1 Einleitung

1.1 Motivation

Den Ausgangspunkt der Arbeit bildet die heutige Situation im Schienenverkehr und die Feststellung, dass trotz eines hohen, technischen Standards der Leit- und Sicherungstechnik, Ausnahmesituationen nicht gänzlich vermieden werden können. Die zu erwartenden Unfallfolgen können, aufgrund von großen transportierten Massen, hohen Geschwindigkeiten und damit verbundenen Energien, langen Bremswegen und einer großen Anzahl an potenziell gefährdeten Personen, ein außerordentlich großes Schadensausmaß annehmen [HOE-00]. Zur Veranschaulichung werden die Umstände des Zugunglücks von Hannover-Misburg vom Dezember 1997 dargestellt, bei dem durch menschliches Versagen ein Personen- und ein Güterzug in einem Industriegelände frontal aufeinander geprallt waren (Bild 1-1, 1-2). Weiteres Bildmaterial und Presseinformationen zu ausgewählten Bahnbetriebsunfällen sind in Anhang A enthalten.

Bild 1-1: Zugunglück von Hannover-Misburg vom Dezember 1997 [HOE-00]

Trotz der 51 Verletzten und des materiellen Schadens von ca. 3 Mio. € haben verschiedene glückliche Umstände dazu beigetragen, dass es nicht zu einer riesigen Katastrophe gekommen war [KOH-97]. Zum einen war der erste Wagen hinter der E-Lok des Personenzuges, der mit 300 Passagieren besetzt war, ein Gepäckwagen. Außerdem hat eine durch den Unfall abgerissene Hochspannungsleitung mit 50.000 V keine Schäden angerichtet und ein Raffineriegelände war glücklicherweise 250 m von der Unglücksstelle entfernt.

Bei diesem Unfall hat der Triebfahrzeugführer des Güterzuges falsch auf ein Vorsignal reagiert und ein Haltesignal überfahren. Die vom zentralen Leit- und Sicherungssystem eingeleitete Zwangsbremsung, konnte den zu schnell fahrenden Güterzug nicht mehr rechtzeitig zum Stillstand bringen.

Bild 1-2: Unfall-E-Lok des Zugunglücks von Hannover-Misburg [HOE-00]

Durch den Einsatz des im Rahmen dieser Arbeit dargestellten, erweiterten Sicherungssystems ist die Chance relativ groß, Fehlverhalten zu kompensieren und den Fokus der heutigen Leit- und Sicherungstechnik zu vergrößern, um auch Bahnbetriebsunfälle dieser Art zu vermeiden oder die Unfallfolgen drastisch zu reduzieren.

Die genauen Ursachen für das Auftreten von Ausnahmesituationen können sehr verschieden sein und lassen sich nur mit beträchtlichem Aufwand durch konventionelle Leit- und Sicherungsfunktionen minimieren. Unfallträchtig sind insbesondere Situationen, an denen vom Leit- und Sicherungssystem nicht überwachte, potenzielle Kollisionspartner beteiligt sind (z.B. Fußgänger im direkten Umfeld des Fahrweges). Weiterhin besteht ein größeres Unfallrisiko in Situationen, die keine oder nur eine vergleichsweise geringe Überwachungsform durch ein übergeordnetes Sicherungssystem aufweisen (z.B. bei Rangierfahrten in Bahnhöfen). Diese Aussagen werden durch die europaweite Unfallstatistik aus dem Schienenverkehr von 1991 bis 1994 [BAR-97] bestätigt. Hiernach wurden 48 % der Unfälle durch menschliche Fehler und 5 % durch technische Fehler hervorgerufen. Bei 47 % der Unfälle lag die Unfallursache nicht im Verantwortungsbereich des Schienenverkehrs. In [BAR-97] werden die Bahnbetriebsunfälle auf die folgenden Unfallkategorien aufgeteilt (Bild 1-3).

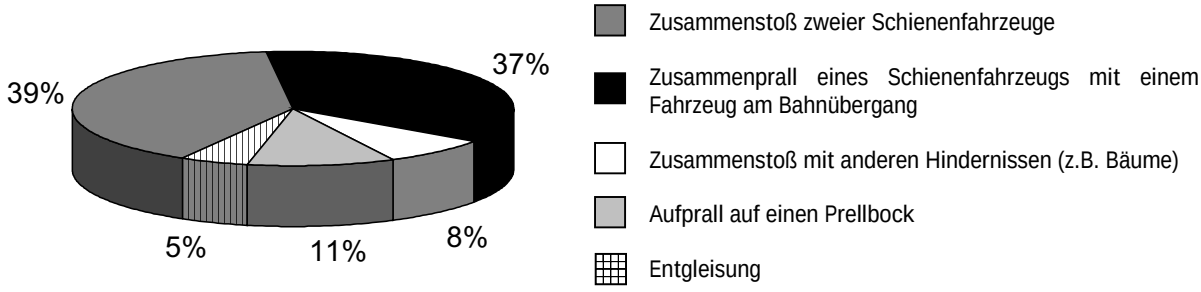

Bild 1-3: Maßgebliche Unfallkategorien und –verteilung

Bemerkenswert sind außerdem die statistischen Merkmale der Kollisionsgeschwindigkeiten in den Unfallkategorien. Danach ereignen sich 90 % aller Unfälle unterhalb einer Kollisionsgeschwindigkeit von 160 km/h.

Das bedeutet, insbesondere bei geringen bis mittleren Geschwindigkeiten und beim Auftreten unvorhergesehener Ereignisse (z.B. außerhalb des Regelbetriebs) sowie in kurzer Entfernung vor und nach Schienenfahrzeugen (< 300 m) werden Fahrzeugführern bei der Übernahme von Sicherheitsverantwortung keine befriedigenden Unterstützungen angeboten. Gerade auf diesem Gebiet wäre es dringend notwendig durch den Einsatz moderner Technologien die Anzahl menschlicher Fehler deutlich zu reduzieren. Hierzu können Unterstützungs-/ Assistenzsysteme einen wesentlichen Beitrag liefern, indem sie angemessen, vorausschauend und unmittelbar und damit wesentlich schneller als der menschliche Bediener („Schrecksekunde“) auf Ereignisse reagieren. Diese Eigenschaften sind besonders bei Prozessen notwendig, die kurze Laufzeiten aufweisen und deren Steuergrößen nur mäßigen Einfluss auf das Prozessgeschehen ausüben.

1.2 Stand der Technik

Im Schienenverkehr wird die Einhaltung der durch die Leit- und Sicherungstechnik vorgegebenen Fahrweise im Regelbetrieb nicht allein dem Menschen überlassen, sondern durch Zugbeeinflussungsanlagen überwacht, die bei Abweichungen von der zulässigen Fahrweise entsprechende Schutzreaktionen, in der Regel Zwangsbremsungen, auslösen. Jedoch greifen diese Schutzreaktionen nicht oder nur sehr eingeschränkt bei unvorhergesehenen Ereignissen oder einer geringen Ausbaustufe der Leit- und Sicherungstechnik. Folglich muss das Verhalten bei drohender Gefahr (beim Übergang von einer Normalsituation zu einer Ausnahmesituation) durch zusätzliche Vorschriften geregelt werden (im Geltungsbereich der DB AG durch die Konzernrichtlinie DS/DV 408.01-09 „Züge fahren und Rangieren“ [HOM-01]). Danach hat jeder Mitarbeiter bei der oben genannten Übernahme von Sicherheitsverantwortung umsichtig und entschlossen alles zu tun, um die drohende Gefahr abzuwenden oder zu minimieren. Das bedeutet, wenn eine Gefahr erkannt wird, die durch das Anhalten des Zuges abgewendet oder gemindert werden kann, muss sofort eine Notbremsung eingeleitet werden. Die Wirksamkeit dieser Richtlinie ist jedoch offenbar begrenzt, da weiterhin etwa die Hälfte aller Unfälle auf menschliches Fehlverhalten zurückgeführt werden können, was zeigt, dass der Mensch in diesen Situationen an die Grenzen seiner Fähigkeiten stößt.

Die heute in der Fachwelt diskutierten Lösungen von technischen Systemen mit Notbremsfunktion dienen der Vermeidung von Unfällen oder der Verringerung von Unfallfolgen und werden mit dem im Rahmen dieser Arbeit dargestellten fahrzeugbasierten Informations- und Entscheidungshilfesystem verglichen.

In dem BMBF-Forschungsprojekt „intermobil Region Dresden“ [IVI-01] wird, im Rahmen einer Gesamtstrategie zur nachhaltigen Mobilitätssicherung, das automatische Fahren am Beispiel einer S-Bahn dargestellt. Auf Basis von Videobild-, Radarsensorik und Auswertetechnik werden Komponenten für die automatische, fahrzeugbasierte Hinderniserkennung entwickelt. Für die Hinderniserkennung spielt, neben der Identifikation von Elementen der Bahninfrastruktur, die Verfolgung der Schiene entlang des Fahrweges und damit verbunden die Festlegung des zu überwachenden Raumes eine wichtige Rolle. Das entwickelte System [KRU-01] zur automatischen fahrzeugbasierten Hinderniserkennung gibt Gefahrenmeldungen an den Fahrzeugführer aus und wurde mit einem Versuchsträger erprobt.

Auch für den Straßenverkehr werden ähnliche Überlegungen angestellt. In [AME-00] wird ein fahrzeugbasiertes Notbremsmodul vorgestellt, das die Umgebung mit einer Kamera und zwei Laserscannern erfasst. Für detektierte Objekte in der Fahrzeugumgebung wird die Position

und Ausdehnung bestimmt. Anhand des Abstands zu einem detektierten Objekt wird die Zeit bis zur Kollision berechnet und mit der benötigten Zeit für eine Notbremsung bis zum Stillstand verglichen. Das Notbremsmodul wurde in einen Versuchsträger integriert und erprobt.

Ein System mit Notbremsfunktion zur Vermeidung von Auffahrunfällen im Straßenverkehr wird in [ARA-97] beschrieben. Die Umgebungssensorik des Systems besteht aus einem Radarsensor und einer CCD-Kamera. Auf Basis des errechneten Notbremsabstandes wird anhand der Umgebungsinformationen ein Zeitabstand zum Hindernis bestimmt. In dieser Ausbaustufe ist das System nicht für den Praxiseinsatz geeignet.

In [WIS-01] wird das vorausschauende Notbremssystem für Nutzfahrzeuge „Protector“ beschrieben. Per Radar registriert das Notbremssystem, wie weit das eigene Fahrzeug noch von einem bevorstehenden Hindernis entfernt ist. Erfolgt keine Bremsung seitens des Fahrers, greift das System ein und bringt das Fahrzeug zum Stehen oder aber auf eine Geschwindigkeit, die einen bestimmten Abstand zum Vordermann gewährleistet.

Notbremssysteme müssen zur Erzielung von Handlungskompetenz in vielfältiger Wechselwirkung mit der Umgebung stehen und besitzen daher eine hohe Systemkomplexität. Bei den bisherigen Ansätzen wurden ausschließlich die aktiven Sicherheitsmaßnahmen zur Unfallvermeidung betrachtet. Eine notwendige übergreifende Strategie zur Unfallvermeidung und -folgenverringerung liegt keinem der dargestellten Systeme zugrunde.

Bei dem im Rahmen dieser Arbeit für den Schienenverkehr vorgeschlagenen Informations- und Entscheidungshilfesystem wird ein neuartiger, gesamtheitlicher Sicherheitsansatz verfolgt. Bei diesem wird, in Ergänzung zu den heutigen Ansätzen, durch eine integrierte Betrachtung von aktiver und passiver Sicherheit eine Unfallvermeidungs- als auch Unfallfolgenverringerungsstrategie umgesetzt, die sich nachweisbar positiv auf die Entwicklung von Ausnahmesituationen auswirkt.

1.3 Zielsetzung

Der Schwerpunkt der Arbeit liegt im Entwurf eines wissensbasierten Informations- und Entscheidungshilfesystems zur Beherrschung von Ausnahmesituationen, dessen Realisierung als Funktionsdemonstrator sowie in der Untersuchung des Verhaltens durch Simulation unter dem Einfluss von charakteristischen Unfallszenarien [BOM-02, BME-02].

Dazu muss nicht nur ein funktionales Modell des wissensbasierten Informations- und Entscheidungshilfesystems (Kernsystem) mit dem internen Systemverhalten erstellt werden, sondern es wird ebenso ein Modell der Systemumgebung, einschließlich des Schienenfahrzeugs, benötigt. In diesem Umweltmodell werden die relevanten Objekte der Umgebung, die als Quellen und Senken von Informationen für das Kernsystem dienen, als Teil des Gesamtsystems soweit beschrieben, wie sie für eine Prüfung des Kernsystems erforderlich sind.

Diese Vorgaben sind besonders bei der Modellierung des fahrdynamischen Verhaltens eines Schienenfahrzeugs, als auch bei der Erstellung eines Modells zur Nachbildung von Stoßvorgängen zu berücksichtigen, da beide maßgeblich für den hohen Rechenaufwand bei der Simulation des dynamischen Verhaltens verantwortlich sind. Einerseits muss das fahrdynamische Verhalten eines Schienenfahrzeugs unter typenvariablen, strecken- und umweltsensitiven Rahmenbedingungen simuliert und der Kraftschluss im Rad-Schiene-Kontakt mit einem vereinfachten Reibungsmodell nachempfunden werden, um ein realistisches Verhalten und damit brauchbare Ergebnisse aus der Simulation von Unfallszenarien zu erhalten. Andererseits muss der Zugverband zur Nachbildung von Stoßvorgängen in Form einer Massenkette

beschrieben werden, um das Energieverzehrverhalten der Einzelfahrzeuge, die mit neuartigen Energieverzehrelementen modelliert sind, zu erfassen.

1.4 Vorgehensweise und gewählte Methoden

Aufbauend auf den im Rahmen dieser Arbeit dargestellten Sicherheitsphilosophien von Straßen- und Schienenverkehr und den sich bietenden Synergiepotenzialen, wird ein gesamtheitlicher Sicherheitsansatz dargestellt, der der integrierten Betrachtung von einer auf Schienenfahrzeugen zu installierenden, fahrzeugbasierten Umfeldsensorik, einem nachgelagerten Informations- und Entscheidungshilfesystem und den zur Verfügung stehenden Schutzsystemen (z.B. aktivierbaren Energieverzehrelementen) zugrunde liegt.

Die Beherrschung von Ausnahmesituationen wird als Lösung einer automatisierungstechnischen Aufgabe angesehen. Dazu wird in der Arbeit ein neuartiges Steuerungskonzept entwickelt, bei dem der Entscheidungsverantwortliche (menschlicher Bediener) in den Entscheidungsprozess mit einbezogen ist. Für die Formulierung des Entscheidungswissens zur Beherrschung von Ausnahmesituationen und dessen Repräsentation in einer Wissensbasis, werden analytische und deklarative Methoden eingesetzt. Mit einem neuen Verfahren zur Bildung von Analogien durch den Vergleich von Prozessdaten, wird das Verhalten in Ausnahmesituationen weiter verbessert, indem auf Basis eines Schätzmodells, Erfahrungen aus vergangenen Ausnahmesituationen für die aktuelle Ausnahmesituation genutzt werden.

Durch die Anwendung eines risikosenkenden Verfahrens werden die Ausnahmesituationen des Schienenverkehrs mit dem größten Risikobeitrag identifiziert. Diese Fokussierung bildet wiederum die Grundlage für die gezielte Ausgestaltung des wissensbasierten Informations- und Entscheidungshilfesystems.

Neben der auf Unfallprognosedaten basierenden situationsadaptiven Auslösung von Brems- oder Beschleunigungsmanövern, werden durch das im Rahmen dieser Arbeit entwickelte wissensbasierte Informations- und Entscheidungshilfesystem nach der gleichen Methode Entscheidungen zur Konditionierung des Zugverbandes für detektierte Ausnahmesituationen abgeleitet. Diese werden durch einen Auslösealgorithmus getroffen, der aus der Untersuchung von charakteristischen Kollisionsszenarien mit einem Mehrkörperzugmodell hervorgeht [BOE-02, BOM-04]. Von dem Informations- und Entscheidungshilfesystem ermittelte Handlungsmaßnahmen (z.B. Brems- oder Beschleunigungsmanöver), werden durch einen schnellen Inferenzmechanismus in Echtzeit umgesetzt.

Das im Rahmen dieser Arbeit entwickelte wissensbasierte Informations- und Entscheidungshilfesystem zur Beherrschung von Ausnahmesituationen ist als Funktionsdemonstrator in der Werkzeug- und Implementierungsumgebung Matlab/Simulink umgesetzt [BMM-02]. Durch die Simulation und den Test des neuartigen Informations- und Entscheidungshilfesystems sowie den Vergleich mit dem heutigen Stand der Technik, anhand von charakteristischen Ausnahmesituationen (Unfallszenarien), werden die markanten Unterschiede und erzielten Verbesserungen dargestellt.

1.5 Struktur der Arbeit

In den folgenden Kapiteln werden, ausgehend von einem neuartigen gesamtheitlichen Sicherheitsansatz, die Anforderungen, das Konzept und der Entwurf eines wissensbasierten Informations- und Entscheidungshilfesystems zur Beherrschung von Ausnahmesituationen beschrieben.

In Kapitel 2 werden mögliche Maßstäbe für Sicherheit dargestellt. Es wird festgestellt, dass Grenzwerte für Sicherheit von der gesellschaftlichen Akzeptanz mitbestimmt werden und

dass aus der Bestimmung von Risiken ein Maßstab für Sicherheit abgeleitet werden kann. Durch die Identifikation von wesentlichen Risikoschwerpunkten im Schienenverkehr wird die Zielsetzung des im Rahmen dieser Arbeit entwickelten Informations- und Entscheidungshilfesystems weiter detailliert.

Ausgangspunkt für den Entwurf des wissensbasierten Informations- und Entscheidungshilfesystems ist der in Kapitel 3 dargestellte neuartige Sicherheitsansatz, bei dem aktive und passive Sicherheit integriert betrachtet werden. Auf Basis der Sicherheitsphilosophien von Straßen- und Schienenverkehr werden Synergiepotenziale für gleiche und kostengerechte Technologieentwicklungen, z.B. im Bereich der Erkennung und Bewertung von Verkehrsszenarien, identifiziert. Darauf aufbauend wird der neuartige Sicherheitsansatz beschrieben, mit dem sich das heutige Sicherheitsniveau in beiden Verkehrssystemen erhöhen lässt.

Aus den in Kapitel 2 und 3 gewonnenen Erkenntnissen wird in Kapitel 4, im Hinblick auf die durch den Sicherheitsansatz geforderte Nutzung von Daten aus dem Fahrzeugumfeld und das damit verbundene Potenzial zur Risikominimierung, ein Systemkonzept für eine Umgebungssensorik zur Unfallfrüherkennung entwickelt, das im Rahmen des Anwendungsbeispiels in Kapitel 6 zum Einsatz kommt.

In Kapitel 5 wird der Aufbau und die Arbeitsweise des wissensbasierten Informations- und Entscheidungshilfesystems für Ausnahmesituationen beschrieben. Ein besonderes Augenmerk wird dabei auf die Wissensgenerierung / -repräsentation, die Nutzung von Erfahrungen aus vergangenen Ausnahmesituationen und auf risikosenkende Verfahren zur Bestimmung der maßgeblichen Ausnahmesituationen eines Anwendungsbereiches gelegt.

Auf dieser Basis wird in Kapitel 6 anhand eines komplexen Anwendungsbeispiels aus dem Schienenverkehr (Prozessklasse „Transportvorgänge im Verkehrswesen“) die risikosenkende Ausgestaltung des wissensbasierenden Informations- und Entscheidungshilfesystems dargestellt. Dabei werden die positiven Effekte durch das frühzeitige Erkennen und Interpretieren von Ausnahmesituationen (Überbrückung der menschlichen Reaktionszeit) und das unmittelbare Ergreifen von situationsadaptiven unfallvermeidenden Maßnahmen (z.B. Bremsungen) und folgenmindernden Maßnahmen (z.B. Aktivierung von Energieverzehrelementen) beschrieben. Im Vordergrund stehen dabei die folgenden Fragestellungen:

- Einfluss des Zeitgewinns durch frühzeitiges Erkennen und angemessenes Reagieren auf die Entwicklung von Ausnahmesituationen,
- Auswirkungen bei verspätetem Reagieren von Fahrzeugführern auf Ausnahmesituationen durch widrige Sichtverhältnisse (z.B. Niederschlag, Dunkelheit),
- Bedeutung von reproduzierbaren Verhaltensweisen des wissensbasierten Informations- und Entscheidungshilfesystems im Vergleich zum variablen Verhalten menschlicher Bediener,
- Einfluss der situationsadaptiven Konditionierung von Schienenfahrzeugen auf die Unfallauswirkungen.

Die softwaretechnische Umsetzung und Implementierung des Assistenzsystems in einem Online-Softwaredemonstrator auf Basis der Werkzeug- und Implementierungsumgebung Matlab / Simulink wird in Kapitel 7 beschrieben.

Auf der Grundlage von Simulationen der Dynamik des Gesamtsystems bei charakteristischen Ausnahmesituationen (Unfallszenarien), wird eine abschließende Prüfung des wissensbasierten Informations- und Entscheidungshilfesystems im Hinblick auf die oben genannten Fragestellungen vorgenommen.

2 Grenzwerte für Sicherheit

Die Begriffe Sicherheit und Risiko werden im Rahmen dieser Arbeit aus dem Blickwinkel des Schienenverkehrs dargestellt. Im Anschluss an die Beschreibung der verschiedenen Kriterien für Sicherheit und Risiko werden Risikoschwerpunkte identifiziert und Abhilfemaßnahmen vorgeschlagen. An bestimmten Stellen werden Parallelen zum Straßenverkehr gezogen.

Für nahezu alle Gebiete menschlicher Tätigkeit werden Grenzwerte definiert und deren Einhaltung vorgeschrieben. Damit soll der Verbleib in einem sicheren Zustand erreicht und der durch ein Ereignis verursachte Übergang in einen unerwünschten (unsicheren) Zustand verhindert werden. Im Bereich der Sicherheitstechnik ist das verursachende Ereignis ein technischer oder menschlicher Fehler, der in erster Linie zu einer erhöhten Gefährdung des Gesundheitszustandes der Prozessteilnehmer führt. Soll die Einhaltung von Grenzwerten den Übergang in einen unerwünschten Zustand vollständig verhindern, müssen Grenzwerte so formuliert werden, dass bei deren Einhaltung keine Ausnahmesituation (Unfall) auftreten kann. In der Praxis lassen sich Grenzwerte dieser Qualität entweder nicht oder nur mit außerordentlich großem Aufwand erreichen. Folglich besteht beim Umgang mit technischen Systemen grundsätzlich ein Restrisiko und es müssen praxistaugliche Maßstäbe formuliert werden, an denen technische Systeme gemessen werden können und bei deren Einhaltung eine ausreichende Sicherheit gewährleistet ist. Diese Maßstäbe werden beispielsweise durch die Anwendung der anerkannten Regeln der Technik vorgegeben, bei deren Einhaltung ein bestimmtes Restrisiko nicht überschritten wird. Bei Veränderung bestehender oder Einführung neuer Systeme (z.B. im Schienenverkehr), die weder den anerkannten Regeln der Technik noch den geltenden Vorschriften entsprechen, müssen Sicherheitsnachweise erbracht werden. Zielsetzung des Sicherheitsnachweises für diese Systeme, die von Vorschriften abweichen oder nicht den anerkannten Regeln der Technik entsprechen, ist der Nachweis der gleichen Sicherheit, wie bei Beachtung dieser Regeln und Vorschriften [EBO-67].

2.1 Definitionen für Sicherheit und Risiko

Die Formulierung eines Maßstabs für Sicherheit ist nicht trivial. In [LEG-98] werden die folgenden möglichen Maßstäbe für Sicherheit genannt (Tabelle 2-1):

Nr.	Maßstäbe für Sicherheit	Bedeutung
1	Absolute Sicherheit	Kein einziges Individuum kommt durch Unfälle mit Beteiligung von technischen Einrichtungen zu Schaden.
2	Sicherheit im Rahmen technischer Machbarkeit	Alle technischen Mittel werden ausgenutzt, um das von einer technischen Einrichtung ausgehende Risiko zu vermindern.
3	Sicherheit bis zu einer Nachweisgrenze	Alle Sicherheitsmaßnahmen werden vorgenommen, deren Wirkung sich statistisch nachweisen lässt.
4	Sicherheit im Rahmen der Bezahlbarkeit	Es werden alle Sicherheitsmaßnahmen durchgeführt, die finanzierbar sind, ohne dass die betrachtete Anlage unrentabel oder unverkäuflich wird.
5	Sicherheit nach dem „Stand der Technik“	Neu entwickelte Einrichtungen müssen mindestens so sicher sein, wie ähnliche bereits vorhandene Einrichtungen. Die vorhandenen Einrichtungen und anerkannten Regeln der Technik definieren den Stand der Technik.
6	Sicherheit im Rahmen volkswirtschaftlicher Rentabilität	Alle volkswirtschaftlich sinnvollen Sicherheitsmaßnahmen werden an technischen Einrichtungen vorgenommen.
7	Sicherheit nach Grenzkostenverfahren	Alle Sicherheitsmaßnahmen bis zu einer festgelegten Kosten / Nutzen-Grenze werden an technischen Einrichtungen vorgenommen.
8	Gleichverteilte individuelle Sicherheit	Alle Individuen sind zu jeder Zeit einem gleich hohen Risiko ausgesetzt. Die Höhe des Risikos bestimmt das volkswirtschaftlich zur Verfügung stehende Finanzvolumen für Sicherheitsmaßnahmen.
9	Sicherheitsdefinitionen durch Experten- und Gerichtsurteile	Die Sicherheit einer Einrichtung ist ausreichend, wenn technische und juristische Experten die Einrichtung als sicher beurteilen.
10	Sicherheit im Rahmen gesellschaftlicher Akzeptanzgrenzen	Die Sicherheit einer Anlage wird so ausgelegt, dass das verbleibende Risiko von der Mehrheit der Bevölkerung akzeptiert wird.

Tabelle 2-1: Maßstäbe für Sicherheit [LEG-98]

Ein in der Praxis verwendbarer Maßstab für Sicherheit muss die folgenden Eigenschaften erfüllen:

- Machbarkeit, d.h. der Maßstab für Sicherheit muss mit entsprechenden Maßnahmen von dem System erreicht werden können.
- Bezahlbarkeit, das bedeutet der Maßstab für Sicherheit muss sich mit vertretbaren finanziellen Aufwendungen erreichen lassen.
- Nachvollziehbarkeit, d.h. es muss transparent sein, mit welchen Maßnahmen der Maßstab für Sicherheit erreicht wird.
- Akzeptanz, das bedeutet der Maßstab für Sicherheit muss von der Gesellschaft auch als solcher anerkannt werden.

Die Maßstäbe 1, 2, 3, 8 für Sicherheit erfüllen aufgrund der zu erwartenden hohen finanziellen Aufwendungen nicht die Eigenschaft „Bezahlbarkeit“. Die rein betriebswirtschaftlich orientierten Maßstäbe für Sicherheit (4, 6, 7) führen nicht zur Akzeptanz in der Gesellschaft. Bei den Maßstäben 5 (Sicherheit nach dem „Stand der Technik“) und 9 (Sicherheitsdefinitionen durch Experten- und Gerichtsurteile) ist die Nachvollziehbarkeit der wesentliche Schwachpunkt.

Bei der Ausrichtung von Sicherheitsrichtlinien an der gesellschaftlichen Akzeptanz (10), lassen sich die genannten Anforderungen an Maßstäbe für Sicherheit erfüllen. Zur Bestätigung seien die im Schienenverkehr häufig eingesetzten risikoorientierten Sicherheitsnachweise [BAS-96, BRA-00] genannt, denen der oben genannte Maßstab für Sicherheit zugrunde liegt. Für diese gesellschaftliche Akzeptanzgrenze müssen nun nachvollziehbare Regeln (Grenzwerte für Sicherheit) existieren, damit sie als Maßstab für Sicherheit gelten kann. Nach [DIN-90] werden die beiden Begriffe „Sicherheit“ und „Risiko“ wie folgt definiert (weitere sicherheitstechnische Grundbegriffe gemäß DIN, s. Anhang B).

Sicherheit:
Sicherheit ist eine Sachlage, bei der das Risiko nicht größer als das Grenzrisiko ist.

Risiko:
Das Risiko, das mit einem bestimmten technischen Vorgang oder Zustand verbunden ist, wird zusammenfassend durch eine Wahrscheinlichkeitsaussage beschrieben, die
- die zu erwartende Häufigkeit des Eintritts eines zum Schaden führenden Ereignisses und
- das beim Ereigniseintritt zu erwartende Schadensausmaß

berücksichtigt.

Das bedeutet, aus der Bestimmung von Risiken für (technische) Anwendungen und deren Vergleich mit anwendungsbezogenen gesellschaftlichen Risikoakzeptanzwerten, ist unmittelbar ein Maßstab für Sicherheit ableitbar.

Aus den genannten Gründen spielen Risikobetrachtungen oder risikoorientierte Ansätze im Bezug auf Sicherheitsnachweise für technische Systeme eine wichtige Rolle. Dabei ist die Zielsetzung, aus der Risikoanalyse für die Komponenten eines definierten abgegrenzten Systems, abzuleiten, ob das modifizierte oder neuartige System ein ausreichendes Sicherheitsniveau aufweist bzw. welche zusätzlichen Maßnahmen zur Risikominimierung ergriffen werden müssen. Risikoorientierte Sicherheitsnachweise bestehen aus den Hauptkomponenten „Risikoanalyse, Risikobewertung, und Maßnahmenplanung“. Nach der Systemabgrenzung und -beschreibung werden in einem ersten Schritt die Risiken des isolierten Systems bestimmt (Risikoanalyse). Darauffolgend werden die Risiken anhand von Kriterien bewertet (Risikobewertung). Auf Basis des Ergebnisses der Risikoanalyse und –bewertung erfolgt, falls erforderlich, die Planung von zusätzlichen Sicherheitsvorkehrungen (Maßnahmenplanung).

Die Analyse und Bewertung von Risiken für unterschiedliche Risikoträger basiert auf den folgenden Risikoformen:

- Individuelles Risiko des Einzelnen, als Wahrscheinlichkeit während der Nutzung eines Systems (z.B. Schienenverkehr) in einem definierten Zeitraum einen bestimmten Schaden zu erleiden.
- Kollektives Risiko, als Wahrscheinlichkeit für das Auftreten von Schäden einer bestimmten Dimension, die die Gesellschaft oder einen bestimmten Teil der Gesellschaft in einem bestimmten Zeitraum treffen.
- Empfundenes Risiko, als Wahrscheinlichkeit für das Auftreten von Schäden einer bestimmten Dimension, deren Größe mit einer subjektiv empfundenen Wertung in Abhängigkeit von Aversionen oder Sympathien bemessen ist.

Die Risikoanalyse bildet die Basis des risikoorientierten Sicherheitsnachweises. Durch sie werden Gefahren identifiziert und von daraus resultierenden Ausnahmesituationen die zu erwartenden Häufigkeiten und Schadensausmaße quantitativ abgeschätzt. Bei der Risikobewer-