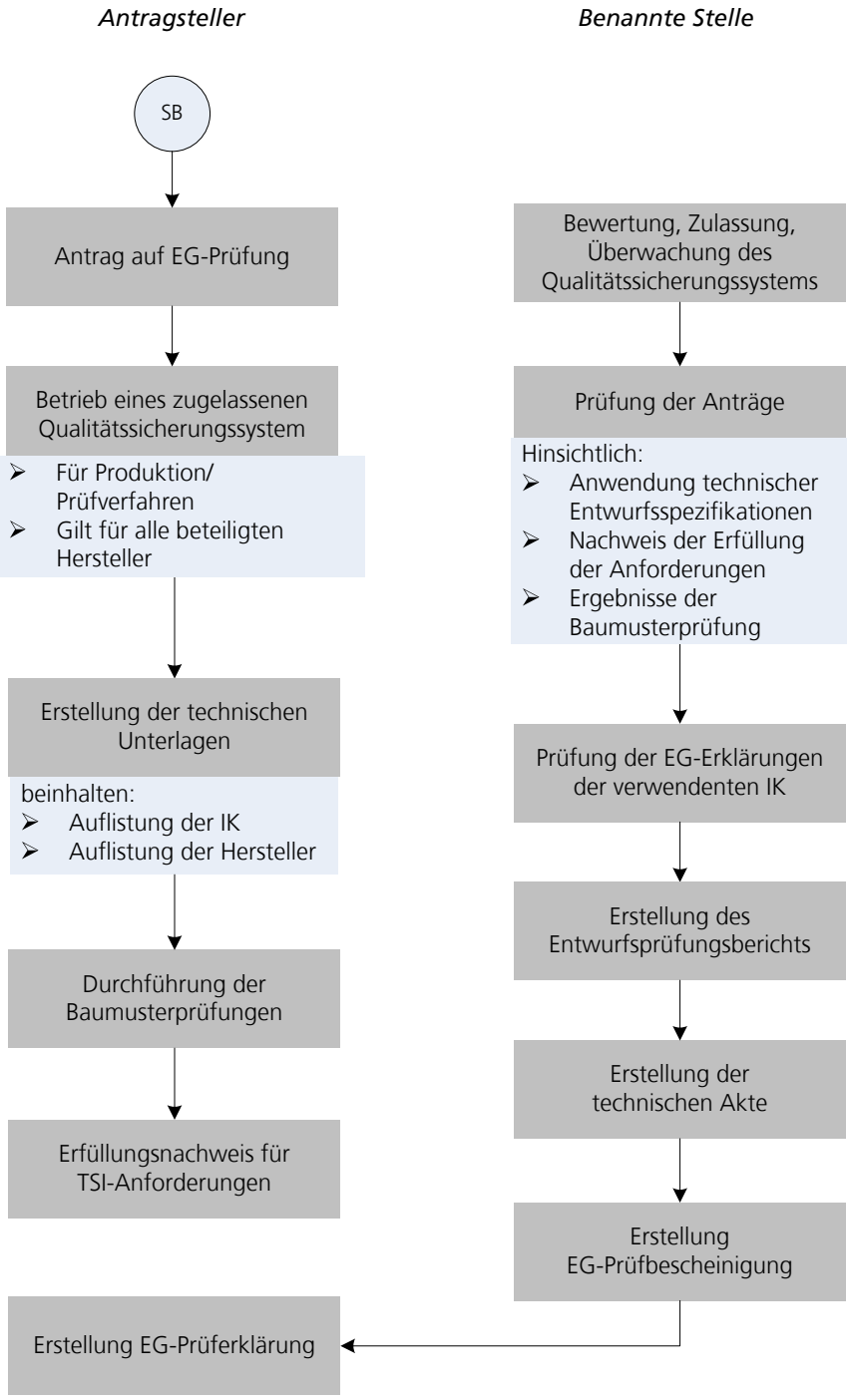

Abbildung 4.5: Graphische Darstellung des Zulassungsprozesses für Schienenfahrzeuge nach den Richtlinien 96/48/EG und 2001/16/EG - Teil 3 Modul SD

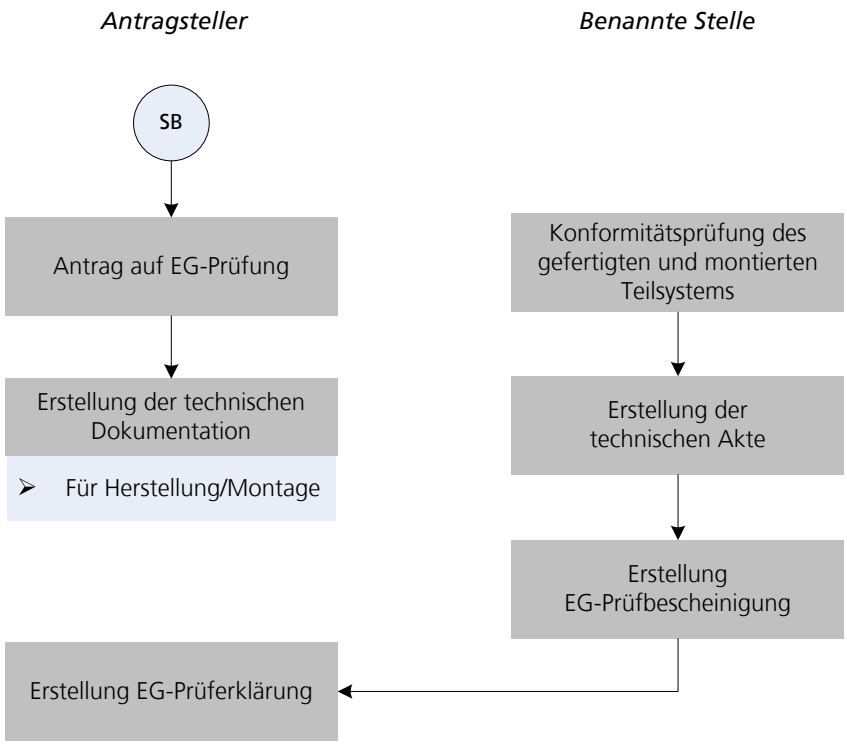

Abbildung 4.6: Graphische Darstellung des Zulassungsprozesses für Schienenfahrzeuge nach den Richtlinien 96/48/EG und 2001/16/EG - Teil 3 Modul SF

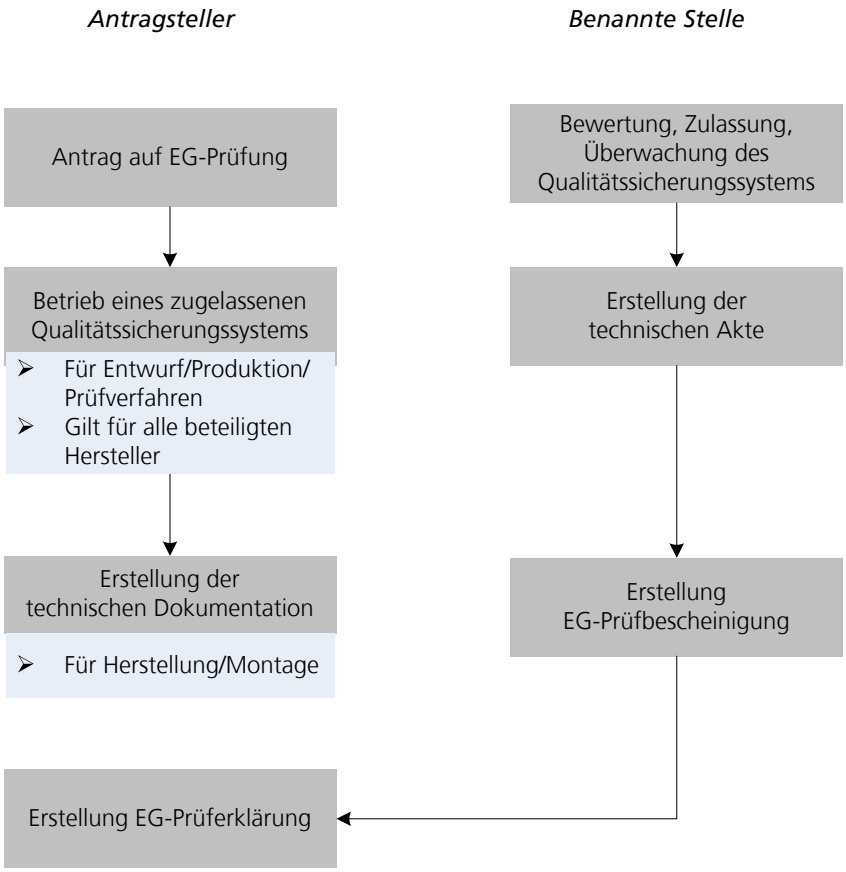

Abbildung 4.7: Graphische Darstellung des Zulassungsprozesses für Schienenfahrzeuge nach den Richtlinien 96/48/EG und 2001/16/EG - Teil 4 Modul SH

4.3 Vergleich der Zulassungsverfahren für Luft- und Schienenfahrzeuge

Das Zulassungsanforderungen für Luftfahrzeuge sind in den Zulassungsspezifikationen (CS) enthalten, für Schienenfahrzeuge in der VwV Abnahme § 32 und in den TSI. In beiden Domänen sollten die Hersteller frühzeitig Absprachen mit der Zulassungsbehörde bzw. benannten Stelle führen, um den Ablauf, die zu erstellenden Unterlagen sowie die durchzuführenden Prüfungen miteinander zu vereinbaren. Die zuständige Behörde für Flugzeuge ist die Europäische Luftfahrtagentur (EASA), für Schienenfahrzeuge das Eisenbahn-Bundesamt (EBA). Die Luftfahrzeugzulassung erfolgt auf europäischer Ebene und wird von allen Mitgliedstaaten der EASA anerkannt. Die Zulassung für Schienenfahrzeuge erfolgt auf nationaler Ebene. Sollen die Fahrzeuge auch außerhalb Deutschlands auf dem transeuropäischen Netz verkehren, muss mit einer Zertifizierung der benannten Stelle die Einhaltung der TSI nachgewiesen werden. Damit soll in Europa ein Mindeststandard gewährleistet werden. Es ist jedoch weiterhin die Zulassung durch das EBA erforderlich. Dafür müssen neben den TSI auch die deutschen Vorschriften eingehalten werden. Damit wird die Zulassung für ein Schienenfahrzeug nicht von allen anderen EU-Staaten akzeptiert. Das Zertifizierungsverfahren bietet aber eine gemeinsame Basis. Durch diese Trennung zwischen innerstaatlichem und europäischem Verkehr müssen Fahrzeuge, die nur in Deutschland verkauft werden sollen, nur nach diesen Vorschriften zugelassen werden. Die Einhaltung der zum Teil darüberhinausgehenden europäischen Vorgaben ist nicht erforderlich. Bei Flugzeugen dürfte dieser Fall nur sehr selten vorkommen, weshalb ein einheitliches Verfahren in der Europäischen Union (EU) effektiver ist.

Voraussetzung für die Entwicklung von Luftfahrzeugen ist eine Design Organisation Approval (DOA). Schienenfahrzeughersteller benötigen keine spezielle Genehmigung, jedoch werden während des Zertifizierungs- und Zulassungsverfahrens die Qualitätsmanagementsysteme der beteiligten Firmen überprüft. Während einer mehrjährigen Entwicklungszeit können sich die Vorschriften ändern. Um den Herstellern dennoch eine Planungssicherheit zu geben, müssen die anzuwendenden Vorgaben festgeschrieben werden. Im Luftverkehr geschieht das automatisch mit dem Antrag auf Musterzulassung, der drei bzw. fünf Jahre gültig ist. Ein Schienenfahrzeughersteller muss erst einen Antrag auf Zusicherung stellen, der dann für drei Jahre gilt. Andernfalls gelten für ihn die Vorgaben vom Tag der Abnahme.

Zum Schluss des Verfahrens müssen die Hersteller von Luft- und Schienenfahrzeugen die Einhaltung aller anzuwendenden Regelungen erklären. Die Zulassungen der EASA und des EBA für den nationalen Verkehr gelten unbegrenzt. Demgegenüber ist die Bauartzulassung basierend auf den TSI auf maximal fünf Jahre befristet. Das bedeutet, dass Hersteller von Schienenverkehrsmitteln nach Ablauf der Geltungsdauer den Entwurf dem Stand der Technik anpassen müssen, sollten sie das Fahrzeug weiter produzieren wollen [39].

5 Methoden und Verfahren für Sicherheitsanalysen

5.1 Allgemeines

5.1.1 Lebenszyklus

Die DIN EN 50126-1 [12] bezeichnet den Systemlebenszyklus als Abfolge mehrerer Stufen mit den zugehörigen Aktivitäten über den gesamten Zeitraum vom ersten Konzept bis zur Stilllegung. Es gibt in der Literatur diverse Lebenszyklusdarstellungen. Die enthaltenen Phasen sind abhängig von den Produkten und Bereichen, für die sie erstellt wurden. Die Anzahl und Namen der Stufen sind verschieden, gleichwohl enthalten sie alle in irgendeiner Form die folgenden Punkte:

- Konzept und Definition,
- Entwicklung,
- Herstellung,
- Installation/Inbetriebnahme,
- Betrieb und Instandhaltung,
- Stilllegung und Entsorgung.

Abbildung 5.1 zeigt Lebenszyklen für Luftfahrzeuge und Bahnanwendungen, die in den folgenden Abschnitten genauer beschrieben werden.

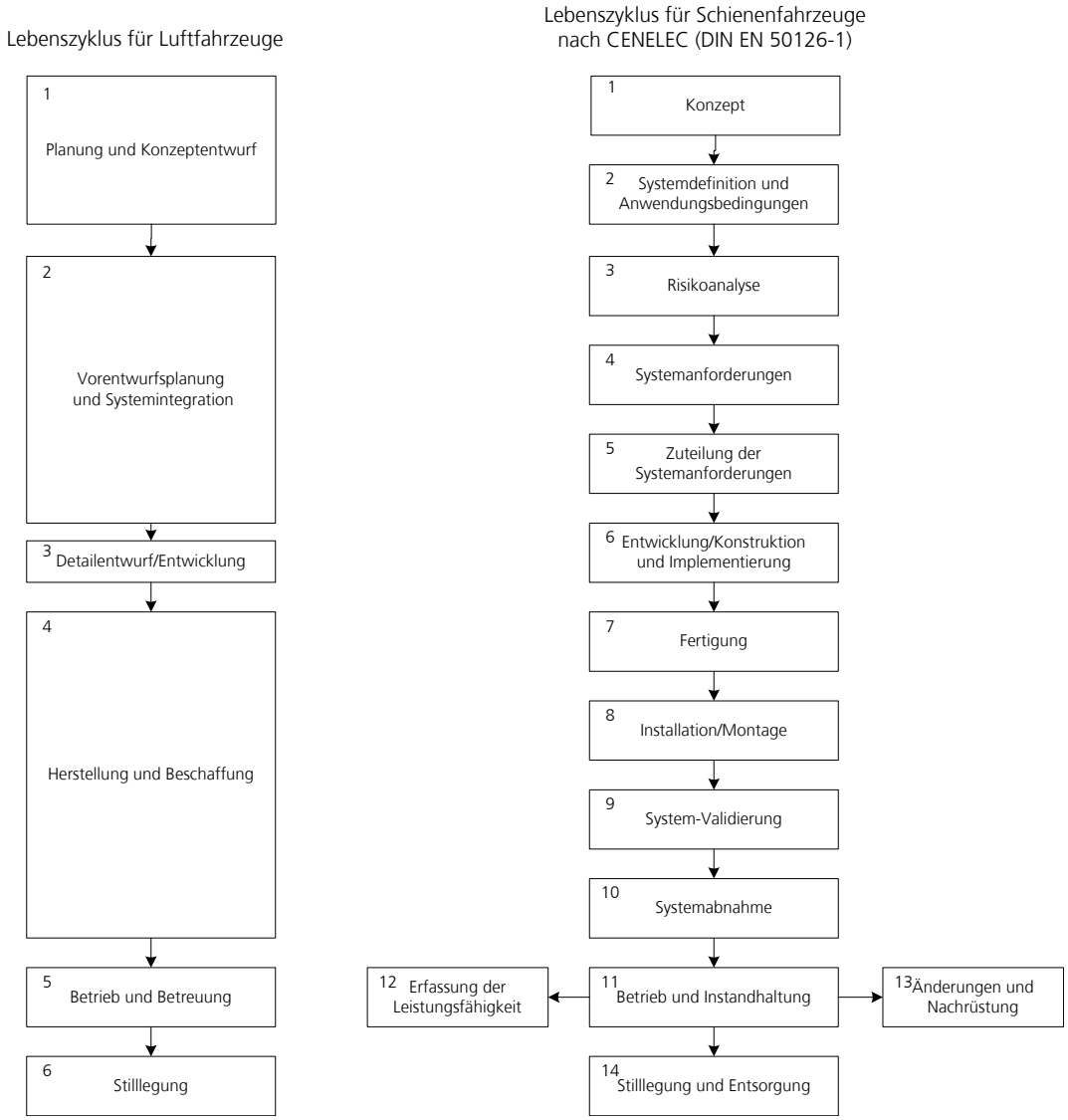

Abbildung 5.1: Lebenszyklen für Luft- und Schienenfahrzeuge

5.1.2 Lebenszyklus für Luftfahrzeuge

Es gibt keinen fest definierten Lebenszyklus für Luftfahrzeuge. Die weiteren Beschreibungen erfolgen an den in Abbildung 5.1 gezeigten Phasen [26]. Dieser Lebenszyklus besteht aus insgesamt sechs Stufen:

1. Planung und Konzeptentwurf,
2. Vorentwurfsplanung und Systemintegration,
3. Detailentwurf und Entwicklung,
4. Herstellung und Beschaffung,
5. Betrieb und Betreuung,
6. Entsorgung.

Zu Beginn eines Luftfahrzeugprojekts werden in der Phase *Planung und Konzeptentwurf (1)* verschiedene Alternativen hinsichtlich der Betriebsparameter untersucht. Die Ergebnisse werden mit den Anforderungen des Marktes und den Verkaufsmöglichkeiten verglichen. Das zum Schluss ausgewählte Konzept wird in der *Vorentwurfsplanung und Systemintegration (2)* weiter bearbeitet. Dazu wird das System in verschiedene Bereiche untergliedert, die dann einzeln bearbeitet werden. Am Ende werden in der Systemintegration die einzelnen Komponenten wieder zusammengefügt. In der Phase *Detailentwurf und Entwicklung (3)* wird das System weiter verfeinert. Es werden Prototypen hergestellt und getestet. Zudem wird die Produktion vorbereitet. Die vierte Phase beinhaltet die *Herstellung und Beschaffung*. Es folgen *Betrieb und Betreuung (5)*. Das Ende des Lebenszyklus bildet die *Stilllegung (6)*. [49]

Lebenszyklus für Schienenfahrzeuge

Der von der CENELEC in der DIN EN 50126-1 [12] veröffentlichte Lebenszyklus für Bahnanwendungen (Abbildung 5.1) besteht aus insgesamt 14 Phasen:

1. Konzept,
2. Systemdefinition und Anwendungsbedingungen,

3. Risikoanalyse,
4. Systemanforderungen,
5. Zuteilung der Systemanforderungen,
6. Entwicklung/Konstruktion und Implementierung,
7. Fertigung,
8. Installation und Montage,
9. System-Validierung,
10. Systemabnahme,
11. Betrieb und Instandhaltung,
12. Erfassung der Leistungsfähigkeit,
13. Änderung und Nachrüstung,
14. Stilllegung und Entsorgung.

Die Norm enthält für jede Stufe Angaben über die Ziele, Anforderungen, Ergebnisse und ihre Dokumentation sowie Verifikations- und Validierungsaufgaben. Der Lebenszyklus verbindet „Planung, Management, Überprüfung und Überwachung aller Systemaspekte, einschließlich RAMS“ [12]. Die folgende kurze Beschreibung der Zielstellungen der einzelnen Phasen entspricht der DIN EN 50126-1 [12].

Die erste Phase, das *Konzept*, bildet die Grundlage für alle weiteren Vorgänge. Sie soll einen Überblick des geplanten Systems, der Umgebung und der Überprüfung der RAMS-Auswirkungen geben. Die nächste Stufe umfasst die Beschreibung der *Systemdefinition und Anwendungsbedingungen*. Auf Basis des Betriebsaufgabenprofils und der Systemdefinition werden Anwendungsvoraussetzungen, z. B. Betriebs- und Instandhaltungsstrategien, identifiziert. Für das Gesamtsystem wird ein Sicherheitsplan erstellt. Im Anschluss wird die *Risikoanalyse (3)* durchgeführt, die die Identifizierung von Gefahren und ihrer Ursachen sowie die Bestimmung des damit verbundenen Risikos beinhaltet. Zur Risikoerfassung und -kontrolle wird das Gefahrenprotokoll erstellt. Die Risikoanalyse

muss bei Bedarf zu einem späteren Zeitpunkt wiederholt werden. Als nächstes werden die *Anforderungen an das System (4)* und alle Nachweis- und Abnahmekriterien hinsichtlich Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit und Sicherheit (RAMS) festgelegt. Ferner wird ein Validierungsplan erstellt. In der fünften Phase erfolgt die *Zuteilung der Systemanforderungen* auf die Komponenten und Subsysteme. Daran schließt sich die *Entwicklung/Konstruktion und Implementierung (6)* der Komponenten und Subsysteme an. Gleichfalls ist der Nachweis zu führen, dass diese den zuvor aufgestellten Anforderungen genügen. Während der *Fertigungsphase (7)* soll ein Prozess eingeführt werden, dessen Erzeugnisse den RAMS-Spezifikationen entsprechen. Es werden ebenfalls Unterstützungsmaßnahmen, z. B. die Dokumentationserstellung oder die Schulungsvorbereitung, gefordert. Das Gesamtsystem wird im Verlauf der *Installation und Montage (8)* aus den Einzelkomponenten und -subsystemen zusammengesetzt. Parallel erfolgt die Fortsetzung weiterer Support-Maßnahmen, u. a. die Ersatzteil- und Werkzeugbereitstellung. Das Ziel der *System-Validierung (9)* ist die Bestätigung, dass das Produkt den Anforderungen für den bestimmungsgemäßen Gebrauch entspricht sowie die Inbetriebnahme aller Systemteile und externen Maßnahmen zur Risikominderung. Anwendungsspezifische Systemsicherheitsnachweise werden vorbereitet und durchgeführt. Die Beurteilung der RAMS-Nachweise wird während der *Systemabnahme (10)* vollzogen. Der Betrieb, die Instandhaltung und Unterstützungsmaßnahmen sind derart auszuführen, dass im Verlauf des *Betriebs und der Instandhaltung (11)* die RAMS-Kriterien an das System erfüllt werden. Die zwölfte Phase, *Erfassung der Leistungsfähigkeit*, dient der Überprüfung, ob die Leistungsansprüche weiterhin eingehalten werden. Änderungen am System fallen in die Phase *Umrüstung und Nachrüstung (13)*. Das Ende des Lebenszyklus bildet die Planung und Steuerung der *Stilllegung und Entsorgung (14)*.

5.1.3 Anforderungsarten

Die Auslegung eines Systems erfolgt immer anhand der vorgegebenen Anforderungen. Diese können in verschiedene Anforderungsarten eingeteilt werden. Die ARP 4754 [3] nennt für den Bereiche Luftverkehr die Gruppen:

- Sicherheitsanforderungen,
- Funktionale Anforderungen,

- Zusätzliche Zulassungsanforderungen,
- Abgeleitete Anforderungen.

Die Sicherheitsanforderungen enthalten die minimalen Leistungsauflagen bezüglich der Integrität und Verfügbarkeit einer Funktion. Für den Betrieb wichtige Vorgaben sind in den funktionalen Anforderungen festgelegt. Diese werden auf Basis der geplanten Einsatzbedingungen und Kundenwünsche erstellt. Zusätzliche Anforderungen können zum Erfüllen weiterer Vorgaben notwendig werden. Auflagen, die aus dem Entwurfsprozess heraus entstehen, werden als abgeleitete Anforderungen bezeichnet.

Die DIN EN 50129 [14] untergliedert die Sicherheitsanforderungen zusätzlich in:

- Funktionale Sicherheitsanforderungen,
- Sicherheitsintegritätsanforderungen.

Die DIN EN 50126-1 [12] benennt außerdem die RAMS-Anforderungen bezüglich Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit und Sicherheit als Teil der Gesamtanforderungen.

5.2 Sicherheitsnachweisführung im Luftverkehr

5.2.1 Risikoanalyse und Gefährdungsbeherrschung

Ein generischer Entwicklungsprozess für Luftfahrzeuge wird in der ARP 4754 [3] beschrieben. Die verschiedenen Entwicklungsschritte verlaufen oftmals parallel und sind voneinander abhängig. Einzelne Änderungen können weitere nach sich ziehen und zu Aktualisierungen der Risikoanalysen führen. Der Sicherheitsanalyseprozess ist in Abbildung 5.2 dargestellt.

Das Flugzeug bildet die oberste Ebene, die aus mehreren Systemen besteht. Zuerst werden im Rahmen eines Functional Hazard Assessments (FHA) (5.4.10) die funktionalen Anforderungen auf Flugzeugebene sowie mögliche Versagensarten identifiziert. Entsprechend der Klassifizierung der Versagensarten erfolgt die Einstufung der Development Assurance Level (DAL). Als nächstes werden die Flugzeugfunktionen den Systemen zugeordnet und jeweils ein System-FHA durchgeführt. Im Anschluss werden im Preliminary System Safety Assessment (PSSA) (5.4.10) die zu den im FHA ermittelten Versagensarten

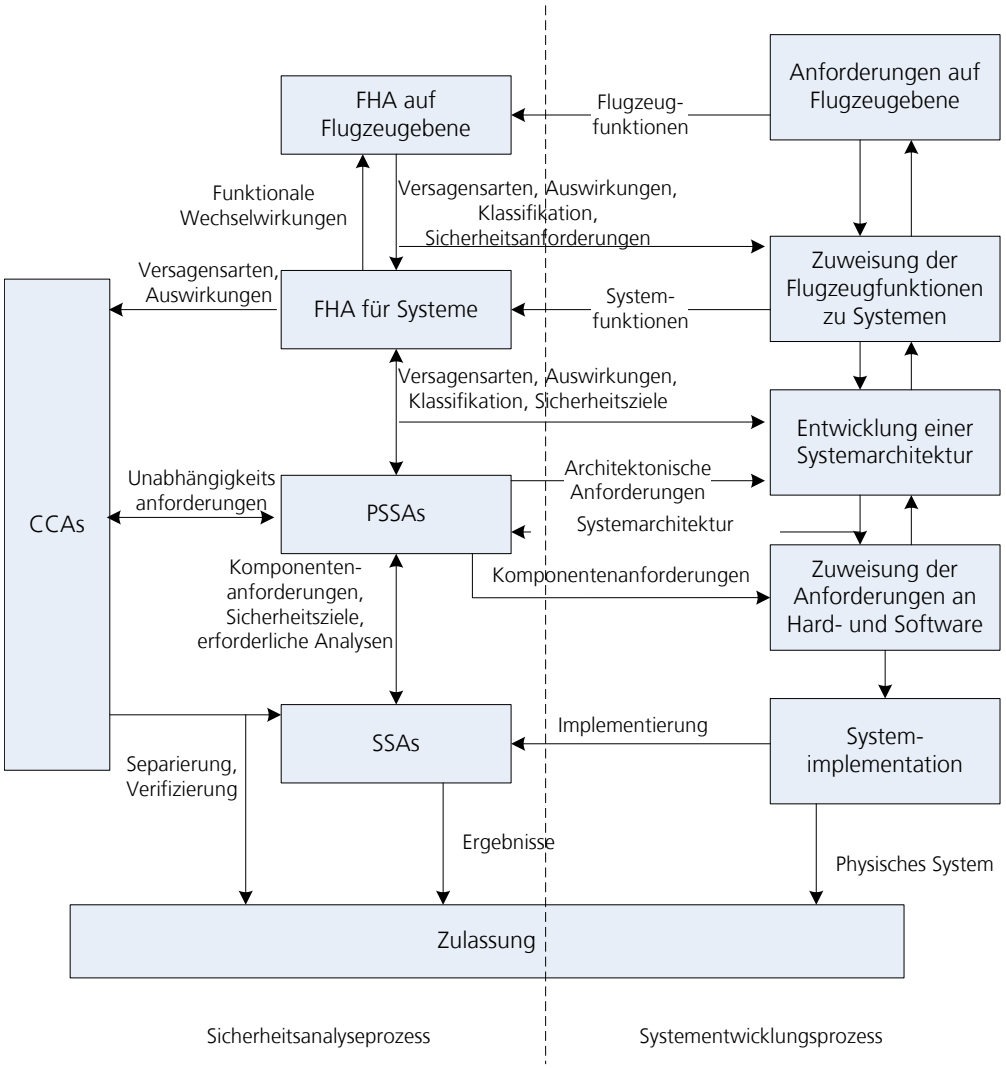

Abbildung 5.2: Sicherheitsanalyse- und Systementwicklungsprozess aus ARP 4754 [3]

gehörenden Ausfälle identifiziert. Das PSSA überprüft ferner die Systemarchitektur darauf, ob die gestellten Anforderungen erreicht werden können. Ist das nicht der Fall, müssen abgeleitete Sicherheitsanforderungen aufgestellt werden. Das gilt ebenso für die Komponentenanforderungen, die der Hard- und Software zugewiesen werden. Für die Überprüfung der Unabhängigkeitforderungen während des FHA und PSSA wird die Common Cause Analysis (CCA) (5.4.1) eingesetzt. Ihre Ergebnisse werden im System Safety Assessment (SSA) (5.4.10) zur Verifizierung der Systemimplementierung mit den zuvor aufgestellten Anforderungen genutzt.

Innerhalb des FHA und PSSA werden bei Bedarf andere Methoden angewandt, z. B. eine Fehlerbaumanalyse (FTA), Markov-Analyse oder Fehler-Möglichkeits- und Einfluss-Analyse (FMEA).

5.2.2 Risikoakzeptanzkriterium im Luftverkehr

Die während der FHA identifizierten Versagensarten werden hinsichtlich ihrer Schwere klassifiziert. Diese Klassen reichen von *Keine Sicherheitsauswirkungen* bis zu *Katastrophal*. Die Einstufung erfolgt entsprechend der in Tabelle 5.1 aufgeführten Auswirkungen auf das Flugzeug, die Insassen und die Flugbesatzung. Die tolerierbare Gefährdungsrate lässt sich anhand Tabelle 5.2 ermitteln. Für jede Klassifikationsstufe der Versagensarten wird eine zulässige qualitative und quantitative Wahrscheinlichkeit angegeben. Als Bezugsgröße wird die *durchschnittliche Wahrscheinlichkeit je Flugstunde* zugrunde gelegt. Die Ermittlung des Wertes für die Klasse *Katastrophal* wird in der CS-25 [9] beschrieben. Den Ausgangspunkt bildete die aus historischen Werten bestimmte Wahrscheinlichkeit eines schweren Unfalls mit $1\ pro\ 1\ Million\ Flugstunden$. Davon wurden 10% durch Ausfälle von Flugzeugsystemen verursacht. Dieser Wert von $10^{-7}\ pro\ Flugstunde$ soll für Flugzeugneuentwürfe nicht überschritten werden. Da dieser Wert während des Entwurfs schwer zu ermitteln ist, wird weiterhin angenommen, dass in einem Flugzeug hundert potentielle katastrophale Versagenszustände existieren. Damit ergibt sich für die durchschnittliche Eintrittswahrscheinlichkeit katastrophaler Versagenszustände ein Grenzwert von $10^{-9}\ pro\ Flugstunde$. Dieser Wert wird als Grenze für *extrem unwahrscheinlich* angenommen. Die Werte für weniger schwerwiegende Versagensarten sind entsprechend geringer. [9]

Tabelle 5.1: Beschreibung der Auswirkungen auf Flugzeug, Insassen und Flugbesatzung in den Klassen der Versagensarten (nach AMC 25.1309 [9])

Klassifikation der Versagensart	Keine Sicherheitsauswirkungen	Gering	Groß	Gefährlich	Katastrophal
Auswirkungen auf Flugzeug	Keine Auswirkungen auf operationelle Fähigkeiten oder Sicherheit	geringe Beeinträchtigung der funktionalen Fähigkeiten oder Sicherheitsspannen	Signifikante Beeinträchtigung der funktionalen Fähigkeiten oder Sicherheitsspannen	Große Beeinträchtigung der funktionalen Fähigkeiten oder Sicherheitsspannen	In der Regel mit Flugzeugverlust
Auswirkungen auf Insassen (ohne Flugbesatzung)	Unannehmlichkeit	Physisches Unbehagen	Physische Beschwerden, ev. mit Verletzungen	Ernste/tödliche Verletzungen weniger Passagiere/ Kabinenbesatzung	mehrere Todesfälle
Auswirkungen auf Flugbesatzung	Keine Auswirkungen	Geringe Steigerung der Workload	Physisches Unbehagen oder signifikanter Anstieg der Workload	Physische Beschwerden oder übermäßige Workload beeinträchtigt die Fähigkeit zur Aufgabenerfüllung	Todesfälle oder Arbeitsunfähigkeit

Tabelle 5.2: Beschreibung der Klassifikationen der Versagensarten (nach AMC 25.1309 [9])

Klassifikation der Versagensart	Keine Sicherheitsauswirkungen (No Safety Effect)	Gering (Minor)	Bedeutend (Major)	Gefährlich (Hazardous)	Katastrophal (Catastrophic)
zulässige qualitative Wahrscheinlichkeit	Keine Anforderungen	wahrscheinlich (probable)	unwahrscheinlich (remote)	sehr unwahrscheinlich (extremely remote)	extrem unwahrscheinlich (extremely improbable)
Beschreibung der qualitativen Wahrscheinlichkeit in *durchschnittliche Wahrscheinlichkeit je Flugstunde*		ein- oder mehrmals während des Flugzeuglebens	unwahrscheinlich während einzelnen Flugzeuglebens, mehrmals in der Flotte	nicht erwartet während einzelnen Flugzeuglebens, mehrmals in der Flotte	nicht erwartet in der gesamten Flotte
zulässige quantitative Wahrscheinlichkeit	Keine Anforderungen	$< 10^{-3}$	$< 10^{-5}$	$< 10^{-7}$	$< 10^{-9}$

5.3 Sicherheitsnachweisführung im Schienenverkehr

Mit Einführung der DIN EN 50126-1 [12] im Jahre 1999 wurde der zuvor gültige regelorientierte Sicherheitsansatz durch einen risikoorientierten abgelöst. Während früher die Einhaltung zuvor aufgestellter detaillierter Vorschriften nachgewiesen werden musste, ist jetzt der Nachweis der Abwesenheit eines zu hohen Risikos erforderlich. Dafür werden zuvor akzeptable Risiken festgelegt. Dieser, dem technischen Fortschritt gegenüber aufgeschlossenere neue Ansatz, wurde durch die Europäische Union (EU) zur Förderung des Wettbewerbs eingeführt. Es wird davon ausgegangen, dass keine absolute Sicherheit

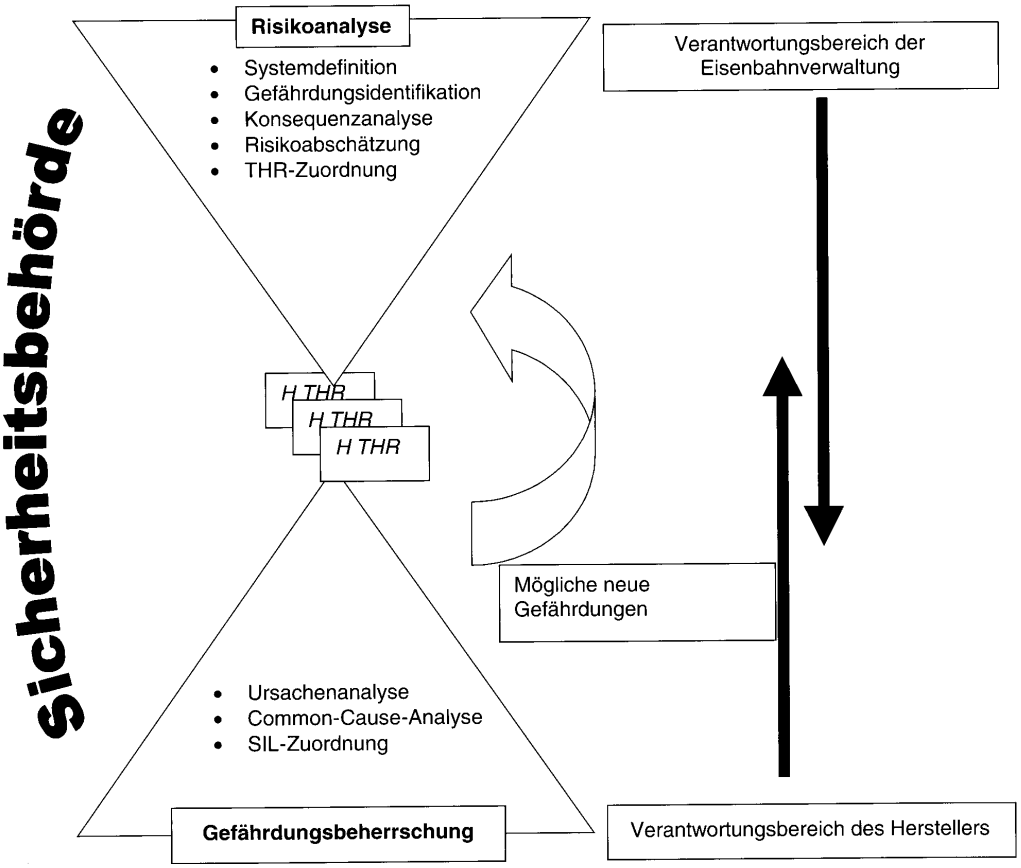

Abbildung 5.3: Bestimmung und Zuteilung der Sicherheitsintegritätsanforderungen (Quelle: DIN EN 50129 [14])

erreicht werden kann. Deshalb muss nachgewiesen werden, dass das Restrisiko einen akzeptablen Wert nicht übersteigt. [8]

Die Sicherheitsnachweisführung wird in der DIN EN 50129 [14] beschrieben. Sie besteht aus:

- Risikoanalyse,
- Gefährdungsbeherrschung.

Der Gesamtprozess mit den Verantwortlichkeiten der Eisenbahnverwaltung und Hersteller ist in Abbildung 5.3 dargestellt. Im Rahmen der Risikoanalyse (5.3.1) werden tolerierbare Gefährdungsraten (THR) aufgestellt. Die Gefährdungsbeherrschung (5.3.2) muss aufzeigen, dass die Gefährdungsrate (H) diesen Wert nicht überschreitet.

5.3.1 Risikoanalyse

Die Risikoanalyse wird von der Eisenbahnverwaltung durchgeführt. Das Ziel besteht in der Zuordnung der tolerierbaren Gefährdungsraten (THR). Der Prozess kann in die folgenden Schritte unterteilt werden [14]:

1. Systemdefinition,
2. Gefährdungsidentifikation,
3. Konsequenzanalyse,
4. Risikoabschätzung,
5. THR-Zuordnung.

Die ersten beiden Schritte dienen der Systemdefinition und Identifizierung der möglichen Gefährdungen für das System. Die Identifikation erfolgt in zwei Phasen:

- empirische Phase (z. B. Checklisten, historische Werte) sowie
- kreative Phase (z. B. Brainstorming).

Tabelle 5.3: Tolerierbare Gefährdungsraten (THR) und Sicherheitsanforderungsstufen (SIL) [14]

Tolerierbare Gefährdungsrate (THR) pro Stunde und pro Funktion	Sicherheitsanforderungsstufe (SIL)
$10^{-9} \leq THR < 10^{-8}$	4
$10^{-8} \leq THR < 10^{-7}$	3
$10^{-7} \leq THR < 10^{-6}$	2
$10^{-6} \leq THR < 10^{-5}$	1

Aus Gründen der Übersichtlichkeit sollten die gefundenen Gefährdungen nach ihrer Risikohöhe sortiert werden. Anschließend folgt die Ermittlung der Folgen der Gefährdungen. Diese Schritte können z. B. mit einer FMEA (5.4.4) durchgeführt werden. Weiterhin ist ein Risikoakzeptanzkriterium (5.3.3) zu bestimmen. Die DIN EN 50129 stellt an dieser Stelle drei Kriterien vor, die Auswahl wird jedoch dem Anwender überlassen. Auf Grundlage dessen sind die THRs abzuleiten und den Gefährdungen zuzuordnen. [14]

5.3.2 Gefährdungsbeherrschung

Die Aufgabe des Herstellers liegt in der Gefährdungsbeherrschung. Er muss nachweisen, das sein System die aufgestellten THRs erfüllt. Die Gefährdungsbeherrschung wird in drei Schritten durchgeführt [14]:

1. Ursachenanalyse,
2. Common-Cause-Analyse,
3. SIL-Zuordnung.

Im Rahmen der Ursachenanalyse erfolgt zuerst, falls noch nicht geschehen, für jede Gefährdung die Zuordnung der THR zu einer Systemfunktion. Die Zuweisung der ensprechenden Sicherheitsintegritätslevel (SIL) erfolgt auf Basis der SIL-Tabelle (Tab. 5.3). Die Stufe vier steht für die höchsten Anforderungen. Ist $THR \geq 10^{-5}$ wird die Sicherheitsanforderungsstufe 0 zugewiesen. Für ein Teilsystem mit mehreren sicherheitsrelevanten Funktionen ist die höchste SIL-Einstufung maßgebend. Zur Reduzierung der daraus entstehenden Erfordernisse, können die Funktionen und Subsysteme getrennt werden. In diesem Fall ist eine

Nachweis der Unabhängigkeit erforderlich. Der zweite Teil der Ursachenanalyse beinhaltet die Zuordnung der Ausfallraten zu den Elementen. In der Ursachenanalyse können z. B. Fehlerbäume (5.4.3), Zuverlässigkeitsblockdiagramme (5.4.9) oder Markov-Modelle (5.4.7) genutzt werden. Zum Nachweis der physikalischen, funktionalen und prozessmäßigen Unabhängigkeit der Funktionen muss eine Common-Cause-Analyse (5.4.1) durchgeführt werden. Während des Entwurfs können neue Gefährdungen auftreten, die ebenfalls identifiziert und bewertet werden müssen. Für jede neue Gefährdung muss eine THR bestimmt werden. Falls erforderlich, muss eine Aktualisierung der Anforderungen erfolgen.

Es müssen alle aufgestellten THRs eingehalten werden. Andernfalls muss der Hersteller an seinem Systementwurf Nachbesserungen vornehmen.

5.3.3 Risikoakzeptanzkriterium

Für den Schienenverkehr wird weder von den Zulassungsbehörden noch von den Normen oder Richtlinien ein Risikoakzeptanzkriterium vorgegen. Die DIN EN 50126-1 [12] führt drei Risikogrundsätze als Beispiel an:

- As Low As Reasonably Practicable (ALARP),
- Globalement Au Moins Aussi Bon (GAMAB),
- Minimum Endogenous Mortality (MEM).

Die Erfahrungen und allgemeine Akzeptanz der Verfahren sind dabei sehr verschieden. Die Auswahl eines Kriteriums wird letztlich dem Anwender überlassen. Es muss jedoch sowohl den europäischen als auch den nationalen Anforderungen entsprechen. Deshalb wird an dieser Stelle als viertes Prinzip noch das Kriterium

- Mindestens gleiche Sicherheit (MGS)

aufgeführt, dass auf der EBO basiert. [12, 6]

ALARP – As Low As Reasonably Practicable

„so niedrig wie vernünftigerweise ausführbar“ [12]

Der ALARP-Grundsatz wird hauptsächlich in Großbritannien angewandt. Er unterscheidet die drei in Abbildung 5.4 dargestellten Bereiche. Sind die Risiken gering und die notwendigen Aufwendungen zur weiteren Reduzierung im Verhältnis unangemessen hoch, können sie auf diesem Stand belassen werden. Im ALARP-Bereich werden Risiken akzeptiert, wenn die Kosten für eine Minderung zu hoch wären. Das Risiko an sich muss aber noch vertretbar sein. Sind die aus den Risiken resultierenden Ereignisse nicht mehr zu rechtfertigen, gelten sie als inakzeptabel und müssen vermieden werden. Der Nachweis des ALARP-Kriteriums kann durch die Anwendung von bewährten Normen und Verfahren erfolgen. Andernfalls muss ein Kostenvorteil verglichen mit dem Wert des Lebens aufgezeigt werden. [12]

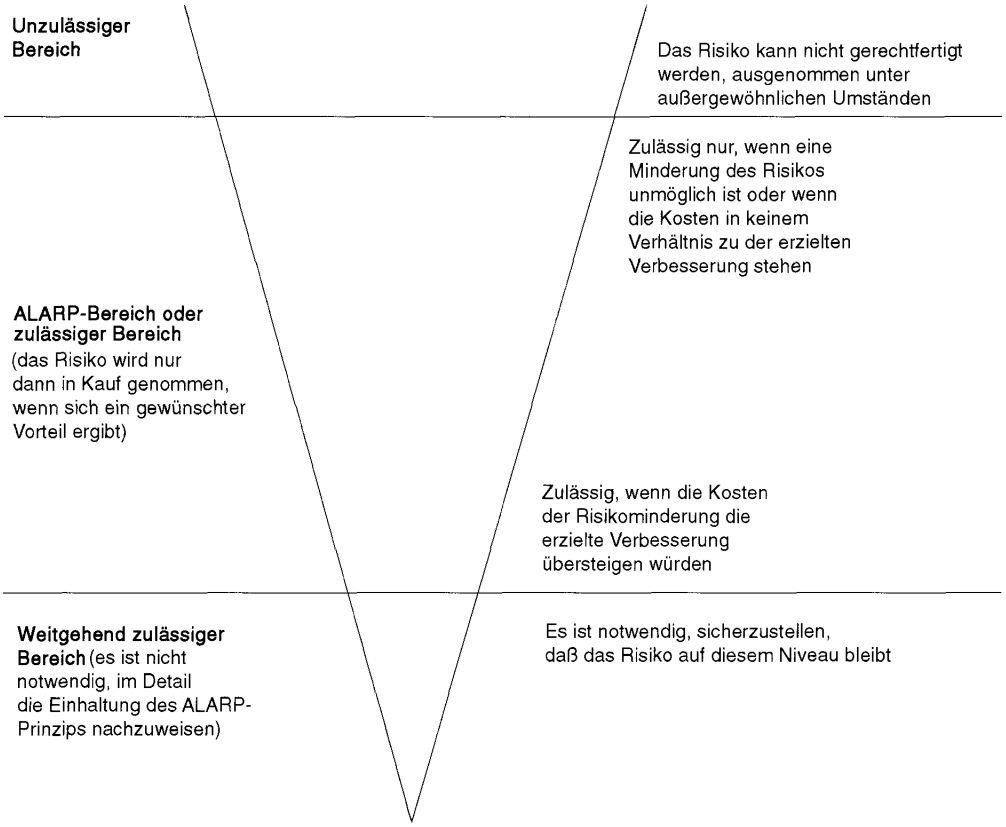

Abbildung 5.4: Bereiche des ALARP-Grundsatzes (Quelle: DIN EN 50126-1 [12])

GAMAB – Globalement Au Moins Aussi Bon

„Alle neuen spurgeführten Transportsysteme müssen insgesamt einen globalen Sicherheits-Level bieten, der mindestens so hoch ist wie der in irgendeinem vergleichbaren existierenden System.“ [12]

Dieses Prinzip setzt den derzeitigen Sicherheitsstand als Mindestanforderung. Neue Systeme müssen diesen Stand wenigstens erreichen. Dadurch werden technische Fortschritte im Laufe der Zeit gefordert. Es wird jedoch kein spezielles Risiko zu Grunde gelegt, sondern es erfolgt eine globale Betrachtung. Daraus können sich Unterschiede zwischen dem derzeitigen tatsächlichen Stand und den Anforderungen ergeben. Dieses Prinzip wird vor allem in Frankreich angewendet. Es ähnelt dem Kriterium *MGS – Mindestens die gleiche Sicherheit*. [12]

MEM – Minimum Endogenous Mortality

„minimale endogene Sterblichkeit“ [12]

Dem Prinzip der minimalen endogenen Sterblichkeit liegt die Annahme zugrunde, dass ein Teil der Todesfälle in die Gruppe *Technologische Tatsachen*, z. B. Verkehr, Sport, Arbeitsmaschinen, fällt. Todesfälle durch Krankheit oder angeborene Gesundheitsschäden zählen nicht dazu. Als *Endogene Sterblichkeit R* wird der Anteil der Todesfälle dieser Gruppe je Person und Jahr bezeichnet. Dieser Wert ist abhängig von der Altersgruppe. Am niedrigsten ist er bei den 5- bis 15-jährigen. Danach wurde der Wert für die *minimale endogene Sterblichkeit* mit $2 \cdot 10^{-4}$ festgelegt. Diese Zahl darf durch ein neues System nicht merklich erhöht werden. Bei vielen möglichen Todesfällen wird noch die Risikoaversion berücksichtigt, wodurch die Schwelle für Todesfälle (R_1) sinkt. In der Praxis wurde dieses Prinzip in Deutschland noch nicht angewandt [6]. [12]

MGS – Mindestens gleiche Sicherheit

Das Prinzip Mindestens gleiche Sicherheit (MGS) wird zwar nicht in der DIN EN 50126-1 [12] aufgeführt, es basiert jedoch auf der Forderung der EBO [15] nach der Einhaltung der anerkannten Regeln der Technik. Dazu heißt es weiterhin: „Von den anerkannten Regeln der Technik darf abgewichen werden, wenn mindestens die gleiche Sicherheit wie bei Beachtung dieser Regeln nachgewiesen ist.“ [15, § 2 (2)] Als Vergleichsbasis für

die Risikoakzeptanz nach MGS werden die anerkannten Regeln der Technik zugrunde gelegt. Es ähnelt damit dem GAMAB-Kriterium, das das globale System betrachtet. Beiden ist jedoch gleich, dass sie keine festen Werte haben, sondern den derzeit existierenden Stand als Referenzwert heranziehen, der nicht unterschritten werden darf. Damit wird bei technischem Fortschritt auch der Bezugswert erhöht. [6]

5.4 Verfahrensübersicht

Eine wichtige Voraussetzung für die Zulassung von Verkehrsmitteln ist der Nachweis der Aufgabenerfüllung. Zu diesem Zweck können verschiedene Methoden angewendet werden. Sie sollen es ermöglichen, Ausfälle, Gefährdungen und die Auswirkungen sowie die Verbindungen untereinander zu identifizieren. Diese Analysen gestatten die Bewertung der betrachteten Systeme. Die Methoden verfolgen zwei verschiedene Analyseansätze: induktiv oder deduktiv. Die induktiven Verfahren werden auch als Bottom-Up-Verfahren bezeichnet. Sie gehen vom speziellen zum allgemeinen. Dazu zählt die Untersuchung der Auswirkungen eines bestimmten Ereignisses, z. B. Versagen. Beispiele für induktive Methoden sind die Ereignisbaumanalyse (ETA) oder auch Fehler-Möglichkeits- und Einfluss-Analyse (FMEA). Die deduktiven oder auch Top-Down-Verfahren folgen dem entgegengesetzten Weg. Die Untersuchung geht vom allgemeinen zum speziellen. Sie werden z. B. zur Identifizierung der Ursachen eines Ausfalls genutzt. Ein Vertreter dieser Art ist die Fehlerbaumanalyse (FTA). Weiterhin wird noch zwischen qualitativen und quantitativen Ansätzen unterschieden. Qualitative Analysen betrachten ein System in einer nichtnummerischen Art. Sie modellieren das System mit den verschiedenen Ereignissen. Sind ausreichend Werte für eine mathematische Betrachtung vorhanden, kann eine quantitative Analyse durchgeführt werden. Diese beiden Ansätze kommen in allen Methoden zusammen vor. In einem qualitativen Verfahren wird oft bewertet, wie wahrscheinlich ein Ereignis ist. Andererseits ist die Systemmodellierung mit einem qualitativen Verfahren die Voraussetzung für die Durchführung einer quantitativen Betrachtung [21]. Die Schwerpunkte der Methoden können jedoch in einem der beiden Ansätze liegen. [41, 9]

Die Auswahl geeigneter Nachweisverfahren ist abhängig von den Zielsetzungen, dem Systemumfang und den betrachteten Bereichen. Die Methoden können in unterschiedlichen Phasen des Lebenszyklus angewandt werden. Dabei gilt, je früher Probleme erkannt werden,

umso leichter und kostengünstiger können sie behoben werden. Viele Methoden wurden ursprünglich in Bereichen mit hohen Sicherheitsanforderungen entwickelt, für das Militär, die chemische Industrie, den Luftverkehr oder die Kernenergie. Später wurden sie auch von anderen Bereichen übernommen.

Die Auswahl der in diesem Abschnitt vorgestellten Methoden erfolgte auf Grundlage ihrer Erwähnung in den Vorgaben zum Sicherheitsnachweis in den Normen ARP 4754 [3] und DIN EN 50129 [14]. Weiter werden einige Verfahren aufgelistet, die mehrfach in diesem Zusammenhang in der Literatur aufgeführt werden. Die Liste ist nicht vollständig und es existieren auch viele Verfahren für spezielle Bereiche, z. B. eine Elektromagnetische Kompatibilitätsanalyse. Viele Methoden haben mehrere Namen, oftmals aufgrund der Übersetzungen aus der Ursprungssprache. Bei den einzelnen Verfahren werden auch verschiedene Namen und die verwendeten Quellen angegeben. Die untersuchten Verfahren finden zum Teil sowohl im Luft- als auch Schienenverkehr Anwendung. Einige andere Methoden stammen direkt aus dem Luftverkehr.

Eine Aufstellung der in diesem Kapitel vorgestellten Methoden ist Tabelle 5.4 zu finden.

Tabelle 5.4: Auflistung der beschriebenen Methoden und ihre Anwendungsbereiche

Methode	Bereich	
	Luft	Schiene
Common Cause Analysis (CCA)	•	•
Ereignisbaumanalyse (ETA)	•	•
Fehlerbaumanalyse (FTA)	•	•
Fehler-Möglichkeits- und Einfluss-Analyse (FMEA)	•	•
Fehler-Möglichkeits-, Einfluss- und Kritikalitäts-Analyse (FMECA)	•	•
Gefahren- und Operabilitätsstudie (HAZOP)	•	•
Markov-Analyse	•	•
Preliminary Hazard Analysis (PHA)	•	•
Zuverlässigkeitsblockschaltbild (RBD)	•	•
Functional Hazard Assessment (FHA)	•	
Preliminary System Safety Assessment (PSSA)	•	
System Safety Assessment (SSA)	•	

5.4.1 Common Cause Analysis (CCA)

Unter folgenden Namen aufgeführt:

- Common Cause Analysis (CCA)
- Common Cause Failure Analysis (CCFA)
- Allgemeine Ursachenanalyse
- Analyse gemeinsamer Fehler

Quellen: CS-25 [9], ARP 4754 [3], Federal Aviation Administration (FAA) u. EUROCONTROL [22], FAA Handbook [21], DIN EN 50128 [13], SoKo [20]

Die Common Cause Analysis (CCA) dient der Überprüfung der Unabhängigkeitsforderungen, die während der Sicherheitsanalysen von diversen Methoden vorausgesetzt werden. Zu diesem Zweck wird sie in der ARP 4754 [3] für den Luftverkehr sowie in der DIN EN 50129 [14] für Bahnanwendungen angeführt. Bei Systemen oder Komponenten gleicher Ausführung, Verwendung gleicher Komponenten oder physischer Nähe können Ausfälle infolge gemeinsamer Ursachen (Common Cause Failures) auftreten. Die CCA identifiziert derartige Ausfälle und liefert Ansätze zur Korrektur und Fehlereindämmung. Dies kann durch Trennung der Backup- und Schutzsysteme oder unterschiedliche Umsetzungen erreicht werden. Diese Methode sollte bereits zeitig in der Entwicklung angewandt werden. An einigen Stellen werden die notwendigen Daten jedoch erst später zur Verfügung stehen. Die untersuchten Ursachen der Ausfälle können z. B. zu den Bereichen Hard- oder Software-Entwicklungsfehler, Programmier-, Anforderungs-, Herstellungsfehler, Hardwareausfälle oder umgebungsbedingte Faktoren sein. Die Common Cause Analysis (CCA) kann in fünf Schritte unterteilt werden:

1. Identifizierung und Gruppenbildung kritischer Komponenten,
2. Prüfung auf Gemeinsamkeiten innerhalb der Gruppen,
3. Prüfung auf glaubhafte Versagensarten innerhalb der Gemeinsamkeiten,
4. Identifizierung potentieller Auslöser für identifizierte Ausfallarten,

5. Zusammenfassung der Ergebnisse, Aufstellen von Eindämmungs- und Korrekturstrategien.

Die Identifizierung der Kandidaten für gemeinsame Fehler kann mit einer Fehlerbaumanalyse, einem Zuverlässigkeitsblockschaltbild, einer FMEA oder anderen zuvor durchgeführten Analysen erfolgen. Das FAA Handbook [21] bezeichnet die Common Cause Failure Analysis (CCFA) als eine Erweiterung der FTA. Es sollten besonders die Fehler beachtet werden, deren Eintrittswahrscheinlichkeit die Summe der Wahrscheinlichkeiten der Einzelfehler deutlich überschreitet. Die CCA selbst besteht nach ARP 4754 [3] aus drei Methoden, für die jeweils die zuvor aufgeführten Schritte durchgeführt werden müssen:

- Zonal Safety Analysis (ZSA),
- Particular Risk Assessment (PRA),
- Common Mode Analysis (CMA).

Die Anwendung der CCA erfordert ein tiefgehendes Systemwissen. Aufgrund des Umfangs ist es schwer, Grenzen für die Betrachtung zu ziehen.

Zonal Safety Analysis

Unter folgenden Namen aufgeführt:

- Zonal Analysis
- Zonal Safety Analysis (ZSA)
- Zonal Safety Analysis for Avionics

Quellen: CS-25 [9], ARP 4754 [3], Federal Aviation Administration (FAA) u. EUROCONTROL [22]

Die Zonal Safety Analysis (ZSA) betrachtet die Einhaltung der Sicherheitsanforderungen innerhalb einzelner Zonen und untereinander. Sie prüft, ob die Unabhängigkeitsanforderungen nicht durch physische Einflüsse oder Einrichtungen verletzt werden. Das Ziel der ZSA ist die Identifizierung der Quellen gemeinsamer Fehler sowie ihrer Auswirkungen auf Nachbarkomponenten. [9, 3, 22]

Particular Risk Analysis

Unter folgenden Namen aufgeführt:

- Particular Risk Analysis (PRA)
- Environmental-related Common Cause Analysis

Quellen: CS-25 [9], ARP 4754 [3], Federal Aviation Administration (FAA) u. EUROCONTROL [22]

Während der Particular Risk Assessment (PRA) werden die sicherheitsbeeinträchtigenden Auswirkungen und Einflüsse bestimmter Gefahren (z. B. Blitzeinschlag, Feuer, geplatzte Reifen) betrachtet. Für jede einzelne Gefahr muss eine eigene Untersuchung durchgeführt werden. Im Gegensatz zur Zonal Safety Analysis (ZSA) werden Ereignisse über mehrere Zonen hinweg betrachtet. Die hier ermittelten Ergebnisse können die Grundlage für spezifische Anforderungen (z. B. Lufttüchtigkeitsanforderungen) bilden.

Common Mode Analysis

Unter folgenden Namen aufgeführt:

- Common Mode Analysis (CMA)
- Process-related Common Mode Analysis

Quellen: CS-25 [9], ARP 4754 [3], Federal Aviation Administration (FAA) u. EUROCONTROL [22]

Die Common Mode Analysis (CMA) beschäftigt sich mit den Auswirkungen der Ereignisse, die noch nicht während der Particular Risk Assessment (PRA) berücksichtigt wurden (z. B. Fehler in den Anforderungen, der Instandhaltung, der Umgebung, des Entwurfs, der Spezifikationen). Sie prüft die Unabhängigkeit der Ereignisse, die als Versagensarten betrachtet wurden. Die CMA kann dabei in vier Schritten durchgeführt werden:

1. Erstellen von Checklisten,
2. Identifizierung der Anforderungen an die CMA,
3. Analyse des Entwurfs zum Nachweis der Anforderungen,
4. Dokumentation der Ergebnisse.

5.4.2 Ereignisbaumanalyse (ETA)

Unter folgenden Namen aufgeführt:

- Event Tree Analysis (ETA)
- Consequence Tree Method (CTM)
- Ereignisbaumanalyse

Quellen: Stephans u. Talso [36], DIN EN 50128 [13], Federal Aviation Administration (FAA) u. EUROCONTROL [22]

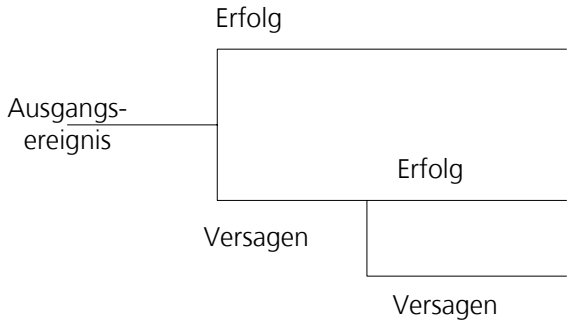

Abbildung 5.5: Darstellung eines Ereignisbaums

Die Ereignisbaumanalyse (ETA) ermöglicht es, Reihen von Ereignissen zu modellieren, die von dem betrachteten Ursprungsereignis ausgehen. Bei Vorhandensein der Wahrscheinlichkeiten für die einzelnen Ereignisse kann neben der qualitativen Betrachtung auch eine quantitative erfolgen. Ein Ereignisbaum ist in Abbildung 5.5 dargestellt. Zuerst wird ein Ausgangsereignis, z. B. eine Gefährdung, definiert. Für jede mögliche Konsequenz wird ein Zweig für das Eintreten (Erfolg) und Ausbleiben (Versagen) eröffnet. Anschließend erfolgt für jeden Zweig wieder die Betrachtung der möglichen Konsequenzen. Die Entscheidungen müssen nicht binärisch sein. Ebenso kann unterschieden werden zwischen zwei, ein oder null Teile defekt. Für die Durchführung ist eine gute Systemkenntnis erforderlich. Der Umfang, Aufwand und die Unübersichtlichkeit der Analyse nehmen mit der Komplexität des betrachteten Systems deutlich zu.

5.4.3 Fehlerbaumanalyse (FTA)

Unter folgenden Namen aufgeführt:

- Fehlerbaumanalyse
- Fault Tree Analysis (FTA)
- Cause Tree Method (CTM)

Quellen: Stamatelatos [33], Villemeur [41], CS-25 [9], Federal Aviation Administration (FAA) u. EUROCONTROL [22]

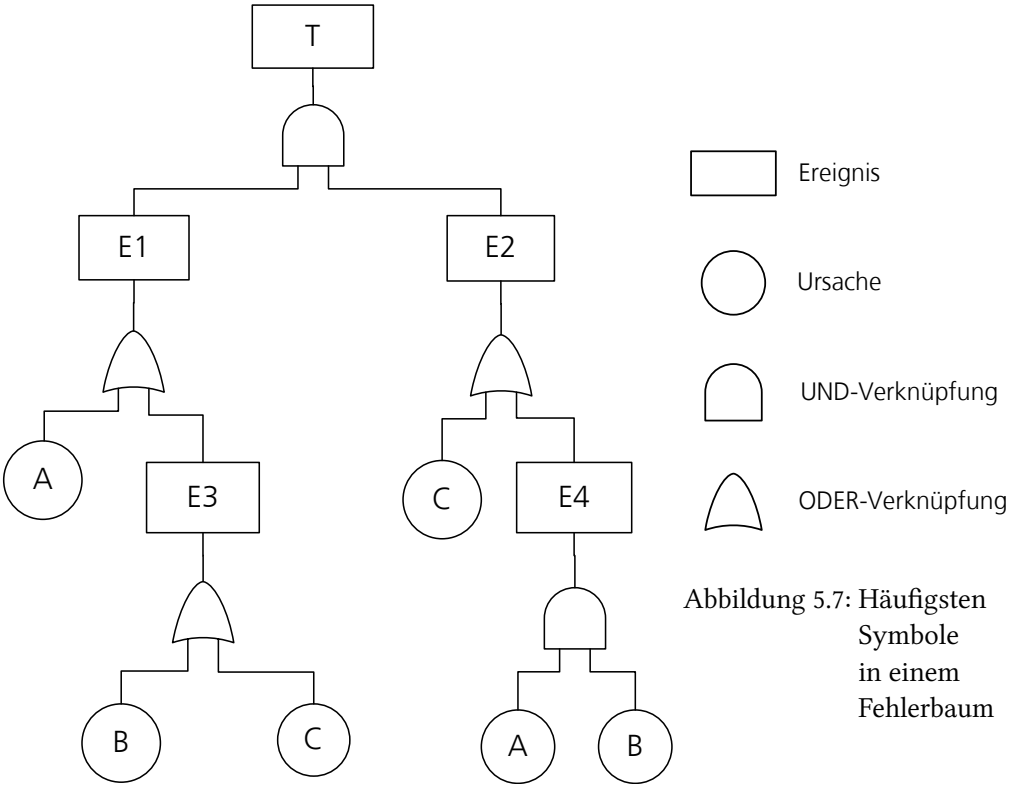

Abbildung 5.6: Darstellung eines Fehlerbaums

Abbildung 5.7: Häufigsten Symbole in einem Fehlerbaum

Die Fehlerbaumanalyse (FTA) ist eine deduktive graphische Methode zur Identifizierung der Ursachen für ein unerwünschtes Ereignis. Sie wurde zuerst in der Telekommunikationsindustrie angewandt und später auch in der Luft- und Raumfahrt sowie Kernenergie. In den letzten Jahren erfolgten Anpassungen, um die Erzeugung dynamischer Fehlerbäume und

die Nutzung für Software zu erleichtern.[33] Die FTA kann in allen Entwicklungsphasen angewandt werden, dennoch ist der Einsatz in der Entwicklung am effektivsten. Aufgrund ihres Umfangs ist allerdings eine vorherige Selektion der näher zu betrachtenden Ereignisse (z. B. mit Hilfe einer FHA, FMEA) sinnvoll. Sie kann für die Ursachenidentifizierung der in einer FHA ermittelten Gefährdungen genutzt werden. Für die Durchführung ist ein umfangreiches Systemwissen und -verständnis sowie Erfahrung unabdingbar. Trotz der Schwierigkeit, alle Möglichkeiten aufzuspüren, sollten alle denkbaren und vernünftigen Varianten identifiziert werden. Mit der FTA lassen sich Fehlerkombinationen und Bedienfehler darstellen. Sie kann auch für Software angewandt werden. Das Ergebnis ist eine graphische Aufschlüsselung der Fehlerketten, was aber auch sehr umfangreich und komplex werden kann.

Zu Anfang wird das Ereignis festgelegt. Alle untergeordneten Ereignisse, die jenes auslösen können, werden im Fehlerbaum verzeichnet. Dies wird soweit fortgesetzt, bis alle Ursachen gefunden wurden. Durch die Verknüpfungen mit boolschen Operatoren, z. B. AND, OR (s. Abb. 5.7), ist die Darstellung von Fehlerkombinationen möglich, die das Top-Ereignis auslösen können. Die kleinsten Fehlerkombinationen können durch eine Reduzierung der bisherigen Wege gefunden werden. Abbildung 5.6 zeigt die Darstellung eines Fehlerbaums.

Sind die Wahrscheinlichkeiten der einzelnen Ereignisse bekannt und unabhängig voneinander, kann zusätzlich eine quantitative Auswertung erfolgen. Sobald mehr als die UND- bzw. ODER-Verknüpfungen enthalten sind, wird die Auswertung schwieriger. Das trifft ebenfalls auf reparierbare Systeme zu. Ferner sind Bedien- und Softwarefehler quantitativ nur sehr schwer darstellbar. Anstelle der Fehlerbaumanalyse kann auch eine Markov-Analyse (5.4.7) durchgeführt werden.

5.4.4 Fehler-Möglichkeits- und Einfluss-Analyse (FMEA)

Unter folgenden Namen aufgeführt:

- Failure Mode and Effects Analysis (FMEA)
- Fehler-Möglichkeits- und Einfluss-Analyse
- Fehlzustandsart- und -auswirkungsanalyse

Quellen: Stephans u. Talso [36], Amberkar u. a. [2], Federal Aviation Administration (FAA) u. EUROCONTROL [22]

Die Fehler-Möglichkeits- und Einfluss-Analyse (FMEA) ist eine induktive Methode zur Identifizierung von Gefährdungen und ihrer Auswirkungen im Entwurf. Sie kann bei der Suche nach Korrektur- oder Überwachungsmaßnahmen helfen. Die bereits 1949 vom US-Militär entwickelte Methode wird in vielen verschiedenen Industriezweigen angewandt [22]. Die FMEA kann ab der Entwicklungsphase eingesetzt werden. Die FMEA ist auf mechanische und elektrische Systeme anwendbar. Der menschliche Faktor wird nicht berücksichtigt.

Die Darstellung der Ergebnisse der FMEA erfolgt in einer Tabelle, deren Spalten u. a. die Bauteile, Funktionen, Ausfallarten, Auswirkungen und anzuwendenden Maßnahmen enthalten. Die Methode wird in mehreren Schritten durchgeführt:

1. Identifizierung und Auflistung aller Komponenten, Funktionen und Prozesse,
2. Bestimmen der Konsequenzen,
3. Bestimmen der möglichen Fehlerarten,
4. Ermitteln der Auswirkungen auf das System,
5. Identifizierung von Sicherheitsvorkehrungen,
6. Identifizierung von Maßnahmen zum Auffinden von Ausfällen,
7. Bewertung der Bedeutung der einzelnen Ereignisse.

Abhängig von der Komplexität des betrachteten Systems sollte die FMEA von einer interdisziplinären Gruppe durchgeführt werden, um möglichst alle wichtigen Risiken zu identifizieren.

5.4.5 Fehler-Möglichkeits-, Einfluss- und Kritikalitäts-Analyse (FMECA)

Unter folgenden Namen aufgeführt:

- Failure Mode, Effects and Criticality Analysis (FMECA)

- Fehler-Möglichkeits-, Einfluss- und Kritikalitäts-Analyse

Die Fehler-Möglichkeits-, Einfluss- und Kritikalitäts-Analyse (FMECA) ist die Erweiterung einer FMEA (5.4.4) um eine Kritikalitätsanalyse. Sie dient der Identifizierung und Bewertung der Auswirkungen von Gefährdungen. Bei einem Einsatz möglichst zeitig in der Entwicklung können rechtzeitig Entwurfsänderungen bei Erkennung eines zu hohen Risikos vorgenommen werden. Die Ergebnisse werden in einer Tabelle dokumentiert. Die FMECA kann in sieben Schritten durchgeführt werden [2]:

1. Identifizierung und Auflistung aller Komponenten, Funktionen und Prozesse sowie deren Ausfallarten,
2. Ermittlung der Auswirkungen für jede Ausfallart auf alle Komponenten und das System,
3. Bestimmen der Schwere der Ausfälle, der möglichen Ursachen sowie die Eintrittswahrscheinlichkeiten,
4. Identifizierung und Bewertung der vorhandenen Schutzeinrichtungen/Gegenmaßnahmen zur Früherkennung,
5. Ermittlung einer Risikoprioritätszahl (RPZ) als Produkt aus der Schwere der Auswirkungen, der Eintrittswahrschweinlichkeit und der Entdeckungsmöglichkeit,
6. Für die höchsten RPZs Ergreifung von Maßnahmen zur Reduzierung eines oder mehrerer Faktoren,
7. Neuermittlung der RPZs nach den Maßnahmen.

Bei der Auswertung der Ergebnisse muss auch das Zustandekommen des Wertes berücksichtigt werden. Derselbe Wert für eine Risikoprioritätszahl (RPZ) kann aus einem ungefährlichen Ereignis mit einer hohen Eintrittswahrscheinlichkeit sowie aus einer kritischen Auswirkung mit einer geringen Eintrittswahrscheinlichkeit gebildet werden. Besonders die RPZs bei Ausfallarten mit kritischen oder katastrophalen Effekten müssen verringert werden. Dies kann durch Änderungen des Entwurfs oder Maßnahmen zur Früherkennung erreicht werden. Die Methode sollte deshalb bereits zeitig in der Entwicklung angewandt werden, sobald ausreichend Daten vorhanden sind. Die FMECA berücksichtigt Bedienfehler ebensowenig wie die FMEA.

5.4.6 Gefahren- und Operabilitätsstudie (HAZOP)

Unter folgenden Namen aufgeführt:

- Gefahren- und Operabilitätsstudie
- Gefährdungs- und Funktionsfähigkeitsuntersuchung
- Hazard and Operability Study (HAZOP)

Quellen: Federal Aviation Administration (FAA) u. EUROCONTROL [22], Stephans u. Talso [36]

Die Gefahren- und Operabilitätsstudie (HAZOP) ist eine qualitative Methode zur Identifizierung von Gefährdungen und potentiellen operationellen Problemen in Systemen mit menschlichen Anwendern. Sie wurde zuerst in der chemischen Industrie angewandt. Die HAZOP wird von einer Gruppe aus 4-8 Mitgliedern durchgeführt, die die verschiedenen Bereiche repräsentieren sollen (u. a. Manager, Ingenieure, technisches Personal, Anwender, Experten für Human Factors und Gesundheit). Diese Mischung soll eine ausführliche und genaue Betrachtung gewährleisten. Die HAZOP kann bereits in der zeitigen Entwicklungsphase angewandt werden, sobald ausreichend Material vorliegt. Damit soll erreicht werden, dass frühzeitig erkannte Gefährdungen mit geringeren Kosten behoben oder reduziert werden können. Die HAZOP wird in der späten Entwicklungsphase, bei Vorliegen der meisten Prozessdaten angewandt. Es erfolgt eine Überprüfung der gesamten Hardware auf noch vorhandene Gefährdungen. Sie kann auch einmal anfangs in der Entwicklung durchgeführt und später aktualisiert werden.

Die HAZOP wird als eine Art strukturiertes Brainstorming durchgeführt. Sie betrachtet das System als eine Ansammlung von Knoten und verbindenden Flüssen. Es betrachtet Abweichungen von erwarteten Werten, welche selbst allerdings nicht überprüft werden. Die Beschreibung der Differenzen erfolgt mittels zuvor definierter Leitwörter (z. B. mehr, weniger, früher, umgekehrt). Die Durchführung einer HAZOP erfolgt in mehreren Schritten (nach [36]):

1. Definition der Prozesselemente,
2. Bestimmung der erwarteten Werte für jedes Element,

3. Bestimmung der Abweichungen von den Planwerten und Beschreibung mit den zuvor definierten Leitwörtern,
4. Bestimmung der Auswirkungen der Abweichungen,
5. Identifizierung der Ursachen,
6. Identifizierung der Schutzmaßnahmen,
7. Identifizierung unzureichender oder fehlender Maßnahmen.

Die Dokumentation der Ergebnisse kann in einer Tabelle erfolgen. Diese können als Ausgangswerte für andere Methoden, z. B. FTA (5.4.3) oder ETA (5.4.2), genutzt werden.

5.4.7 Markov-Analyse

Unter folgenden Namen aufgeführt:

- Markov Analysis
- Markov Analyse

Quellen: CS-25 [9], SoKo [20]

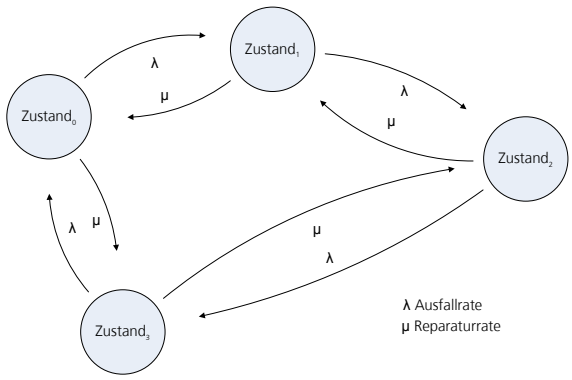

Abbildung 5.8: Darstellung eines Markov-Graphen

Die Markov-Analyse ist eine graphische, quantitative Methode zur Darstellung der Systemzustände und Ereignisse sowie ihrer Verbindungen untereinander. Sie kann anstelle einer Fehlerbaumanalyse (FTA) (5.4.3) angewandt werden. Die Systemzustände werden in

der Markov-Analyse als Knoten, die Ausfall- und Reparaturraten als Übergänge zwischen den Knoten dargestellt (Abbildung 5.8). Damit ist es möglich, auch redundante Systeme und Reparaturen darzustellen. Bei redundanten Komponenten lassen sich die verschiedenen Systemzustände zeigen, (z. B. alle Einheiten funktionstüchtig, eine Einheit defekt, ..., alle Einheiten defekt). Die Markov-Graphen liefern eine graphische Modellierung, werden aber vorrangig für eine quantitative Auswertung genutzt.

5.4.8 Preliminary Hazard Analysis (PHA)

Unter folgenden Namen aufgeführt:

- Vorbereitende Gefährdungsanalyse
- Preliminary Hazard Analysis (PHA)

Quellen: Villemeur [41], FAA Handbook [21], Stephans u. Talso [36], Amberkar u. a. [2], Stamatelatos [33]

Die vorbereitende Gefährdungsanalyse (PHA) dient der Identifizierung möglicher Gefährdungen und ihrer Ursachen sowie der Folgenbewertung. Zugleich müssen bei schwerwiegenden Risiken Vorbeugemaßnahmen ausgewählt werden. Die Anwendung der PHA sollte möglichst frühzeitig in der Entwicklung erfolgen, sobald ausreichend Daten vorhanden sind. Die Analyse sollte bei Verfügbarkeit weiterer Daten und Identifizierung neuer Gefährdungen aktualisiert werden. Mit Hilfe der in der PHA identifizierten Gefährdungen können Schwerpunkte für eine weitere Beobachtung, z. B. mit einer Fehlerbaumanalyse (FTA), gesetzt werden. Die Darstellung der Ergebnisse erfolgt in tabellarischer Form.

Die Durchführung erfolgt in den nachstehenden Schritten [2]:

1. Identifizierung der möglichen Gefährdungen,
2. Beschreibung der Gefährdungen und der Folgen,
3. Identifizierung möglicher Ursachen der Gefahren,
4. Schwereklassifikation für die Gefährdung mit ihren Folgen,
5. Bei zu hohen Risiken Festlegen von Vorbeugemaßnahmen.

Die Identifizierung der gefährlichen Einheiten und Situationen kann anhand von Checklisten abgearbeitet werden. Die Gefährdungsidentifizierung und -bewertung sollte zumindest die folgenden Punkte berücksichtigen [21]:

- Gefährliche Komponenten (z. B. . Treibstoffe, Giftstoffe, Drucksysteme),
- Sicherheitsrelevante Elementschnittstellen (z. B. Materialkompatibilität, Elektromagnetische Interferenzen),
- Umweltbedingungen (z. B. extreme Temperaturen, Blitzeinschlag, Feuer),
- Verfahren für Betrieb, Tests, Instandhaltung und Notfälle (z. B. Analyse von Bedienfehlern, Lebensrettungsanforderungen)
- Einrichtungen, Anlagen und Training (z. B. Lagerung brennbarer Materialien, Lärmquellen),
- Sicherheitsrelevante Anlagen, Schutzvorrichtungen, Alternativen (z. B. Systemredundanz, Branderkennung und -bekämpfung).

5.4.9 Zuverlässigkeitsblockschaltbild (RBD)

Unter folgenden Namen aufgeführt:

- Zuverlässigkeitsblockschaltbild
- Zuverlässigkeits-Blockdiagramme
- Reliability Block Diagram (RBD)

Quellen: Amberkar u. a. [2], Stamatelatos [33]

Zuverlässigkeitsblockschaltbilder bilden die Verknüpfungen einzelner Komponenten und Teile eines Systems graphisch ab. Ein Beispiel wird in Abbildung 5.9 gezeigt. Die Blöcke stellen Komponenten, Elemente oder Subsysteme dar. Die Eingangswerte stehen auf der linken, die Ausgangswerte auf der rechten Seite. Redundante Systeme werden über parallele Schaltungen abgebildet, nichtredundante über Reihenschaltungen. In dem gezeigten Beispiel sind zum Funktionieren die Komponenten A und B *oder* C und D erforderlich.

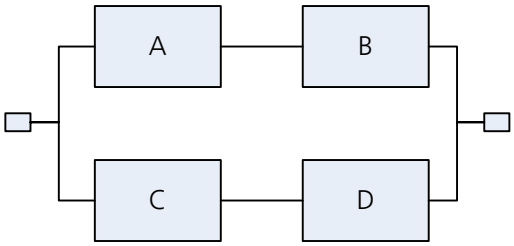

Abbildung 5.9: Zuverlässigkeitsblockschaltbild

Ist diese Mindestanforderung nicht erfüllt, kommt es zum Ausfall. Anhand dieser Aufstellungen können Kombinationen, die zu Ausfällen führen können, identifiziert werden. Wiederholen sich bestimmte Blöcke in allen Pfaden, liegt ein Ausfall infolge gemeinsamer Ursachen (Common Cause Failure) vor. Es müssen für alle möglichen Gefährdungen Zuverlässigkeitsblockschaltbilder erstellt werden. Wird die Methode im Rahmen einer anderen Gefahrenanalyse angewandt, ist auch eine Anwendung nur auf die schwerwiegendsten Gefährdungen möglich. Die Durchführung erfolgt in vier Schritten [2]:

1. Festlegen der zu untersuchenden Gefährdung,
2. Festlegen des Anfangs und Endes der Betrachtung,
3. Identifizierung aller Komponenten zwischen Ein- und Ausgang, deren Ausfall die Gefährdung mit auslösen können,
4. Darstellen jeder identifizierten Komponente als Block im Schaltbild.

Die Blockschaltbilder können mit Boolscher Algebra ausgedrückt werden. Reihenschaltungen ergeben UND-, Parallelschaltungen ODER-Verknüpfungen. Die Blöcke der Schaltbilder können einzelne Komponenten, aber auch größere Einheiten, wie Systemteile, darstellen.

5.4.10 Spezielle Methoden im Luftverkehr

Die bisher vorgestellten Methoden werden nicht nur im Luft- und Schienenverkehr sondern auch in vielen anderen Bereichen angewandt. Die drei folgenden Methoden entstammen dem Luftverkehr und finden im Rahmen des Sicherheitsnachweisprozesses nach der ARP 4754 [3] Anwendung:

- Functional Hazard Assessment (FHA)
- Preliminary System Safety Assessment (PSSA)
- System Safety Assessment (SSA)

Ihre Einordnung in das Sicherheitsnachweisverfahren wurde in Abschnitt 5.2.1 beschrieben. Das Zusammenwirken der drei Verfahren wird in Abbildung 5.2 verdeutlicht.

Functional Hazard Assessment (FHA)

Unter folgenden Namen aufgeführt:

- Functional Hazard Assessment (FHA)
- Functional Hazard Analysis

Quellen: ARP 4754 [3], CS-25 [9], SoKo [20]

Die Functional Hazard Assessment (FHA) ist eine qualitative Methode aus dem Luftverkehrsbereich. Sie dient der Identifizierung funktionaler Ausfälle. Ferner werden die Gefährdungen entsprechend ihrer Versagensarten klassifiziert. Gleichzeitig werden Schwerpunkte für weitere Untersuchungen gesetzt. Die Anwendung des FHA erfolgt zeitig in der Entwicklung. Bei Identifizierung neuer Funktionen oder Versagensarten muss sie aktualisiert werden. Die Darstellung der Ergebnisse erfolgt in einer Tabelle, die ebenfalls Vorsorgemaßnahmen enthalten sollte.

Das FHA wird in zwei Stufen durchgeführt, zuerst auf Flugzeugebene, anschließend auf der untergeordneten Systemebene. Die Anwendung erfolgt auf beiden Ebenen ähnlich:

1. Identifizierung der Funktionen,
2. Ermittlung der Versagensarten,
3. Ermittlung der Folgen,
4. Klassifikation der Versagensarten,
5. Ermittlung der Sicherheitsanforderungsstufen (DAL).

Tabelle 5.5: Versagensklassen und die zugehörigen DAL-Werte nach ARP 4754 [3]

Klassifikation der Versagensart	Development Assurance Level (DAL)
Katastrophal	A
Gefährlich	B
Bedeutend	C
Gering	D
Keine Sicherheitsauswirkungen	E

Die Ermittlung der Versagensarten und ihrer zugehörigen Folgen erfolgt durch Experten der verschiedenen Bereiche. Die Konsequenzenidentifizierung soll die Fähigkeiten der Flugbesatzung, ihre Aufgaben ordnungsgemäß auszuführen, berücksichtigen. Dazu zählen z. B. Hinweise oder Alarmmeldungen für die Piloten bei Problemen oder auch eingeschränkte Sicht bei Rauch. Die Klassifizierung der Versagensarten erfolgt anhand der Auswirkungen auf das Flugzeug, die Insassen und die Flugbesatzung, die in Tabelle 5.1 beschrieben sind. Bei den Bewertungen muss ferner die Betriebsphase, z. B. Rollen, Start oder Reiseflug, berücksichtigt werden, in dem das Versagen auftritt. Bei unterschiedlichen Auswirkungen müssen getrennte Betrachtungen der Phasen erfolgen. Im Rahmen der Flugzeug-FHA erfolgt außerdem die Zuweisung der DAL anhand Tabelle 5.5. Die letzte Klasse, *keine Sicherheitsauswirkungen* sowie der DAL *E*, werden in der ARP 4754 eingeführt. Die CS-25 kennt nur die vier übrigen Klassen. In der zweiten Stufe, dem *System-FHA*, wird das FHA für jedes einzelne Flugzeugsystem durchgeführt. Der Umfang ist abhängig von der Komplexität des Systems. Für einfache Systeme wird meist eine Überprüfung des Entwurfs ausreichend sein. Bei komplexeren Systemen sollte eine qualitative Top-Down-Methode ausgehend von der Flugzeugebene gewählt werden.

Einige Probleme bei der Anwendung einer FHA werden in Wilkinson u. Kelly [48] aufgeführt. So ist es z. B. schwierig, die Folgen eines Versagens zu beurteilen, wenn es sich um ein tieferliegendes Subsystem handelt.

Das Flugzeug wird in mehrere Systeme unterteilt, die wiederum diverse Subsysteme beinhalten. Das wird in Abbildung 5.10 am Beispiel einer Triebwerkssteuerung verdeutlicht. Diese gehört zum System Triebwerk, das zum Antrieb, welches wiederum ein Subsystem des Flugzeugs ist. Die Schwierigkeit liegt in der Identifizierung der Versagensauswirkungen

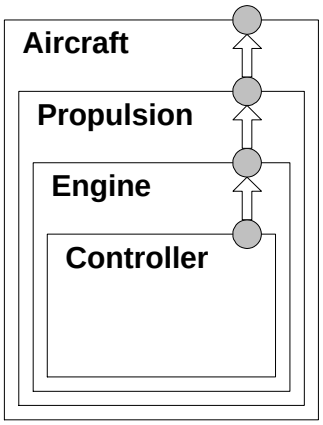

Abbildung 5.10: Fortplanzung der Versagensauswirkungen durch mehrere Schichten [48]

durch alle Schichten hindurch, in der Trennung der Auswirkungen der Steuerung und der der anderen Subsysteme, wie z. B. das Triebwerk.

Die notwendigen Anforderungen für die festgelegten Sicherheitsziele werden im nachfolgenden Preliminary System Safety Assessment (PSSA) zugewiesen.

Preliminary System Safety Assessment (PSSA)

Unter folgenden Namen aufgeführt:

- Preliminary System Safety Assessment
- Preliminary System Safety Analysis

Quellen: ARP 4754 [3], Dawkins u. a. [10]

Das Preliminary System Safety Assessment (PSSA) ist eine Methode aus dem Luftverkehr. Es wird in der ARP 4754 [3] beschrieben. Das Ziel des PSSA besteht in der Gewährleistung, dass alle Versagensarten zuvor im FHA (5.4.10) erkannt wurden. Weiterhin sollen die Sicherheitsanforderungen um die abgeleiteten Sicherheitsanforderungen vervollständigt und die Notwendigkeit weiterer Vorsorgemaßnahmen ermittelt werden. Als Drittes soll aufgezeigt werden, wie die Systemarchitektur die Anforderungen bezüglich der Gefährdungen erreichen soll. Das PSSA kann zur Bewertung verschiedener Systementwürfe und zur Vermeidung zu hoher Anforderungen genutzt werden[10]. Das PSSA wird im Anschluss an das FHA durchgeführt. Es ist ein iterativer Prozess mit vielen Rückkopplungen.

Während des PSSA werden die zu den identifizierten Ausfallarten gehörenden Ausfälle und Ausfallkombinationen ermittelt. Für diese Aufgabe kann z. B. eine Fehlerbaumanalyse

(FTA) (5.4.3) oder eine Markov-Analyse (5.4.7) genutzt werden. Der Unabhängigkeitsnachweis der Separierungs- und Isolationsanforderungen kann mit einer Common Cause Analysis (CCA) (Abschnitt 5.4.1) erfolgen. In dieser Phase müssen neben Hard- und Software-Fehlern auch operationelle Fehler berücksichtigt werden. Ist nach qualitativen oder quantitativen Analysen nicht zu erwarten, dass die Vorgaben erfüllt werden können, müssen alternative Vorsorgemaßnahmen aufgestellt werden. Sind zur Einhaltung der Bestimmungen weitere Auflagen erforderlich, müssen zu diesem Zweck abgeleitete Sicherheitsanforderungen aufgestellt werden. Bei der Berechnung der Eintrittswahrscheinlichkeiten der Versagensarten muss die Dauer latenter Ausfälle und der Betrieb mit ausgefallenen Komponenten oder Systemen sowie die Möglichkeiten ihrer Entdeckung betrachtet werden. Oftmals können Ausfälle bereits durch die Flugbesatzung im normalen Betrieb entdeckt werden. In anderen Fällen können sie jedoch nur durch spezielle Untersuchungen aufgespürt werden. Durch das Aufstellen entsprechender Wartungs- und Instandhaltungsprogramme soll das rechtzeitige Auffinden der Ausfälle sichergestellt werden. Die Aufgaben und Intervalle dieser abgeleiteten Sicherheitsanforderungen werden im nachfolgend ausgeführten System Safety Assessment (SSA) verifiziert. [3, 10]

System Safety Assessment (SSA)

Unter folgenden Namen aufgeführt:

- System Safety Assessment (SSA)

Quellen: ARP 4754 [3]

Das System Safety Assessment (SSA) verifiziert die Implementierung der Sicherheitsfunktionen mit den während des Functional Hazard Assessments (FHA) und des Preliminary System Safety Assessment (PSSA) aufgestellten Anforderungen, deren Ergebnisse hier als Eingangsdaten verwendet werden. Das SSA kann die folgenden Dinge enthalten:

- abgestimmte Wahrscheinlichkeiten externer Ereignisse,
- Systembeschreibung mit seinen Funktionen und Schnittstellen,
- Auflistung der Versagensarten,
- Ergebnisse qualitativer und quantitativer Analysen der Versagensarten,

- Ergebnisse der Common Cause Analysis (CCA),
- Auflistung der sicherheitsrelevanten Instandhaltungsaufgaben und -intervalle,
- Bestätigung über Berücksichtigung aller Gefährdungen der Implementierung des Systems mit der anderer Systeme.

5.5 Übertragbarkeit der Methoden zwischen den Domänen

Die meisten der in diesem Kapitel vorgestellten Methoden werden nicht nur im Luft- und Schienenverkehr sondern auch in vielen anderen Bereichen, z. B. der Automobilindustrie, angewandt. Im Schienenverkehr wird der Nachweis der geforderten Unabhängigkeit mit der Common Cause Analysis (CCA) durchgeführt [14]. Ansonsten ist die Auswahl der Methoden zum Nachweis der Erfüllung der Anforderungen den Herstellern und Betreibern überlassen. Der Sicherheitsanalyseprozess des Luftverkehrs basiert auf dem Functional Hazard Assessment (FHA), dem Preliminary System Safety Assessment (PSSA), dem System Safety Assessment (SSA) und der Common Cause Analysis (CCA). Die Common Cause Analysis (CCA) dient in diesem Fall ebenso wie bereits beim Schienenverkehr dem Nachweis der Einhaltung der Unabhängigkeitsforderungen. Innerhalb dieser Methoden können wiederum die Ergebnisse anderer Verfahren, z. B. einer Fehlerbaumanalyse (FTA) genutzt werden.

Das Functional Hazard Assessment (FHA) dient der Gefährdungsidentifizierung, -klassifizierung und Bestimmung der Development Assurance Level (DAL). Die Ermittlung erfolgt unter Zuhilfenahme von Tabellen für die Eintrittswahrscheinlichkeiten entsprechend der fünf festgelegten Klassifikationen der Versagensarten. Die zugrunde liegenden Werte wurden aus historischen Daten ermittelt und sind einheitlich für Luftfahrzeuge festgelegt. Ausgehend von den Zielen des FHA ist eine Nutzung im Schienenverkehr vorstellbar. Ein Problem bei der Anwendung wird jedoch die Bestimmung des Sicherheitsintegritätslevel (SIL) entsprechend der tolerierbaren Gefährdungsraten sein. Während diese im Luftverkehr aus Tabellen in Abhängigkeit von der Versagensklasse bestimmt werden können, ist im Schienenverkehr der Betreiber für die Wahl eines Risikoakzeptanzkriteriums und die Ermittlung der tolerierbaren Gefährdungsraten (THR) zuständig. Für den

Einsatz im Schienenverkehr wäre die einheitliche Definition eines Risikoakzeptanzgrundsatzes und die quantitative Beschreibung der Klassifikationen erforderlich. Eine direkte Anwendung der Tabelle aus dem Luftverkehr sollte ohne weitere Prüfung nicht umgesetzt werden, da diese Werte auf Unfalldaten von Flugzeugen basieren, und somit nicht auf den Schienenverkehr übertragen werden kann.

Das Preliminary System Safety Assessment (PSSA) wird im Luftverkehr zur Identifizierung weiterer Sicherheitsanforderungen und Prüfung des Systementwurfs genutzt. Diese Aufgaben werden beim Schienenverkehr in der Gefährdungsbeherrschung durchgeführt. Für die Prüfung der geforderten Unabhängigkeit wird in beiden Bereichen die Common Cause Analysis (CCA) angewandt. Die Übertragung des PSSA auf den Schienenverkehr erscheint möglich.

Das System Safety Assessment (SSA) dient im Sicherheitsanalyseprozess für Luftfahrzeuge der Verifizierung. In diesem Zusammenhang müssen die unterschiedlichen Definitionen beider Domänen berücksichtigt werden. Der Luftverkehr verifiziert die Systemimplementierung mit den zuvor im FHA und PSSA aufgestellten und validierten Anforderungen. Dem gegenüber erfolgt im Schienenverkehr die Verifizierung jeweils innerhalb einer Lebenszyklusphase. Die Validierung prüft die Erfüllung aller spezifischen Anforderungen des betrachteten Systems. Eine direkte Anwendung im Schienenverkehr erscheint ohne Anpassung nicht möglich.

Von den drei speziell im Luftverkehr genutzten Methoden erscheint die Anwendung des Functional Hazard Assessments (FHA) und Preliminary System Safety Assessment (PSSA) im Schienenverkehr möglich. Es sollte jedoch ein Risikoakzeptanzkriterium für das FHA definiert werden. Die Übertragung des System Safety Assessments (SSA) erscheint aufgrund der unterschiedlichen Auslegung der Validierung und Verifizierung in beiden Verkehrsdomänen schwierig.

6 Gestaltungsvorschläge für Zulassungsverfahren

6.1 Gestaltungsvorschläge für den Schienenverkehr

Nach der Untersuchung der Zulassungsverfahren für Luft- und Schienenfahrzeuge sollen in diesem Abschnitt Gestaltungsvorschläge für das Verfahren im Schienenverkehr vorgestellt werden.

Die Zulassung bestätigt, dass ein Verkehrsmittel den rechtlich vorgeschriebenen Anforderungen der Zulassungsbehörde entspricht und von seinem Einsatz keine Gefahr ausgeht. In diesem Sinne werden die gültigen Regelungen und Vorgaben vom Tag der Abnahme herangezogen. Damit fehlt den Herstellern bei größeren Projekten jegliche Planungssicherheit. Dieses Problem soll durch den Antrag auf Zusicherung behoben werden. Damit werden die zu erfüllenden Anforderungen auf Basis des Pflichtenheftes festgelegt. Es wäre sinnvoll, dieses Verfahren standardmäßig in das Zulassungsverfahren aufzunehmen, wie dass bereits beim Luftverkehr der Fall ist. Änderungen, wie die Anwendung neuerer Vorgaben, könnten bei Einverständnis des Antragstellers und der zuständigen Stelle genehmigt werden.

Mit den Technischen Spezifikationen für Interoperabilität (TSI) wurden u. a. Anforderungen an neue Fahrzeuge, die auf dem transeuropäischen Netz verkehren sollen, vorgegeben. Durch die verpflichtende Anwendung dieser Vorschriften sollen einheitliche Mindeststandards in allen Mitgliedsländern sichergestellt werden. Die Europäische Union (EU) verfolgt den Ansatz, nur das notwendigste zu regulieren und ansonsten den Herstellern und Betreibern die freie Wahl zu lassen. Für die Inbetriebnahmegenehmigung, eine Voraussetzung für den operationellen Einsatz, müssen neben den Anforderungen der TSI auch die nationalen Vorgaben eingehalten werden. Damit ergeben sich für die EU-Staaten wieder

unterschiedliche Anforderungen. Das kann wiederum für den Hersteller beim geplanten Verkauf der Fahrzeuge in verschiedene Staaten einen Mehraufwand bedeuten, der sich wirtschaftlich negativ auswirken könnte. Im Verlauf der Harmonisierung des europäischen Luftverkehrs wurden mit den Joint Aviation Requirements (JARs) Vorgaben aufgestellt, die von den einzelnen Mitgliedstaaten der Joint Aviation Authorities (JAA) angepasst werden konnten. Das resultierte in diversen Versionen der einheitlich konzipierten Standards. Als Reaktion wurde die Europäische Luftfahrtagentur (EASA) gegründet, deren Vorgaben direkt umgesetzt werden müssen. Es ist zu überprüfen, in wie weit sich die nationalen Anforderungen für Schienenfahrzeuge untereinander und von den Anforderungen der TSI tatsächlich unterscheiden. Bei größeren Differenzen sollte eine stärkere Harmonisierung angestrebt werden. Diese Aufgaben fallen in den Verantwortungsbereich der Europäischen Eisenbahnagentur (ERA), die u. a. die Vorschläge für die TSI erarbeitet. Ein weiteres Problem im Zusammenhang mit dem Prinzip, nur das Notwendigste zu regulieren und den Rest den Anwendern zu überlassen, ist die Wahl der Nachweisverfahren zur Erfüllung der Anforderungen. Es wäre zu empfehlen, ein Verfahren als Leitfaden aufzuzeigen, mit dem die Erfüllung der Anforderungen aufgezeigt werden kann. Dadurch könnten viele Unsicherheiten, die sich aus der Einführung der TSI und CENELEC-Normen ergeben haben, beseitigt werden. Dieser Wunsch wurde bereits mehrfach seitens der Eisenbahnindustrie geäußert. Eine dieser Unsicherheiten betrifft die Wahl eines Risikoakzeptanzprinzips. Obwohl in der CENELEC-Norm DIN EN 50126-1 drei Grundsätze vorgestellt werden, bleibt die Wahl den Anwendern überlassen. Die präsentierten Ansätze werden zudem in einigen Ländern rechtlich kontrovers betrachtet. Das trifft besonders auf das ALARP-Kriterium zu. Es sollte ein einheitliches Risikoakzeptanzprinzip gewählt werden, dass von allen EU-Staaten gebilligt wird. In diesen Bereich fällt auch die Ableitung der tolerierbaren Gefährdungsraten (THR) aus dem Risikoakzeptanzkriterium. Zur Zeit muss es von der Eisenbahnverwaltung für jede einzelne Eisenbahnanwendung festgelegt werden. Im Luftverkehr wurden die Werte hingegen nach Ermittlung aus historischen Unfalldaten definiert und werden bereits seit langem erfolgreich angewandt. Die Festlegung eines Risikoakzeptanzkriteriums könnte in den Zuständigkeitsbereich der Europäischen Eisenbahnagentur (ERA) im Rahmen ihrer Aufgabe zur Erarbeitung gemeinsamer Sicherheitsmethoden und -ziele fallen. Der Verband europäischer Eisenbahnhersteller (UNIFE) hat sich inzwischen auf ein Risikoakzeptanzkriterium für technische Systeme (RAC-TS) mit einem Wert von 10^{-9} $pro\ Betriebsstunde$ für ein Ereignis mit katastrophalen Auswirkungen verständigt,

das dann gemäß der betrachteten Situation angepasst werden soll[7]. Ferner sollten die Begriffsdefinitionen innerhalb der CENELEC-Normen vereinheitlicht werden.

6.2 Gestaltungsvorschläge für andere Verkehrssektoren

Im vorhergehenden Abschnitt wurden Gestaltungsvorschläge für das Zulassungsverfahren für Schienenfahrzeuge unterbreitet. An dieser Stelle sollen Empfehlungen für ein gemeinsames Verfahren der Domänen Luft- und Schienenverkehr vorgestellt werden.

Ein interessanter Ansatz im Schienenverkehr ist die Befristung der Bauartzulassung auf fünf Jahre. Damit soll sichergestellt werden, dass Neufahrzeuge dem Stand der Technik entsprechen[39]. Musterzulassungen für Luftfahrzeuge haben hingegen eine unbegrenzte Gültigkeit. Die Zulassungsinhaber sind verpflichtet, die Sicherheit ihrer Flugzeuge weiterhin aufrechtzuerhalten. Sie müssen die Entwürfe aber nicht kontinuierlich dem technischen Fortschritt anpassen.

Im Schienenverkehr erfolgte die Umsetzung des modularen Prüfverfahrens zur Zertifizierung der Teilsysteme auf Basis der Richtlinien zur technischen Harmonisierung[1]. Damit können Komponenten oder Teilsysteme mit einer Prüf- oder Konformitätserklärung vereinfacht weiterverwendet werden. Dieses Verfahren wird außerdem auch in anderen Branchen innerhalb der EU in der CE-Zertifizierung angewandt, z. B. in der Elektrotechnik.

Ein gemeinsames Zulassungsverfahren müsste auf eine einheitliche Terminologie zurückgreifen. Die verwendeten Definitionen in den einzelnen Domänen, auch innerhalb dieser selbst, sind zur Zeit teilweise sehr voneinander abweichend.

Ein domänenübergreifendes Zulassungsverfahren müsste aus einem branchenunabhängigen Fundament und speziellen Erweiterungen für die einzelnen Sektoren Luft- und Schienenverkehr bestehen. Derzeit liegt die Ausrichtung des Zulassungsprozesses für Luftfahrzeuge auf internationaler Ebene. Im Eisenbahnverkehr gehen die Bestrebungen in Richtung Harmonisierung im Raum der OTIF, in der hauptsächlich eurasische Staaten vertreten sind. Ein Zulassungsverfahren für die Verkehrsmittel beider Domänen müsste

[1] 93/465/EWG: Beschluß des Rates vom 22. Juli 1993 über die in den technischen Harmonisierungsrichtlinien zu verwendenden Module für die verschiedenen Phasen der Konformitätsbewertungsverfahren und die Regeln für die Anbringung und Verwendung der CE- Konformitätskennzeichnung

dann auch in diesen Räumen anerkannt werden. Die derzeitigen Verfahren innerhalb der EU sind in einigen Punkten sehr verschieden. Für Luftfahrzeuge wird die Zulassung durch die EASA erteilt und muss von allen Mitgliedstaaten anerkannt werden. Schienenfahrzeuge müssen zuerst im europäischen Zertifizierungsprozess eine EG-Prüfbescheinigung durch eine benannte Stelle erlangen. Für die Zulassung in einem Staat ist zusätzlich die Einhaltung der über die in den TSI hinausgehenden nationalen Anforderungen erforderlich. Die gegenseitige Anerkennung der Zulassungen zwischen den EU-Staaten ist derzeit noch nicht gegeben.

Ein weiterer Unterschied liegt in der Auslegung der Validierung. Im Luftverkehr erfolgt eine Validierung der Anforderungen. Im Schienenverkehr wird ein Produkt in Bezug auf seine Anforderungen validiert. Die Verifikation erfolgt beim Luftverkehr im System Safety Assessment (SSA) mit den Anforderungen, wohingegen im Schienenverkehr die Ergebnisse der einzelnen Lebenszyklusphasen mit den Ergebnissen der jeweils vorherigen Phase verifiziert werden.

Für ein domänenübergreifendes Zulassungsverfahren müssten erst einige grundlegende Dinge aneinander angepasst werden. Dabei darf die derzeitige Ausrichtung auf Verfahren außerhalb der Europäische Union (EU) jedoch nicht vergessen werden. Die Verfahren im Luftverkehr wurden denen der Federal Aviation Administration (FAA) angepasst, im Schienenverkehr soll das Verfahren mit den Vorgaben der OTIF harmonisiert werden.

Literaturverzeichnis

[1] *Allgemeines Eisenbahngesetz (AEG).* http://www.eur-lex.europa.eu/de/index.htm. – i. d. F. v. 16.07.2007

[2] Amberkar, Sanket ; Czerny, Barbara J. ; D'Ambrosio, Joseph G. ; Demerly, Jon D. ; Murray, Brian T.: *A Comprehensive Hazard Analysis Technique for Safety--Critical Automotive Systems.* Version: March 2001. http://delphi.com/pdf/techpapers/2001-01-0674.pdf, Abruf: 30. 10. 2007. SAE Technical Paper Series

[3] Norm ARP 4756 04 1996. *Certification Considerations for Highly-Integrated or Complex Aircraft Systems*

[4] Automotive Engineers (SAE), Society of (Hrsg.): http://www.sae.org/technical/standards/ARP4754, Abruf: 15. 08. 2007

[5] Banal, F.: *Panel: Teaching the regulators to follow the rules.* Version: 2007. http://www.easa.europa.eu/conf2007/agenda.htm. Vortrag auf der EU/US International Aviation Safety Conference 2007

[6] Braband, Jens: Risikoakzeptanzkriterien und -bewertungsmethoden – Ein systematischer Vergleich. In: *Signal + Draht* (2004), 4, S. 6 – 9

[7] Braband, Jens: *Ein einheitliches Risikoakzeptankriterium für Eisenbahntechnik.* Version: 2007. http://rzv113.rz.tu-bs.de/Bieleschweig/B10/4_Braband.pdf, Abruf: 25. 01. 2008. – Vortrag auf dem 10. Bieleschweig-Workshop zum Systems Engineering: Modellierung betrieblicher Aspekte & Risikoanalyse

[8] Braband, Jens ; Brehmke, Bernd-E. ; Griebel, Stephan ; Peters, Harald ; Suwe, Karl-Heinz: *Die CENELEC-Normen zur Funktionalen Sicherheit /The CENELEC-Standards regarding Functional Safety.* 1. Hamburg : Eurailpress, 2006

[9] EASA (Hrsg.): *Certification Specifications for Large Aeroplanes CS-25.* 10 2006

[10] Dawkins, S.K. ; Kelly, T.P. ; McDermid, J.A. ; Murdoch, J. ; Pumfrey, D.J.: *Issues in the Conduct of PSSA.* Version: August 1999. http://www-users.cs.york.ac.uk/~tpk/pssa.pdf, Abruf: 18. 10. 2007

[11] Norm DIN EN 45020 März 2007. *Normung und damit zusammenhängende Tätigkeiten – Allgemeine Begriffe (ISO/IEC Guide 2:2004); Dreisprachige Fassung EN 45020:2006*

[12] Norm DIN EN 50126-1 September 2006. *Bahnanwendungen - Spezifikation und Nachweis der Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit, Sicherheit (RAMS) - Teil 1: Grundlegende Anforderungen und genereller Prozess*

[13] Norm DIN EN 50128 November 2001. *Bahnanwendungen - Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme - Software für Eisenbahnsteuerungs- und Überwachungssysteme*

[14] Norm DIN EN 50129 Dezember 2003. *Bahnanwendungen - Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme - Sicherheitsrelevante elektronische Systeme für Signaltechnik*

[15] *Eisenbahn-Bau- und Betriebsordnung (EBO).* `http://www.eur-lex.europa.eu/de/index.htm`. – i. d. F. v. 31. 10. 2006

[16] *Vertrag zur Gründung der Europäischen Gemeinschaft (EGV).* – i. d. F. v. 16. 04. 2003

[17] Erckmann, Ralf ; Böwning, Klaus: *Internal Working Procedure Type Certification (TCP).* Version: 12 2004. `http://www.easa.eu.int/doc/Certification/Working_Procedures/EASA_TCP_Issue_1_CF_20122004.pdf`

[18] *EUROCAE.* `http://www.eurocae.org/cgi-bin/home.pl?Target=va/description/background.html&Num=1`, Abruf: 19. 07. 2007

[19] EUROCONTROL (Hrsg.): *Single European Sky ATM Research.* Version: 2007. `http://www.eurocontrol.int/sesar/gallery/content/public/docs/sesar_2007_brochure_eurocontrol.pdf`, Abruf: 25. 01. 2008

[20] Experimentelles Software Engineering IESE, Fraunhofer-Institut für (Hrsg.): *Softwarekompetenz.* `http://softwarekompetenz.de/?21965`, Abruf: 16. 07. 2007. – übergeordnete Internetseite

[21] *FAA System Safety Handbook.* : *FAA System Safety Handbook*, Dezember 2000. `http://www.faa.gov/library/manuals/aviation/risk_management/ss_handbook/`, Abruf: 30. 10. 2007

[22] Federal Aviation Administration (FAA) (Hrsg.) ; EUROCONTROL (Hrsg.): *ATM Safety Techniques and Toolbox.* Version: Januar 2005. `http://www.eurocontrol.int/eec/gallery/content/public/documents/EEC_safety_documents/Safety_Techniques_and_Toolbox_1.0.pdf`, Abruf: 24. 10. 2007

[23] Fischer, Caroline: Die Europäische Eisenbahnagentur (ERA). In: *Der Eisenbahningenieur* (2007), 5, Nr. 58, S. 59 – 65

[24] *Grundgesetz für die Bundesrepublik Deutschland (GG).* – i. d. F. v. 28. 08. 2006

[25] (ICAO), International Civil Aviation O. (Hrsg.): *Convention on International Civil Aviation – Doc 7300/9.* Version: 9, 2006. http://www.icao.int/icaonet/dcs/7300_cons.pdf. – Chicagoer Abkommen

[26] Kesseler, E. ; Kos, J.: *The next step in collaborative aerospace engineering.* Version: 2005. http://137.205.176.10/vivace/content/advanced/vivace-rivf05.pdf, Abruf: 9. 1. 2008

[27] Kommission, Europäische (Hrsg.): *Das transeuropäische Hochgeschwindigkeitsbahnsystem.* Luxemburg, 2004

[28] *Luftfahrt-Bundesamt.* Version: 03 2006. http://www.lba.de/cln_009/nn_57316/DE/LBA/Organisation/Abteilung_20T/T2/T2__EASA.html, Abruf: 10. 08. 2007

[29] OTIF (Hrsg.): *Zwischenstaatliche Organisation für den Internationalen Eisenbahnverkehr.* Version: Juni 2005. http://www.otif.org/otif/_dpdf/OTIF_Info_Juni_2005_d.pdf, Abruf: 19. 07. 2004

[30] Riedel, Daniel: *Schriften zum Europäischen Recht.* Bd. 118: *Die Gemeinschaftszulassung für Luftfahrtgerät. Europäisches Verwalten durch Agenturen am Beispiel der EASA.* 1. Berlin : Duncker & Humblot, 2006

[31] *RICHTLINIE 2001/16/EG DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 19. März 2001 über die Interoperabilität des konventionellen Eisenbahnsystems.* – i. d. F. v. 01. 06. 2007

[32] *RICHTLINIE 96/48/EG DES RATES vom 23. Juli 1996 über die Interoperabilität des transeuropäischen Hochgeschwindigkeitsbahnsystems.* – i. d. F. v. 01. 06. 2007

[33] Stamatelatos, Michael et. a.: *Fault Tree Handbook with Aerospace Applications*, August 2002

[34] Statistisches Bundesamt (Hrsg.): *Verkehr in Zahlen.* Version: September 2006. https://www-ec.destatis.de/csp/shop/sfg/bpm.html.cms.cBroker.cls?cmspath=struktur,vollanzeige.csp&ID=1019215, Abruf: 22. 10. 2007 (Im Blickpunkt)

[35] Steinke, Sebastian: A380 ist zugelassen. In: *Flugrevue* (2007), Februar, S. 33

[36] Stephans, Richard E. (Hrsg.) ; Talso, Warner W. (Hrsg.): *System Safety Analysis Handbook*. 2. Albuquerque : System Safety Society, 1997. – E-Book

[37] Ständer, Tobias ; Becker, Uwe: *Eine vergleichende Betrachtung globaler Sicherheitsstandards für Verkehrssysteme*. Version: 2006. http://www.automotive2006.de/programm/Staender.pdf, Abruf: 01. 10. 2007. – Vortragsfolien

[38] *Verordnung über die Interoperabilität des transeuropäischen Eisenbahnsystems (Transeuropäische-Eisenbahn-Interoperabilitätsverordnung - TEIV)*. http://www.eisenbahn-bundesamt.de/. – i. d. F. v. 05. 07. 2007

[39] Thomasch, Andreas: Die europäischen Zulassungsprozesse für Eisenbahnfahrzeuge. In: *Eisenbahntechnische Rundschau (ETR)* (2005), 12, S. 789 – 803

[40] UIC (Hrsg.): *UIC Homepage*. http://www.uic.asso.fr/apropos/article.php3?id_article=209, Abruf: 13. 08. 2007

[41] Villemeur, Alain: *Reliability, availability, maintainability and safety assessment*. Bd. 1: *Methods and Techniques*. Chichester : Wiley, 1992

[42] *VERORDNUNG (EG) Nr. 1592/2002 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 15. Juli 2002 zur Festlegung gemeinsamer Vorschriften für die Zivilluftfahrt und zur Errichtung einer Europüischen Agentur für Flugsicherheit*. http://www.eur-lex.europa.eu/de/index.htm. – i. d. F. v. 29. 03. 2007

[43] *VERORDNUNG (EG) Nr. 1702/2003 DER KOMMISSION vom 24. September 2003 zur Festlegung der Durchführungsbestimmungen für die Erteilung von Lufttüchtigkeits- und Umweltzeugnissen für Luftfahrzeuge und zugehörige Erzeugnisse, Teile und Ausrüstungen sowie für die Zulassung von Entwicklungs- und Herstellungsbetrieben*. http://www.eur-lex.europa.eu/de/index.htm. – i. d. F. v. 05. 04. 2007

[44] *VERORDNUNG (EG) Nr. 593/2007 DER KOMMISSION vom 31. Mai 2007 über die von der Europäischen Agentur für Flugsicherheit erhobenen Gebühren und Entgelte*. http://www.eur-lex.europa.eu/de/index.htm. – i. d. F. v. 31. 05. 2007

[45] *VERORDNUNG (EG) NR. 881/2004 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 29. April 2004 zur Errichtung einer Europäischen Eisenbahnagentur (Agenturverordnung)*. http://www.eur-lex.europa.eu/de/index.htm. – i. d. F. v. 29. 03. 2007

[46] *Verwaltungsvorschrift für die Abnahme von Eisenbahnfahrzeugen gemäß § 32 Abs. 1 EBO im Zuständigkeitsbereich des Eisenbahn-Bundesamt (VwV Abnahme § 32).* `http://www.eisenbahn-bundesamt.de/`. – i. d. F. v. 01. 09. 2004

[47] Weber, Ludwig ; Holderbach, Hans: Type certification of commercial aircraft calls for enhanced international rules. In: *ICAO Journal* (2001), 2, Nr. 56, S. 4 – 6, 27 – 28

[48] Wilkinson, P.J. ; Kelly, T.P.: *Functional Hazard Analysis for Highly Integrated Aerospace Systems.* Version: Februar 1998. `http://www-users.cs.york.ac.uk/%7Etpk/ieefha.pdf`, Abruf: 18. 10. 2007

[49] Zhao, Wei: *Feature-Based Hierarchical Knowledge Engineering for Aircraft Life Cycle Design Decision Support*, School of Aerospace Engineering Georgia Institute of Technology, Diss., 2007