

Technische Universität Dresden
Fakultät Verkehrswissenschaften „Friedrich List“
Institut für Verkehrssystemtechnik

Diplomarbeit

Anwendung der Functional Hazard Analysis (FHA) in der
Eisenbahnsignaltechnik am Beispiel ETCS Level 2

eingereicht von

Sten Wery

Betreuer:

Dr. Jens Braband (Siemens AG, Transportation Systems)

Prof. Dr. rer. nat. Jörg Schütte (Institut für Verkehrssystemtechnik)

Dresden, 23.09.2002

Sten Wery

Bibliografischer Nachweis

Wery, Sten

Anwendung der Functional Hazard Analysis (FHA) in der Eisenbahnsignaltechnik am Beispiel ETCS Level 2

– 2002 – 65 Seiten, 6 Tabellen, 25 Bilder, 1 Anlage

Technische Universität Dresden

Fakultät Verkehrswissenschaften „Friedrich List“

Institut für Verkehrssystemtechnik

Professur Verkehrssystemtechnik

Prof. Dr. rer. nat. Jörg Schütte

Diplomarbeit

Autorenreferat:

In der vorliegenden Arbeit wird am Beispiel ETCS Level 2 untersucht, ob die bei der Systementwicklung in der Luftfahrt zur Ableitung von Sicherheitsanforderungen verwendete Methode „Functional Hazard Analysis (FHA)“ auch zur Ableitung von Sicherheitsanforderungen in der Eisenbahnsignaltechnik eingesetzt werden kann.

Nach einer Kurzbeschreibung der Ausrüstungsstufen des ETCS und einem Überblick über zum Verständnis der Methode hilfreiche Zusammenhänge des Luftverkehrs wird die FHA im Detail vorgestellt und anschließend an einer ETCS-Funktion angewendet, für die zu vermuten ist, dass sie nicht die höchsten Sicherheitsanforderungen erfüllen muss.

Für die Anwendung finden die derzeitigen Aktivitäten zur Ableitung von Sicherheitsanforderungen für ETCS bewusst keine Beachtung.

Thesen

- Eine bis heute inhaltlich nicht zufriedenstellend geklärte Frage ist die Frage nach den Sicherheitsanforderungen für ETCS (European Train Control System). Dies liegt zum einen daran, dass es kein einheitliches Vorgehen für die Ableitung der Sicherheitsanforderungen gibt und zum anderen keine gemeinsame Risikoakzeptanz im Eisenbahnbereich existiert.
- Ein weiteres Problem bei der Beurteilung der mit ETCS verbundenen Risiken und der deswegen erforderlichen Sicherheit ist die Tatsache, dass es keine europäisch einheitliche Betriebsvorschrift für das Fahren unter Sicherheitsverantwortung des ETCS gibt. Somit könnte das Versagen einer ETCS-Funktion während des Betriebes bei einem Betreiber zu nicht sicherheitsrelevanten Folgen führen, während das gleiche Versagen bei einem anderen Betreiber katastrophale Folgen haben könnte.
- Für die Beurteilung der erforderlichen Sicherheit ist die Kenntnis über das betriebliche Umfeld des zu beurteilenden Systems zwingend notwendig. Da es keine einheitliche Betriebsvorschrift für das Fahren mit ETCS gibt, wurde für diese Untersuchung ein einfaches betriebliches Umfeld definiert.
- In anderen Industriebereichen (z.B. Kernkraft, chemische Industrie, Luftfahrt) sind risikoorientierte Methoden zur Herleitung von Sicherheitsanforderungen schon längere Zeit Stand der Technik. Eine Methode ist die „Functional Hazard Analysis (FHA)“, bei der die Sicherheitsanforderungen über eine Betrachtung der Systemfunktionen hergeleitet werden. Diese Methode wird hier auf eine Funktion des ETCS Level 2 angewendet, um zu untersuchen, ob sie für die Herleitung von Sicherheitsanforderungen für ETCS geeignet ist.
- Eine geeignete Aufteilung auf von der Implementierung unabhängige Funktionen und deren Beschreibung ist nicht trivial. Für die Ableitung von Sicherheitsanforderungen mittels FHA wurde eine Funktion des ETCS-Fahrzeuggerätes ausgewählt, von der zu vermuten war, dass sie nicht die höchsten Sicherheitsanforderungen erfüllen muss.
- Für die Herleitung der Sicherheitsanforderungen an ein System ist eine Festlegung der Akzeptanz der mit dem Betreiben des Systems verbundenen Risiken notwendig. Da es für ETCS keine einheitliche Risikoakzeptanz gibt, wurde in dieser Arbeit ersatzweise die Risikoakzeptanztabelle für das System „Verkehrsflugzeug“ verwendet.
- Trotz der in dieser Arbeit verwendeten Annahmen und Vereinfachungen erscheint der Weg zu Sicherheitsanforderungen für ETCS mittels FHA gangbar zu sein. Für die Anwendung in der Eisenbahnsignaltechnik (und möglicherweise anderer Anwendungen, z.B. Fahrzeugtechnik) müsste als Voraussetzung dazu eine funktionale Zerlegung des Systems „Eisenbahn“ erfolgen.

Es ist zu vermuten, dass sich diese Zerlegung aufgrund der physikalisch engen Verzahnung bei der Eisenbahn zwischen Fahrweg, Fahrwegverwaltung und Fahrzeug sehr schwierig gestalten wird.

- Obwohl aktuelle Ansätze zur Ableitung von Sicherheitsanforderungen bei ETCS bei der Anwendung der FHA außer Acht gelassen wurden, konnten mit dem während der Bearbeitung gewonnenen Erkenntnisstand keine Anhaltspunkte herausgefunden werden, die der normativen Situation der Eisenbahn (EN 50129) entgegenstehen.

1	Einleitung	8
1.1	Motivation.....	8
1.2	Zielstellung und Aufbau der Arbeit.....	9
2	European Train Control System (ETCS)	10
2.1	Entwicklungsstand und Historie des ETCS	10
2.2	Einführungsstrategie und Ausrüstungsstufen für ETCS	11
2.3	Probleme bei der Einführung von ETCS	16
2.3.1	Kompatibilität der technischen Komponenten.....	16
2.3.2	Einheitliche Betriebsvorschriften (Interoperabilität)	17
2.3.3	Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit, Sicherheit (RAMS)	18
3	FHA – Functional Hazard Assessment	21
3.1	Luftverkehr - Einordnung und Überblick	21
3.1.1	Grundsätzliche Organisation	21
3.1.2	Arten des Luftverkehrs.....	23
3.1.3	Sicherheit im Luftverkehr	23
3.2	Der Sicherheitsprozess der Society of Automotive Engineers (SAE).....	28
3.3	Functional Hazard Assessment (FHA) - Durchführung.....	33
3.3.1	Ziele und Anwendungsbereiche	33
3.3.2	Vorgehensweise FHA	35
3.3.3	Erfahrungen und Probleme mit FHA.....	40
4	Anwendung der FHA an ETCS Level 2	42
4.1	Vorgehen	42
4.2	Schritt 1: Systemdefinition und Funktionsaufteilung	42
4.2.1	Betriebliche Randbedingungen	46
4.2.2	Überwachungsphasen.....	46
4.3	Schritt 2: Ausfallarten der Funktion und Abschätzung der Folgen	50
4.3.1	Ausfallarten.....	50
4.3.2	Folgenabschätzung.....	50
4.4	Schritt 3: Klassifizierung der Folgen und Ableitung einer Sicherheitsanforderung für die Funktion	51
5	Diskussion der Ergebnisse	53
5.1.1	Vorgehensweise zur Ableitung von Sicherheitsanforderungen.....	53
5.1.2	Systemdefinition und Betriebliches Umfeld.....	56
5.1.3	einheitliche Risikoakzeptanz.....	58
5.1.4	Terminologie.....	61
6	Ausblick	62
	Literaturverzeichnis	63

Anlage

Abbildungsverzeichnis

Bild 1-1: Untersuchungsgegenstand der Aufgabenstellung.....	9
Bild 2-1: ETCS Zeitplan.....	10
Bild 2-2: ERTMS/ETCS Application Level 0	12
Bild 2-3: ERTMS/ETCS Application Level STM	13
Bild 2-4: ERTMS/ETCS Application Level 1 with in-fill function by Euroloop or Radio in-fill	14
Bild 2-5: ERTMS/ETCS Application Level 2	15
Bild 2-6: ERTMS/ETCS Application Level 3	15
Bild 2-7: Referenzarchitektur ETCS.....	17
Bild 2-8: Main ERTMS/ETCS Onboard Functions	19
Bild 3-1: grundsätzliche organisatorische Aufteilung im Luftverkehr	22
Bild 3-2: Arten des Luftverkehrs	23
Bild 3-3: geografische Verteilung ausgewählter Zulassungsbehörden und Normungsgremien	24
Bild 3-4: Safety Assessment process model	31
Bild 3-5: Aircraft Function Tree and allocation to systems.....	32
Bild 3-6: Gegenüberstellung von FHA (SAE) und FHA (EUROCONTROL).....	34
Bild 3-7: Ablauf der FHA.....	37
Bild 4-1: Festlegung der Betrachtungsebene.....	42
Bild 4-2: Betrachtungsebenen der Aufgabenstellung.....	43
Bild 4-3: Betrachtungsebenen für ETCS-Funktionen	45
Bild 4-4: Entscheidungsbaum zur Auswahl der zu untersuchenden Modi	48
Bild 4-5: Überwachungsarten der Modi.....	49
Bild 5-1: Vorgehen zur Bestimmung der THR bei der Eisenbahn	54
Bild 5-2: Vorgehen zur Bestimmung der tolerierten Ausfallwahrscheinlichkeit in der Luftfahrt	55
Bild 5-3: Vorgehensvergleich zur Ableitung von Sicherheitsanforderungen (THR).....	57
Bild 5-4: Entwicklung der „THR“ für große Verkehrsflugzeuge.....	60

Tabellenverzeichnis

Tabelle 3-1:	Examples of Generic Failure Modes	35
Tabelle 3-2:	Failure Condition Severity as Related to Probability Objectives and Assurance Levels	38
Tabelle 3-3:	Hazard Classification Scheme.....	39
Tabelle 3-4:	Risk Classification Scheme.....	40
Tabelle 4-1:	Modi des ETCS nach [UNISIG 26].....	47
Tabelle 4-2:	Zusammenfassung der Ergebnisse der FHA für die Funktion „Anzeigen der aktuellen Geschwindigkeit“	52

Abkürzungsverzeichnis

ARP	Aerospace Recommended Practice (SAE)
ATA	Airline Transport Association of America
ATC	Air Traffic Control
BMVBW	Bundesministerium für Verkehr, Bau- und Wohnungswesen
CENELEC	European Committee for Electrotechnical Standardization
CNS	Communications, Navigation, Surveillance
CS	Ceiling Speed
CSM	Ceiling Speed Monitoring
DAL	Design Assurance Level
DB AG	Deutsche Bahn AG
DFS	Deutsche Flugsicherung GmbH
DoD	Department of Defence (USA)
DSM	Dynamic Speed Monitoring
EASA	European Aviation Safety Agency
ECAC	European Civil Aviation Conference
EoA	End of Movement Authority
ERTMS	European Railway Traffic Management System
ESROG	ERTMS Safety Requirements and Objectives Group
ESTW	Elektronisches Stellwerk
ETCS	European Train Control System
ETCS on-board	ETCS Fahrzeuggerät
ETCS Track side	ETCS Streckengerät
EU	Europäische Union
EUROCAE	European Organization for Civil Aviation Electronics
EUROCONTROL	European Organisation for the Safety of Air Navigation
EVC	European Vital Computer
FAA	Federal Aviation Administration
FAR	Federal Aviation Regulations
FHA	Functional Hazard Assessment (SAE), Functional Hazard Analysis (EUROCONTROL)
GSM-R	Global System of mobile Communication – Railway
ICAO	International Civil Aviation Organisation
Indusi	Induktive Zugbeeinflussung
JAA	Joint Aviation Authorities

JAR	Joint Airworthiness Requirement
LBA	Luftfahrtbundesamt
LEU	Line side electronic unit
LZB	Linienförmige Zugbeeinflussung
MA	Movement Authority
MIL	Military Standard
MMI	Man Machine Interface
RAMS	Reliability, Availability, Maintainability, Safety
RENFE	Spanische Eisenbahngesellschaft
RTCA	Radio Technical Commission for Aeronautics, Inc.
SAE	Society of Automotive Engineers
SBB	Schweizerische Bundesbahn
SIL	Safety Integrity Level
SL	Supervised Location
SNCF	Französische Eisenbahngesellschaft
STM	Specific Transmission Module
Tf	Triebfahrzeugführer
THR	Tolerable Hazard Rate
UIC	Internationaler Eisenbahnverband
UNISIG	the combined European signalling industry
UNISIG Class 1	Dokumentensatz der für die Interoperabilität notwendigen ETCS Funktionen
USA	United States of America

1 Einleitung

1.1 Motivation

Das European Train Control System (ETCS) ist ein einheitliches Zugsteuerungssystem, um die Vielfalt der in Europa eingesetzten Zugsicherungs- und Zugbeeinflussungssysteme abzulösen und die damit verbundenen Möglichkeiten zur Steigerung von Effizienz und Effektivität im grenzüberschreitenden Eisenbahnverkehr ausnutzen zu können.

Ausgangspunkt der Entwicklung von ETCS war die Functional Requirement Specification (FRS), die in 1990 von einem Zusammenschluss von Betreibern (UIC, ERTMS User Group) erstellt wurde und als funktionales Lastenheft für die Entwicklung und Implementierung von ETCS dienen sollte.

Dieser Anforderung war die FRS jedoch nicht gewachsen, so dass darauf aufbauend ein Zusammenschluss von Firmen der europäischen Signalbauindustrie (UNISIG) detailliertere Spezifikationen erstellte. Nach diesen Spezifikationen entwickelten die Hersteller von Leit- und Sicherungstechnik jeweils in eigener Verantwortung die technischen Komponenten des ETCS. Derzeit laufen auf Pilotanlagen die ersten nationalen Tests des neuen Zugsteuerungssystems [SD2002 (4)]. Mit diesen Tests sollen sowohl Funktionsfähigkeit und Funktionalität des ETCS als auch die technische Kompatibilität der national entwickelten und hergestellten Komponenten getestet werden [SD2002 (1)].

Eine der ungeklärten Fragen ist die Frage nach der erforderlichen Sicherheit des ETCS dar. Einigkeit bei Herstellern, Betreibern und Zulassungsbehörden besteht in der Feststellung, dass ETCS als Zugsteuerungssystem Sicherheitsverantwortung im Transportsystem „Eisenbahn“ hat. Unklar ist, wie groß diese ist und vor allem, wie die Sicherheit implementiert werden soll. Eine Möglichkeit zur Bestimmung der erforderlichen Sicherheit ist der risikoorientierte Ansatz, der inzwischen auch bei der Eisenbahn Stand der Technik ist. Dabei werden die Gefährdungen, die mit dem Einsatz eines Systems verbunden sind, bereits bei dessen Entwicklung analytisch ermittelt und entsprechend bewertet.

Allerdings bereitet die Anwendung des risikoorientierten Ansatzes Probleme, so dass es derzeit noch keine einheitlich abgestimmten und akzeptierten Aussagen zur notwendigen Sicherheit des ETCS gibt [SD2002 (2)].

Die Identifikation und die Bewertung der Gefährdungen stellen sich als besonders schwierig heraus, da sie viele Interessen (Betreiber, Hersteller, Behörden, Öffentlichkeit) berühren und häufig subjektiv geprägt sind. Es ist aber gerade die Bewertung der Gefährdungen, die entscheidend für die Beantwortung der Frage „Wie sicher muss das System sein?“ und damit für dessen Auslegung ist.

Es gibt bei Eisenbahnanwendungen bisher wenig Erfahrungen mit dem risikoorientierten Ansatz zur Ermittlung der erforderlichen Sicherheit. In anderen Industriebereichen (Kernkraft, chemische Industrie, Luftfahrt) wird das methodische Vorgehen zur risikoorientierten Betrachtung schon länger angewendet.

1.2 Zielstellung und Aufbau der Arbeit

Gegenstand dieser Arbeit ist es, die in der Luftfahrt angewandte Methode „Functional Hazard Analysis (FHA)“ auf ihre Tauglichkeit zur Ableitung von Sicherheitsanforderungen für ETCS zu untersuchen (Bild 1-1). Dabei geht es nicht um die Ableitung konkreter Sicherheitsanforderungen für ETCS.

Nach einer kurzen Zusammenfassung der ETCS-Ausrüstungsstufen wird die FHA im Detail vorgestellt und anschließend versuchsweise auf ETCS Level 2 angewendet. Die dabei gewonnenen Erkenntnisse werden zusammengefasst und in einem Ausblick mögliche weitere Schritte und Konsequenzen aufgezeigt.

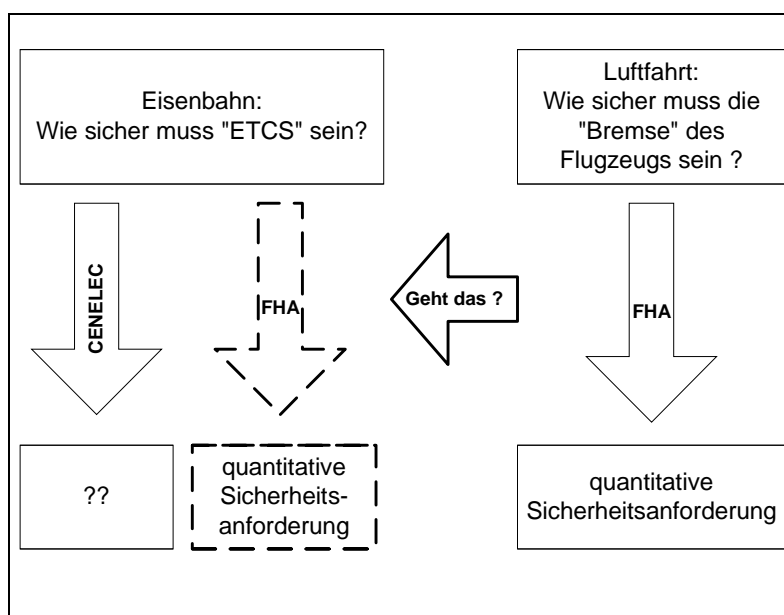


Bild 1-1: Untersuchungsgegenstand der Aufgabenstellung

Der größte Anteil der verwendeten Literatur ist in englischer Sprache verfasst. An einigen Stellen gibt es für englische Begriffe keine geeignete deutsche Übersetzung, so dass in solchen Fällen die englischen Begriffe verwendet werden.

Da die Anwendung der Methodik der FHA aus der Luftfahrt an einem Sachverhalt der Eisenbahn zunächst ohne Berücksichtigung derzeitiger Aktivitäten bei der Sicherheitsbetrachtung nach CENELEC erfolgen soll, wird in dieser Arbeit weitestgehend die Terminologie der Luftfahrt verwendet. In Fällen, wo terminologische oder inhaltliche Unvereinbarkeiten bestehen, wird für die Anwendung der Methode eine für ETCS passende Interpretation verwendet.

2 European Train Control System (ETCS)

2.1 Entwicklungsstand und Historie des ETCS

ETCS ist als Teil des von der EU geförderten Programms ERTMS (European Railway Management System) als erstes europaweit (EU) einheitlich einsetzbares Zugsteuerungssystem geplant. In diesem Rahmen wird ETCS sowohl Signalisierungsaufgaben als auch Aufgaben der Zugsicherung übernehmen.

Die Einführung von ETCS soll durch verschiedene funktionale und technische Ausbaustufen erleichtert werden. Dazu war der in Bild 2-1 dargestellte (vereinfachte) Zeitplan vorgesehen. Der aktuelle Stand der Entwicklung ist Schritt 3 („Test & Improvement“). In der Mitte dieses Jahres begann in der Schweiz in einer Zusammenarbeit zwischen Bombardier und der SBB der erste Test des ETCS [SD2002 (4)]. In Kürze werden weitere ETCS-Projekte [W2] folgen.

An der Umsetzung des Zeitplanes sind im wesentlichen drei Interessengruppen beteiligt. Unter den Bahnen werden im folgenden die Betreiber von Infrastruktur und rollendem Material für den Eisenbahnverkehr verstanden. Ein Zusammenschluss der in Europa führenden Hersteller von Leit- und Sicherungstechnik (UNISIG) bildet im Zusammenhang mit ETCS die Industrie. Als Zulassungsbehörden sollen im weiteren im Zusammenhang mit ETCS die zuständigen Stellen der beteiligten europäischen Länder für Zulassungen von Eisenbahnanwendungen verstanden werden.

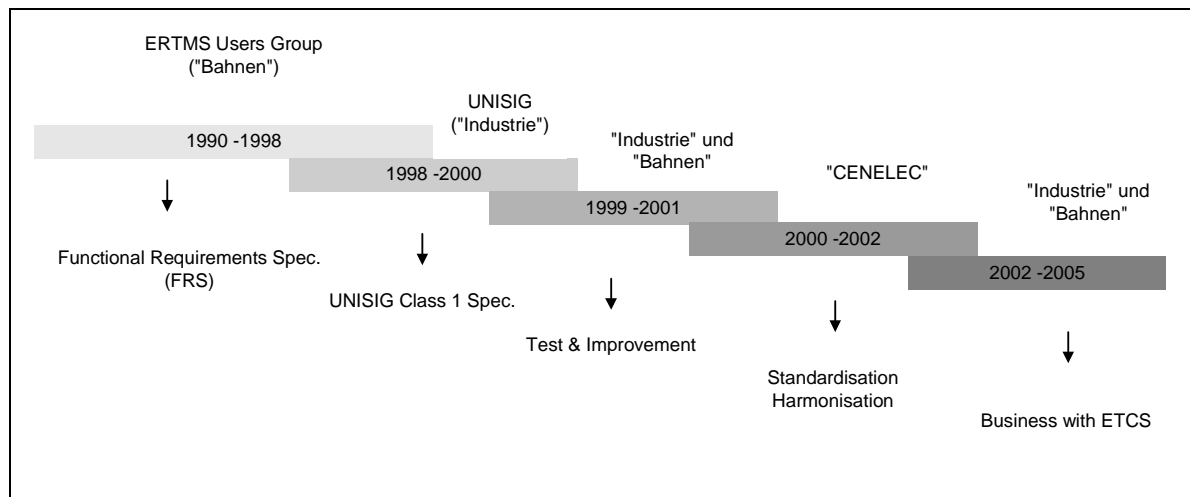


Bild 2-1: ETCS Zeitplan

Quelle: nach [W1]

Den Ausgangspunkt der Entwicklung des einheitlichen europäischen Zugsicherungssystems stellt die „Functional Requirements Specification“ [FRS99] dar. Diese wurde von den Bahnen erstellt und enthält alle der von den verschiedenen Bahnen gewünschten Funktionalitäten sowie teilweise Festlegungen zu deren Implementierung (z.B. Punkt 3.3.1.1: „Traction units must be equipped with a

European Vital Computer (EVC) together with equipment for receiving information from infrastructure installations, equipment for speed measurement and equipment for Data Entry.“). Im Sinne der Interoperabilität ist es notwendig, Implementierungsvorgaben zu machen. Allerdings sollte die Verwendung von Designvorgaben bei der Definition von Funktionen strengstens vermieden werden [KELLY].

Bei der Erstellung von [FRS99] sind im Wesentlichen die Wünsche und Vorstellungen der großen europäischen Bahnen (DB AG, RENFE, SNCF) eingeflossen. Bei Sachverhalten, in denen keine Einigung erzielt wurde, werden allgemein nationale Regelungen (national values) gefordert. Im wesentlichen betrifft dies Funktionen, die nahe an den Betrieb und damit an unterschiedliche, historisch gewachsene, betriebliche Vorschriften und Verfahren der beteiligten Bahnen heranreichen (z.B. Rangiergeschwindigkeit). Die wiederholte Forderung nach nationalen Regelungen widerspricht jedoch dem eigentlichen Ziel eines europäisch einheitlichen Zugsteuerungssystems.

Weil [FRS99] sich nicht als Vorgabe für die Herstellung und Zulassung des ETCS eignete, schlossen sich die in Europa führenden Firmen der Signalbauindustrie unter der Bezeichnung „UNISIG“ zusammen, um aufbauend auf [FRS99] eine gemeinsame technische Basis für die Implementierung des ETCS zu schaffen.

Im Ergebnis wurden die Anforderungen in drei Klassen eingeteilt, deren erste Klasse (UNISIG - Class 1: Mandatory for Interoperability) nur die für die Interoperabilität zwingend notwendigen Funktionen, Schnittstellen und technischen Spezifikationen enthält. Dieser Dokumentensatz ist von allen beteiligten europäischen Zulassungsbehörden anerkannt (approved). Gegenstand der derzeitigen Tests ist die Implementierung der Funktionen und Anforderungen aus UNISIG - Class 1.

Zur zweiten (UNISIG - Class 2: Useful) und dritten Klasse (UNISIG - Class 3: Nice to have) existieren derzeit keine zugelassenen Dokumente. Diese Stufen finden in dem Zeitplan für die Implementierung derzeit keine Beachtung. Weiterführende Angaben zur Historie lassen sich unter [W3] finden.

2.2 Einführungsstrategie und Ausrüstungsstufen für ETCS

Für ETCS werden 5 Ausbaustufen (Level: 0, STM, 1, 2, 3) unterschieden, die sich neben dem Funktionsumfang auch in der technischen Realisierung unterscheiden [UNISIG 26]. Die Level werden an dieser Stelle, nach steigendem Funktionsumfang geordnet, im Überblick vorgestellt. Erläuterungen allgemeiner Art zu ETCS können in [W4] nachgelesen werden.

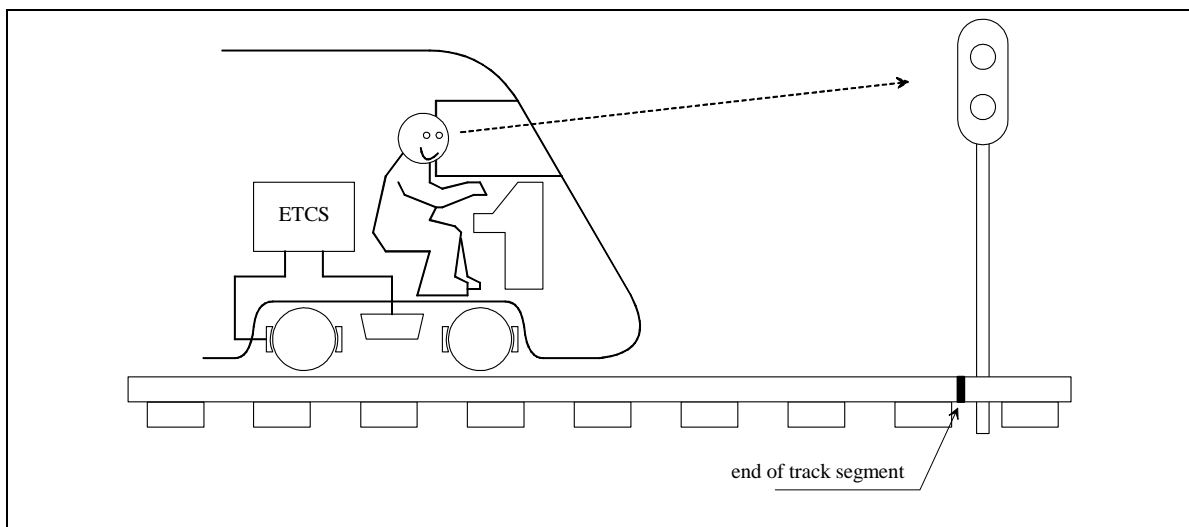
Die Funktionen von ETCS sind systembedingt auf Fahrzeuggerät (ETCS on-board) und Streckengerät (ETCS Track-side) aufgeteilt. Die Fahrzeuggeräte der verschiedenen Ausrüstungsstufen sind bezüglich der Streckenausrüstung abwärtskompatibel und erkennen einen Wechsel der

Ausrüstungsstufe des Streckengerätes selbstständig. In allen Ausrüstungsstufen wird das Fahrzeug vom Triebfahrzeugführer (Tf) manuell gesteuert, indem dieser die aktuelle Geschwindigkeit mit der zulässigen Geschwindigkeit vergleicht und das Ergebnis entsprechend in Bedienhandlungen umsetzt.

Level 0

Ein mit ETCS ausgerüstetes Fahrzeug wird auf einer nicht mit ETCS oder einem anderen Zugsicherungssystem ausgerüsteten Strecke betrieben (Bild 2-2). Der Triebfahrzeugführer steuert das Fahrzeug entsprechend dem streckenseitig vorhandenen Signalsystem. Es erfolgt keine Führerraumsignalisierung.

ETCS überwacht auf dem Fahrzeug die zulässige Fahrzeuggeschwindigkeit sowie die zulässige Geschwindigkeit für das Fahren ohne Zugsicherungssystem (nationale Unterschiede).



Quelle: [UNISIG 26], 2.6.3, Fig. 2

Bild 2-2: ERTMS/ETCS Application Level 0

Level STM

Das ETCS Fahrzeuggerät nutzt die Übertragungsmechanismen des nationalen Zugbeeinflussungssystems für die Kommunikation Strecke/Fahrzeug und wertet die empfangenen Informationen aus (Bild 2-3).

Das Fahrzeuggerät ist zu diesem Zweck mit Hilfe eines Zusatzmoduls (Specific Transmission Module STM) kompatibel mit dem nationalen Zugbeeinflussungssystem der befahrenen Strecke und verarbeitet dessen Informationen. Es erkennt den Übergang von einem nationalen Zugbeeinflussungssystem zu einem anderen und verwaltet diesen Wechsel selbstständig. Die nutzbaren Funktionen des ETCS sind somit vom Funktionsumfang des jeweiligen nationalen

Zugbeeinflussungssystem abhängig, z.B. erfolgt in Deutschland je nach Zugbeeinflussungssystem eine Führerraumsignalisierung (LZB) oder nicht (Indusi).

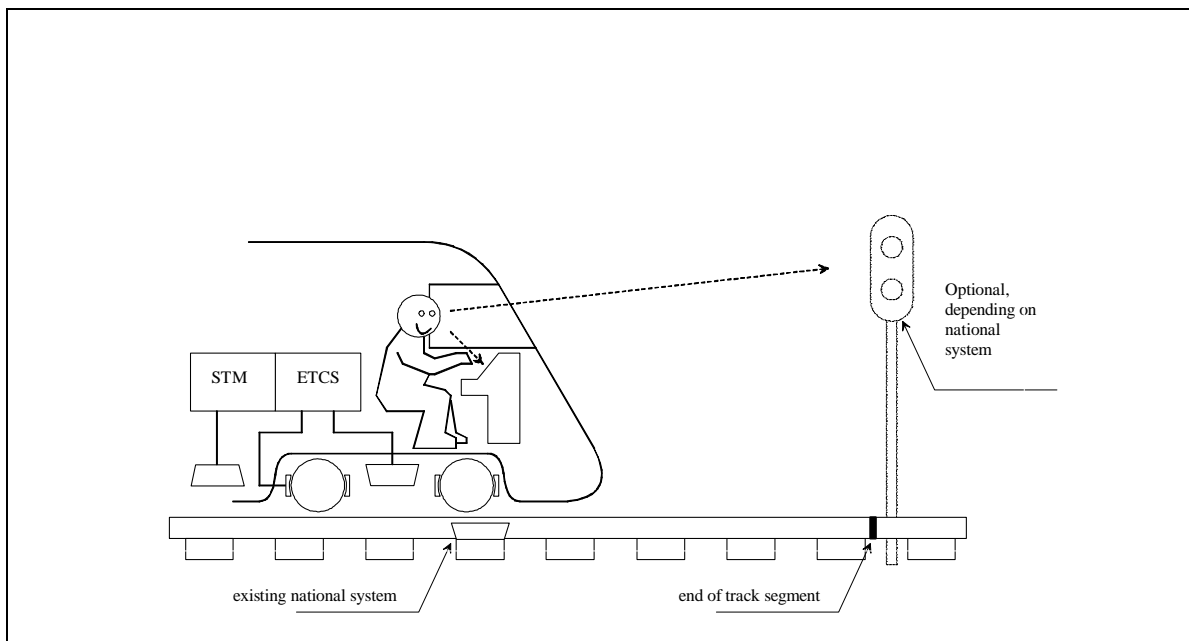


Bild 2-3: ERTMS/ETCS Application Level STM

Quelle: [UNISIG 26], 2.6.4, Fig. 3

Level 1

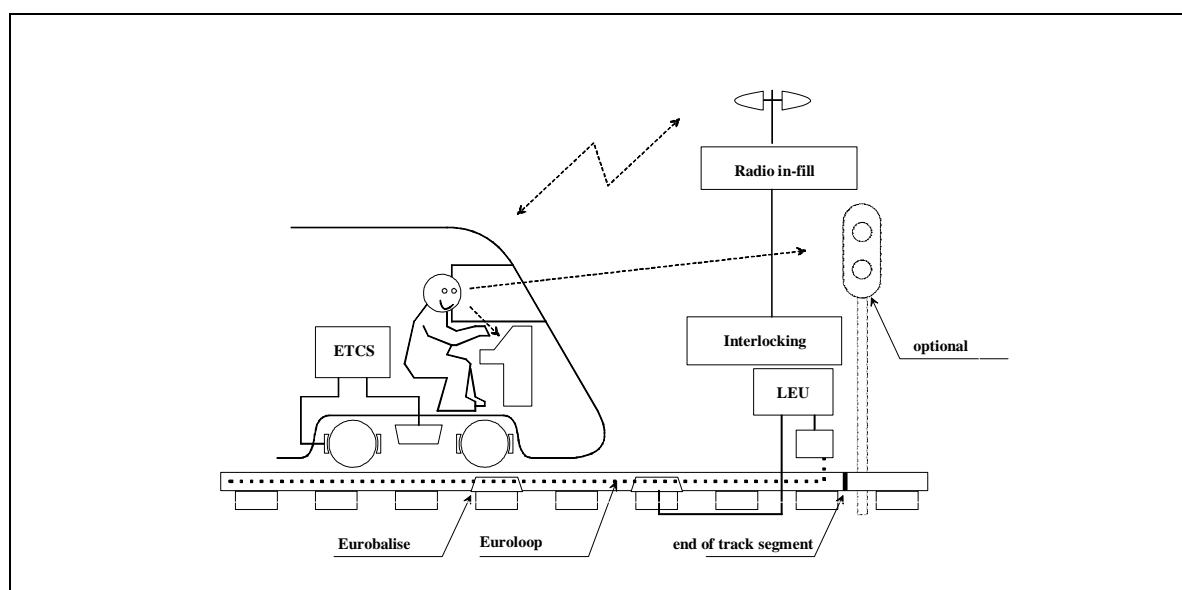
Das ETCS-Streckengerät erhält die Signalisierungsinformationen (Signalbild) vom vorhandenen nationalen Signalsystem und überträgt diese zusammen mit den im ETCS-Streckengerät gespeicherten Streckendaten punktförmig (schaltbare Eurobalise), im Bereich von ortsfesten Signalen linienförmig (Euroloop), zum ETCS-Fahrzeuggerät (Bild 2-4). Dieses ermittelt aus den empfangenen (Streckendaten + Signalbild) und den im Fahrzeuggerät gespeicherten (Fahrzeugdaten) Informationen ein Geschwindigkeitsprofil, anhand dessen die aktuelle Geschwindigkeit des Zuges überwacht und bei Überschreitung der zulässigen Geschwindigkeit eine Zwangsbremmung eingeleitet wird.

Die übertragenen Informationen sind signal- (und damit orts-) bezogen und nicht vom empfangenden Fahrzeug abhängig. Die Informationsübertragung ist unidirektional, d.h. ein direkter Datenfluss findet nur zum Fahrzeug statt. Durch die LEU (Line side Electronic Unit) wird der angeschaltete Signalbegriff ausgewertet und das entsprechende ETCS-Telegramm zur Übertragung mittels Balise bzw. Euroloop ausgewählt).

Die Gleisfreimeldung obliegt der vorhandenen Stellwerkstechnik.

Ohne Verfügbarkeit der in-fill-Funktion (linienförmige Übertragung von Signalaufwertungen im Bereich zwischen ortsfestem Vor- und Hauptsignal) gelten für den Triebfahrzeugführer die

streckenseitigen Signale. Bei Verfügbarkeit der in-fill Funktion findet eine Führerraumsignalisierung statt und die streckenseitigen Signale werden dunkelgeschaltet.



Quelle: [UNISIG 26], 2.6.5, Fig. 5

Bild 2-4: ERTMS/ETCS Application Level 1 with in-fill function by Euroloop or Radio in-fill

Level 2

Level 2 ist ein funkbasiertes (Euroradio GSM-R) linienförmig wirkendes Zugsteuerungssystem (Bild 2-5). Es wird aufbauend auf die vorhandene (elektronische) Stellwerkstechnik installiert. Von dort werden vom ETCS-Streckengerät die Fahrweg- und Signalisierungsinformationen abgegriffen und zusammen mit den im ETCS-Streckengerät gespeicherten Fahrzeug- und Streckendaten an das entsprechende Fahrzeug übertragen.

Aus den empfangenen fahrzeugbezogenen Streckendaten und den im Fahrzeuggerät gespeicherten Fahrzeugdaten wird ein Geschwindigkeitsprofil ermittelt, anhand dessen die aktuelle Geschwindigkeit des Zuges überwacht und bei Überschreitung der zulässigen Geschwindigkeit eine Bremsung eingeleitet wird.

Der Abgriff der Fahrweg- und Signalisierungsinformationen durch das ETCS-Streckengerät vom nationalen Stellwerk erfordert Kompatibilität mit den entsprechenden länderspezifischen Signalsystemen und die Übersetzung deren Daten in ETCS-Daten.

Die Gleisfreimeldung wird vom vorhandenen Stellwerk realisiert und ist nicht Bestandteil des ETCS. Die punktförmig wirkenden Balisen dienen hauptsächlich als Referenzpunkte bei der Selbstortung der mit ETCS ausgerüsteten Fahrzeuge.

Ortsfeste Signale sind nicht mehr notwendig. Es erfolgt Führerraumsignalisierung (gegebenenfalls werden ortsfeste Signale dunkel geschaltet).

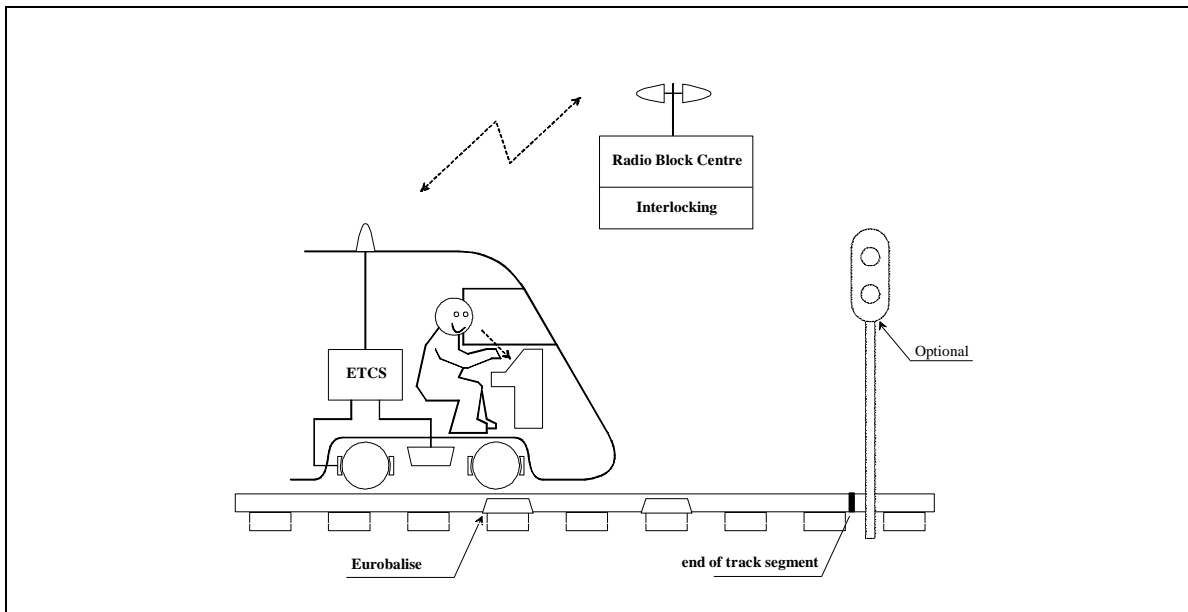


Bild 2-5: ERTMS/ETCS Application Level 2

Quelle: [UNISIG 26], 2.6.6, Fig. 6

Level 3

Level 3 ist ebenso wie Level 2 ein funkbasiertes linienförmig wirkendes Zugsteuerungssystem (Bild 2-6).

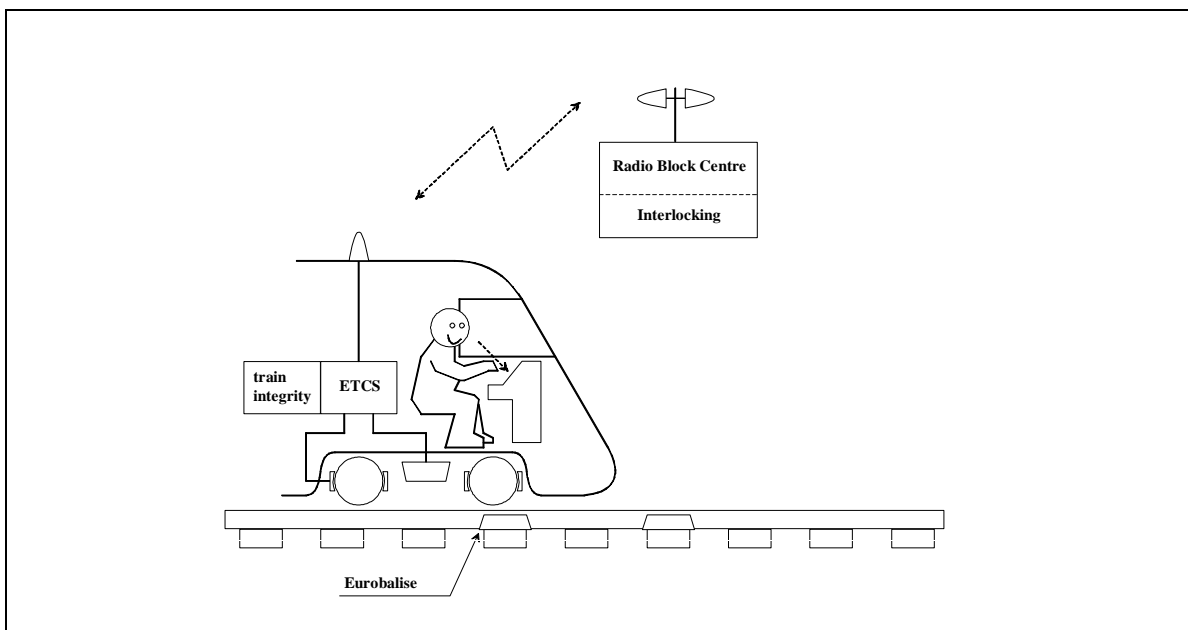


Bild 2-6: ERTMS/ETCS Application Level 3

Quelle: [UNISIG 26], 2.6.7, Fig. 7

Die Prinzipien zur Selbstortung der Züge und zur Überwachung der aktuellen Geschwindigkeit sind mit denen in Level 2 identisch. Es gibt keine ortsfesten Signale und keine streckenseitigen Einrichtungen zur Gleisfreimeldung. Letztere erfolgt, in dem das ETCS-Streckengerät kontinuierlich den Ort des Fahrzeugs verfolgt und daraus in Verbindung mit der vom Fahrzeug empfangenen Information über die Zugintegrität die Gleisfreiheit feststellt. Die Überwachung der Zugintegrität ist jedoch nicht Bestandteil des ETCS.

2.3 Probleme bei der Einführung von ETCS

Bei der Einführung des ETCS gibt es mehrere Probleme. In den derzeitigen Tests wird im wesentlichen die technische Interoperabilität von Komponenten unterschiedlicher Hersteller getestet. Unklar ist derzeit, nach welchen Betriebsvorschriften unter der Verantwortung von ETCS gefahren werden soll. Ein weiteres Problem ist die erforderliche Sicherheit des ETCS. Dazu gibt es bis heute noch keine Einigung zwischen Betreibern, Herstellern und Zulassungsbehörden.

2.3.1 Kompatibilität der technischen Komponenten

Die von UNISIG entwickelte Referenzarchitektur für ETCS (Bild 2-7) besteht aus den Hauptkomponenten Fahrzeuggerät (ETCS on-board) und Streckengerät (ETCS Track side). Diese interagieren mit den nicht zum ETCS gehörenden Elementen Fahrzeug, Fahrer und der externen Streckenausrüstung (z.B. vorhandenes ESTW).

Hauptaugenmerk bei der Entwicklung und Implementierung von ETCS liegt derzeit auf der Interoperabilität technischer Komponenten unterschiedlicher Hersteller [SD2002 (1)]. In mehreren europäischen Ländern laufen dazu Pilotversuche [SD2002 (4)] oder sind in Vorbereitung [W2]. Die Trennung der Ausrüstungsstufen (Level) und der entsprechenden Funktionen erfolgte auch in [UNISIG 26] nicht konsequent. Zum Beispiel heißt es in der Beschreibung des Modus SL (Sleeping): „...The ERTMS/ETCS on-board equipment shall open a communication session with the RBC when following events occur in all levels...“. Ein RBC (Radio Block Centre) ist jedoch erst ab dem Level 2 Bestandteil des ETCS.

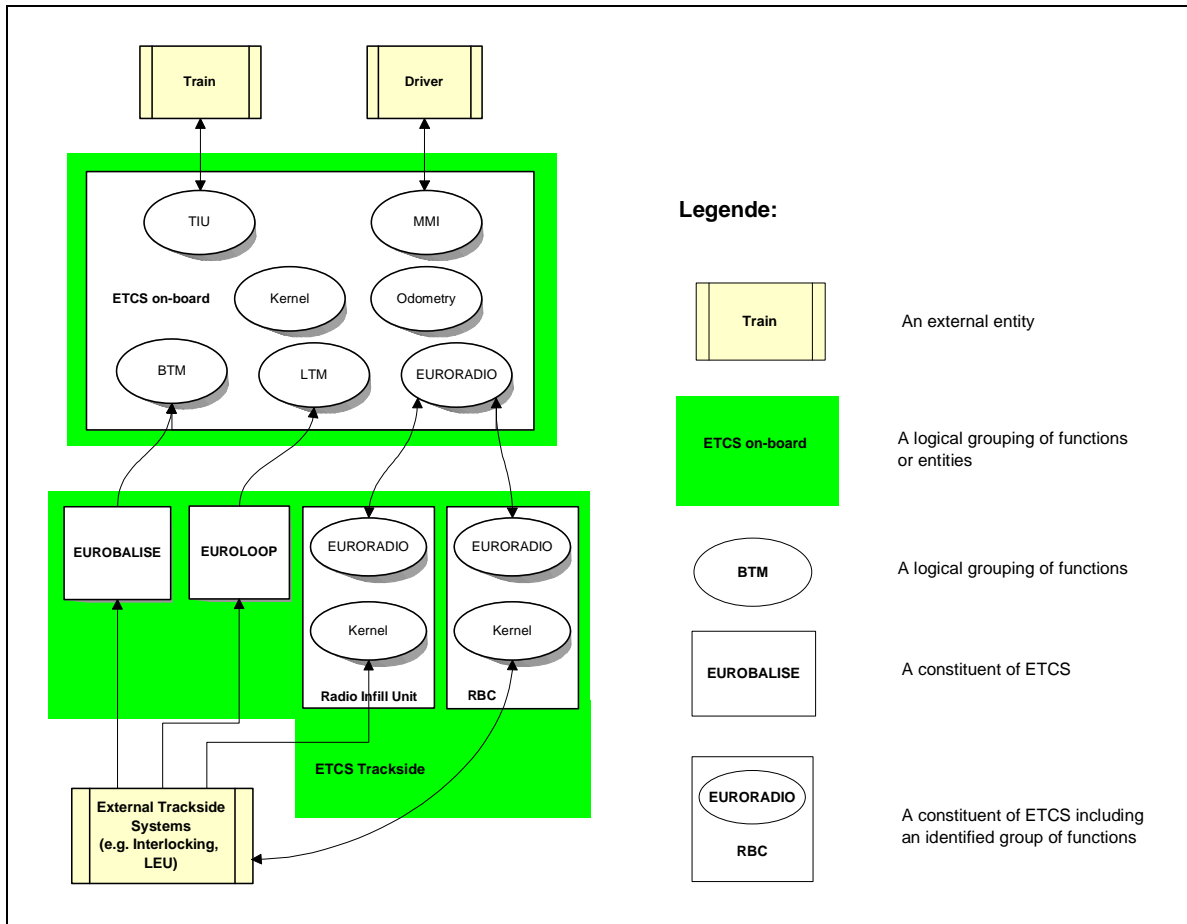


Bild 2-7: Referenzarchitektur ETCS

Quelle: [UNISIG 30], 4.4, Fig. 2

Diese Tests sollen nach der in [SD2002 (1)] vorgeschlagenen Strategie durchgeführt werden. Nach der Testmatrix werden nur ca. 11% der möglichen Kombinationen getestet (43% nicht machbar bzw. unpassend (not feasible), 26% keine Aussage). Es ist zu vermuten, dass die gewünschte technische Interoperabilität bei exakter Definition der Schnittstellen zwischen den verschiedenen Hardware-Komponenten erreicht werden kann, aber es drängt sich die Frage auf, ob beim Einsatz eines komplexen Systems wie ETCS die Abarbeitung dieser Testmatrix ausreicht, um die Interoperabilität zu gewährleisten [STO1996].

Ein vollständiger Test der Software-Komponenten sowie deren Zulassung ist weitaus schwieriger, wenn nicht sogar unmöglich, da die logischen Beziehungen und Strukturen nicht mehr überschaubar sind [SAE 4754] [STO1996]. Das Vorhandensein vieler unterschiedlicher nationaler Festlegungen (national values) erweitert den „Zustandsraum“ des ETCS zusätzlich.

2.3.2 Einheitliche Betriebsvorschriften (Interoperabilität)

Weder in [FRS99] noch in UNISIG - Class 1 werden Festlegungen zur Betriebsdurchführung unter der Verantwortung von ETCS getroffen. In [UNISIG 26], Punkt 1.7.1.3, heißt es dazu: „...It is not the

scope of this specification to mandate a specific use of ETCS.“ Das verwundert nicht, denn die Festlegung des Betriebes von ETCS kann nicht alleinige Aufgabe der Hersteller sein. Nicht zuletzt sind die Forderungen der Bahnen in [FRS99] nach nationalen Regelungen Ausdruck der Uneinigkeit über die Betriebsdurchführung. Aus [SD2002 (1)] entsteht sogar der Eindruck, Aufgabe der derzeitigen Tests sei es, erst einmal herauszufinden, wie man ETCS betrieblich nutzen kann.

Bei dem derzeitigen Pilotprojekt in Deutschland (Strecke Jüterbog-Halle/Leipzig) werden ersatzweise die betrieblichen Vorschriften der DB AG für das Fahren nach Führungsgrößen bei der Linienförmigen Zugbeeinflussung verwendet. Bei den Pilotprojekten der anderen Bahnen (SNCF, SBB, RENFE) werden deren Betriebsvorschriften zu Grunde gelegt. Es liegt nahe, dass eine solche Vorgehensweise keine geeignete Basis für Interoperabilität eines gemeinsamen Zugsteuerungssystems ist, da allein technische Interoperabilität noch keine vollständige Interoperabilität (grenzüberschreitend einheitlichen Betrieb) gewährleistet.

Unfälle und Gefährdungen beim Betrieb der Eisenbahn resultieren zu einem großen Anteil aus Abweichungen vom Regelbetrieb oder schwer durchschaubarer Vorschriftenlage [EBA], [SD2002 (5)]. Dies wird umso komplizierter bei dem geplanten Mischbetrieb (Fahrzeuge und Strecke haben nicht überall den gleichen Ausrüstungsgrad) verschiedener ETCS-Level.

Besonders in den Ausrüstungsstufen, in denen das jeweilige nationale Signalsystem parallel betrieben wird und als Rückfallebene dienen soll, muss das Betriebspersonal für mehrere nationale Betriebsvorschriften und Signalsysteme geschult sein sowie mehrere Sprachen beherrschen (z.B. beim Fahren auf Befehl). Die Risiken dieser Strategie sind derzeit nicht überschaubar. Für die angestrebte technische Interoperabilität zur Verbesserung des Wettbewerbes im Herstellerbereich ist eine einheitliche betriebliche Vorgabe notwendig, da sonst die Gefahr nationaler (hersteller- und bahnspezifischer) Implementierungen nahe liegt.

2.3.3 Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit, Sicherheit (RAMS)

Die Entwicklung und der Betrieb von ETCS stellen hohe Anforderungen an die Sicherheit und Zuverlässigkeit. In [FRS99], Kapitel 8: „Reliability, Availability, Maintainability, Safety (RAMS)“ findet sich dazu lediglich die Aussage „For interoperability the RAMS targets will be defined in other documentation outside this specification. (M)“. Bis heute gibt es keine einheitlich abgestimmte Definition der RAMS-Anforderungen [TSI].

Besonders schwierig gestaltet sich die Beantwortung der Frage nach der erforderlichen Sicherheit des ETCS. Der Versuch, diese Frage mit Risikoanalysen zu beantworten, scheitert bisher unter anderem daran, dass es keine einheitliche Risikoakzeptanz gibt. Auch in der Risikoanalyse steht die Frage, ob das in der Analyse ermittelte Risiko akzeptierbar ist oder nicht. Das bedeutet, dass die Bemühungen und der Aufwand für diverse Risikoanalysen zur Ableitung von Sicherheitsanforderungen so lange vergeblich sein werden, wie keine Einigkeit bei der Risikoakzeptanz erzielt werden kann.

Das Risiko eines bestimmten Systems wird bestimmt von technischen und betrieblichen Randbedingungen [FENNER] [SAE 4754], die bei der Ermittlung der erforderlichen Sicherheit beachtet werden müssen. Aus [SD2002 (3)] geht jedoch hervor, dass im Rahmen der dort beschriebenen Folgenanalyse erkannte betriebliche Risiken keinen Einfluss auf Anforderungen an ETCS-Produkte haben sollen.

Den ETCS-Komponenten der Referenzarchitektur (Bild 2-7) sind in [UNISIG 26], 2.6.6.2.4, bereits Funktionen zugeordnet. Die Hauptfunktionen des ETCS-Fahrzeuggerätes sind aus Bild 2-8 ersichtlich. Sie wurden zur besseren Adressierbarkeit im laufenden Text mit den Nummern 1 bis 6 bezeichnet.

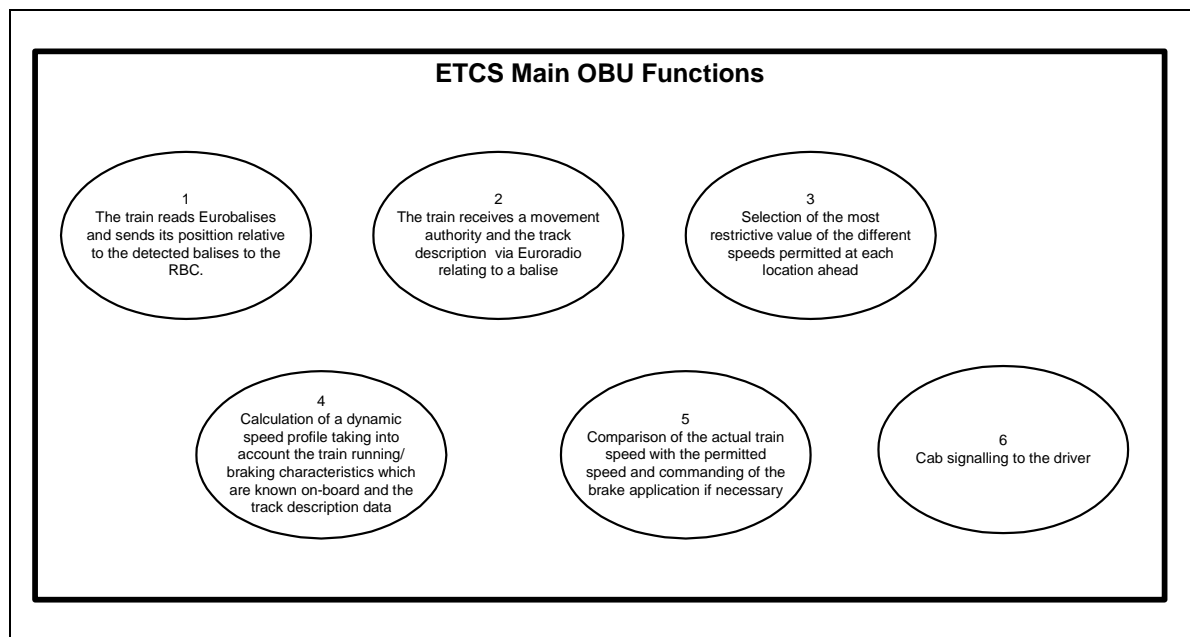


Bild 2-8: Main ERTMS/ETCS Onboard Functions

Da an der Erfüllung jeder dieser Funktionen mehrere Elemente des Fahrzeuggerätes beteiligt sind (dieses also nach [SAE 4754] hochintegriert ist), ist die Bestimmung der erforderlichen Sicherheit für die jeweiligen Elemente des Fahrzeuggerätes nur über die Bestimmung der erforderlichen Sicherheit der Funktion möglich. Natürlich kann man fragen: „Wie sicher muss das MMI sein?“ oder „Wie sicher muss das Display sein?“ oder „Wie sicher muss die Informationsübertragung sein?“. Diese komponentenbezogenen Fragen lassen sich jedoch nicht beantworten, wenn nicht genau definiert ist, mit welcher Sicherheit das Element seine Funktion erfüllen muss. Implizit ist dabei unterstellt, dass die Funktion des Elementes bereits genau beschrieben ist. Die Beschreibung muss dabei so sein, dass die Analyse eines Funktionsausfalls möglich ist [PORT2000]. Unmöglich wird die Bestimmung der erforderlichen Sicherheit für ein Element, wenn die zu erfüllende Funktion Teil einer übergeordneten Funktion ist, an deren Erfüllung mehrere Elemente beteiligt sind und nicht definiert ist, wie sicher die übergeordnete Funktion erfüllt werden muss [SAE 4754]. Die Sicherheitsanforderung an eine Funktion muss also unabhängig von der Implementierung sein.

Andernfalls liegt die Gefahr nahe, dass die Zuweisung von Funktionen zu Architekturelementen ohne Kenntnis der Sicherheitsanforderung an die zugewiesene Funktion zu einer unausgewogenen Systemarchitektur führt. Diese lässt sich nur mit großem Aufwand und damit hohen Kosten korrigieren, wenn nach der vollständigen Festlegung der Systemarchitektur und u.U. nach der Implementierung des Systems die getroffene Funktionsverteilung als nicht sicher erkannt wird. Andererseits kann es passieren, dass die Systemarchitektur überdimensioniert und das System damit zu teuer wird. Sicherheitsanalyse und Entwicklung der Systemarchitektur sollten deswegen parallel verlaufen [SAE 4754].

3 FHA – Functional Hazard Assessment

„Functional Hazard Assessment (FHA)“ ist eine in der Luftfahrt anerkannte Methode zur Ableitung von Sicherheitsanforderungen bei der Entwicklung und Zulassung komplexer und hochintegrierter Systeme. In einigen Bereichen wird die Methode auch „Functional Hazard Analysis (FHA)“ genannt. Die Abkürzung FHA wird synonym für beide Bezeichnungen der Methode verwendet.

Für ein gutes Verständnis von FHA ist es hilfreich, zunächst einen Überblick über den Luftverkehr zu geben. Dazu erfolgt eine kurze Betrachtung der organisatorischen Aufteilung des Betriebes sowie die Vorstellung einiger wichtiger Behörden und Institutionen. Im Anschluss daran wird das Vorgehen beim Functional Hazard Assessment im Detail vorgestellt.

3.1 Luftverkehr - Einordnung und Überblick

Der Luftverkehr wird unterteilt in militärischen und zivilen Luftverkehr. In beiden Bereichen gibt es eine Trennung zwischen Fluggerät und Flugsicherung. Der zivile Luftverkehr ist heutzutage ein wichtiger Bestandteil der globalen Logistik. Durch diese Internationalität werden vielseitige hoheitliche, kommerzielle, juristische und öffentliche Interessen berührt. Um die Wirtschaftlichkeit und die Sicherheit des internationalen Luftverkehrs zu verbessern, werden kontinuierlich national unterschiedliche Regelungen zwischenstaatlich harmonisiert. Dies gilt insbesondere für die Sicherheit im Luftverkehr.

3.1.1 Grundsätzliche Organisation

Die Aufsicht über den Luftverkehr ist weltweit hoheitliche Aufgabe eines jeden Staates. In Deutschland wird diese Aufgabe vom Bundesministerium für Verkehr, Bau- und Wohnungswesen (BMVBW) wahrgenommen.

Der Luftraum des Hoheitsgebietes ist in Sektoren aufgeteilt, in denen jeweils die Bewegungen am Boden und in der Luft aller im Sektor befindlichen Flugzeuge von der Flugsicherung organisiert und überwacht werden. Die Flugsicherung autorisiert die Flugzeugbesatzung (Crew) zu Bewegungen am Boden, erteilt Start- und Landeerlaubnis und informiert die Crew während des Fluges über die Freiheit der Flugbahn [TUD].

Die Kommunikation (Bild 3-1) zwischen Flugsicherung und Crew erfolgt verbal nach von der ICAO weltweit einheitlich festgelegten Regeln, sogenannten Sprechgruppen. Diese sind grundsätzlich in englischer Sprache verfasst, wobei auch Kunstwörter zum Einsatz kommen. Damit ist die Grundvoraussetzung für einen international einheitlichen Betrieb geschaffen. Dass dieser auch in der Luftfahrt nicht lückenlos definiert ist, hat die Flugzeugkollision am 01.07.02 in Überlingen, Deutschland eindrucksvoll gezeigt [W11].

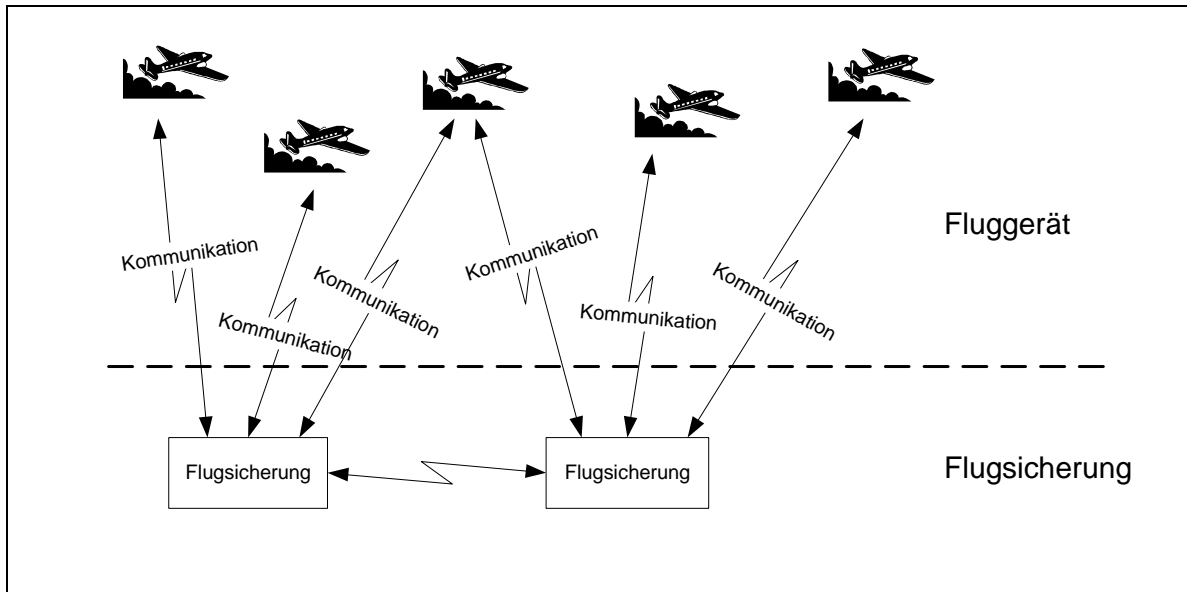


Bild 3-1: grundsätzliche organisatorische Aufteilung im Luftverkehr

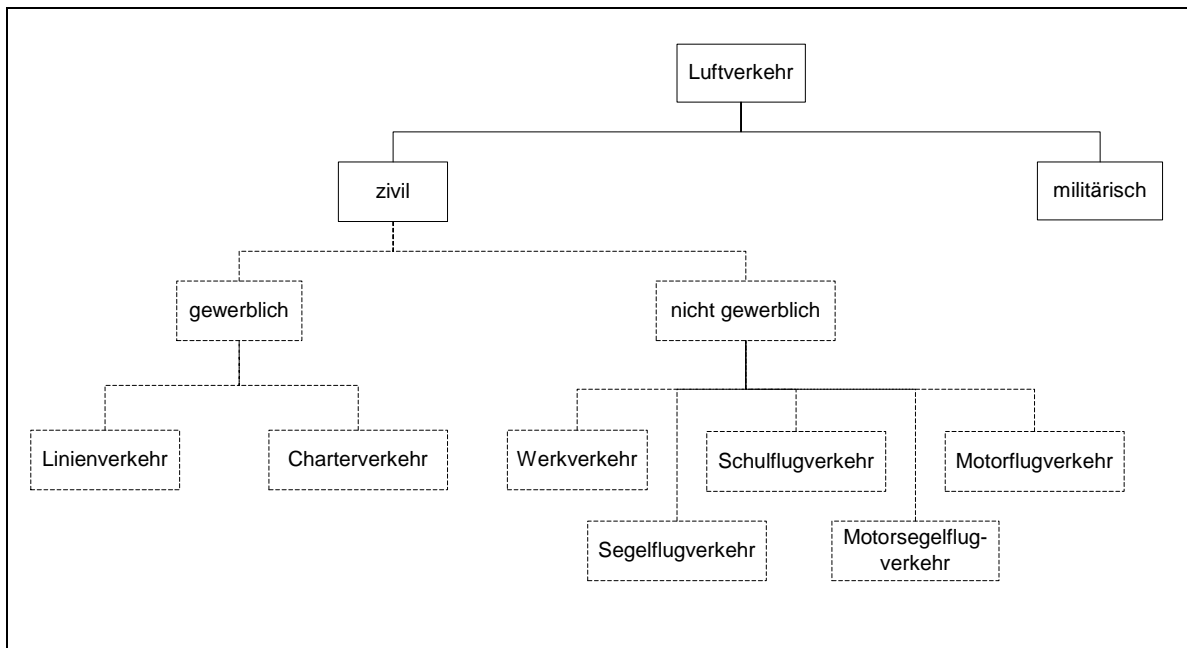
Die Entscheidungshoheit über die Steuerung des Flugzeuges obliegt in der letzten Konsequenz dem Piloten. Das heißt, dass dieser sich über alle Anweisungen von der Flugsicherung oder Hinweise und Warnungen des Bordgerätes hinwegsetzen kann, wenn es nach seiner Meinung für die Fortsetzung des Fluges bzw. die Landung erforderlich ist. Das Flugzeug kann somit über eine gewisse Strecke autark, d.h. ohne Kontakt zum Boden, kontrolliert gesteuert werden.

Das BMVBW hat für das deutsche Hoheitsgebiet die Aufsicht über Fluggerät (Flugzeug einschließlich allen Bordgerätes) an das Luftfahrtbundesamt (LBA) und die Aufsicht für die Flugsicherung an die Deutsche Flugsicherung GmbH (DFS) delegiert [W12]. Die DFS ist ein privatrechtlich organisiertes Unternehmen, dessen alleinige Gesellschafterin die Bundesrepublik Deutschland ist [W12]. Es gibt somit keinen freien Marktzugang und keinen Wettbewerb im Bereich der Flugsicherung.

Zur Entwicklung und Herstellung von Fluggerät ist eine spezielle Zulassung des Betriebes durch die Zulassungsbehörde erforderlich.

3.1.2 Arten des Luftverkehrs

Der Luftverkehr kann grundsätzlich in zivilen und militärischen Luftverkehr unterschieden werden (Bild 3-2).



Quelle: nach [TUD]

Bild 3-2: Arten des Luftverkehrs

Aufgrund der größeren Nähe der Eisenbahn als ziviles Transportsystem für Güter und Personen zum zivilen Luftverkehr werden für die weiteren Untersuchungen in dieser Arbeit nur Regelwerke des zivilen Luftverkehrs betrachtet. (In einigen Fällen bilden allerdings Standards aus dem militärischen Bereich (MIL) die Grundlage für Vorschriften im zivilen Luftverkehr.)

3.1.3 Sicherheit im Luftverkehr

Entsprechend der Trennung zwischen Fluggerät und Flugsicherung existieren für jeden dieser Bereiche zahlreiche Normen, Vorschriften und Standards zur Gewährleistung der erforderlichen Sicherheit. Das dem Luftverkehr innewohnende hohe Schadenspotential (viele Tote, hoher Sachschaden) erzwingt bereits vor der Zulassung, d.h. bei der Entwicklung und Implementierung von Fluggerät und Anlagen der Flugsicherung hohe Anforderungen an die zu realisierende Sicherheit [SAE 4754].

Da ein sehr großer Teil des internationalen Luftverkehrs zwischen Nordamerika (USA) und Europa abgewickelt wird, ist es wirtschaftlich zwingend notwendig, dass Fluggesellschaften Flugzeuge betreiben, die für den Betrieb in allen berührten Hoheitsbereichen zugelassen sind. Da eine zulassungsfähige Entwicklung von Fluggerät sehr teuer ist, geht auf Drängen der Industrie seit einigen

Jahren das Bestreben europäischer (JAA) und nordamerikanischer (FAA) Zulassungsbehörden zu einem einheitlichen Zulassungsprozess. Dieser Weg wird konsequent vorangetrieben [W6].

Bild 3-3 gibt einen Überblick über die im weiteren verwendeten Vorschriften und deren Zuordnung zum jeweiligen Herausgeber. Die Darstellung enthält selbstverständlich nur einen geringen Auszug der vielfältigen Beziehungen zwischen Behörden, Interessenverbänden und Vorschriften.

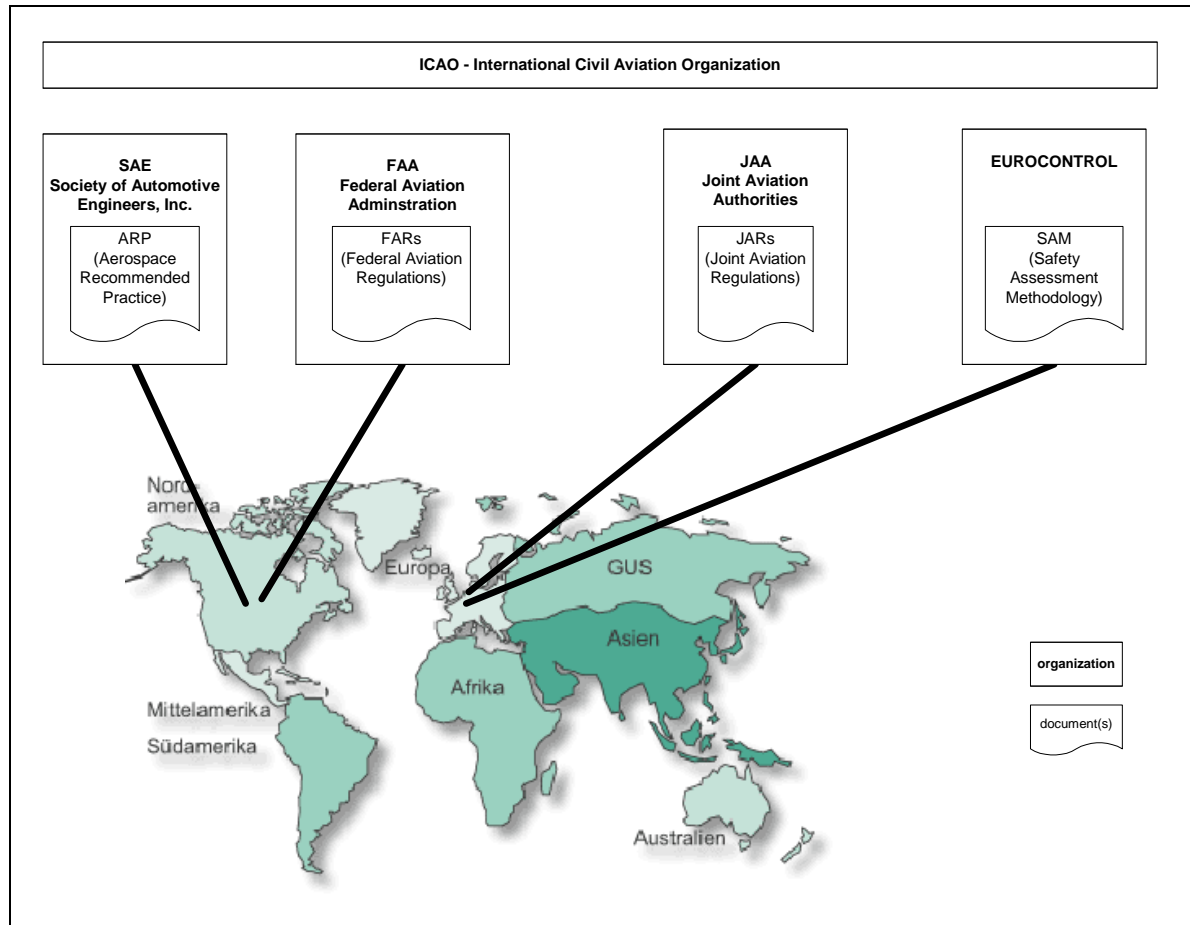


Bild 3-3: geografische Verteilung ausgewählter Zulassungsbehörden und Normungsgremien

ICAO

Die International Civil Aviation Organization (ICAO) ist der Dachverband der Weltluftfahrt. Er unterstützt die Entwicklung und Einführung von Standards für Flugbetrieb, Navigation und Luftraummanagement, Ausbildung des Personals, Auslegung von Flughäfen und Fragen der Sicherheit im Luftverkehr [W9].

Die dem Luftverkehr als weltweites Transportmittel immanente Internationalität bringt auch internationale Probleme mit sich. Die Koordinierung von Technologien und Gesetzen sowie die Veröffentlichung von technischen und wirtschaftlichen Informationen können nicht von jeder

einzelnen Regierung bewältigt werden. Die Notwendigkeit der Sicherheit und Regulierung im Luftverkehr beinhalten u.a. die Errichtung von Flughäfen, die Aufstellung von Navigationshilfen und Wetterstationen. Die Standardisierung von betrieblichen Vorgängen für den internationalen Betrieb ist von fundamentaler Bedeutung, so dass Fehler durch Missverständnisse oder Unerfahrenheit vermieden werden [W9].

FAA – Federal Aviation Administration

Die Bundesluftfahrtbehörde (FAA) ist als Abteilung des Transportministeriums (Department of Transportation) Teil der Regierung der USA und primär für die Sicherheit der Zivilluftfahrt verantwortlich. Ihre Hauptaufgaben [W7] umfassen die

- Regelung der Zivilluftfahrt zur Förderung der Sicherheit und zur Erreichung der Anforderungen der Nationalverteidigung,
- Förderung und Entwicklung der zivilen Luftfahrt, einschließlich neuer Luftfahrttechnologien,
- Entwicklung und Betrieb eines gemeinsamen Systems für die Flugsicherung von Zivil- und Militärflugzeugen,
- Forschung und Entwicklung in den Bereichen Raumfahrt und zivile Luftfahrt,
- Entwicklung und Einführung von Maßnahmen zur Kontrolle von Fluglärmemissionen und anderen Umweltfolgen der zivilen Luftfahrt und
- Regulierung der kommerziellen Raumfahrt der USA.

Die FAA gibt Regelungen und Standards bezüglich der Sicherheit bei Herstellung, Betrieb und Wartung von Flugzeugen heraus und setzt deren Einhaltung durch. Sie ist außerdem verantwortlich für die Lizenzierung des Flugpersonals und für die Zulassung von Flughäfen [W7].

Zur sicheren und effektiven Nutzung des verfügbaren Luftraums betreibt die FAA ein Netz von Tower und Stationen zur Flugsicherung sowie Luftverkehrsleitzentralen. Sie entwickelt Regelungen für die Abwicklung des Luftverkehrs, organisiert die Nutzung des Luftraumes und unterstützt dessen Überwachung zur Wahrung der nationalen Sicherheit.

Im Auftrag des Gesetzgebers fördert die FAA die Sicherheit der Luftfahrt im Ausland. Dies umfasst den Austausch aeronautischer Informationen mit ausländischen Behörden, Zertifizierung ausländischer Reparaturwerkstätten sowie fremden Flug- und Servicepersonals, technische Unterstützung und Ausbildung, Abschluss bilateraler Abkommen zur Harmonisierung von Normen und Standards sowie Ausrichtung internationaler Konferenzen.

Die FAA treibt die Forschung und Entwicklung von Systemen und Verfahren zur sicheren und leistungsfähigen Steuerung des Luftverkehrs voran (Flugmedizin, Flugzeuge, Triebwerke, Ausrüstung) und überprüft, testet und überarbeitet bestehende Spezifikationen.

Die Behörde überwacht im Rahmen der Zulassung eine jeweils ausreichende Versicherung (z.B. für den Betrieb eines Flugzeuges), entwickelt Vorgaben für Statistiken und sammelt die notwendigen Daten. Außerdem veröffentlicht sie Informationen über Fluggesellschaften, Flughäfen und technische Themen der Luftfahrt. Die Vorschriften der FAA erscheinen unter der Bezeichnung „Federal Aviation Requirement“ (FAR).

JAA – Joint Aviation Authorities

Die JAA entstand 1970 als ein Zusammenschluss nationaler europäischer Luftfahrtbehörden. Anfänglich nur zur Harmonisierung von Zulassungsvorschriften für große Verkehrsflugzeuge und Triebwerke gedacht, umfasst der Arbeitsbereich seit 1987 auch Betrieb, Wartung und Zulassung von Entwicklungsstandards für alle Klassen von Verkehrsflugzeugen [W6]. Die Vorschriften der JAA erscheinen unter der Bezeichnung Joint Aviation Regulation (JAR) und sind seit 1992 in den JAA-Mitgliedsstaaten Gesetz durch die nationalen Behörden zum Gesetz erhoben [W13].

Die JAA entstand im wesentlichen als „behördliches Gegengewicht“ zur FAA, um die Interessen der europäischen gegenüber der nordamerikanischen Industrie zu vertreten. In der JAA sind die zivilen Luftfahrtbehörden derjenigen europäischen Länder vertreten, die der „Kooperationsvereinbarung zur Entwicklung und Implementierung gemeinsamer Sicherheitsstandards und Sicherheitsprozeduren“ (Zypern, September 1990) zugestimmt haben [W6]. Mit dieser Kooperation sollen hohe und konsistente Sicherheitsstandards erreicht werden, um eine Basis für einen fairen Wettbewerb innerhalb Europas bei der Entwicklung und Herstellung großer Verkehrsflugzeuge zu schaffen. Die Kooperationsvereinbarung umfasst folgende [W6] Ziele:

- „Luftfahrt-Sicherheit“: Durch Zusammenarbeit innerhalb der Mitgliedsstaaten soll ein einheitlicher und durchgängiger Sicherheitsstandard erreicht werden.
- „Übergang von der JAA zur EASA (European Aviation Safety Agency)“: Durch den schnellen Übergang zu einer europäischen Sicherheitsbehörde soll sichergestellt werden, dass die EU und die Mitglieder der JAA, die nicht Mitglied der EU sind, den gleichen Beitrag zur Sicherheit leisten.
- „Wirtschaftlicher Erfolg“: Einführung eines kostengünstigen Sicherheitssystems als Beitrag zu einem effizienten zivilen Luftverkehr.
- „Harmonisierung von Standards“: Beitrag zur Förderung eines fairen Wettbewerbs innerhalb der Mitgliedsstaaten durch einheitliche Anwendung gemeinsamer Standards und regelmäßige Überprüfung existierender Standards.

- “Verbesserung der Sicherheit in der weltweiten Luftfahrt“: Durch internationale Kooperationen sollen die Regelwerke der JAA auch zur Verbesserung der Sicherheit der Luftfahrt weltweit beitragen.

Dazu wurden der JAA folgende Aufgaben und übertragen:

- Entwicklung und Anpassung von Joint Aviation Requirements (JARs) in den Bereichen der Entwicklung und Herstellung sowie dem Betrieb und der Wartung von Flugzeugen und Lizenzierung von Flugzeugbesatzungen.
- Entwicklung administrativer und technischer Prozesse zur Implementierung der JARs.
- Einheitliche Implementierung der JARs und der entsprechenden administrativen und technischen Prozesse.
- Ergreifung von Maßnahmen um sicherzustellen, dass die Verfolgung von Sicherheitszielen der JAA den Wettbewerb in der Luftfahrtindustrie innerhalb der Mitgliedsstaaten nicht beeinträchtigt oder Firmen aus Mitgliedsstaaten einen Wettbewerbsnachteil gegenüber Firmen aus Nicht-Mitgliedsstaaten haben.
- Unterstützung des europäischen Kompetenzzentrums zur Harmonisierung europäischer Vorschriften und Regelwerke.
- Einführung von gemeinschaftlichen Prozessen zur Zulassung von Produkten und Betrieb mit dem Ziel der gegenseitigen Anerkennung von Zulassungen.
- Zusammenarbeit bei der Harmonisierung von Anforderungen und Prozessen anderer Zulassungsbehörden, insbesondere mit der FAA, und wenn möglich Zusammenarbeit bei der Zulassung von Produkten und Betrieb.

Dabei liegt großes Augenmerk auf der Harmonisierung der Vorschriften und Regelwerke der JAA mit denen der FAA. In 1992 trafen JAA und FAA eine Vereinbarung zur Harmonisierung der JARs und FARs, wo nötig, bis zur vollständigen Übereinstimmung.

Die in dieser Arbeit verwendete Vorschrift [JAR 25.1309] sowie die begleitenden [AMJ 25.1309] und [ACJ 25.1309] sind zwischen FAA und JAA weitestgehend harmonisiert.

SAE – Society of Automotive Engineers, Inc.

Die SAE ist ein Netzwerk von weltweit über 83.000 Ingenieuren, Führungskräften, Ausbildern und Studenten zum Informations- und Ideenaustausch zur Förderung der Entwicklung von Technik verschiedenster Industriebereiche, hauptsächlich aber von Verkehrssystemen jeglicher Art [W8]. Die technischen Ausschüsse der SAE erstellen nach eigenen Angaben mehr Standards für Luftfahrt- und Automobiltechnikanwendungen als jedes andere Standardisierungsgremium der Welt.

Unter der Beteiligung von Zulassungsbehörden, Herstellern und Betreibern entwickelte die SAE im Auftrag der FAA einen einheitlichen Prozesses zur Entwicklung und Zulassung großer Verkehrsflugzeuge. Dessen Beschreibung erschien als “Aerospace Recommended Practice 4754: Certification Considerations for highly-integrated or complex aircraft systems” [SAE 4754] und “Aerospace Recommended Practice 4761: Guidelines and methods for conducting the safety assessment process on civil airborne systems and equipment” [SAE 4761].

EUROCONTROL

EUROCONTROL (European Organisation for the Safety of Air Navigation) ist eine europäische Organisation und ein Zusammenschluss der europäischen Aufgabenträger der Flugsicherung. Im Rahmen der Einführung eines Programms für ein europäisches Luftraummanagement (European Air Traffic Management Programme) ist EUROCONTROL auch für die Bewertung der Sicherheit der neuen Systeme für die Flugsicherung verantwortlich [W10]. Das zu diesem Zweck erstellte Dokument wird unter dem Titel „Air Navigation System Safety Assessment Methodology“ [EC2000] geführt.

3.2 Der Sicherheitsprozess der Society of Automotive Engineers (SAE)

Mit der fortschreitenden technologischen Entwicklung und insbesondere mit dem zunehmendem Einsatz von Elektronik und Software in Flugzeugen stieg deren Komplexität an, so dass die Entwicklung von Flugzeugen und deren Zulassung durch die Behörde (FAA) immer schwieriger wurde [SAE 4754].

Bei der Revision des Standards DO-173: „Minimum Operational Performance Standards for Airborne Weather and Ground Mapping Pulsed Radars“ der Radio Technical Commission of Aeronautics, Inc. (RTCA) durch die FAA wurde offensichtlich, dass für die Entwicklung von Software Informationen aus der Systemebene unerlässlich sind [SAE 4754].

Da aber Entscheidungen auf Systemebene fundamental die Sicherheit und Funktionalität von Fluggerät beeinflussen, ist die Einbeziehung der Zulassungsbehörden bereits in den Entwicklungsprozess nicht nur notwendig, sondern auch sinnvoll [SAE 4754].

Die FAA beauftragte daraufhin die SAE mit der Entwicklung eines einheitlichen Systementwicklungsprozesses. Dieser durfte dabei nicht in Widerspruch zu bestehenden Vorschriften und Gesetzen stehen. Unter internationaler Beteiligung von Zulassungsbehörden, Herstellern, Betreibern und weiteren Interessenverbänden entstanden [SAE 4754] und [SAE 4761].

[SAE 4754] beinhaltet Hinweise und Überlegungen im Zusammenhang mit der Zulassung von großen Verkehrsflugzeugen. Es werden keine exakten Handlungsanweisungen gegeben. Im Vordergrund stehen die Übersicht über die Anwendung bestehender Standards und Normen.

[SAE 4761] enthält als Ergänzung zu [SAE 4754] detaillierte Beschreibungen des Sicherheitsprozesses sowie Hinweise auf geeignete Methoden für jede Stufe des Sicherheitsprozesses. Systementwicklungs- und Systemdesignprozesse werden dort nicht detailliert beschrieben, da dies bereits an anderen Stellen (Normen, Standards) erfolgt ist. [SAE 4754] und [SAE 4761] haben den Charakter von Richtlinien, die hauptsächlich einem breiten Verständnis für das Zusammenspiel zwischen Sicherheits- und Entwicklungsprozess dienen sollen. Sie bilden zusammen als Konsens aller beteiligten Interessen eine gemeinsame Grundlage für die Entwicklung und Zulassung großer Verkehrsflugzeuge. Damit kann in Bezug auf Entwicklung und Zulassung eine hohe und gleichbleibende Sicherheit erreicht werden.

Während der gesamten Entwicklung dieses Sicherheitsprozesses gab es mehrfach von den beteiligten Parteien kontroverse Forderungen nach der Detailliertheit der Festlegungen für die Zulassung [SAE 4754]. Man stellte explizit fest, dass die Zulassung jedes nicht-idealen Systems ingenieurmäßige Beurteilungen von allen Beteiligten erfordert [SAE 4754], d.h. dass bei der Entwicklung und Beurteilung nicht-idealer Systeme nicht jeder Sachverhalt in exakten Zahlen ausgedrückt werden kann, sondern ein gewisses Augenmaß und Erfahrung erforderlich sind. Eine hohe Qualität wird nur dann erreicht, wenn alle Seiten von einem gemeinsamen Verständnis fundamentaler Prinzipien und Methoden ausgehen und diese konsequent beachten und anwenden [SAE 4754].

Mit Hilfe der nach eigenen Angaben vielfältigen Expertise der SAE flossen in die Entwicklung dieses Sicherheitsprozesses zusätzlich zu den existierenden Normen, Standards und Gesetzen auch Erkenntnisse aus anderen Industriebereichen (z.B. Kernkraft und chemische Industrie) ein.

In diesem Zusammenhang weist die SAE explizit darauf hin, dass dieser Sicherheitsprozess nicht auf die Entwicklung von Fluggerät beschränkt ist, sondern dass er auch, sinngemäß angepasst, in anderen sicherheitskritischen Industriebereichen anwendbar ist.

Auf eine detaillierte Beschreibung des gesamten Sicherheitsprozesses wird an dieser Stelle verzichtet, da dies eine Übersetzung von [SAE 4754] und [SAE 4761] bedeuten würde. Stattdessen seien folgende Kerngedanken des Prozesses zusammengefasst:

1. Anwendbarkeit

Der Sicherheitsprozess ([SAE 4754] und [SAE 4761]) ist speziell auf die Entwicklung, Herstellung und Zulassung großer Verkehrsflugzeuge einschließlich allen Bordgerätes zugeschnitten. Ein großes Verkehrsflugzeug ist gemäß der Definition in [SAE 4754] ein komplexes und hochintegriertes System. Die oberste Betrachtungsebene umfasst das komplette Flugzeug einschließlich allen Bordgerätes (aircraft-level).

2. Akzeptanz und Einheitlichkeit des Sicherheitsprozesses

Durch die weltweite Einbindung von Herstellern (Flugzeugbauer, Konsortialindustrie), Betreibern (Fluggesellschaften), Zulassungsbehörden (FAA, JAA) und anderen

Interessenvertretungen und Behörden (ICAO, ATA, DoD, RTCA, EUROCAE und weitere) in die Entwicklung des Sicherheitsprozesses ist dieser international akzeptiert. Die Entwicklung und Zulassung großer Verkehrsflugzeuge folgen dem gleichen Prozess. Durch die im Sicherheitsprozess enthaltenen Vorgaben zur Dokumentation werden bei konsequenter Anwendung des Sicherheitsprozesses Transparenz und Nachvollziehbarkeit erzwungen.

3. Parallelität von Sicherheitsanalyse und Systementwicklung

Sicherheitsprozess und Systementwicklungsprozess laufen parallel ab. Der Sicherheitsprozess beeinflusst dabei frühzeitig die Entwicklung der Architektur des Systems. Dadurch wird eine Dimensionierung des Systems entsprechend der erforderlichen Sicherheit erreicht.

4. Objektivität

Grundlage für die Ableitung der Sicherheitsanforderungen für die Funktionen des Systems „Flugzeug“ ist die zwischen allen Beteiligten in fünf Stufen abgestimmte Risikoakzeptanz für den Betrieb großer Verkehrsflugzeuge. Dadurch und durch das einheitliche Vorgehen zur Ermittlung und Gegenüberstellung von Anforderungen wird der mit der Bewertung von Risiken verbundenen Subjektivität des Menschen (Entwickler, Zulassender, Gutachter) vorgebeugt.

Für diese Arbeit wird nur der Teil des Sicherheitsprozesses näher betrachtet, der im Rahmen der Systementwicklung für die Ableitung von Sicherheitsanforderungen vorgesehen ist (Bild 3-4). Diese Sicherheitsanforderungen werden mittels einer funktionalen Betrachtung des Systems „Flugzeug“ gewonnen. Dies erfolgt in der Phase des Functional Hazard Assessment (FHA). Die weiteren Schritte und Interaktionen zwischen Sicherheitsprozess und Entwicklungsprozesses sind vereinfacht dargestellt.

Gegenstand der Preliminary System Safety Analysis (PSSA) ist die Beantwortung der Frage: „Wie sicher ist die Systemarchitektur?“. Die PSSA stellt einerseits sicher, dass die während der FHA ermittelten Ausfallbedingungen vollständig sind und dient andererseits der Vervollständigung der Sicherheitsanforderungen. Außerdem dient die PSSA dem Nachweis, dass das Gesamtsystem die Sicherheitsanforderungen aus der FHA erfüllt. In der PSSA werden die funktionalen Sicherheitsanforderungen aus der FHA zuerst auf Teilsysteme und im weiteren auf Hardware und Software verteilt [SAE 4754] sowie die Notwendigkeit alternativer Schutzmechanismen (z.B. Überwachung, Redundanz; Diversität, Wartungsintervalle) ermittelt. Dazu werden verschiedene Methoden verwendet, z.B. Fault Tree Analysis, Dependence Diagramms, Markov Analysis. Dabei werden die Ursachen für Funktionsausfälle ermittelt sowie Abhängigkeiten zwischen Funktionen und Funktionsausfällen untersucht. PSSA ist die Grundlage für die Zuteilung von Zuverlässigkeitsanforderungen (zufällige Hardwareausfälle) an Architekturelemente.

Gegenstand der System Safety Analysis (SSA) ist die Beantwortung der Frage: „Wie sicher ist das implementierte System?“. SSA umfasst den Sicherheitsnachweis für das System. Darin ist nachzuweisen, dass die Anforderungen aus FHA und PSSA mit dem System erfüllt werden.

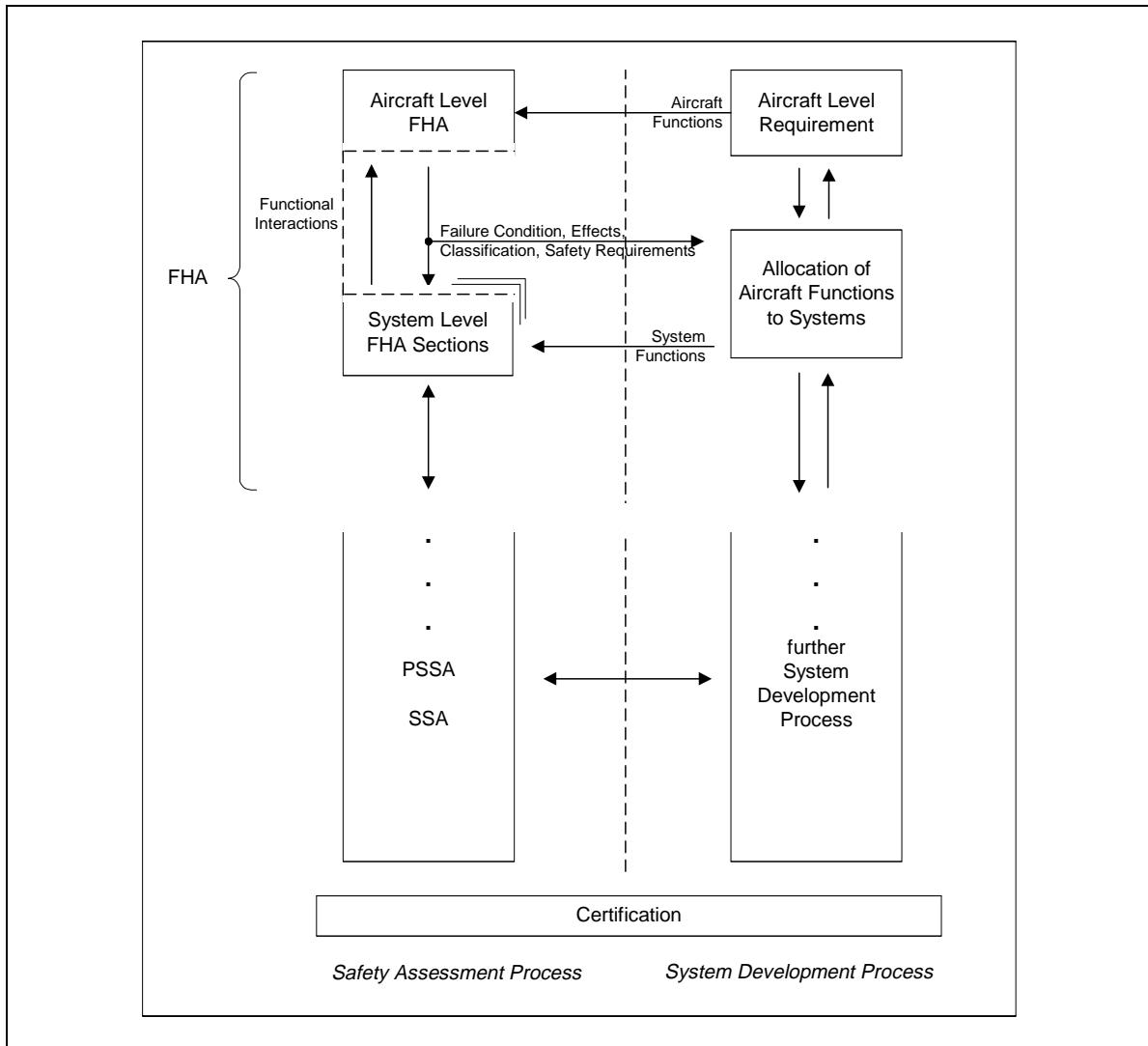
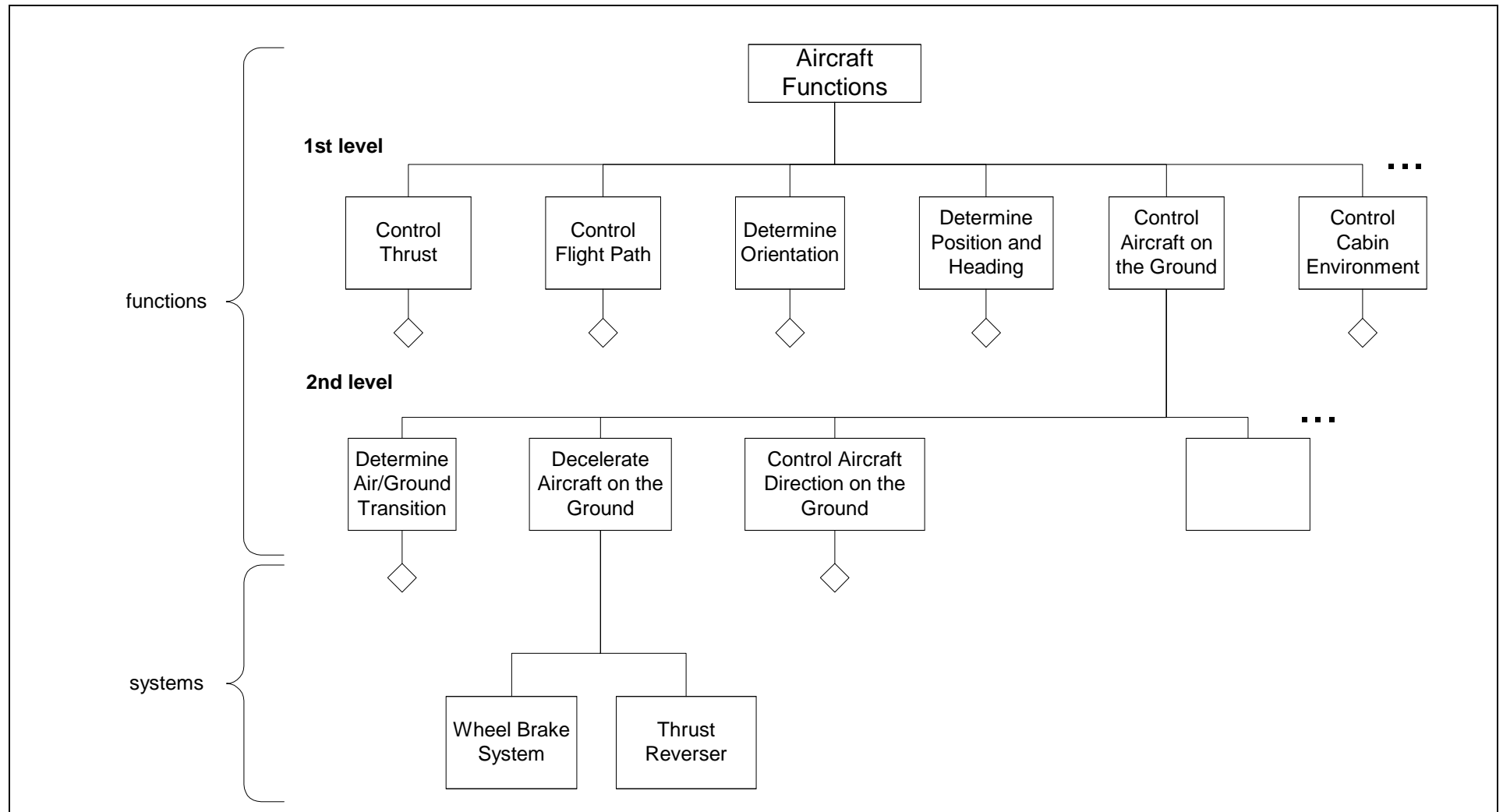


Bild 3-4: Safety Assessment process model

Quelle: nach [SAE 4754]

In Bild 3-5 ist beispielhaft die (unvollständige) Aufteilung von Funktionen für ein Flugzeug dargestellt. Die Funktionen der ersten Ebene sind im wesentlichen Flugzeugfunktionen, deren Ausfall jeweils katastrophale Folgen hat. In der zweiten Ebene ist die jeweilige Flugzeugfunktion in Teilfunktionen zerlegt. Diese werden dann bestimmten Systemen zugewiesen. So ist die Funktion „Bremsen des Flugzeugs am Boden“ („Decelerate Aircraft on the Ground“) verteilt auf die Systeme „Radbremse“ und „Schubumkehr“.



Quelle: nach [SAE 4761]

Bild 3-5: Aircraft Function Tree and allocation to systems

Diese beiden Systeme haben jeweils die Funktion „Bremsen des Flugzeugs am Boden“ zu erfüllen. Mit der FHA für die Funktion „Bremsen des Flugzeugs am Boden“ wird ermittelt, mit welcher Sicherheit diese Funktion für das Flugzeug (Aircraft Level FHA) erfüllt werden muss. Mit der FHA für die (jeweils gleichen) Teilfunktionen der beiden Bremssysteme (System Level FHA) kann die Sicherheitsanforderung der Funktion „Bremsen des Flugzeugs am Boden“ (Aircraft Level) auf die Teilsysteme „Radbremse“ und „Schubumkehr“ verteilt werden [SAE 4761].

3.3 Functional Hazard Assessment (FHA) - Durchführung

3.3.1 Ziele und Anwendungsbereiche

Software-basierte Systeme, die mit anderen Systemen in einer übergeordneten Funktionsumgebung interagieren, sind häufig komplex und hochintegriert [SAE 4754]. Komplexität heißt, dass die Sicherheit nicht allein durch Tests nachgewiesen werden kann und das System aufgrund der umfangreichen logischen Verknüpfungen ohne analytische Methoden nicht überschaubar ist [SAE 4754].

Häufig werden die einzelnen Elemente solcher Systeme von verschiedenen Mitarbeitern, Abteilungen oder Firmen entwickelt. Damit die Sicherheit dieser Systeme gewährleistet ist, erfordert deren Entwicklung besondere Entwicklungsmethoden und Strukturen, um zu gewährleisten, dass die Systeme die funktionalen und Sicherheitsanforderungen erfüllen können [SAE 4754] [STO1996].

Der Einsatz und Betrieb von sicherheitskritischen Systemen mit hohem Schadenspotential (Personenschäden, Sachschäden) erfordert schon bei der Entwicklung des Systems Aussagen zur Sicherheit, mit der das System seine Funktionen erfüllen soll (Betreiberanforderung, Firmenphilosophie) oder muss (Forderung der Zulassungsbehörde, gesetzliche Anforderung) [SAE 4754] [Anlage]. Diese Aussagen zur erforderlichen Sicherheit des Systems können in den meisten Fällen nicht ohne weiteres getroffen werden [STO1996]. Aufgabe der FHA ist es, die Antwort auf die Frage „Wie sicher muss das System sein?“ zu liefern, d.h. festzustellen, mit welcher Sicherheit die Systemfunktionen realisiert werden müssen.

FHA kann sowohl bei der Entwicklung neuer als auch bei der Modifikation existierender Systeme (funktionale Erweiterungen oder Reduktionen) eingesetzt werden.

Der Sicherheitsprozess nach [SAE 4754] und [SAE 4761] ist auf das System „großes Verkehrsflugzeug“ zugeschnitten, aber (als Prozess) grundsätzlich offen für die Anwendung in anderen Systemen. So hat EUROCONTROL seine Methodik zur Sicherheitsbewertung der Flugsicherung [EC2000] im Rahmen des „European Air Traffic Management Programme“ am Sicherheitsprozess nach [SAE 4754] und [SAE 4761] ausgerichtet. Die Ableitung von Sicherheitsanforderungen für das System „Flugsicherung“ wird von EUROCONTROL als Functional Hazard Analysis bezeichnet.

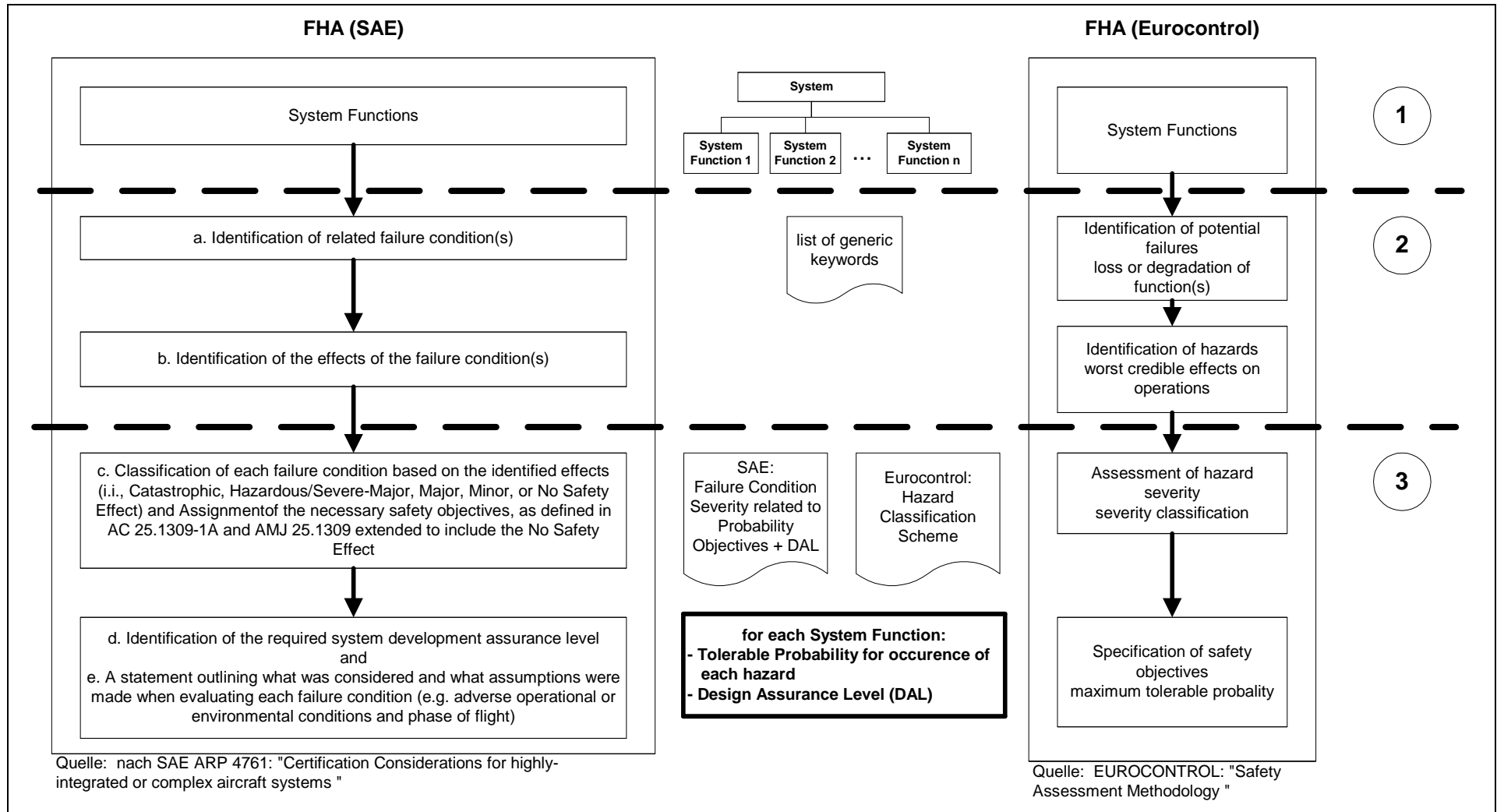


Bild 3-6: Gegenüberstellung von FHA (SAE) und FHA (EUROCONTROL)

3.3.2 Vorgehensweise FHA

In Bild 3-6 sind Functional Hazard Assessment (SAE) und Functional Hazard Analysis (EUROCONTROL) gegenübergestellt. Da Bedeutung und Aufgaben sowohl des Functional Hazard Assessment als auch der Functional Hazard Analysis sowie das jeweilige Vorgehen zur Ableitung der Sicherheitsanforderungen identisch sind, wird im weiteren stellvertretend für beide Prozesse die Bezeichnung „FHA“ und das Vorgehen nach Bild 3-7 in folgenden Hauptschritten verwendet:

1. Definition des Systems und der Systemfunktionen (Aufgaben, funktionales Lastenheft)

Zur Definition des Systems gehört die Beschreibung des Systems einschließlich der Grenzen zu seiner Umgebung. Grundlage für die Entwicklung des (neuen) Systems sind die funktionalen Anforderungen an das System, d.h. welche Aufgaben (betriebliche Vorgaben) soll es unter welchen Umweltbedingungen (z.B. Witterung) erfüllen [SAE 4754] [EC2000]. Die Systembeschreibung ist die Grundlage der Betrachtung der Funktionen [EC2001]. Die Beschreibung der Funktionen muss so gewählt werden, dass die Analyse von Funktionsausfällen möglich ist [PORT2000].

2. Bestimmung der Ausfallarten der Systemfunktionen und Abschätzung der Folgen

Für jede Systemfunktion und für Kombinationen von Systemfunktionen werden die möglichen Ausfallarten analysiert. Zur Identifikation von möglichen Ausfallarten bietet sich eine Liste mit generell möglichen Ausfallarten (z.B. Tabelle 3-1) von Funktionen und Komponenten an. Dabei muss nicht immer jede Ausfallart zu jeder Funktion oder Komponente passen [SAE 4754] [EC2000].

Error of input	Error of output
Failure to start	Misdirection of data
Failure to stop	Delayed operation
Failure to switch	Inadvertent operation
Loss or unavailability of input	Intermittent or erratic operation
Loss or unavailability of output	Premature operation
Partial loss	Out of sequence
Corruption of data	Erroneous updating
Misunderstood	Misheard
Used beyond intent	Inconsistent information
Modified operation	

Die Liste der generischen Ausfallarten soll dazu dienen, bei der Identifikation von Ausfallarten von Funktionen und Komponenten eine nahezu vollständige Liste der möglichen Ausfälle zu erhalten. Je nach Anwendung und Funktionen muss die generische Liste verfeinert werden. Nach der Ermittlung der Ausfallarten werden die Auswirkungen (potentiell gefährliche Zustände, Unfälle, Personenschäden, Sachschäden) der Ausfälle auf den Betrieb des Systems selbst sowie auf dessen Umwelt qualitativ abgeschätzt (z.B. Auswirkung eines Triebwerksausfalls auf das Flugzeug, Auswirkung eines Radargerätes der Flugsicherung auf den Flugbetrieb im betreuten Sektor). Bei der Abschätzung der Folgen sind zur Berücksichtigung betrieblicher Erfahrungen unbedingt Fachexperten (z.B. Piloten, Lotsen) einzubeziehen [PORT2000].

3. Bewertung der Folgen und Festlegung von Sicherheitsanforderungen sowie der Methodik zur Implementierung der Systemfunktionen

Mittels einer anwendungsspezifischen Risikoakzeptanztabelle (z.B. Tabelle 3-2 für das System „großes Verkehrsflugzeug“) werden die Sicherheitsanforderungen aus der Klassifizierung der Folgen eines Funktionsausfalls abgeleitet. Als Ergebnis liefert FHA die tolerierte Wahrscheinlichkeit für das Auftreten jeder der identifizierten Ausfallarten der Funktion. Für die Abschätzung der Folgen sollen die schlimmsten glaubhaften Folgen („most credible effects“ [EC2000]) angenommen werden. Häufig werden die Funktionsausfälle zu unterschiedlichen Folgen führen können [EC2000] [SAE 4754]. Die Bewertung der Folgen sollte durch erfahrene Ingenieure (Sicherheitsexperten) durchgeführt werden [PORT2000]. Für die Sicherheitsanforderung an die Funktion sowie für die methodischen Vorgaben zur Entwicklung und Implementierung der Funktion und für den Nachweis der Erfüllung der Sicherheitsanforderung sind die schlimmsten der für die jeweiligen Funktionsausfälle ermittelten Folgen maßgebend.

Die FHA ist ein Teilprozess des den Systementwicklungsprozess begleitenden Sicherheitsprozesses. Sie wird typischerweise zu Beginn der Systementwicklung (eines neuen Systems) auf Systemebene das erste Mal ausgeführt. Bei der Modifikation bestehender Systeme kann sie zur Beurteilung der funktionalen Veränderungen eingesetzt werden [EC2000] [SAE 4754]. Dabei hängt die Tiefe der Analyse von der Komplexität des Systems sowie von der Klassifizierung der Ausfallfolgen ab [SAE 4754] [TRE2000].

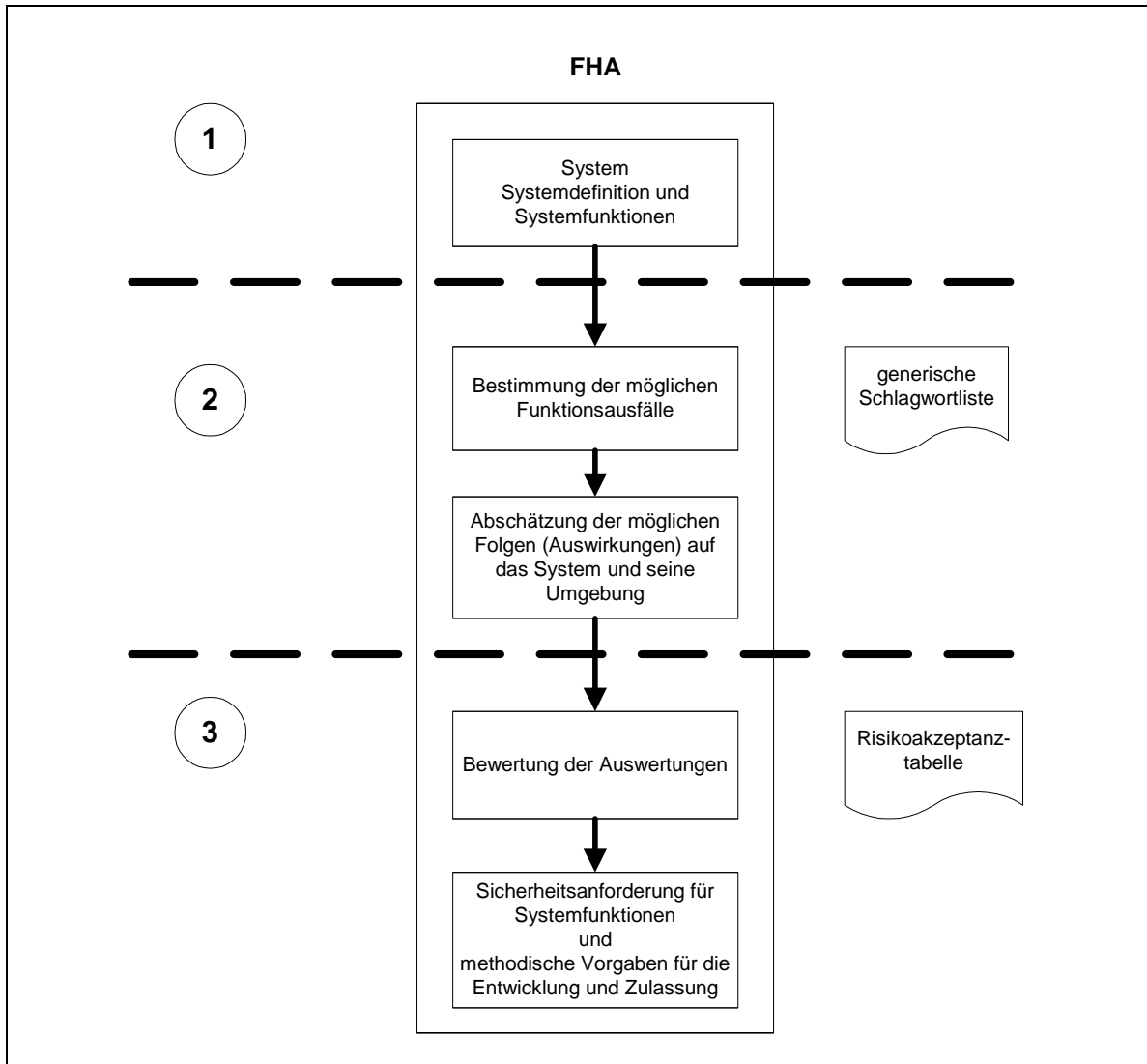


Bild 3-7: Ablauf der FHA

In Tabelle 3-2 ist die Zuordnung der „Failure Condition Severity“ zu tolerierten Ausfallaufretenswahrscheinlichkeiten für große Verkehrsflugzeuge dargestellt. Diese Risikoakzeptanztabelle ist international (FAA, JAA) abgestimmt und für die Entwicklung großer Verkehrsflugzeuge (einschl. Bordgerät) bindend. Sie ist in dieser Form auch nur für das System „großes Verkehrsflugzeug“ gültig.

In der Tabelle sind keine absoluten Schadensbeschreibungen enthalten, sondern Zustände und Situationen, die potentiell zu Unfällen oder Schäden führen können. Aus persönlichen Gesprächen am Rande von Fachveranstaltungen [SAG2002] [Anlage] ging hervor, dass für die Erstellung dieser Tabelle umfangreiche Untersuchungen, Analysen sowie ingenieurmäßige Beurteilungen der möglichen Schäden nötig waren und der Abstimmungs- und Einigungsprozess sich über mehrere Jahre erstreckte.

Tabelle 3-2: Failure Condition Severity as Related to Probability Objectives and Assurance Levels							
Quelle: [SAE 4761]							
Probability (Quantitative)	Per flight hour						
	1.0	1.0E-3	1.0E-5	1.0E-7	1.0E-9		
Probability (Descriptive)	FAA	Probable		Improbable		Extremely Improbable	
	JAA	Frequent	Reasonably Probable	Remote	Extremely Remote	Extremely Improbable	
Failure Condition Severity Classification	FAA	Minor		Major	Severe Major	Catastrophic	
	JAA	Minor		Major	Hazardous	Catastrophic	
Failure Condition Effect	FAA & JAA	<ul style="list-style-type: none"> - slight reduction in safety margins - slight increase in crew workload - some inconvenience to occupants 		<ul style="list-style-type: none"> - significant reduction in safety margins or functional capability - significant increase in crew workload or in conditions impairing crew efficiency - some discomfort to occupants 		<ul style="list-style-type: none"> - large reduction in safety margins or functional capability - higher workload or physical distress such that the crew could not be relied upon to perform tasks accurately or completely - adverse effects upon occupants 	<ul style="list-style-type: none"> - all failure conditions which prevent continued safe flight and landing
Development Assurance Level	ARP 4754	Level D		Level C	Level B	Level A	

Note A “No Safety Effect” Development Assurance Level E exists which may span any probability range

Die SAE legte der Tabelle 3-2 die zwischen FAA und JAA harmonisierte Risikoakzeptanztabelle aus [AMJ 25.1309] zugrunde und erweiterte diese um eine Klasse „No Safety Affect“ (DAL E), für die keine Sicherheitsanforderungen gestellt werden. Das Konzept des Development Assurance Level (DAL) ist vergleichbar mit dem Konzept des Safety Integrity Level (SIL).

Die Tabelle 3-3 von EUROCONTROL zur Klassifizierung der Ausfallfolgen entspricht, bezogen auf die Klassifizierungsstufen, der Tabelle 3-2, wurde aber inhaltlich an das System „Flugsicherung“ angepaßt. Die Klasse 1 (Severity Class) entspricht dem DAL A aus Tabelle 3-3. Die Entsprechung der anderen Klassen und DALs ist analog.

Tabelle 3-3: Hazard Classification Scheme					
Quelle: [EC2000]					
Severity Class	1 [Most Severe]	2	3	4	5 [Least Severe]
Effect on Operations	Complete loss of safety margins	Large reduction in safety margins	Major reduction in safety margins	Slight reduction in safety margins	No effect on safety
Examples include:	<p>A hazard that results in accidents (including one or more catastrophic accidents, one or more mid-air collisions or one or more collisions on the ground between two aircraft.)</p> <p>A hazard that results in a complete loss of separation from another aircraft, terrain, or obstacles.</p> <p>A hazard that results in a total loss of flight control.</p> <p>No independent source of recovery mechanism, such as surveillance or ATC and/or flight crew procedures can reasonably be expected to prevent the accident(s).</p>	<p>A hazard that results in serious incidents.</p> <p>A hazard that causes (a) large reduction in separations (e.g., higher than half the separation minima), without crew or ATC fully controlling the situation or able to recover from the situation.</p> <p>A hazard that causes one or more aircraft to deviate from their intended clearance, and</p> <p>Abrupt collision or terrain avoidance manoeuvres are required to avoid a catastrophic accident (or when an avoidance action would be appropriate).</p>	<p>A hazard that results in major incidents.</p> <p>A hazard that causes (a) large (e.g., higher than half the separation minima) reduction in separations with crew or ATC controlling the situation and able to recover from the situation.</p> <p>Or</p> <p>A hazard that causes (a) major (e.g., lower than half the separation minima) reduction in separation without crew or ATC fully controlling the situation, hence jeopardising the ability to recover from the situation (without the use of collision or terrain.</p>	<p>A hazard that results in significant incidents.</p> <p>A hazard that has no direct impact on safety but may indirectly impact safety by increasing the workload of the air traffic controller or airplane flight crew, or slightly degrading the functional capability of the enabling CNS system.</p> <p>A hazard that causes (a) major (e.g., lower than half the separation minima) reduction in separations with crew or ATC controlling the situation and fully able to recover from the situation.</p>	<p>An event that results in no hazardous condition i.e. results in no direct or indirect impact to the operations.</p>

Die Tabelle 3-3 enthält keine Angaben über die tolerierten Wahrscheinlichkeiten des Auftretens von Ausfallfolgen bestimmter Schwere.

Bei gegebener Schwere der Ausfallfolge lässt sich mit Hilfe Tabelle 3-4 der tolerierte Wahrscheinlichkeitsbereich des Ausfalls qualitativ ermitteln. Für die Flugsicherung gibt es bisher eine quantitativ abgestimmte Risikoakzeptanz nur für die Klasse 1. Diese liegt bei $1,55 \times 10^{-8}$ pro Flugstunde [ESARR4].

Tabelle 3-4: Risk Classification Scheme

Quelle: [EC2000]

		SAFETY OBJECTIVES			
		PROBABLE	REMOTE	EXTREMELY REMOTE	EXTREMELY IMPROBABLE
HAZARD SEVERITY	1				
	2				
	3				
	4	UNACCEPTABLE			
	5	ACCEPTABLE/ TOLERABLE			

Nachdem die FHA auf oberster Ebene (aircraft-level) durchgeführt und die Sicherheitsanforderungen für die Flugzeugfunktionen ermittelt wurden, kann die FHA eine Betrachtungsebene tiefer auf (Teil)Systemebene angewendet werden. Sie dient nunmehr als Hilfsmittel bei der Verteilung der Funktionen auf bestimmte Architekturelemente. Vor der FHA ist bei neuen Systemen die Architektur noch nicht festgelegt. In der Praxis finden der Systementwicklungsprozess und der Systembewertungsprozess häufig parallel statt und einige Funktionen können schon bestimmten Systemelementen zugewiesen sein, insbesondere bei Systemmodifikationen. Die FHA kann grundsätzlich auf beliebiger Betrachtungsebene durchgeführt werden.

3.3.3 Erfahrungen und Probleme mit FHA

In [SAE 4754] [EC2000] [PORT2000] [TRE2000] werden Hinweise zur Durchführung von FHA gegeben sowie häufig auftretende Probleme und bereits gemachte Erfahrungen beschrieben. Dies soll dazu dienen, Probleme und Fehler, die bei einer funktionalen Betrachtung mit großer Wahrscheinlichkeit auftreten, von Beginn an zu vermeiden, um Zeit und Geld zu sparen. Unter anderem sind folgende Hinweise zu FHA enthalten:

- Systemdefinition

Die Ableitung der Sicherheit einer Funktion stellt ein nicht triviales Problem dar, da eine funktionale Betrachtungsweise ein erhebliches Maß an Abstraktionsvermögen und Systemwissen verlangt.

Häufig bereitet eine funktionale Betrachtung anfangs Schwierigkeiten, da, vor allem bei bestehenden Systemarchitekturen, die Gefahr besteht, Funktionsausfälle von Funktionen, die

schon bestimmten Systemelementen zugewiesen sind, als Ausfälle des Systemelementes zu betrachten [EC2000] [STO1996]. Dessen Ausfälle sind jedoch nur eine Teilmenge der Funktionsausfälle, da z.B. Bedienungsfehler zwar einen Ausfall der zu erfüllenden Funktion hervorrufen können, jedoch nicht zwangsläufig einen Ausfall des Systemelementes. Die Zuordnung und Beschreibung von Funktionen wird zunehmend schwieriger, je weiter man sich von der Grenze System/Umwelt entfernt [SAE 4754], [PORT2000] [STO1996]. Eine brauchbare Systemdefinition erfordert demnach viel Expertise, ingenieurmäßiges Verständnis und viel Abstimmungsarbeit zwischen den Beteiligten [TRE2000].

- Ermittlung der Funktionsausfälle und Folgenabschätzung

In diesen Teil von FHA fließt umfangreiches Fachexpertenwissen ein. Dazu gehören u.a. Erfahrungen und Wissen von Entwicklungsingenieuren sowie von Fachexperten des Betriebes (z.B. Fluglotsen) [TRE2000]. Um dieses Wissen abzugreifen, werden FHA-Sitzungen mit jeweils diesen Fachexperten durchgeführt [EC2000]. Zu einem guten Erfolg dieser Sitzungen trägt eine gründliche Vorbereitung genauso bei wie die zielführende Moderation. Bezüglich der Folgenbewertung wird in [SAE 4754] [EC2000] [TRE2000] darauf hingewiesen, dass dazu ingenieurmäßiger Verstand und Urteilungsvermögen zwingend notwendig sind. Die Identifizierung und Bewertung von Ausfallfolgen ist besonders für Systeme schwierig, die mehrere Ebenen von der System/Umweltgrenze entfernt sind [STO1996]. Die Planung und Evaluation der FHA sind von Art und Umfang des zu bewertenden Systems abhängig [EC2000] [TRE2000]. Der Aufwand für FHA nimmt mit steigender Komplexität des Systems zu (z.B. Vollständigkeit der identifizierten Ausfälle und Folgen). Die FHA eignet sich besonders gut zur Analyse unabhängiger Funktionen [KELLY].

- Bewertung der Ausfallfolgen

Eine Beurteilung der Ausfallfolgen hängt häufig vom Standpunkt (oder der persönlichen Sicht) des Beurteilenden (Entwickler, Zulassender, Gutachter) ab und ist somit subjektiv geprägt [STO1996]. Deshalb ist eine einheitliche Festlegung zur Bewertung der Ausfallfolgen beim Einsatz des Systems zu treffen.

Häufig ist es so, dass anfangs alle identifizierten Ausfallfolgen katastrophal sind. Meist ist die Ursache dafür eine unzureichende Systemdefinition oder eine ungeeignete Funktionsaufteilung bzw. -beschreibung [EC2000].

- Terminologie

Besonderes Augenmerk ist auf die Verwendung einer einheitlichen Terminologie zu legen. Unterschiedliches Verständnis von Termen oder Sachverhalten ist in vielen Fällen Ursache für Missverständnisse und zeitraubende Diskussionen. Ein besonders großes Missverständnispotential haben die Begriffe „System“ und „Funktion“ [SAE 4754]. Für diese beiden Begriffe gibt es keine einheitliche Definition.

4 Anwendung der FHA an ETCS Level 2

4.1 Vorgehen

Zur Ableitung von Sicherheitsanforderungen wird die FHA in den 3 Schritten nach Bild 3-6 angewendet. Ziel dieser Untersuchung ist es, festzustellen, ob die Methode FHA eine für ETCS Level 2 geeignete Methode zur Ableitung von Sicherheitsanforderungen ist.

Im Rahmen der versuchsweisen Anwendung der FHA zur Bestimmung von Sicherheitsanforderungen ist die Anwendung auf eine Funktion des ETCS Level 2 beschränkt.

4.2 Schritt 1: Systemdefinition und Funktionsaufteilung

Der Wahl der Betrachtungsebene (z.B. aircraft-level, System-level) kommt eine entscheidende Bedeutung bei der Beurteilung eines Systems spielt. Für diese Wahl gibt es keine Vorschrift, vielmehr ist sie abhängig vom Standpunkt des Betrachters. Deshalb wird für diese Arbeit die kausale Verknüpfung der Betrachtungsebenen entsprechend Bild 4-1 definiert.

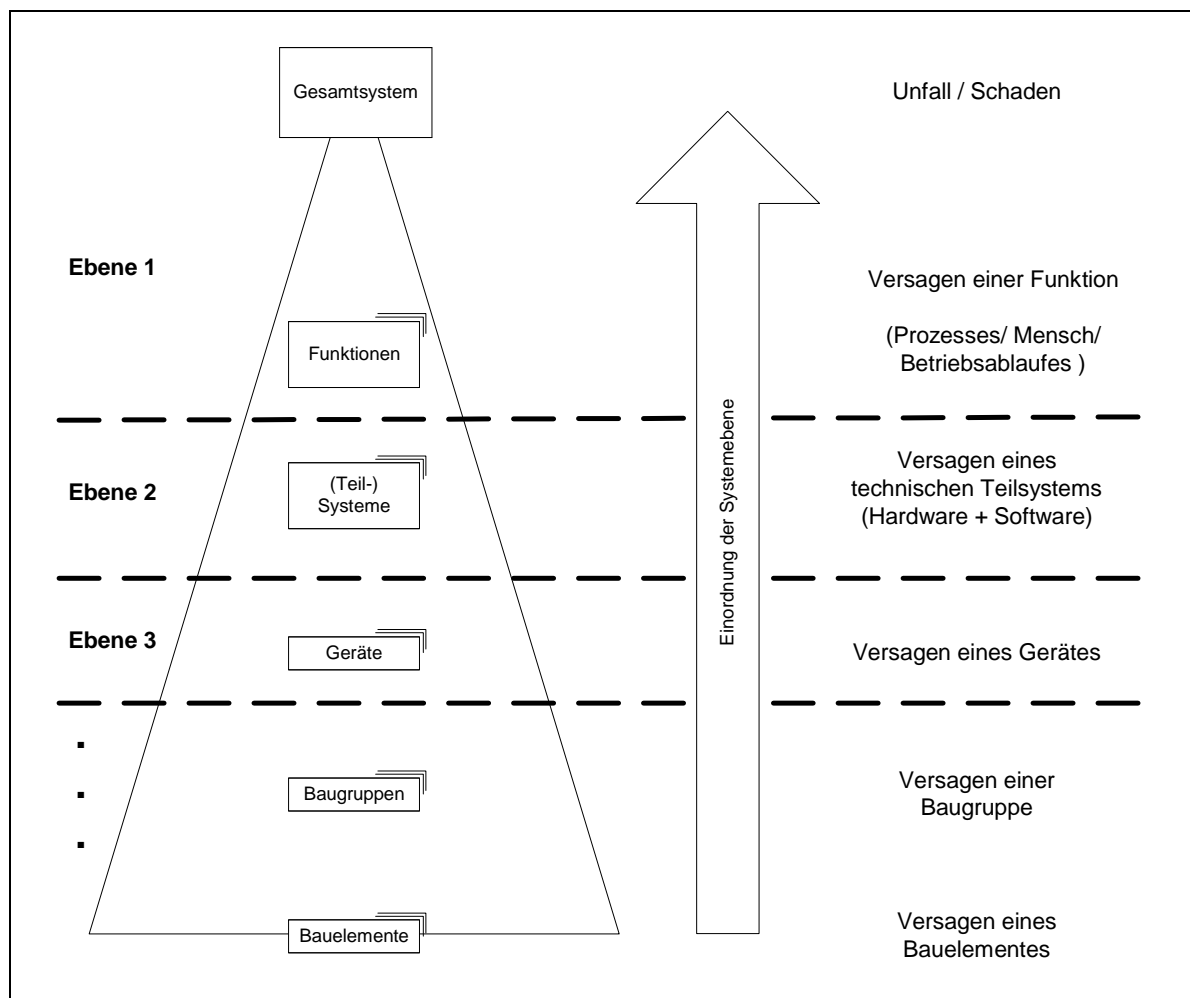


Bild 4-1: Festlegung der Betrachtungsebene

Das Gesamtsystem (Ebene 1, z.B. Flugzeug) hat bestimmte Funktionen (z.B. Schubsteuerung). Diese sind verschiedenen Teilsystemen zugeordnet (Ebene 2, z.B. Antriebssystem). Teilsysteme bestehen aus (technischen) Geräten (z.B. Triebwerk), die in Zusammenarbeit mit dem Menschen (z.B. Steuern der Triebwerksleistung) der Erfüllung der Gesamtsystemfunktionen dienen. Ein Gerät besteht aus Baugruppen (z.B. Propeller) und Bauelementen (z.B. Propellerblatt). Jedes Element (Technik und Mensch) des Gesamtsystems kann ausfallen und dabei unterschiedliche Auswirkungen hervorrufen.

Die Beurteilung der Auswirkungen auf das Gesamtsystem zur Beurteilung der erforderlichen Sicherheit wird dabei mit zunehmender Betrachtungstiefe schwieriger [PORT2000].

Bei der Einordnung der Funktionsaufteilung des ERTMS/ETCS aus der Aufgabenstellung ergibt sich die in Bild 4-2 dargestellte Zuordnung von Betrachtungsebenen. ERTMS/ETCS stellt dort das Gesamtsystem (Ebene 1 = oberste Systemebene) dar.

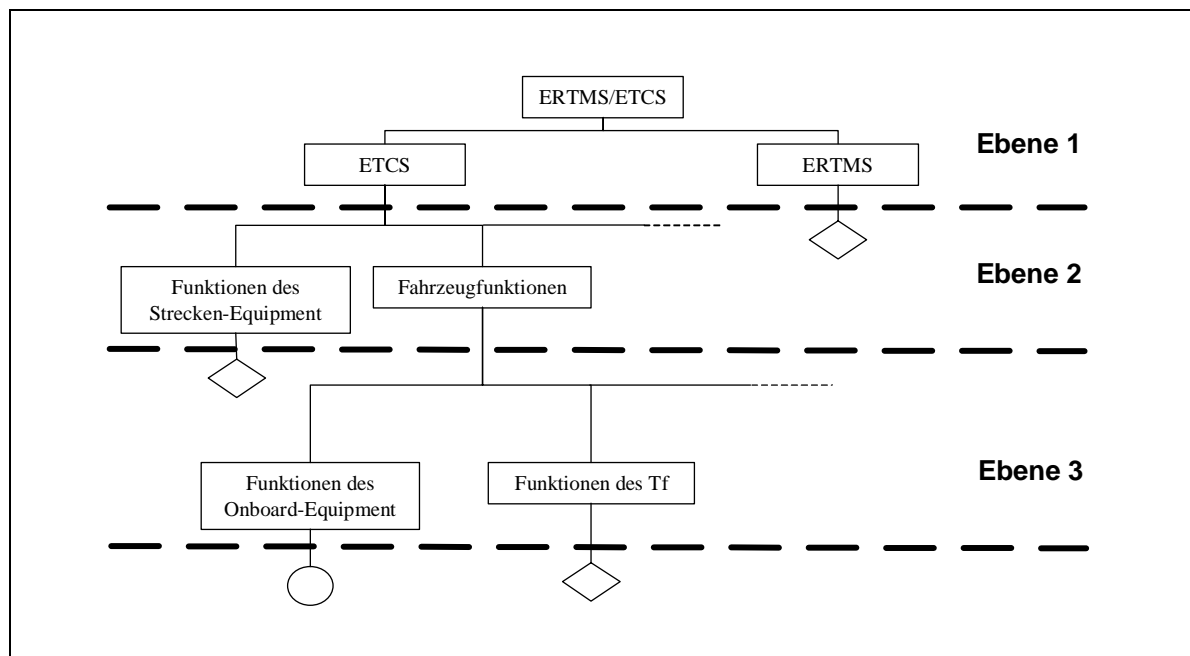


Bild 4-2: Betrachtungsebenen der Aufgabenstellung

Für die Ermittlung der erforderlichen Sicherheit für ETCS ist dessen Einordnung in den Gesamtkontext „Bahnbetrieb“ entscheidend. Bei einer Trennung zwischen Fahrzeug und Strecke (analog Flugzeug und Flugsicherung) ergibt sich eine Einteilung der Betrachtungsebenen wie in Bild 4-3. Die in Ebene 2 dargestellten (Teilsystem-)Funktionen des ETCS-Fahrzeuggerätes sind [UNISIG 26] entnommen. Dort gibt es keine Definition des Begriffes „Cab Signalling“ (Führerraumsignalisierung). In [W5] ist Führerraumsignalisierung definiert als „...Anzeige der Signalbegriffe auf einem Display im Führerraum des Triebfahrzeugs.“ Neben den Signalbegriffen sollen dem Tf bei ETCS noch weitere Informationen im Führerraum angezeigt werden. Diese sind

dem laufenden Text von [UNISIG 26] [UNISIG 30] [UNISIG 31] entnommen und in Bild 4-3 der Funktion 6 zugeordnet worden.

Für die Anwendung des FHA in dieser Arbeit wird bewusst das Anzeigen der aktuellen Geschwindigkeit (actual speed) herausgegriffen und im weiteren als Funktion „Anzeigen der aktuellen Geschwindigkeit“ bezeichnet. Die Funktionsbeschreibung soll lauten: „Der Triebfahrzeugführer soll zu jedem Zeitpunkt die aktuelle Geschwindigkeit seines Fahrzeuges (Zuges) kennen“. In dieser Beschreibung der Funktion ist keine Vorgabe zur Implementierung enthalten. Es ist zu vermuten, dass diese Funktion nicht die höchsten Sicherheitsanforderungen erfüllen muss.

Die Funktionen „Antriebssteuerung“, „Bremssteuerung“ und „Spurführung“ des Zuges in der Ebene 1 (Bild 4-3) seien nur zur Illustration genannt und erheben keinen Anspruch auf Vollständigkeit und Korrektheit. Sie werden hier nicht weiter betrachtet.

Wie in Bild 3-4 ersichtlich ist, wird die FHA nacheinander auf den Ebenen „aircraft-level“ und „System-level“ durchgeführt. Analog dazu ist die Anwendung an ETCS auf den Ebenen „Zugfunktionen (Ebene 1)“ und „(Teil)Systemfunktionen (Ebene 2)“ durchzuführen.

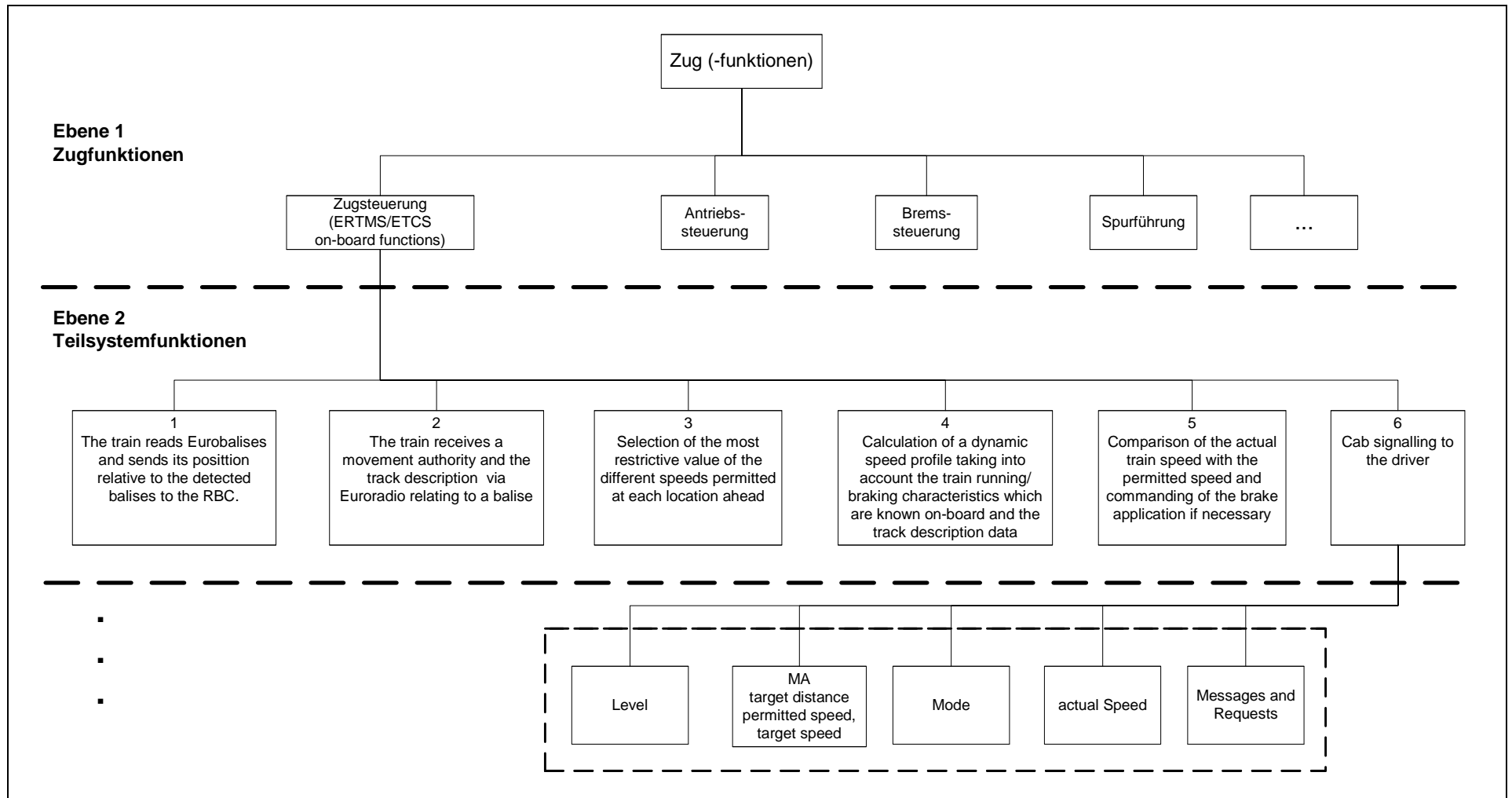


Bild 4-3: Betrachtungsebenen für ETCS-Funktionen

4.2.1 Betriebliche Randbedingungen

Für das Fahren unter der Sicherheitsverantwortung von ETCS gibt es derzeit keine einheitliche europäische Vorschrift. Für die Bearbeitung der Aufgabenstellung wird an dieser Stelle folgendes vereinfachte betriebliche Umfeld definiert:

1. Die Ausrüstung von Strecke und Fahrzeug ist vollständig in Level 2 realisiert, d.h. es liegt ein sortenreines Netz vor.
2. Die Länge des Fahrzeuges (Lok, Zug) wird hier vernachlässigt. In einem Zug befindet sich genau ein arbeitendes Triebfahrzeug.
3. Die Bewegung von Fahrzeugen erfolgt in der Beispielumgebung nur vorwärts, d.h. der Tf befindet sich immer im Führerraum der führenden Spitze des Zuges.
4. Dem Triebfahrzeugführer werden die zum Bedienen des Zuges notwendigen Informationen im Führerraum angezeigt. Eine wichtige Information ist die aktuelle Geschwindigkeit. Der Tf vergleicht die aktuelle Geschwindigkeit mit der zulässigen Geschwindigkeit und setzt das Ergebnis dieses Vergleiches in manuelle Steuerhandlungen (Antriebsregelung, Bremsregelung) um, d.h. es findet kein automatisches Fahren des Zuges statt. Das Fahren ohne Information über die aktuelle Geschwindigkeit ist verboten.
5. Zum Schutz des Fahrzeuges vor Überschreitung der zulässigen Geschwindigkeit wird die Einhaltung der zulässigen Geschwindigkeit überwacht und bei Überschreitung eine Zwangsbremse eingeleitet.

4.2.2 Überwachungsphasen

Gemäß den Forderungen aus [FRS99] nach Möglichkeiten der vollständigen (Full Supervision) bzw. der teilweisen (Partial Supervision) Überwachung eines Fahrzeuges unter der Sicherheitsverantwortung des ETCS sowie der geforderten Möglichkeit nach Fahren ohne Überwachung wurden in UNISIG Class 1 16 verschiedene Modi definiert. Ein Überblick über diese Modi (Bezeichnung, Kurzbeschreibung, Aufteilung der Sicherheitsverantwortung) befindet sich in Tabelle 4-1. Zu jedem Modus ist die Sicherheitsverantwortung für Tf und ETCS beschrieben. In dieser Tabelle wurden die verbalen Beschreibungen [UNISIG 26] zusammengefasst, auch wenn die Sicherheitsverantwortung des ETCS unterschiedliche Funktionen betrifft. So kommt es z.B. dazu, dass das ETCS-Fahrzeuggerät im ausgeschalteten Zustand (No Power) trotzdem Sicherheitsverantwortung hat. Diese bezieht sich in diesem Modus nur auf die Ansteuerung der Notbremse („The ERTMS/ETCS on-board equipment has no responsibility in this mode, except commanding the emergency break.“)

Tabelle 4-1: Modi des ETCS nach [UNISIG 26]				
Modus	Bezeichnung	Kurzbeschreibung	Sicherheitsverantwortung	
			ETCS	Tf
FS	Full Supervision	Vollüberwachung auf dynamischer Überwachungskurve bei Vorhandensein aller notwendigen Daten, automatischer Modus	ja	ja
IS	Isolation	ETCS-OBU vollständig vom restlichen Fahrzeug (einschl. Tf und Bremse) getrennt	nein	ja
NL	Non Leading	(elektrisch) nicht gekuppelte Doppeltraktion, d.h. Fz ist nicht führend, aber mit Tf besetzt, Tf ist verantwortlich für Auswahl des Modus, kein Schutz vor Missbrauch des Modus möglich	nein	ja
NP	No Power	ETCS-OBU ist ausgeschaltet	ja	nicht relevant
OS	On Sight	Fahren auf Sicht (Modus nur auf Anweisung vom Streckengerät)	ja	ja
PT	Post Trip	Automatischer Modus nach Bestätigung des Modus TR durch Tf (nur für Rücksetzen des Fahrzeugs)	ja	ja
RV	Reversing	Kopf- und Wendefahrt, Tf befindet sich nicht in der führenden Spitze des Fahrzeuges	ja	ja
SB	Stand By	Automatischer Modus beim Einschalten, Selbsttest	ja	nein
SE	STM European	ETCS-ausgerüstetes Fahrzeug auf Strecke mit nationalem Zugsicherungssystem	ja	ja
SF	System Failure	Bei erkanntem sicherheitskritischen Systemausfall, Zwangsbremmung bis Stillstand	ja	nein
SH	Shunting	Rangierbewegungen	ja	ja
SL	Sleeping	für ferngesteuerte Triebfahrzeuge	nein	nicht relevant
SN	STM National	ETCS-ausgerüstetes Fahrzeug auf Strecke mit nationalem Zugsicherungssystem	ja	ja
SR	Staff Responsible	Fahren auf Befehl (nationale Unterschiede), wenn das ETCS-OBU keine Fahrwegdaten hat	ja	ja
TR	Trip	Zwangsbremmung bis zum Stillstand	ja	nein
UN	Unfitted	ETCS-ausgerüstetes Fahrzeug auf nicht ausgerüsteter Strecke und ohne nationales Zugsicherungssystem	ja	ja

Die Vielzahl der Modi ist Ausdruck der verschiedenen von den Bahnen gewünschten betrieblichen Szenarien des ETCS.

Da alle Modi unterschiedliche betriebliche Situationen darstellen (jedoch ohne, dass diese genau beschrieben sind) müsste die FHA für alle Modi einzeln durchgeführt werden. Für die Untersuchung der Methode werden nur die für den definierten Beispielbetrieb im Level 2 relevanten Modi herausgearbeitet. Dazu wurde der in Bild 4-4 dargestellte Entscheidungsbaum entwickelt.

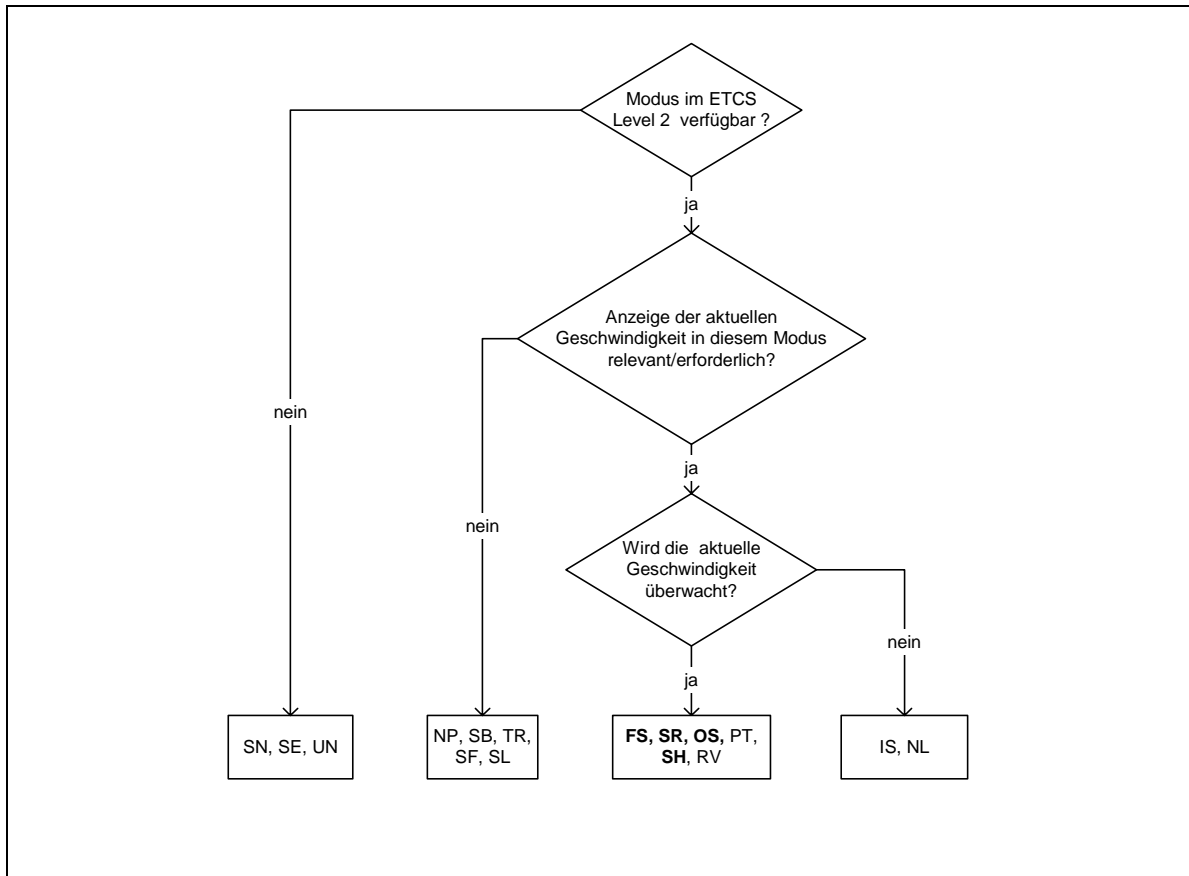


Bild 4-4: Entscheidungsbaum zur Auswahl der zu untersuchenden Modi

Anhand der Beschreibung in [UNISIG 26] werden zuerst die Modi ausgeschieden, die im ETCS Level 2 nicht zur Verfügung stehen. Im nächsten Schritt entfallen die Modi, in denen das „Anzeigen der aktuellen Geschwindigkeit“ nicht relevant (Zwangsmodi ohne Verantwortung des Tf für die Geschwindigkeit: SF, TR, NP) bzw. nicht möglich (Modi für Fahrzeug im Stand: SB) ist. Danach verbleiben die Modi, in denen der Tf die Geschwindigkeit des Fahrzeugs anhand der angezeigten aktuellen Geschwindigkeit regelt. Die Modi RV, PT und NL entfallen, weil sie für den definierten Beispielbetrieb nicht relevant sind. Der Modus IS findet keine Beachtung, da ETCS in diesem Modus per Definition keine Sicherheitsverantwortung hat.

Die am Ende des Entscheidungsbaumes fett hervorgehobenen Modi FS, SR, OS und SH wurden dabei als relevant für die Ableitung der Sicherheitsanforderung der Funktion „Anzeigen der aktuellen Geschwindigkeit“ im definierten Beispielbetrieb herausgefunden.

In diesen Modi gibt es unterschiedliche Überwachungsarten. Entweder erfolgt die Überwachung der Geschwindigkeit anhand eines dynamischen Geschwindigkeitsprofils (Dynamic Speed Monitoring DSM) oder es wird eine Höchstgeschwindigkeit (Ceiling Speed) überwacht (Ceiling Speed Monitoring CSM) (Bild 4-5).

Beim DSM wird der Zug entsprechend seiner Bremscharakteristik entlang einer berechneten

Geschwindigkeitskurve überwacht. Beim Überschreiten dieser Geschwindigkeitskurve wird der Zug im schlimmsten Fall auf einer Zwangsbremskurve (Emergency Break Intervention EBI) am Ende der Movement Authority (EoA) zum Stehen gebracht. Für die Modi FS, OS und SR gibt es nur die Überwachungsart DSM.

Beim CSM wird eine konstante Höchstgeschwindigkeit überwacht. Beim Überschreiten dieser Höchstgeschwindigkeit (CS) wird der Zug ebenfalls auf einer Zwangsbremskurve (EBI) gebremst. Im schlimmsten Fall beginnt somit die Zwangsbremskurve am Ende der Movement Authority (EoA), wenn der Zug an diesem Punkt (wo er eigentlich zum Stand gekommen sein müsste) die überwachte Höchstgeschwindigkeit erreicht. Dann beginnt die EBI an der EoA und endet an der Supervised Location (SL). Die Überwachungsart CSM gibt es nur im Modus SH. Die größte mögliche Geschwindigkeit, mit welcher der Zug die EoA überfährt, beträgt somit 30 km/h.

Fasst man diese Möglichkeiten zusammen, so verbleiben die Überwachungsphasen:

1. Fahrt mit $v > 0$ km/h: Dynamische Geschwindigkeitsüberwachung (DSM)
2. Fahrt mit $v \leq 30$ km/h: Statische Geschwindigkeitsüberwachung (CSM),

in denen die Funktion „Anzeigen der aktuellen Geschwindigkeit“ benötigt wird.

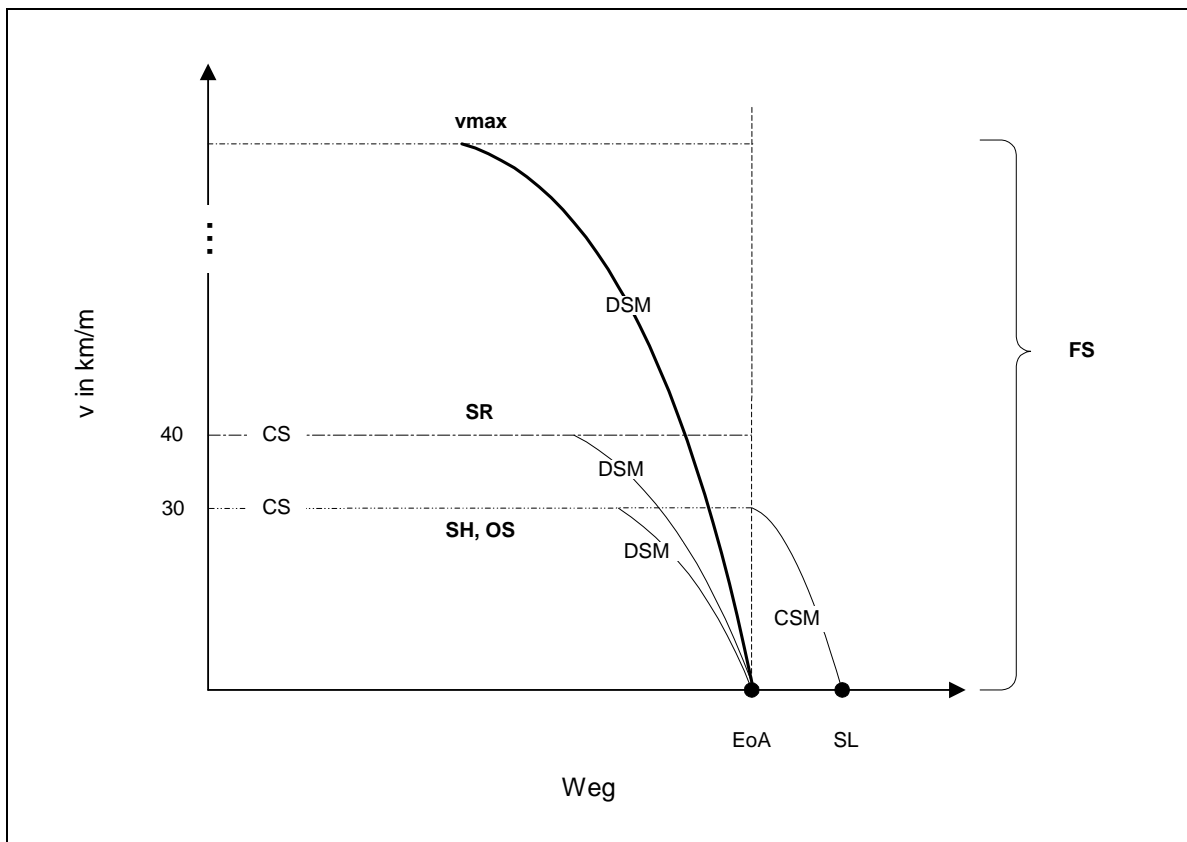


Bild 4-5: Überwachungsarten der Modi

Quelle: nach [UNISIG 26]

4.3 Schritt 2: Ausfallarten der Funktion und Abschätzung der Folgen

4.3.1 Ausfallarten

Unter Zuhilfenahme der Tabelle 3-1 wurden für die ausgewählte Funktion „Anzeigen der aktuellen Geschwindigkeit“ die Ausfallarten

Ausfallart 1: aktuelle Geschwindigkeit wird nicht angezeigt (oder ist nicht erkennbar)
(Loss or unavailability of output)

Ausfallart 2: aktuelle Geschwindigkeit wird falsch angezeigt
(Error of output)

ermittelt. Bei Ausfallart 1 kann davon ausgegangen werden, dass das Fehlen der Anzeige der aktuellen Geschwindigkeit in jedem Fall vom Tf bemerkt wird, da dieser die aktuelle Geschwindigkeit als Grundlage für seine Bedienhandlungen zwingend benötigt und somit einen Ausfall der Funktion erkennt.

Bei Ausfallart 2 ist die Beschreibung für eine Betrachtung der Folgen nicht ausreichend. Die Anzeige kann in zwei Richtungen falsch sein, so dass dieser Ausfall in die Ausfallarten 2a und 2b unterschieden werden muss.

Ausfall 2a: aktuelle Geschwindigkeit wird zu hoch angezeigt

Ausfall 2b: aktuelle Geschwindigkeit wird zu niedrig angezeigt

Diese beiden Ausfallarten können durchaus unerkannt eintreten. Es hängt zum einen von der Größe der Abweichung der angezeigten von der tatsächlich gefahrenen Geschwindigkeit, zum anderen von der Erfahrung des Tf ab, ob dieser bemerkt, dass ein andere als die tatsächlich gefahrene Geschwindigkeit angezeigt wird.

4.3.2 Folgenabschätzung

Die für die definierte Beispielumgebung ermittelten Folgen sind in Tabelle 4-2 zusammengefasst. Das betriebliche Beispielumfeld und die Systemdefinition aus Abschnitt 2.3.1 gestatten eine Abschätzung der möglichen Folgen ohne Verwendung analytischer Mittel (z.B. Ereignisbaumanalyse). Die letzten 3 Spalten der Tabelle 4-2 werden im nächsten Abschnitt erläutert.

Eine Beurteilung der Ausfallfolgen ist nur möglich beim Blick auf das betriebliche Umfeld [FENNER] [EC2000] [EC2001] [SAE 4754]. Die Ausfallfolgen der Funktion „Anzeigen der aktuellen Geschwindigkeit“ wurden unabhängig von Funktionsausfällen anderer Funktionen (z.B. gleichzeitiger Ausfall der Funktion „Überwachen der aktuellen Geschwindigkeit“) ermittelt.

Bei der Abschätzung der Folgen wurde jedoch erkannt, dass es eine Abhängigkeit der Funktionen „Überwachen der aktuellen Geschwindigkeit“ und „Anzeigen der aktuellen Geschwindigkeit“ geben könnte. Die Untersuchung dieser Abhängigkeit ist jedoch nicht Gegenstand der FHA, sondern der Methoden PSSA und SSA im Sicherheitsprozess nach SAE (Bild 3-4).

4.4 Schritt 3: Klassifizierung der Folgen und Ableitung einer Sicherheitsanforderung für die Funktion

In den letzten 3 Spalten der Tabelle 4-2 ist die Bewertung und Klassifizierung der Ausfallfolgen im Beispielumfeld eingetragen. Die Klassifizierung wurde mit Hilfe der Tabelle 3-2 abgeschätzt. Diese ist auf die Belange des Systems „Flugzeug“ zugeschnitten, konnte aber, inhaltlich einigermaßen zutreffend, angewendet werden, weil ein Zug (als ein vom Menschen gesteuertes Objekt) eine größere Nähe zum Flugzeug aufweist als zu einer Zentrale der Flugsicherung.

Für die ausgewählte Funktion wurde unter den definierten Bedingungen eine Ausfallfolge ermittelt, die als nicht sicherheitsrelevant (DAL E) eingestuft werden kann und für die deshalb keine Einschränkungen für eine tolerierte Auftrittswahrscheinlichkeit gemacht werden. Alle anderen Ausfallfolgen wurden qualitativ mit dem Schweregrad (Failure Condition Severity Classification) „Minor“ bewertet.

Für die Ableitung der Sicherheitsanforderung an die Funktion ist die schlimmste Ausfallfolge entscheidend. Die tolerierte Ausfallhäufigkeit der Funktion liegt somit zwischen 10^0 und 10^{-5} „pro Flugstunde“. Die Funktion ist nach dem Development Assurance Level DAL D zu entwickeln.

Die Beschreibungen der Wahrscheinlichkeitsklassen und die zugeordnete quantitativen Sicherheitsanforderungen für den Schweregrad „Minor“ unterscheiden sich zwischen JAA und FAA. Bei FAA wird die gesamte „Häufigkeitsbreite“ ($10^0 - 10^{-5}$) mit „Probable“ bezeichnet. Bei JAA wird dieser Bereich noch einmal unterteilt in „Frequent“ ($<10^0$) und „Reasonably Probable“ ($<10^{-3}$). Diese Unterteilung wirkt sich weder auf die generische Beschreibung der Ausfallauswirkung („Failure Condition Effect“) zur Klassifizierung noch auf die methodischen Vorgaben für die Entwicklung (DAL) aus. Deshalb wurde hier keine weitere Unterscheidung getroffen.

Tabelle 3-3 (EUROCONTROL) konnte aufgrund inhaltlicher Unvereinbarkeit der generischen Beschreibungen für die Klassifizierung der Ausfallfolgen bei der „Flugsicherung“ nicht für die Beurteilung des Systems „Fahrzeug“ verwendet werden. Für die Tabelle 3-3 könnte auf diese Weise eher eine Parallele zu einem Stellwerk oder einer Betriebszentrale gezogen werden als zu einem Zug.

Tabelle 4-2: Zusammenfassung der Ergebnisse der FHA für die Funktion „Anzeigen der aktuellen Geschwindigkeit“						
Ausfallart	Betriebliche Faktoren	Überwachungsphase	Folge/ Auswirkung des Ausfalls	Klassifizierung abgeschätzt nach Tabelle 3-2)		
				Schwere	DAL	Tolerierte Wahrscheinlichkeit des Ausfalls
1	Ausfall besteht bereits vor dem Start und Tf bemerkt beim Anfahren den Ausfall	1 (DSM) 2 (CSM)	Tf bringt das in Bewegung gesetzte Fahrzeug sofort wieder zum Stehen. Die Überwachungsfunktion tritt nicht in Kraft, da das Fahrzeug sich bis zum Erkennen des Ausfalls durch den Tf in jedem Fall unterhalb der zulässigen Geschwindigkeit bewegt.	No safety effect	E	jede
	Ausfall tritt während der Fahrt auf und Tf bemerkt den Ausfall	1 (DSM) 2 (CSM)	Tf bremst das Fahrzeug umgehend bis zum Stillstand ab. Da er keine Anzeige der aktuellen Geschwindigkeit hat, muss er „nach Gefühl“ bremsen.	Minor	D	$1 - 10^{-5}$
2a	viel (merklich) zu hoch	1 (DSM) 2 (CSM)	Tf bemerkt den Fehler und fährt „nach Gefühl“, bei intakter Überwachung liegt die Überwachungsfunktion immer oberhalb der aktuellen Geschwindigkeitskurve, beim Überschreiten der zul. (überwachten) Geschwindigkeit wird die normale (vorgesehene) Zwangsbremskurve eingehalten, Achtung: Unabhängigkeit zur Überwachungsfunktion prüfen!!	Minor	D	$1 - 10^{-5}$
	Wenig (unmerklich) zu hoch	1 (DSM) 2 (CSM)	Tf bemerkt den Fehler nicht: Fahrzeug fährt Verspätung ein, u.U. Betriebliche Behinderungen im nachfolgenden Verkehr	Minor	D	$1 - 10^{-5}$
2b	viel (merklich) zu niedrig	1 (DSM)	Tf bemerkt den Fehler, Betriebliche Regelung muss getroffen sein, deshalb Annahme: Fahren auf Sicht: beim Überschreiten der zul. (überwachten) Geschwindigkeit wird die normale Bremskurve eingehalten, Achtung: Unabhängigkeit zur Überwachungsfunktion prüfen!!	Minor	D	$1 - 10^{-5}$
	Wenig (unmerklich) zu hoch		Tf bemerkt den Fehler nicht: beim Überschreiten der zul. (überwachten) Geschwindigkeit wird die normale Zwangsbremskurve eingehalten, Achtung: Unabhängigkeit zur Überwachungsfunktion prüfen!!	Minor	D	$1 - 10^{-5}$
	viel (merklich) zu niedrig	2 (CSM)	Tf bemerkt den Fehler, Betriebliche Regelung muss getroffen sein, deshalb Annahme: Fahren auf Sicht: beim Überschreiten der zul. (überwachten) Geschwindigkeit wird die normale Bremskurve eingehalten, Achtung: Unabhängigkeit zur Überwachungsfunktion prüfen!!	Minor	D	$1 - 10^{-5}$
	Wenig (unmerklich) zu hoch		Tf bemerkt den Fehler nicht: beim Überschreiten der zul. (überwachten) Geschwindigkeit wird die normale Zwangsbremskurve eingehalten, Achtung: Unabhängigkeit zur Überwachungsfunktion prüfen!!	Minor	D	$1 - 10^{-5}$

5 Diskussion der Ergebnisse

Die versuchsweise Anwendung der FHA an der Funktion „Anzeigen der aktuellen Geschwindigkeit“ ergab eine grundsätzliche Eignung der Methode für die Anwendung in der Eisenbahnsignaltechnik. Die Vorgehensweise zur Ableitung von Sicherheitsanforderungen ist dem Vorgehen nach [EN 50129] ähnlich.

5.1.1 Vorgehensweise zur Ableitung von Sicherheitsanforderungen

Während der Literaturrecherche bei der versuchsweisen Anwendung der FHA an einem Beispiel der Eisenbahnsignaltechnik ergab sich ein Überblick über die aktuellen Ansätze zur Ableitung von Sicherheitsanforderungen für ETCS und die damit verbundenen Probleme.

In Bild 5-1 ist das grundsätzliche Vorgehen nach [EN 50129] zur Ableitung von Sicherheitsanforderungen für Funktionen bei Eisenbahnanwendungen dargestellt, das bisher jedoch bei ETCS nicht konsequent angewendet wurde [SD2002 (1)] [SD2002 (2)]. Es wird für jede Gefährdung bzw. Funktion eine jeweils sehr detaillierte Folgen- und Schadenanalyse erstellt, an deren Ende die Frage nach der Akzeptanz des ermittelten Risikos steht. Im Gegensatz zu einigen erfolgreichen Anwendungen bei der DB AG [SD2002 (6)] [ETR2002] wird die Antwort auf diese Frage im internationalen Kontext erschwert durch die Uneinigkeit zum einen über den Weg zur Ermittlung des Risikos sowie zum anderen über die Akzeptanz von Risiken selbst. Wird ein bestimmtes Risiko akzeptiert, dann war die vor der Durchführung geschätzte THR auf jeden Fall gut genug. Wird das Risiko nicht akzeptiert, so muss das System abgeändert und die Risikoanalyse „neu aufgerollt“ werden.

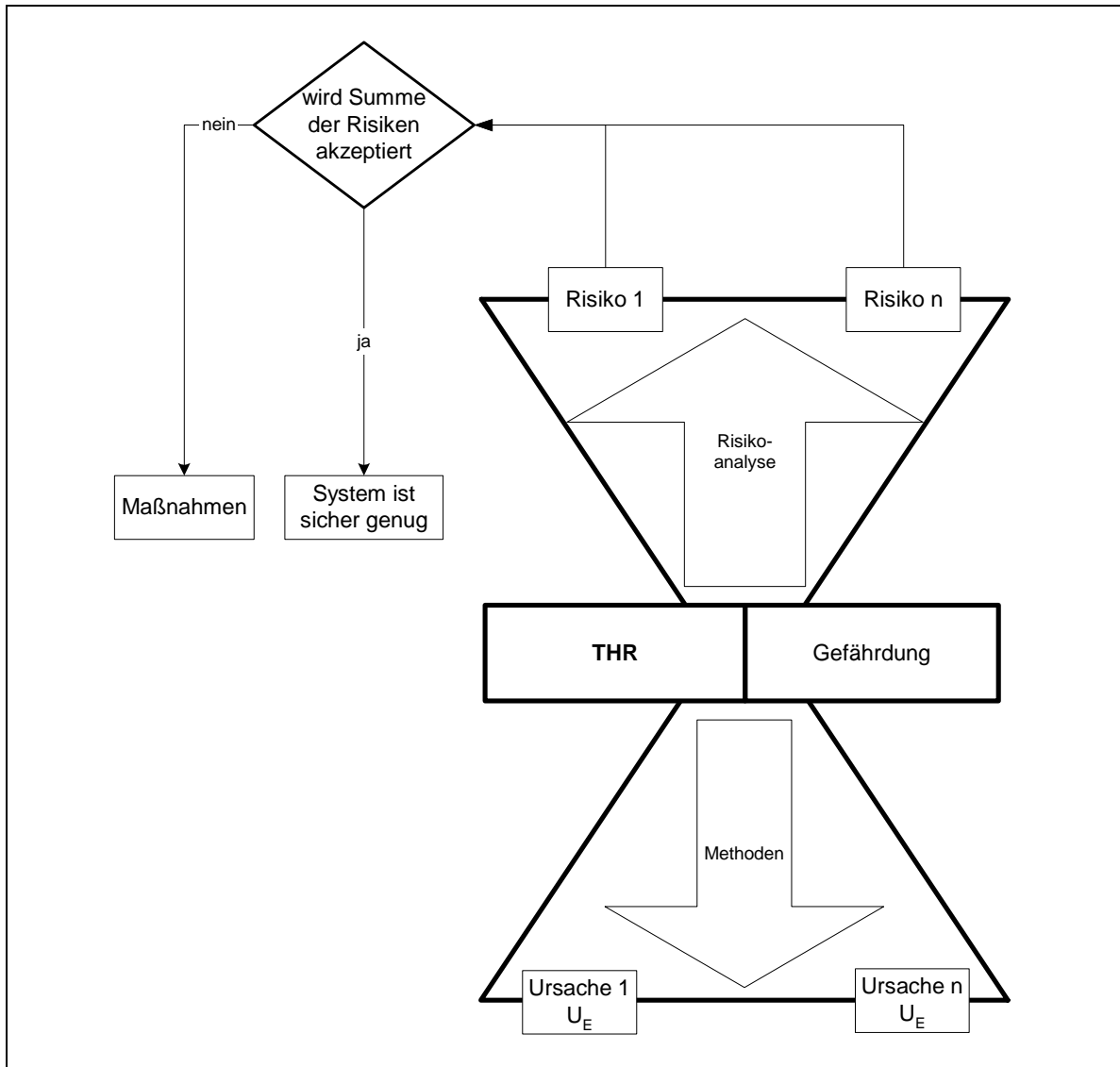


Bild 5-1: Vorgehen zur Bestimmung der THR bei der Eisenbahn

Im oberen Teil in Bild 5-2 ist das Vorgehen der FHA in dem für Eisenbahnanwendungen üblichen „Sanduhr-Modell“ dargestellt [SD1999]. Ausgehend von einem Funktionsausfall werden ohne quantitative Folgen- und Schadensanalyse die „unerwünschten Ereignisse“ (hazards) ermittelt und anschließend einzeln, entsprechend der abgestimmten Klassifizierung, bewertet. Die für die Funktionsausfälle einer Funktion ermittelten Folgen mit der „schlimmsten“ Klassifizierung sind maßgebend für die Sicherheitsanforderung an die Funktion. Daraus werden DAL (vergleichbar mit SIL) und „Tolerable Probability for occurrence of each hazard“ (vergleichbar mit THR nach [EN 50129]) für die Funktion abgeleitet. Der quantitative Teil der Risikoanalyse ist dabei bereits in der Risikoakzeptanztabelle (z.B. Tabelle 3-2) eingearbeitet.

Dem unteren Teil der Sanduhr entsprechen die Schritte PSSA und SSA des Sicherheitsprozesses nach SAE. Sie sind der Vollständigkeit halber dargestellt, wurden jedoch nicht näher betrachtet.

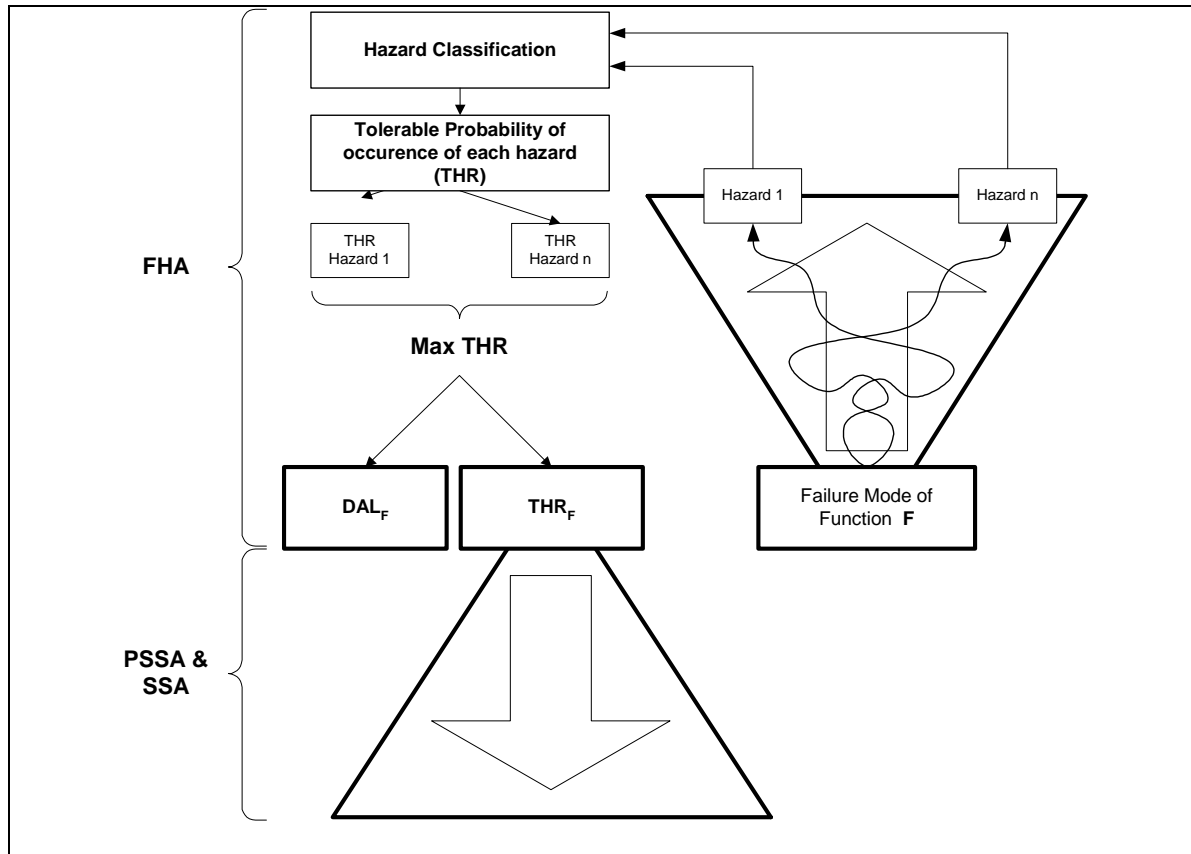


Bild 5-2: Vorgehen zur Bestimmung der tolerierten Ausfallwahrscheinlichkeit in der Luftfahrt

Beim Vergleich der beiden Vorgehensweisen (Bild 5-3) konnten neben Unterschieden auch wichtige Gemeinsamkeiten festgestellt werden:

- **Aufgabenteilung**

In beiden Anwendungsgebieten gibt es Verantwortungsbereiche der Hersteller, der Betreiber und der Zulassungsbehörden sowie Mischbereiche, in denen jeweils eine Abstimmung zwischen mehreren Beteiligten erforderlich ist. Die Vorgabe der Sicherheitsanforderungen an die Funktionen des zu betreibenden Systems obliegt in beiden Fällen dem Betreiber des Systems. Der Nachweis, dass das System die Sicherheitsanforderungen erfüllt, ist Aufgabe des Herstellers. Sowohl die Ermittlung der Sicherheitsanforderungen als auch der Nachweis der Erfüllung müssen von der Zulassungsbehörde geprüft und zugelassen werden. Sowohl bei der Eisenbahn als auch bei der Luftfahrt gibt es dabei einen Bereich, in dem Betreiber, Hersteller und Zulassungsbehörde zusammenarbeiten müssen [SAE 4754], [SD2002 (3)].

- **Vorgehensweise**

In der Luftfahrt ist das grundsätzliche Vorgehen dem bei der Eisenbahn zwar ähnlich, jedoch gibt es Unterschiede im Detail. Es ist festzustellen, dass aus dem Ausfall einer Funktion nicht direkt das Risiko (als eine Kombination von Schadensausmaß und Schadenshäufigkeit) des

Ausfalls ermittelt wird, sondern zunächst die jeweiligen unerwünschten Folgen (hazards) aller Ausfälle einer Funktion abgeschätzt werden. Diese „hazards“ beinhalten neben Unfällen auch gefährliche Vorfälle (z.B. Beinahe-Unfälle). Aus der für das betrachtete System (z.B. „großes Verkehrsflugzeug“) abgestimmten Risikoakzeptanztabelle wird abgelesen, welche Wahrscheinlichkeit für das Auftreten eines jeden „hazards“ toleriert wird. Für die Sicherheitsanforderung an die Funktion ist die restriktivste der für die Ausfälle ermittelten Anforderungen maßgebend.

Der Vorteil dieses Vorgehens liegt darin, dass zur Herleitung der Sicherheitsanforderung an eine Funktion nicht jedes Mal eine neue quantitative Folgen- und Schadensanalyse durchgeführt und die Akzeptanz jedes ermittelten Schadens nicht einzeln argumentiert werden muss. Auch die Beschreibung der Schäden (z.B. „schwere Verletzung“ nach ICAO) ist einheitlich und somit subjektiven Bewertungen entzogen. Die einmal aufgestellte Risikoakzeptanztabelle kann immer wieder verwendet werden. Auf diese Weise werden Zeit und Kosten gespart. Der Nachteil ist, dass die Erstellung und Abstimmung der Risikoakzeptanztabelle aufwändig ist.

- cross-acceptance

Ein weiterer Vorteil der abgestimmten Risikoakzeptanz in der Luftfahrt ist die Möglichkeit der cross-acceptance. Dabei wird die Zulassung eines Systems durch eine Zulassungsbehörde durch eine andere, an der Abstimmung der Risikoakzeptanztabelle ebenfalls beteiligte, Zulassungsbehörde für den eigenen Verantwortungsbereich anerkannt.

5.1.2 Systemdefinition und Betriebliches Umfeld

Das einfache betriebliche Umfeld wurde für die Untersuchung der Methode definiert. Die Beschreibung der realen Betriebsumgebung ist ungleich umfangreicher und komplexer.

Die Beschreibung der Funktionen in UNISIG Class 1 erwies sich als nicht ausreichend für die Anwendung der FHA zur Ableitung von Sicherheitsanforderungen.

Es gibt keine Funktionshierarchie, sondern nur eine Architektur mit zugewiesenen Funktionen. Dabei liegt die Gefahr nahe, ein Architekturelement, welches an der Erfüllung mehrerer Funktionen beteiligt ist (z.B. MMI des ETCS), selbst als Funktion zu betrachten. Während der FHA zur Ableitung von Sicherheitsanforderungen für die Funktionen eines Systems findet die Implementierung der Funktionen jedoch keine Beachtung.

Das definierte betriebliche Umfeld und die Verwendung von Risikoakzeptanztabellen der Luftfahrt bedingen zwangsläufig eine Ungenauigkeit der ermittelten quantitativen Aussagen bezüglich der erforderlichen Sicherheit der Funktion „Anzeigen der aktuellen Geschwindigkeit“. Die Arbeit hat jedoch gezeigt, dass die Anwendung der Methode FHA grundsätzlich auch für ETCS möglich ist.

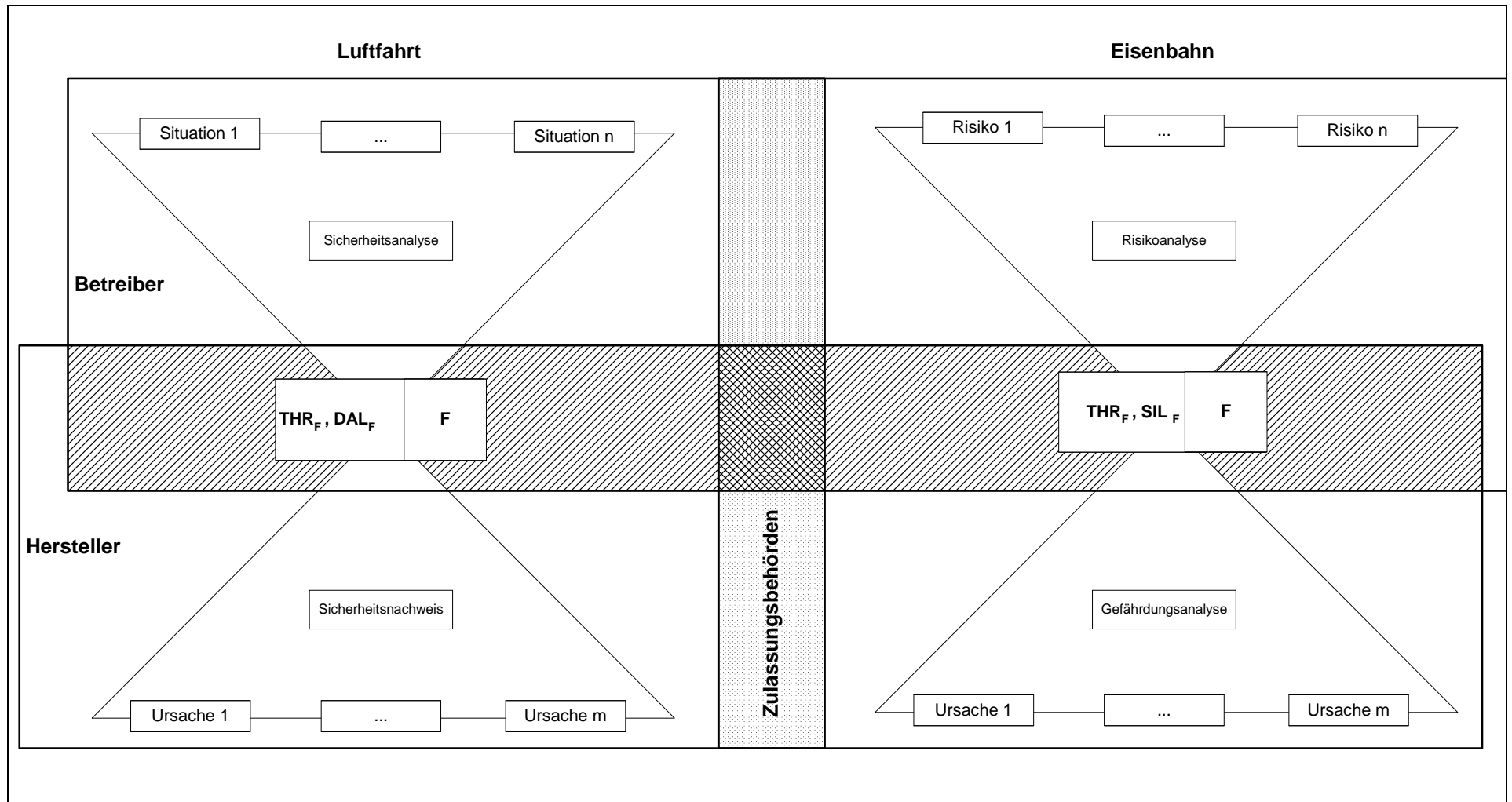


Bild 5-3: Vorgehensvergleich zur Ableitung von Sicherheitsanforderungen (THR)

Für die Ableitung von Sicherheitsanforderungen mittels der FHA müssen folgende Voraussetzungen erfüllt sein:

- **Hierarchische Funktionsaufteilung**
Die Funktionen des ETCS müssen im Kontext des Systems „Eisenbahn“ in geeigneter Weise hierarchisch gegliedert und eindeutig beschrieben werden.
- **betriebliche Regelungen für das Fahren unter Sicherheitsverantwortung**
Das betriebliche Umfeld für das Fahren unter ETCS-Sicherheitsverantwortung muss definiert werden, um die Folgen der Funktionsausfälle von ETCS-Funktionen abschätzen zu können.

Im Sinne der Interoperabilität ist es notwendig, die oben genannten Punkte einheitlich für alle Benutzer des ETCS zu formulieren und umzusetzen. Durch die derzeitigen betreiberspezifischen Unterschiede ist es nicht absehbar, ob ein Funktionsausfall bei einem Betreiber nur geringe Auswirkungen auf die Sicherheit hat, während der gleiche Funktionsausfall sich bei einem anderen Betreiber (aus betrieblichen Gründen) schwerwiegend auf die Sicherheit auswirkt.

Die nationalen Unterschiede im Betrieb erschweren den gewünschten Wettbewerb zwischen den Herstellern, da jeder Hersteller im wesentlichen sein nationales (Betriebs-)Wissen hat. Eine einheitliche Betriebsvorschrift für ETCS würde gleiche Voraussetzungen für alle Hersteller schaffen.

Bei dem geplanten Betrieb des ETCS, aufgesetzt auf nationale Stellwerks- und Signalsysteme - und mit diesen als Rückfallebene - werden wahrscheinlich keine einheitlichen Regelungen erreichbar sein. Würde man jedoch eine mit ETCS ausgerüstete Strecke als abgeschlossenes System betrachten, wären diese durchaus machbar.

Ein Unterschied zur Eisenbahn liegt im Luftverkehr in der (fast) vollständigen Autonomie des Flugzeuges. Bei erkannten Fehlern und Ausfällen der Bodentechnik kann der Pilot das Flugzeug völlig autonom bewegen. Die bei der Eisenbahn systemtypische zwangsweise Spurführung des Fahrzeugs durch den Fahrweg existiert in dieser Form im Luftverkehr nicht. Einem Flugzeug wird zwar auch ein „Fahrweg“ zugewiesen und freigehalten, das Flugzeug wird jedoch nicht zwanghaft auf diesem Fahrweg gehalten, sondern kann ihn ungehindert verlassen. Auf diese Weise kann der Pilot gefährliche Situationen entschärfen oder aber auch erst herbeiführen bzw. verschlimmern [SAE 4754].

5.1.3 einheitliche Risikoakzeptanz

Die hier versuchsweise verwendete Risikoakzeptanztabelle (Tabelle 3-2) gilt nur für das System „großes Verkehrsflugzeug“. Die Einheit „Flugstunde“ bezieht sich dort auf den Ausfall einer Funktion eines Flugzeuges (Funktionsausfall pro Flugstunde und Flugzeug). In [AMJ 25.1309] ist die Entwicklung der quantitativen Sicherheitsanforderungen für Flugzeugfunktionen wie folgt beschrieben:

„...Historical evidence indicates that the risk of a serious accident due to operational and air-frame-related causes is approximately 1 per million hours of flight. Furthermore, about 10 percent of the total can be attributed to Failure Conditions caused by aeroplane's system problems. It seems reasonable that serious accidents caused by systems should not be allowed a higher probability than this in new aeroplane designs. It is thereby possible to require for new designs that the probability of a serious accident from all such Failure Conditions be not greater than 1 per ten million flight hours or 1×10^{-7} per flight hour.

The difficulty with this is that it is not possible to say whether the target has been met until all the systems on the aeroplane are collectively analysed numerically.

For this reason it is assumed, arbitrarily, that there are about 100 potential Failure Conditions in an aeroplane which would prevent continued Safe Flight an Landing. The target allowable risk of 1×10^{-7} was thus apportioned equally among these Conditions, resulting in a risk allocation of not greater than 10^{-9} to each. The upper-risk limit for Failure Conditions which would prevent Continued Safe Flight an Landing would be 10^{-9} for each hour of flight which establishes an approximate probability value for the term „Extremely Improbable“. Failure Conditions having less severe effects could be relatively more likely to occur...”.

Diese Verteilung der Sicherheitsanforderungen auf sicherheitskritische Flugzeugfunktionen ist in Bild 5-4 dargestellt. In [AMJ 25.1309] werden keine Aussagen dazu getroffen, wie die restlichen 90 Prozent des „...risk of a serious accident due to operational and air-frame-related causes...“ verteilt werden. Statistisch ermittelt wurde, dass ca. 10 Prozent der Unfälle auf das Versagen von Flugzeugsystemen entfallen. Im nächsten Schritt wurde angenommen, dass es ca. 100 Ausfallzustände (Failure Conditions) in einem Flugzeug geben kann, von denen jeder einzelne eine sichere Fortsetzung des Fluges oder eine sichere Landung verhindert, so dass das „Häufigkeitspotential“ gleichmäßig auf diese Zustände verteilt wurde. Es ist nicht erläutert, wie die Einteilung der Risikoklassen mit weniger schweren Folgen vorgenommen wurde.

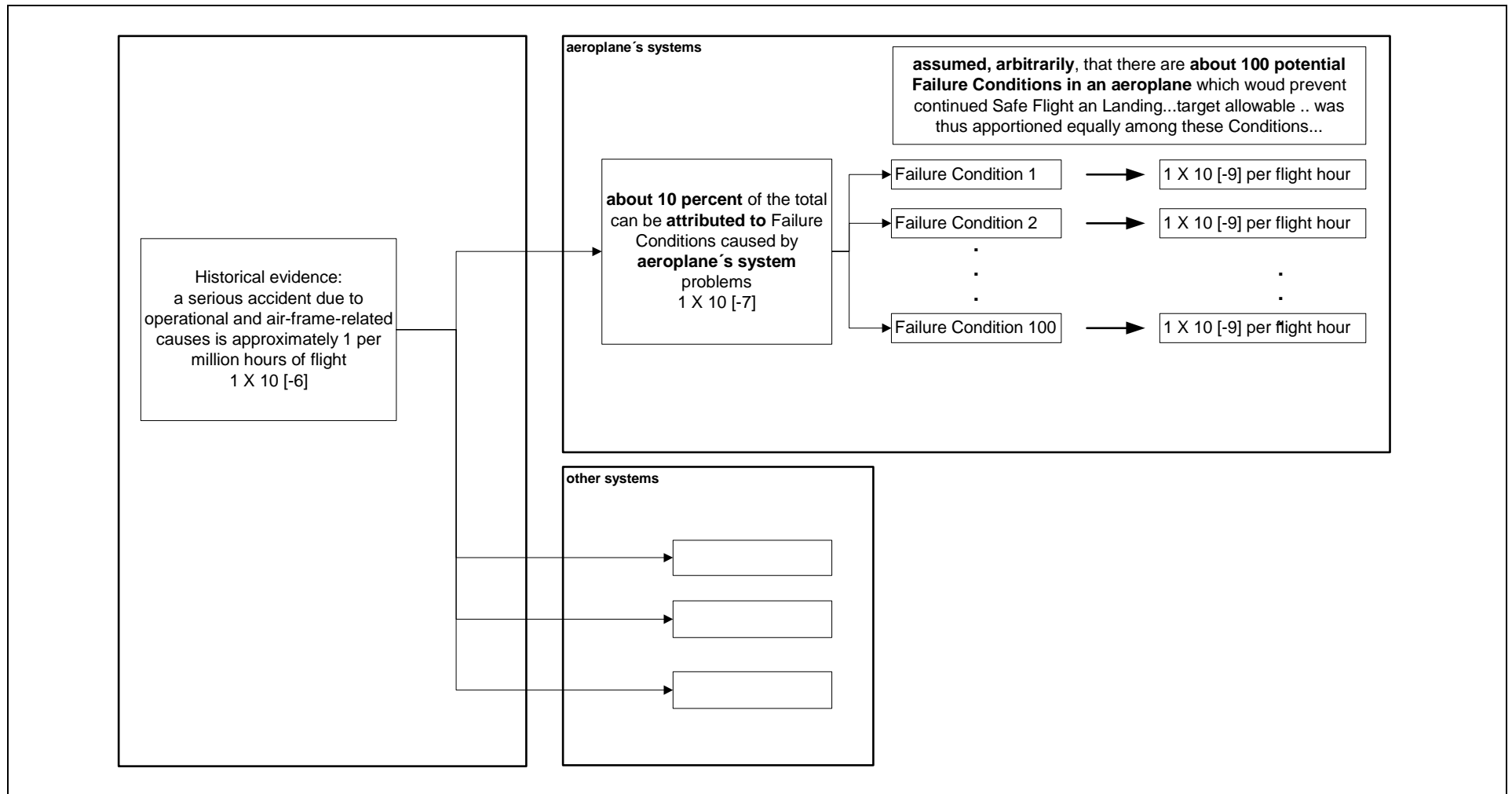


Bild 5-4: Entwicklung der „THRs“ für große Verkehrsflugzeuge

Für die Flugsicherung gibt es dazu eine ähnliche, aber auf das System „Flugsicherung“ abgestimmte, Risikoakzeptanz. Auch dort wird die Einheit „Flugstunde“ verwendet. Für die Flugsicherung im Bereich der ECAC-Mitgliedsstaaten beträgt die „maximum tolerable probability of ATM directly contributing to an accident of a commercial Air Transport aircraft“ $1,55 \times 10^{-8}$ pro Flugstunde [ESARR4]. Dieses Sicherheitsziel für den Schweregrad („severity class“) 1 bezieht sich somit auf die gesamte Flugsicherung. Die Aufteilung auf Sicherheitsanforderungen für Funktionen ist noch nicht erfolgt. Auch gibt es noch keine quantitativen Sicherheitsziele für Ausfallfolgen der Schweregrade 2, 3, 4 und 5 [ESARR4].

Es gibt somit keine einheitliche Risikoakzeptanz für „den Luftverkehr“. Die Risikoakzeptanz ist jeweils zugeschnitten auf ein bestimmtes System (Flugzeug, Flugsicherung).

Die Erstellung der Risikoakzeptanztabellen erforderte neben dem Aufwand für statistische Untersuchungen umfangreiche Abstimmungen [SAE 4754] [Anlage] zwischen den beteiligten Interessenten (Betreiber, Hersteller, Zulassungsbehörden). Sie ermöglicht aber die Ableitung von Sicherheitsanforderungen für Funktionen ohne den Besitz der für eine Risikoanalyse erforderlichen Expertise [SAE 4754]. Das bedeutet für die Eisenbahnsignaltechnik jedoch nicht, dass auf eine Risikoanalyse verzichtet werden kann. Man erspart sich durch die Verwendung der Risikoakzeptanztabelle lediglich die quantitative Ermittlung der Auftretenswahrscheinlichkeiten von bestimmten Ausfallfolgen.

5.1.4 Terminologie

Die Etablierung eines Sicherheitsprozesses im Zusammenhang mit Entwicklung, Herstellung, Zulassung und Betrieb eines Systems erfordert ingenieurmäßiges Verständnis, personelle und finanzielle Ressourcen und den gemeinsamen Willen aller Beteiligten [SAE 4754], [EC2000] [STO1996]. Es wird nicht in allen Phasen des Entwicklungsprozesses eine exakte Trennung der Aufgaben geben können. In Mischbereichen ist eine offene Kommunikation der betroffenen Beteiligten erforderlich. Diese Kommunikation muss von einem gemeinsamen Verständnis geprägt sein [EC2000]. Dafür ist eine einheitliche Terminologie sehr hilfreich.

6 Ausblick

In allen Systemen, in denen Menschen mit der Unterstützung durch Technik Aufgaben erfüllen, müssen Technik und Betrieb aufeinander abgestimmt sein. Die Erstellung der erforderlichen Systemdefinition und damit der Definition von Aufgaben und Funktionen sowie Aufgabenträgern ist besonders schwierig. Ein gemeinsames Verständnis aller beteiligten Interessengruppen (Hersteller, Betreiber, Zulassungsbehörden, Öffentlichkeit u.a.) für das System ist dabei unerlässlich.

Mit dem dargestellten Erkenntnisstand konnten keine Kriterien gefunden werden, welche die Anwendung der FHA für die Eisenbahn aufgrund von Widersprüchen zur normativen Situation für Eisenbahnanwendungen verhindern. Wie diese Untersuchung gezeigt hat, kann die Methode des „FHA“ auch bei Eisenbahnanwendungen zur Ableitung von Sicherheitsanforderungen angewendet werden.

Für eine „reale“ Anwendung der FHA zur Ableitung von Sicherheitsanforderungen an ETCS müssen folgende Voraussetzungen erfüllt werden:

- Erstellung einer hierarchisch gegliederten Funktionsstruktur des ETCS
- Definition der betrieblichen Bedingungen für das Fahren unter Verantwortung des ETCS
Dieser Teil der Systembeschreibung muss auch im Rahmen einer Risikoanalyse nach [EN 50129] erfolgen und bedeutet somit keinen Mehraufwand bei der Anwendung der FHA.
- Aufstellung einer geeigneten Schadensklassifikation und Risikoakzeptanztabelle, z.B. für die Eisenbahnsignaltechnik
Der dadurch zu erreichende Vorteil liegt in der einmaligen Auswertung der statistischen Daten.

Im Sinne der Interoperabilität sollten diese Voraussetzungen für alle Anwender des ETCS die gleichen sein. Dabei ist nicht zu erwarten, dass der Aufwand für die Ableitung von Sicherheitsanforderungen grundsätzlich geringer ist als bei Risikoanalysen nach [EN 50129]. Der Vorteil liegt im Vorhandensein und der Verwendung von abgestimmten Risikoakzeptanztabellen.

Bei Anwendung des gesamten Sicherheitsprozesses der SAE erfolgt eine Ausrichtung der Systemarchitektur an der Funktionshierarchie des Gesamtsystems und führt damit zu einer ausgewogenen Systemarchitektur. Es ist zu prüfen, ob die FHA ihre Wirksamkeit erreichen kann, wenn sie aus dem Systementwicklungsprozess der SAE herausgerissen und isoliert verwendet wird.

Literaturverzeichnis

- [ACJ 25.1309] Joint Aviation Authorities: Advisory Circular Joint 25.1309: Equipment, Systems, Installations (Interpretative Material), October 1, 2000
- [AMJ 25.1309] Joint Aviation Authorities: Advisory Material Joint 25.1309: System Design and Analyses, October 1, 2000
- [EBA] Eisenbahnbundesamt (Hrsg.): Untersuchungsbericht Entgleisung des D 203 im Bahnhof Brühl am 06.02.2000, 20.04.2000
- [EC2000] EUROCONTROL (Hrsg.): Air Navigation System Safety Assessment Methodology, Edition 1.0, 17.04.2000
- [EC2001] EUROCONTROL (Hrsg.): Link2000+ High Level Safety Plan, Edition 1.0, 09.03.2001
- [EN 50129] CENELEC: European Standard (Final Draft) prEN 50129, Railway applications – Communication, signalling and processing systems – Safety related electronic systems for signalling, May 2002
- [ESARR4] EUROCONTROL (Hrsg.): Eurocontrol Safety Regulatory Requirement 4 (ESARR4): Risk Assessment and Mitigation in ATM, Edition 1.0, 05.04.2001
- [ETR2002] Braband, J.: Erfahrungen mit Risikoanalysen in der Eisenbahnsignaltechnik, Eisenbahntechnische Rundschau, Nr. 9, 2002, 575-582
- [FENNER] Fenner, W., Naumann, P. (Hrsg.: Siemens-Aktiengesellschaft, Berlin und München): Verkehrssicherungstechnik, Publicis-MCD-Verlag, 1998
- [FRS99] ERTMS USER GROUP (Hrsg.): ERTMS/ETCS Functional Requirements Specification, Version 4.29, 03.12.1999
- [JAR 25.1309] Joint Aviation Authorities: Joint Aviation Regulation 25.1309 Equipment, Systems, Installations, October 1, 2000
- [KELLY] Kelly, T.P., Wilkinson P. J.: Functional hazard analysis for highly integrated aerospace systems, In Proceedings of IEE Seminar on Certification of Ground / Air Systems, London, U.K., February 1998
<http://www-users.cs.york.ac.uk/~tpk/ieefha.pdf>
- [PORT2000] Portwood, B.: Functional Hazard Assessments, 2000 Designated Engineering Representatives Recurrent Seminar, Los Angeles Aircraft Certification Office
<http://av-info.faa.gov/dst/larec00/c2-02-Portwood.pdf>
- [SAE 4754] Society of Automotive Engineers, Inc.: Aerospace Recommended Practice 4754, Certification Considerations for highly-integrated or complex aircraft systems, issued 1996-11
- [SAE 4761] Society of Automotive Engineers, Inc.: Aerospace Recommended Practice 4761, Guidelines and methods for conducting the safety assessment process on civil airborne systems and equipment, issued 1996-12
- [SAG2002] Siemens AG: Workshop zum Thema "Sicherheitsanforderungen und FHA", Referent Prof. Dr. Michael Miller, Fachhochschule Gelsenkirchen, 15./16.07.2002
- [SD1999] Braband, J., Lennartz, K.: Systematisches Verfahren zur Festlegung von Sicherheitszielen, Signal + Draht, Nr. 9, 1999, 5-10

- [SD2002 (1)] Dijkman, R.: ERTMS/ETCS – Consolidation Strategy, Signal + Draht (94) 5/2002
- [SD2002 (2)] Dijkman, R.: ERTMS/ETCS – The ESROG Project, Signal + Draht 3/2002
- [SD2002 (3)] Mihm, P., Kiel, H., Maschek, U.: Sicherheitsanforderungen an eine moderne Zugbeeinflussung, Signal + Draht 3/2002
- [SD2002 (4)] Kurzberichte, Signal + Draht 6/2002, S. 41
- [SD2002 (5)] Braband, J., Günther, J., Lennartz, K., Reuter, D.: Risikoakzeptanzkriterien für den FunkFahrBetrieb (FFB), Signal + Draht 5/2001
- [SD2002 (6)] Braband, J., Porzig, A., Wunder, H.-J.: Risikoanalysen für Elektronische Stellwerke, Signal + Draht, Nr. 9, 2002, 11-16
- [STO1996] Storey, N.: Safety-critical computer systems, Addison-Wesley 1996
- [TRE2000] Treacy, J.: Recent Safety Assessment Process Activities, 2000 Designated Engineering Representatives Recurrent Seminar, Los Angeles Aircraft Certification Office
<http://av-info.faa.gov/dst/larec00/c2-06-Treacy.pdf>
- [TSI] Amtsblatt der Europäischen Gemeinschaften L245: Technische Spezifikation für die Interoperabilität des Teilsystems „Zugsteuerung, Zugsicherung und Signalgebung“ des transeuropäischen Hochgeschwindigkeitsbahnsystems, Aktenzeichen K(2002) 1947) (1), 12.09.2002
- [TUD] TU Dresden, Fakultät Verkehrswissenschaften „Friedrich List“, Institut für Luftfahrt, Prof. Dr.Ing. habil. E. Schesky: privates Vorlesungsskript zur Vorlesungsreihe „Luftverkehrssicherheit“ im WS 96/97
- [UNISIG 23] UNISIG: ERTMS/ETCS – Class 1, Glossary of UNISIG Terms and Abbreviations, Subset –023-, issue 2.0.0
- [UNISIG 26] UNISIG: ERTMS/ETCS – Class 1, System Requirements Specifications, Subset –026-, issue 2.2.0
- [UNISIG 30] UNISIG: ERTMS/ETCS – Class 1, UNISIG SSRS, Part 1: System macro functions overview, Subset –030-, issue 2.0.0
- [UNISIG 31] UNISIG: ERTMS/ETCS – Class 1, UNISIG SSRS Part 2: On-Board Subsystem Requirement Specification, Subset –031-, issue 0.2.1
- [VDI2000] Verein Deutscher Ingenieure (Hrsg.), VDI Berichte 1546, 2000
- [W1] ERTMS
<http://www.ertms.com/specifications.html>
Letzte Änderung: n.n.
Letzter Besuch: 11.07.2002
- [W2] ERTMS
<http://www.ertms.com/project.html>
Letzte Änderung: n.n.
Letzter Besuch: 11.07.2002
- [W3] ERTMS
<http://www.ertms.com/history.html>
Letzte Änderung: n.n.
Letzter Besuch: 11.07.2002

- [W4] ERTMS
<http://www.ertms.com/level.html>
Letzte Änderung: n.n.
Letzter Besuch: 11.07.2002
- [W5] DFG
<http://ivev8.ivev.bau.tu-bs.de/~pachl/glossar.htm>
Letzte Änderung: 12.05.2002
Letzter Besuch: 10.09.2002
- [W6] What is the JAA?
<http://www.jaa.nl/whatisthejaa/jaainfo.html#2.8>
Letzte Änderung: June 2002 (Issue 26)
Letzter Besuch: 02.08.2002
- [W7] FAA – Office of Public Affairs
<http://www.faa.gov/apa/history/overview.cfm?nav=about>
Letzte Änderung: 22.05.2002
Letzter Besuch: 15.08.2002
- [W8] About SAE
<http://www.sae.org/about/index.htm>
Letzte Änderung: 2002
Letzter Besuch: 03.09.2002
- [W9] International Civil Aviation Organization (ICAO)
<http://www.icao.int/index.cfm>
Letzte Änderung: 2002
Letzter Besuch: 03.09.2002
- [W10] LINK 2000 Programme Management
<http://www.eurocontrol.int/link2000/index.htm>
Letzte Änderung: 10.06.2002
Letzter Besuch: 10.09.2002
- [W11] Aktuelles
<http://www.bfu-web.de/olderinfo/aktuinfo-d28.htm>
Letzte Änderung: 2002
Letzter Besuch: 16.09.2002
- [W12] DFS Deutsche Flugsicherung GmbH
<http://www.luftrecht-online.de/einzelheiten/verwaltung/dfs.htm>
Letzte Änderung: 19.05.2002
Letzter Besuch: 20.09.2002
- [W13] Regelungen im Bereich der Luftfahrt
<http://www.luftrecht-online.de/grundlagen/grundlagen/lr-jar.htm>
Letzte Änderung: 14.04.2002
Letzter Besuch: 20.09.2002

Anlage

Protokoll zum Workshop „Functional Hazard Analysis“

Datum: 13.06.02

Teilnehmer: Dr. Jens Braband (Siemens AG)
Dr. Clemens Fuhrmann (Siemens AG)
Frank Renpenning (Siemens AG)
Frank Leißner (DB AG)
Prof. Dr. Jörg Schütte (TU Dresden)
Sten Wery (TU Dresden)
Prof. Dr. Michael Miller (FH Gelsenkirchen)

Tagesordnung:

1. Begrüßung, Vorstellungsrunde
2. Kurzer Überblick über Funktionsweise ETCS
3. Vortrag Hr. Wery über den Arbeitsstand seiner Diplomarbeit
(Thema: „Anwendung der FHA in der Eisenbahnsignaltechnik am Beispiel ETCS, Level 2“)
4. fachliche Diskussionen
5. Weiteres Vorgehen

Zielsetzung und Charakter des Workshops

Ein Problem bei der Etablierung des ETCS ist die Herleitung der Sicherheitsziele für dieses System. Im Rahmen der Diplomarbeit soll beispielhaft versucht werden, die „Functional Hazard Analysis“ methodisch auf die Eisenbahnsignaltechnik anzuwenden. Wie der Name der Methode schon zum Ausdruck bringt, handelt es sich dabei um einen funktionalen Ansatz. Dieser für die Eisenbahn neue Weg wird in der Luftfahrt schon länger beschritten.

Ziel des informellen Workshops war, Erfahrungen bei der Anwendung der FHA zur Herleitung von Sicherheitszielen in der Luftfahrt für die Eisenbahn verfügbar zu machen. Dabei sollten Verständnisfragen geklärt sowie Parallelen und Unterschiede zu einer möglichen Anwendung der FHA in Bereichen der Eisenbahn erkannt und diskutiert werden.

Zusammenfassung:

Nach einer kurzen Einleitung durch Dr. Braband und einer Vorstellungsrunde gab Hr. Leißner einen kurzen Überblick über die Funktionsweise des ETCS. Während des Vortrages von Hr. Wery zum Arbeitsstand seiner Diplomarbeit ergaben sich intensive Fachgespräche zwischen allen Beteiligten. Folgende Erkenntnisse sind dabei besonders hervorzuheben:

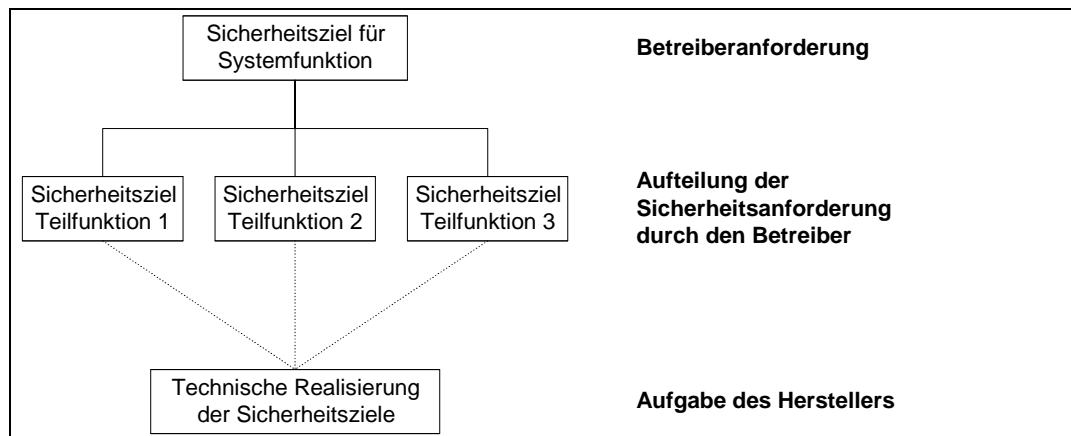
In der kommerziellen, zivilen Luftfahrt findet bei der Sicherheitsbetrachtung eine Trennung der für den Flugbetrieb notwendigen Systeme statt. So werden z.B. die Systeme „Flugzeug“ und „Flugsicherungssystem“ unterschieden.

Im Gegensatz zur restriktiven Wirkungsweise der Zugbeeinflussungssysteme bei der Eisenbahn haben Überwachungssysteme im Flugzeug in letzter Konsequenz nur eine warnende Funktion. Die Entscheidung über seine Handlungen trifft der Pilot anhand der ihm zur Verfügung stehenden Informationen selbst. Er kann sich dabei bewusst über Hinweise und Handlungsvorschläge der installierten Überwachungssysteme hinwegsetzen. Der Pilot hat somit das Kommando über das Flugzeug.

In der Luftfahrt gibt es einheitlich zwischen Zulassungsbehörden, Betreibern und Herstellern abgestimmte Sicherheitsziele. Diese sind als Standard festgelegt und werden nicht bei jeder Neuentwicklung oder Systemanpassung neu nachgewiesen. Die Verteilung des übergeordneten Sicherheitszieles für ein Gesamtsystem auf Sicherheitsziele für die Teilsysteme obliegt dem Betreiber des Gesamtsystems. Die Realisierung dieser Sicherheitsziele auf Teilsystemebene ist Aufgabe des Herstellers des Systems.

Im übertragenen Sinne bedeutet das für ETCS, dass es Aufgabe der ETCS betreibenden Bahnen ist,

die Sicherheitsziele zu definieren (Bild unten). Diese Ziele müssen aber im Sinne der Interoperabilität zwischen den beteiligten Bahnen abgestimmt und einheitlich sein. Sonst ist es möglich, dass unterschiedliche Betreiber das Sicherheitsziel für das Gesamtsystem unterschiedlich auf die Teilsysteme verteilen und dadurch unterschiedliche technische Realisierungen notwendig sind.



Hinter dem Sicherheitsziel für ein System verbirgt sich bei einem risikoorientierten Ansatz letztendlich eine Bewertung des Lebens einer einzelnen Person. (Preisfrage: Was kostet ein Leben?) Diese Sichtweise wird jedoch nicht öffentlich diskutiert und die zugehörigen Zahlen stellen Unternehmensgeheimnisse dar.

Sicherheitsanforderungen können (und müssen) zur Beseitigung von Verständnisproblemen zielgruppenspezifisch formuliert sein. Dies ist vor allem für die FHA-Sitzungen notwendig, wenn es darum geht, von den Benutzern eines bestehenden Systems quantitative Schätzungen über die Häufigkeit des Auftretens von bestimmten Situationen zu erhalten. (z.B.: Verwendung der Formulierung „einmal in 30 Jahren“ anstatt „2,6 * 10⁻⁶ pro Stunde“). Die Herleitung der Sicherheitsziele ist aufwendig und damit teuer, weil viele Gespräche u.a. mit Benutzern des bestehenden Systems (z.B. Fluglotsen, Piloten, Bodencrew usw.) geführt werden müssen. Dadurch finden jedoch ganz konkrete Erfahrungen von einzelnen Personen Eingang in die Sicherheitskonzeption eines neuen technischen Systems. Um diesem Personenkreis die Angabe der benötigten Informationen zu ermöglichen, gibt es in der Luftfahrt spezielle Fragebögen und Datenbanken.

Es muss festgehalten werden, dass es Unterschiede in der Begriffswelt der Methodiken für Sicherheitsbetrachtungen in der Luftfahrt bzw. der Eisenbahn gibt. Diese Unterschiede sind bei der Übertragung der Methodik der Luftfahrt auf Sicherheitsbetrachtungen für die Eisenbahn zu beachten und entsprechende Anpassungen abzustimmen.

Die FHA kann auf beliebige Funktionen und Systeme in jeder beliebigen Detaillierungsstufe angewendet werden. Diese Anwendung ist jedoch an die Anpassung der methodischen Hilfsmittel (Tabellen) für die FHA gebunden, so dass die Anwendung der FHA eine Frage der Komplexität des betrachteten Systems ist. Sie wird deshalb vorwiegend in den oberen Detaillierungsstufen angewendet.

Die FHA liefert für bestimmte gefährliche Situationen (Hazards) Aussagen zu den möglichen Folgen der Gefahrensituation. Durch die Methodik der FHA lässt sich die Verteilung der Sicherheitsziele für Teilfunktionen- bzw. Systeme wirtschaftlich optimieren. Dies kann u.U. zur Folge haben, dass Funktionen vom Betreiber ausgelagert werden (outsourcing, Risikomanagement). Dies erfordert den verantwortungsbewussten Umgang mit bekannten und unbekanntem Risiken.

Die Sicherheitsziele resultieren unter Anwendung der abgestimmten Tabellen aus den Folgen eines möglichen Funktionsversagens.

Weitere Schritte:

Tabelle der Ausmaßkategorien für Eisenbahn anpassen

Tabelle der Situationen (Reduktionsfaktoren) für Eisenbahn anpassen

Beispielhafte Durchführung einer FHA an einer Funktion unter Annahme der angepassten Tabellen
Definition (willkürliche Festlegung, ggf. vereinfacht) der für die FHA notwendigen (betrieblichen)
Randbedingungen.

Identifizierung innerhalb ETCS abzustimmender Punkte

gez. Sten Wery