Menschliche Fehler in der Fehlerbaumanalyse

Paweł Buczek

Die Familie der CENELEC-Normen sieht eine enge Zusammenarbeit zwischen dem Betreiber und dem Hersteller des Signalsystems vor. Um die Sicherheitsanforderungen an das technische System ermitteln zu können, müssen die betrieblichen Abläufe und damit verbundenen Gefährdungen analysiert werden. Sehr oft wird dazu eine Fehlerbaumanalyse erstellt, um die Gefährdungsrate für jede Sicherheitsfunktion zu ermitteln. Ihr zulässiger Höchstwert, die tolerable hazard rate, wird dem Hersteller vom Betreiber vorgegeben und stellt bezüglich der Sicherheit die typische Schnittstelle zwischen beiden dar. Daher muss er unmissverständlich definiert und bestimmt werden.

1 Einführung

Der Mensch ist ein wesentlicher Teil des Systems Eisenbahn. Seine Handlung ist oft der letzte Rettungsanker im Falle einer technischen Störung. Ebenso können menschliche Fehler zu Beeinträchtigung der Sicherheit führen. Im Gegensatz zu dem Fall technischer Einrichtungen sind menschliche Fehler normalerweise nicht durch eine Rate gegeben, sondern durch die Wahrscheinlichkeit einer Fehlhandlung.

Der Einbezug der menschlichen Fehler in eine Fehlerbaumanalyse (FTA) beinhaltet demzufolge mehrere formale Probleme, die richtig beherrscht werden müssen. In diesem Artikel werden am Beispiel einer konkreten Systemfunktion, des Einrichtens der Langsamfahrstelle (Lfst) in einem Radio Block Center (RBC), die Schwierigkeiten in der Quantifizierung der Fehlerbäume in der betrieblichen Gefährdungsanalyse erläutert.

Unser heutiger Wissensstand erlaubt es nicht, ein Bahnsystem auf quantitative Weise vollständig zu beschreiben. Aufgrund der Komplexität solcher Systeme muss jede quantitative Beschreibung statistischen Charakters sein und könnte daher beträchtliche systematische Gefährdungen außer Acht lassen [1]. Dennoch eignet sich das quantitative statische Verfahren ausgezeichnet, um mit den zufälligen Fehlern von technischen Systemen und von betrieblichen Abläufen umzugehen. Weiterhin definiert die quantitative Vorgehensweise eine natürliche Schnittstelle zwischen dem Betreiber der Bahninfrastruktur und dem Hersteller des technischen Systems (Sanduhr-Modell), die mittels der zulässigen Gefährdungsrate bestimmt, welche Risiken – bezogen auf den Bahnbetrieb – toleriert werden dürfen. Dies erfolgt im Rahmen der so genannten betrieblichen Gefährdungsanalyse (BGA).

Im diesem Artikel konzentrieren wir uns auf die niederste Stufe der betrieblichen Gefährdungsanalyse und analysieren ein idealisiertes Beispiel einer Systemfunktion „Langsamfahrstelle einrichten“. Die Funktion basiert auf einem betrieblichen Ablauf, der sowohl die technischen Komponenten als auch Menschen einbezieht. Es wird analysiert, wie man die menschlichen Fehler auf Augenhöhe mit den technischen Ausfällen in einer Fehlerbaumanalyse quantitativ erfassen kann und welche konzeptionellen Schwierigkeiten dabei zu erwarten sind. Weiterhin werden die Ergebnisse der Analyse in den Kontext der systemischen betrieblichen Gefährdungsanalyse eingeordnet. Dabei nehmen wir an, dass die betriebliche Gefährdungsanalyse auf quantitativem Prinzip, wie z. B. der minimalen endogenen Mortalität (MEM) [2], als Risikoakzepttanzkriterium basiert.

2 Der Kontext der betrieblichen Gefährdungsanalyse

Eine vollständige Beschreibung der betrieblichen Gefährdungsanalyse sprengt den Rahmen dieses Beitrags. Trotzdem ist es notwendig, unsere spätere Analyse in den Kontext der betrieblichen Gefährdungsanalyse einordnen zu können. Im Folgenden konzentrieren wir uns auf den Fall der Fahrgäste, die täglich die Bahn als Verkehrsmittel nutzen. Dabei werden wichtige Fragen, wie die Sicherheit des Personals oder der weiteren Personen, die nicht direkt in dem Zugverkehr involviert sind, außer Acht gelassen. Falls notwendig kann unsere Methodologie erweitert werden, um sie ebenfalls zu erfassen.

Die systemische Top-Gefährdung sind alle Ereignisse, die zum Tod oder zu einer schweren Körperverletzung einer Person führen können. Dabei muss die betriebliche Gefährdungsanalyse drei Aspekte betrachten:

- Es müssen Kriterien definiert werden, die erlauben, die Beförderung der Fahrgäste als sicher einzustufen. Ein solches Kriterium kann als die tolerierte Anzahl der gefährlichen Ereignisse pro eine Stunde Zugfahrt definiert werden und wird mit λ_s bezeichnet. Eine Schätzung der Größe wird unten gegeben.
- Da die systemische Top-Gefährdung eine Konsequenz des Versagens einer der unterliegenden sicherheitsrelevanten Systemfunktionen ist, muss die betriebliche Gefährdungsanalyse im zweiten Schritt die Top-tolerable hazard rate λ_s auf die tolerable hazard rate (THR) der einzelnen Funktionen herunterbrechen. Beispiele solcher Systemfunktionen sind die Zugbremsung, die Signalgebung, die richtige Lage der Weiche und das Einrichten der Langsamfahrstelle.
- Letztendlich untersucht die betriebliche Gefährdungsanalyse, ob die vorhandenen betrieblichen Abläufe und der Stand der Technik überhaupt genügen können, um das oben ermittelte Sicherheitsniveau zu erreichen. Der Betreiber geht denn normalerweise davon aus, dass die Entwicklung neuer technischer Lösungen oder die Änderung der bestehenden Abläufe mit hohen Kosten verbunden sein kann. Falls die Anforderungen auf vernünftige Weise realisierbar sind, kann die THR für einzelne technische Komponenten am Ende der Phase ermittelt werden. In dem Artikel wird ein repräsentatives Beispiel einer solchen Analyse gegeben.

Aus der Sicht der quantitativen betrieblichen Gefährdungsanalyse lassen sich

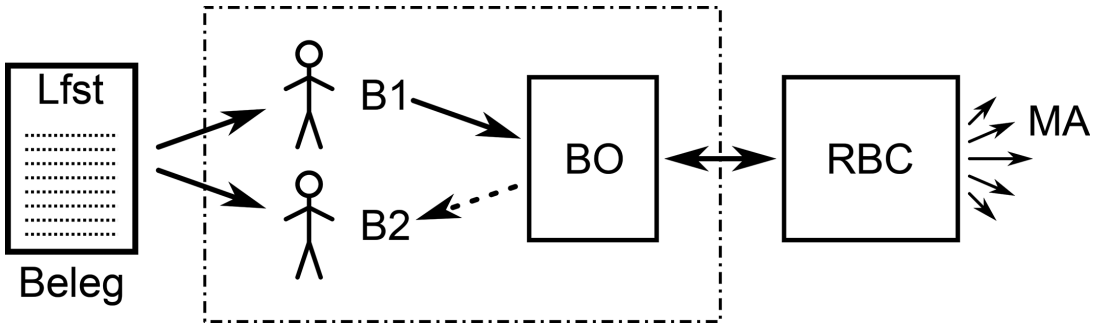

Bild 1: Betrieblicher Ablauf bei der Funktion „Langsamfahrstelle einrichten“. Die Grenze des betrachteten Systems ist mit der punktierten Linie gekennzeichnet.

drei Typen des Versagens von Systemfunktionen definieren:

- Die gefährlichen Ausfälle der fahrzeugseitigen Ausrüstung, z. B. das Versagen der Bremse oder eine gefährliche Falschauswertung der Movement Authority (MA), sind mit Ausfallraten verbunden, die direkt zu der systemischen Top-Gefährdungsrate λ_s additiv beitragen.
- Die streckenseitigen Sicherheitsfunktionen, wie z. B. die falsche Lage einer Weiche. Bei ihrer Quantifizierung muss die mittlere Geschwindigkeit v des Zuges berücksichtigt werden. In diesem Fall ergibt sich der Beitrag zur Top-Gefährdungsrate $p \cdot \mu \cdot v$, wobei p die Wahrscheinlichkeit ist, dass eine Weiche in einer bestimmten Fahrstraße nicht in der richtigen Lage verschlossen wurde, μ ist die mittlere Zahl der Weichen pro Streckenkilometer, die der Zug auf seinem Weg befährt.
- Andere Fälle, z. B. die Ausfälle anderer Fahrzeuge, die zu einem Zusammenstoß führen könnten. Diese Kategorie ist besonders schwierig zu analysieren, denn es muss hierfür auch die Verkehrsdichte einbezogen werden.

Hilfreich ist es schließlich, eine realistische Abschätzung der Größe λ_s zu eruieren. Wir nehmen an, dass der durchschnittliche Fahrgast die Bahn drei Stunden am Tag nutzt. Aus dem MEM-Prinzip ergibt sich

$$3\lambda_s \cdot 365{,}25 < 10^{-5} \qquad (1)$$

d. h. $\lambda_s < 10^{-8}\ h^{-1}$, was ein Maß für das individuelle Risiko darstellt. Ein großes europäisches Bahnunternehmen rechnet im Jahr mit der Fahrgastbeförderung von etwa $80 \cdot 10^9$ Personenkilometer. Bei einer durchschnittlichen Geschwindigkeit von 80 km/h entspricht dies 10^9 Personenstunden im Jahr, was in zehn Verkehrstoten im Jahr resultieren würde. Da die Zahl aus Sicht der Gesellschaft vermutlich nicht akzeptabel ist, muss die Anforderung an λ_s weiter verschärft werden. Bezogen auf die Fahrgäste rechnet man im deutschen Bahnsystem durchschnittlich mit ca. 2,4 Todesfällen im Jahr [3]. Die Größe kann als Definition des kollektiven Risikos gesehen werden. Der resultierende THR-Wert befindet sich wie erwartet in dem SIL 4-Bereich [1].

Nun haben wir uns die richtige Perspektive verschafft, um das betriebliche Szenario „ Langsamfahrstelle einrichten“ zu analysieren.

3 Fallstudie

Im Folgenden analysieren wir als Beispiel eine untergeordnete Systemfunktion „Langsamfahrstelle einrichten“. Obwohl die unten beschriebene Prozedur stark vereinfacht ist, erhält sie alle relevanten Merkmale eines eigentlichen Ablaufs, der Menschen und Technik einbezieht. Eine Langsamfahrstelle ist nach Wikipedia [4] „ein Gleisabschnitt einer Bahnstrecke, der nicht mit der für diesen Streckenabschnitt zulässigen Höchstgeschwindigkeit befahren werden darf“. Langsamfahrstellen werden typischerweise aufgrund der Trassierungsgegebenheiten eingerichtet, z. B. wegen der Bauarbeiten oder der Verschlechterung der Fahrwegeigenschaften (Schienenbruch).

3.1 Betrieblicher Ablauf

Der Ablauf ist schematisch in Bild 1 dargestellt. Wir gehen von einer vorübergehenden Langsamfahrstelle aus, die z. B. als Schutzmaßnahmen für eine Baustelle vorgesehen ist. Die Eigenschaften der Langsamfahrstellen werden in einer Verwaltung bestimmt (Gleis, Anfang und Ende, Geschwindigkeit oder Sperre, Datum und Zeit der Gültigkeit) und in Form eines Druckbelegs an den Arbeitsplatz des Fahrdienstleiters geliefert.

Auf den mit ETCS [5] ausgerüsteten Strecken werden normalerweise im RBC Funktionen für eine solche temporäre Parametrisierung des Fahrweges vorgesehen. Die Eingabe der Parameter und die Aktivierung der Langsamfahrstelle erfolgt mittels einer computergestützten Bedienoberfläche. Das RBC speichert die Parameter der Langsamfahrstelle und erteilt entsprechend die Movement Authorities (MA).

Zwei Bediener werden in das Einrichten der Langsamfahrstelle einbezogen. Bediener 1 (B1) gibt die Daten bezüglich der Langsamfahrstelle ein und aktiviert sie. Nach dem Vier-Augen-Prinzip überprüft der Bediener 2 (B2) die richtige Wirksamkeit der Langsamfahrstelle. Wir gehen davon aus, dass ein unabhängiger, sicherer Prozess die Erstellung des Druckbelegs gewährleistet. Weiterhin wird angenommen, dass das RBC sicher

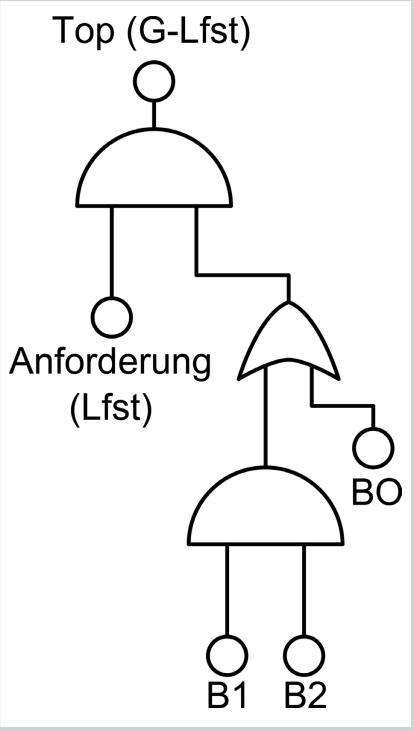

Bild 2: Fehlerbaum für die G-Lfst-Gefährdung: fehlgeschlagenes Einrichten einer Langsamfahrstelle.

arbeitet. Die zwei Bedienungen definieren die Grenze unseres Ablaufs.

Die mit der Funktion verbundene Top-Gefährdung (G-Lfst) lautet „Die notwendigen und richtigen Eingaben zur Langsamfahrstelle wurden nicht an das Radio Block Center übermittelt“. Sie kann zu katastrophalen Folgen führen und als solche trägt sie zu der systemischen Gefährdungsrate λ_s bei.

3.2 Fehlerbaumanalyse

Die Ursachen der Top-Gefährdung G-Lfst werden mittels des Fehlerbaums gemäß Bild 2 dargestellt. Die Gefährdung kann nur dann auftreten, wenn eine Langsamfahrstelle angefordert wird und daher verbindet das Top-UND-Gatter die Anforderungsrate λ der Langsamfahrstelle mit der Wahrscheinlichkeit p, dass die richtigen Eingaben an das RBC nicht übermittelt werden. Die Wahrscheinlichkeit wiederum bezieht sich auf das Versagen des Vier-Augen-Prinzips (ein UND-Gatter verbindet die Fehler der zwei Bediener B1 und B2) und des technischen Systems (Bedienoberfläche), das unabhängig die Daten auf dem Weg zum RBC verfälschen oder verlieren kann (ODER-Gatter).

Unser Ziel ist, den Baum zu quantifizieren und den Beitrag λ_{Lfst} (die Ausfallrate der Funktion) zu der systemischen Gefährdungsrate λ_s zu bestimmen.

3.3 Poisson-Verfahren mit Ausfällen

Das in der Analyse abgebildete Szenario stellt einen betrieblichen Ablauf dar, in dem die Bediener, unterstützt von einem technischen System, eine sich wiederholende Anforderung (die Einrichtung einer Langsamfahrstelle) richtig behandeln sollen. Dabei muss die Möglichkeit zugelassen werden, dass die entsprechende notwendige Bedienung jedes Mal mit einer Wahrscheinlichkeit p fehlschlägt. Dies führt zu einer Gefährdung. Unter der Annahme, dass die Anforderungen unabhängig voneinander mit einer Rate λ ankommen, lässt sich die betriebliche Situation mit einem Poisson-Prozess modellieren (Bild 3) [6].

Das Ziel der vorliegenden Analyse ist es, die mit dem Prozess verbundene Gefährdungsrate zu ermitteln. Die Wahrscheinlichkeit, dass innerhalb des Betriebsintervalls t sich genau n Anforderungen ergeben, ist nach dem Poisson-Prozess durch die folgende Formel gegeben:

$$P_n = \frac{(\lambda t)^n}{n!} e^{-\lambda t} \qquad (2)$$

Eine Bedienung gelingt mit der Wahrscheinlichkeit 1-p. Die Wahrscheinlichkeit, dass n Anforderungen richtig behandelt werden, ist mit n gelungenen unabhängigen Bedienungen verbunden und beträgt $(1-p)^n P_n$. In einem Betriebsintervall t kann sich keine oder eine beliebige Zahl der Anforderungen ergeben. Die Wahrscheinlichkeit des störungsfreien Betriebsintervalls kann als Summe der unabhängigen erfolgreichen Bedienungen dargestellt werden:

$$R(t) = \sum_{n=0}^{\infty} (1-p)^n P_n = e^{-p\lambda t} \qquad (3)$$

Aus der Gleichung (3) ergibt sich sofort, dass die Gefährdungsrate des Poisson-Prozesses mit Ausfällen durch

$$\lambda_{Lfst} = \frac{1}{R(t)} \frac{dR(t)}{dt} = p\lambda \qquad (4)$$

gegeben ist. Dies ist auch intuitiv der richtige Wert.

Im Folgenden wird gezeigt, wie die notwendigen Größen ermittelt werden können:

- die Anforderungsrate λ der Funktion (die Zahl der Langsamfahrstellen pro Stunde Zugfahrt) und
- die Wahrscheinlichkeit p, dass das Einrichten der Langsamfahrstelle nicht richtig an das RBC übermittelt wird.

3.4 Anforderungsrate

Eine falsch oder unwirksam eingerichtete Langsamfahrstelle wird durch den ersten Zug, der sie beansprucht, sehr wahrscheinlich mit katastrophalen Folgen aufgedeckt. Es muss ermittelt werden, wie viele gerade (neu) eingerichtete Langsamfahrstellen der Zug innerhalb einer Fahrtstunde antrifft. Unter der Annahme, dass die Langsamfahrstellen gleichmäßig über das Schienennetz verteilt sind und der Zug sich mit der mittleren Geschwindigkeit v bewegt, lässt sich λ auf folgende Weise berechnen:

$$\lambda = \rho \nu \Delta t \qquad (5)$$

wobei ρ die Zahl der Langsamfahrstellen pro Stunde und Streckenkilometer und Δt die mittlere Zeit zwischen zwei Durchfahrten einer Langsamfahrstelle ist. Die letzte Größe lässt sich wiederum aus der Bahnverkehrsdichte ableiten.

Es ist interessant, dass eine größere Verkehrsdichte eine kürzere Zeit Δt ergibt, was zur Verkleinerung des individuellen Risikos führt. Es bedeutet allerdings nicht ohne Weiteres, dass auch das kollektive Risiko abnimmt, da die kürzere Δt mit der Vergrößerung der Zahl von Fahrgästen in dem gesamten Bahnsystem verbunden sein kann.

3.5 Die Versagenswahrscheinlichkeit

Es bleibt noch die Wahrscheinlichkeit p des fehlgeschlagenen Einrichtens einer Langsamfahrstelle zu bestimmen. Sie setzt sich aus der Wahrscheinlichkeit des Versagens der technischen Bedienoberfläche p_{BO} und der Bedienfehler (p_1 und p_2) zusammen:

$$p = p_{BO} + p_1 p_2 - p_{BO} p_1 p_2 \qquad (6)$$

In komplizierteren Fällen ist für die entsprechenden Berechnungen das Verwenden spezieller Fehlerbaumsoftware notwendig.

Die Wahrscheinlichkeit p_{BO} ist relativ einfach aus der Ausfallrate des technischen Systems λ_{BO} zu bestimmen:

$$p_{BO} = 1 - e^{-\lambda_{BO} \tau} \qquad (7)$$

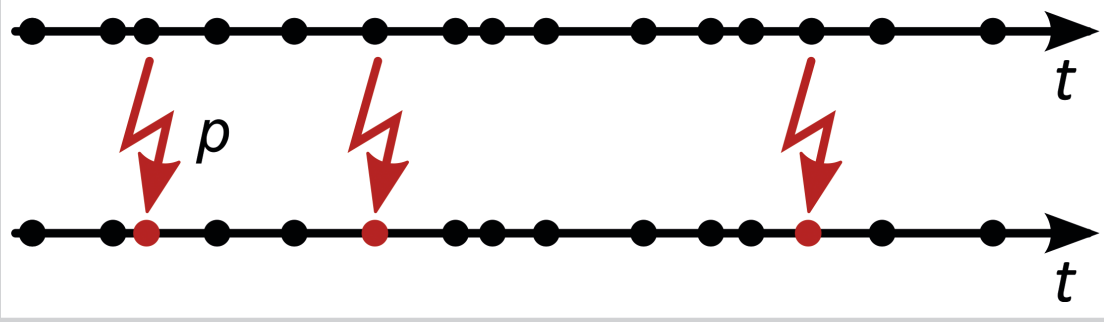

Bild 3: Poisson-Prozess mit Ausfällen. Die schwarzen Punkte stehen für eine einzurichtende Langsamfahrstelle. Das Einrichten versagt mit einer Wahrscheinlichkeit p, was zu einer Gefährdung führt.

34 Länder

1.250 Unternehmen

15.000 Triebfahrzeuge

3.000 Personen

Die Marktübersicht **Europäische Bahnen** liefert Ihnen zum Bahnmarkt in Europa einen aktuellen Überblick.

Ihre Vorteile:

- Wettbewerbsvorteil gegenüber Wettbewerbern
- noch schnellere Handhabung mit der Web App
- bessere Entscheidungsfindung durch erstklassige Brancheninformationen

Jetzt bestellen:

Telefon: 040-237 14-440 | **Fax:** 040-237 14-450 | **E-Mail:** buch@dvvmedia.com
oder per Post an: DVV Media Group GmbH, Kundenservice, 74590 Blaufelden

Preis: EUR 229,– (inkl. MwSt, zzgl. Versand) | **Sonderpreis für RBS-Abonneten:** EUR 193,90 (inkl. MwSt, zzgl. Versand)

Bestellen Sie online unter www.eurailpress.de/eb8

DVV Media Group

Eurail press

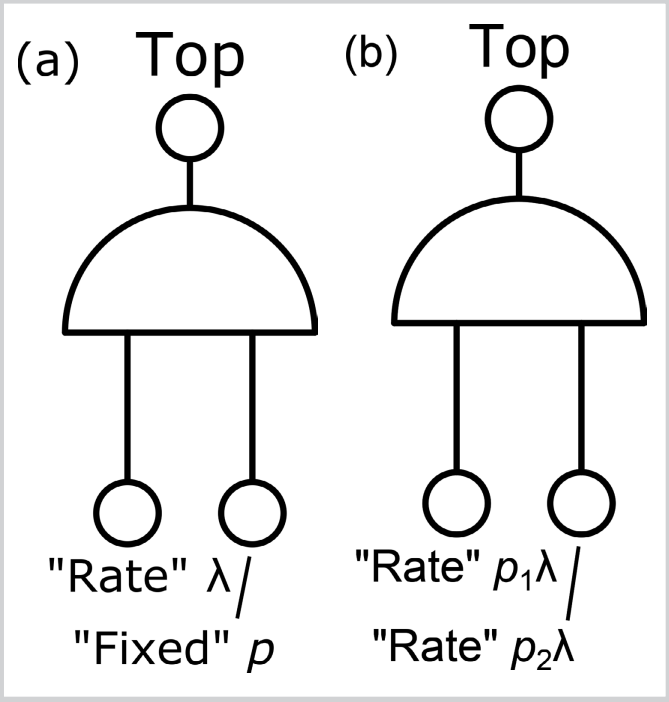

Bild 4: Fallgruben der Fehlerbaumanalyse: (a) Das Verknüpfen von Raten und Wahrscheinlichkeiten verlangt äußerste Aufmerksamkeit. (b) Bei Verknüpfen von zwei Raten muss die Abhängigkeit der Basisereignisse überprüft werden.

wobei τ die Ausfalloffenbarungszeit ist.

Die Quantifizierung der Eintrittswahrscheinlichkeit für menschliche Fehlhandlungen erfolgt auf grundsätzlich andere Weise. Im Gegenteil zu Maschinen lassen sich die Menschen nicht durch eine Ausfallrate sinnvoll charakterisieren. Wenn ein Mensch mit einer einfachen Aufgabe konfrontiert wird, erfüllt er sie mit einer bestimmten Wahrscheinlichkeit 1-p. Diese Wahrscheinlichkeit wird von der Art der Aufgabe, der Anforderungsrate, der Arbeitsbedienungen, der Tageszeit sowie dem physischen und psychischen Zustand des Bedieners etc. beeinflusst.

Im Bahnbereich gilt dafür die Studie von Hinzen als Standardreferenz [7]. Angenommen, dass an dem Arbeitsplatz günstige Umweltbedingungen herrschen und der Bediener in guter Form ist, fällt die Eingabe der Daten und die Aktivierung der Langsamfahrstellen unter die Kategorie „fertigbasierendes Verhalten". Die Entsprechende Wahrscheinlichkeit beträgt typischerweise zwischen 10^{-3} und 10^{-2}. Es ist weiterhin durchaus denkbar, dass die Versagenswahrscheinlichkeit für den zweiten Bediener aufgrund seiner Unterforderung sogar größer als für den ersten Bediener angenommen werden muss. Es soll abschließend erwähnt werden, dass eine solche Analyse nur für zufällige menschliche Fehler geeignet ist. Ausgeschlossen sind Fehler, die durch das Missachten der betrieblichen Regel oder aufgrund mangelnder Weiterbildung vorkommen.

4 Fallgruben

Typische betriebliche Abläufe bei einem Bahnunternehmen beinhalten mehrere Schritte und technische Komponenten, was zu sehr komplexen Fehlerbäumen führen kann. Die Analyse von solchen Fällen wird in der Praxis einer zweckbestimmten Software überlassen. Die Erfahrung zeigt, dass die Software für subtile systematische Fehler anfällig ist, die die Ergebnisse vollkommen verfälschen können. In dem Kontext des Artikels werden nun zwei solcher Fallgruben analysiert.

4.1 Raten und Reduktionsfaktoren

Die Top-Gefährdung verknüpft die Anforderungsrate und die Wahrscheinlichkeit der misslungenen Aktivierung. Dies führt zu der Versuchung, die zwei Basisereignisse mittels vorhandener „Prototypen" abzubilden (Bild 4a). Für die Rate wählt man den Typ „Rate" mit Parameter λ und für die Wahrscheinlichkeit den Typ „Fixed" mit dem Parameter p. Bei der Berechnung mittels typischer Fehlerbaumsoftware geht dabei die Ausfallrate des Top-Gatters mit der Zeit zu null, was dem richtigen Ergebnis $p\lambda$ widerspricht. Es ist auch intuitiv falsch, da es keinen Grund gibt, wieso die Abläufe mit der Zeit sicherer werden sollten.

Diese Tatsache ist kein Fehler der Software. Nach ihrer Spezifikation bildet sie intern aus dem Ereignis „Rate" eine Wahrscheinlichkeit $1\text{-}e^{-\lambda t}$ und verknüpft sie mit der Wahrscheinlichkeit p, sodass sich die folgende Ausfallwahrscheinlichkeit für das Top-Gatter wie folgt ergibt:

$$1-R(t) = 1-p\,(1-e^{-\lambda t}) \tag{8}$$

Für die Top-Rate gilt

$$\lambda_{TOP} = \frac{1}{R(t)}\frac{dR(t)}{dt} = \frac{p\lambda e^{-\lambda t}}{1-p\,(1-e^{-\lambda t})} \xrightarrow[t\to\infty]{} 0 \tag{9}$$

Typische FT-Software kann mit dem Poisson-Prozess nicht umgehen. Sie nimmt implizit an, dass sich in dem ganzen Betriebsintervall nur eine einzige Langsamfahrstellen-Anforderung ergibt. Man kann die Software nur zur Berechnung der Wahrscheinlichkeit verwenden.

Ähnliche Schwierigkeiten sind auch zu erwarten, wenn in der FT-Analyse neben den Ausfallraten auch Barrieren (Reduktionsfaktoren) einbezogen werden.

4.2 Zwei abhängige Raten

Wenn man die Fehler in der Bedienoberfläche außer Acht lässt, könnte man versuchen, den Ablauf mittels des Baumes in Bild 4b zu simulieren. Die Bediener führen ihre Aufgaben jeweils mit Raten $p_1\lambda$ und $p_2\lambda$ ($p_1 < p_2$) fehlerhaft. Dabei könnten (fälschlicherweise) zwei Basisereignisse des Typs „Rate" verwendet werden. Die handelsübliche Software liefert hierbei bei längeren Betriebszeiten

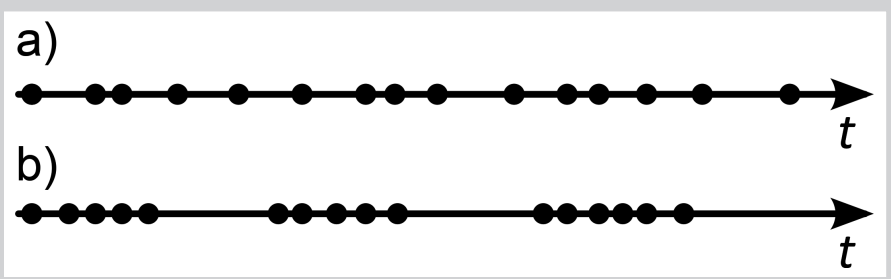

Bild 5: (a) Poissonscher und (b) nicht-Poissonscher Prozess.

$$\lambda_{TOP} \underset{1 \to \infty}{\rightarrow} p_1 \lambda \quad (10)$$

was dem richtigen Ergebnis $p_1 p_2 \lambda$ widerspricht.

Wie in dem vorhergehenden Fall ist es kein Fehler der Software. Sie nimmt stillschweigend an, dass die zwei Basisereignisse statistisch unabhängig sind, was bedeutet, dass die zwei Bediener nicht die gleiche, sondern zwei unterschiedliche Langsamfahrstellen betrachten. Es gibt keinen einfachen Weg, solche Abhängigkeiten der typischen FT-Software zu kommunizieren.

5 Zusammenfassung und Ausblick

Der Einbezug von menschlichen Fehlern in der quantitativen betrieblichen Gefährdungsanalyse führt zu mehreren methodologischen Problemen, die richtig beherrscht werden müssen. In dem Artikel wurde die komplexe Fragestellung am Beispiel der Fehlerbaummodellierung veranschaulicht. Es wurde gezeigt, wie betriebliche Abläufe, die Menschen und Maschinen einbeziehen, sich mittels der FT-Analyse abbilden lassen. Als zugrundeliegendes mathematisches Modell muss der Poisson-Prozess mit Ausfällen angewandt werden. Allerdings ist das Modell in einer typischen FT-Software nicht vorhanden und deren blinde Verwendung kann zu systematischen Fehlern führen, die die Ergebnisse unbrauchbar machen. Zwei solche Fallgruben wurden präsentiert. Sie sind subtil, trotzdem in der täglichen Praxis weit verbreitet.

Schließlich soll erwähnt werden, dass die Annahme konstanter Raten (bezogen entweder auf Ausfälle oder Anforderungen) der Erwartung entspricht, dass sie voneinander unabhängig auftreten. In Wahrheit ist zu erwarten, dass sie miteinander stark in Zeit und Raum korrelieren, insbesondere in Bereichen intensiver Bauarbeiten (Bild 5). Dies führt zu nicht-Poissonschen Prozessen, die mathematisch viel schwieriger zu beschreiben sind. Sie dürfen aber leider nicht außer Acht gelassen werden, da sie lokal zu einer erhöhten Gefährdungsrate führen können.

Einen Ausweg bietet die direkte numerische Modellierung von realen Bahnsystemen unter Einbeziehung von konkreten Streckentopologien, zeitlichen Abweichungen von der mittleren Verkehrsdichte und der Zahl der Fahrgäste etc. Das geeignete Werkzeug dafür sind die Monte-Carlo-Simulationen.

Der Autor

Dr. Paweł Buczek
RAMS Ingenieur
RAMS Competence Center
Informatik Consulting Systems AG,
Business Unit Transportation
Anschrift: Sonnenbergstr.13,
D-70184 Stuttgart
E-Mail: pawel.buczek@ics-ag.de

LITERATUR

[1] EN 50129:2003 Bahnanwendungen, Telekommunikationstechnik, Signaltechnik und Datenverarbeitungssysteme, Sicherheitsrelevante elektronische Systeme für Signaltechnik
[2] http://de.wikipedia.org/wiki/Minimale_endogene_Mortalität
[3] Vorndran, I.: Unfallstatistik – Verkehrsmittel im Risikovergleich, Wirtschaft und Statistik 12/2010
[4] http://de.wikipedia.org/wiki/Langsamfahrstelle
[5] http://de.wikipedia.org/wiki/European_Train_Control_System
[6] http://de.wikipedia.org/wiki/Poisson-Prozess
[7] Hinzen, A.: Der Einfluß des menschlichen Fehlers auf die Sicherheit der Eisenbahn (Dissertation RWTH Aachen), Juni 1993

SUMMARY

Human mistakes in the fault tree analysis

The family of CENELEC standards envisages a close cooperation between the operator and the manufacturer of a signalling system. An analysis of operational scenarios and related hazards is necessary to determine the safety requirements to be met by the technical system. The investigation resorts commonly to the fault tree analysis to determine the hazard rate associated with each of the safety functions. Humans are essential actors in any railway system. Their action is often the last resort in cases of technical malfunctions. On the other hand, their errors can compromise the system safety. Contrary to the technical components, human errors cannot be reasonably defined by means of a failure rate, but rather through the probability of the event of an error. This is why several formal problems arise in the fault tree analysis (FTA) which require a careful treatment, when human factors are introduced. Based on an idealised example of a specific safety function, the creation of a temporary speed restriction in the ETCS radio block centre, this article discusses the problems in the quantification of fault trees in the operational hazard analysis.