

Von der Fakultät Verkehrswissenschaften "Friedrich List"
an der Technischen Universität Dresden
genehmigte Dissertation
zur Erlangung des akademischen Grades eines
Doktors der Ingenieurwissenschaften (Dr.-Ing.)

Ein Beitrag zur ganzheitlichen Sicherheitsbetrachtung des Bahnsystems

von Dipl.-Ing. Enrico Anders
geboren am 16. April 1975 in Dresden

Eingereicht am 29. Februar 2008
Tag der Verteidigung: 7. November 2008

Betreuender Hochschullehrer:
Prof. Dr.-Ing. Jochen Trinckauf

Promotionskommission:
Prof. Dr. rer. nat. habil. Karl Nachtigall (TU Dresden, Vorsitzender)
Prof. Dr.-Ing. Jochen Trinckauf (TU Dresden, 1. Gutachter)
Prof. Dr. rer. nat. Jens Braband (TU Braunschweig/Siemens AG, 2. Gutachter)
Prof. Dr.-Ing. Géza Tarnai (TWU Budapest, 3. Gutachter)
Prof. Dr.-Ing. habil. Hans-Joachim Jentschel (TU Dresden)
Prof. Dr.-Ing. Wolfgang Fengler (TU Dresden)

Danksagung

Diese Arbeit entstand während meiner Tätigkeit als wissenschaftlicher Mitarbeiter an der Fakultät Verkehrswissenschaften „Friedrich List“ der Technischen Universität Dresden, der Professur für Verkehrsicherungstechnik unter der Leitung von Herrn Prof. Dr.-Ing. Jochen Trinckauf.

Die Idee zur vorliegenden Arbeit reifte in einer Vielzahl von Gesprächen sowie in verschiedenen Projekten und Veranstaltungen, in denen Fachleute des Bahnwesens über die mangelnde Beachtung und Betrachtung von betrieblichen Einflüssen auf das Bahnsystem, besonders in den frühen Phasen des Bahnlebenszyklus berichteten.

Mein außerordentlicher Dank für die fachliche Begleitung und die mir gebotene Möglichkeit zur Erstellung der Promotion im Rahmen meiner wissenschaftlichen Tätigkeit gebührt meinem Doktorvater, Herrn Prof. Dr.-Ing. Jochen Trinckauf. Trotz der hohen Arbeitsbelastung nahm er sich immer wieder Zeit für motivierende Kritik und wertvolle Anregungen.

Einen ebenso herzlichen Dank richte ich an Herrn Prof. Dr. rer. nat. Jens Braband und Herrn Prof. Dr.-Ing. Géza Tarnai für die Bereitschaft zur Begutachtung der Arbeit sowie die vielen lohnenden Hinweise. Ebenso danke ich Herrn Prof. Dr. rer. nat. habil. Karl Nachtigall für die Übernahme des Vorsitzes der Promotionskommission. Ich danke Herrn Prof. Dr.-Ing. habil. Hans-Joachim Jentschel sowie Herrn Prof. Dr.-Ing. Wolfgang Fengler in ihrer Funktion als Mitglieder der Promotionskommission.

Darüber hinaus gilt ein großer Dank Herrn Dr.-Ing. Ulrich Maschek und den Mitarbeitern der Professur für Verkehrssicherungstechnik. Ohne deren Bereitschaft zur konstruktiven Diskussion über spezielle Ergebnisse der Arbeit hätte diese nicht die notwendige Entwicklung nehmen können.

Ohne die familiäre Unterstützung, die ich im Laufe der Bearbeitungszeit erfahren habe, wäre der Abschluss der Dissertation nur schwer vorstellbar gewesen. Besonderer Dank gilt daher meiner Frau Julia Anders für die emotionale Unterstützung und meiner Tochter Pauline für die ruhigen Nächte, in denen die Erkenntnisse des Tages zu Papier gebracht werden konnten.

Enrico Anders

Dresden im März 2009

Inhaltsverzeichnis

Abkürzungsverzeichnis	V
Bildverzeichnis	VI
1 Motivation	1
2 Grundlagen zur Sicherheit	5
2.1 Rechtliche Grundlagen	5
2.2 Nachweis von Sicherheit	6
2.2.1 Anforderungen.....	6
2.2.2 Aufgaben	6
2.2.3 Aufgabenverteilung	8
3 Herleitung des risikoorientierten Sicherheitsbegriffs	10
3.1 Gefahr und Gefährdung	10
3.2 Identifikation von Gefährdungen	12
3.3 Gefährdungsrate.....	14
3.4 Schadensausmaß.....	14
3.5 Risiko	15
3.6 Risikoarten	16
3.6.1 Natürliches und technisches Risiko	16
3.6.2 Subjektives und objektives Risiko	17
3.6.3 Individuelles und kollektives Risiko	18
3.6.4 Grenzkrisiko.....	20
3.7 Sicherheit.....	25
3.8 Safety und Security	26
3.9 Verfügbarkeit.....	28
3.10 Zuverlässigkeit.....	28
3.10.1 Kenngrößen der Zuverlässigkeit.....	28
3.10.2 Ermittlung der Zuverlässigkeit.....	29
3.11 Instandhaltbarkeit.....	29
3.11.1 Kenngrößen der Instandhaltung.....	30
3.11.2 Ermittlung der Instandhaltbarkeit.....	30
4 Unterscheidung zwischen Fehlern, Ausfällen und Störungen	32
4.1 Begriffliche Einordnung	32
4.2 Definitionen.....	33
4.3 Zeitliche Einordnung	34
4.4 Fehler	35
4.4.1 Fehlerarten.....	35
4.4.2 Quellen für Fehler	36

4.4.3	Technische Fehler	37
4.4.4	Menschliche Fehler.....	38
4.5	Ausfall.....	47
4.5.1	Ausfallarten.....	47
4.5.2	Quellen für Ausfälle	47
4.5.3	Ausfallzeitpunkte.....	48
4.6	Störung	48
4.7	Kategorisierung von Fehlern, Ausfällen und Störungen	49
4.8	Fehler, Ausfälle und Störungen im Regelkreis des Bahnsystems	50
5	Sicherungstechnische Grundsätze im Bahnsystem	53
5.1	Umgang mit Fehlern, Ausfällen und Störungen.....	53
5.1.1	Ausschluss von Fehlern, Ausfällen und Störungen	53
5.1.2	Ausschluss von F/A/S-Folgen	54
5.1.3	Begrenzung von F/A/S-Folgen.....	56
5.2	Verwendung von Zuständen zur Systemanalyse.....	57
5.2.1	Sicherer Zustand	57
5.2.2	Hemmender Zustand	58
5.2.3	Gefährlicher Zustand.....	59
5.3	Darstellung und Analyse von Systemkennwerten	59
5.3.1	Verfügbarkeits-Sicherheits-Diagramm	59
5.3.2	Beispiel eines Verfügbarkeits-Sicherheits-Diagramms.....	60
6	Darstellung der ganzheitlichen Sicherheitsbetrachtung von Bahnsystemen im Modell.....	67
6.1	Zusammenfassung der Grundlagen für das Modell	67
6.2	Normative Grundlagen für das Modell.....	68
6.3	Modell der ganzheitlichen Sicherheitsbetrachtung von Bahnsystemen.....	69
6.4	Zulassungsverfahren mit betrieblichem Sicherheitsnachweis	73
7	Zusammenfassung und Ausblick	75
	Glossar	77
	Quellenverzeichnis.....	87

Abkürzungsverzeichnis

2v3	2 von 3
AEG	Allgemeines Eisenbahngesetz
ALARP	As low as reasonably practicable (dt. so niedrig wie vernünftigerweise praktikabel)
BZ	Betriebszentrale (der DB AG)
CEN	Europäisches Komitee für Normung (franz. Comité Européen de Normalisation)
CENELEC	Europäisches Komitee für elektrotechnische Normung (franz. Comité Européen de Normalisation Electrotechnique)
DB AG	Deutsche Bahn Aktiengesellschaft
DIN	Deutsches Institut für Normung e.V.
DKE	Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE
EBA	Eisenbahn-Bundesamt
EBO	Eisenbahn-Bau- und Betriebsordnung
EN	Europäische Norm
ETA	Event Tree Analysis (dt. Ereignisbaumanalyse)
F/A/S	Fehler/Ausfall/Störung
Fdl	Fahrdienstleiter
FMEA	Ausfalleffektanalyse (engl. failure mode and effects analysis)
FTA	Fault Tree Analysis (dt. Fehlerbaumanalyse)
FV-NE	Fahrdienstvorschrift für Nichtbundeseigene Eisenbahnen
Hp	Hauptsignal(begriff)
HR	Gefährdungsrate (engl. hazard rate)
HSig	Hauptsignal
IEC	Internationale Elektrotechnische Kommission (engl. International Electrotechnical Commission)
IH	Instandhaltung
IHP	Instandhaltungspersonal
ISO	Internationale Normungsorganisation
MGS	Mindestens gleiche Sicherheit
MMI	Mensch-Maschine-Schnittstelle
MSR	Messen, Steuern, Regeln
OKZ	Ordnungskennzahl
PZB	Punktförmige Zugbeeinflussung
RAMS	Reliability, Availability, Maintainability, Safety (dt. Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit, Sicherheit)
RAMS(S)	Reliability, Availability, Maintainability, Safety, Security (dt. Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit, Sicherheit)
RIL 819	Richtlinie 819 (der Deutschen Bahn AG)
Sifa	Sicherheitsfahrschaltung
SIL	Safety Integrity Level (dt. Sicherheitsintegritätsstufe)
Tf	Triebfahrzeugführer
THR	Tolerierbare Gefährdungsrate (engl. Tolerable Hazard Rate)
UIC	Internationaler Eisenbahnverband (franz. Union Internationale des Chemins de Fer)
VDE	Verband der Elektrotechnik Elektronik Informationstechnik e.V.
Zs 1	Ersatzsignal

Bildverzeichnis

Bild 1:	Merkmale des Bahnsystems.....	1
Bild 2:	Phasen des Lebenszyklus eines Systems im V-Diagramm nach [DIN00].....	5
Bild 3:	Zulassungsverfahren von Bahnanlagen nach [VVB03].....	9
Bild 4:	Zusammenhang der RAMS-Komponenten.....	10
Bild 5:	Unterschied zwischen Gefahr und Gefährdung	11
Bild 6:	Gefahr, Gefährdung und Ereignis am Beispiel eines Steinschlages	11
Bild 7:	Todesfälle verschiedener Verkehrsträger im Jahr 2001 gemäß [SCH04].....	17
Bild 8:	Szenario zur Abschätzung des Risikos	19
Bild 9:	Zusammenhang zwischen verschiedenen Risikoarten.....	22
Bild 10:	Effektivität der Risikoreduktion nach [KRO96].....	23
Bild 11:	Risikomatrix nach [DIN00]	25
Bild 12:	Zusammenhang zwischen Grenzrisiko und Restrisiko	25
Bild 13:	Methoden der Instandhaltung nach [DIN03a]	30
Bild 14:	Einordnung der Begriffe Fehler und Ausfall	33
Bild 15:	Fehler, Ausfall und Störung während des Lebenszyklus.....	34
Bild 16:	Kausale Zusammenhänge für organisatorische Fehler nach Reason [REA94]	40
Bild 17:	3-Ebenen-Modell der menschlichen Informationsverarbeitung nach Rasmussen [RAS80].....	42
Bild 18:	Einteilung sicherheitsgefährdender Handlungen nach Reason [REA94]	44
Bild 19:	Badewannenkurve nach [FIS90].....	48
Bild 20:	Stellen potenzieller Anomalien im beliebigen Regelungssystem	51
Bild 21:	Regelkreis des Bahnsystems [PRO07a].....	51
Bild 22:	Zeitliche Zusammenhänge der F/A/S-Offenbarung.....	55
Bild 23:	Vorgehensweise beim Umgang mit F/A/S	57
Bild 24:	Verfügbarkeits-Sicherheits-Diagramm	60
Bild 25:	Einordnung der Systemzustände im Verfügbarkeits-Sicherheits-Diagramm	62
Bild 26:	Systemzustände und Übergänge im Verfügbarkeits-Sicherheits-Diagramm.....	65
Bild 27:	RAMS-Faktoren für Bahnen [DIN00]	68
Bild 28:	Einfluss der Sicherheitsfaktoren Mensch, Technik und Organisation auf RAMS für Bahnen nach [DIN00].....	69
Bild 29:	Modell zur ganzheitlichen Sicherheitsbetrachtung des Bahnsystems.....	72
Bild 30:	Zulassungsverfahren von Bahnanlagen mit betrieblichem Sicherheitsnachweis.....	74

1 Motivation

Schon immer beschäftigen sich Menschen mit dem Thema Sicherheit. Stand zu Beginn der Menschheit vornehmlich der Schutz vor klimatischen Einflüssen, wilden Tieren und Kriegen im Mittelpunkt des Interesses, wandelte sich der Fokus der Betrachtungen mit der Industrialisierung zunehmend. Die Überwindung großer Entfernungen mit Hilfe schneller Verkehrsmittel bedurfte erster Überlegungen hinsichtlich deren Sicherheit. Die entwickelten Technologien und eingesetzten Techniken aller Verkehrsträger funktionieren statistisch betrachtet seither immer besser. Wer in ein Auto, ein Flugzeug oder einen Zug steigt, erwartet, dass er unversehrt an das gewünschte Ziel gelangt. Allerdings nimmt man bewusst oder unbewusst durch deren Nutzung Risiken in Kauf, fordert aber gleichzeitig auch ein Maximum an Sicherheit.

Die Eisenbahn gilt seit ihrer Entstehung zu Beginn des 19. Jahrhunderts als besonders sicheres Verkehrsmittel, vor allem im Vergleich mit dem zu Beginn des 20. Jahrhunderts aufgekommenen Straßenverkehr. Die hohe, vom Gesetzgeber geforderte und vom Kunden erwartete Sicherheit des Bahnsystems fußt vornehmlich auf zwei Faktoren:

- Langer Bremsweg infolge geringer Haftreibung zwischen Stahlrad und Stahlschiene und hoher Geschwindigkeit
- Große Schäden bei einer Kollision durch Umformung der großen kinetischen Energie infolge großer Masse und hoher Geschwindigkeit.

Die langen Bremswege führen dazu, dass nur geringe Möglichkeiten der Gefährdungsabwehr bestehen. Um einen akzeptablen Bremsweg zu erhalten, müsste die Bremsverzögerung derart hoch gewählt werden, dass weder transportierte Personen noch Güter diese Beschleunigungen unbeschadet überstehen würden.

Die große kinetische Energie müsste zudem, wie beim Straßenverkehr, zur Vermeidung großer Schäden ausreichend kompensiert (z. B. durch Verformung) bzw. in andere Energieformen gewandelt werden (z. B. in thermische Energie mittels Reibung). Bild 1 veranschaulicht diesen Zusammenhang.

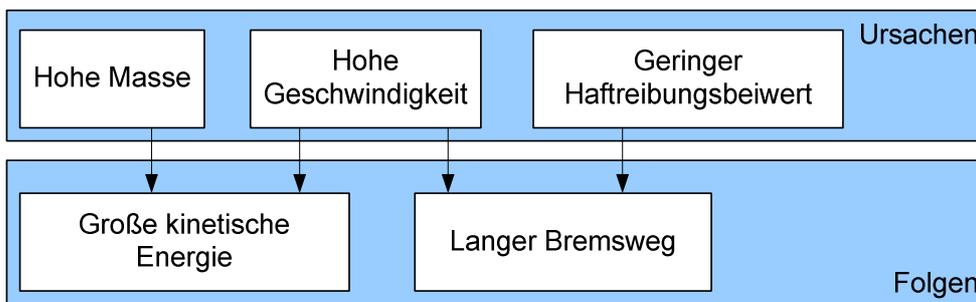


Bild 1: Merkmale des Bahnsystems

Die beiden physikalisch bedingten Merkmale des Verkehrsträgers Eisenbahn haben wesentlichen Einfluss auf dessen Systemgestaltung und sind die entscheidenden Gründe für den hohen technischen und damit meist auch kommerziellen Aufwand, der betrieben wird, um das Bahnsystem sicher zu gestalten.

Sicherungsmaßnahmen im spurgeführten Verkehr dienen insbesondere der Vermeidung von Kollisionen und Entgleisungen und damit dem Schutz von Personen, Gütern und der Umwelt. Daraus erwachsen verschiedene Anforderungen hinsichtlich der Sicherheit aller am Verkehr Beteiligter. Diese bedürfen eines wirtschaftlich tragbaren Grades der Sicherheit entsprechend der gesellschaftlichen Akzeptanz und des individuellen Risikoempfindens des Einzelnen. Grundsätzlich sind alle unzulässigen Risiken für Personen, Güter und die Umwelt auszuschließen, um eine möglichst hohe Sicherheit zu erreichen. Nichtsdestotrotz verbleibt auch bei hohen Anforderungen und Anstrengungen immer ein gewisses Restrisiko, infolge der Benutzung eines Verkehrsmittels verletzt oder sogar getötet zu werden. Betreiber und Hersteller von Eisenbahnen sind daher angehalten, ausreichende Maßnahmen zum Schutz aller Beteiligter zu ergreifen. Die Aufsichtsbehörde wiederum ist verantwortlich, deren Umsetzung zu kontrollieren.

Grundsätzlich wird, und das nicht nur im spurgeführten Verkehr, zwischen aktiver (unfallvorbeugender) und passiver (unfallfolgenmildernder) Sicherheit unterschieden [TRI03]. Die aktive Sicherheit verfolgt dabei das Ziel der Unfallvermeidung durch Ausschluss von Gefährdungen respektive unsicheren Zuständen. Unter dem Begriff *aktive Sicherheit* werden somit Maßnahmen zusammengefasst, die

- Abweichungen vom sicheren Zustand verhindern,
- frühzeitiges Erkennen von Gefährdungen ermöglichen und
- geeignete Reaktionen darauf veranlassen.

Die Erfassung des Zustandes erfolgt über fahrzeug- oder infrastrukturseitige Detektoren. Beim Erreichen bzw. Überschreiten von definierten Schwellwerten (z. B. bezüglich Geschwindigkeit, Achslagertemperatur, Endlage) werden der Triebfahrzeugführer oder andere Stellen (z. B. Fahrdienstleiter) informiert (z. B. akustisch, optisch) und ggf. Reaktionen (z. B. Zwangsbremmung) seitens der Technik erzwungen oder eine Fahrt nicht zugelassen.

Wie die Technik, wird vielfach auch die Einsatzfähigkeit des Menschen überwacht. Die Sicherheitsfahrschaltung (Sifa) überprüft in regelmäßigen Abständen die Wachsamkeit des Triebfahrzeugführers. Reagiert dieser auf ein entsprechendes optisches bzw. akustisches Signal durch Betätigung eines Tasters nicht, erfolgt die Einleitung einer Zwangsbremmung.

Eine zunehmende Bedeutung erlangt hierbei der Einsatz von Telematiksystemen in Fahrzeugen und Anlagen der Infrastruktur. Diese sind zudem in der Lage, Informatio-

nen zu speichern und Hinweise für Wartungstätigkeiten im Rahmen regulärer Inspektionen zur Verfügung zu stellen.

Im Gegensatz zur aktiven Sicherheit ist es das Ziel der *passiven Sicherheit*, im Falle eines Unfalls dessen Folgen zu mindern. Allerdings sind diesem Anliegen im spurgeführten Verkehr aufgrund der bereits dargelegten physikalischen Randbedingungen Grenzen gesetzt. Im Straßenverkehr mit der begrenzten Einflussnahme auf den Fahrer hingegen ist das Mittel der passiven Sicherheit sehr weit verbreitet. Beispiele dafür bieten Komponenten wie Airbag, Seitenaufprallschutz, Sicherheitsgurt, Überrollbügel oder Helm.

Im täglichen Umgang mit verkehrlichen Anlagen, wie Kraftfahrzeugen, Lichtzeichenanlagen oder Bahnübergängen, gehen wir von deren zuverlässigen und sicheren Funktionalität aus. Aufgrund von bisherigen Erfahrungen vertrauen wir den ihnen innewohnenden Sicherheitsprinzipien. Dabei ist der „normale Bereich“ im Funktionsspektrum eines Systems aber häufig nur ein schmales Band. Der Fehlerbereich ist dagegen der große Rest. Um das System in diesem schmalen Band zu halten, muss die Regelung bzw. Steuerung je nach Eigenschaften und Umgebungsbedingungen des Systems kontinuierlich gewährleistet sein. Eine kurze Unterbrechung oder eine kleine Anomalie kann bereits zu Unfällen führen. Um dieses zu verhindern, müssen für alle denkbaren Anomalien geeignete Lösungen gefunden werden. Alles was nicht vor(her)gesehen wurde, stellt eine latente Gefahr dar. Die zentrale Aufgabe besteht somit darin, Antworten auf die Frage zu finden, was alles geschehen kann.

Allerdings gestaltet sich die Ermittlung der Antworten sehr schwierig, da das Bahnsystem von jeher ein komplexes Gefüge darstellt. Heute ist es mehr denn je durch den Einsatz unterschiedlicher Techniken (z. B. Außenanlagen, Stellwerken, Fahrzeugen, Instandhaltungswerkzeugen) von verschiedenen Herstellern und einer zunehmenden Anzahl an Bahnbetreibern sowie der Beteiligung vieler Personen (z. B. Reisende, Bahnbedienstete, Dritte) mit unterschiedlichen Erwartungen und Vorstellungen geprägt. Das Zusammenspiel von Technik und Mensch wird dabei von verschiedenen Randbedingungen (z. B. Regelwerken, Organisationsstrukturen, Betriebsverfahren, Umgebungsbedingungen) beeinflusst und nicht zuletzt prägen die bereits zu Beginn beschriebenen physikalischen Merkmale das Bahnsystem.

Im Rahmen dieser Arbeit wird der Begriff *Sicherheit* aus verschiedenen Blickwinkeln beleuchtet, Randbedingungen aus Theorie und Praxis zielorientiert strukturiert und Lösungen für einen verantwortungsvollen Umgang mit der Sicherheit dargelegt. Dazu werden in Kapitel 2 zunächst die normativ verankerten Lebenszyklusphasen des Bahnsystems und die darin verankerten Verantwortlichkeiten vorgestellt. Kapitel 3 leitet im

Anschluss daran den kausalen Zusammenhang des risikoorientierten Sicherheitsbegriffs her. Daran schließen sich in Kapitel 4 ein Vorschlag zur inhaltlichen Unterscheidung zwischen Fehlern, Ausfällen und Störungen und in Kapitel 5 die Beschreibung vom Umgang mit diesen im Bahnsystem an. Kapitel 5 endet mit der beispielhaften Beschreibung einer neuen Analyseverfahren in Verfügbarkeits-Sicherheits-Diagrammen für Szenarien des Bahnsystems. Das in Kapitel 6 entwickelte Modell zur ganzheitlichen Sicherheitsbetrachtung des Bahnsystems integriert abschließend die zuvor gewonnenen Erkenntnisse.

2 Grundlagen zur Sicherheit

2.1 Rechtliche Grundlagen

Grundsätzlich ist davon auszugehen, dass jede technische Komponente irgendwann ausfallen wird, jeder am Prozess Beteiligte einen Fehler machen kann und aus der Systemumgebung Störungen auftreten können. Umso wichtiger ist daher, dass sich alle Beteiligten in den verschiedenen Lebenszyklusphasen eines Systems (vgl. Bild 2) auf *Regelwerke* berufen und sich dieser bedienen können.

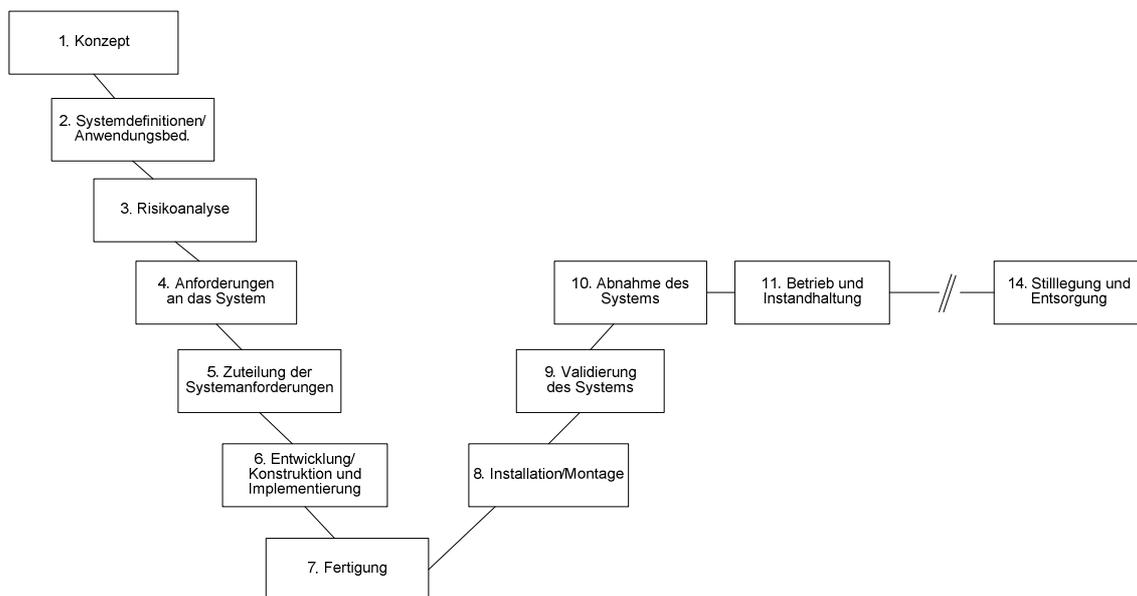


Bild 2: Phasen des Lebenszyklus eines Systems im V-Diagramm nach [DIN00]

Im Sinne einer Betrachtung vom Allgemeinen zum Speziellen werden nachfolgend wesentliche, die Sicherheit betreffende Regelwerke sowohl auf nationaler als auch internationaler Ebene geordnet.

Die oberste und damit sehr abstrakte Ebene in der Vielzahl der Regelwerke bilden die hoheitlich entstandenen *Rechtsnormen*. Diese, unterteilt in Gesetze (z. B. AEG, [AEG93]) und Rechtsverordnungen (z. B. EBO, [EBO67]), enthalten in den seltensten Fällen konkrete Handlungsanweisungen dahingehend, wie die erforderliche Sicherheit im Einzelfall zu gewährleisten ist. Zu diesem Zweck werden von verschiedensten Institutionen *Normen* (z. B. DIN EN 50126, [DIN00]) und *normative Vorschriften* (z. B. FV-NE, [FVN84]) erarbeitet, um die jeweils gültigen Gesetze und Rechtsverordnungen zu ergänzen und zu konkretisieren. Der Eisenbahningenieur greift in der Praxis auf *Regelwerke der Eisenbahn* (z. B. RIL 819, [RIL06]) zurück, um die erforderliche Sicherheit im Bahnsystem zu gewährleisten und den *anerkannten Regeln der Technik* zu entsprechen.

2.2 Nachweis von Sicherheit

2.2.1 Anforderungen

Bevor eine neue Technologie unter Sicherheitsverantwortung eingesetzt werden darf, muss die Einhaltung der Sicherheitsbedingungen nachgewiesen werden. Diese Bedingungen, auch Schutzziele genannt, resultieren aus hoheitlich vorgeschriebenen Forderungen hinsichtlich der Sicherheit. Wie bereits im vorherigen Abschnitt dargestellt wurde, dient eine Hierarchie von Regelwerken zu deren Einhaltung. Damit soll der Gefahr begegnet werden, dass es bei Abweichung eines technischen Systems von den festgeschriebenen Anforderungen zur Einnahme ungewollter Systemzustände kommen kann. Daraus können zwei übergeordnete Anforderungen an (technische) Systeme im Allgemeinen und das Bahnsystem im Speziellen abgeleitet werden [BÖR04], [GRA02], [MON99]:

- Keine Person, die durch das zu beurteilende System potenziell gefährdet ist, trägt ein vergleichsweise höheres Risiko.
- Alle Sicherheitsmaßnahmen sind getroffen worden, die als verhältnismäßig bezeichnet werden können.

Die erste Forderung zielt in Richtung der Analyse von Gefährdungen und der ihnen zugeordneten Risiken im Rahmen einer Risikoanalyse. Der zweite Gedanke fordert, dass (aufbauend auf der Risikoanalyse) Maßnahmen ergriffen werden, die dazu führen, das analysierte Risiko zu begrenzen und, falls es als zu hoch eingestuft wurde, zu verringern.

2.2.2 Aufgaben

Die Weiterentwicklung der Eisenbahn und deren Sicherung waren besonders in den Anfängen überwiegend empirischen Ursprungs. Immer wieder kam es zu Ereignissen, aus denen Schlussfolgerungen gezogen und Erkenntnisse zur Erhöhung der Sicherheit des Bahnsystems gewonnen wurden. Diese Aktivitäten mündeten zumeist als betriebliche Festlegungen in Regelwerken der Eisenbahn oder in technischen Neuerungen (z. B. Isolierte Schiene). Die Ingenieure wurden somit sprichwörtlich aus Schäden klüger und mithin das System nach und nach immer sicherer, aber auch komplexer. Damit stieg auch die Zahl der möglichen Schutzmaßnahmen gegen Gefährdungen wie Kollisionen und Entgleisungen. Allerdings wurden diese Erfahrungen z. T. mit schweren Unfällen erkaufte.

In der heutigen Zeit gibt man sich mit einer derartigen reaktiven Vorgehensweise nicht zufrieden. Unfälle werden im Bahnsystem, anders als im Straßenverkehr, nicht akzeptiert. Das Prinzip der aktiven Sicherheit im Bahnsystem verfolgt das Ziel der Vermeidung

derung von Unfällen. Denn das mit Unfällen meist einhergehende hohe Schadensausmaß infolge der physikalischen Randbedingungen (vgl. Bild 1) erfordert die Entwicklung eines vorausschauenden Sicherheitsdenkens. Diese proaktiven Maßnahmen können allerdings nur in geeigneter Weise entwickelt werden, wenn ausreichende Kenntnis über das Sicherheitsniveau vorhandener und geplanter Komponenten bzw. Systeme besteht.

Grundlage und Voraussetzung für die Strategie der aktiven Sicherheit bilden folgende Kriterien:

- Qualität der Sicherheitsstrategie
- Kompetenz und Motivation der Mitarbeiter
- Stand der technischen Entwicklung
- Einsatz finanzieller Mittel

Besonders der letzte Gedanke erzeugt oftmals ein Spannungsfeld. Viele Maßnahmen bieten zwar einen wirksamen Schutz vor potenziellen Gefährdungen (z. B. Umzäunung/Einhausung von Bahnanlagen, Ersatz von Bahnübergängen durch Brücken oder Unterführungen), erfordern aber gleichzeitig einen enormen finanziellen Aufwand.

Wesentliche Aufgaben der Sicherheitsverantwortlichen sind es, interne und externe Einflüsse auf das System zu erkennen, die Erfordernis von Maßnahmen zur Senkung des vom System ausgehenden Risikos darzulegen und deren Umsetzung gegen unternehmensinterne und externe Widerstände zu verteidigen. Grundsätzlich wird dabei zwischen unbekanntem Risiken, die meist aus Kosten- und Zeitdruck unbekannt bleiben, und bekannten Risiken, die aus Kostengründen bewusst eingegangen werden, unterschieden. Zielstellung einer Sicherheitsstrategie muss es daher vor allem sein, finanzielle Mittel in dem Bereich bereitzustellen, wo sich nachweislich das höchste im System verbliebene Risiko befindet (vgl. Bild 10).

Methodisch wird dabei auf den analytischen Nachweis der Sicherheit zurückgegriffen. Dies wird meist durch Prüfung der sicherheitsrelevanten Funktionen der Komponenten in Teilsystemen bzw. im Gesamtsystem sowie umfangreichen Tests begleitet. Das eigentliche Ergebnis der Sicherheitsanalyse mündet im als „Sicherheitsnachweis“ bezeichneten Dokument. Die Aufgabe des analytischen Nachweises der Sicherheit besteht somit in der Bereitstellung eines ausreichenden Sicherheitsniveaus und dessen Durchsetzung entgegen vorhandener, meist finanzieller Widerstände.

Im Mittelpunkt der Sicherheitsbetrachtung steht nicht zwingend die Bestimmung des absoluten Gesamtrisikos, sondern die Optimierung des sicherheitsgerichteten Aufwandes und der Festlegung des Grenzniveaus (vgl. Abschnitt 3.6.4). Diese Aufgabe mündet

in der Diskussion, wie viel Risiko es zu reduzieren bedarf und welches im System verbliebenes Risiko als akzeptabel bewertet werden kann (vgl. Bild 12).

2.2.3 Aufgabenverteilung

Die für Sicherheitsanalysen wichtige DIN EN 50129 schlägt eine Rollenverteilung für die im Bahnsystem beteiligten Akteure vor. Die Aufgaben sind unterteilt in zwei wesentliche Teile [DIN03b]:

- die Risikoanalyse, mit der die tolerierbaren Gefährdungsraten (THR)¹ unter Beachtung von Risikoakzeptanzkriterien für sicherheitsrelevante Kernfunktionen des Systems vom Betreiber vorgegeben werden und
- die Gefährdungsanalyse², in der vom Hersteller nachgewiesen werden muss, dass er die durch die Risikoanalyse geforderten Vorgaben realisiert und eingehalten hat.

Eine kompakte Beschreibung der konkreten Aufgaben bei der Risikoanalyse durch den Betreiber bzw. bei der Gefährdungsanalyse durch den Hersteller befindet sich in [BRA05b].

Die Sicherheitsanalyse soll möglichst schon bei der Systemkonzeption beginnen. Sie stellt aber keinen Prozess dar, der nur zu Beginn oder zu einem speziellen Zeitpunkt im Verlauf der Systementwicklung stattfindet und dann abgeschlossen ist, sondern während des gesamten Entwicklungsprozesses weitergeführt wird. Jede Entwicklungsphase bringt neue Erkenntnisse hinsichtlich des Systemverhaltens und ermöglicht es dadurch, weitere Gefährdungen zu identifizieren. Deshalb begleitet die Sicherheitsanalyse alle Entwicklungsphasen im Lebenszyklus.

Die sowohl auf nationaler als auch auf internationaler Ebene vorgegebenen Abläufe im Rahmen der Zulassung bzw. des Nachweises der Sicherheit einerseits und der daraus erwachsenden Aufgaben für die am Prozess der Sicherheitsanalyse Beteiligten andererseits können, wie in Bild 3 dargestellt, zusammengefasst werden.

¹ Die THR stellte eine quantitative Kenngröße zur Beschreibung der Häufigkeit des gefährlichen Ausfalls der betreffenden Sicherungsfunktion dar.

² Diese wird in der aktuellen deutschsprachigen Übersetzung der normativen Anlage A der EN 50129 als „Gefährdungsbeherrschung“ bezeichnet.

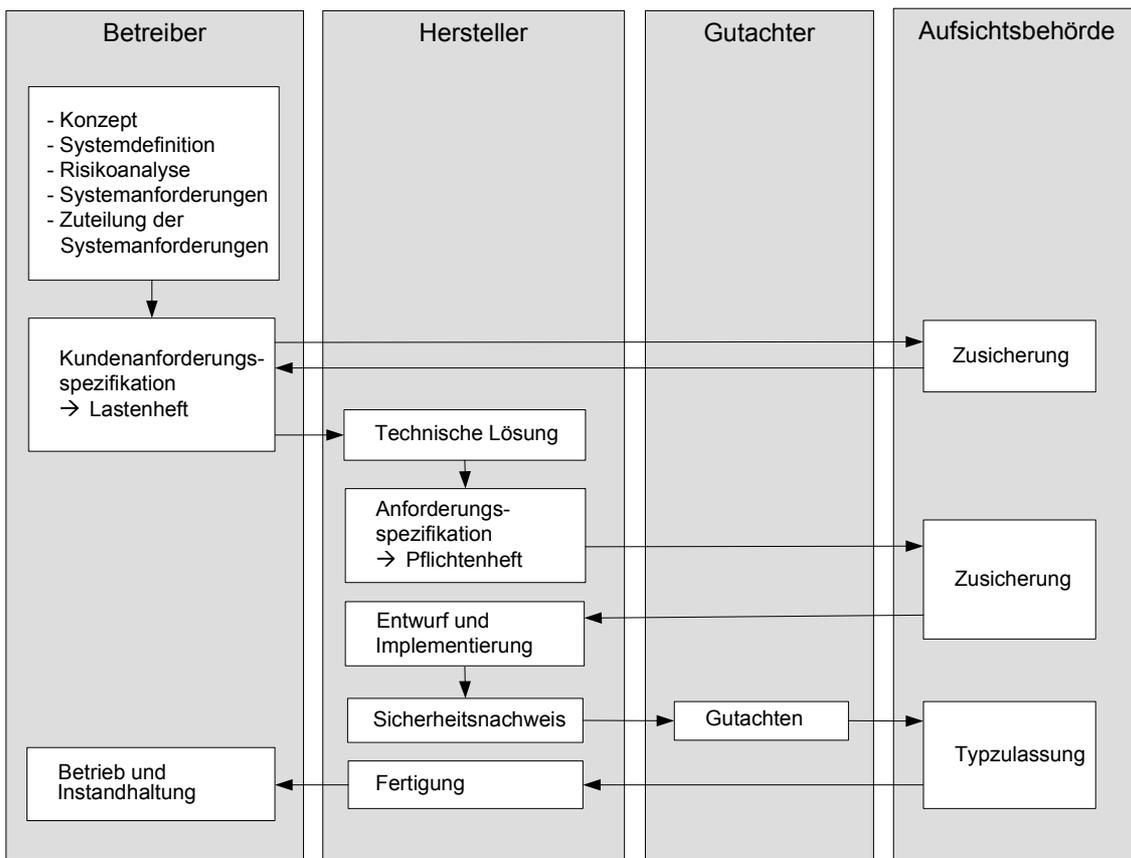


Bild 3: Zulassungsverfahren von Bahnanlagen nach [VVB03]

Die in Bild 3 dargestellte Vorgehensweise wird anhand des Systems „Bahnübergang“ in [BRA06] beispielhaft und ausführlich erläutert. Auf eine detaillierte Beschreibung wird im Rahmen dieser Arbeit verzichtet.

3 Herleitung des risikoorientierten Sicherheitsbegriffs

Bevor anhand spezieller Methoden beispielhaft die Vorgehensweise bei einer Risikoanalyse aufgezeigt wird, soll zunächst der Zusammenhang zwischen den Begriffen *Risiko* und *Sicherheit* einerseits und dem Begriff RAMS als Akronym für *Zuverlässigkeit*, *Verfügbarkeit*, *Instandhaltbarkeit* und *Sicherheit* andererseits erläutert werden. Die für Sicherheitsbetrachtungen wesentlichen Begrifflichkeiten werden in diesem Kapitel erläutert und ihr Zusammenspiel hergeleitet. Zur besseren Nachvollziehbarkeit wird in den nachfolgenden Abschnitten auf die Ordnungskennzahlen (OKZ) 1 bis 9 aus Bild 4 zurückgegriffen.

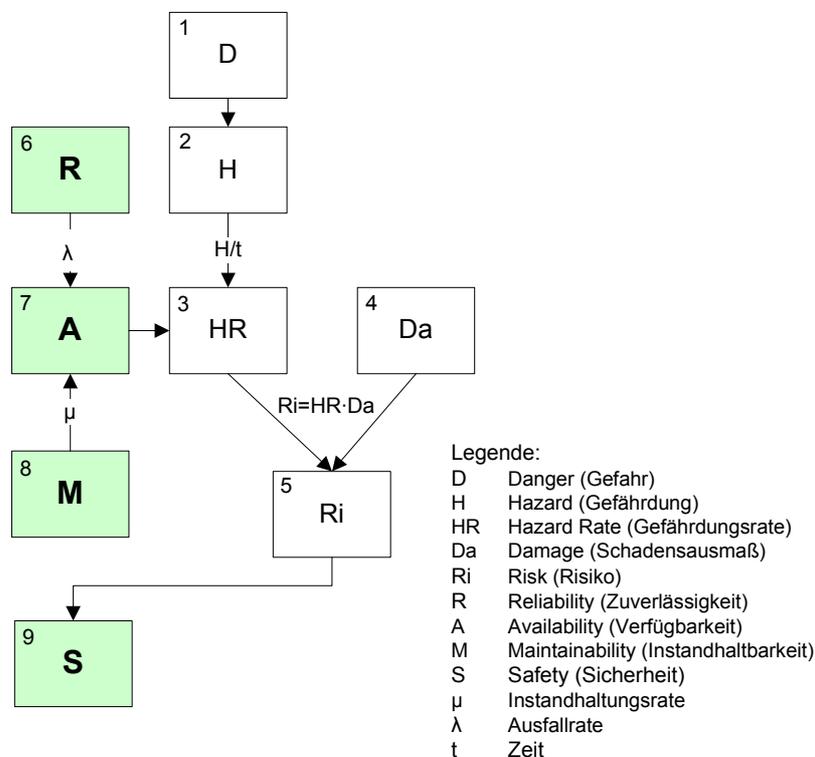


Bild 4: Zusammenhang der RAMS-Komponenten

3.1 Gefahr und Gefährdung

Für das Auslösen eines Ereignisses bedarf es zunächst einer Gefahr (vgl. OKZ 1 in Bild 4), die in DIN EN 50126 wie folgt definiert ist:

„Eine physikalische Situation, die potenziell einen Schaden für den Menschen beinhaltet.“ [DIN00]

Eine Gefahr wird dabei mit etwas *Potenziellem* (Quelle, Situation) verbunden. Ein Steinschlag fern jeglicher Zivilisation (vgl. Bild 6) kann als eine solche Gefahr verstan-

den werden. Solange sich in ihrer Reichweite keine schutzwürdigen Ziele befinden, bleibt sie lediglich eine potenzielle Gefahr.

Sobald sich die Gefahr aber auf Personen, Güter oder die Umwelt konkretisiert, wird sie zur Gefährdung für diese schutzwürdigen Ziele. In DIN EN 50129 findet sich eine diesbezügliche Definition für eine Gefährdung:

„Bedingung, die zu einem Unfall führen kann.“ [DIN03b]

Eine Gefährdung (vgl. OKZ 2 in Bild 4) wird somit mit etwas *Konkretem* (Bedingung, Umstand) verbunden, bei dem zur Gefahr der/das Gefährdete hinzutritt, die Gefahr sich also auf Personen, Güter oder die Umwelt konkretisiert. Bild 5 soll dies anhand einer im Erdreich befindlichen Fliegerbombe verdeutlichen. Solange niemand auf diese Bombe stößt (z. B. durch Erdarbeiten beim Bau einer Bahntrasse), stellt sie lediglich eine potenzielle Gefahr dar. Sollte aber ein Bagger mit ihr in Berührung kommen, konkretisiert sich die Gefahr auf diesen, dessen Fahrer und die nähere Umgebung.

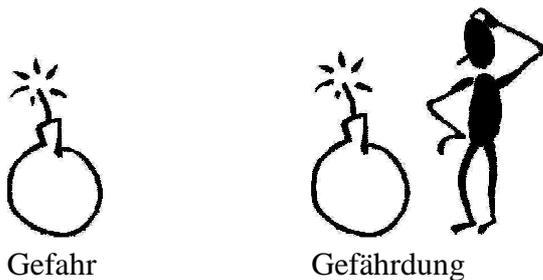


Bild 5: Unterschied zwischen Gefahr und Gefährdung

Genauso wird im Beispiel des bereits erwähnten Steinschlages dieser zur Gefährdung, falls sich eine Bahnstrecke in dessen Nähe befindet (vgl. Bild 6), die dann durch Geröll unbefahrbar wird.

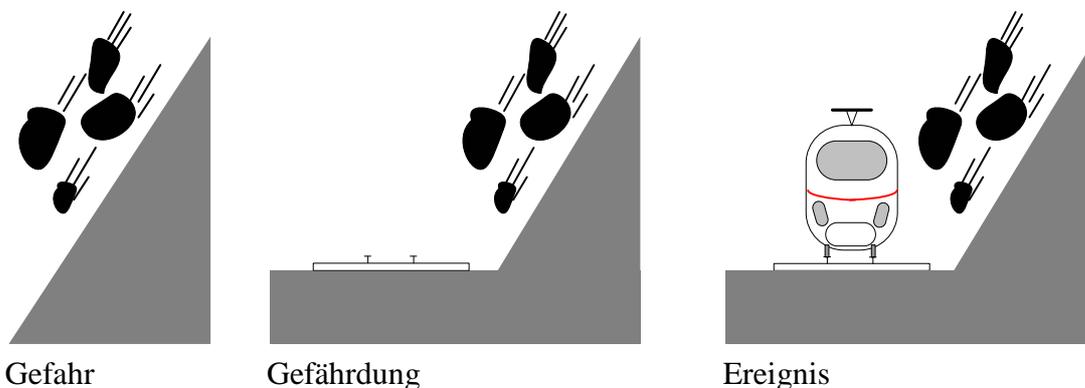


Bild 6: Gefahr, Gefährdung und Ereignis am Beispiel eines Steinschlages

Diese Unterscheidung zwischen Gefahr und Gefährdung deckt sich zudem mit folgender Definition des Begriffs *Gefährdung*:

„Eine Gefährdung ist ein Objekt, eine Bedingung oder ein Zustand, das/die/der zu einem Unfall führen könnte. In Zusammenhang mit der Systemsicherheit ist eine Gefährdung ein ungesicherter Zustand des Systems, der unter bestimmten äußeren Bedingungen zu einem Unfall führt.“ [BRA99]

An dieser Stelle wird ausdrücklich darauf hingewiesen, dass vielfach keine Unterscheidung zwischen den Begriffen *Gefahr* und *Gefährdung* erfolgt und zudem, oftmals aus Übersetzungsfehlern resultierend, auch widersprüchliche Aussagen im Schrifttum gemacht werden. Die falschen Übersetzungen von *failure* (dt. *Ausfall*) als „Fehler“, *dependability* (dt. *Verlässlichkeit*) als „Zuverlässigkeit“ oder *reliability* (dt. *Zuverlässigkeit*) als „Funktionsfähigkeit“ stellen nur einige Beispiele dar.

3.2 Identifikation von Gefährdungen

Ein Grundsatz bei der Entwicklung sicherheitsrelevanter Systeme besteht darin, dass Systemanomalien, mit denen zu rechnen ist, sich nicht gefährlich auswirken dürfen. Für die Gewährleistung dieser Forderung ist es erforderlich, möglichst alle potenziellen Gefahren und die daraus resultierenden Gefährdungen vor Inbetriebnahme des Systems zu identifizieren. Hierfür bedient man sich folgender Strategie::

- Vorwärts- bzw. Rückwärts-Suche [MON99]

Vorwärts-Suche bedeutet, dass von einem auslösenden Ereignis ausgegangen und dabei versucht wird, dessen Folgen herauszufinden. Diese zeitlich in die Zukunft („vorwärts“) gerichtete Tätigkeit wird auch als induktive Suche bezeichnet. Der durch das auslösende Ereignis erreichte Zustand kann wiederum eine Wirkung hervorrufen, d. h. ein neues Ereignis auslösen und möglicherweise indirekt zu einem gefährlichen Zustand führen. Bei der Vorwärts-Suche wird von einem auslösenden Ereignis ausgegangen und als Ergebnis werden meist mehrere Endzustände erhalten. Diese Strategie ist geprägt von der Frage:

- Was passiert, wenn das Ereignis A eintritt?

Zur systematischen Beantwortung dieser Frage bedient man sich standardisierter Methoden. Ein Beispiel für Vorwärts-Suche ist die Ereignisbaumanalyse (ETA³). Detaillierte Beschreibungen zur ETA befinden sich in [DIN85].

Die Rückwärts-Suche wird auch als deduktive Suche bezeichnet. Bei dieser Strategie wird von gefährlichen Zuständen ausgegangen und versucht, den Grund dafür zu finden. Man schaut also zeitlich gesehen in die Vergangenheit („rückwärts“). Bei der Rück-

³ Event Tree Analysis

wärts-Suche wird folglich von einem Endzustand ausgegangen und mehrere auslösende Ereignisse als Ergebnis erhalten. Diese Strategie ist geprägt von der Frage:

- Was ist die Ursache für Zustand A?

Eine standardisierte Methode für Rückwärts-Suche ist die Fehlerbaumanalyse (FTA⁴). Detaillierte Beschreibungen zur FTA befinden sich in [DIN81] bzw. [DIN93].

Welche Methode Anwendung findet, hängt davon ab, ob die Ursachen für eine bestimmte Gefährdung im Fokus der Untersuchungen stehen oder ob die Folgen eines bestimmten Ausfalls ermittelt werden sollen. Eine vielfach verwendete Methode, die die Vorwärts- bzw. Rückwärts-Suche miteinander verknüpft, ist die FMEA⁵. Dabei werden sowohl Ausfallursachen als auch die daraus entstehenden Ereignisse analysiert. Detaillierte Beschreibungen zur FMEA befinden sich in [DIN95b], [DIN06].

Andere, eher systemorientierte Vorgehensweisen zur Identifikation von Gefährdung münden in folgender Klassifizierung:

- Top-Down-Analyse bzw.
- Bottom-Up-Analyse [MON99]

Die Bottom-Up-Analyse beginnt bei einem Ausfall in einer Komponente und untersucht, welche übergeordneten Teilsysteme dadurch betroffen werden. Die Top-Down-Analyse hingegen zerlegt ein Gesamtsystem gemäß der Architektur in seine Teilsysteme und Komponenten und bestimmt die Ausfallursachen in diesen.

Beide Strategien haben Vor- und Nachteile. Die Bottom-Up-Analyse stößt sehr schnell an Grenzen hinsichtlich des zeitlichen und finanziellen Aufwandes, wenn alle Komponenten im System untersucht werden sollen. Außerdem bietet sie keine Unterstützung bei der Untersuchung von Ausfallkombinationen. Bei der Top-Down-Analyse läuft man Gefahr, das System zu oberflächlich zu betrachten oder die erforderliche Analysetiefe aus Aufwandsgründen nicht zu erreichen.

In der Praxis haben sich daher Kombinationen von Analysemethoden bewährt, die verschiedene Blickrichtungen auf das System und die darin befindlichen Gefährdungen ermöglichen. Auf Grund der Vielzahl an Analysemethoden wird im Rahmen dieser Arbeit auf deren Beschreibung verzichtet, zumal viele der standardisierten Methoden normativ verankert sind [DIN00], [DIN01a], [DIN02], [DIN03b].

Die Methoden zur Identifikation von Gefährdungen stellen übrigens kein Mittel dar, das nur zu Beginn oder zu einem bestimmten Zeitpunkt der Systementwicklung wirkt.

⁴ Fault Tree Analysis

⁵ Failure Mode and Effects Analysis

Vielmehr erfolgt deren Anwendung während des gesamten Lebenszyklus. Jede Lebenszyklusphase liefert neue Erkenntnisse über das System, wodurch neue Gefährdungen ermittelt werden können. Gefährdungen werden jedoch auch durch neue, unerwartete und unbekannte Situationen hervorgerufen. Der Sturz eines Traktors vom Weinberg auf die Bahntrasse bei Efringen-Kirchen in der Nähe von Freiburg im Jahr 2004 stellt ein solches Beispiel dar.

Großes Potenzial für das Auffinden und Schließen von Sicherheitslücken bietet neben der strukturierten Analyse technischer Faktoren die analytische Betrachtung von betrieblichen Abläufen sowohl während der Entwicklung des Systems als auch nach dessen Inbetriebnahme. Nach Ansicht des Autors fließen die beim Einsatz des Systems durch das Bahnpersonal gesammelten Erfahrungen bisher nur ungenügend in die Sicherheitsbetrachtungen ein, was auch in der fehlenden Rückkopplung von der Systemphase „Betrieb und Instandhaltung“ auf frühe Phasen im Lebenszyklus von Bahnsystemen (vgl. Bild 2) gut zu erkennen ist. Als Folge dessen dienen „Betreiberhinweise“ in der Praxis gelegentlich als „Papierverschluss“ und sollen nichttechnischen Schutz vor erkannten Gefährdungen bieten, die erst nach Inbetriebnahme des Systems offenbar wurden. Allerdings birgt gerade die Verlagerung der Sicherheitsverantwortung auf den Menschen ein erhöhtes Gefahrenpotenzial (vgl. Abschnitt 4.4.4 und 5.3.2). Frühzeitige Betrachtung und Beachtung von betrieblichen Prozessen kann diese Sicherheitslücke schließen (vgl. 6.4).

3.3 Gefährdungsrate

Wird der Fokus auf die Häufigkeit gelenkt, mit der eine bestimmte Gefährdung auftritt, ergibt sich daraus die Gefährdungsrate (vgl. OKZ 3 in Bild 4). Diese beschreibt die Anzahl der Gefährdungen pro Zeiteinheit. Ein prominentes Beispiel für Gefährdungsrate liefert die im Rahmen von Risikoanalysen ermittelte tolerierbare Gefährdungsrate (THR) [DIN03b]. Sie stellt die zulässige Gefährdungsrate bei quantifizierbaren Sicherheitszielen dar [BRA06].

3.4 Schadensausmaß

Zur Ermittlung des Schadensausmaßes (vgl. OKZ 4 in Bild 4) greift man auf die vor Schäden zu schützenden Ziele zurück. Diese schutzwürdigen Ziele sind Personen, Güter sowie die Umwelt. Nachfolgend werden die daraus abgeleiteten Schadenskategorien genannt [PRO07b]:

- Personenschäden (z. B. Tote, Schwerverletzte, Leichtverletzte, Evakuierte)
- Sachschäden (z. B. Bahninfrastruktur, Fahrzeuge, Betriebsstörungen, Betriebsunterbrechungen, Dritte)

- Umweltschäden (z. B. Boden, Gewässer, Grundwasser, Luft)

Zur Einordnung der Schäden bedarf es ihrer Gewichtung. Im Rahmen von Analysen im Bahnbereich wird zur Bezifferung der Personenschäden oft auf die einfache Formel [UIC02]:

$$\text{Opfer} = \text{Tote} + \frac{1}{10} \text{Schwerverletzte} + \frac{1}{100} \text{Leichtverletzte} \quad \text{Formel 1}$$

zurückgegriffen. Im Gegensatz zur Versicherungsbranche setzt sich im Bahnbereich die Monetarisierung von Schäden nur zögerlich durch. Im angelsächsischen Raum hingegen erfolgt diese Form der „Schadensübersetzung“ bereits längere Zeit [BRA05b]. Diese Tatsache rührt vor allem aus der Verwendung des monetär geprägten Risikoakzeptanzkriteriums ALARP⁶, bei dem das zulässige Risiko „so niedrig wie vernünftigerweise praktikabel“ festzulegen ist (vgl. 3.6.4).

3.5 Risiko

Die Kategorisierung und Bewertung von Gefährdungen ist grundsätzlich von zwei Parametern abhängig, einerseits von der Häufigkeit des Auftretens einer Gefährdung, der Gefährdungsrate (vgl. OKZ 3 in Bild 4), und andererseits von deren Schwere in der Auswirkung, dem Schadensausmaß (vgl. OKZ 4 in Bild 4). Durch diese beiden Faktoren kann das für eine bestimmte Gefährdung geltende Risiko (vgl. OKZ 5 in Bild 4) ermittelt werden.

Das Risiko kann als das Produkt der Wahrscheinlichkeit eines Schadensereignisses und des im Ereignisfall zu erwartenden Schadensausmaßes verstanden werden. Die beiden nachfolgenden Definitionen unterstreichen diese Aussage:

„Risiko ist die Wahrscheinlichkeit des Auftretens einer Gefahr, die einen Schaden verursacht, sowie der Schweregrad eines Schadens.“ [DIN00]

„Risiko ist die Kombination aus der Wahrscheinlichkeit, mit der ein Schaden auftritt, und dem Ausmaß dieses Schadens.“ [DIN02]

In aktuellen Regelwerken (z. B. [DIN01a], [DIN03b]) befinden sich weitere Definitionen des Risikos. Wenn sie auch einen durchaus unterschiedlichen Wortlaut haben, ähneln sich fast alle Definitionen dahingehend, dass sie die Begriffe *Risiko*, *Wahrscheinlichkeit* und *Schaden* vereinigen. Die mathematische Kurzfassung dieses Zusammenhangs lautet:

$$Ri_w = w \cdot Da \quad \text{Formel 2}$$

Ri_w Risiko (bezogen auf Wahrscheinlichkeit)

w Wahrscheinlichkeit

Da Schadensausmaß (engl. damage)

An dieser Stelle soll besonders darauf hingewiesen werden, dass ein Risiko meist einen Zeitbezug erfordert. Durch diesen wird festgelegt, über welchen Zeitraum hinweg das Risiko wirkt(e). Mathematisch führt dieser Zusammenhang zum Übergang von der Wahrscheinlichkeit zur Häufigkeit und damit zu einer Rate. Dementsprechend wird bei Berechnungen im weiteren Verlauf der Arbeit folgende sehr wichtige Formel verwendet (vgl. Bild 4):

$$R_i = HR \cdot Da$$

Formel 3

Ri Risiko

HR Gefährdungsrate (engl. hazard rate)

Da Schadensausmaß (engl. damage)

Da der Begriff *Risiko* den Kern aktueller Sicherheitsanalysen bildet, werden im nachfolgenden Abschnitt verschiedene Arten von Risiken vorgestellt und deren Bedeutung für die Sicherheit im Bahnsystem erläutert.

3.6 Risikoarten

3.6.1 Natürliches und technisches Risiko

Natürliche Risiken beziehen sich auf Naturkatastrophen ausgehend von Schneestürmen, Hagel, Dürren, Überschwemmungen, Wirbelstürmen, Vulkanausbrüchen, Erdbeben oder Meteoriteneinschlägen. Bei Letzteren kann aus Statistiken ermittelt werden, dass die Erde ca. 20.000 Meteoriten pro Jahr ausgesetzt ist [KRO00]. Allerdings sind die tatsächlichen Erfahrungen des Auftreffens von Meteoriten auf der Erde sehr gering. Dies liegt darin begründet, dass es sich hierbei vornehmlich um sehr kleine Meteoriten handelt und der Einschlag eines großen Meteoriten ein Ereignis mit einer sehr geringen Wahrscheinlichkeit darstellt. Dieses hat im Fall eines Eintrittes allerdings sehr große Konsequenzen. Ein Beispiel dafür liefert die Permian Katastrophe. Innerhalb von 100.000 Jahren starben dabei auf der Erde zwischen 50% und 90% aller biologischen Arten aus [KRO00].

Andererseits gibt es technische Risiken mit außergewöhnlich geringen Eintrittswahrscheinlichkeiten, aber großen Schäden. Als Beispiel sei hier der Tod durch einen Flugzeugabsturz genannt. Gemäß [ICA06] stürzten im Zeitraum von 1987 bis 2006 weltweit 429 Passagiermaschinen mit mehr als 2.250 kg im Linienverkehr ab, bei denen insgesamt 15.061 Fluggäste starben. Pro Jahr ergeben sich damit etwa 21 derartige Flugzeugabstürze mit rund 753 Toten. Dieses hoch erscheinende jährliche Schadensausmaß rela-

⁶ As Low As Reasonably Practicable

tiviert sich allerdings, wenn die Anzahl der jährlich zurückgelegten Passagierkilometer einfließt. Damit ergibt sich ein durchschnittliches Risiko von jährlich 0,33 getöteten Fluggästen pro Mrd. Passagierkilometern. In [SCH04] wird für das Jahr 2001 ein Wert von 0,43 getöteten Fluggästen pro Mrd. Personenkilometern angegeben (vgl. Bild 7). Gemäß dieser Statistik kann das Bahnsystem mit 0,23 getöteten Fahrgästen pro Mrd. Personenkilometern als der sicherste Verkehrsträger betrachtet werden.

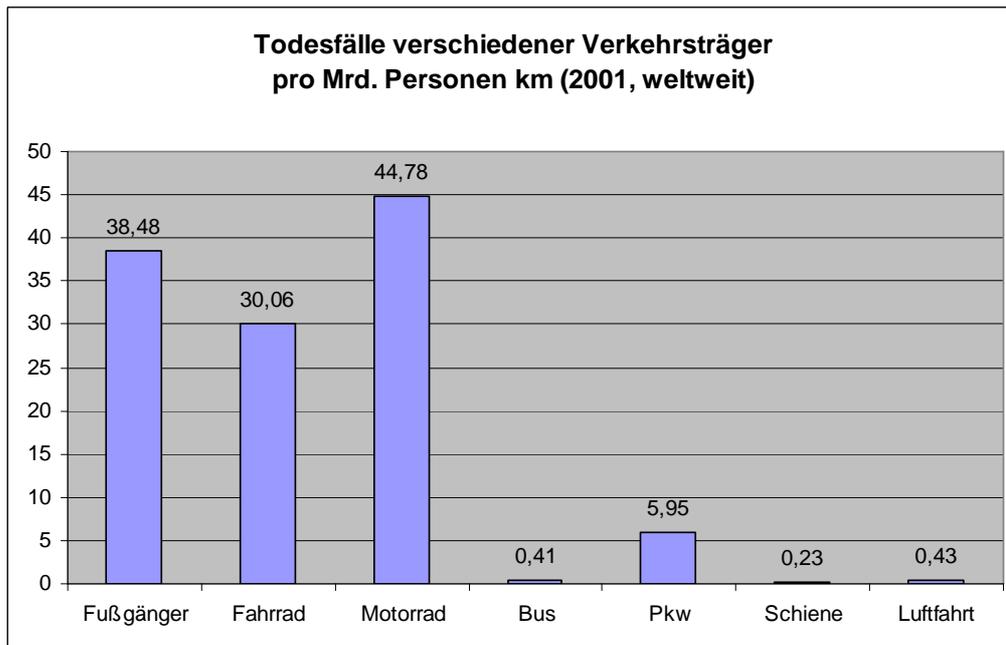


Bild 7: Todesfälle verschiedener Verkehrsträger im Jahr 2001 gemäß [SCH04]

3.6.2 Subjektives und objektives Risiko

Allgemein kann das Risiko als die Quantifizierung der Angst vor einem möglichen Schaden und folglich als Indikator für die Entstehung eines Schadens aus einem Zustand bzw. Vorgang verstanden werden. Die Angst steigt dabei mit der zu erwartenden Höhe des Schadens. Diese Tatsache wird auch als Risikoaversion bezeichnet. Mathematisch wird das subjektiv empfundene Risiko als der Erwartungswert des subjektiven Schadens verstanden[GRA02]:

$$Ri_s = w \cdot s(Da)$$

Formel 4

- Ri_s subjektives Risiko
- w Wahrscheinlichkeit
- Da Schadensausmaß (engl. damage)
- s(Da) Schwere (engl. severity) als Funktion von Da

Die in obiger Formel genannte subjektive Bewertungsfunktion s für die Schwere von Schäden ist abhängig von Wertvorstellungen, sozialen Beziehungen verschiedener gesellschaftlicher Gruppen sowie kulturellen Einflüssen.

Zur Risikoaversion tritt zusätzlich die subjektive Einschätzung hinsichtlich der Wahrscheinlichkeit des Eintretens eines gefährlichen Ereignisses mit einem bestimmten Schaden (z. B. Tod einer Person), da das Angst- und somit Risikoempfinden von Person zu Person variiert. Ängstliche bzw. in Unkenntnis über bestimmte Zusammenhänge befindliche Menschen fürchten sich manchmal bereits vor Situationen, die für andere nicht aufregend sind. Ein erfahrener Fallschirmspringer wird bei einem Tandemsprung den freien Fall anders empfinden als seine Begleitperson. Ein Fahrlehrer wird bestimmte Verkehrssituationen hinsichtlich des Risikos anders beurteilen als sein Fahrschüler.

Die intuitive Wahrnehmung und Beurteilung eines Ereignisses kann aber nicht für eine belastbare Risikoanalyse als Grundlage dienen. Aus diesem Grund ist ein Übergang zum objektiven Risiko erforderlich. Dabei wird ein Risiko als der mathematisch gefasste Erwartungswert objektiver Schäden verstanden und mit $s(Da) = Da$ die Bewertungsfunktion als ein konstanter Wert definiert:

$$Ri_o = w \cdot Da$$

Formel 5

Ri_o	objektives Risiko
w	Wahrscheinlichkeit
Da	Schadensausmaß (engl. damage)

Bei der Berechnung und Interpretation des (objektiven) Risikos sind gemäß der Ausführungen in [BRA05b] grundsätzlich folgende Einschränkungen zu beachten:

- Die Eingangsdaten Wahrscheinlichkeit und Schadensausmaß sind meist nur grobe und infolge fehlender statistischer Daten meist subjektive Abschätzungen.
- Eine wissenschaftliche Analyse des akzeptablen Risikos endet bei der Frage nach dessen Vertretbarkeit und kann somit nur schwer mit Zahlen beantwortet werden.

Der erste Gedanke liegt darin begründet, dass die Wahrscheinlichkeit für ein Ereignis in einigen technischen Systemen zwar extrem klein ist, dieses aber gleichzeitig ein großes Schadensausmaß haben kann bzw. könnte (z. B. Unfall im Kernkraftwerk). Der zweite Gedanke wird in Abschnitt 3.6.4 ausführlich beschrieben.

3.6.3 Individuelles und kollektives Risiko

Neben den bisher beschriebenen Risikoarten kann zwischen individuellem und kollektivem Risiko unterschieden werden. Die Beschreibung der Personengefährdungen durch ein technisches System benennt das individuelle Risiko Ri_i . Die Gefährdung jeder potenziell betroffenen Person wird durch die Wahrscheinlichkeit beschrieben, infolge eines technischen Systems zu Schaden zu kommen. Das individuelle Risiko spiegelt damit die Sicht des Einzelnen wider.

Im Gegensatz dazu verkörpert das kollektive Risiko Ri_o das Gesamtrisiko, das ein System für eine exponierte Personengruppe darstellt (vgl. Bild 9). Dies verkörpert die Betreibersicht bzw. die Sicht der Gesellschaft.

Anhand des in Bild 8 dargestellten Szenarios soll der Unterschied verdeutlicht werden.

Es sei: ein Steinschlag auf eine Bahnstrecke finde einmal in 10 Jahren statt. Ein Wochenendpendler möge 100-mal pro Jahr an dieser Stelle vorbeifahren. Der Pendler soll ferner im Zug 4 Sekunden benötigen, um an dieser Gefahrenstelle vorbeizukommen. Sollte er jedoch vom Steinschlag getroffen werden, so kommt er zu Tode. Der Zug möge zudem mit 650 Fahrgästen besetzt sein.

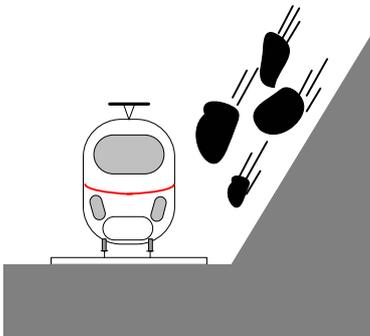


Bild 8: Szenario zur Abschätzung des Risikos

Das individuelle Risiko kann dann wie folgt berechnet werden:

$$Ri_i = HR_i \cdot Da_i = \frac{1 \text{ Ereignis}}{10 a \cdot 365 \frac{d}{a}} \cdot \frac{4 \frac{s}{\text{Ereignis} \cdot \text{Fahrt}} \cdot 100 \frac{\text{Fahrten}}{a}}{24 \cdot 60 \cdot 60 \frac{s}{d}} \cdot 1 \frac{\text{Toter}}{\text{Person}}$$

$$Ri_i = 1,2 \cdot 10^{-6} \frac{\text{Toter}}{\text{Person} \cdot a} \quad \text{Formel 6}$$

Das kollektive Risiko hingegen wird berechnet aus der Summe der individuellen Risiken:

$$Ri_o = \sum Ri_i = 650 \text{ Personen} \cdot 1,2 \cdot 10^{-6} \frac{\text{Toter}}{\text{Person} \cdot a} = 7,8 \cdot 10^{-4} \frac{\text{Tote}}{a} \quad \text{Formel 7}$$

Der Mensch unterscheidet und nimmt bewusst oder unterbewusst wahr, ob er einem Risiko hilflos ausgesetzt ist oder aktiv auf dieses Einfluss nehmen kann. Entsprechend nimmt er ein bis zu drei Zehnerpotenzen höheres individuelles Risiko auf sich, wenn er selbst darüber entscheiden kann [REA94]. Risikosportarten (z. B. Fallschirmspringen, Bergsteigen, Skifahren) sind typische Beispiele für bewusst eingegangene hohe individuelle Risiken.

Eine Ursache für diesen Effekt ist der sogenannte „Optimism Bias“ [REA94]. Er beschreibt den systematischen, kognitiven Fehler bei der Einschätzung von Risiken, auf die der Mensch selbst Einfluss ausüben kann. Neben „Optimism Bias“ gibt es noch die sogenannte „Homeostatis“ [REA94]. Darunter versteht man die konstante Höhe des Risikos, das Menschen unabhängig von technischen Hilfsmitteln auf sich nehmen. Sicherere Straßen und Autos führen nicht zwangsläufig zu weniger Unfällen. Vielmehr nutzen Menschen neue technische Hilfsmittel, um riskanter zu agieren. Dabei erzeugen sie eine erhöhte Fehlerwahrscheinlichkeit. Dieses Phänomen wird auch als Risikokompensation bezeichnet, die letztlich ein annähernd konstantes Gesamtrisiko zur Folge hat.

3.6.4 Grenzzisiko

Risiko kann als quantitative Größe für eine Gefährdung betrachtet und aus dem Produkt der Eintrittswahrscheinlichkeit und dem Ausmaß des möglichen Schadens ermittelt werden (vgl. Formel 2). Mit Hilfe dieses einfachen Zusammenhanges werden gelegentlich Werte mit vielen signifikanten Stellen berechnet. Ein grundlegendes Problem wird dabei aber meist verschwiegen. Die Eingangsdaten sowohl für die Wahrscheinlichkeit als auch die Ausmaß des möglichen Schadens rühren oft aus groben und zudem subjektiven Abschätzungen (vgl. Abschnitt 3.6.2).

Immer wieder entspinnt sich deshalb an der einfachen Formel für das Risiko die Frage nach der Tolerierbarkeit von Risiken und damit nach der Höhe der zumutbaren Eintrittswahrscheinlichkeit eines Schadens. Eine mit gesellschaftlichem Konsens behaftete Antwort stellt die Folgende dar:

- „Welcher Grad an Wahrscheinlichkeit [für die Beantwortung der Frage] hinreichend ist, wird entsprechend dem Verhältnismäßigkeitsgrundsatz nach dem Grad der betroffenen Rechtsgüter bestimmt.“ [SCH01]

Im Bereich des Arbeitsschutzes, wo es um das Leben bzw. die Gesundheit der Mitarbeiter geht, muss eine geringere Eintrittswahrscheinlichkeit gefordert werden als bei der Gefährdung von Sachgütern. Da eine absolute Sicherheit unter Ausschluss aller Gefährdungen nicht realisierbar ist, muss ein akzeptables Risiko bestimmt werden. Dieses muss entsprechend dem Verhältnismäßigkeitsgrundsatz einen umso geringeren Grad an Wahrscheinlichkeit haben, je schwerwiegender die zugehörigen Folgen sind. Bei quantitativen Betrachtungen fließt die Höhe des Schadensausmaßes des Ereignisses ein. Eine hohe Eintrittswahrscheinlichkeit eines schweren Schadens verpflichtet zur Ergreifung hochwertiger Sicherheitsmaßnahmen. Ein optimaler Schutz besteht immer darin, wenn Gefahrenquellen vermieden bzw. ausgeschlossen werden (z. B. Sperrung des Nachbargleises zum Ausschluss von Zugfahrten bei Bauarbeiten im Gleisbereich). Sollte dieses nicht realisiert werden können, sind technische und/oder organisatorische Maßnahmen

zu treffen, die die Gefährdungen möglichst gering halten (z. B. Verringerung der zulässigen Geschwindigkeit im Nachbargleis bei Bauarbeiten im Gleisbereich). Die Methoden für den Umgang mit Gefährdungen im Allgemeinen und Fehlern, Ausfällen bzw. Störungen im Speziellen werden in Abschnitt 5.1 ausführlich beschrieben. Dabei ist zudem der jeweils aktuelle Stand der Technik zu Grunde zu legen.

Übrigens wird bei der Beantwortung der Frage nach der Tolerierbarkeit dieses Risikos im Rahmen von Diskussionen seitens der Fürsprecher oft nur von Wahrscheinlichkeiten und seitens der Gegner nur von möglichen Folgen, d. h. dem resultierenden Schaden, gesprochen. Das Produkt beider Werte ist allerdings die entscheidende Größe. Um die Festlegung einer Akzeptanzgrenze kommt man allerdings nicht umhin, denn eine wissenschaftliche Analyse des Risikos endet immer bei der Frage nach der Vertretbarkeit des ermittelten Wertes. Erschwerend kommt hinzu, dass meist nicht die Verursacher der Risiken, sondern andere (z. B. Fahrgäste, Anwohner) die Folgen eines Unfalls zu tragen haben. Im Rahmen von Unfalluntersuchungen wird daher ermittelt, ob ein Risiko aus Kostengründen bewusst eingegangen wurde oder tatsächlich unbekannt war und falls letzteres der Fall ist, ob es aus Kosten- oder Zeitdruck unbekannt geblieben ist. Grundsätzlich wird gefordert, dass ein Risiko weder auf Grund minimaler Folgen noch wegen dessen minimaler Wahrscheinlichkeit ignoriert werden darf. Vielmehr ist die Toleranz ausreichend und plausibel zu begründen.

Daraus ergibt sich die Frage, wie ein derartiges Grenzzisiko⁷ festgelegt werden kann? Zwei Tendenzen sind im Schrifttum (z. B. [BRA05b], [KRO96], [KRO00], [KUH81], [KUH00], [MON99]) zu erkennen:

- Bestimmung einheitlicher Risikogrenzwerte, mittels:
 - Festlegung eines Grenzwertes für die Wahrscheinlichkeit des Eintretens einer Gefahr (maximale Gefährdungswahrscheinlichkeit) bzw.
 - Festlegung eines Grenzwertes für die Häufigkeit des Eintretens einer Gefahr pro Zeiteinheit (maximale Gefährdungsrate) und gleichzeitiger
 - Festlegung von Grenzschadensausmaß bzw. Grenzschadenssummen oder
 - Festlegung eines Grenzwertes für die Wahrscheinlichkeit des Eintretens repräsentativer Schadenskategorien.
- Bestimmung einheitlicher Sicherheitskennwerte, mittels:

⁷ Gleichwertige Begriffe sind „tolerierbares Risiko“ und „vertretbares Risiko“.

- Festlegung eines zumutbaren Grenzkostenwertes, dem Verhältnis zwischen Risikominderung und zugehörigem finanziellem Aufwand (vgl. Bild 10)

Der erste Gedanke, also die Bestimmung eines einheitlichen Risikogrenzwertes, impliziert die Betrachtung individueller bzw. kollektiver Risiken. Bild 9 verdeutlicht den Einfluss des festgelegten Referenzwertes für ein zulässiges individuelles Risiko auf eine entsprechende Anzahl von Personen (P_{RiMi}). Diese erfahren durch Maßnahmen der Risikominderung einen Schutz. Alternativ kann auch die Festlegung eines Referenzwertes für ein zulässiges kollektives Risiko erfolgen. Hierzu bedarf es zudem der Festlegung der betrachteten Personengruppe („exponierte Personen“), also derjenigen Anzahl an Personen, die in die Berechnung des kollektiven Risikos einfließen. Ein Vorteil des Bahnsystems mit begrenztem Schadensausmaß im Ereignisfall gegenüber Bereichen mit höherem Schadensausmaß (z. B. Luftverkehr, chemische Industrie, Kernenergietechnik) besteht in der vergleichsweise leichten Festlegung der exponierten Personen.

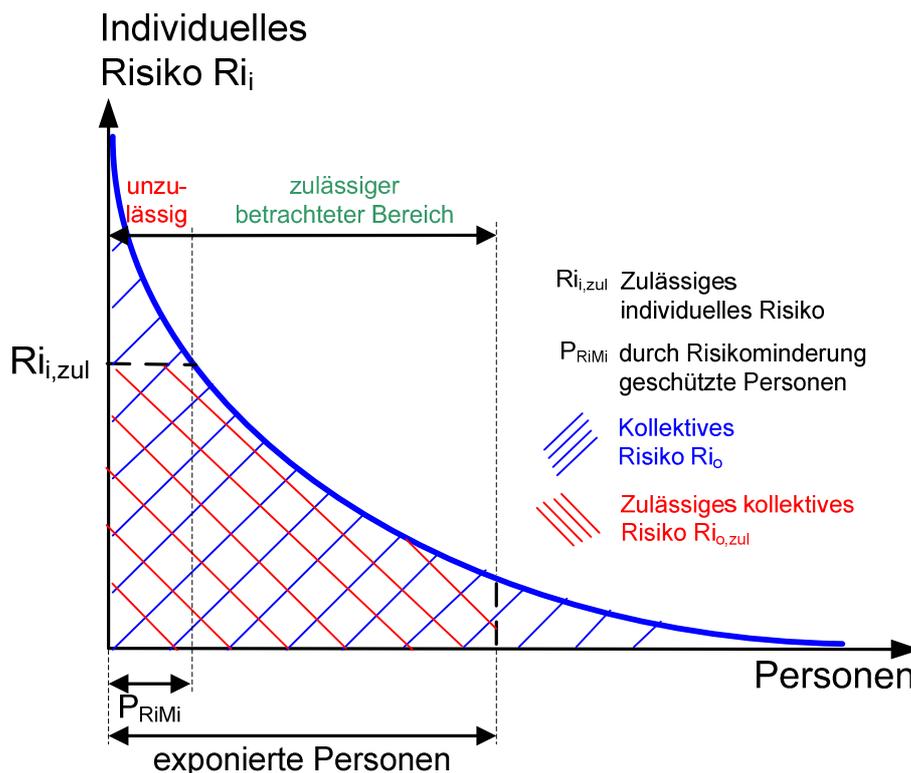


Bild 9: Zusammenhang zwischen verschiedenen Risikoarten

Der zweite Gedanke, die Bestimmung eines einheitlichen Sicherheitskennwertes, zielt auf die monetäre Effektivität der Risikominderung ab. Für die in Bild 10 dargestellten gleich großen Risikoreduktionen $\Delta Ri_a = Ri_2 - Ri_1$ und $\Delta Ri_b = Ri_4 - Ri_3$ fallen unterschiedliche Kosten $\Delta K_a = K_2 - K_1$ bzw. $\Delta K_b = K_4 - K_3$ an. Unter Beachtung des effektiven Einsatzes der

finanziellen Mittel ist die Reduktion des im System befindlichen Risikos um den Wert ΔRi_b zu bevorzugen, da die aufzubringenden Kosten ΔK_a geringer als ΔK_b sind. Zudem sollte das Kostenwirksamkeitsverhältnis $\Delta K_a/\Delta Ri_b$ den absoluten Wert 1 (Grenzkostenkriterium) nicht übersteigen [KRO96]. Je geringer das Kostenwirksamkeitsverhältnis ist, desto geeigneter ist die entsprechende Maßnahme zur Risikominderung. Ein Kostenwirksamkeitsverhältnis von 0,5 bedeutet beispielsweise, dass sich pro investierten Euro das Risiko um zwei Euro reduziert [KRO96]. Dieser Betrachtung liegt die in Abschnitt 3.4 beschriebene Monetarisierung des Schadens inne.

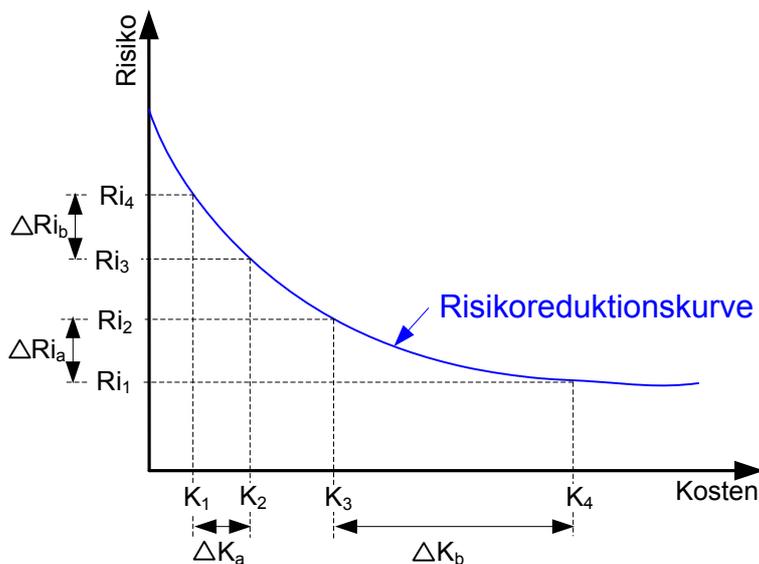


Bild 10: Effektivität der Risikoreduktion nach [KRO96]

Das Entstehen einer Gefährdung ist dem System bzw. Teilsystem gut zuzuordnen. Im Zweifelsfall kann dies auch per Definition erfolgen. Welche Schadensart sich allerdings aus einer Gefährdung entwickelt und welches Schadensausmaß bzw. welche vordefinierte Schadenskategorie daraus resultiert, ist nicht zwangsläufig deterministisch, da dieser Prozess vielfältigen, stochastischen und nicht ausschließlich vom System abhängigen Einflüssen unterliegt. Die Auswertung von Statistiken im Rahmen des Projektes „Signalsicht“ an der TU Dresden [MAS07] konnte dieses bestätigen.

Von den potenziellen Möglichkeiten zur Festlegung eines (rechts-)verbindlichen Grenzkrisikos erfüllen vor dem genannten Hintergrund der nicht zwangsläufigen Korrelation zwischen Gefährdung und Schadensart bzw. -ausmaß nur die Festlegung eines Grenzwertes der Gefährdungswahrscheinlichkeit oder die Festlegung eines Grenzwertes der Gefährdungshäufigkeit die Voraussetzungen. Im Gegensatz zum Schadensausmaß sind diese Größen als direkte Systemeigenschaft ableit- und berechenbar.

Somit kann festgestellt werden, dass alle Methoden zur Festlegung von Risikogrenzwerten bzw. Sicherheitskennwerten, welche die Schadensart, das Schadensausmaß, die

Schadenssumme bzw. die entstehenden Kosten beinhalten, hinsichtlich proaktiver Sicherheitsbetrachtungen lediglich qualitative Aussagen zulassen.

Nichtsdestotrotz erlauben derartige Methoden erkenntnisreiche Vergleiche zwischen einzelnen Systemen und deren Zuständen einerseits und reaktiven Analysen der Erfolge von Maßnahmen zur Risikoreduktion andererseits. Neben der Ermittlung der vorhandenen Risiken ist es zwingend notwendig, diese mit anderen vorhandenen und akzeptierten Risiken zu vergleichen. Prinzipiell gibt es dafür zwei Möglichkeiten. Die erste besteht in der Angabe der Sterbewahrscheinlichkeit bzw. Sterbehäufigkeit pro Jahr pro Person bei einer bestimmten Aktivität oder in einer bestimmten Situation. Es handelt sich hierbei um individuelle Risiken (vgl. Abschnitt 3.6.3). Diese Darstellungsweise erlaubt es allerdings nicht, die Schwere eines einzelnen Unglückes zu berücksichtigen. Auf Grund dieses Nachteiles wird häufiger von der zweiten Möglichkeit Gebrauch gemacht, bei der für die Darstellung von Risiken sogenannte F-N-Diagramme (Frequency-Numbers-Diagrams) verwendet werden. In dieser Darstellung werden die Konsequenzen eines Versagens bzw. eines Unfalles der Häufigkeit gegenübergestellt. Die Konsequenzen werden überwiegend in der Anzahl von Opfern (vgl. Abschnitt 3.4), gelegentlich auch in monetären Einheiten angegeben. Aufgrund der Berücksichtigung der Anzahl der Opfer spricht man auch von kollektiven Risiken. Im Rahmen dieser Arbeit werden F-N-Diagramme nicht näher betrachtet. Vielmehr wird auf Veröffentlichungen (z. B. [ELM99], [KUM96]) zu diesem Thema verwiesen.

Auf der Grundlage der Ergebnisse der Gefährdungsidentifikation und Konsequenzanalyse sowie unter Verwendung des individuellen bzw. kollektiven Risikos erfolgt die Risikoabschätzung für jede sicherheitsrelevante Funktion. Dabei gilt besonders für das individuelle Risiko die bereits in Abschnitt 2.2 formulierte Forderung an ein System [BÖR04], [GRA02], [MON99]:

- Keine Person, die durch das zu beurteilende System potenziell gefährdet ist, trägt ein vergleichsweise höheres Risiko.

Als Hilfsmittel zur Erfüllung dieser Forderung dient die in DIN EN 50126 verankerte Risikomatrix. Dabei handelt es sich um eine abstrakte Matrix (vgl. Bild 11), wobei die einzelnen Kategorien (z. B. „unbedeutend“, „kritisch“, „selten“, „unvorstellbar“) und das Grenzkrisiko (vgl. Abschnitt 3.6.4) vom Betreiber individuell für das betrachtete System bzw. für dessen einzelne Funktionen festgelegt werden müssen. Dies bedeutet, dass letztlich bestimmt werden muss, wie viel „unbedeutend“, „kritisch“, „selten“ und „unvorstellbar“ ist.

Häufigkeit von Gefahrenfällen	Risikostufen			
	häufig			
wahrscheinlich		unzulässiger Bereich		
gelegentlich				
selten				
unwahrscheinlich	zulässiger Bereich			Grenzrisiko
unvorstellbar				
	unbedeutend	marginal	kritisch	katastrophal
	Gefahrenstufen			

Bild 11: Risikomatrix nach [DIN00]

Grundsätzlich wäre ein Risiko leicht kalkulierbar, wenn nicht die Eintrittswahrscheinlichkeit und das Schadensausmaß eines Ereignisses in der Praxis meist unbestimmte Parameter blieben. Daher behilft man sich in qualitativen Sicherheitsbetrachtungen damit, dass Sicherheit als Zustand verstanden wird, bei dem das noch im System verbliebene Risiko nicht größer als das Grenzrisiko ist. Dadurch kann postuliert werden, dass alle unzulässigen Risiken eliminiert wurden und das System nicht in den unsicheren Risikobereich gerät. Bild 12 stellt diesen Zusammenhang grafisch dar.

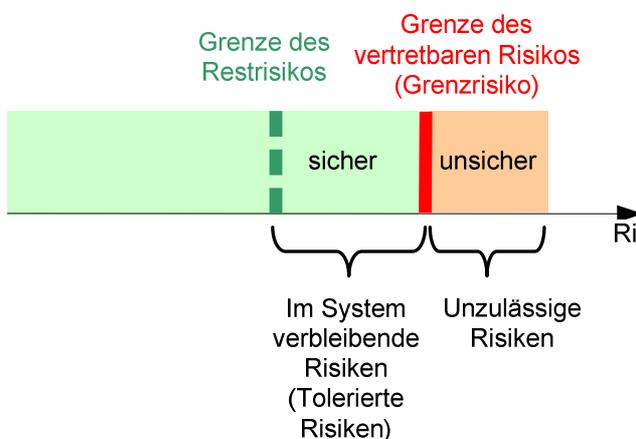


Bild 12: Zusammenhang zwischen Grenzrisiko und Restrisiko

3.7 Sicherheit

Der vierte und letzte Bestandteil von RAMS, die Sicherheit, kann in Bild 4 eingeordnet werden, wenn das in den Abschnitten 3.5 bzw. 3.6 ausführlich beschriebene Risiko und dessen Arten als Indikator für Sicherheit (OKZ 9 in Bild 4) verstanden wird. In der risikoorientierten DIN EN 50126 wird der Begriff *Sicherheit* folgerichtig definiert als:

„Das Nichtvorhandensein eines unzulässigen Schadensrisikos.“ [DIN00]

Eine geforderte Sicherheit wird demnach erreicht, wenn sämtliche unzulässige Risiken ausgeschlossen werden können. Diese Definition liefert die Verknüpfung von *Risiko* und *Sicherheit* einerseits und damit einhergehend der Begriffe *Zuverlässigkeit*, *Instandhaltbarkeit*, *Verfügbarkeit* und *Sicherheit* andererseits dar (vgl. Bild 4). Das Verständnis für diesen Zusammenhang ist für eine ganzheitliche Betrachtung des Bahnsystems von wesentlicher Bedeutung.

Eine weitere Definition der Sicherheit befindet sich in DIN EN 50128:

„Die Erwartung, dass ein System unter festgelegten Bedingungen nicht zu einem Zustand führt, in dem menschliches Leben, die körperliche Unversehrtheit und Gesundheit oder die Umwelt gefährdet sind.“ [DIN01a]

Der darin verwendete Begriff *Erwartung* impliziert die Tatsache, dass niemals, selbst bei Einsatz größter finanzieller Mittel, eine absolute Sicherheit erreichbar ist.

3.8 Safety und Security

In einigen Publikationen (z. B. [DUC02], [KON07], [WIK07]) werden die Abkürzungen „RAMSS“ bzw. „RAMS(S)“ verwendet. Dort wird beim Begriff *Sicherheit* im Sinne der englischen Übersetzungen zwischen „*safety*“ und „*security*“ unterschieden.

Dabei beschreibt *Safety* die funktionale Sicherheit des Systems und schützt gegen Schäden durch Technik sowie fahrlässige, menschliche Handlungen. Funktionale Sicherheit ist hierbei derjenige Teil der Sicherheit, der von der korrekten (sicherheitsrelevanten) Funktion des betrachteten Systems abhängt.

Security schützt hingegen vor Schäden durch vorsätzliche, menschliche Handlungen. Überwachungskameras an Eingängen zu sensiblen Gebäuden (z. B. Betriebszentrale) oder Zugangshemmnisse in Form von Gittern an Türen bzw. Fenstern von Stellwerken bilden Beispiele für Sicherheit im Sinne von *Security*.

Die Mehrheit der Komponenten im Bereich der Bahnsicherungstechnik (z. B. Gleisfreimeldeanlagen, Stellwerke, Signale, Bahnübergänge) wie auch die Übertragung sicherheitsrelevanter Informationen [FEN04]:

- innerhalb der Systeme, Teilsysteme und Komponenten der Bahnsicherungstechnik (z. B. Stellwerke, Gleisfreimeldeanlagen)
- zwischen ortsfesten Systemen, Teilsystemen und Komponenten der Bahnsicherungstechnik (z. B. vom Signal zum PZB-Streckenmagnet, vom Stellwerk zur Weiche)

- zwischen ortsfesten und beweglichen Systemen, Teilsystemen und Komponenten der Bahnsicherungstechnik (z. B. vom PZB-Streckenmagnet zum PZB-Fahrzeugmagnet)
- zwischen sicherheitsrelevanten Systemen, Teilsystemen und Komponenten auf dem Fahrzeug (z. B. vom PZB-Fahrzeugmagnet zur Bremssteuerung)

sind der Sicherheit im Sinne von Safety zuzuordnen.

In DIN EN 50159-1 [DIN01b] und DIN EN 50159-2 [DIN01c] wird eine Auswahl an Maßnahmen zur Sicherung bei der Datenübertragung in Systemen, Teilsystemen und Komponenten der Bahnsicherungstechnik genannt. Dabei wird zwischen:

- geschlossenen (nicht öffentlichen) und
- offenen (öffentlichen) Netzen

unterschieden. Bahneigene Netze zur Übertragung sicherheitsrelevanter Informationen werden der Gruppe der geschlossenen Netze zugeordnet. Bei diesen kann von der Bekanntheit und der Überwachung der Übertragungseigenschaften sowie der Beschränkung auf autorisierte Zugriffe ausgegangen werden. Aufgrund dieser Randbedingungen sind F/A/S, die zur Verfälschung oder gar zum Verlust der Informationen führen können, auf Sicherheit im Sinne von Safety im Allgemeinen und:

- F/A/S im Empfänger bzw. Sender
- (systeminterne) Ausfälle des Übertragungskanals
- (systemexterne) Störungen des Übertragungskanals durch elektrische Beeinflussung
- menschliche Fehler bei der Instandhaltung

im Speziellen beschränkt.

Die zunehmende Nutzung von offenen Netzen im Bahnbereich erfordert zusätzliche Sicherungsmaßnahmen im Sinne von Security, die einen Schutz vor vorsätzlichen

- passiven Angriffen (Lesen und ggf. Entschlüsselung von Informationen) sowie
- aktiven Angriffen (ggf. Entschlüsselung und Verfälschung bzw. Zurückhaltung von Informationen)

von außen bieten. Als Konsequenz dieser potenziellen Angriffe werden sicherheitsrelevante Daten in offenen Netzen durch Verschlüsselungen geschützt, wobei man sich der Methoden F/A/S-Ausschluss (vgl. Abschnitt 5.1.1) bzw. F/A/S-Folgenausschluss (vgl. Abschnitt 5.1.2) bedient. Ziel ist dabei die Sicherstellung der Informationsintegrität (keine Verfälschung oder Veränderung) und Informationsauthentizität (keine falsche Quelle oder Senke).

3.9 Verfügbarkeit

Die zunehmenden Forderungen seitens der Bahnbetreiber nach hoher Verfügbarkeit sicherheitsrelevanter Teilsysteme im Bahnbereich können nur erfüllt werden, wenn die eingesetzten Komponenten über geringe Ausfall- und große Reparaturraten verfügen [TRI02]. Dieser Zusammenhang wird in Bild 4 deutlich, wenn die Einflüsse von Zuverlässigkeit (OKZ 6) bzw. Instandhaltbarkeit (OKZ 8) auf die Verfügbarkeit (OKZ 7) und deren Einfluss auf die Gefährdungsrate (OKZ 3) betrachtet werden.

Daraus können zwei Lösungswege für das Erreichen einer hohen Systemverfügbarkeit abgeleitet werden:

- geringe Ausfallraten durch zuverlässig funktionierende Komponenten (vgl. Abschnitt 3.10) sowie
- hohe Reparaturraten durch zeitoptimale präventive sowie kurzfristige korrektive Instandhaltung (vgl. Abschnitt 3.11).

Nachfolgend werden die Grundlagen für die Umsetzung der obigen zwei Lösungswege kurz erläutert sowie die wichtigsten Kenngrößen der Zuverlässigkeit und der Instandhaltbarkeit genannt. Auf eine detaillierte Beschreibung wird im Rahmen dieser Arbeit verzichtet. Vielmehr wird auf Veröffentlichungen (z. B. [FIS90], [ELM99]) zu diesem Thema verwiesen.

3.10 Zuverlässigkeit

Die Entwicklung zuverlässiger Bahninfrastruktur und Fahrzeuge erfolgt heute unter Randbedingungen, die sich zunehmend durch hohe Komplexität, umfangreiche Funktionalität, steigende Produkthaftung, gestiegene Kundenanforderungen und kürzere Entwicklungszeiten auszeichnet. Neben geringen Anschaffungskosten ist daher eine hohe Zuverlässigkeit der Komponenten, mit ihrem Einfluss auf die laufenden Betriebskosten, ein entscheidender Wettbewerbsfaktor [VDI05]. Aussagen zu Zuverlässigkeitskenngrößen sind deshalb heute unerlässlich.

3.10.1 Kenngrößen der Zuverlässigkeit

Zuverlässigkeit kann durch Quantifizierung ihrer Eigenschaften unter Verwendung folgender Zuverlässigkeitskenngrößen ermittelt werden [FIS90]:

- Ausfallwahrscheinlichkeit $Q(t)$
- Überlebenswahrscheinlichkeit $R(t)$
- Ausfallwahrscheinlichkeitsdichte $f(t)$
- Ausfallrate $\lambda(t)$

3.10.2 Ermittlung der Zuverlässigkeit

Die hohe geforderte Systemzuverlässigkeit wird heute nicht mehr allein auf dem klassischen Weg über ausgereifte Konstruktionsmethoden und -verfahren sichergestellt, vielmehr werden mit der Anwendung spezieller analytischer Zuverlässigkeitsmethoden die gestiegenen Anforderungen erfüllt. Dabei werden sowohl qualitative als auch quantitative Zuverlässigkeitsanalysen durchgeführt. Im Rahmen des Zuverlässigkeitsmanagements wird zwischen folgenden Bereichen unterschieden:

- Experimentelle Zuverlässigkeitsuntersuchungen
- Simulation von Zuverlässigkeit
- Erfassung und Auswertung von Ausfalldaten

3.11 Instandhaltbarkeit

Neben der Zuverlässigkeit hat die Instandhaltbarkeit (OKZ 8 in Bild 4) der verwendeten Komponenten eine große Bedeutung für die Verfügbarkeit eines Systems. Die Instandhaltbarkeit ist gemäß ihrer Definition in DIN EN 50126:

„Wahrscheinlichkeit dafür, dass für eine Komponente unter gegebenen Einsatzbedingungen eine bestimmte Instandhaltungsmaßnahme innerhalb einer festgelegten Zeitspanne ausgeführt werden kann, wenn die Instandhaltung unter festgelegten Bedingungen erfolgt und festgelegte Verfahren und Hilfsmittel eingesetzt werden.“ [DIN00]

Die Instandhaltbarkeit einer Komponente stellt ein Maß für die Qualität der Randbedingungen für den Prozess der Instandhaltung dar. Kriterien der Instandhaltbarkeit hinsichtlich der Sicherheit sind vor allem:

- Einfachheit der Instandhaltung von sicherheitsrelevanten Komponenten,
- Wahrscheinlichkeit von menschlichen Fehlern während der Instandhaltung sicherheitsrelevanter Komponenten,
- erforderliche Zeit bis zur Wiederherstellung des sicheren Zustandes.

Grundsätzliches Ziel ist es, Instandhaltungs- und Erneuerungsmaßnahmen so aufeinander abzustimmen, dass die erforderliche Verfügbarkeit des Gesamtsystems unter Beachtung von Sicherheit und Wirtschaftlichkeit gewährleistet werden kann.

Die Vorhaltung von Informationen zu technischen Kennzahlen (z. B. Alter und Zustand der Anlagen, Ausfalldauer) dienen ebenso der Gewährleistung geeigneter Instandhaltbarkeit wie die Ergreifung organisatorischer Maßnahmen (z. B. Zuständigkeiten, Wartungszyklen).

3.11.1 Kenngrößen der Instandhaltung

Wartungs- und Instandsetzungsintervalle müssen in Folge der in Bild 13 genannten Methoden festgelegt und aufeinander abgestimmt werden. Dazu bedarf es Kenngrößen, mit deren Hilfe Eigenschaften der Instandhaltung quantifiziert werden können [FIS90]:

- Erneuerungswahrscheinlichkeit $H(t)$
- Erneuerungsdichte $h(t)$
- Reparaturrate $\mu(t)$

3.11.2 Ermittlung der Instandhaltbarkeit

Technische Komponenten und Systeme unterliegen während ihrer Betriebszeit Beanspruchungen, die zum Verlust der Gebrauchseigenschaften führen können. Bei vielen Komponenten ist festzustellen, dass neben ihrem Alter vor allem die Intensität ihrer Inanspruchnahme entscheidenden Einfluss auf den Instandhaltungsbedarf hat. Abnutzungserscheinungen in Form von Verschleiß, Korrosion oder Ermüdung sind oft die Folge, die unter bestimmten Bedingungen zum Ausfall der Komponente führen. Eine wesentliche Aufgabe der Instandhaltung ist daher die Vermeidung von Abnutzungserscheinungen. Hierzu bedient man sich, wie in Bild 13 dargestellt, der Methoden „Wartung“, „Inspektion“, „Instandsetzung“ und „Verbesserung“ [DIN03a].

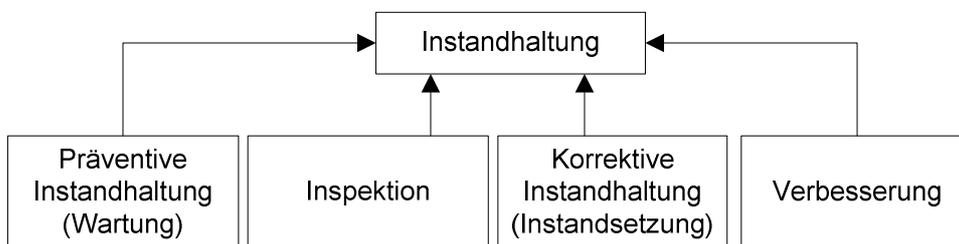


Bild 13: Methoden der Instandhaltung nach [DIN03a]

Die Forderung nach hoher Verfügbarkeit sicherungstechnischer Systeme und die daraus resultierende Zielstellung neben geringer Ausfallraten auch große Reparaturraten zu realisieren, kann mittels zeitoptimaler *präventiver Instandhaltung (Wartung)* sowie kurzfristiger *korrektiver Instandhaltung (Instandsetzung)* gewährleistet werden.

Regelmäßige *Inspektionen* sind daher unverzichtbar, um einerseits eine vor dem Ausfall stehende Komponente zu reparieren bzw. zu erneuern und andererseits eine bereits ausgefallene Komponente möglichst schnell zu ersetzen. Ziel ist dabei, die Ausfalloffenbarungszeit möglichst zu minimieren.

Zudem sollten unter Verwendung von ermittelten Daten ständig *Verbesserungen* am System vorgenommen werden. Das kann u. U. dazu führen, dass eine Systemstruktur verändert werden muss. In Bezug auf den in Bild 2 dargestellten Lebenszyklus kann

dies bedeuten, dass der gesamte Prozess ab der Phase 2 „Systemdefinition und Anwendungsbedingungen“ erneut durchlaufen werden muss.

4 Unterscheidung zwischen Fehlern, Ausfällen und Störungen

Wie aus Kapitel 3 hervorgeht, wird für (sicherheitsrelevante) Komponenten des Bahnsystems nicht zwingend ein fehlerfreies Funktionieren, sondern die Verhinderung nicht vertretbarer Risiken, d. h. die Einnahme kritischer Systemzustände für eine bestimmte Zeitdauer, gefordert. Dieses wird durch die Überführung des Systems in den sicheren Zustand im Fall eines Fehlers, Ausfalls oder einer Störung (F/A/S) erreicht. Aufgrund dieser Forderung lohnt eine tiefgründige Auseinandersetzung mit den Begriffen *Fehler*, *Ausfall* und *Störung*. Dies rührt aus der Tatsache, dass sie einerseits direkten Einfluss auf die Zuverlässigkeit der eingesetzten Komponenten haben und andererseits aus F/A/S Gefährdungen entstehen können, falls sie vor Inbetriebnahme des Systems nicht analysiert wurden (vgl. Bild 2). Die nachfolgenden Ausführungen sollen die Grundlagen für eine Analyse von F/A/S im Bahnsystem legen.

4.1 Begriffliche Einordnung

Leider sind die Begriffe *Fehler*, *Ausfall* und *Störung* in der Fachliteratur nicht einheitlich definiert. In manchen Veröffentlichungen wird der Begriff *Fehler* im Sinne der englischen Übersetzung „*mistake*“ vornehmlich als menschlicher Fehler verstanden [REA94]. Dieses ist aber eine Betrachtung, die der Komplexität des Begriffes nur bedingt gerecht wird.

Deutsche Normen und Richtlinien definieren *Fehler* oftmals im Sinne der englischen Übersetzung „*nonconformity*“ als die „Nichterfüllung einer Forderung“ [MUE07] oder die „Nichterfüllung der Spezifikation“ [DIN95a] und fokussieren damit auf einen Mangel in der Umsetzung einer Vorgabe. Ein Fehler wird in diesem Zusammenhang auch als „unzulässige Nichtübereinstimmung eines bestimmten Istmerkmals mit dem Soll einer Betrachtungseinheit“ [MUE07] verstanden.

Diesen Gedanken trägt auch DIN EN 50128 in sich, in der ein *Fehler* im Sinne der englischen Übersetzung „*error*“ als die „Abweichung vom beabsichtigten Entwurf, die zu unerwünschtem Systemverhalten oder Ausfall führen kann“ [DIN01a], definiert ist.

Noch differenzierter wird der Begriff *Fehler* in den europäischen Normen DIN EN 50126, DIN EN 50129 und DIN EN 61508-4 behandelt. Dabei wird zwischen Fehlzustand (engl. „*error*“) und Fehlfunktion (engl. „*failure*“) unterschieden.

Zur Vermeidung von Verwechslungen mit dem Begriff *Ausfall*, welcher in DIN EN 61508-4 ebenfalls im Sinne von „*failure*“ verwendet wird, empfiehlt sich eine grundsätzliche Annahme:

- Ein Fehler („error“) ist eine Abweichung während der Planung, Entwicklung, Fertigung und Installation bzw. während des Betriebes und der Instandsetzung einer Komponente oder des Systems.
- Ein Fehler („nonconformity“) ist ein fehlerhafter Zustand einer Komponente oder eines Systems *bis* zu dessen Inbetriebnahme.
- Ein Fehler („fault“) ist ein fehlerhafter Zustand einer Komponente oder eines Systems *nach* dessen Inbetriebnahme.
- Ein Ausfall („failure“) ist ein Ereignis, welches den Übergang einer Komponente oder eines Systems vom fehlerfreien in den fehlerhaften Zustand während des Betriebes eines Systems bezeichnet.

Bild 14 soll diese begriffliche Unterscheidung verdeutlichen.

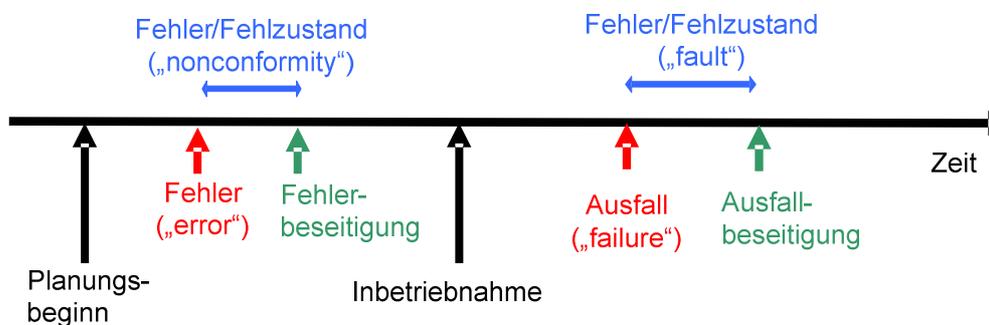


Bild 14: Einordnung der Begriffe Fehler und Ausfall

Vereinfacht können *error* bzw. *failure* jeweils als *Zeitpunkt* des Fehlers bzw. Ausfalls sowie *nonconformity* bzw. *fault* als die *Zeitspanne* des Fehlers bzw. Ausfalls verstanden werden.

4.2 Definitionen

Aus der Fülle an Definitionen der Begriffe *Fehler*, *Ausfall* und *Störung* in nationalen und internationalen Regelwerken (vgl. Definitionen im Glossar) wurden vom Autor die nachfolgenden drei Definitionen als Basis für die weiteren Ausführungen gewählt, da diese den Kern der jeweiligen, oben vorgeschlagenen Bedeutung treffen und eine sinnvolle Abgrenzung untereinander erlauben:

Fehler: „Unzulässige Nichtübereinstimmung eines bestimmten Istmerkmals mit dem Soll in einer Betrachtungseinheit“ [DIN90a]

Ausfall: „Verletzung mindestens eines Ausfallkriteriums bei einer zu Beanspruchungsbeginn als fehlerfrei angesehenen Betrachtungseinheit“ [DIN90a]

Störung: „Verhindern oder Beeinträchtigen einer oder mehrerer Systemfunktionen durch äußere Einwirkungen auf das System“ [DIN90a]

Während *Fehler* einerseits in den frühen Phasen vornehmlich als zufällige oder systematische menschliche Fehler in Form von Design- bzw. Herstellungsfehlern und andererseits während des Betriebes und der Instandhaltung in Form von Bedienungs- bzw. Instandhaltungsfehlern auftreten, erfolgen *Ausfälle* durch den Übergang vom fehlerfreien in den fehlerhaften Zustand nach Inbetriebnahme des Systems also während der Betriebsphase. Werden zudem eine oder mehrere Systemfunktionen durch äußere Einwirkungen auf das System verhindert oder beeinträchtigt, so handelt es sich um eine *Störung*. Diese kann zu jeder Phase des Lebenszyklus auf das System einwirken, deren Auswirkung offenbart sich allerdings nur während der Betriebsphase. Störungen weisen damit Ähnlichkeiten zu Ausfällen auf.

Insbesondere den während der Betriebsphase auftretenden Ausfällen von Komponenten, durch Instandhaltungsmaßnahmen entstehenden Fehlern und durch äußere Einflüsse hervorgerufenen Störungen muss durch das Systemdesign (z. B. Dimensionierung) bzw. geeignete Schutzmaßnahmen (z. B. Redundanz) entgegengewirkt werden. Dabei müssen die Forderungen hinsichtlich der Sicherheit und der Verfügbarkeit des Systems erfüllt und im Rahmen des Sicherheitsnachweises dargelegt werden. Die nachfolgenden Ausführungen dienen der Abgrenzung von F/A/S untereinander.

4.3 Zeitliche Einordnung

Die begriffliche Einordnung und die gewählten Definitionen für *Fehler*, *Ausfall* und *Störung* erlauben Schlussfolgerungen hinsichtlich deren Beeinflussung des Bahnsystems im Lebenszyklus. Negative Auswirkungen auf RAMS des Bahnsystems haben:

- Technische, menschliche oder organisatorische Fehler während der Planung, Entwicklung, Fertigung und Installation bzw. während des Bahnbetriebes und der Instandhaltung
- (Systeminterne) Ausfälle bzw. (systemexterner) Störungen während des Bahnbetriebes

Bild 15 stellt beispielhaft eine zeitliche Abfolge von F/A/S dar.

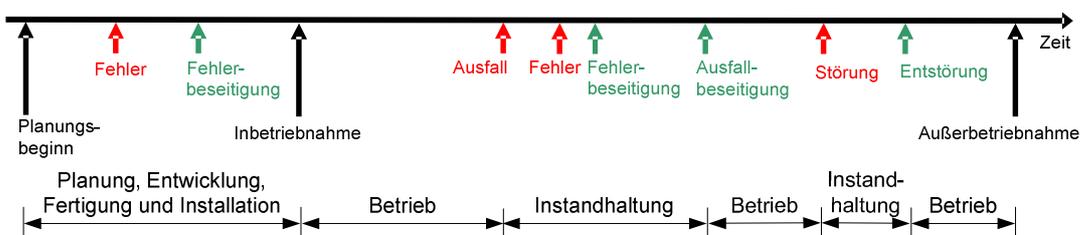


Bild 15: Fehler, Ausfall und Störung während des Lebenszyklus

4.4 Fehler

Nach der begrifflichen Einordnung und Definition von *Fehler*, *Ausfall* und *Störung* werden diese in den nachfolgenden Ausführungen hinsichtlich ihrer Ursachen und Folgen analysiert und eine Kategorisierung vorgenommen.

4.4.1 Fehlerarten

4.4.1.1 Zufällige Fehler

Zufällige technische Fehler sind bis zum Finden ihrer Ursache, meist durch das Zusammenwirken mehrerer voneinander unabhängiger Faktoren, nicht reproduzierbar. Mit dem Auftreten des gleichen Fehlers bei allen Exemplaren bzw. allen Exemplaren einer Serie muss dabei nicht gerechnet werden [FEN04]. Zufällige Fehler können zeitlich als annähernd konstant betrachtet werden (vgl. Bild 19).

Zufällige menschliche Fehler werden insbesondere von Einzelpersonen bei Planung, Herstellung, Installation, Betrieb und Instandhaltung von Hardware sowie Anwendung und Pflege von Software begangen. Zufällige Fehler treten beim Menschen oder innerhalb von Komponenten spontan, d. h. statistisch unabhängig auf.

4.4.1.2 Systematische Fehler

Systematische technische Fehler können bei Wiederholungen unter identischen Bedingungen reproduziert werden und basieren auf Fehlern, die nur durch eine Modifikation des Entwurfs oder des Fertigungsprozesses, der Art und Weise des Betriebes, der Bedienungsanleitung oder anderer Einflussfaktoren beseitigt werden. Eine Instandsetzung ohne derartige Modifikation beseitigt in der Regel nicht die Fehlerursache, welche meist auf einem systematischen menschlichen Fehler einer Einzelperson bei Spezifikation, Entwurf, Herstellung, Installation, Betrieb oder Instandhaltung der Hardware bzw. Entwurf oder Implementierung der Software beruht. Auf Grund dieser Zusammenhänge muss bei Erkennen eines systematischen technischen Fehlers mit dem Auftreten dieses Fehlers bei allen Exemplaren bzw. allen Exemplaren einer Serie/Teilsérie gerechnet werden.

Systematische menschliche Fehler in Hard- oder Software basieren gemäß [DIN03b] auf Denk- oder Ausführungsfehlern. Sie sollten grundsätzlich vermieden, auf jeden Fall aber vor Inbetriebnahme eines Systems offenbart und behoben werden. Bei sicherheitsrelevanten Systemen ist dieses zwingend erforderlich, da sie anderenfalls als unentdeckte Fehler („error“) zu einem nicht vorhersehbaren Zeitpunkt zu einem gefährlichen Systemzustand („nonconformity“) führen können (vgl. Bild 14).

Systematische Fehler können nur schwer bzw. gar nicht quantifiziert und äußerst ungenau vorausgesagt werden [FEN04].

4.4.1.3 Einzelfehler

Einzelfehler können die Folge menschlicher und/oder technischer Fehler sein. Dabei muss nicht jeder Einzelfehler automatisch zu einem Ausfall der Komponente bzw. des Systems führen, da durch Redundanz, sicherheitsgerichtete Fehlerreaktion oder unverlierbare Eigenschaften Ausfälle vermieden werden können. Gleichzeitig besteht die Forderung nach Nichtfortpflanzung von (gefährlichen) Einzelfehlern. Durch eine schnelle Offenbarung und Behandlung von Einzelfehlern oder eine sicherungstechnische Unabhängigkeit der Komponenten kann das gleichzeitige Auftreten weiterer Fehler (Mehrfachfehler) vermieden werden.

4.4.1.4 Mehrfachfehler

In vielen Systemen besteht die Forderung der Einnahme des sicheren Zustandes bei (gefährlichen) Mehrfachfehlern. Falls eine gemeinsame Fehlfunktion von zwei oder mehr funktionell zusammenwirkenden Komponenten zu einem gefährlichen Zustand führen kann, müssen diese in sicherungstechnischen Systemen voneinander unabhängig sein. Dieses dient dem Ausschluss systematischer Mehrfachfehler. In der Praxis wird eine kurze Fehleroffenbarungszeit mittels betätigungsbezogener (datenflussabhängiger) Prüfung bzw. bei schaltungstechnisch nicht erkennbaren Fehlern durch regelmäßige Prüfungen gewährleistet.

Zudem wird oft von Folgefehlern gesprochen [FEN04]. Dabei führt der Fehler in einer Komponente zu einem oder mehreren Fehlern in weiteren Komponenten. Ein Folgefehler ist somit ein spezieller systematischer Mehrfachfehler.

4.4.2 Quellen für Fehler

Die Auswertung von Unfällen mittels Grundursachenanalysen [TUB07] (z. B. Why-Because-Analyse [LAD01]) liefert drei verschiedenen Quellen für Fehler:

- Menschen
- Technik
- Organisation

Aus dieser Tatsache heraus ist es notwendig, geeignete Methoden bereitzustellen, um technische Fehler bzw. menschliche Fehlhandlungen auszuschließen bzw. rechtzeitig zu erkennen oder zumindest deren Folgen zu minimieren. Zudem müssen Organisations- und Managementstrukturen bestehen, in denen die Randbedingungen für möglichst wenige Fehler vorhanden sind [TRI07].

Neben diesen grundsätzlichen Aufgaben ist die Genauigkeit der Fehlervorhersage von Interesse. Diese hängt allerdings in starkem Maße davon ab, inwieweit die Einflussgrößen erkannt werden, welche die Fehler verursachen. Ziel sollte es daher sein, sowohl die

Bedingungen, unter denen ein Fehler auftritt, als auch die Fehlerform vorherzubestimmen.

4.4.3 Technische Fehler

4.4.3.1 Einteilung technischer Fehler

Das Schrifttum schlägt Möglichkeiten für die Einteilung technischer Fehler vor (z. B. [HIN93], [MON99], [BÖR04]). Nach deren Analyse kristallisiert sich die Klassifizierung in folgenden Kategorien heraus:

- Art
- Bereich
- Quelle

Die erste Möglichkeit zur Klassifizierung bietet die *Art* eines technischen Fehlers. Dabei wird einerseits zwischen systematischen (technischen) Fehlern und zufälligen (technischen) Fehlern unterschieden. Diese haben jeweils einen starken Bezug zur Fehlerquelle. Dabei ist entscheidend, ob der Fehler zufällig durch eine physikalisch bedingte Materialabweichung oder systematisch durch eine Unterdimensionierung einer Komponente auftritt. Zudem werden bedingte technische Fehler betrachtet, welche durch Ausfälle oder Störungen verursacht werden und nur schwer reproduzierbar sind.

Die zweite Möglichkeit der Klassifizierung technischer Fehler erfolgt mit Hilfe des *Bereiches*, in welchem sie auftreten. Die Qualität von Daten hängt von der Generierung eines korrekten Wertes zum richtigen Zeitpunkt ab. Technische Fehler können somit im Wert- und/oder Zeitbereich liegen.

Die dritte Form der Klassifikation stellt die *Quelle* dar. Die Abweichung vom vorgesehenen Zeitfenster für eine Reaktion des Systems kann durch Entwicklungsfehler oder Laufzeitfehler verursacht werden. Entwicklungsfehler sind permanent im System befindliche Fehler, die sich unerwartet bemerkbar machen. Sie können durch verschiedene Methoden (z. B. Tests) entdeckt werden. Falls sie aber unentdeckt bleiben, stellen sie eine latente Gefahr dar. Seitens der Fehlerart (vgl. Abschnitt 4.4.1.2) werden sie als systematische Fehler bezeichnet. Laufzeitfehler treten nachträglich ins System ein und werden z. B. durch Hardwareausfälle, unerwartetes Umgebungsverhalten, Bedienungsfehler, Kommunikationsfehler oder vorübergehende Überlastung verursacht. Man spricht von Laufzeitfehlern, wenn das System vorübergehend außerhalb der vorgesehenen Parameter arbeitet oder eine theoretisch beherrschbare Belastung praktisch nicht erbringen kann. Seitens der Fehlerart (vgl. Abschnitt 4.4.1.1) werden sie als zufällige Fehler bezeichnet.

4.4.3.2 Ursachen technischer Fehler

Nachdem eine Klassifizierung der Fehler vorgenommen wurde, kann nach deren Ursachen gefragt werden. Grundsätzlich sind alle technischen Komponenten eines Systems anfällig für technische Fehler. Diese können die verschiedensten Ursachen haben. Der Grund für Fehler innerhalb einer Komponente kann ein Fehler in der Steuerung sein, der wiederum aus einer unvorhersehbaren oder nicht spezifizierten Situation entstehen kann [RAM05].

Aber auch menschliche Planungs- und Entwicklungsfehler, vor allem im Bereich der Software, führen zu technischen Fehlern. Die falsche Implementierung einer korrekten Anforderungsspezifikation im Stellwerkskern stellt ein Beispiel dar. Der Mensch ist dabei oft das erste und entscheidende Glied in der Ursachenkette für technische Fehler. Dieses ist auch der Grund dafür, warum es wichtig ist, ein System über dessen gesamten Lebenszyklus hinweg auf technische Fehler und den Einfluss des Menschen hin zu prüfen.

4.4.3.3 Konsequenzen aus technischen Fehlern

Eine Lösung zur Verhinderung technischer Fehler ist deren ausreichende Analyse während der Planung und Entwicklung des Systems bzw. deren frühzeitige Offenbarung während des Betriebes. Nur wenn bekannt ist, welche Ursachen die Situation auslösen, können Präventivmaßnahmen getroffen werden. Allerdings führen bei komplexen, eng gekoppelten Systemen technische Vorkehrungen dazu, dass die Systeme noch komplexer werden und daraus neue Beeinflussungsmöglichkeiten resultieren. Die technische Vorkehrung muss daher als ein zusätzliches Teilsystem im Gesamtsystem betrachtet werden. Eine adäquate Wahl von Präventivmaßnahmen ist daher für die Gewährleistung der Sicherheit des Systems sehr wichtig.

4.4.4 Menschliche Fehler

Menschliche Fehler gelten als häufigste Ursache für Unfälle auch und ganz besonders in technischen Systemen. Verschiedene Statistiken gehen davon aus, dass die Mehrzahl aller technischen Unfälle bzw. Katastrophen auf menschliche Fehler zurückgeführt werden können [INP84], [INP85]. Eine diesbezügliche Untersuchung bezogen auf das Bahnsystem weist anhand der Unfallstatistik der DB AG nach, dass 96% der Unfälle mit Verletzungen von Fahrgästen, die auf die Betriebsführung zurückgehen, auf menschlichen Fehlern basieren [BRA05a]. Der Begriff *Betriebsführung* umfasst in diesem Zusammenhang alle Aktivitäten des Bedieners an den Anlagen sowie den dazugehörigen organisatorischen Rahmen (z. B. Regelwerke, Anweisungen).

Die Möglichkeiten im Fehlerumgang sind vielschichtig und deren Wirksamkeit hängt von der jeweiligen Systemumgebung und den entsprechenden Randbedingungen ab. Als ein probates Mittel gegen menschliche Fehler wird oft Routine genannt. Durch sie wird die Analyse von Handlungen durch den Menschen erleichtert bzw. überflüssig und somit die Aktivität automatisiert (vgl. Bild 17). Dieses bringt in aller Regel einen Sicherheitsgewinn mit sich, da die menschliche Fehlerrate sinkt. Allerdings birgt zuviel Routine wiederum Gefahren. Dieses verdeutlicht die Tatsache, dass viele schwere Unfälle nicht von Anfängern mit mangelnder Prozesskenntnis, sondern erfahrenen Anwendern verursacht werden. Aufgrund ihrer Erfahrung fühlen sie sich in besonderen Situationen zu sicher, leiden an mangelnder Sensibilisierung für Risiken und neigen dadurch zu Unvorsichtigkeit bzw. verstoßen leichtfertig gegen Sicherheitsbestimmungen [REA94].

Grundsätzlich ist davon auszugehen, dass es keinen unfehlbaren Menschen gibt. Wird der Beobachtungszeitraum ausreichend lang gewählt, begehen selbst erfahrene und zuverlässige Personen Fehler, da diese unmittelbar zur menschlichen Existenz gehören. Angesichts dieser Tatsache ist es falsch, von „menschlichem Versagen“ zu sprechen, denn Fehler zu machen, ist eine grundlegende Eigenschaft des Menschen und insofern völlig normal. Zudem sind die meisten Fehler harmlos, lassen sich leicht korrigieren oder werden durch die Technik abgewiesen. Probleme entstehen erst bei sicherheitsrelevanten Aufgaben in komplexen Systemen, denn der Mensch ist nicht geeignet, schwer durchschaubare Systeme zu beherrschen. Innerhalb komplexer Prozesse wirken viele Faktoren zusammen, bei deren Überschaubarkeit der Mensch an Grenzen gerät.

Die begrenzte menschliche Aufnahmefähigkeit ist auch der Grund dafür, warum der Schnittstelle zwischen Mensch und Technik eine wichtige Rolle zukommt. Die Mensch-Maschine-Schnittstelle (MMI) umfasst diejenigen Faktoren, welche die Wahrnehmungsmöglichkeiten und Handlungsoptionen hinsichtlich des Umgangs mit der Technik betreffen. Der unzureichend organisatorisch abgestimmte Übergang zwischen Mensch und Maschine ist Hintergrund vieler Unfälle, die später vordergründig auf menschliche Fehler zurückgeführt werden. „Im Grunde genommen nimmt auch das Organisationsverschulden seinen Anfang in menschlichem Versagen“ [TRI07]. Organisatorische Fehler können mithin als Folge menschlicher Fehlhandlungen verstanden werden. Gleichzeitig führen die von der jeweiligen Organisation (z. B. Betreiber, Hersteller, Aufsichtsbehörde) bereitgestellten Randbedingungen (z. B. Qualität des Arbeitsplatzes bzw. der Arbeitsmittel, Informationszugang) zu einem für menschliche Fehler mehr oder minder anfälligen Arbeitsumfeld.

Menschliche und organisatorische Fehler stehen meist in einem engen kausalen Zusammenhang (vgl. Bild 16). Im Rahmen von Sicherheitsbetrachtungen bedarf es deren strukturierter Analyse, denn auf höherer Organisationsebene hervorgerufenen Mängel

führen oft auf der „Arbeitsebene“ zu menschlichen Fehlern, die das Organisationsversagen im Falle eines Unfalls zur Folge haben können.

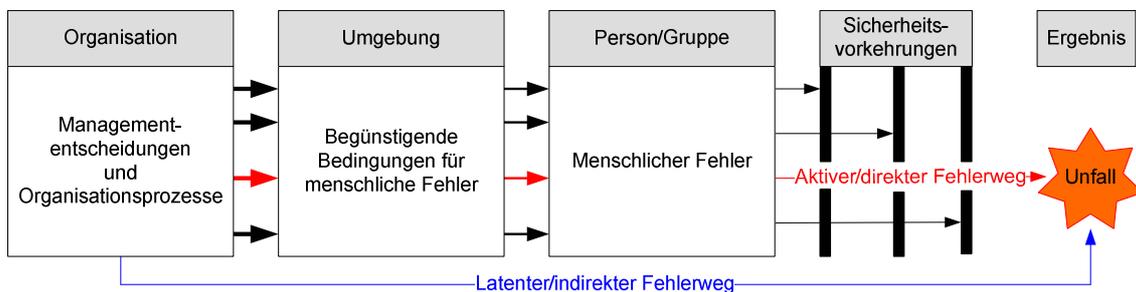


Bild 16: Kausale Zusammenhänge für organisatorische Fehler nach Reason [REA94]

Auf eine Beschreibung organisatorischer Fehler wird im Rahmen dieser Arbeit verzichtet, da diese maßgeblich von der Sicherheitskultur der jeweiligen Organisation abhängen.

4.4.4.1 Einteilung menschlicher Fehler

Zur Auswertung und Zuordnung der Grundursachen von bedarf es der Klassifizierung menschlicher Fehler. Da es im Schrifttum (z. B. [HIN93], [MON99], [BÖR04], [FEN04]) keine einheitliche Klassifizierung menschlicher Fehler gibt, werden nachfolgend das 3-Ebenen-Modell von Rasmussen [RAS80] sowie das darauf aufbauende Modell der organisationalen Unfallverursachung von Reason [REA94] analysiert und darauf basierend ein Vorschlag zur Einteilung menschlicher Fehler unterbreitet.

3-Ebenen-Modell nach Rasmussen

Das fehlerorientierte Modell von Rasmussen zielte im Rahmen seiner Entwicklung ursprünglich nur auf die Analyse von Fehlern ab, die bei der Ausübung der Kontrollaufsicht von sicherheitsrelevanten Industrieanlagen insbesondere bei Notfällen begangen wurden. Die Unterscheidung zwischen den drei Ausführungsebenen Fähigkeit, Regel und Wissen (vgl. Bild 17) kann inzwischen als Standard bei Betrachtungen hinsichtlich der menschlichen Zuverlässigkeit angesehen werden.

Fertigkeitsbasierte Ebene

In der fertigkeitbasierten Ebene werden Handlungen automatisch, d. h. ohne bewusste Kontrolle ausgeführt. Dazu gehören Automatismen und Routinetätigkeiten, wie das Einleiten des Bremsvorganges durch den Triebfahrzeugführer bei entsprechender Signalisierung.

Regelbasierte Ebene

Die regelbasierte Ebene ist dadurch geprägt, dass das Handeln eine bewusste Zuwendung des Menschen zur Situation verlangt. Ist die jeweilige Situation durch unbekannte Bedingungen geprägt oder verfügt der Mensch nicht über ausreichendes Wissen hinsichtlich potenzieller Möglichkeiten, einen gewünschten Sollzustand zu erreichen, so sind Problemlösekompetenzen erforderlich, mit deren Hilfe der Betreffende neue Handlungsweisen für diese neuartigen Situationen schaffen kann. Gleiches gilt für den Fall, dass der gewünschte Sollzustand bisher unbekannt sein sollte. Diese erfolgt durch die Analyse des Geschehens und anschließender Anwendung bereits erworbener und verfügbarer „Wenn-Dann-Regeln“. Damit die erlernten Regeln ausgeführt werden können, müssen sie bewusst im Gedächtnis abgerufen und nachvollzogen werden, wofür mehr Zeit benötigt wird als bei fertigkeitbasierten Handlungen.

Fehler beruhen vor allem auf Erinnerungsproblemen, Versäumnissen beim Prüfen der Situation, deren Fehleinschätzung und dadurch bedingte falsche Anwendung der Regeln, durch unzutreffenden Abruf der Prozeduren und Verwechslungen der Handlungsreihenfolge. Somit verlangt das regelbasierte Verhalten eine Hierarchie von Regeln. Als Beispiel sollen nachfolgend mögliche Regeln für den Fahrdienstleiter im Fall der Rotausleuchtung eines Fahrwegelementes am Monitor eines elektronischen Stellwerkes dienen:

Regel 1: „Wenn Rotausleuchtung eines Fahrwegelementes, dann Gleisabschnitt besetzt“

Regel 2: „Wenn Besetzung des Gleisabschnitts durch Fahrzeug nicht anzunehmen, dann Gleisfreimeldeeinrichtung möglicherweise defekt“

Regel 3: „Wenn Gleisfreimeldeeinrichtung möglicherweise defekt, dann Abschnittsprüfung durch Hinsehen“

Regel 4: „Wenn Abschnittsprüfung durch Hinsehen vom Fahrdienstleiter nicht möglich, dann Personal vor Ort beauftragen“

Regel 5: „Wenn kein Personal vor Ort, dann Räumungsprüfung einführen“

Der Fahrdienstleiter wird nach Prüfung und Vergleich der verfügbaren Regeln eine Entscheidung treffen. Diese Liste ist lediglich ein Teil der notwendigen Regeln, die erforderlich sind, um die Situation fehlerfrei zu meistern. An dieser Stelle ist bereits deutlich erkennbar, dass die Qualität der menschlichen Handlung auf dieser Ebene unmittelbar von der Qualität der Regeln, deren Anwendbarkeit sowie deren Kenntnis abhängt.

Wissensbasierte Ebene

Die wissensbasierte Ebene ist dann erreicht, wenn Probleme auftreten, die nicht durch die beiden bereits beschriebenen Ebenen abgedeckt werden, also weder durch Automa-

tismen noch durch Regeln gelöst werden können. An dieser Stelle sind allgemeines Wissen über das Systemverhalten, die Charakteristik der Randbedingungen und die Ziele, die erreicht werden müssen, gefragt. Diese Ebene ist typisch für unmittelbar geplante Handlungen und bewusste analytische Prozesse bei denen gespeichertes Wissen verwendet wird. Beispiele aus dem Eisenbahnbereich bilden Diagnosen, Entscheidungen und Problemlöseverhalten bei dispositiven Entscheidungen. In dieser Ebene ist der Mensch besonders empfänglich für Fehler und benötigt erheblich mehr Zeit, um zu einer Entscheidung zu gelangen. Fehler entstehen durch begrenzte Ressourcen (z. B. Zeit, Informationen) bzw. durch unvollständiges oder fehlerhaftes Wissen.

Die drei Ebenen menschlicher Informationsverarbeitung stellen allerdings keine Wertigkeit der Entscheidung dar. Vielmehr verkörpert jede Ebene für verschiedene Verhaltensformen in unterschiedlichen Situationen ein Merkmal sicheren Verhaltens, wenn die Wahl automatisch auf die richtige Handlungsebene unter den gegebenen Umständen fällt. Dabei sinkt die Vertrautheit mit der gestellten Aufgabe oder der Umgebung von der wissensbasierten zur fertigkeitbasierten Ebene. Bild 17 fasst die drei Verhaltensebenen zusammen.

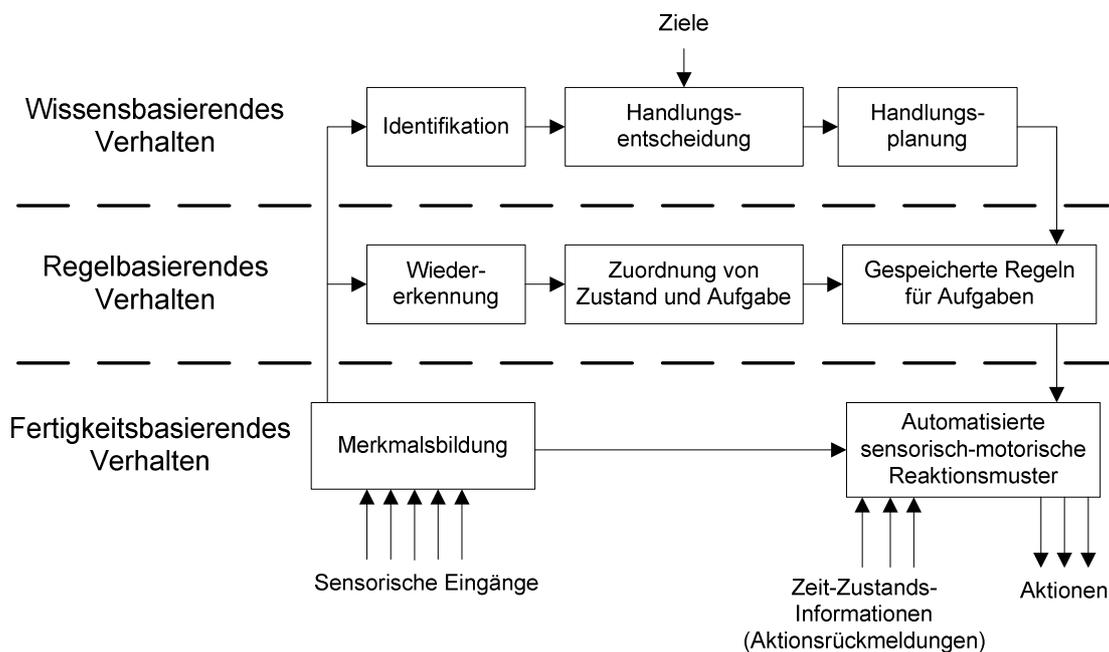


Bild 17: 3-Ebenen-Modell der menschlichen Informationsverarbeitung nach Rasmussen [RAS80]

Modell der organisationalen Unfallverursachung nach Reason

Auf der Grundlage des oben beschriebenen Modells von Rasmussen entwickelte Reason [REA94] eine Kategorisierung sicherheitsgefährdender Handlungen. Dabei wird zwischen unbeabsichtigten und beabsichtigten Handlungen unterschieden. Sicherheitsgefährdende Handlungen sind in diesem Zusammenhang:

- Patzer
- Schnitzer
- Fehler
- Verstöße

Ein *Verstoß* wird bei bewusster Akzeptanz einer potenziellen Gefahr begangen, wie das bewusste Vorbeifahren durch den Triebfahrzeugführer am Halt gebietenden Signal oder das Nichttragen einer Warnweste des Instandhaltungspersonals im Gleisbereich. Verstöße können eindeutig der Gruppe der beabsichtigten Handlungen zugeordnet werden.

Schnitzer und *Patzer*, zusammen als *Versehen* bezeichnet, sind auf mangelnde Aufmerksamkeit und/oder Speicherdefizite zurückzuführen und somit der Gruppe der unbeabsichtigten Handlungen zuzuordnen. Derartige Handlungen sind dadurch gekennzeichnet, dass einerseits die Ausführung einer weitgehend automatisierten Aufgabe in vertrauter Umgebung erfolgt und andererseits die Aufmerksamkeit des Menschen deutlich durch etwas anderes als die gerade ausgeübte Tätigkeit beeinträchtigt wird. Die Ablenkung des Triebfahrzeugführers durch Fahrgäste bei der Übermittlung eines schriftlichen Befehls an den Fahrdienstleiter bildet ein Beispiel dafür.

Patzer entstehen durch die unbeabsichtigte Aktivierung weitgehend automatisierter Prozesse und gehen oft mit einer unzureichenden Überwachung der Aufmerksamkeit des Menschen einher. Folglich ist bei ihnen die Aufmerksamkeit nicht auf die gerade durchgeführte Routinetätigkeit (z. B. Fahrzeugführung) gerichtet. Daraus folgt die Erkenntnis, dass je seltener eine Handlung erfolgt, desto mehr kontrollierende Überwachung des menschlichen Handelns ist erforderlich. Als Beispiel dient das Betätigen eines Schlüsseltasters für die visuelle Gleisfreimeldung.

Der Begriff *Fehler* im Rahmen von sicherheitsgefährdenden Handlungen wird bei Reason nur auf beabsichtigte Handlungen angewendet. In Bezug auf unbeabsichtigte Handlungen hat der Begriff *Fehler* keine Bedeutung, da „Fehlertypen entscheidend auf zwei Arten des Versagens beruhen: auf dem Misserfolg, wenn Handlungen nicht so wie beabsichtigt ablaufen (*Patzer* und *Schnitzer*) und auf Misserfolgen, wenn beabsichtigte Handlungen nicht die erwünschten Folgen haben (*Fehler*)“ [REA94].

Einige Beispiele für *Patzer*, *Schnitzer*, *Fehler* und *Verstöße* sind in Bild 18 dargestellt.

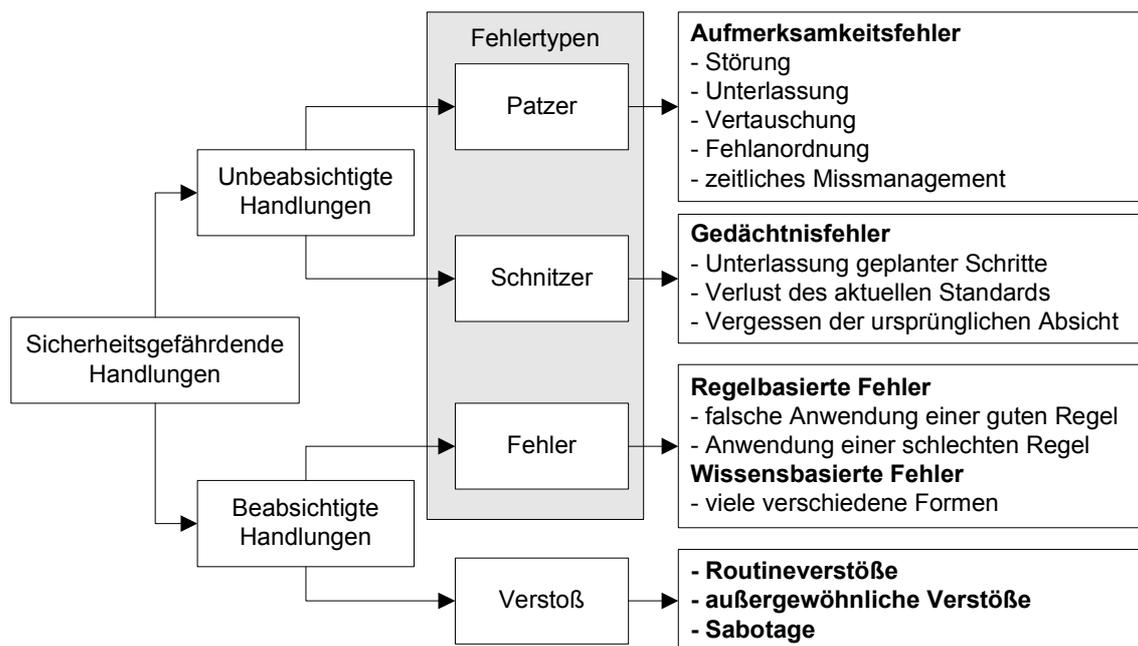


Bild 18: Einteilung sicherheitsgefährdender Handlungen nach Reason [REA94]

Vereinfacht kann gesagt werden, dass ein Patzer oder Schnitzer dann auftritt, wenn die *Handlung* nicht so verläuft wie (ursprünglich) gewollt und dadurch eine Diskrepanz zwischen gewünschter und tatsächlicher Handlung entsteht. Ein Fehler hingegen liegt vor, wenn die *Absicht* nicht angemessen ist. Daraufhin kommt es zur Diskrepanz zwischen (ursprünglich) geplanter Absicht und den tatsächlichen Folgen. Patzer und Schnitzer nach [REA94] charakterisieren damit „zufällige menschliche Fehler“ (vgl. 4.4.1.1), Fehler hingegen „systematische menschliche Fehler“ (vgl. 4.4.1.2).

Basierend auf der Analyse der Modelle menschlicher Denk- und Handlungsweisen von Rasmussen [RAS80] und Reason [REA94] wird in Tabelle 1 ein Vorschlag zur Einteilung menschlicher Fehler hinsichtlich ihres Typs, ihrer Art und des Bewusstseins der Handlung unterbreitet. Dabei wird die Liste der Fehlertypen gemäß Reason (vgl. Bild 18) um den des Verstoßes erweitert.

Bezeichnung des Fehlertyps	Bezeichnung der Fehlerart	Bewusstsein der Handlung	Beispiel
Patzer und Schnitzer (Diskrepanz zwischen gewünschter und tatsächlicher Handlung)	zufällige Fehler	unbewusst	- Irrtümliche Annahme des Sehens eines Ersatzsignals durch Tf - Haltstellen eines Fahrt zeigenden Signals durch Fdl zur Unzeit - Versehentliches Vergessen der visuellen Gleisfreimeldung durch Fdl
Fehler (Diskrepanz zwischen geplanter Absicht und tatsächlichen Folgen)	systematische Fehler	bewusst	- Korrekte Anwendung einer falsch vorgegebenen Regel bei Rotausleuchtung eines Fahrwegelements durch den Fdl - Fehlerhaftes Verhalten des Fdl bei Rotausleuchtung eines Fahrwegelements
Verstoß			- Vorsätzliches Nichttragen einer Warnweste im Gleisbereich - Vorbeifahrt des Tf am ausgefallenen, Halt gebietenden Signal

Tabelle 1: Klassifikation und Beispiele menschlicher Fehler im Bahnsystem

4.4.4.2 Ursachen menschlicher Fehler

Grundsätzlich können menschliche Fehler in Systemen mittels zweier Erklärungsansätze begründet werden [REA94]:

- fehlerhafte Passung („Mismatch-Gedanke“)
- widersprüchliche Arbeitsanforderungen („Harrisburg-Syndrom“)

Fehlerhafter Passung

Fehlerhafte Passung bedeutet, dass eine Diskrepanz zwischen den Verhaltensanforderungen des technischen Systems und den Handlungsmöglichkeiten der am Prozess beteiligten Akteure besteht. Diese sollen möglichst alle Situationen vorhersehen und in diesen korrekt handeln, was allerdings einerseits wegen der Systemkomplexität und andererseits wegen der begrenzten menschlichen Aufmerksamkeit, Wahrnehmungs-, Verarbeitungs- und Prognosefähigkeit unmöglich ist.

Widersprüchliche Arbeitsanforderungen

Eine Erklärung für Fehler liefern widersprüchliche Arbeitsanforderungen. Einerseits versuchen Systementwickler den Menschen als fehleranfälligen Teil des Systems weitgehend aus dem Prozess herauszuhalten, sodass er regulär nicht ins System einzugreifen braucht. Infolgedessen verlernt der Bediener allerdings die bereits erworbenen Kompe-

tenzen wieder. Gleichzeitig wird ihm aber die Verantwortung in der Rückfallebene⁸ (vgl. Abschnitt 5.3) übertragen, wo er sogar bei unvorhergesehenen Situationen mit höchster Kompetenz und zudem zeitnah eingreifen muss. Erschwerend kann hinzukommen, dass er in einem künstlichen Arbeitsumfeld agiert, weit vom Prozess entfernt ist und die Rückmeldungen über die Wirksamkeit der eigenen Eingriffe abstrakt sind. Beispiele dafür bieten Bedienplätze in Betriebszentralen (BZ).

Diese beschriebene Problematik, die sich während des Betriebes eines Systems darstellt, wird durch die Fehleranfälligkeit der Systementwickler ergänzt. Diese unterliegen der Gefahr, bei der Planung und Entwicklung Fehler in das System hineinzubringen, die erst später im Betrieb offenbart werden. In diesem Zusammenhang spricht man von systematischen Fehlern (siehe Abschnitt 4.4.1.2).

Beide Erklärungsansätze, fehlerhafte Passung sowie widersprüchliche Arbeitsanforderungen, führen letztlich zur Erkenntnis, dass die Fehleranfälligkeit des Menschen im Wesentlichen von drei Faktoren abhängt:

- dessen Eigenschaften, Fähigkeiten und Fertigkeiten,
- der Art der jeweiligen Tätigkeit sowie
- den konkreten Randbedingungen des Tätigkeitsumfeldes.

Diese Erkenntnis kann als Basis für eine zielorientierte Sicherheitsstrategie verstanden werden, die den Menschen als einflussreichen Akteur im Gesamtsystem integriert.

4.4.4.3 Konsequenzen aus menschlichen Fehlern

Aus den obigen Ausführungen erwächst die Frage, welche Möglichkeiten es gibt, die Gefährdungspotenziale von Systemen zu verringern. Die Tatsache, dass Fehler im menschlichen Handeln unvermeidlich sind, führt somit zu der Forderung im Rahmen der Systementwicklung nicht nur Fehler möglichst auszuschließen, sondern zudem mit den Konsequenzen aus Fehlern umzugehen und Bewältigungsstrategien zu entwickeln. Fehler dienen daher besonders in frühen Phasen des Systemlebenszyklus als Lernquelle, um geeignete und effiziente Schutzmaßnahmen in späteren Phasen ergreifen zu können.

Grundsätzlich kann der Einfluss menschlicher Fehler auf ein System auf drei Arten vermieden werden [FEN04]:

- Verwendung geeigneter Methoden zur Gewährleistung der fehlerfreien Tätigkeit des Menschen (z. B. durch hohe Qualifikation des Menschen für die jeweilige Tätigkeit),

⁸ Im Rahmen von Sicherheitsbetrachtungen im Allgemeinen und im Bahnsystem im Speziellen wird zwischen Regelebene und betrieblicher bzw. technischer Rückfallebene unterschieden [PRO07b].

- Verwendung geeigneter Methoden zur Erkennung und Korrektur menschlicher Fehler (z. B. durch gezielte und ständig wiederholte Prüfungen und diversitäre Arbeits- und Prüfverfahren),
- Einsatz technischer Lösungen zur Verhinderung fehlerhafter Handlungen.

Da der Einfluss des Menschen ein System über seinen gesamten Lebenszyklus hinweg begleitet, sehen u. a. die aktuellen Normen im Bereich Bahnsicherheit (DIN EN 50126, DIN EN 50128, DIN EN 50129) Maßnahmen vor, mit deren Hilfe ein erforderlicher Grad an systematischer Sicherheit erzielt werden soll. Die diesbezüglichen Anforderungen hinsichtlich der Begrifflichkeiten:

- Qualitätsmanagement
- Sicherheitsmanagement
- technischer Sicherheitsbericht

werden in diesen Normen hinreichend beschrieben.

4.5 Ausfall

Die bereits erwähnte Tatsache der uneinheitlichen Definitionen des Begriffs *Fehler* im Schrifttum trifft ebenso auf den Begriff *Ausfall* zu. Ein oft verwendetes Synonym von Ausfall ist Versagen. So wird in der DIN EN 61508-4 Ausfall und Versagen im Sinne der englischen Übersetzung „failure“ verwendet und als „Beendigung der Fähigkeit einer Funktionseinheit, eine geforderte Funktion auszuführen“ [DIN02] definiert. Der Ausfall ist somit, wie bereits in Abschnitt 4.4 beschrieben, ein Ereignis und kann als der Zeitpunkt des Aussetzens der Ausführung einer festgelegten Funktion verstanden werden.

4.5.1 Ausfallarten

In Analogie zur Einteilung der Fehlerarten in Abschnitt 4.4.1 wird bei den Ausfallarten zwischen zufälligen Ausfällen (vgl. Abschnitt 4.4.1.1), welche statistisch unabhängig auftreten und meist durch das Zusammenwirken mehrerer voneinander unabhängiger Faktoren entstehen, und systematischen Ausfällen (vgl. Abschnitt 4.4.1.2) unterschieden. Ebenso erfolgt eine Unterscheidung zwischen Einzelausfällen (vgl. Abschnitt 4.4.1.3) und Mehrfachausfällen (vgl. Abschnitt 4.4.1.4). Die in den jeweiligen Abschnitten genannten Eigenschaften gelten ebenso für Ausfälle nach Inbetriebnahme des Systems.

4.5.2 Quellen für Ausfälle

Grundsätzlich führen entweder technische Fehler (vgl. Abschnitt 4.4.3) oder menschliche Fehler (inklusive organisatorischer Fehler, vgl. Abschnitt 4.4.4) zu einem Ausfall. Die Praxis zeigt, dass oft Kombinationen der Fehlerquellen Technik, Mensch und Organisation, letztere werden oft auch als latente Fehler bezeichnet, zunächst zu Ausfällen

und später zu Unfällen führen, falls diese Fehler bzw. Ausfälle nicht oder zu spät offenbart werden.

4.5.3 Ausfallzeitpunkte

Betrachtet man die Häufigkeit von Ausfällen zu einem bestimmten Zeitpunkt erhält man die Ausfallrate λ . Bei beliebig häufiger Beobachtung zu infinitesimal kleinen Betrachtungszeiträumen über eine gewisse Zeitspanne hinweg ergibt sich die Ausfallkurve für eine Komponente. Bei vielen Komponenten treten Ausfallkurven in Form von „Badewannen“, wie in Bild 19 dargestellt, auf.

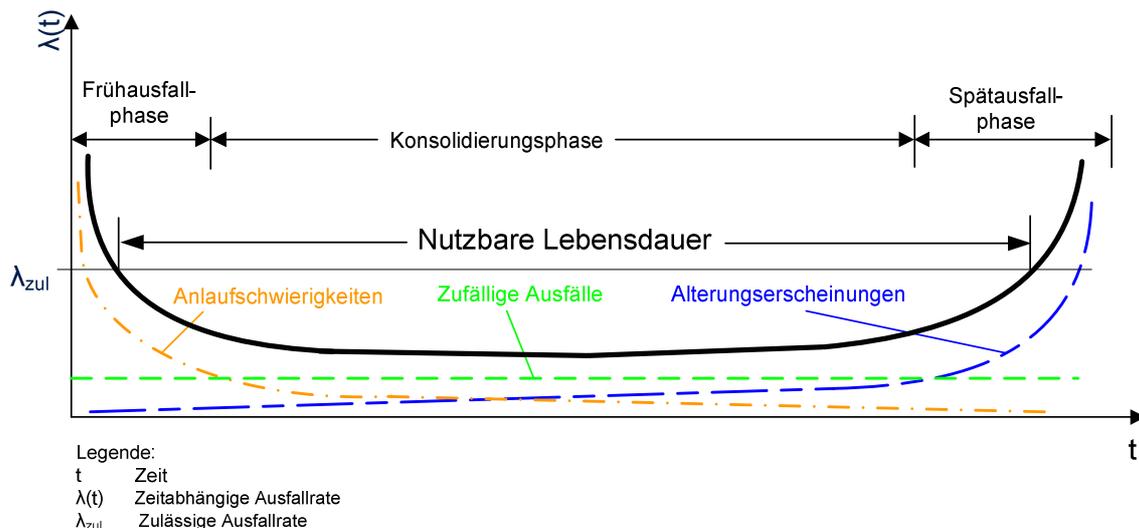


Bild 19: Badewannenkurve nach [FIS90]

Im Bereich der Konsolidierungsphase wirken vornehmlich zufällige Ausfälle. Die Ausfallrate λ ist in diesem Bereich annähernd konstant und am niedrigsten. Sicherheitstechnische Anlagen sollten möglichst im Bereich der Konsolidierungsphase betrieben werden, da sich dann die Instandhaltung auf die Beseitigung zufälliger Ausfälle beschränkt.

4.6 Störung

Eine Störung ist ein externes Ereignis, das eine oder mehrere Systemfunktionen während der Betriebsphase verhindert oder beeinträchtigt. Sie tritt entweder vorübergehend oder ständig auf. Diese *externen* Ereignisse können mechanische, elektrische oder thermische Gründe haben oder klima- bzw. witterungsbedingt sein. Störungen können zu jeder Zeit auf ein System einwirken, sich aber nur nach Inbetriebnahme des Systems auswirken. Störungen sind hinsichtlich ihrer Folgen für das System somit mit Ausfällen vergleichbar. Nachfolgend werden einige Beispiele genannt, die für die korrekte Funktion der Komponenten des Bahnsystems hinderlich sein können:

- Erschütterungen (z. B. durch schlechte Gleislage)
- Verunreinigungen im Gleisbereich (z. B. Metallspäne, Salze)
- Verunreinigungen in der Luft (z. B. Staub, Rauch, Dampf)

- Temperatureinflüsse (z. B. Frost, starke Sonneneinstrahlung)
- Luftfeuchtigkeit (z. B. Kondenswasserbildung)
- Luftdruck (z. B. horizontale und vertikale Schwankungen)
- witterungsbedingte elektrische Beeinflussung (z. B. Blitzschlag)
- elektrische Einflüsse (z. B. Traktionsströme, Weichenheizung)

Eine Störung ist jedes Ereignis, das den Bahnbetrieb aus der Systemumgebung heraus behindert. In technischer Hinsicht stellen Störungen damit all diejenigen externen Ereignisse dar, die das Bahnsystem in seiner Funktionsfähigkeit beeinträchtigen. Im Rahmen des Sicherheitsnachweises muss gezeigt werden, dass alle ermittelten Gefährdungen, die aus derartigen Störungen resultieren können, vom System beherrscht bzw. durch Schutzmaßnahmen abgefangen werden.

Besonders schwierig und meist unlösbar ist die Beachtung sämtlicher denkbarer Gefährdungen, die aus Störungen durch vorsätzliche menschliche Fehlhandlungen im Sinne von „Security“ auftreten können. Entsprechenden Schutzmaßnahmen (z. B. Umzäunung, Aufstellen von Warnschildern) sind meist finanzielle Grenzen gesetzt.

4.7 Kategorisierung von Fehlern, Ausfällen und Störungen

Auf der Grundlage der Ausführungen in Kapitel 4 erfolgt in Tabelle 2 die zusammenfassende Kategorisierung von Fehlern, Ausfällen und Störungen unter Verwendung nachfolgender Parameter:

- F/A/S-Art
- hemmend
- gefährlich
- zufällig (aus Übersichtsgründen nicht in Tabelle 2 integriert)
- systematisch (aus Übersichtsgründen nicht in Tabelle 2 integriert)
- F/A/S-Quelle
- Menschen
- Technik
- Organisation
- Lebenszyklusphase
- Planung, Entwicklung, Fertigung und Installation
- Betrieb
- Regelbetrieb
- Abweichung vom Regelbetrieb
- Instandhaltung

		Fehler		Ausfall		Störung		
		hemmend	gefährlich	hemmend	gefährlich	hemmend	gefährlich	
Menschen	Planung, Entwicklung, Fertigung und Installation		$\lambda_{hmF,PEFI}$	$\lambda_{gmF,PEFI}$	---	---	---	---
	Betrieb	Regelbetrieb	$\lambda_{hmF,RB}$	$\lambda_{gmF,RB}$	---	---	$\lambda_{hmS,RB}$	$\lambda_{gmS,RB}$
		Abw. vom Regelbetrieb	$\lambda_{hmF,ARB}$	$\lambda_{gmF,ARB}$	---	---	$\lambda_{hmS,ARB}$	$\lambda_{gmS,ARB}$
		Instandhaltung	$\lambda_{hmF,IH}$	$\lambda_{gmF,IH}$	---	---	$\lambda_{hmS,IH}$	$\lambda_{gmS,IH}$
Technik	Planung, Entwicklung, Fertigung und Installation		$\lambda_{htF,PEFI}$	$\lambda_{gtF,PEFI}$	---	---	---	---
	Betrieb	Regelbetrieb	$\lambda_{htF,RB}$	$\lambda_{gtF,RB}$	$\lambda_{htA,RB}$	$\lambda_{gtA,RB}$	$\lambda_{htS,RB}$	$\lambda_{gtS,RB}$
		Abw. vom Regelbetrieb	$\lambda_{htF,ARB}$	$\lambda_{gtF,ARB}$	$\lambda_{htA,ARB}$	$\lambda_{gtA,ARB}$	$\lambda_{htS,ARB}$	$\lambda_{gtS,ARB}$
		Instandhaltung	$\lambda_{htF,IH}$	$\lambda_{gtF,IH}$	$\lambda_{htA,IH}$	$\lambda_{gtA,IH}$	$\lambda_{htS,IH}$	$\lambda_{gtS,IH}$
Organisation	Planung, Entwicklung, Fertigung und Installation		$\lambda_{hoF,PEFI}$	$\lambda_{goF,PEFI}$	---	---	---	---
	Betrieb	Regelbetrieb	$\lambda_{hoF,RB}$	$\lambda_{goF,RB}$	---	---	---	---
		Abw. vom Regelbetrieb	$\lambda_{hoF,ARB}$	$\lambda_{goF,ARB}$	---	---	---	---
		Instandhaltung	$\lambda_{hoF,IH}$	$\lambda_{goF,IH}$	---	---	---	---

Legende:

λ	Fehler- bzw. Ausfallrate	F	Fehler
h	hemmend	A	Ausfall
g	gefährlich	S	Störung
t	technisch	PEFI	Planung, Entwicklung, Fertigung und Installation
m	menschlich	RB	Regelbetrieb
o	organisatorisch	ARB	Abweichung vom Regelbetrieb
		IH	Instandhaltung

Tabelle 2: Kategorisierung von Fehlern, Ausfällen und Störungen

Tabelle 2 verdeutlicht nochmals die bereits in Bild 15 illustrierte Erkenntnis, dass (technische, menschliche oder organisatorische) Fehler sowohl während der Planung, Entwicklung, Fertigung und Installation als auch während des Bahnbetriebes und der Instandhaltung negative Auswirkungen auf RAMS im Bahnsystem haben können. Systeminterne (technische) Ausfälle sowie systemexterner (menschliche oder technische) Störungen wirken sich hingegen ausschließlich nach Inbetriebnahme negativ auf RAMS des Bahnsystems aus.

4.8 Fehler, Ausfälle und Störungen im Regelkreis des Bahnsystems

Die Verwendung von Regelkreisen erlaubt sowohl die Einordnung als auch die Analyse der Vielzahl potenzieller F/A/S im jeweils betrachteten System. Bild 20 stellt den generellen Aufbau eines Regelungssystems dar.

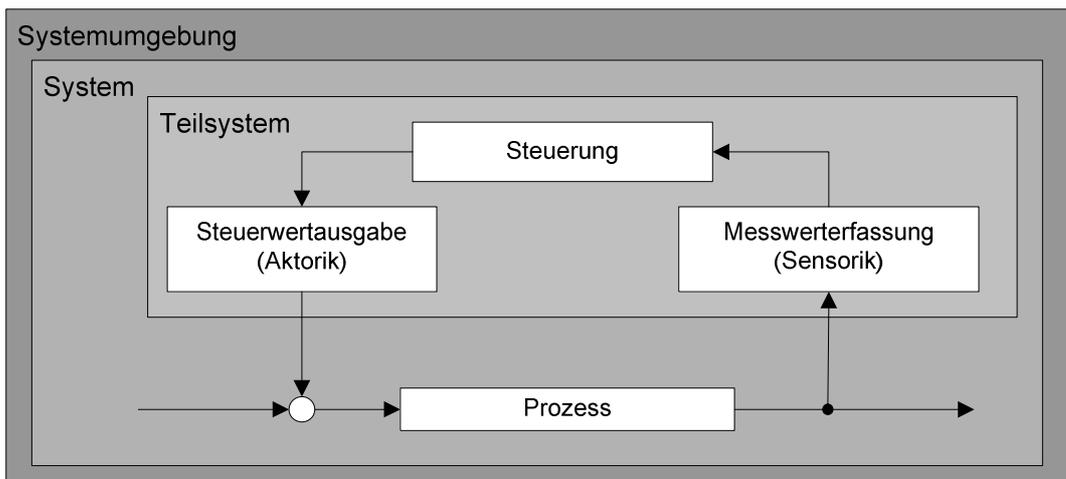


Bild 20: Stellen potenzieller Anomalien im beliebigen Regelungssystem

Kernstück eines Regelkreises bildet die darin befindliche Steuerung. Sie ermittelt auf Grundlage der von Sensoren (z. B. Thermometer, Barometer) erfassten Messwerte (z. B. Temperatur, Luftdruck) entsprechende Stellbefehle (z. B. Temperatur erhöhen, Druck senken). Nach deren Übertragung an die Aktorik (z. B. Fenster, Sperrhahn) werden die Stellbefehle ausgeführt (z. B. Fenster schließen, Sperrhahn öffnen) und beeinflussen den zu steuernden Prozess (z. B. Raumtemperatur, Luftdruck in Brennkammer) in entsprechender Weise (z. B. Raumtemperatur steigt, Luftdruck in Brennkammer sinkt).

Durch den modularen Aufbau des beschriebenen Regelkreises ist es möglich, diesen auf das Bahnsystem zu übertragen (vgl. Bild 21) und zudem auftretende F/A/S den jeweiligen Teilsystemen bzw. Komponenten, deren Wechselwirkungen an Schnittstellen sowie den Informations- und Übertragungswegen zuzuordnen.

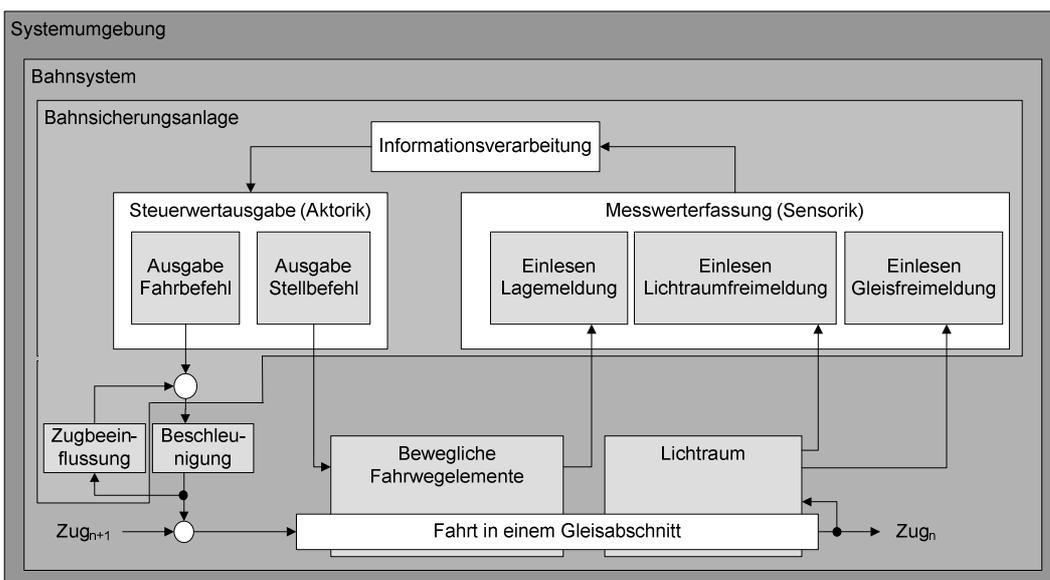


Bild 21: Regelkreis des Bahnsystems [PRO07a]

Im weiteren Verlauf der Arbeit wird es mithin möglich sein, anhand des Regelkreises in Bild 21 F/A/S strukturiert zu analysieren und im Gesamtkontext einzuordnen. Ebenso erlaubt der Regelkreis die Ermittlung von sicherheitsrelevanten Teilsystemen und die anschließende Aufteilung der durch sie zu erbringenden Funktionen auf die in den Teilsystemen befindlichen Komponenten, was für die Ermittlung der Ursachen von Gefährdungen und deren Vermeidung wesentlich ist [TRI06]. Dieses gilt vor allem für die Lebenszyklusphase 11 „Betrieb und Instandhaltung“, in der der Regelkreis ständig durchlaufen wird. Anhand eines Beispiels in Kapitel 5.3.2 werden die betrieblichen Abläufe unter Verwendung eines Szenarios im Verfügbarkeits-Sicherheits-Diagramm ausführlich betrachtet.

5 Sicherungstechnische Grundsätze im Bahnsystem

5.1 Umgang mit Fehlern, Ausfällen und Störungen

Grundsätzlich besteht in sicherheitsrelevanten Systemen die Forderung, dass bei auftretenden oder bestehenden Anomalien in Form von F/A/S keine (übermäßigen) Risiken auf Personen, Güter und die Umwelt wirken dürfen (vgl. Abschnitt 2.2.1). Dies ist dann der Fall, wenn das System eine sicherheitsgerichtete Reaktion ausführt und im Anschluss einen sicheren Zustand einnimmt. Die Basis für die Definition des sicheren Zustandes ist eine fundierte Kenntnis hinsichtlich des F/A/S-Verhaltens der verwendeten Komponenten im System. Diese Kenntnis hat wesentlichen Einfluss auf die Auswahl derjenigen Maßnahmen, die ergriffen werden müssen, um ausreichende Sicherheit zu gewährleisten. Ein (systematischer) Fertigungsfehler kann durch sorgfältige Kontrolle noch vor Inbetriebnahme des Systems festgestellt werden. Ein spontaner (zufälliger) Ausfall während der Betriebsphase ist hingegen nicht zu verhindern. Durch konstruktive Maßnahmen kann aber erreicht werden, dass es zu keiner sicherheitskritischen Fehlfunktion des Systems kommt.

Zur Gewährleistung der erforderlichen Sicherheit in einem System werden folgende Strategien beim Umgang mit F/A/S verfolgt [FEN04], [NAU02], [PRO07b]:

- F/A/S-Ausschluss
- F/A/S-Folgenausschluss
- F/A/S-Folgenbegrenzung

Nachfolgend werden die drei Strategien und ihre Anwendung im Bahnsystem insoweit beschrieben, wie es dem Verständnis der nachfolgenden Kapitel dient. Detaillierte Ausführungen diesbezüglich finden sich in [FEN04].

5.1.1 Ausschluss von Fehlern, Ausfällen und Störungen

Jede Komponente in einem System besitzt bestimmte physikalische Eigenschaften. Ein Ausschluss von Fehlern, Ausfällen und Störungen (F/A/S) kann angenommen werden, wenn diese *unverlierbar* sind, d. h. das Eintreten von F/A/S infolge der Eigenschaften ausgeschlossen werden kann. Komponenten, die im Bahnsystem zum Einsatz kommen, sollen meist hohe mechanische und/oder hohe elektrische Robustheit besitzen, sogenannte Bahnfestigkeit, wobei Erschütterungen im Fahrzeug oder Triebrückströme im Gleisbereich keine Beeinträchtigung der gewünschten Systemfunktionen verursachen dürfen. Ein Schutz wird durch geeignete Werkstoffe (z. B. unverschweißbares Kontaktmaterial), spezielle Konstruktionen (z. B. durch mechanische Stabilität) und entsprechende Herstellungsverfahren (z. B. Verwendung von Checklisten) erreicht. Im

Rahmen des Sicherheitsnachweises wird meist theoretisch und experimentell der Ausschluss aller denkbaren F/A/S dargelegt.

Die Annahme des Ausschlusses von F/A/S kann auch getroffen werden, wenn der Nachweis gelingt, dass die Wahrscheinlichkeit für das Auftreten von F/A/S ausreichend klein ist. Was im konkreten Fall ausreichend ist, wird im Rahmen der Sicherheitsanforderungsspezifikation festgelegt. Praktisch *gelten* dann die physikalischen Eigenschaften *als unverlierbar* und damit *gelten* auch die F/A/S *als ausgeschlossen*. Ein Beispiel für einen technischen Schutz vor F/A/S erzwingt der Ausschluss des Verschweißens von Kontakten oder des Nichtabfallens des Ankers bei Typ N Relais. Nichttechnischen Ausschluss von F/A/S liefert das Verbot des Abstellens von Fahrzeugen in bestimmten Gleisen oder das Verbot des Anbringens von Gleissperren in Hauptgleisen im Geltungsbereich der EBO.

5.1.2 Ausschluss von F/A/S-Folgen

Falls es nicht gelingt, den Ausschluss von F/A/S zu begründen, muss nachgewiesen werden, dass durch bestimmte F/A/S keine gefährlichen Folgen auftreten, d. h. der sichere Zustand eingenommen wird (siehe Abschnitt 5.2.1). Dieser Nachweis basiert auf der Erfüllung folgender grundsätzlicher Sicherheitsanforderung [FEN04]:

- Ungefährlichkeit von Einzel- und Mehrfach-F/A/S
- durch Nichtfortpflanzung von Einzel-F/A/S bzw.
- durch Nachweis der Unabhängigkeit von Einzel-F/A/S

5.1.2.1 Ungefährlichkeit von Einzel-F/A/S

Für jedes sicherungstechnische System besteht gemäß DIN EN 50129 die Forderung, dass keiner der anzunehmenden Einzel-F/A/S einen gefährlichen Zustand (vgl. Abschnitt 5.2.3) herbeiführen, sondern nur einen der zulässigen sicheren Zustände (vgl. Abschnitt 5.2.1) zur Folge haben darf. Im Rahmen des Sicherheitsnachweises muss dieser Forderung nachgekommen werden. Falls dieser Nachweis misslingt, muss die Architektur des Systems geändert werden. In der Praxis wird dann meist auf redundante Strukturen zurückgegriffen.

5.1.2.2 Ungefährlichkeit von Mehrfach-F/A/S

In vielen Systemen besteht neben der Forderung der Ungefährlichkeit von Einzel-F/A/S die der Ungefährlichkeit von (gefährlichen) Mehrfach-F/A/S. Falls eine gemeinsame Fehlfunktion von zwei oder mehr funktionell zusammenwirkenden Komponenten zu einem gefährlichen Zustand führen kann, müssen diese in sicherungstechnischen Systemen voneinander unabhängig sein.

5.1.2.3 Nichtfortpflanzung von Einzel-F/A/S

Der Forderung nach Nichtfortpflanzung von (gefährlichen) Einzel-F/A/S wird in sicherungstechnischen Systemen durch deren schnelle Offenbarung und Behandlung nachgekommen. Dadurch kann das Auftreten von Mehrfach-F/A/S (vgl. Abschnitt 5.1.2.2) vermieden werden. Die F/A/S-Offenbarungszeit hat entsprechend großen Einfluss auf das Sicherheitsniveau.

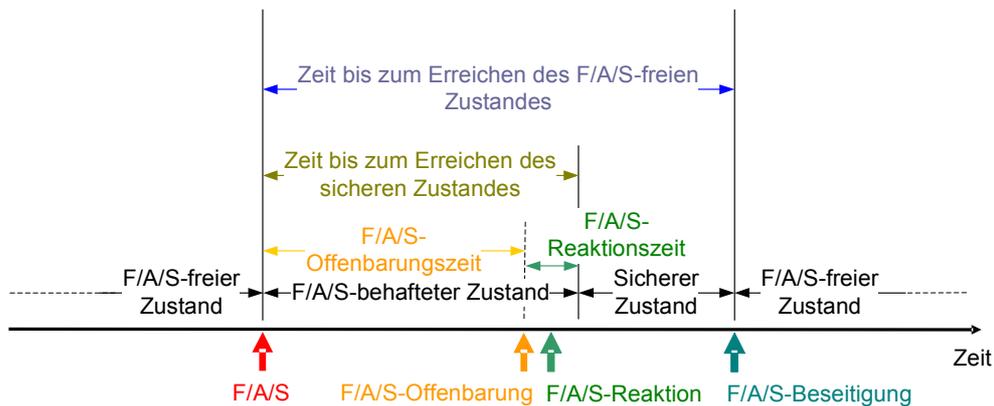


Bild 22: Zeitliche Zusammenhänge der F/A/S-Offenbarung

An dieser Stelle sei darauf hingewiesen, dass die in Bild 22 dargestellte F/A/S-Offenbarungszeit dem Wortsinn nach als Zeitspanne zwischen F/A/S-Eintritt und F/A/S-Offenbarung gewählt wurde. Dieses ist normenkonform, denn gemäß DIN EN 50129 ist die Ausfalloffenerungszeit diejenige „Zeitspanne, die zu dem Zeitpunkt beginnt, an dem ein Ausfall auftritt, und die endet, wenn das Vorhandensein dieses Ausfalls erkannt wird.“ [DIN03b]

Die Reaktionszeit bis zum Erreichen des sicheren Zustandes ist gemäß DIN EN 50129 die „Zeitspanne, die mit dem Entdecken eines Ausfalls beginnt und mit der Einnahme eines sicheren Zustandes endet.“ [DIN03b]

Die praktisch unvermeidbare Zeitspanne zwischen F/A/S-Offenbarung und F/A/S-Reaktion und die F/A/S-Reaktionszeit selbst müssen in Abhängigkeit vom geforderten Sicherheitsniveau möglichst gering gehalten werden. Im Mittelpunkt steht dabei die Forderung, dass F/A/S vor der nächsten sicherheitsrelevanten Funktion offenbart werden müssen. Im Bahnbereich wird eine schnelle F/A/S-Offenbarung mittels betätigungsbezogener (datenflussabhängiger) Prüfung bzw. bei schaltungstechnisch nicht erkennbaren F/A/S durch regelmäßige Prüfungen gewährleistet. In elektronischen Systemen bedient man sich dazu sehr kurzer Überwachungszyklen weit unter einer Sekunde.

5.1.2.4 Unabhängigkeit von Einzel-F/A/S

Die zweite Möglichkeit zur Erfüllung der Forderung nach Ungefährlichkeit von Einzel- und Mehrfach-F/A/S bildet, neben der schnellen Offenbarung von Einzel-F/A/S und Behandlung, die Sicherstellung der Unabhängigkeit von Komponenten bzw. der in ihnen auftretenden oder auf sie wirkenden F/A/S. Daraus leiten sich Forderungen nach Redundanz ab. Diese ist ein probates Mittel, um F/A/S zu kompensieren. Allerdings bedürfen redundante Strukturen besonderer Verfahren und Methoden, damit ihre signaltechnische Unabhängigkeit tatsächlich gegeben ist. Anderenfalls könnte eine gemeinsame Fehlfunktion in Form von systematischen Mehrfach-F/A/S (vgl. Abschnitt 5.1.2.2) zu einem gefährlichen Zustand des Systems führen. Kabel mit Sicherheitsfunktion in Stellwerken werden daher örtlich getrennt verlegt, damit die Gefahr des gleichzeitigen Ausfalls ausgeschlossen werden kann.

Praktisch ist der Nachweis der Unabhängigkeit sehr aufwendig, da ein Einzel-F/A/S die gemeinsame Grundursache für andere ursprünglich als voneinander unabhängig betrachtete Einzel-F/A/S sein kann. Beispielsweise gilt es als unwahrscheinlich, dass zwei redundante Steuerungseinheiten mit getrennten Netzteilen gleichzeitig ausfallen. Falls diese Netzteile aber an einem gemeinsamen Verteiler angeschlossen sind und dessen Stromversorgung durchtrennt wird, tritt genau dieser als unwahrscheinlich geltende Fall ein.

An diesem Beispiel ist deutlich zu erkennen, welche entscheidende Rolle einer exakten Systemdefinition sowie der Wahl der Systemgrenzen bei Sicherheitsbetrachtungen zukommt.

5.1.3 Begrenzung von F/A/S-Folgen

Falls weder der F/A/S-Ausschluss gelingt noch der Ausschluss von F/A/S-Folgen nachgewiesen werden kann, muss zumindest die Wahrscheinlichkeit für gefährliche Folgen beim Eintreten von F/A/S ausreichend klein sein. Im Rahmen der Sicherheitsanforderungsspezifikation muss die zulässige Wahrscheinlichkeit für gefährliche Folgen von F/A/S festgelegt werden. Diese wird in der Literatur auch als der „Grad der Ausfallfolgenbegrenzung“ [FEN04] bezeichnet.

Als Mittel der Begrenzung von F/A/S-Folgen dient einerseits die schnelle Offenbarung von F/A/S (vgl. Abschnitt 5.1.2.3) und andererseits die Begrenzung des möglichen Schadens. Im Bahnsystem erfolgt diese durch Herabsetzung der Geschwindigkeit in der Rückfallebene und der damit einhergehenden Reduzierung der Wahrscheinlichkeit gefährlicher Folgen. Ein Beispiel dafür lieferte die Begrenzung der Geschwindigkeit beim bei der Deutschen Reichsbahn zugelassenen permissiven Fahren.

Zusammengefasst kann festgestellt werden, dass das oberste Ziel der Bahnsicherungstechnik der Ausschluss von F/A/S ist. Infolge technischer und finanzieller Restriktionen verfolgen viele Sicherheitsmaßnahmen in Komponenten und Systemen der Sicherungstechnik aber die Strategie des F/A/S-Folgenausschlusses oder als Minimalziel die F/A/S-Folgenbegrenzung. Bild 23 stellt diese Zusammenhänge grafisch dar:

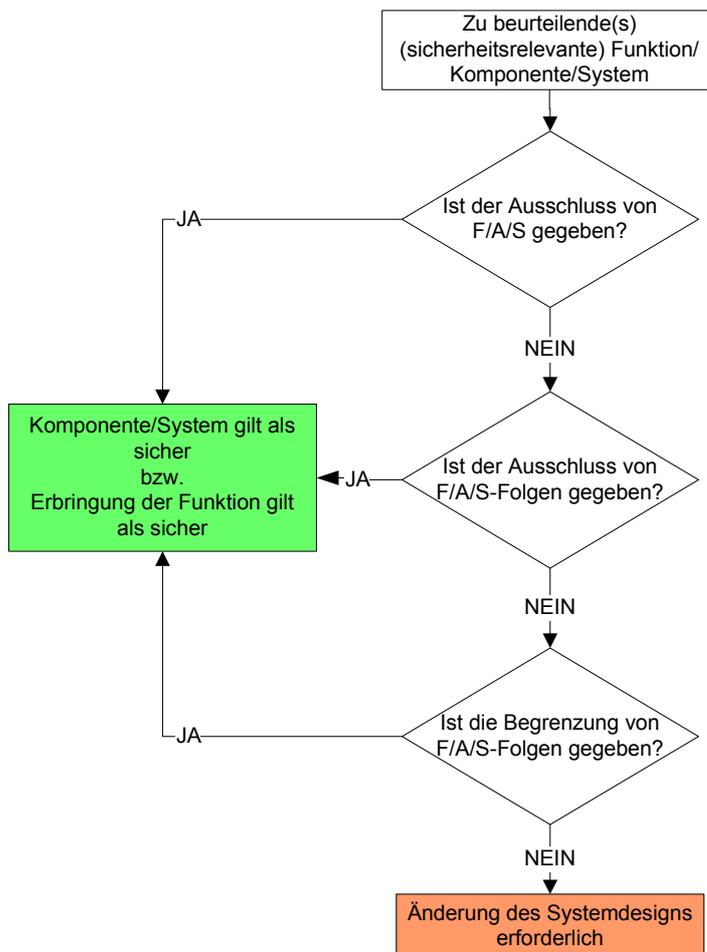


Bild 23: Vorgehensweise beim Umgang mit F/A/S

5.2 Verwendung von Zuständen zur Systemanalyse

5.2.1 Sicherer Zustand

Grundsätzlich besteht an Systeme der Bahnsicherungstechnik die Forderung, dass F/A/S zur Einnahme des sicheren Zustandes führen. Dabei wird der in Grundstellung, d. h. bei Freiheit von F/A/S, eingenommene sichere Ausgangszustand (vgl. Zustand 0 in Bild 26) zwar verlassen, aber sofort ein anderer sicherer Zustand in der Rückfallebene (vgl. Zustand 1 in Bild 26) erreicht. Entsprechend ist auch die Definition des sicheren Zustandes als ein „Zustand, der die Sicherheit weiterhin bewahrt“ [DIN03b] formuliert.

Zudem dürfen zusätzlich auftretende F/A/S nicht das Verlassen des sicheren Zustandes nach sich ziehen. Diese Eigenschaft sicherheitsrelevanter Systeme wird als Fail-Safe-

Prinzip bezeichnet. Ferner muss dieser Zustand solange beibehalten bleiben, bis sämtliche F/A/S behoben wurden. Nur durch entsprechend geschultes Instandhaltungspersonal darf es möglich sein, den sicheren Zustand im Rahmen einer Entstörung zu verlassen.

Im Betrieb des Eisenbahnwesens ist der sichere Zustand der Stillstand des Fahrzeugs. Dieser wird erreicht, indem bestimmte Komponenten unverlierbare technische Zustände (z. B. Abschmelzen einer Sicherung im Lampenstromkreis) einnehmen. Alternativ können mehrere Komponenten eine redundante Speicherung vornehmen (z. B. 2v3-System), wodurch auch der sichere Zustand beibehalten bleibt.

Ein Beispiel für das Erzwingen des sicheren Zustandes ist das Ausschalten der grünen Lampe und das Einschalten der roten Lampe für den Fall, dass im Signalbild Hp 2 (gelbes und grünes Licht) die gelbe Lampe ausfällt. Dieser Ausfall würde einen höherwertigen Geschwindigkeitsbegriff nach sich ziehen, was in Anbetracht des Fail-Safe-Prinzips verhindert werden muss.

Im komplexen Bahnsystem bestehen mehrere sichere Zustände bzw. Rückfallebenen. Diese werden in Abhängigkeit von der Art der F/A/S solange durchlaufen, bis der geeignete (meist energetisch niedrigste) sichere Zustand erreicht wird.

Ein Beispiel für eine derartige Hierarchie an sicheren Zuständen bildet das Ersatzsignal und im Falle dessen Nichtvorhandenseins der schriftliche Befehl an den Lokführer, falls eine Fahrstraße nicht einstellbar ist und somit das Signal nicht in Fahrtstellung gebracht werden kann (vgl. Abschnitt 5.3.2).

Der Definition der sicheren Zustände kommt eine große Bedeutung im Rahmen der Planung und Entwicklung von Komponenten und Systemen der Bahnsicherungstechnik zu. Ein hohes Maß an Prozesskenntnis ist erforderlich, um für alle denkbaren F/A/S den jeweils sicheren Zustand festlegen zu können.

5.2.2 Hemmender Zustand

Verlässt ein System auf Grund von F/A/S den sicheren Ausgangszustand und kann nicht sofort wieder in diesen zurückgeführt werden, geht es in den hemmenden Zustand über. In diesem verbleibt das System, bis es vom Instandhaltungspersonal wieder in den Ausgangszustand überführt wird.

Der Ausfall eines Hauptsignals in Folge eines Aderbruchs und dessen anschließende Dunkelschaltung (vgl. λ_{01} in Bild 26) sowie die nachfolgende Reparatur des Kabels (vgl. μ_{10} in Bild 26) bilden entsprechende Beispiele.

In der Praxis zeigt sich, dass beim Verlassen des hemmenden Zustandes oft der Mensch mit höherer Fehlerrate gegenüber der Technik zum Einsatz kommt. Geeignete Prozedu-

ren zur sicheren Überführung des Systems in den Ausgangszustand sind daher im Rahmen der Planung und Entwicklung des Systems frühzeitig zu erstellen.

5.2.3 Gefährlicher Zustand

Systeme, bei denen nachgewiesen werden konnte, dass F/A/S ausgeschlossen sind oder als ausgeschlossen gelten, können theoretisch keine gefährlichen Zustände hervorrufen. Praktisch kann allerdings die Einnahme eines gefährlichen Zustandes durch ein System nie ganz ausgeschlossen werden. Dieses bedeutet, dass das Fail-Safe-Prinzip bei sicherheitsrelevanten Systemen gefährliche Zustände mit einer möglichst hohen Wahrscheinlichkeit verhindert. Falls ein gefährlicher Zustand dennoch eingenommen wird, muss das System schnellstmöglich wieder in einen sicheren Zustand überführt werden (vgl. Abschnitte 5.1.2.1 und 5.1.2.3).

5.3 Darstellung und Analyse von Systemkennwerten

5.3.1 Verfügbarkeits-Sicherheits-Diagramm

Im Rahmen dieser Arbeit erfolgt auf der Grundlage von Forschungsergebnissen hinsichtlich der Verlässlichkeit von Verkehrssystemen in Verfügbarkeits-Sicherheits-Diagrammen im Allgemeinen [SCH03] deren Anwendung auf das Bahnsystem im Speziellen.

In Verfügbarkeits-Sicherheits-Diagrammen können die verschiedenen Systemzustände grafisch dargestellt werden. Dabei handelt es sich um einen Markow-Graphen, bei dem die x,y-Position der Zustände mit den Systemkennwerten Sicherheit und Verfügbarkeit bewertet wird. Je nach Anzahl der Zustände werden Abstufungen (z. B. sicher, eingeschränkt sicher, unsicher) vorgenommen. Zudem werden die Übergänge zwischen den einzelnen Zuständen mittels zeitbezogener Übergangsraten (Ausfallraten λ_{nm} bzw. Reparaturraten μ_{mn}) ergänzt⁹. Bild 24 verdeutlicht diesen Zusammenhang.

⁹ Im Bereich der Zuverlässigkeitstheorie können die Indizes n und m der Übergangsraten in umgekehrter Reihenfolge auftreten.

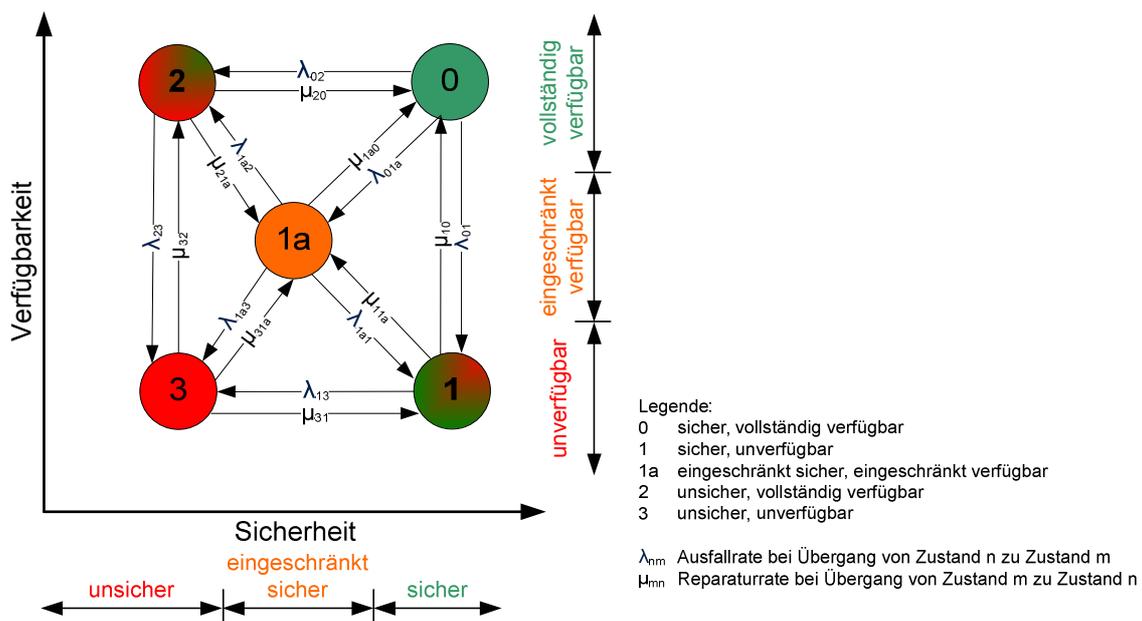


Bild 24: Verfügbarkeits-Sicherheits-Diagramm

5.3.2 Beispiel eines Verfügbarkeits-Sicherheits-Diagramms

Im Folgenden soll das Verfügbarkeits-Sicherheits-Diagramm anhand eines einfachen Beispiels veranschaulicht werden. Ein System besteht aus den Komponenten Hauptsignal (HSig), Ersatzsignal (Zs 1), Fahrdienstleiter (Fdl), Triebfahrzeugführer (Tf), Instandhaltungspersonal (IHP) Zug und Zugbeeinflussung mit 2000-Hz-Magnet (PZB). Das folgende Szenario kann dabei eintreten:

Ein Zug steht vor einem HSig und soll aus dem Bahnhof ausfahren. Sollte das HSig infolge eines technischen Ausfalls nicht in Fahrtstellung gebracht werden können, muss der Tf vor dem Signal warten, bis der Fdl das Zs 1 gibt. Falls auch dieses nicht möglich ist, muss der Fdl per Funk einen schriftlichen Befehl an den Tf diktieren. Der Tf notiert den Befehl in ein Formular, welches sich im Führerstand befindet. Der am HSig befindliche 2000-Hz-Magnet der punktförmigen Zugbeeinflussung (PZB) soll eine Vorbeifahrt des Zuges am HSig zur Unzeit durch eine Zwangsbremmung verhindern.

Für dieses System werden im ersten Schritt möglichst alle Systemzustände ermittelt und hinsichtlich Sicherheit und Verfügbarkeit eingeordnet (vgl. Tabelle 3).

Zu- stand	Funktion der Technik			Handlung des Men- schen			Bewertung		Beschreibung des Zustandes
	HSig	Zs 1	PZB	Fdl	Tf	IHP	Sicher- heit	Verfüg- barkeit	
0	k	---	---	k	k	---	+	+	Vorbeifahrt des Zuges am funktionsfähigen, Fahrt zeigenden HSig
1	h	---	---	---	k	---	+	-	Ausfall der Fahrtstellung des HSig, Warten des Zuges vor HSig
1a	h	k	k	k	k	---	0	0	Möglichkeit der Vorbeifahrt des Zuges am HSig mittels Zs 1; Leistungsfähigkeit wegen geringerer Geschwindigkeit herabgesetzt
1b	h	h	k	k	k	---	0	0	Fahren mit schriftlichem Befehl wird eingeführt, Möglichkeit der Vorbeifahrt des Zuges am HSig mit Befehl; Leistungsfähigkeit wegen Befehlsübermittlungszeit herabgesetzt
2	k	---	k	---	g	---	-	+	Vorbeifahrt des Zuges am Halt zeigenden HSig zur Unzeit durch Betätigung der PZB-Freigabetaste durch Tf
	k	---	h	---	g	---			Vorbeifahrt des Zuges am Halt zeigenden HSig zur Unzeit bei gleichzeitigem Ausfall der PZB
	h	---	h	---	g	---			Vorbeifahrt des Zuges am ausgefallenen (dunklen) HSig zur Unzeit bei gleichzeitigem Ausfall der PZB
	g	---	---	---	k	---			Vorbeifahrt des Zuges am HSig, das ein gefährlich falsches Signalbild in Folge eines technischen Ausfalls zeigt.
	k	---	---	---	k	g			Vorbeifahrt des Zuges am HSig, das ein gefährlich falsches Signalbild in Folge eines Instandhaltungsfehlers zeigt.
2a	h	---/k	k	g	k	---	0	-	Fehler beim Fahren auf Zs 1 oder mit Befehl durch Fdl, Zwangsbremmung durch PZB
	h	---/k	k	k	g	---			Fehler beim Fahren auf Zs 1 oder mit Befehl durch Tf, Zwangsbremmung durch PZB
	h	---/k	k	g	g	---			Fehler beim Fahren auf Zs 1 oder mit Befehl durch Fdl und Tf, Zwangsbremmung durch PZB
2b	h	---/k	h	g	k	---	-	0	Fehler beim Fahren auf Zs 1 oder mit Befehl durch Fdl bei gleichzeitigem Ausfall der PZB
	h	---/k	h	k	g	---			Fehler beim Fahren auf Zs 1 oder mit Befehl durch Tf bei gleichzeitigem Ausfall der PZB
	h	---/k	h	g	g	---			Fehler beim Fahren auf Zs 1 oder mit Befehl durch Fdl und Tf bei gleichzeitigem Ausfall der PZB

Legende:

- k korrekte technische Funktion bzw. korrekte menschliche Handlung
- h hemmend ausgefallenen Technik
- g gefährlich ausgefallenen Technik bzw. gefährliche menschliche Handlung
- ohne technische Funktion bzw. ohne menschliche Handlung
- + volle Sicherheit bzw. volle Verfügbarkeit gegeben
- 0 eingeschränkte Sicherheit bzw. eingeschränkte Verfügbarkeit gegeben
- keine Sicherheit bzw. keine Verfügbarkeit gegeben

Tabelle 3: Mögliche Systemzustände im Beispiel

Die ermittelten Zustände werden im zweiten Schritt entsprechend ihrer Bewertung hinsichtlich der Systemparameter Sicherheit und Verfügbarkeit im Diagramm angeordnet (vgl. Bild 25).

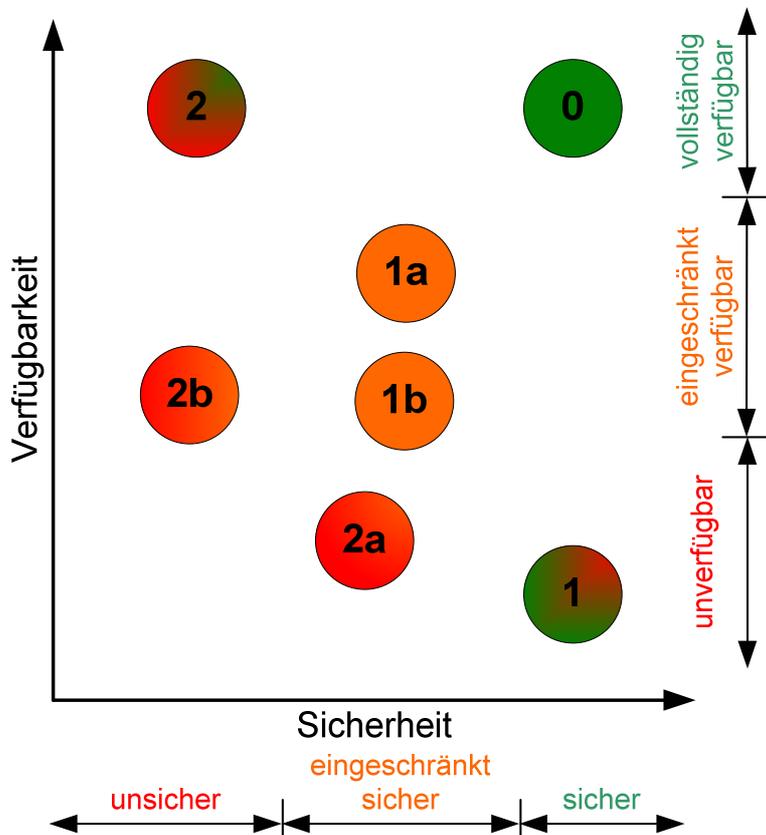


Bild 25: Einordnung der Systemzustände im Verfügbarkeits-Sicherheits-Diagramm

Darauf aufbauend werden im dritten Schritt in Tabelle 4 mögliche Übergänge zwischen den Zuständen mit Beispielen hinterlegt und gemäß Abschnitt 4.7 kategorisiert.

Übergang	Beispiel	F/A/S-Kategorie
λ_{01}	Ausfall des HSig (z. B. in Folge eines Aderbruchs)	$\lambda_{htA, RB}$
μ_{10}	Instandsetzung des HSig während dessen Unverfügbarkeit; es wird nicht gefahren.	μ_m
λ_{1a1}	Ausfall des Zs 1 (z. B. in Folge eines Lampenausfalls)	$\lambda_{htA, ARB}$
μ_{11a}	Fdl entscheidet, auf Zs 1 zu fahren.	μ_m
λ_{1b1}	Korrektter schriftlicher Befehl vom Fdl kommt beim Tf nicht an. (z. B. in Folge einer Funkstörung)	$\lambda_{htA, ARB}$
μ_{11b}	Fdl entscheidet, auf schriftlichen Befehl zu fahren.	μ_m
λ_{02}	Anzeigen eines gefährlich falschen (höherwertigen) Signalbegriffs am HSig aufgrund eines technischen Ausfalls	$\lambda_{gtA, RB}$
μ_{20}	Offenbarung des Ausfalls und Reaktion der Technik auf den gefährlich falschen (höherwertigen) Signalbegriff am HSig	μ_t
λ_{02b}	Unzulässige Vorbeifahrt des Zuges am Halt zeigenden HSig <i>UND</i> gleichzeitiger Ausfall der PZB	$\lambda_{gmF, RB} \cap \lambda_{gtA, RB}$

μ_{2b0}	Offenbarung des Fehlers und Reaktion durch Tf vor Passieren des Halt zeigenden HSig	μ_m
λ_{12b}	Unzulässige Vorbeifahrt des Zuges am ausgefallenen, Halt gebietendem HSig <i>UND</i> gleichzeitiger Ausfall der PZB	$\lambda_{gmF,ARB} \cap \lambda_{gtA,RB}$
	Irrtümliche Annahme des Sehens eines Zs 1 durch Tf <i>UND</i> gleichzeitiger Ausfall der PZB.	$\lambda_{gmF,ARB} \cap \lambda_{gtA,RB}$
μ_{2b1}	Offenbarung des Fehlers und Reaktion durch Tf vor Passieren des ausgefallenen, Halt gebietenden HSig	μ_m
λ_{12a}	Zwangsbremung des Zuges nach irrtümlicher Annahme des Sehens eines Zs 1 durch Tf.	$\lambda_{gmF,ARB} \cap S_{ht}$
μ_{2a1}	Offenbarung des Fehlers und Reaktion durch Tf vor Passieren des Signals und Zwangsbremung	μ_m
λ_{1a2a}	Zwangsbremung des Zuges nach irrtümlicher Annahme des Sehens eines Zs 1 durch Tf.	$\lambda_{gmF,ARB} \cap S_{ht}$
	Zwangsbremung des Zuges nach (gefährlichem) Fehler des Fdl beim Bedienen des Zs 1.	$\lambda_{gmF,ARB} \cap S_{ht}$
μ_{2a1a}	Offenbarung des Fehlers und Reaktion durch Tf vor Passieren des Signals und Zwangsbremung	μ_m
	Offenbarung des Fehlers und Reaktion durch Fdl auf (gefährlichen) Fehler beim Bedienen des Zs 1.	μ_m
λ_{1b2a}	Zwangsbremung des Zuges nach irrtümlicher Annahme des Sehens eines Zs 1 durch Tf	$\lambda_{gmF,ARB} \cap S_{ht}$
	Zwangsbremung des Zuges nach (gefährlichem Fehler) des Fdl/Tf beim Diktieren/Schreiben des schriftlichen Befehls	$\lambda_{gmF,ARB} \cap S_{ht}$
μ_{2a1b}	Offenbarung des Fehlers und Reaktion durch Tf vor Passieren des Signals und Zwangsbremung	μ_m
	Offenbarung des Fehlers und Reaktion durch Fdl auf (gefährlichem Fehler) beim Diktieren/Schreiben des schriftlichen Befehls	μ_m
μ_{1a0}	Instandsetzung des HSig während der eingeschränkten Verfügbarkeit; es wird auf Zs 1 gefahren.	μ_m
μ_{1b0}	Instandsetzung des HSig (während der eingeschränkten Verfügbarkeit; es wird mit schriftlichem Befehl gefahren.	μ_m
λ_{1a2b}	Vorbeifahrt des Zuges nach irrtümlicher Annahme des Sehens eines Zs 1 durch Tf <i>UND</i> gleichzeitiger Ausfall der PZB	$\lambda_{gmF,ARB} \cap \lambda_{gtA,RB}$
	(Gefährlicher) Fehler des Fdl beim Bedienen des Zs 1 <i>UND</i> gleichzeitiger Ausfall der PZB	$\lambda_{gmF,ARB} \cap \lambda_{gtA,RB}$
μ_{2b1a}	Offenbarung des Fehlers und Reaktion durch Tf vor Passieren des Signals	μ_m
	Offenbarung des Fehlers und Reaktion durch Fdl vor Passieren des Signals	μ_m
λ_{1b2b}	Vorbeifahrt des Zuges nach irrtümlicher Annahme des Sehens eines Zs 1 durch Tf <i>UND</i> gleichzeitiger Ausfall der PZB	$\lambda_{gmF,ARB} \cap \lambda_{gtA,RB}$
	(Gefährlicher) Fehler des Fdl/Tf beim Diktieren/Schreiben des schriftlichen Befehls <i>UND</i> gleichzeitiger Ausfall der PZB	$\lambda_{gmF,ARB} \cap \lambda_{gtA,RB}$
μ_{2b1b}	Offenbarung des Fehlers und Reaktion durch Tf vor Passieren des Signals	μ_m
	Offenbarung des Fehlers und Reaktion durch Fdl auf Fehler beim Diktieren/Schreiben des schriftlichen Befehls	μ_m
λ_{12}	Anzeigen eines gefährlichen falschen (höherwertigen) Signalbegriffs am HSig aufgrund eines Instandhaltungsfehlers	$\lambda_{gmF,IH}$
μ_{21}	Offenbarung des Fehlers und Reaktion durch IHP	μ_m

λ_{12b}	Irrtümliche Annahme des Sehens eines Zs 1 durch Tf <i>UND</i> gleichzeitiger Ausfall der PZB	$\lambda_{gmF,ARB} \cap \lambda_{gtA,RB}$
μ_{2b1}	Offenbarung des Fehlers und Reaktion durch Tf vor Passieren des Signals	μ_m

Legende:

- $\lambda_{hmF,RB}$ Rate für hemmend menschliche Fehlhandlung im Regelbetrieb
- $\lambda_{hmF,ARB}$ Rate für hemmend menschliche Fehlhandlung bei Abweichung vom Regelbetrieb
- $\lambda_{hmF,IH}$ Rate für hemmend menschliche Fehlhandlung bei Instandhaltung
- $\lambda_{gmF,RB}$ Rate für gefährlich menschliche Fehlhandlung im Regelbetrieb
- $\lambda_{gmF,ARB}$ Rate für gefährlich menschliche Fehlhandlung bei Abweichung vom Regelbetrieb
- $\lambda_{gmF,IH}$ Rate für gefährlich menschliche Fehlhandlung bei Instandhaltung
- $\lambda_{htA,RB}$ Rate für hemmend technischen Ausfall im Regelbetrieb
- $\lambda_{htA,ARB}$ Rate für hemmend technischen Ausfall bei Abweichung vom Regelbetrieb
- $\lambda_{gtA,RB}$ Rate für gefährlich technischen Ausfall im Regelbetrieb
- $\lambda_{gtA,ARB}$ Rate für gefährlich technischen Ausfall bei Abweichung vom Regelbetrieb
- μ_m Rate für korrekte menschliche Handlung (im Regelbetrieb, bei Abweichung vom Regelbetrieb, bei Instandhaltung)
- μ_t Rate für korrekte technische Aktion (im Regelbetrieb, bei Abweichung vom Regelbetrieb, bei Instandhaltung)
- S_{ht} hemmend technische Schutzmaßnahme
- \cap UND-Verknüpfung

Tabelle 4: Mögliche Übergangsraten im Beispiel

Im letzten Schritt werden die ermittelten Übergangsraten zwischen den Zuständen in das Verfügbarkeits-Sicherheits-Diagramm eingefügt (vgl. Bild 26).

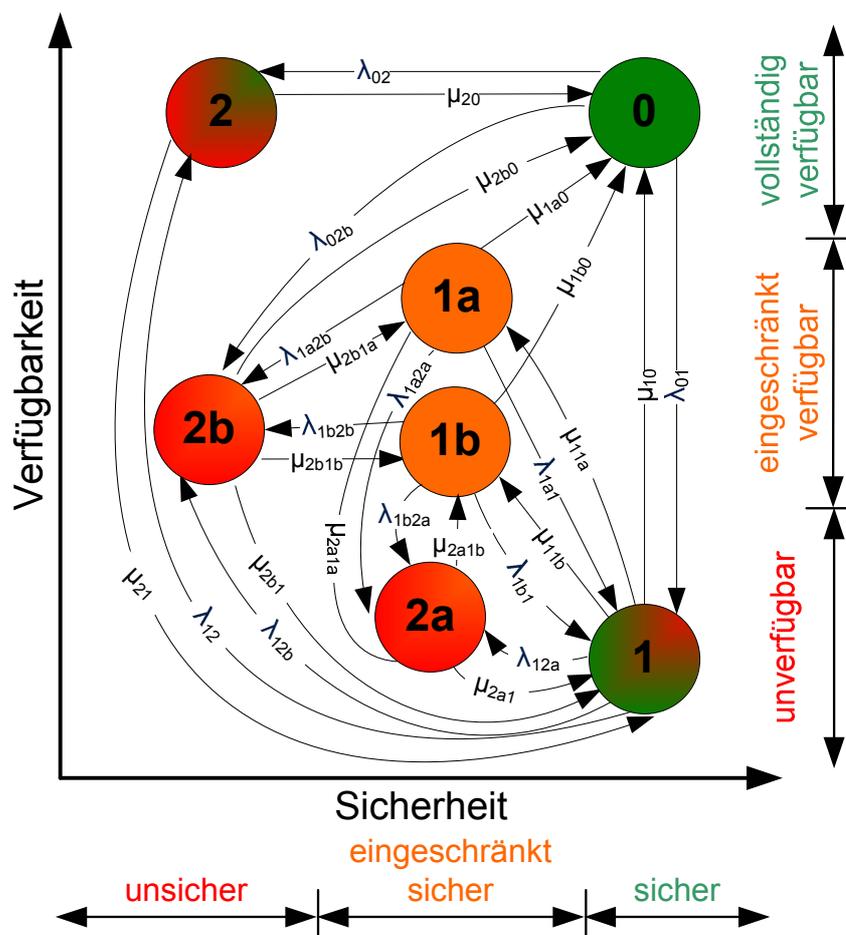


Bild 26: Systemzustände und Übergänge im Verfügbarkeits-Sicherheits-Diagramm

Auf der Grundlage der beispielhaften Erstellung des Verfügbarkeits-Sicherheits-Diagramms für das beschriebene Szenario können Aussagen hinsichtlich der zu fordernden Verhältnisse der jeweiligen Ausfall- bzw. Reparaturrate getroffen werden:

Da sich F/A/S im Bahnsystem im Allgemeinen und im betrachteten betrieblichen Szenario im Speziellen nicht vollständig ausschließen lassen, muss dafür gesorgt werden, dass bei ihrem Auftreten, ein sicherer Zustand eingenommen wird. Daraus lässt sich folgende Forderung postulieren [FIS90]:

- $\lambda_{02} \ll \lambda_{01}$, um möglichst nicht in den unsicheren Zustand 2 zu kommen.

Aufgrund der Tatsache, dass in den Zuständen 1, 1a und 1b teilweise oder sogar vollständig menschliche Ersatzhandlungen für die Sicherung des Bahnbetriebes genutzt werden, bei denen eine sehr viel höhere Fehlerwahrscheinlichkeit besteht als bei technischer Sicherung, kann näherungsweise davon ausgegangen werden, dass $\lambda_{12b} \approx \lambda_{1a2b} \approx \lambda_{1b2b} \gg \lambda_{02}$ gilt. Es besteht also eine weitaus höhere Wahrscheinlichkeit, vom Zustand 1, 1a bzw. 1b in den gefährlichen Zustand 2b als vom sicheren Zustand 0 in den gefährlichen Zustand 2b überzugehen. Deshalb sollten die Zustände 1, 1a bzw.

1b wegen ihrer potenziellen Gefährlichkeit möglichst bald wieder verlassen werden. Als Ergebnis dessen kann eine weitere Forderung postuliert werden [FIS90]:

- $\mu_{10} > \lambda_{01}$

Diese qualitativen Untersuchungen im Verfügbarkeits-Sicherheits-Diagramm können in einem weiteren Schritt unter Verwendung konkreter Werte aus der Praxis quantitativ untermauert werden. Zudem besteht die Möglichkeit, diese realen Werte der Parameter λ_{nm} oder μ_{mn} zu variieren, um auf der Grundlage der daraus ermittelten Zustandszeiten eine faktenbezogene Argumentation der Verantwortlichen für Sicherheit zu ermöglichen. Ggf. münden diese Diskussionen auch darin, dass das Systemdesign eine Änderung erfährt und zusätzliche technische Zustände bereitgestellt werden müssen.

Verfügbarkeits-Sicherheits-Diagramme können zukünftig in betrieblichen Sicherheitsnachweisen (vgl. Abschnitt 6.4) eine wichtige Rolle spielen, da sie neben technischen Komponenten auch menschliche und organisatorische Merkmale in sich vereinigen. Folgende generelle Schritte sollten bei der Analyse von betrieblichen Szenarien vollzogen werden:

- Ermittlung aller Systemzustände und deren Einordnung hinsichtlich Sicherheit und Verfügbarkeit
- Anordnung der Systemzustände im Verfügbarkeits-Sicherheits-Diagramm entsprechend ihrer Bewertung hinsichtlich Sicherheit und Verfügbarkeit
- Ermittlung aller Übergänge zwischen den Zuständen und deren Kategorisierung unter Verwendung repräsentativer Beispiele
- Ergänzung der Übergänge zwischen den Zuständen im Verfügbarkeits-Sicherheits-Diagramm und deren qualitative Bewertung
- Quantitative Ergänzung der Übergänge zwischen den Zuständen mittels konkreter Werte aus der Praxis
- Variation der praxisnahen Werte zur Optimierung des Systemdesigns

6 Darstellung der ganzheitlichen Sicherheitsbetrachtung von Bahnsystemen im Modell

6.1 Zusammenfassung der Grundlagen für das Modell

Die gewonnenen Erkenntnisse aus den bisherigen Kapiteln bezüglich des Bahnsystems sowie der Zusammenhänge hinsichtlich des Themas Sicherheit können wie folgt zusammengefasst werden:

- Klare Trennung der Lebenszyklusphasen durch normative Vorgaben (vgl. Kapitel 2, Abschnitt 2.1)
- Verfolgung des risikoorientierten Ansatzes bei Sicherheitsbetrachtungen (vgl. Kapitel 2, Abschnitte 2.2.1 und 2.2.2)
- Klare Verteilung der Verantwortlichkeiten in den einzelnen Lebenszyklusphasen (vgl. Kapitel 2, Abschnitt 2.2.3)
- Herleitung des kausalen Zusammenhangs zwischen den einzelnen RAMS-Komponenten (vgl. Kapitel 3)
- Vorschlag zur inhaltlichen Unterscheidung zwischen Fehlern, Ausfällen und Störungen und deren Einordnung im Bahnsystem (vgl. Kapitel 4, Abschnitt 4.2)
- Kategorisierung menschlicher Handlungen auf fertigkeit-, regel- und wissensbasierter Ebene (vgl. Kapitel 4, Abschnitt 4.4.4.1)
- Kategorisierung von Fehlern, Ausfällen und Störungen unter Verwendung der Parameter F/A/S-Art, F/A/S-Quelle sowie Lebenszyklusphase (vgl. Kapitel 4, Abschnitt 4.7)
- Darstellung der Komplexität des Bahnsystems im Regelkreis (vgl. Kapitel 4, Abschnitt 4.8)
- Darlegung des Umgangs mit Fehlern, Ausfällen und Störungen im Bahnsystem (vgl. Kapitel 5, Abschnitt 5.1)
- Möglichkeit der Darstellung von betrieblichen Szenarien und der darin auftretenden Abhängigkeiten zwischen den RAMS-Komponenten in Verfügbarkeits-Sicherheits-Diagrammen (vgl. Kapitel 5, Abschnitt 5.3.1)

Diese Erkenntnisse erlauben eine ganzheitliche Sicherheitsbetrachtung des Bahnsystems. Wesentliche Anforderungen an ein zu erstellendes Modell sind einerseits die Beachtung der menschlichen und technischen Aspekte und andererseits die Integration organisatorischer Randbedingungen. Damit soll es zukünftig möglich sein, sowohl technische Ausfälle als auch menschliche Fehlhandlungen qualitativ zu ermitteln und ggf. unter Verwendung von Verfügbarkeits-Sicherheits-Diagrammen detailliert zu analysieren. Für den Fall des Vorhandenseins entsprechender Ausfall- bzw. Fehlerraten für die Zustandsübergänge im Verfügbarkeits-Sicherheits-Diagramm können zudem quantitative Aussagen hinsichtlich der RAMS-Komponenten erfolgen. Ziel der ganzheitlichen

Sicherheitsbetrachtung ist die Anregung einer faktenbezogenen Diskussion hinsichtlich des Themas „Sicherheit“ zwischen den verantwortlichen Stellen im Bahnsystem unter der Maßgabe der Vermeidung von Fehlern, Ausfällen und Störungen im Lebenszyklus.

6.2 Normative Grundlagen für das Modell

Die Eigenschaften des Bahnsystems bezüglich RAMS werden laut DIN EN 50126 (vgl. Bild 27) im Wesentlichen durch drei Aspekte beeinflusst. Erstens durch Anomalien, die sich innerhalb des Systems in jeder beliebigen Phase der Systemlebensdauer bemerkbar machen können (Systembedingungen), zweitens durch Einflüsse, denen das System während des Betriebes ausgesetzt ist (Betriebsbedingungen) und drittens durch Maßnahmen, die im Rahmen der Instandhaltung durchgeführt werden. Jeder dieser drei Aspekte wird in unterschiedlicher Art von den Sicherheitsfaktoren Mensch, Technik und Organisation hinsichtlich RAMS geprägt. Während bei den Systembedingungen vor allem technische Merkmale auf RAMS Einfluss nehmen, werden sowohl die Betriebsbedingungen als auch die Instandhaltungsbedingungen durch menschliche Faktoren sowie organisatorische Abläufe (z. B. Betriebs- und Instandhaltungsverfahren) gekennzeichnet.

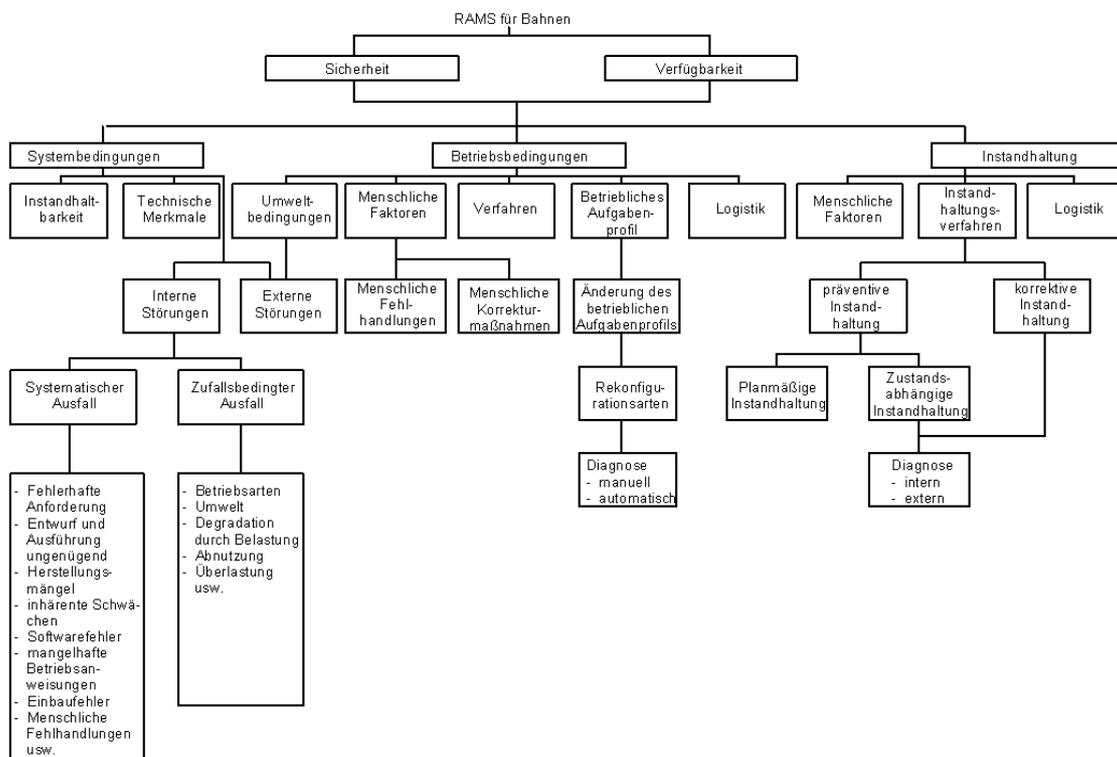


Bild 27: RAMS-Faktoren für Bahnen [DIN00]

Die Übersicht in Bild 27 muss als Ergebnis der vorliegenden Arbeit im Bereich der Systembedingungen dahingehend ergänzt werden, dass der Mensch und die organisatorischen Randbedingungen, unter denen er handelt, wesentlichen Einfluss auf die techni-

schen Merkmale haben. Bild 28 liefert, aufbauend auf der in DIN EN 50126 verankerten Grafik, die Einflussmöglichkeiten menschlicher, technischer und organisatorischer Faktoren auf das Bahnsystem in den maßgeblichen Lebenszyklusphasen.

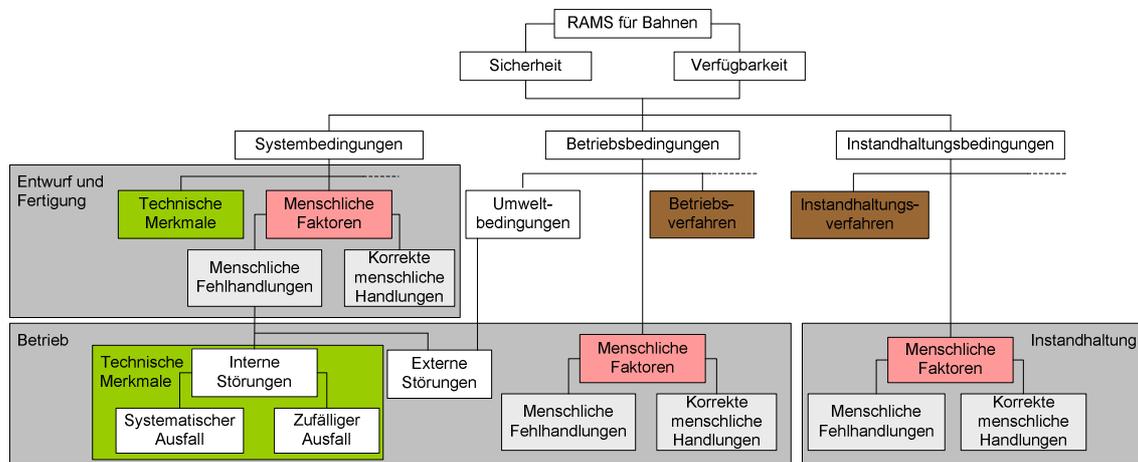


Bild 28: Einfluss der Sicherheitsfaktoren Mensch, Technik und Organisation auf RAMS für Bahnen nach [DIN00]

In den letzten Jahrzehnten wurden große Anstrengungen seitens aller am Bahnsystem Beteiligten unternommen, um einen adäquaten Umgang mit Ausfällen der Technik zu gewährleisten. Mit der Einführung des risikoorientierten Ansatzes bei Sicherheitsbetrachtungen im Bahnsystem wurde zunehmend Augenmerk auf menschliche Einflüsse und organisatorische Randbedingungen gelegt.

Die aus den bisherigen Betrachtungen gewonnenen Erkenntnisse werden nachfolgend in einem Modell zusammengefasst. Darin erfolgt erstens die Unterscheidung hinsichtlich Fehlern, Ausfällen und Störungen, zweitens deren Zuordnung zu menschlichen Handlungen, technischen Komponenten sowie organisatorischen Prozessen in den einzelnen Lebenszyklusphasen und drittens die Darstellung von deren Auswirkung auf die Sicherheit im Bahnsystem.

6.3 Modell der ganzheitlichen Sicherheitsbetrachtung von Bahnsystemen

An vielen Prozessen im Bahnsystem ist der Mensch beteiligt und muss dabei mit technischen Systemen interagieren. Betrachtet man in Bild 28 zunächst die *Betriebsbedingungen im Regelbetrieb* (vgl. Zustand 0 in Bild 26), so sind diese im Wesentlichen durch das Betriebspersonal wie den Triebfahrzeugführer geprägt, der im Führerstand die Fahrt des Zuges steuert. Zudem beeinflusst der Fahrdienstleiter im Stellwerk den Regelbetrieb durch Stellen der beweglichen Fahrwegelemente oder das Zulassen von Zugfahrten.

Dabei wird über Zugmeldungen mit nachgeordnetem Betriebspersonal kommuniziert. Die Zugmeldungen selbst sind dabei nicht sicherheitsrelevant, wenn die Sicherung durch technische Anlagen erfolgt.

Bei technischen Ausfällen im Regelbetrieb (vgl. $\lambda_{htA, RB}$, $\lambda_{gtA, RB}$, in Tabelle 4 bzw. Bild 29) und dem Übergang des Bahnsystems in die Rückfallebene (vgl. Zustand 1 in Bild 26) erlangen diese Zugmeldungen jedoch Sicherheitsrelevanz. Wie bereits am Beispiel in Abschnitt 5.3.2 anhand des Verfügbarkeits-Sicherheits-Diagramms dargelegt wurde, sind alle diese Handlungen im Rahmen der *Betriebsbedingungen bei Abweichung vom Regelbetrieb* mehr oder minder anfällig für menschliche Fehler (vgl. $\lambda_{hmF, ARB}$ und $\lambda_{gmF, ARB}$ in Tabelle 4 bzw. Bild 29), vollziehen diese sich doch eher selten auf fertigungsbasierter Ebene. Vielmehr handelt der Bediener in der Rückfallebene oft regel- oder wissensbasiert (vgl. 4.4.4.1).

Eine wesentliche Aufgabe im Rahmen von RAMS-Analysen bildet die sicherheitsbezogene Betrachtung im Bereich *Systembedingungen*, da hier menschliche, technische und organisatorische Einflüsse wirken. Unentdeckte menschliche Fehlhandlungen (vgl. $\lambda_{hmF, PEFI}$ und $\lambda_{gmF, PEFI}$ in Tabelle 4 bzw. Bild 29) während der Planung, des Entwurfes, der Fertigung oder der Inbetriebnahme von Komponenten des Bahnsystems führen zur Abweichung von der geplanten Spezifikation und damit zu Fehlzuständen. An dieser Stelle zeigt sich besonders gut, ob die in DIN EN 50126 vorgegebenen Verfahren (z. B. Sicherheits- und Qualitätsmanagement), Konzepte (z. B. fail-safe-Prinzip) und Werkzeuge (z. B. Softwaretools und -programme) in ausreichendem Umfang angewendet und deren Anwendung überwacht sowie belastbar nachgewiesen wurden, um den geforderten Grad an systematischer Sicherheit (SIL) zu erreichen. Durch verschiedene Methoden, wie die Verwendung von Checklisten, die Beachtung des Vier-Augen-Prinzips bei der Prüfung von Dokumenten und Komponenten oder deren unabhängige Begutachtung durch Dritte, können frühzeitig in der Technik verborgene Fehler (vgl. $\lambda_{htF, PEFI}$ und $\lambda_{gtF, PEFI}$ in Tabelle 4 bzw. Bild 29) offenbart werden, die anderenfalls ein erhöhtes Potenzial für technische Ausfälle im Regelbetrieb oder bei Abweichung vom Regelbetrieb (vgl. $\lambda_{htA, RB}$, $\lambda_{gtA, RB}$, $\lambda_{htA, ARB}$ und $\lambda_{gtA, ARB}$ in Tabelle 4 bzw. Bild 29) darstellen würden.

Aber auch die *Instandhaltungsbedingungen*, also „die Kombination aller technischen und administrativen Tätigkeiten einschließlich Aufsichtsmaßnahmen, um ein Produkt in einem Zustand zu halten oder wieder in einen Zustand zu versetzen, in dem es eine geforderte Funktion erfüllen kann“ [DIN00], sind von menschlichen Faktoren geprägt und daher mit menschlichen Fehlern behaftet (vgl. $\lambda_{hmF, IH}$ und $\lambda_{gmF, IH}$ in Tabelle 4 bzw. Bild 29). Deswegen sind geeignete Instandhaltungsverfahren erforderlich, um eine möglichst geringe Anzahl an organisatorisch bedingten Instandhaltungsfehlern (vgl. $\lambda_{hoF, IH}$

und $\lambda_{\text{goF,IH}}$ in Tabelle 4 bzw. Bild 29) zu erlangen. Ausreichendes und gut ausgebildetes Personal oder hinreichende Zeitfenster für Instandhaltungsmaßnahmen bilden dafür wichtige Grundlagen.

Weitere Fehler verbergen sich in den Planungs-, Entwicklungs-, Fertigungs-, Inbetriebnahme- und Betriebsverfahren. Über institutionelle Wege gelangen diese organisatorischen Fehler (vgl. $\lambda_{\text{hoF,PEFI}}$, $\lambda_{\text{goF,PEFI}}$, $\lambda_{\text{hoF,RB}}$, $\lambda_{\text{goF,RB}}$, $\lambda_{\text{hoF,ARB}}$ und $\lambda_{\text{goF,ARB}}$ in Tabelle 4 bzw. Bild 29) an den jeweiligen Arbeitsplatz (z. B. Schreibtisch des Planers, Bedienplatz im Stellwerk, Führerstand), wo sie jene Bedingungen schaffen (z. B. Zeitmangel, schlechte Arbeitsverhältnisse, ungeeignete Arbeitsmittel), in denen dann ein erhöhtes Potenzial für gefährliche menschliche Fehler (vgl. $\lambda_{\text{gmF,PEFI}}$, $\lambda_{\text{gmF,RB}}$, $\lambda_{\text{gmF,ARB}}$ in Tabelle 4 bzw. Bild 29) besteht.

Bild 29 vereint alle genannten Randbedingungen zur Gewährleistung einer ganzheitlichen Sicherheitsbetrachtung im Bahnsystem:

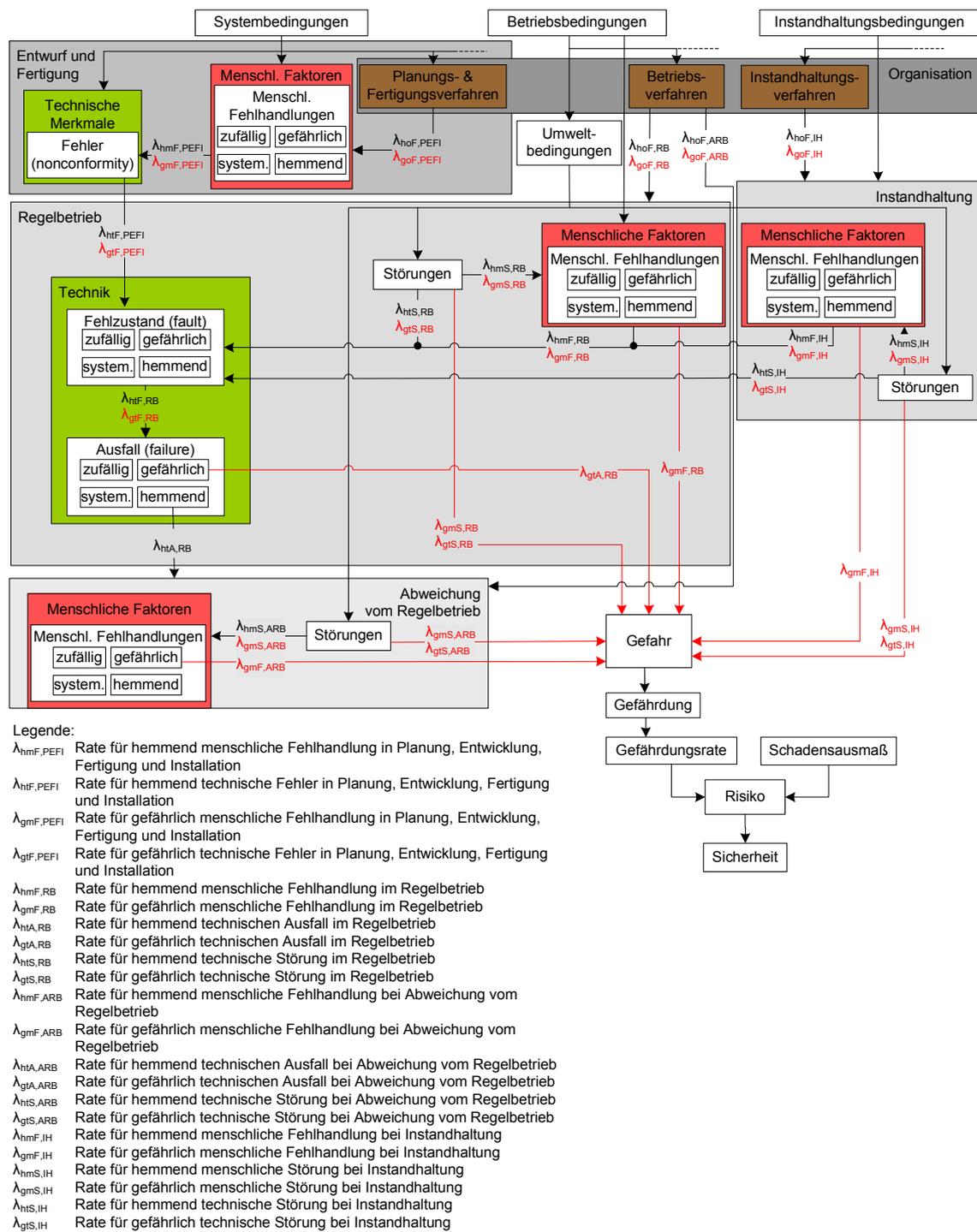


Bild 29: Modell zur ganzheitlichen Sicherheitsbetrachtung des Bahnsystems

Das Modell beschränkt sich aus Gründen der Übersicht auf Raten von Fehlern, Ausfällen und Störungen. Folglich steht auch die Betrachtung der *Sicherheit* im Mittelpunkt. Eine Erweiterung und Ergänzung des Modells durch Reparaturraten ist allerdings möglich und würde damit auch die *Verfügbarkeit* ins Analysespektrum einbeziehen. Zudem wird im Modell bei Abweichung vom Regelbetrieb und bei der Instandhaltung auf den Einsatz von Technik verzichtet. Bei Abweichung von Regelbetrieb handelt es sich folg-

lich um eine rein menschliche Rückfallebene und die Instandhaltung erfolgt ohne technische Unterstützung. Auch diesbezüglich kann das Modell ergänzt werden.

Durch den modularen Aufbau können die im Modell befindlichen *menschlichen Faktoren* jeweils mit einem vorhandenen Modell menschlicher Handlungen, wie dem im Rahmen dieser Arbeit auf der Grundlage von Rasmussen und Reason entwickelten Modell in Bild 18, verfeinert werden.

Zudem werden Bahnsystemhersteller einerseits in die Lage versetzt, ihre vorhandene *Technik* zu integrieren und andererseits ihre *organisatorischen Prozesse und Strukturen* im Rahmen von Planungs- und Fertigungsverfahren zu validieren. Gleiches gilt für die Betriebs- und Instandhaltungsverfahren der verschiedenen Betreiber von Bahnsystemen.

Ferner können für jede Phase im Lebenszyklus des Bahnsystems jeweils vom aktuell Verantwortlichen (Hersteller, Betreiber, Aufsichtsbehörde) Maßnahmen gegen menschliche, technische und organisatorische Fehler, Ausfälle und Störungen ergriffen werden. Als Hilfsmittel für deren Auffindung dient zum einen der Regelkreis des Bahnsystems (vgl. Bild 21), der die Analyse der Lebenszyklusphase 11 *Betrieb und Instandhaltung* gemäß DIN EN 50126 architekturorientiert vollzieht, und zum anderen die Detailanalyse betrieblicher Szenarien des Bahnsystems in Form von Verfügbarkeits-Sicherheitsdiagrammen (vgl. Bild 26).

6.4 Zulassungsverfahren mit betrieblichem Sicherheitsnachweis

Auf der Grundlage der in den Kapiteln 5 und 6 gewonnenen Erkenntnisse bezüglich der Vorgehensweise bei der Analyse betrieblicher Szenarien im Verfügbarkeits-Sicherheitsdiagramm (vgl. Abschnitt 5.3.2) sowie bei der Integration der darin ermittelten qualitativen bzw. quantitativen Aussagen in das Modell zur ganzheitlichen Sicherheitsbetrachtung des Bahnsystems (vgl. Bild 29) wird in Bild 30 ein Vorschlag zum Zulassungsverfahren von Bahnanlagen unter Verwendung eines betrieblichen Sicherheitsnachweises unterbreitet.

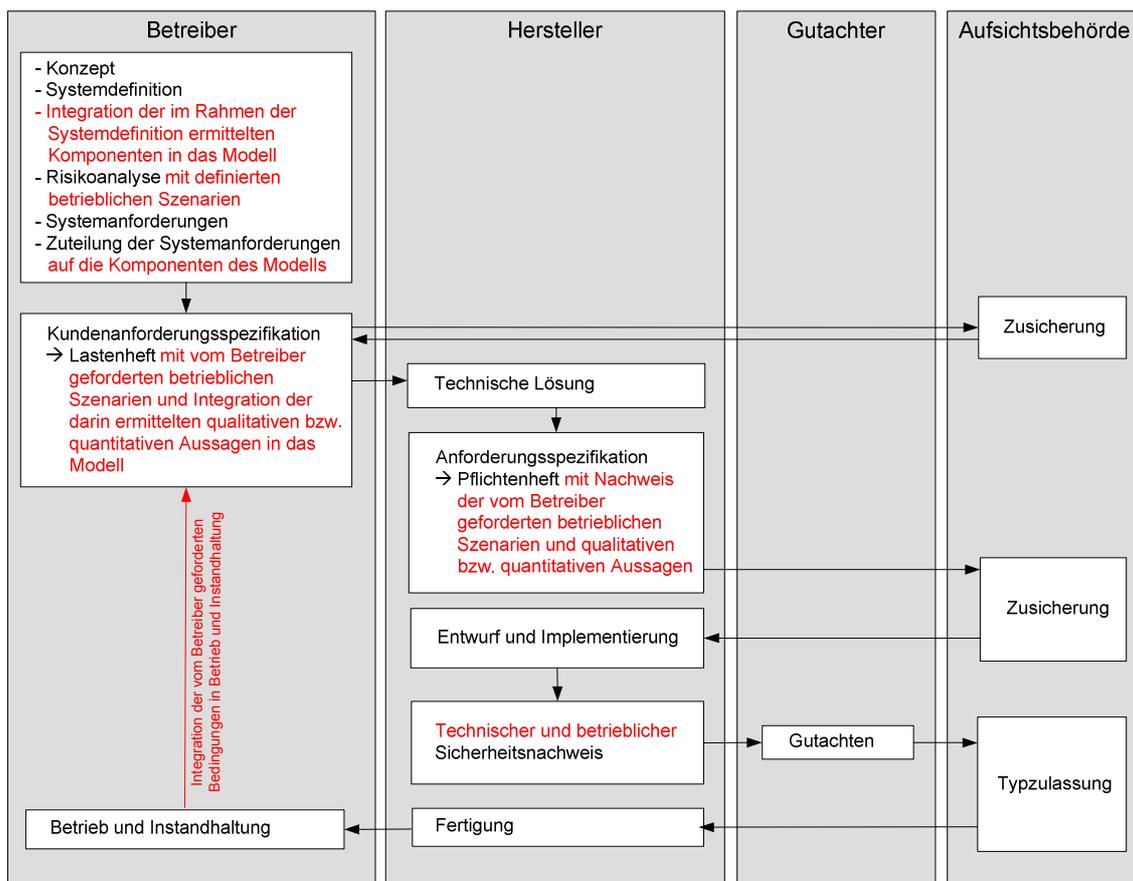


Bild 30: Zulassungsverfahren von Bahnanlagen mit betrieblichem Sicherheitsnachweis

Das Verfahren orientiert sich am auf nationaler sowie internationaler Ebene vorgegebenen und bewährten Ablauf im Rahmen der Zulassung von Bahnanlagen und ergänzt den Nachweis der technischen Sicherheit (vgl. Bild 3) um betriebliche Aspekte. Damit dürfte eine allgemeine Akzeptanz in der Fachwelt im Sinne des Risikoakzeptanzkriteriums „mindestens gleiche Sicherheit (MGS)“ leicht zu erlangen sein.

7 Zusammenfassung und Ausblick

Das Ansinnen der vorliegenden Arbeit besteht in der Betrachtung des Begriffs *Sicherheit* aus verschiedenen Blickwinkeln unter Beachtung des komplexen Beziehungsgeflechts im Bahnsystem. Unter Verwendung der Ergebnisse wird es zukünftig möglich sein, neben den bisher vornehmlich in Sicherheitsbetrachtungen einfließenden technischen Aspekten, ebenso menschlichen und organisatorischen Faktoren Beachtung zu schenken.

Im Sinne einer Struktur vom Allgemeinen zum Speziellen werden zunächst in Kapitel 2 die normativen Vorgaben mit der Einteilung der Sicherheitsaufgaben in verschiedenen Lebenszyklusphasen, die darin festgelegten Verantwortlichkeiten für Sicherheit und der risikoorientierte Ansatz bei Sicherheitsbetrachtungen erläutert. Die Darstellung der übergeordneten Anforderungen an das Bahnsystem, die Voraussetzungen für eine Strategie der aktiven Sicherheit sowie Erläuterungen hinsichtlich des Zusammenspiels der Akteure beim Zulassungsprozess von Bahnkomponenten beschließen das Kapitel 2.

Die Erläuterungen des Zusammenhangs zwischen den Begriffen *Risiko* und *Sicherheit* einerseits und „RAMS“ als Akronym für *Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit* und *Sicherheit* andererseits bilden den Schwerpunkt von Kapitel 3. Die Herleitung der kausalen Kette, ausgehend von einer Gefahr bis hin zur Sicherheit, und das Zusammenspiel der RAMS-Komponenten kann als „gedankliche Klammer“ für die gesamte Arbeit verstanden werden und dient zudem als Grundlage für die nachfolgenden Kapitel. Besondere Beachtung wird dem Begriff *Risiko* geschenkt, da derzeitige und zukünftige Sicherheitsbetrachtungen maßgeblich durch ihn geprägt sind bzw. werden.

Der Definition und Kategorisierung der Begriffe *Fehler, Ausfall* und *Störung* widmet sich Kapitel 4 und ordnet diese im Systemlebenszyklus ein. Der auf der Analyse des Schrifttums fußende Vorschlag zur Klassifikation *menschlicher Fehler* im Bahnsystem bietet einen Ansatz für weitere wissenschaftliche Arbeiten, ggf. auch anderer Kompetenzbereiche (z. B. Arbeitspsychologie und -wissenschaften). Ein wichtiges Ergebnis dieses Kapitels stellt die Kategorisierung von Fehlern, Ausfällen und Störungen unter Verwendung ihrer Art und Quelle einerseits sowie ihres Auftretens in einer bestimmten Lebenszyklusphase andererseits dar.

Die Erläuterung des Umgangs mit Fehlern, Ausfällen und Störungen im Bahnsystem in Form der drei sicherungstechnischen Grundsätze *F/A/S-Ausschluss, F/A/S-Folgausschluss* und *F/A/S-Folgenbegrenzung* beinhaltet der erste Teil von Kapitel 5. Der zweite Teil beschreibt die wesentlichen Zustände (sicher, hemmend, gefährlich),

die technische Systeme einnehmen können. Die Anwendung vorhandener Forschungsergebnisse hinsichtlich der Verlässlichkeit von Verkehrssystemen auf ein betriebliches Szenario des Bahnsystems im Verfügbarkeits-Sicherheits-Diagramm und die Erweiterung des bisherigen Standes der Forschung durch die Anwendung der gewonnenen Erkenntnisse aus den Kapiteln 2 bis 5 prägen den dritten Teil von Kapitel 5.

Den Abschluss der Arbeit bildet Kapitel 6. Darin wird ein Modell zur ganzheitlichen Sicherheitsbetrachtung des Bahnsystems vorgeschlagen, das menschliche Aspekte beinhaltet, technische und organisatorische Randbedingungen integriert und diese jeweils den einzelnen Phasen im Systemlebenszyklus zuordnet. Zudem erfolgt in Kapitel 6 auf Grundlage der gewonnenen Erkenntnisse bei der Analyse eines betrieblichen Szenarios im Verfügbarkeits-Sicherheits-Diagramm ein Vorschlag zum zukünftigen Zulassungsverfahren von Bahnanlagen unter Verwendung eines betrieblichen Sicherheitsnachweises.

Auf der Grundlage dieses Modells und der darin enthaltenen Raten für menschliche, technische und organisatorische Fehler, Ausfälle und Störungen können vertiefende Untersuchungen (z. B. durch Arbeitsgruppen von Normungsgremien wie DIN, CEN, ISO, CENELEC, IEC) erfolgen. Ziel derartiger Arbeiten sollte die Bestimmung tolerierbarer Gefährdungsraten und individueller Risiken für die im Modell verankerten Komponenten (Technik, Mensch, Organisation) in den einzelnen Lebenszyklusphasen (Planung, Entwicklung, Fertigung, Inbetriebnahme, Regelbetrieb, Abweichung vom Regelbetrieb, Instandhaltung) sein.

Bei konsequenter Umsetzung dieser Überlegungen kann das Modell als Grundlage für die in der Praxis zu kontroversen Diskussionen führende Verteilung des Gesamtrisikos auf die einzelnen Beteiligten im Bahnsystem („Risikokuchen“) dienen. Überdies erlaubt die Einführung des vorgeschlagenen Zulassungsverfahrens von Bahnanlagen mit betrieblichem Sicherheitsnachweis die als Thema und Ziel dieser Arbeit formulierte ganzheitliche Sicherheitsbetrachtung des Bahnsystems.

Glossar

Ausfall/Versagen (engl. failure)

Beendigung der Fähigkeit einer Funktionseinheit, eine geforderte Funktion auszuführen. [DIN02]

Ein Ausfall ist das Aussetzen der Ausführung einer festgelegten Aufgabe (wobei auch ein erstmaliger Ausfall als Aussetzen der Ausführung gilt.) Als Ausfall wird somit der Übergang vom fehlerfreien in den fehlerhaften Zustand bezeichnet. Der Ausfall ist also ein Ereignis. [DIN90a]

Verletzung mindestens eines Ausfallkriteriums bei einer zu Beanspruchungsbeginn als fehlerfrei angesehenen Betrachtungseinheit. [DIN90a]

Ausfall, bedingter/abhängiger

Der Ausfall als Folge mehrerer Ereignisse, dessen Wahrscheinlichkeit nicht als das einfache Produkt der absoluten Wahrscheinlichkeit der Einzelereignisse ausgedrückt werden kann. [DIN00]

Ausfall (durch eine gemeinsame Ursache)

Ein Ausfall als Folge eines Ereignisses/von Ereignissen, das/die ein Zusammentreffen von Fehlerzuständen von zwei oder mehreren Bauteilen bewirkt/bewirken, was dazu führt, dass ein System seine geforderte Funktion nicht mehr ausüben kann. [DIN00]

Ausfall, gleichartig wirkender (engl. common-cause failure)

Gemeinsamer Ausfall in mehreren Betrachtungseinheiten, die unabhängig voneinander sein sollten. [DIN03b]

Ausfall, systematischer (engl. systematic fault)

Ausfall infolge von Fehlern (auch Irrtümern) bei einer beliebigen sicherheitsrelevanten Aktivität während einer beliebigen Phase des Lebenszyklus, die bewirken, dass diese bei einer bestimmten Kombination von Einwirkungen oder unter bestimmten besonderen Umweltbedingungen ausfällt. [DIN00]

Systematisches Versagen/Ausfall, bei dem eindeutig auf eine Ursache geschlossen werden kann, die nur durch eine Modifikation des Entwurfs oder des Fertigungsprozesses, der Art und Weise des Betriebes, der Bedienungsanleitung oder anderer Einflussfaktoren beseitigt werden kann. [DIN01a]

Ausfall, zufälliger (engl. random fault)

Nichtvorhersehbares Eintreten eines Ausfalls. [DIN03b]

Ausfallart

Die vorhergesagten oder beobachteten Ergebnisse einer Ausfallursache an einem gegebenen Objekt in Bezug auf die Einsatzbedingungen zum Zeitpunkt des Ausfalls. [DIN00]

Ausfallgrenzwert (engl. target failure measure)

Zu unterschreitende Wahrscheinlichkeit gefahrbringender Ausfallarten, die aufgrund der Anforderungen zur Sicherheitsintegrität festgelegt wird als:

- mittlere Ausfallwahrscheinlichkeit der Funktion im Anforderungsfall (in der Betriebsart mit niedriger Anforderungsrate) oder
- Wahrscheinlichkeit eines gefahrbringenden Ausfalls pro Stunde (in der Betriebsart mit hoher oder kontinuierlicher Anforderungsrate). [DIN02]

Ausfalloffenbarungszeit (engl. fault detection time)

Zeitspanne, die zu dem Zeitpunkt beginnt, an dem ein Ausfall auftritt, und die endet, wenn das Vorhandensein dieses Ausfalls erkannt wird. [DIN03b]

Ausfallrate (engl. failure rate)

Der grenzwert, falls ein solcher existiert, der Verhältniszahl von der bedingten Wahrscheinlichkeit, dass der Zeitpunkt T des Ausfalls eines Produktes in ein gegebenes Zeitintervall $(t, t+\Delta t)$ fällt, und der Länge dieses Intervalls Δt , wenn Δt gegen 0 geht, vorausgesetzt, das Objekt ist zu Beginn des Zeitintervalls in einem einwandfreien Zustand. [DIN00]

Ausfallreaktion, sicherheitsgerichtete

Das Herbeiführen eines sicheren Zustandes, nachdem ein gefährlicher Ausfall entdeckt wurde. [DIN03b]

Ausfallursache

Die Umstände, die bei der Konstruktion, bei der Herstellung oder im Einsatz zu einem Ausfall geführt haben. [DIN00], [IEC90]

Ausfallzeit

Die Zeitspanne, während der sich das Produkt in einem Unklarzustand befindet. [DIN00], [IEC90]

Element

Teil eines Produktes, der als Grundeinheit oder Grundbaustein bestimmt wurde. Ein Element kann einfach oder komplex sein. [DIN00]

EUC (engl. equipment under control)

Einrichtung, Maschine, Apparat oder Anlage, verwendet zur Fertigung, Stoffumformung, zum Transport, zu medizinischen oder anderen Tätigkeiten. [DIN02]

Fehler (engl. nonconformity)

Nichterfüllung einer Forderung. [MUE07]

Nichterfüllung der Spezifikation. [DIN95a]

Ein Fehler ist die Nichterfüllung vorgegebener Forderung durch einen Merkmalswert. Ein Fehler ist also ein Zustand (z. B. auch ein falscher logischer Zustand). [DIN90a]

Unzulässige Nichtübereinstimmung eines bestimmten Istmerkmals mit dem Soll in einer Betrachtungseinheit. [DIN90a]

Abweichung vom beabsichtigten Entwurf, die zu unerwünschtem Systemverhalten oder Ausfall führen kann. [DIN01a]

Fehler (engl. fault)

Nicht normale Bedingung, die eine Verminderung oder den Verlust der Fähigkeit einer Funktionseinheit verursachen kann, eine geforderte Funktion auszuführen. [DIN02]

Fehler, systematischer

Fehler in der Spezifikation, im Entwurf, in der Konstruktion, in der Installation, im Betrieb oder in der Instandhaltung eines Systems, eines Teilsystems oder einer Einrichtung. [DIN03b]

Fehlerart

Einer der möglichen Zustände eines fehlerhaften Produkts für eine gegebene geforderte Funktion. [DIN00], [IEC90]

Fehlfunktion/Fehler (engl. failure)

Abweichung vom spezifizierten Verhalten des Systems. Eine/ein Fehlfunktion/Ausfall ist die Folge einer Fehlerursache (fault) oder eines Fehlzustandes (error) im System. [DIN03b]

Fehlfunktion/Ausfall

Abweichung vom spezifizierten Verhalten des Systems. Eine Fehlfunktion/Ausfall ist die Folge einer Fehlerursache oder eines Fehlers im System. [DIN01a]

Fehlersicherheit (engl. fail-safe)

Konzept, das in den Entwurf eines Produktes so einfließt, dass bei Eintreten einer Fehlfunktion ein sicherer Zustand eingenommen oder beibehalten wird. [DIN03b]

Fehlerursache/Ausfall (engl. fault)

Abnormaler Zustand, der zu einem Fehler oder einer Fehlfunktion/Ausfall in einem System führen kann. Eine Fehlerursache kann zufällig oder systematisch sein. [DIN03b]

Fehlerursache/Ausfall (engl. fault)

Abnormaler Zustand, der zu einem Fehler oder einer Fehlfunktion/Ausfall in einem System führen kann. Eine Fehlerursache kann zufällig oder systematisch sein. [DIN01a]

Fehlzustand (engl. error)

Abweichung vom beabsichtigten Entwurf, die zu unerwünschtem Systemverhalten oder Ausfall führen kann. [DIN03b]

Funktionsfähigkeit (engl. reliability performance)

Fähigkeit einer Einheit, eine geforderte Funktion unter gegebenen Anwendungsbedingungen für ein gegebenes Zeitintervall zu erfüllen. [DIN04], [IEC90]

Gefahr

Eine physikalische Situation, die potenziell einen Schaden für den Menschen beinhaltet. [DIN00]

Gefährdung (engl. hazard)

Bedingung, die zu einem Unfall führen kann. [DIN03b]

Potenzielle Schadensquelle. [DIN02]

Gefährdungssituation (engl. hazardous situation)

Umstand, durch den eine Person einer Gefährdung ausgesetzt ist. [DIN02]

Gefährdungsanalyse

Prozess der Identifikation von Gefährdungen und der Analyse ihrer Ursache sowie der Ableitung von Anforderungen, um die Wahrscheinlichkeit und die Folgen von Gefährdungen auf ein akzeptables Maß zu begrenzen. [DIN03b]

Instandhaltbarkeit (engl. maintainability performance)

Die Wahrscheinlichkeit, dass für eine Komponente unter gegebenen Einsatzbedingungen eine bestimmte Instandhaltungsmaßnahme innerhalb einer festgelegten Zeitspanne ausgeführt werden kann, wenn die Instandhaltung unter festgelegten Bedingungen erfolgt und festgelegte Verfahren und Hilfsmittel eingesetzt werden. [DIN00]

Fähigkeit einer Einheit, unter gegebenen Anwendungsbedingungen in einem Zustand erhalten bzw. in ihn zurückversetzt werden zu können, in dem sie eine geforderte Funktion erfüllen kann, wobei vorausgesetzt wird, dass die Instandhaltung unter den gegebenen Bedingungen mit den vorgeschriebenen Verfahren und Hilfsmitteln durchgeführt wird. [DIN04], [IEC90]

Instandhaltung

Die Kombination aller technischen und administrativen Tätigkeiten einschließlich Aufsichtsmaßnahmen, um ein Produkt in einem Zustand zu halten oder wieder in einen Zustand zu versetzen, in dem es eine geforderte Funktion erfüllen kann. [DIN00], [IEC90]

Kombination aller technischen und administrativen Tätigkeiten einschließlich Überwachungsmaßnahmen, mit denen eine Betrachtungseinheit im funktionsfähigen Zustand erhalten oder in ihn zurückversetzt werden soll. [DIN03b]

Zur Instandhaltung zählen Wartung (Maßnahmen zur Bewahrung des Sollzustandes), Inspektion (Maßnahmen zur Feststellung und Beurteilung des Istzustandes) und Instandsetzung (Maßnahmen zur Wiederherstellung des Sollzustandes) einer Bahnanlage. [DIN03a]

Instandhaltung, korrektive

Die nach der Erkennung eines Fehlzustandes ausgeführte Instandhaltung, um ein Produkt in einen Zustand zu versetzen, in dem es eine geforderte Funktion erfüllen kann. [DIN00]

Instandhaltung, präventive

Die Instandhaltung in vorgegebenen Zeitabständen oder nach vorgeschriebenen Kriterien, die zur Verringerung der Ausfallwahrscheinlichkeit oder der Verschlechterung der Funktion einer Einheit vorgesehen ist. [DIN00], [IEC90]

Instandhaltungsbereitschaft (engl. maintenance support performance)

Fähigkeit einer Instandhaltungsorganisation, unter gegebenen Bedingungen bei Bedarf die Mittel bereitzustellen, die für die Instandhaltung einer Einheit unter Beachtung der festgelegten Instandhaltungsgrundsätze erforderlich sind. [DIN04], [IEC90]

Instandsetzung

Der Vorgang, wenn eine Einheit nach einem Fehler ihre geforderte Wiedereinsatzfähigkeit erlangt. [DIN00], [IEC90]

Lastenheft

Gesamtheit der Anforderungen des Auftraggebers an die Lieferungen und Leistungen eines Auftragnehmers. Darin enthalten sind auch die Anforderungen des Eisenbahn Bundesamtes. [MUE07]

Gesamtheit der Forderungen des Auftraggebers an die Lieferungen und Leistungen eines Auftragnehmers. [DIN97]

Pflichtenheft

Vom Auftragnehmer erarbeitete Realisierungsvorgaben aufgrund der Umsetzung des Lastenheftes. [MUE07]

Vom Auftragnehmer erarbeitete Realisierungsvorhaben aufgrund der Umsetzung des Lastenheftes. [DIN97]

Reaktionszeit bis zum Erreichen des sicheren Zustandes

Die Zeitspanne, die mit dem Entdecken eines Ausfalls beginnt und mit der Einnahme eines sicheren Zustandes endet. [DIN03b]

Redundanz

Die Bereitstellung von einem oder mehreren zusätzlichen, gewöhnlich identischen Maßnahmen, um die Fehlertoleranz zu erhalten. [DIN03b]

Reparatur

Teil der korrektiven Instandhaltung, bei der handwerkliche Handlungen an einer Einheit ausgeführt werden. [DIN00], [IEC90]

Maßnahme zur Wiederherstellung des geforderten Zustandes eines Systems, Teilsystems oder einer Einrichtung nach einem Ausfall/Fehler. [DIN03b]

Restrisiko (engl. residual risk)

Das trotz Schutzmaßnahmen verbleibende Risiko. [DIN02]

Risiko (engl. risk)

Die Wahrscheinlichkeit des Auftretens einer Gefahr, die einen Schaden verursacht, sowie der Schweregrad eines Schadens. [DIN00]

Die Kombination aus Häufigkeit oder Wahrscheinlichkeit und den Folgen eines spezifizierten gefährlichen Ereignisses. [DIN03b]

Kombination aus der Wahrscheinlichkeit, mit der ein Schaden auftritt, und dem Ausmaß dieses Schadens. [DIN02]

Risiko, tolerierbares (engl. tolerable risk)

Risiko, das basierend auf den aktuellen gesellschaftlichen Wertvorstellungen in einem gegebenen Zusammenhang tragbar ist. [DIN02]

Risiko, vertretbares

Der maximale Grad an Risiko durch ein Produkt, der für ein Bahnunternehmen toleriert werden kann. [DIN00]

Schaden (engl. harm)

Physische Verletzung oder Schädigung der Gesundheit von Menschen, entweder direkt oder indirekt als ein Ergebnis von Schäden von Gütern oder der Umwelt. [DIN02]

Sicherheit (engl. safety)

Das Nichtvorhandensein eines unzulässigen Schadensrisikos. [DIN00]

Freisein von nicht akzeptierbaren Risiken eines Schadens. [DIN03b]

Freiheit von unververtretbaren Risiken. [DIN02]

Sicherheit (engl. security)

Resistenz eines Systems gegenüber Vandalismus und unvernünftigem menschlichen Verhalten. [nach DIN00, Abschnitt 4.3.3]

Sicherheit, signaltechnische

Die Fähigkeit einer Sicherungsanlage, bei bestimmungsgemäßem Einsatz, ordnungsgemäßer Instandhaltung und vorschriftsmäßiger Handhabung während einer vorgegebenen Brauchbarkeitsdauer Gefährdungen durch Funktionsversagen in dem Umfang, der nach dem Stand der Technik erforderlich ist, auch dann zu verhindern, wenn Bauelementausfälle und Störungen in der zu Beanspruchungsbeginn als fehlerfrei angesehenen Sicherungsanlage eintreten. [MUE07]

Sicherheit gegen systematische Fehler

Der Grad in dem ein System frei von nicht identifizierten gefährlichen Fehlzuständen ist, und die Ursachen dafür. [DIN03b]

Sicherheit gegen zufällige Fehler

Der Grad mit dem ein System frei von gefährlichen zufälligen Ausfällen ist. [DIN03b]

Sicherheitsanforderungsstufe (SIL) (engl. safety integrity level)

Eine von einer festgelegten Anzahl diskreter Stufen für die Spezifizierung der ausreichenden Sicherheit von Sicherheitsfunktionen, die sicherheitsrelevanten Systemen zugeordnet sind. Der Safety Integrity Level mit der höchsten Ordnungsziffer hat den höchsten Level der ausreichenden Sicherheit. [DIN00]

Zahl, die den erforderlichen Grad des Vertrauens anzeigt, mit dem ein System seine spezifizierten Sicherheitseigenschaften bezüglich systematischer Fehler einhält. [DIN03b]

Eine von vier diskreten Stufen für die Spezifizierung der Anforderungen für die Sicherheitsintegrität der Sicherheitsfunktionen, die dem E/E/EP-sicherheitsbezogenen System zugeordnet werden, wobei der Sicherheits-Integritätslevel 4 die höchste Stufe der Sicherheitsintegrität und der Sicherheits-Integritätslevel 1 die niedrigste darstellt. [DIN02]

Sicherheitsintegrität (engl. safety integrity)

Die Wahrscheinlichkeit dafür, dass ein System die festgelegten Sicherheitsanforderungen unter allen festgelegten Bedingungen innerhalb einer bestimmten Zeitspanne erfüllt. [DIN00]

Die Fähigkeit eines sicherheitsrelevanten Systems, seine geforderten Sicherheitsfunktionen unter allen festgelegten Bedingungen innerhalb einer festgelegten betrieblichen Umgebung und innerhalb eines festgelegten Zeitintervalls zu erbringen. [DIN03b]

Sicherheitsmanagement (engl. safety management)

Die Managementstruktur, die sicherstellt, dass der Sicherheitsprozess richtig umgesetzt wird. [DIN03b]

Sicherheitsprozess (engl. safety process)

Reihe von Verfahren, deren Abfolge sicherstellt, dass die Sicherheitsanforderungen eines Produktes identifiziert und erfüllt werden. [DIN03b]

Störung

Fehlende, fehlerhafte oder unvollständige Erfüllung einer geforderten Funktion durch eine Einheit. [MUE07]

Verhindern oder Beeinträchtigen einer oder mehrerer Systemfunktionen durch äußere Einwirkungen auf das System. [DIN90a]

System

Zusammenstellung technisch-organisatorischer Mittel zur autonomen Erfüllung eines Aufgabenkomplexes. [MUE07]

Menge von Teilsystemen, die entsprechend einem Entwurf zusammenwirken. [DIN03b]

Systemlebenszyklus

Die Aktivitäten während einer Zeitspanne, die mit der Konzipierung eines Systems beginnt und mit seiner Stilllegung, wenn das System nicht länger für den Gebrauch verfügbar ist, endet. [DIN00]

Reihe von Tätigkeiten, die während eines Zeitraumes durchgeführt werden, der mit dem Konzept für ein System beginnt und mit der Außerbetriebnahme, nach der das System nicht mehr nutzbar ist, endet. [DIN03b]

Teilsystem

Ein Teil eines Systems, der eine spezielle Funktion erfüllt. [DIN03b]

Unfall

Ein nicht beabsichtigtes Ereignis oder eine Reihe von Ereignissen mit der Folge von Toten, von Verletzten, des Verlustes eines Systems oder Umweltschäden. [DIN03b]

Validation

Der auf Tests und Analysen beruhende Nachweis, dass ein Produkt in allen Belangen seine spezifizierten Anforderungen erfüllt. [DIN03b]

Validierung

Bestätigung durch Überprüfung und objektiven Nachweis, dass die besonderen Anforderungen für einen spezifischen, bestimmungsgemäßen Gebrauch erfüllt wurden. [DIN00]

Verifikation

Bestätigung durch Überprüfung und objektiven Nachweis, dass die festgelegten Anforderungen erfüllt wurden. [DIN00]

Die auf Analysen und Tests beruhende Feststellung in jeder Phase des Lebenszyklus, dass die Anforderungen der betrachteten Phase das Ergebnis der vorausgehenden Phase

erfüllen und dass das Ergebnis der betrachteten Phase die Anforderungen erfüllt. [DIN03b]

Verfügbarkeit

Die Fähigkeit eines Produktes, in einem Zustand zu sein, in dem es zu einem vorgegebenen Zeitpunkt oder während eines vorgegebenen Zeitintervalls eine geforderte Funktion unter vorgegebenen Bedingungen erfüllen kann, vorausgesetzt, dass die erforderlichen äußeren Mittel bereitgestellt sind. [DIN03b]

Die Fähigkeit eines Produktes, in einem Zustand zu sein, in dem es unter vorgegebenen Bedingungen zu einem vorgegebenen Zeitpunkt oder während einer vorgegebenen Zeitspanne eine geforderte Funktion erfüllen kann unter der Voraussetzung, dass die geforderten äußeren Hilfsmittel bereitstehen. [DIN00]

Fähigkeit eines Produktes, in einem Zustand zu sein, die geforderte Funktion unter vorgegebenen Bedingungen zu einer bestimmten Zeit oder über ein vorgegebenes Zeitintervall auszuüben, unter der Annahme, dass die erforderlichen externen Ressourcen zur Verfügung stehen. [DIN01a]

Versagen, menschliches (engl. human error)

Eine menschliche Handlung, die zu einem ungewollten Verhalten des Systems oder zu einer Fehlfunktion führen kann. [DIN03b]

Handlung oder Unterlassung eines Menschen, die zu einem unerwünschten Ergebnis führt. [DIN02]

Vorfall, gefährlicher (engl. hazardous event)

Gefährdungssituation, die zu einem Schaden führt. [DIN02]

Zustand, sicherer (engl. safe state)

Ein Zustand, der die Sicherheit weiterhin bewahrt. [DIN03b]

Zustand der EUC, in dem die Sicherheit erreicht ist. [DIN02]

Zuverlässigkeit

Die Wahrscheinlichkeit dafür, dass eine Einheit ihre geforderte Funktion unter gegebenen Bedingungen für eine gegebene Zeitspanne (t_1 , t_2) erfüllen kann. [DIN00], [IEC90]

Die Fähigkeit einer Betrachtungseinheit, eine geforderte Funktion unter gegebenen Bedingungen für eine gegebene Zeitdauer zu erbringen. [DIN03b]

Quellenverzeichnis

[AEG93]

Bundesministerium für Verkehr, Bau- und Wohnungswesen. Allgemeines Eisenbahngesetz 1993 (zuletzt geändert 2005).

[AND04]

Anders, E.: Ein Beitrag zur komplexen Sicherheitsbetrachtung des Bahnsystems. Signal + Draht 06/2004.

[AND05]

Anders, E.: Ein Beitrag zur komplexen Sicherheitsbetrachtung des Bahnsystems. 20. Verkehrswissenschaftliche Tage in Dresden. 19./20. September 2005.

[AND06a]

Anders, E.; Maschek, U.: Ein Beitrag zur komplexen Sicherheitsbetrachtung des Bahnsystems (Teil 2). Signal + Draht 04/2006.

[AND06b]

Anders, E.; Maschek, U: Anwendung des Verfügbarkeits-Sicherheits-Diagramms zur Bewertung von Prozessen im Bahnsystem. Rail Automation 2006 in Braunschweig. 22. Juni 2006.

[AND06c]

Technische Grundlagen der Sicherheit. Lehrheft SIM 01 für den Studiengang „Sicherheitsmanagement“ an der Privaten Fernfachhochschule in Darmstadt. 2006.

[AND06d]

RAMS-Analysen im Eisenbahnwesen. Lehrheft SIM 02 für den Studiengang „Sicherheitsmanagement“ an der Privaten Fernfachhochschule in Darmstadt. 2006.

[AND06e]

Spezifikation und Verifikation von LST-Anlagen. Lehrheft SIM 03 für den Studiengang „Sicherheitsmanagement“ an der Privaten Fernfachhochschule in Darmstadt. 2006.

[AND07]

Anders, E.; Maschek, U: Ein Beitrag zur komplexen Sicherheitsbetrachtung des Bahnsystems. 20. Verkehrswissenschaftliche Tage in Dresden. 24./25. September 2007.

[BÖR04]

Börcsök, J.: Elektronische Sicherheitssysteme. Heidelberg 2004.

[BRE01]

van Breugel, K.: Establishing Performance Criteria for Concrete Protective Structures. fib-Symposium: *Concrete & Environment*. Berlin, 3.–5. Oktober 2001.

[BRA99]

Braband, J.; Lennartz, K.: Systematisches Verfahren zur Festlegung von Sicherheitszielen. *Signal + Draht*. 09/1999.

[BRA05a]

Braband, J.; Yanna, J.-E.: Über das Verhältnis von Verfügbarkeit und Sicherheit in der betrieblichen Rückfallebene. *Rail Automation* 2005. Mai 2005.

[BRA05b]

Braband, J.: Risikoanalysen in der Eisenbahn-Automatisierung. Eurailpress Tetzlaff-Hestra GmbH & Co. KG. 2005.

[BRA06]

Braband, J. et al.: Die CENELEC-Normen zur Funktionalen Sicherheit. Edition *Signal und Draht*. 2006.

[DKE05]

www.dke.de. Juli 2005.

[DIN81]

DIN 25424-1: Fehlerbaumanalyse. Methoden und Bildzeichen, September 1981.

[DIN82]

DIN 31004. Teil 1. Entwurf: „Begriffe der Sicherheitstechnik – Grundbegriffe“, November 1982.

[DIN85]

DIN 25419: Ereignisablaufanalyse: Verfahren, graphische Symbole und Auswertung, November 1985.

[DIN89]

DIN V 19250: Grundlegende Sicherheitsbetrachtungen für MSR-Schutzeinrichtungen, Mai 1989.

[DIN90a]

DIN 40041: Zuverlässigkeit; Begriffe. Dezember 1990.

[DIN90b]

DIN 25448: Ausfalleffektanalyse (Fehler-Möglichkeiten- und -Einfluß-Analyse) 1990. Ersetzt 2006 durch DIN IEC 60812 [DIN06].

[DIN93]

DIN IEC 61025:1993: Störungsbaumanalyse. 1993.

[DIN95a]

DIN 55350-11:1995: Begriffe zu Qualitätsmanagement und Statistik – Teil 11: Begriffe des Qualitätsmanagements. 1995.

[DIN95b]

DIN V 19251: MSR-Schutzeinrichtungen, Anforderungen und Maßnahmen zur gesicherten Funktion, Februar 1995.

[DIN97]

DIN 69905: Projektabwicklung, Begriffe. Mai 1997.

[DIN00]

DIN EN 50126:1999: Bahnanwendungen – Spezifikation und Nachweis der Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit und Sicherheit (RAMS). März 2000.

[DIN01a]

DIN EN 50128:2001: Bahnanwendungen – Software für Eisenbahnsteuerungs- und Überwachungssysteme. November 2001.

[DIN01b]

DIN EN 50159-1:2001: Bahnanwendungen – Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme – Teil 1: Sicherheitsrelevante Kommunikation in geschlossenen Übertragungssystemen: November 2001.

[DIN01c]

DIN EN 50159-2:2001: Bahnanwendungen – Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme – Teil 2: Sicherheitsrelevante Kommunikation in offenen Übertragungssystemen: Dezember 2001.

[DIN02]

DIN EN 61508-4:2001: Funktionale Sicherheit elektrischer/elektronischer/programmierbar elektronischer sicherheitsbezogener Systeme – Teil 4: Begriffe und Abkürzungen. November 2002.

[DIN03a]

DIN 31051:2003: Grundlagen der Instandhaltung. Juni 2003.

[DIN03b]

DIN EN 50129:2003: Bahnanwendungen – Sicherheitsrelevante elektronische Systeme für Signaltechnik. Dezember 2003.

[DIN04]

DIN EN 60300:2004: Zuverlässigkeitsmanagementsysteme. Februar 2004.

[DIN06]

DIN IEC 60812: Analysetechniken für die Funktionsfähigkeit von Systemen – Verfahren für die Fehlerzustandsart- und –auswirkungsanalyse (FMEA). November 2006.

[DUC02]

Duczek, E., Braband, J.: Die Einführung der CENELEC-Normen – eine Herausforderung für die betriebliche Weiterbildung. *Signal + Draht*. 04/2002.

[EBO67]

Eisenbahn- Bau- und Betriebsordnung 1967 (zuletzt geändert 2005). Bundesministerium für Verkehr, Bau- und Wohnungswesen.

[ELM99]

Elms, D. G.: Achieving structural safety: theoretical considerations. *Structural Safety* 21 (1999) Seite 311–333.

[ETS05]

www.etsi.org

[FEN98]

Fenner, W., Naumann, P.: Verkehrssicherungstechnik: Steuern, Sichern und Überwachen von Fahrwegen und Fahrgeschwindigkeiten im Schienenverkehr. Erlangen 1998.

[FEN04]

Fenner, W., Naumann, P., Trinckauf, J.: Bahnsicherungstechnik. Erlangen 2004.

[FIS90]

Fischer, K.: Zuverlässigkeits- und Instandhaltungstheorie. Transpress-Verlag Berlin 1990.

[FVN84]

Fahrdienstvorschrift für Nichtbundeseigene Eisenbahnen (FV-NE). Verband Deutscher Verkehrsunternehmen. 1984 (zuletzt geändert 2005).

[GES74]

Gesetz zum Schutz vor schädlichen Umwelteinwirkungen durch Luftverunreinigungen, Geräusche, Erschütterungen und ähnliche Vorgänge (Bundes-Immissionsschutzgesetz). 1974 (zuletzt geändert 1. Juli 2005).

[GRA02]

Grams, T.: Risiko – Unser Umgang mit der Angst. Tagungsband des 7. Fuldaer Elektrotechnik-Kolloquiums. Fulda 2002.

[HIN93]

Hinzen, A.: Der Einfluss des menschlichen Fehlers auf die Sicherheit der Eisenbahn. Veröffentlichungen des Verkehrswissenschaftlichen Institutes der RWTH Aachen. 1993.

[ICA06]

ICAO – International Civil Aviation Organization. Doc 9876: Annual Report of the Council 2006.

[IEC90]

IEC 60050-191: International Electrotechnical Vocabulary. Chapter 191: Dependability and quality of service. Dezember 1990.

[INP84]

An Analysis of Root Causes in 1983 Significant Event Report. Institut of Nuclear Power Operations. INPO 84-027. Atlanta, Georgia 1984.

[INP85]

An Analysis of Root Causes in 1983 and 1984 Significant Event Report. Institut of Nuclear Power Operations. INPO 85-027. Atlanta, Georgia 1985.

[KON07]

Konakovsky, R.: Vorlesungsskript „Zuverlässigkeit und Sicherheit von Automatisierungssystemen“. Institut für Automatisierungs- und Softwaretechnik der Universität Stuttgart. 2007.

[KRO96]

Kröger, W.; Seiler, H.; Gheorghe A.: Technik, Risiko und Sicherheit. Abschlussbericht des Polyprojektes "Risiko und Sicherheit technischer Systeme" der ETH Zürich 1991-1994. VDF Hochschulverlag der ETH Zürich. 1996.

[KRO00]

Kröger, W.; Hoj, N. P.: Risk Analyses of Transportation on Road and Railway. Proceedings – Part 2/2 of Promotion of Technical Harmonization on Risk-Based Decision-Making. Mai 2000..

[KUH81]

Kuhlmann, A.: Einführung in die Sicherheitswissenschaft. Vieweg-Verlag. Wiesbaden 1981

[KUH00]

Kuhlmann, A.: Sicherheitskultur. TÜV-Verlag, Köln 2000.

[KUM96]

Kumamoto, H.; Henley, E.: Probabilistic risk assessment and management for engineers and scientists. IEEE Press. 1996.

[LAD01]

Ladkin, P.: Causal system analysis, volume RVS-Bk-05-01. RVS Group, University of Bielefeld, 2001.

[MAS05]

Maschek, U.: Vorlesungsskript „Verkehrssicherungstechnik“. Unveröffentlicht. Technische Universität Dresden, Fakultät Verkehrswissenschaften „Friedrich List“. Mai 2005.

[MAS07]

Maschek, U.: Rail Automation 2007. Braunschweig. Juni 2007.

[MIL05]

US MIL HDBK 217: Military Handbook, Reliability Prediction for Electronic Systems. 1992.

[MON99]

Montenegro, S.: Sichere und fehlertolerante Steuerungen/Entwicklung sicherheitsrelevanter Systeme. Carl Hanser Verlag. September 1999.

[MUE07]

Mü 8004: Eisenbahn-Bundesamt. Technische Grundsätze für die Zulassung von Sicherungsanlagen. Februar 2007.

[NAU02]

Naumann, P.; Pahl, J.: Leit- und Sicherungstechnik im Bahnbetrieb, Fachlexikon, Hamburg 2002.

[NIE00]

Niedziella, W.: Wie funktioniert Normung? VDE Verlag, Berlin und Offenbach. 2005.

[PRO07a]

Professur für Verkehrssicherungstechnik: Technische Universität Dresden, Fakultät Verkehrswissenschaften „Friedrich List“. Auf allgemeiner Lehrmeinung basierende Grafik Vorlesungsskript „Verkehrssicherungstechnik“. Maschek, U. Unveröffentlicht. Oktober 2007.

[PRO07b]

Professur für Verkehrssicherungstechnik: Technische Universität Dresden, Fakultät Verkehrswissenschaften „Friedrich List“. Auf allgemeiner Lehrmeinung basierende Ausführungen im Vorlesungsskript „Sicherheitswissenschaft“. Anders, E. Unveröffentlicht. November 2007.

[PUL02]

Pulvermüller, Fritz: Rechtliche Aspekte der Sicherheitsverantwortung im Eisenbahnverkehr. Signal + Draht. 07+08/2004.

[RAM05]

<http://www.rams.de>

[RAS80]

Rasmussen, J.: What can be learned from human error report? John Wiley & Sons, Chichester, 1980.

[REA94]

Reason, J.: Menschliches Versagen. Spektrum Akademischer Verlag. Heidelberg 1994.

[REN02]

Renpenning, F.: Zuverlässigkeitsprognosen in der Eisenbahnsignaltechnik. Signal + Draht. 09/2002.

- [RIL06]
Deutsche Bahn: RIL 819 „LST-Anlagen planen“. Planungsrichtlinie der Deutschen Bahn. Zuletzt geändert am 10.12.2006.
- [SCH01]
Schierle, J.; Lesjak, H.: Sicherheit im Gleisbereich. DB-Fachbuch. Eisenbahn-Fachverlag. Heidelberg/Mainz 2001.
- [SCH03]
Schnieder, E.: Verlässlichkeit von Verkehrssystemen in Verfügbarkeits-Sicherheitsdiagrammen. SIGNAL+DRAHT, 2003, Heft 10.
- [SCH04]
Schröder, F.; Salander-Ludwig, C.; Huwald, E.: Das Sicherheitsmanagementsystem der europäischen Eisenbahnen. Eisenbahn-Fachverlag Mainz. Deine Bahn 12/2004.
- [TAR03]
Tarnai, G.; Schnieder, E.: Formal Methods for Railway Operation and Control Systems. Proceedings of Symposium FORMS 2003. Budapest, May 2003.
- [TRI02]
Trinckauf, J.: Grundsätzliche Betrachtungen zur Verfügbarkeit. 2. Internationaler S+D-Kongress am 17./18.10.2002 in Fulda.
- [TRI03]
Trinckauf, J.: Die Sicherheit des Bahnsystems. Signal und Draht 5/2003.
- [TRI06]
Trinckauf, J.: Wie kann Modularisierung zur Lösung von Problemen beitragen? 6. Internationaler S+D-Kongress am 12./13.10.2006 in Fulda.
- [TRI07]
Trinckauf, J.: Menschliches Versagen?. Signal und Draht 3/2007.
- [TUB07]
www.tu-braunschweig.de/ifev/veranstaltungen/bieleschweig
- [UIC02]
UIC Safety Platform: Common safety targets, common safety indicators and common safety methods, 2002.
- [UIC04]
UIC Merkblatt 736 Signalrelais. 4. Ausgabe. Juni 2004.
- [UIC05]
www.uic.asso.fr/applications/catalogue/edito_de
- [VDI05]
22. Tagung Technische Zuverlässigkeit. VDI-Bericht 1884. Düsseldorf. 2005.

[VVB03]

Verwaltungsvorschrift für die Bauaufsicht über Signal-, Telekommunikations- und Elektrotechnische Anlagen (VV BAU-STE). 01.01.2003.

[WIK07]

<http://de.wikipedia.org/wiki/RAMS>

[WIT06]

Wittenberg, K.-D. et al.: Kommentar zur Eisenbahn- Bau- und Betriebsordnung (EBO). 5. Auflage. Darmstadt 2006.