Risikoanalysen in der Eisenbahn-Automatisierung

Jens Braband

Herausgegeben von der **Siemens AG**

EDITION SIGNAL + DRAHT

Eurail press

Vorwort

Bis vor wenigen Jahren stand bei der Beurteilung von Funktionen von signaltechnischen Einrichtungen die Frage im Vordergrund, ob diese Funktion sicher oder nicht sicher ausgeführt werden muss. Die Antwort wurde von dem Ergebnis der Analyse bestimmt, ob es bei einem technischen Versagen zu einem Unfall kommen kann. Wie wahrscheinlich ein solches Ereignis sein würde, ob es trotz einer Gefährdung überhaupt zu einem Unfall kommen könnte und welche Folgen der Unfall haben würde, wurde nicht eingehend untersucht. Sicher oder nicht sicher war die Fragestellung, aber nicht, wie sicher.

Dies führte bei der Relaistechnik zu relativ einfachen Regeln über die anzunehmenden und zu beherrschenden Fehler, was im Sicherheitsnachweis durch die Reaktion zur sicheren Seite zu belegen war. Mit Einführung der Elektronik und Rechnersysteme reichte diese Betrachtungsweise nicht mehr aus. Es wurden komplexe Regelwerke - wie die Mü 8004 - geschaffen, mit denen die neue Herausforderung aber auf der Basis der bis dahin geltenden „Philosophie“ gemeistert werden sollte und auch wurde. Dabei wurden in die Richtlinien der Mü 8004 bereits Ansätze zu einer differenzierteren Betrachtungsweise nach dem Grad der erforderlichen Sicherheit aufgenommen, z.B. bei Anzeigeeinrichtungen von elektronischen Stellwerken.

Diese Situation hat sich grundlegend mit der Einführung der risikoorientierten Betrachtungsweise durch die EN 50126 und insbesondere die EN 50129 geändert. Plötzlich standen Begriffe wie Risikoanalyse, Gefährdungsanalyse, Risikomatrix, Risikograph, Risikoprioritätszahlen und THR im Blickfeld des Signalingenieurs, mit denen er zuvor nicht umgehen musste. Die Diskussion war durch eine erhebliche Unsicherheit auch unter Fachleuten geprägt.

Der Autor dieses Buchs hat durch Mitarbeit in Gremien sowie an zahlreichen Veröffentlichungen und Vorträgen die Entwicklung hin zu einer „Kultur der Risikoanalysen“ in der Eisenbahnsignaltechnik – zumindest in Deutschland – stark geprägt. Daher ist er besonders qualifiziert, das in den letzten Jahren entstandene neue Wissen über die Bewertung der Sicherheit in diesem Buch darzustellen.

Neben einer grundlegenden Einführung in die „Welt der Bewertung von Risiken“ werden die bei unterschiedlichen Anwendungen (auch außerhalb der Eisenbahnsignaltechnik) eingesetzten Methoden zur Risikoanalyse vorgestellt und diskutiert. Wenn auch die beschriebenen, tatsächlich ausgeführten Risikoanalysen im Wesentlichen auf die Signaltechnik beschränkt sind, so möchte ich dem Autor insbesondere dafür danken, dass er die Notwendigkeit der integrierten Betrachtung der Funktionen des Menschen und der Technik im Zuge der Risikobewertung eines Prozesses herausgestellt hat. Das gilt auch für die Betonung des generischen Ansatzes bei Risikoanalysen im Zuge der Definition und Entwicklung neuer Systeme. Da mit Risikoanalysen in der Regel ein hoher Aufwand verbunden ist, können die Kosten zum Nutzen nur in einem vernünftigen Verhältnis gehalten werden, wenn die Analysen typ- und bauformorientiert (generisch) – und nicht fokussiert auf jede einzelne Anlage – ausgeführt werden.

Meine hohe Anerkennung hat gefunden, dass Herr Prof. Dr. Braband seine Erkenntnisse und Erfahrungen dazu genutzt hat, basierend auf eingeführten Methoden einen einfachen, aber rigorosen Ansatz für Risikoanalysen in der Eisenbahntechnik unter dem Begriff „Best Practice Risk“ (BP-Risk) zu definieren. Mit dieser Vorgehensweise kann der für Risikoanalysen erforderliche Aufwand erheblich gesenkt werden. Eine Anerkennung durch das Eisenbahn-Bundesamt liegt bereits vor.

Das Handbuch dürfte hauptsächlich für in Ausbildung befindliche Eisenbahningenieure, aber auch für die Weiterbildung und als Nachschlagewerk für ausgebildete Fachleute von Bedeutung sein. Dabei kann es sich um Mitarbeiter in der Eisenbahnindustrie, „Techniker und Betriebler“ bei der Deutsche Bahn AG, der Europäischen Eisenbahnagentur, dem Eisenbahn-Bundesamt und anderen Aufsichtsbehörden, um Mitarbeiter von benannten Stellen, Planungsbüros und Consultant-Firmen sowie um anerkannte Sachverständige und Studenten handeln.

Es bleibt festzustellen, dass die Problematik der Risikoanalysen in dem Eisenbahnsektor in der hier angebotenen Tiefe und Praxisorientierung bisher nicht zusammenhängend behandelt worden ist. Dem Autor spreche ich daher meinen Dank und meine Anerkennung dafür aus, dass er der eisenbahntechnischen Fachwelt dieses Buch zur Verfügung gestellt hat.

Karl-Heinz Suwe

Chefredakteur der Fachzeitschrift
SIGNAL+DRAHT

Inhaltsverzeichnis

1 Motivation

1.1 Zielsetzung

In diesem Buch wird der Versuch unternommen, verschiedene Ansätze und Aspekte bei Risikoanalysen in der Eisenbahntechnik ganzheitlich darzustellen. Dies bedeutet, dass der Schwerpunkt mehr auf der Verdeutlichung von Zusammenhängen und Hintergründen liegt, als in der Erzielung neuer Forschungsergebnisse oder der Darstellung von technischen Details. Letzteres ist bereits in der umfangreichen Fachliteratur dokumentiert worden, allerdings wird beim üblichen Format und Umfang von Zeitschriftenartikeln oder Tagungsbeiträgen häufig der Blick für das Ganze und das Verständnis für Zusammenhänge erschwert. Unter Eisenbahntechnik wird dabei in diesem Buch im engeren Sinn Eisenbahn-Automatisierungstechnik verstanden, d.h. Automatisierung des Eisenbahnbetriebs durch programmierbare elektronische Systeme.

Den Schwerpunkt der Ausführungen bildet zum einen eine systematische Vorgehensweise zur Festlegung von Sicherheitszielen für eisenbahntechnische Einrichtungen sowie zum anderen ein generischer Ansatz zur Bewertung individueller Risiken. Durch Vergleich mit alternativen Ansätzen sowie Diskussion einiger Fallstudien sollen die wesentlichen Charakteristika dieses Ansatzes herausgearbeitet werden.

Eine wesentliche Erkenntnis, die aus zahlreichen Fallstudien gewonnen wurde, bildet die Zusammenstellung der wesentlichen Anforderungen an eine optimierte Vorgehensweise für Risikoanalysen in der Eisenbahntechnik. Auf dieser Grundlage wird der Versuch unternommen, eine Methode zu konstruieren, die diese Anforderungen erfüllt.

Obwohl hier Anwendungen aus der Eisenbahnsignaltechnik im Vordergrund stehen, ist der Anwendungsbereich der vorgestellten Ergebnisse keinesfalls auf die Eisenbahnsignaltechnik beschränkt [1]. Es steht zu erwarten, dass die hier dargestellten Grundsätze und Erfahrungen aus der Eisenbahnsignaltechnik auch zur Basis von Risikoanalysen in der gesamten Eisenbahntechnik werden, so sieht es jedenfalls ein Entwurf für einen Anwendungsleitfaden der Norm DIN EN 50126 [2] vor.

1.2 Ein Fallbeispiel

Die natürlich sofort zu Beginn eines solchen Buchs auftretende Frage „Wozu überhaupt Risikoanalysen?“ soll zunächst anschaulich anhand eines Fallbeispiels verdeutlicht werden.

Am 4. Januar 2000 kam es im norwegischen Åsta zu einem schweren Eisenbahnunfall auf einer eingleisigen Strecke *(Bild 1)*. Die Strecke wird aus einem Kontrollzentrum in Hamar ferngesteuert, die meisten Bahnhöfe sind unbesetzt. Die Einführung einer Zugbeeinflussung war geplant, aber noch nicht realisiert.

Bild 1: Unfall bei Åsta

Stark vereinfacht war der zeitliche Ablauf wie folgt

13:07 Beide Züge fahren ab.
13:08 Weiche Nr. 2 in Rudstadt wird aufgefahren.
13:12 Im Kontrollzentrum in Hamar wird bemerkt, dass sich beide Züge auf Kollisionskurs befinden. Es ist aber unmöglich, die Handy-Nummern der beiden Triebfahrzeugführer rechtzeitig zu finden, um diese noch zu warnen.
13:13 Die beiden Züge kollidieren und geraten in Brand (Dieseltriebzüge).

Der Untersuchungsbericht [3] konnte leider nicht mehr mit Sicherheit feststellen, ob es sich um einen menschlichen Fehler oder sogar technisches Versagen gehandelt hat, denn

– die Triebfahrzeugführer wurden bei dem Unfall getötet,
– die Diagnosedaten des Stellwerks waren nicht umfassend und aussagekräftig genug,
– es konnte durch die Analyse nicht ausgeschlossen werden, dass das Ausfahrsignal in Rudstadt mehrere Sekunden lang einen falschen Signalbegriff gezeigt haben könnte.

Allerdings macht der Bericht sehr deutliche Aussagen zu Management-Defiziten, die zu diesem Unfall beigetragen haben:

- „The Norwegian National Rail Administration should have conducted more risk analyses over the last few years in the light of the changes introduced that affected safety."
- „In the view of the commission, the Åsta accident occurred because of basic inadequacies in the Norwegian National Rail Administration with regard to safety consciousness and safety management."

Zu den angesprochenen Änderungen oder Versäumnissen zählten insbesondere:

- Im Kontrollzentrum wurde die aufgefahrene Weiche nur durch einen Hinweistext am Bildschirmrand angezeigt, nicht durch einen akustischen Alarm. Dadurch wurde diese Situation erst sehr spät erkannt.
- Bisher mussten sowohl Triebfahrzeugführer als auch Zugführer die Ausfahrsignale beobachten und der Abfahrt zustimmen. Nach einer Änderung der Vorschriften war hierfür nur noch der Triebfahrzeugführer verantwortlich.
- Der Zugbahnfunk war auf dieser Strecke abgeschafft worden. Stattdessen wurden Handys an die Triebfahrzeugführer ausgegeben. Es gab keine Vorschriften, wie diese Rufnummern bekannt gemacht und verwaltet werden sollten. Das Personal im Kontrollzentrum hatte sich eine praktische Handhabung überlegt, die aber am Unglückstag versagte.
- Die Kreuzung der Züge war nicht vorab bestimmt, sondern wurde dynamisch nach Betriebslage vereinbart (Luftkreuzung).
- Berichten über die Anzeige von fehlerhaften Signalbegriffen von Triebfahrzeugführern wurde nicht ausreichend nachgegangen.

Dieser Fall ist exemplarisch für viele Unfälle und zeigt grundsätzliche Probleme auf:

- Bei den meisten Eisenbahnen sind die Vorschriften historisch gewachsen und - insbesondere was die Sicherheit angeht - auch durch Erfahrungen aus Unfällen stark geprägt.
- Der rasche technologische Fortschritt - aber auch der Kostendruck - zwingt die Eisenbahnen zu betrieblichen und technischen Änderungen in einer höheren Geschwindigkeit als jemals zuvor in ihrer Geschichte. Dies erfolgt unter den Randbedingungen von immer komplexeren technischen Systemen sowie starkem Personalabbau.
- Dabei ist es schwer, die Sicherheit des Gesamtbetriebs sicherzustellen, wenn nur einzelne Maßnahmen oder Änderungen bewertet werden (und häufig auch noch verschiedene Stellen dafür zuständig sind).

Risikoanalysen sind ein probates Mittel, sich eine solche Gesamtübersicht zu verschaffen, die Auswirkungen von Änderungen zu bewerten und auf Grundlage der zur Verfügung stehenden

Informationen bewusste und optimierte Entscheidungen zu treffen. Es sei am Rande bemerkt, dass Entscheidungen auch ohne Risikoanalysen getroffen werden. Risikoanalysen sind im Grunde nur ein Mittel, diese Entscheidungen methodisch fundiert und nachvollziehbar zu treffen.

Die Probleme, die zum Unfall bei Åsta führten, wären schon durch eine Risikoanalyse mit einfachen Methoden klar offenbart worden. Wären die Erkenntnisse einer solchen Analyse auch noch konsequent durch ein entsprechendes Sicherheitsmanagement der Betriebsleitung in die Praxis umgesetzt worden, so wäre es zu diesem Unfall sicherlich nicht gekommen.

4.5.4 Risikobewertung

4.5.4.1 Risikoakzeptanz

Wir verwenden, um umfangreiche Kosten-Nutzen-Analysen oder Aufteilungen von globalen Risikogrenzwerten auf Teilsysteme zu vermeiden, die Benchmark-Werte aus dem Sicherheitsplan von Railtrack (1997/98) als feste Zielvorgaben. Darin heißt es wie folgt:

„Bis zum Jahr 2000 werden angemessene durchführbare Programme realisiert, deren Ziel es ist, sicherzustellen, dass das Risiko eines Todesfalls für die einzelnen Insassen eines Straßenfahrzeugs nicht größer ist als ein Todesfall pro 100.000 normale Benutzer pro Jahr."

Um die „allgemein akzeptierbare Grenze" nach ALARP zu definieren, bei deren Erreichen keine Kosten-Nutzen-Analysen durchgeführt werden müssen, wird ein zusätzlicher Sicherheitsfaktor von 10 berücksichtigt. Das heißt, dass das aus $IRF_i < 10^{-5}$ Todesfälle/(Person x Jahr) abgeleitete individuelle Risiko für einen normalen Benutzer kleiner als 10^{-6} pro Jahr sein sollte, das als Zielwert des individuellen Risikos (TIR) festgesetzt wird.

Interessanterweise wurde mittlerweile dieser spezifische Risikogrenzwert für Insassen von Straßenfahrzeugen durch wesentlich globalere Risikovorgaben ersetzt.

4.5.4.2 Ermittlung des individuellen Risikos

Das individuelle Risiko wird anhand der Formel (4-1) berechnet. Für unser Beispiel betrachten wir ein bestimmtes Individuum, nämlich einen Pendler, der den Bahnübergang regelmäßig benutzt, sagen wir N_i = 1.000 Mal pro Jahr. Andere Benutzer, wie etwa Fußgänger oder Radfahrer, finden hier keine Berücksichtigung.

Wir gehen davon aus, dass wir aus betrieblicher Erfahrung wissen, dass die Gefährdung H_1, wenn sie eintritt, länger dauert als die Zeit, die das Individuum dem System ausgesetzt ist, d. h., die Zeit, die zum Überqueren des Bahnübergangs nötig ist. Das bedeutet, dass wir die Zeit E_{i1}, die das Individuum in der Formel (4-1) dem System ausgesetzt ist, außer Acht lassen können. Als pessimistische Schätzung setzen wir eine Gefährdungsdauer von D_1=10 Stunden an, während der ein gefährlicher Ausfall (wrong-side failure) der BÜSA besteht (bis er in einen sicheren Zustand überführt oder repariert ist).

4.5.4.3 Ermittlung der tolerierbaren Gefährdungsrate

Nun können wir die tolerierbare Gefährdungsrate THR_1 für die Gefährdung H_1 aus den Eingabeparametern anhand der Formel (4-1) berechnen:

$$IRF_i = N_1 \times HR_1 \times (D_1 + E_{i1}) \sum_{\text{Unfälle } A_k} C_{1k} \times F_{ik} \qquad (4\text{-}1)$$

$$= 1000 \times HR_1 \times 10 \times (0.007 \times 0.2 + 0.003 \times 0.05)$$

$$\leq TIR = 10^{-6}$$

Obige Berechnung ergibt $HR_1 \approx 7 \times 10^{-8}\ h^{-1}$, nun als THR_1 bezeichnet. Dies entspricht ungefähr einer tolerierbaren Gefährdung pro Bahnübergang in 1.600 Jahren und wäre nun die Zielvorgabe für die sich anschließende Gefährdungsanalyse im Rahmen einer Systementwicklung.

5 Vergleich mit alternativen Ansätzen

In diesem Kapitel wird der in der EN 50129 definierte Prozess sowie der in Formel (4-1) zusammengefasste Ansatz zur Risikobewertung (der nicht in der EN 50129 enthalten ist) mit anderen Ansätzen – überwiegend aus anderen Normen – verglichen.

5.1 Target Failure Measure in der IEC 61508

In der IEC 61508 wird ein SIL mit einem quantitativen Sicherheitsziel, dem „Target Failure Measure for a safety function (Probability of a dangerous failure per hour)“ (TFM) gleichgesetzt. Dabei umfasst das TFM sowohl systematische wie zufällige Ursachen für Funktionsversagen, wobei nur die Letzteren quantifiziert nachgewiesen werden (identisch zum THR-Konzept in der EN 50129). Nach Erfüllen der qualitativen Maßnahmen für den SIL sowie quantitativen Anforderungen darf behauptet werden (claim), dass die Sicherheitsfunktion das quantitative Zielmaß bezüglich aller Ursachen erfüllt (es wird angenommen, dass nach Erfüllung aller Maßnahmen für einen SIL der Einfluss systematischer Fehler vernachlässigbar klein ist). Dabei werden allerdings die quantitativen Betrachtungen unter konservativen Randbedingungen durchgeführt.

Sicherheitsanforderungen werden in der IEC 61508 für Sicherheitsfunktionen definiert. In der EN 50129 darf man dagegen Anforderungen zur Beherrschung von Gefährdungen allgemeiner auf jeder Systemebene definieren. Gefährdungen werden in der EN 50129 durch eine oder mehrere Sicherheitsfunktionen vermieden oder beherrscht, während in der IEC 61508 in der Regel eine Gefährdung dem Versagen einer Sicherheitsfunktion gleichgesetzt wird. Das *Bild 17* verdeutlicht den Zusammenhang und den Unterschied zwischen IEC 61508 und EN 50129.

Auch die SIL-Tabellen in der IEC 61508 und der EN 50129 stimmen überein, wobei sich die EN 50129 allerdings aus Gründen der Vereinheitlichung auf den so genannten Continuous Mode nach IEC 61508 beschränkt, der Zielvorgaben in Form von Ereignishäufigkeiten statt Ereignis-

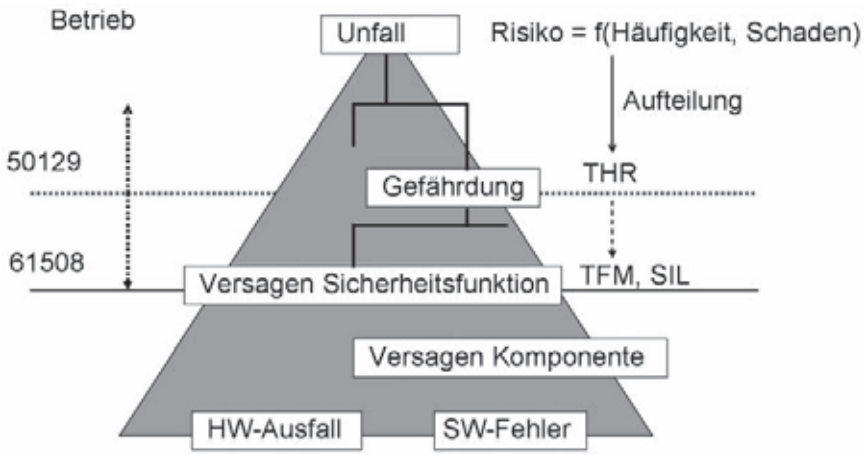

Bild 17: Zusammenhang zwischen TFM und THR

(Kabelabschlussgestell), die Datenverbindungen nach außen und den Übergang zu Systemen mit anderen Aufgabenbereichen (zum Beispiel Achszählrechner) abgegrenzt. Außerdem wurde der Signalschaltkasten beim ESTW als architekturabhängige Komponente der Außenanlage als Teil der Stellwerksinnenanlage angesehen.

Logisch erfolgte die Abgrenzung der Stellwerksinnenanlage durch die Festlegung, dass außerhalb der Stellwerksinnenanlage keine Informationsverarbeitung zur Sicherung des vorgegebenen Bereichs entsprechend der Stell- und Sicherungslogik stattfindet.

Die zentrale Aufgabe der Stellwerksinnenanlage besteht in der Steuerung und Sicherung der Fahrwege. Die Steuerung und Sicherung erfolgt durch die Einstellung der Fahrstraße und die Signalstellung entsprechend dem Regelwerk der DB AG zur Abwicklung des Bahnbetriebs. Dabei gibt es zwei Aufgabenbereiche, die jeweils durch das Bedien- und Anzeigesystem und das Stell- und Sicherungssystem übernommen werden.

Die Eingaben zur Steuerung der Fahrwege und die Rückmeldungen des Stell- und Sicherungssystems erfolgen über das lokal installierte Bedien- und Anzeigesystem. Das Bedien- und Anzeigesystem verarbeitet Bedienhandlungen zu elektronischen Kommandos und überträgt diese an das Stell- und Sicherungssystem. Die Meldungen des Stell- und Sicherungssystems werden durch das Bedien- und Anzeigesystem in geeigneter Weise dem Fahrdienstleiter angezeigt. Die Zugnummernmeldung und -weitergabe sowie die Zuglenkung gehören ebenfalls zu den Funktionen des lokalen Bedien- und Anzeigesystems.

Das Stell- und Sicherungssystem verarbeitet die Bedienungen des Fahrdienstleiters oder der Zuglenkung in Abhängigkeit vom Zustand der Stellwerksaußenanlage sowie der Funktions- und Sicherungslogik und erteilt die resultierenden Aufträge an die Stellwerksaußenanlage. Durch die Überwachung der Stellwerksaußenanlage hat das Stell- und Sicherungssystem ein korrektes

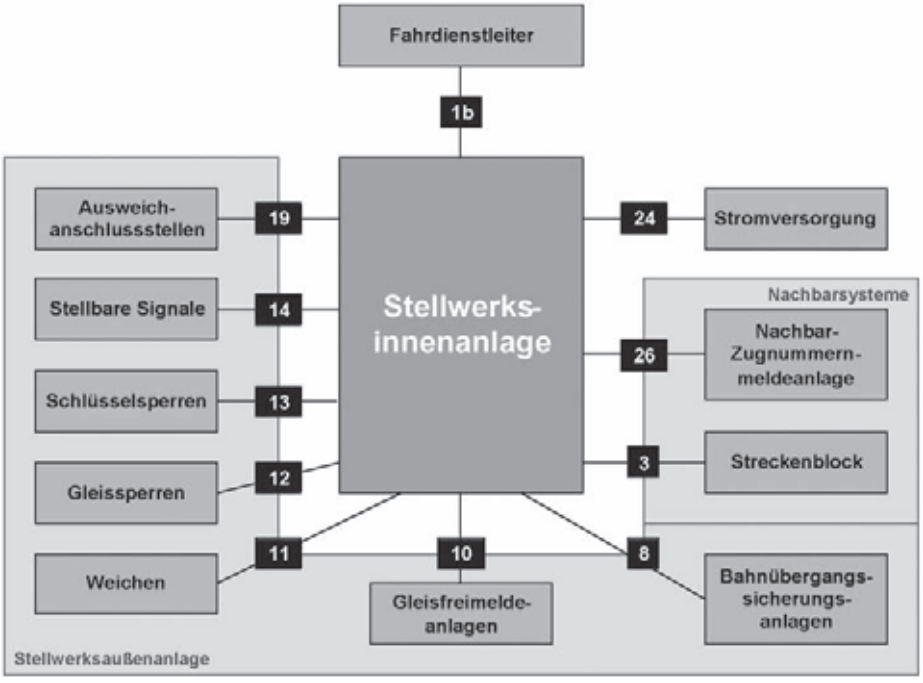

Bild 40: Schnittstellen der Stellwerksinnenanlage

Abbild der Situation innerhalb des Stell- und Überwachungsbereichs des Stellwerks. Dieses Abbild wird über das Bedien- und Anzeigesystem an den Fahrdienstleiter weitergegeben.

Die Schnittstellen der Stellwerksinnenanlage lassen sich aufteilen in Schnittstellen zur Außenanlage, zu Nachbarsystemen und zur Bedienebene. Die Schnittstellen zur Ansteuerung und Überwachung der Außenanlage sind durch die bestehenden Spezifikationen für die jeweiligen Außenelemente definiert. Die Schnittstellen zu Nachbarsystemen dienen der Informationsweitergabe, sodass die Fahrwege über Bereichsgrenzen hinaus gesichert werden können. Durch die Realisierung von Blocksystemen sind die Schnittstellen ausreichend definiert. Schließlich sind die Schnittstellen zur Bedienebene durch die Lastenhefte der DB AG vorgegeben. Das *Bild 40* zeigt die detaillierte Darstellung der Schnittstellen.

6.3.3 Gefährdungsidentifikation

Als Methode für die Phase 1 wurde eine Schnittstellenanalyse im Stil einer FMEA in Verbindung mit der Definition generischer Gefährdungen gewählt. Die Stellwerksinnenanlage kann sich nur durch die falsche Ansteuerung der Außenanlage, die falsche Weitergabe von Informationen oder eine falsche Abbildung des Anlagenzustands gefährlich auf den Bahnbetrieb auswirken. Alle funktionalen Interaktionen finden über eine der in der Systemdefinition genannten Schnittstellen statt. Deshalb wurde eine Schnittstellenanalyse durchgeführt, bei der für jede Schnittstelle aus der Systemdefinition die auftretenden Gefährdungen ermittelt werden.

Die Ableitung und Aufzählung der konkreten Gefährdungen orientierte sich dabei an den Schnittstellen der Stellwerksinnenanlage in der Systemdefinition. Die Randbedingungen für die Gefährdungsidentifikation waren

– die Unabhängigkeit von Architektur und Konfiguration,
– die Vermeidung einer betrieblichen Analyse und
– die Beschränkung auf Gefährdungen mit technischen Ursachen.

Als zu betrachtende Ebene wurde die technische Ebene der Stellwerksinnenanlage gewählt. Da betriebliche Einflüsse zur Risikoreduktion nicht betrachtet wurden, wurde auf eine differenzierte Untersuchung aller möglichen Funktionen des jeweils an der Schnittstelle angeschlossenen Außenelements verzichtet. Damit ergaben sich generische Gefährdungen für alle Schnittstellen, die allein auf der Funktion der Ein- und Ausgabe der jeweiligen Schnittstelle beruhten. Die Stellwerksinnenanlage konnte demnach als abstraktes informationsverarbeitendes System angesehen werden.

Das *Bild 41* zeigt das Modell der Verarbeitung von Ein- und Ausgaben in der Stellwerksinnenanlage. Dabei wird davon ausgegangen, dass ein logisches Abbild des Stellwerks existiert. Auf der Basis dieses logischen Abbilds werden die Ausgaben ermittelt und an die jeweiligen Schnittstellen weitergegeben. Die Eingaben an die Stellwerksinnenanlage werden erfasst, weitergeleitet und ebenfalls verarbeitet, sodass der logische Zustand des Stellwerks an den realen Zustand der Stellwerksaußenanlage und der Nachbarsysteme angepasst wird. Die Verarbeitung und Weitergabe der Ein- und Ausgaben wird entsprechend der in den Lastenheften vorgegebenen Stellwerksfunktionen durchgeführt.

Die Gefährdung in Ausgaberichtung durch die falsche Verarbeitung oder Weitergabe von Kommandos an die Stellwerksaußenanlage oder von Informationen an Nachbarsysteme ist sofort einsichtig, da unmittelbar eine gefährliche Auswirkung auf den Bahnbetrieb erfolgt.

Die Verfälschung von Eingaben in die Stellwerksinnenanlage wird als Gefährdung angesehen, da einerseits die Rückmeldungen auf Ausgaben sicherheitsrelevant sind und andererseits eine

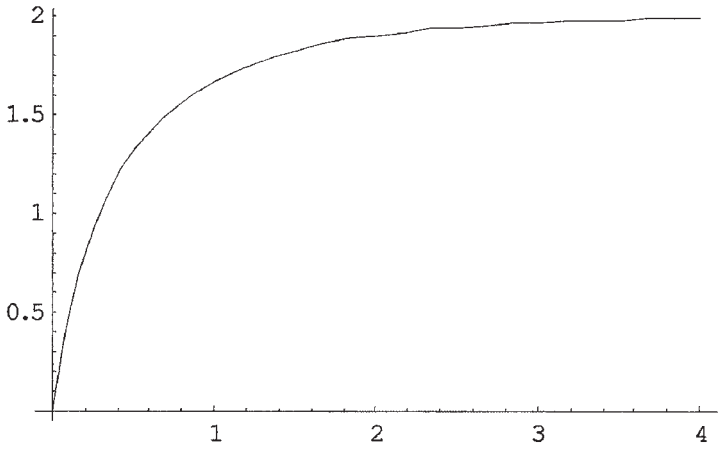

Bild 8: Ausfallrate für 2-von-3-System

Wichtig ist die Beobachtung, dass sich die Ausfallraten in der Zuverlässigkeitsanalyse von den Gefährdungsraten in der Sicherheitsanalyse nur dadurch unterscheiden, dass bei Sicherheitsanalysen nur bestimmte - nämlich gefährliche oder unentdeckte - Ausfälle betrachtet werden. Die mathematischen Grundlagen und Eigenschaften sind identisch.

Zum Abschluss sei noch bemerkt, dass Lebensdauern von verschleißbehafteten (z.B. mechanischen) Bauteilen mit der Weibull-Verteilung modelliert werden können. Die Weibull-Verteilung ist eine Verallgemeinerung der Exponentialverteilung mit weiteren Formparametern, die es auch erlauben, steigende oder fallende Ausfallraten zu modellieren. Für weitere Details siehe [107].

9 Anwendung: Fehlerbaumanalyse

Das Ziel der Fehlerbaumanalyse (FTA) besteht in der systematischen Erfassung möglicher Ursachen eines bestimmten unerwünschten Ereignisses (TOP-Ereignis). Der Fehlerbaum ist ein logisches Diagramm von Ereigniskombinationen, die zum TOP-Ereignis führen.

Die Analyse erfolgt Top-Down (im Gegensatz zur Ereignisbaumanalyse), rückwärts (auch zeitlich gesehen) vom TOP-Ereignis zu den Ursachen. Jedes Ereignis im Baum, für das keine weiteren Ursachen ermittelt werden (können), stellt ein „Basisereignis“ dar.

Die Verknüpfungen der Ereignisse erfolgen in Bool'scher Logik (im Wesentlichen durch logische UND- und ODER-Verknüpfungen).

Die Symbole für FTA sind leider nicht standardisiert, aber in den angelsächsischen Tools sind die in *Bild 9* abgebildeten Symbole am gebräuchlichsten (alternative Symbole sind z.B. in

Bild 9: Wichtige Fehlerbaum-Symbole

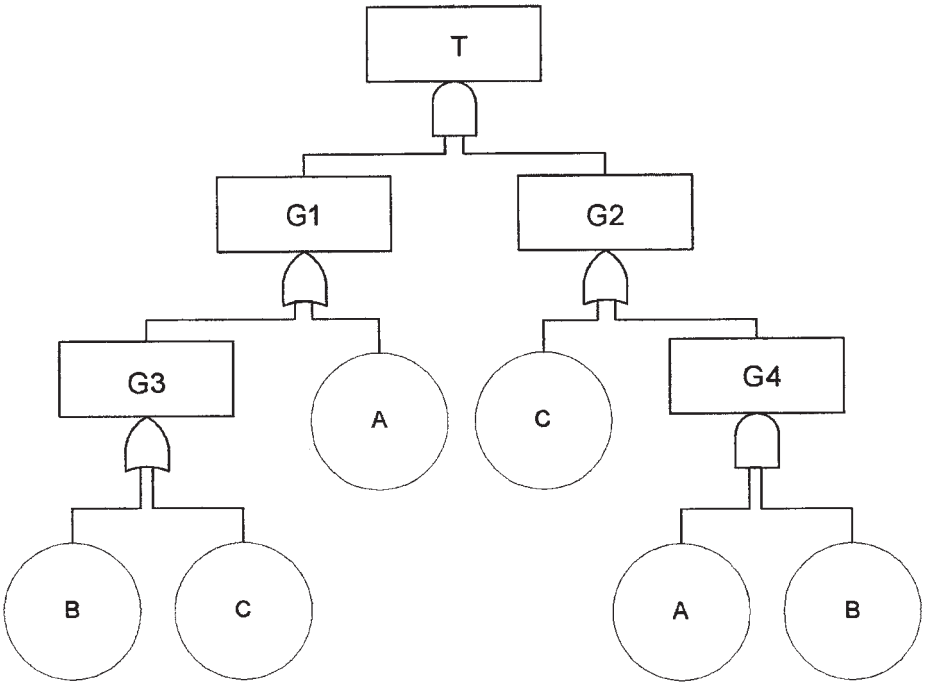

Bild 10: Beispiel Fehlerbaum

Bild 35 gezeigt). Ereignisse werden durch Rechtecke, Basisereignisse durch Kreise gekennzeichnet.

Das *Bild 10* zeigt einen Fehlerbaum, bei dem zunächst die inhaltliche Bedeutung der Ereignisse unbedeutend ist. Ziel ist die Bestimmung der Wahrscheinlichkeit des TOP-Ereignisses T. Dazu kann man sich auch intuitiv eingängiger Rechenregeln bedienen, die man erhält, wenn man in den logischen Gleichungen das ODER durch + sowie das UND durch * ersetzt:

- Distributivgesetz: (A + B) * (C + D) = A*C + A*D + B*C + B*D ,
- Idempotenzgesetze: A + A = A A * A = A ,
- Absorption: A + A * B = A .

Im Beispiel bedeutet dies

T = (B + C + A) * (C + A * B)
= B * C + B * A * B + C * C + C * A * B + A * C + A * A * B
= B * C + A * B + C + C * A * B + A * C + A * B
= A * B + C .

Im Vergleich erkennt man die wesentliche Vereinfachung des logischen Ausdrucks, die man auch wieder als Baum darstellen kann *(Bild 11)*. An diesem Beispiel kann man auch erkennen, dass man mittels der genannten Rechenregeln einen Fehlerbaum immer in eine Form bringen kann, die logisch aus einer Summe von Produkten besteht:

$$\text{TOP} = \sum_{i=1}^{n} C_i, \text{ mit } C_i = \prod_{j=1}^{n_i} C_j^i .$$

Prof. Dr. Jens Braband ist Diplom-Mathematiker und promovierte 1992 an der Technischen Universität Braunschweig im Bereich Stochastische Modellierung. Seit 1993 ist er bei Siemens AG Transportation Systems, Geschäftsgebiet Rail Automation, als Sicherheitsexperte beschäftigt. In dieser Funktion hat er an zahlreichen Projekten mit grundlegenden Themen, wie z. B. sicherheitsrelevante Kommunikation, Risikoanalyse, Ursachenanalyse oder Sicherheitskultur, sowie deren praktischer Anwendung mitgearbeitet. Seit 2003 verantwortet er als Executive Expert das Thema RAMSS.

Seit 2000 lehrt er am Institut für Eisenbahnwesen und Verkehrssicherung (IfEV) der TU Braunschweig und wurde 2004 zum Honorarprofessor für „Risiko- und Sicherheitsanalyse von Verkehrssystemen" bestellt.

In diesem Buch wird der aktuelle Stand der Technik bei Risikoanalysen in der Eisenbahn-Automatisierungstechnik umfassend dargestellt. Insbesondere der normative Hintergrund sowie Erfahrungen mit konkreten Anwendungen werden diskutiert. Diese Überlegungen bzw. Erfahrungen münden in einen Vorschlag für eine neue, effiziente Vorgehensweise

Eurail press