SCIENTIFIC PAPERS
OF THE UNIVERSITY OF PARDUBICE
Series B
The Jan Perner Transport Faculty
4 (1998)

MODELL FÜR DIE SICHERHEITSANALYSE EINES EISENBAHNSICHERUNGSSYSTEMS

Karol RÁSTOČNÝ

Katedra informačných a zabezpečovacích systémov, Elektrotechnická fakulta,
Žilinská Univerzita v Žiline

1. Einleitung

Die Sicherheitsanalyse kann man mit den quantitativen oder qualitativen Methoden, vor allem mit einer Kombination von diesen Methoden, durchführen. Quantitative und qualitative Methoden sollen sich dabei sinnvoll ergänzen.

Qualitative Methoden helfen die Auswirkungen der Ausfälle von Systemkomponenten an System und eine logische Struktur ihrer Wechselbeziehungen zu begreifen. Die Sicherheit von Eisenbahnsignalanlagen wird qualitativ als Fähigkeit des Systems begriffen, in einer Betrachtungseinheit innerhalb einer bestimmten Beanspruchungsdauer und unter bestimmten Nutzungs- und Instandhaltungsbedingungen die Auswirkungen der Ausfälle an System oder an Teile des Systems einzuschränken.

Quantitative Methoden nutzen erreichbare Angaben über Komponentenausfall, Menschenfehler u. a. für die Berechnung der Wahrscheinlichkeit eines Gefährdungszustandes aus. Die Sicherheit von Eisenbahnsignalanlagen wird quantitativ als Wahrscheinlichkeit definiert, daß in einer Betrachtungseinheit innerhalb einer bestimmten Beanspruchungsdauer und unter bestimmten Nutzungs- und Instandhaltungsbedingungen kein Gefährdungszustand auftritt.

Die klassische Methoden der Signaltechnik lehnen sich an Normen und Vorschriften an, die intuitiv aufgrund Erfahrung entstanden haben. Der Sicherheitsnachweis bei klassischen Eisenbahnsignalanlagen wird über die qualitative Analyse realisiert. Eine wichtige Voraussetzung für die Anwendung der qualitativen Analyse ist eine gute Kenntnis des

Ausfallverhaltens der verwendeten Systemkomponenten. Für die rechnergesteuerten Sicherheitssysteme ist die qualitative Analyse, als die Grundmethode des Sicherheitsnachweises, nicht denkbar. Eine Rechnertechnologie mit ihren Eigenschaften (Sicherheit, Zuverlässigkeit, ...) unterscheidet sich ausdrucksvoll von einer Relaistechnologie. Aus diesem Grund müssen auch die Regeln für die Verifikation, Validierung, Begutachtung und Autorisation der Rechnersicherheitssystemen notwendig verschieden sein. Zuvor muß man aber die Theorie, als ein Werkzeug der Analyse und Synthese für die neue technologische Stufe erbauen.

Bei der Sicherheitsanalyse von Eisenbahnsignalanlagen läßt sich eine Fehlerbaumanalyse (FTA) sehr erfolgreich anwenden.

2. Fehlerbaumanalyse

Eine Fehlerbaumanalyse ist eine deduktive Methode der Analyse, orientiert auf Ermittlung der Ursachen oder ihrer Kombination, die zum festgelegten TOP-Ereignis führen können. Ein TOP-Ereignis kann die Entstehung eines Gefährdungszustandes oder eine Unfähigkeit des Systems bestimmte Funktionen zu erfüllen, verursachen.

Eine Fehlerbaumanalyse beginnt mit der Bestimmung des TOP-Ereignisses. Das TOP-Ereignis ist der Ausgang des Gatters auf dem Gipfel, die Ausgangsereignisse der Gatter auf einer niedrigeren Stufe deuten hingegen an mögliche Ursachen, die zum TOP-Ereignis führen können. Jedes Ausgangsereignis des Gatters auf einer niedrigeren Stufe kann das Eingangsereignis des Gatters auf einer höheren Stufe sein. Die Gestaltung der bestimmten Art vom Baum geht zu Ende, wenn:
ein Grundereignis, oder

- ein Ereignis, das weiter nicht zu entwickeln ist, oder
- ein Ereignis, das weiter in anderem Fehlerbaum entwickelt wird,

erreicht wird.

Eine Fehlerbaumanalyse kann qualitativ (logisch) oder quantitativ (numerisch) sein. Eine wichtige Voraussetzung für numerische Analyse ist eine Kenntnis der Ausfallraten von Systemkomponenten.

2.1 Mathematische Grundlagen

Ein System beinhalte n Komponenten und x_i sei der Indikator des Zustandes der *i-ten* Komponente. Die binäre Zuordnung der Komponenten– und Systemzustände ist wie folgt:

$x_i = 1$, wenn die Komponente i funktionsfähig ist,

$x_i = 0$, wenn die Komponente i ausgefallen ist,

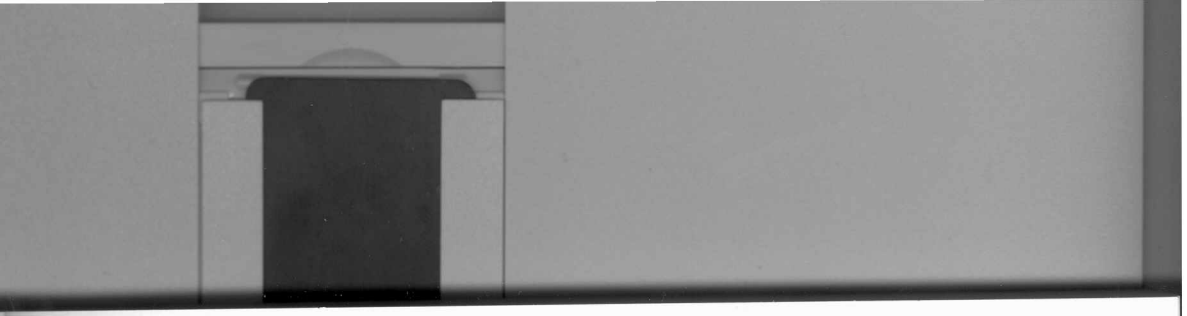
für $i = 1, 2, ..., n$ und (1)

$\varphi(\mathbf{x}) = 1$, wenn das System funktionsfähig ist,

$\varphi(\mathbf{x}) = 0$, wenn das System ausgefallen ist,

für $\mathbf{x} = (x_1, x_2, ... x_n)$.

$\varphi(\mathbf{x})$ ist Strukturfunktion des Systems, die die Beziehung zwischen den Komponenten des Systems und dem System ausdrückt. Die Strukturfunktion stellt Spezialfall einer Booleschen Funktion dar.



Die Strukturfunktion $\varphi(\mathbf{x})$ mit dem Indikatorvektor $\mathbf{x} = (x_1, x_2, ... x_n)$ und die Strukturfunktion $\varphi(\mathbf{y})$ mit dem Indikatorvektor $\mathbf{y} = (y_1, y_2, ... y_n)$ seien vorhanden. Es gelte

$$\varphi(\mathbf{x}) = \varphi(\mathbf{y}),$$

mit $x_i = y_i$ für $i = 1, 2, ..., n$.

Eine Strukturfunktion heißt monoton, falls die Bedingungen

$\varphi(\mathbf{x}) = 1$, für $\mathbf{x} = (1, 1, ...1)$,

$\varphi(\mathbf{x}) = 0$, für $\mathbf{x} = (0, 0, ... 0)$,

$\varphi(\mathbf{x}) \geq \varphi(\mathbf{y})$, für alle $x_i \geq y_i$

erfüllt sind.

Wenn $\varphi(\mathbf{x}) = 1$ für $\mathbf{x} = (1, 1, ...1)$ heißt das, daß ein System, bei dem alle Komponenten funktionsfähig sind, auch funktionsfähig ist.

Wenn $\varphi(\mathbf{x}) = 0$ für $\mathbf{x} = (0, 0, ... 0)$ heißt das daß ein System, bei dem alle Komponenten ausgefallen sind, auch ausgefallen ist.

Wenn $\varphi(\mathbf{x}) \geq \varphi(\mathbf{y})$ für alle $x_i \geq y$ heißt das, daß eine Strukturfunktion mit dem Hinzufügen der Komponenten steigt oder wenigstens sinkt.

Durch die Monotonie-Eigenschaft wird die Darstellung der Strukturfunktion bekanntlich stark vereinfacht.

Eine Struktur kann einfach oder kompliziert sein. Die einfache Struktur läßt sich in eine Seriell- und Parallelanordnung der Komponenten umändern.

Für die Seriellanordnung der Komponenten gilt

$$\varphi(x) = \prod_{i=1}^{n} x_i \qquad (2)$$

und für die Parallelanordnung der Komponenten gilt

$$\varphi(x) = \coprod_{i=1}^{n} x_i = 1 - \prod_{i=1}^{n} (1 - x_i)\,. \qquad (3)$$

Jede monotone Strukturfunktion läßt sich durch Minimalwege oder Minimalschnitte darstellen.

$$\varphi(\mathbf{x}) = \coprod_{j=1}^{m} C_j(\mathbf{x}) = 1 - \prod_{j=1}^{m} \left[1 - C_j(\mathbf{x})\right], \qquad (4)$$

wo $C_j(\mathbf{x})$ die Strukturfunktion vom *j-ten* Minimalweg ist, die durch solche Indikatoren des Vektors **x** gebildet wird, daß wenn alle diesen Indikatoren entsprechenden Komponenten funktionsfähig sind, ist auch die Struktur funktionsfähig.

$$\varphi(\mathbf{x}) = \prod_{j=1}^{m} R_j(\mathbf{x})\,, \qquad (5)$$

wo $R_j(\mathbf{x})$ die Strukturfunktion vom *j-ten* Minimalschnitt ist, die durch solche Indikatoren des Vektors **x** gebildet wird, daß wenn alle diesen Indikatoren entsprechenden Komponenten ausgefallen sind, ist auch die Struktur ausgefallen.

Die Strukturfunktion $\varphi(\mathbf{x})$ mit dem Indikatorvektor der Komponentenzustände $\mathbf{x} = (x_1, x_2, \ldots x_n)$ und die Strukturfunktion $\varphi(\mathbf{y})$ mit dem Indikatorvektor der Komponentenzustände $\mathbf{y} = (y_1, y_2, \ldots y_n)$ seien vorhanden. Es sei $y_i = (1 - x_i)$ für $i = 1, 2, \ldots, n$. Wenn

$$\varphi(\mathbf{y}) = 1 - \varphi(\mathbf{x}),$$

sind die Strukturfunktion $\varphi(\mathbf{x})$ und die Strukturfunktion $\varphi(\mathbf{y})$ einander dual.

Die Eigenschaft der Dualität der Strukturfunktionen läßt sich bei der Beschreibung des Fehlerbaumes durch eine logische Funktion ausnutzen.

Ein Fehlerbaum beinhalte n Grundereignisse (Eingangsereignisse) und u_i sei der Indikator des Zustandes vom *i-ten* Grundereignis. Die binäre Zuordnung der Zustände der Grundereignisse und des TOP-Ereignisses sei

$u_i = 1$, wenn das Grundereignis *i* eingetreten ist,

$u_i = 0$, wenn das Grundereignis *i* nicht eingetreten ist,

für $i = 1, 2, \ldots, n$ und (6)

$\Psi(\mathbf{u}) = 1$, wenn das TOP-Ereignis eingetreten ist,

$\Psi(\mathbf{u}) = 0$, wenn das TOP-Ereignis nicht eingetreten ist,

für $\mathbf{u} = (u_1, u_2, \ldots u_n)$.

$\Psi(\mathbf{u})$ ist die logische Funktion von den Fehlerzuständen, die die Beziehung zwischen den Grundereignissen des Fehlerbaumes und dem Fehlerbaum ausdrückt. Diese logische Funktion stellt auch Spezialfall einer Booleschen Funktion dar.

Dann

$$\psi(\mathbf{u}) = \coprod_{j=1}^{m} R_j(\mathbf{u}), \tag{7}$$

wo $R_j(\mathbf{u})$ die logische Funktion vom *j-ten* Minimalschnitt ist, die durch solche Indikatoren des Vektors **u** gebildet wird, daß wenn alle diesen Indikatoren entsprechenden Grundereignisse eintreten, dann wird auch das TOP-Ereignis eintreten.

$$\psi(\mathbf{u}) = \prod_{j=1}^{m} C_j(\mathbf{u}), \tag{8}$$

Wo $C_j(\mathbf{u})$ die logische Funktion vom *j-ten* Minimalweg ist, die durch solche Indikatoren des Vektors **u** gebildet wird, daß wenn alle diesen Indikatoren entsprechenden Grundereignisse nicht eintreten, dann wird auch das TOP-Ereignis nicht eintreten.

2.2 Die Wahrscheinlichkeit des TOP-Ereignisses

Die Grundereignisse seien statistisch unabhängig und die Wahrscheinlichkeiten der einzelnen Grundereignisse seien bekannt. Die Wahrscheinlichkeit, daß das TOP-Ereignis durch den Minimalschnitt R_j eingetreten ist, ist dann durch

$$P\{Rj(\mathbf{u}) = 1\} = \coprod_{i=1}^{n} p_i \tag{9}$$

gegeben.

p_i ist die Wahrscheinlichkeit, daß das *i-te* Grundereignis des Minimalschnittes eingetreten ist.

Weil jeder Minimalschnitt zum TOP-Ereignis führt, läßt sich die Wahrscheinlichkeit, daß das TOP-Ereignis eingetreten ist, aus

$$P\{\psi(\mathbf{u}) = 1\} = 1 - \prod_{j=1}^{m} \left[1 - P\{R_j(\mathbf{u}) = 1\}\right] \qquad (10)$$

berechnen.

Europäische Sicherheitstandarden [1], [2], [3], [4] setzen bei der quantitativen Analyse des Rechnersicherheitssystems mit der kompositen Sicherheit die Exponentialverteilung des Ausfallverhaltens voraus und sie definieren für jede Sicherheitsanforderungsstufe die Gefährdungsrate λ_{NM}.

Ein Nachweis, daß ein System in der Übereinstimmung mit der Sicherheitsanforderungsstufe ist, wird also unter der Voraussetzung konstanter Ausfallrate realisiert. Praktische Erfahrungen zeigen, daß die Zeitabhängigkeit der Ausfallrate für die meisten elektronischen Komponenten nicht konstant ist. Im besten Falle hat die Zeitabhängigkeit der Ausfallrate die Form einer sog. Wannenkurve. Aus Sicht der Sicherheit kann man die Brauchbarkeitsdauer des Sicherheitssystems mit der Zeit der konstanten Ausfallrate t_P gleichstellen, für die die Sicherheitsstufe über den Sicherheitsnachweis garantiert wird. Theoretisch könnte man die Brauchbarkeitsdauer des Sicherheitssystems mit der kompositen Sicherheit auf die Zeit t_{PM} (Bild 1) verlängern, weil es gilt

$$\lambda_N < \lambda_{NM},$$

wo λ_N Gefährdungsrate des Sicherheitssystems ist.

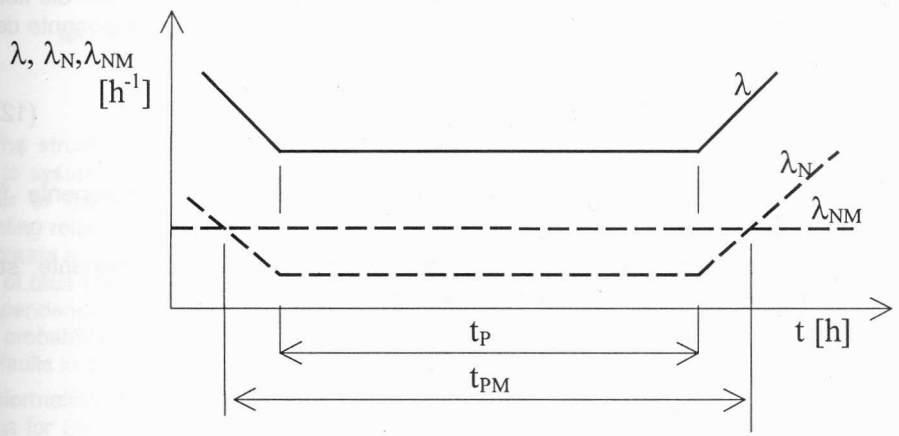


Bild 1 *Brauchbarkeitsdauer des Sicherheitssystems mit der kompositen Sicherheit*

2.3 Die Sicherheitsanalyse des Systems und die logische Funktion von den Fehlerzuständen

Die folgenden Voraussetzungen seien erfüllt:

1. Die Grundereignisse sind statistisch unabhängig.
2. Das TOP-Ereignis des Fehlerzustandsbaumes bedeutet den Gefährdungszustand des Systems und die logische Funktion, die die Beziehung zwischen den Grundereignissen des Fehlerbaumes und dem Fehlerbaum ausdrückt, hat die Form der Gleichung (7). In diesem Falle wäre es besser, für sicherheitstechnische Betrachtungen die Bezeichnungen Gefährdungsbaum anzuwenden.
3. Das *i-te* Grundereignis wird nur dann eintreten, wenn die i-te Komponente des Systems, für die der Gefährdungsbaum gebildet worden ist, ausgefallen ist.

Dann werden folgende Behauptungen gelten:

1. Wenn solche Komponente des Systems vorhanden ist, die die Nullwichtigkeit in der logischen Funktion von den Fehlerzuständen hat, dann beinhaltet keine logische Funktion vom Minimalschnitt den Indikator des Zustandes von dem mit dieser Komponente verbundenen Grundereignis und die Komponente hat keinen Einfluß auf die Sicherheit des Systems.
2. Wenn die logische Funktion vom Minimallschnitt $R_j(\mathbf{u})$ durch ein Grundereignis gebildet wird und $R_j(\mathbf{u}) = u_i$, wo $j = 1, 2, ..., m$ und $i = 1, 2, ..., n$, dann hat die *i-te* Komponente die höchste Wichtigkeit in der Systemstruktur. Es gilt

$$\psi(\mathbf{u})_{u_i=1} = 1 . \tag{11}$$

Die Komponente *i* muß über eine Selbstsicherheit disponieren, um bei dem Ausfall immer einen sicheren Zustand einzunehmen.

3. Wenn die Komponente keine Einswichtigkeit in der Struktur hat, dann kann die Sicherheit der Struktur im Hinblick auf diese Komponente über die komposite Sicherheit erreicht werden.
4. Wenn die Sicherheit des Systems im Hinblick auf die *i-te* Komponente über die komposite Sicherheit erreicht wird, dann darf die Ausfalloffenbarungszeit der *i-ten* Komponente den Wert t_{oi} nicht übersteigen. Es gilt

$$\frac{1}{t_{oi}} = \sum_{j=1}^{m} \frac{1}{t_{oij}} , \tag{12}$$

wo t_{oij} die maximal zulässige Ausfalloffenbarungszeit der *i-ten* Komponente für den Minimalschnitt R_j ist.

Die maximal zulässige Ausfalloffenbarungszeit der *i-ten* Komponente steht im indirekten Verhältnis zur Wichtigkeit der *i-ten* Komponente in der Struktur.

Lektoroval: Prof. Ing. Milan Kejzlar, CSc.
Předloženo v červenci 1998.

Literatur

[1] prEN 50 126: Railway applications: The specification and demonstration of dependability, reliability, availability, maintainability and safety (RAMS). 1995.

[2] prEN 50 128: Railway applications: Software for railway control systems and protection systems. 1995.

[3] prEN 50 129: Railway applications: Safety related electronic systems. 1996.

[4] prEN 50159 - 1: Railway applications: Communication, signalling, and processing systems - Part 1: Safety-related communication in closed transmission systems. 1996.

[5] prEN 50159 - 2: Railway applications: Communication, signalling and processing systems - Part 2: Safety - related communication in open transmission systems. 1996.

Resumé

MODEL PRE ANALÝZU BEZPEČNOSTI ŽELEZNIČNĚHO ZABEZPEČOVACIEHO SYSTÉMU

Karol RÁSTOČNÝ

Štrukturálna funkcia vyjadruje vzťahy medzi elementmi systému bez ohľadu na bezpečnosť systému. Naopak, stromom poruchových stavov možno opísať vplyv porúch na správania sa systému. Logická funkcia poruchových stavov je matematický zápis vyjadrujúci vzťah medzi základnými udalosťami a vrcholovou udalosťou. Vhodným prepojením týchto modelov možno vytvoriť model opisujúci vplyv porúch prvkov na bezpečnosť systému. Na základe znalosti logickej funkcie poruchových stavov sa dajú definovať bezpečnostné požiadavky na prvky systému, ktoré sú zviazané s jednotlivými základnými udalosťami, v zhode s požadovanou úrovňou bezpečnosti. Časovú závislosť správania sa systému možno vniesť do modelu ohodnotením základných udalostí pravdepodobnosťami ich výskytu. Strom poruchových stavov však nie je vhodný na modelovanie účinkov viacnásobných porúch na správanie sa systému. Za predpokladu určitých zjednodušení možno výskyt viacnásobných porúch v systéme modelovať Markovovým procesom.

Informácie publikované v tonto článku súvisia s riešením výskumnej úlohy "Teoretický aparát pre analýzu s definovanou úrovňou bezpečnosti.", VÚ 1/5230/98 ŽU v Žiline.

Summary

MODEL FOR SAFETY ANALYSIS OF THE INTERLOCKING SYSTEM

Karol RÁSTOČNÝ

The structural function represents relations among elements of the system without any respect to system safety. On the contrary, a fault tree can be used to describe fault effects on behaviour of the system. The logical function of fault states is a mathematical statement representing relationship between basic event and a top event. Connecting these models suitably we can create a model describing effects of element faults on system safety. On the base of logical function of fault states there can individual basic event, in accordance with required safety stage. Time dependence of system behaviour can be applied to the model by evaluating basic events through probabilities of their occurrence. But the fault tree is not suitable to model effects of multiple faults in the system can be modelled by Markov´s process.

Information given in this paper is related to solution of the research project „Theoretical Apparatus for Safety Analysis of the System with Defined Level of Safety", VÚ1/5230/98, at the University of Žilina.

Zusammenfassung

MODELL FÜR DIE SICHERHEITSANALYSE EINES EISENBAHNSICHERUNGSSYSTEMS

Karol RÁSTOČNÝ

Eine Strukturfunktion drückt die Beziehung zwischen den Komponenten des Systems ohne Rücksicht auf die Sicherheit des Systems aus. Im Gegenteil, Ausfallauswirkungen auf die Systemtätigkeit lassen sich über den Fehlerbaum beschreiben. Logische Funktion von den Fehlerzuständen ist eine mathematische Gleichung, die die Beziehung zwischen den Grundereignissen und dem TOP-Ereignis ausdrückt. Durch zweckmäßige Verbindung dieser Modelle kann man ein Modell bilden, das die Ausfallauswirkungen der Komponenten auf die Sicherheit des Systems beschreibt. Aufgrund logischer Funktion von den Fehlerzuständen kann man, in Übereinstimmung mit der System – Sicherheitsanforderungsstufe, Sicherheitsanforderungen für die Komponenten bestimmen. Die Zeitabhängigkeit des Systemverhaltens kann man durch die Wahrscheinlichkeiten der Grundereignisse in das Modell einführen. Der Fehlerbaum ist zur Modellierung der Auswirkungen von den Mehrfachausfällen nicht geeignet. Unter bestimmten Voraussetzungen können Auswirkungen von den Mehrfachausfällen über die Markov-Technik modelliert werden.

Informationen, die durch diesen Artikel publiziert werden, sind mit der Lösung der Forschungsaufgabe „Theoretischer Apparat für die Analyse des Systems mit der definierten Sicherheitsstufe", VÚ 1/5230/98 Universität Žilina, verknüpft.