PERIODICA POLYTECHNICA SER. TRANSP. ENG. VOL. 26, NO. 1-2, PP. 175-186 (1998)

ERHÖHUNG DER BAHNSICHERHEIT DURCH FORMALE METHODEN

Géza TARNAI und Balázs SÁGHI

Lehrstuhl für Verkehrsautomatik
Technische Universität Budapest
Phone: +36 1 463 1013
E-mail: tarnai—saghikaut.kka.bme.hu

Eingegangen: 20 Dezember, 1998

Abstract

The aim of this paper is to demonstrate the current problems of system development and to show, how formal methods can eliminate some of these problems. First the safety procass will be shown with its particioants and their roles as an introduction. In the first chapter the developing phases will be presented from the customer statement of requirements to the system specification, with their classification and deficiencies. In the next chapter the basics of the formal methods in area of test and simulation will be presented detailed with help of applications. Finally the current state of the application of formal methods and the future tasks are sketched.

Keywords: safety-relevant systems, railway signalling, formal methods.

Der Sicherheitsvorgang bei der Errichtung einer neuen Sicherungsanlage hat grundsätzlich vier Teilnehmer: die Bahn als Kunden und Betreiber, den Lieferanten (Entwickler, Hersteller), den unabhängigen Gutachter und die Behörde (Zulassen).

Die Anforderungen für eine zu errichtende Sicherungsanlage werden vom Kunden formuliert und nach einer Analyse mit dem Lieferanten abgestimmt. Die Anlagendokumentation und die Anlage selbst müssen durch einen von dem Kunden beauftragten Gutachter vor der Inbetriebnahme überprüft werden. Der Prüfbericht ist eine der Voraussetzungen, daß der Kunde die Zulassung zur Inbetriebnahme von der Behörde erhält.

Bei diesem Vorgang spielt der Kunde eine zentrale Rolle (s. *Abb. 1*). Besonders wichtig ist dabei die Kunden-Lieferanten-Verbindung, insbesondere die gute Fachverständigung zwischen beiden Parteien. Um dies zu erreichen wäre es vorteilhaft, auf allen Kommunikationsebenen bzw. in allen Entwicklungsphasen von der Anforderungsformulierung/-abstimmung bis zur Inbetriebnahme eine einheitliche, eindeutige Kommunikationssprache zu benutzen. Dies ist auch für die Kommunikation mit dem Gutachter und der Behörde wichtig.

Zur Spezifikation einer bestimmten Aufgabe dienen heute mehrere unterschiedliche Dokumente. Die verschiedenen Dokumente haben unterschiedliche Zielrichtungen und spezifizieren die Aufgabe aus unterschiedli-

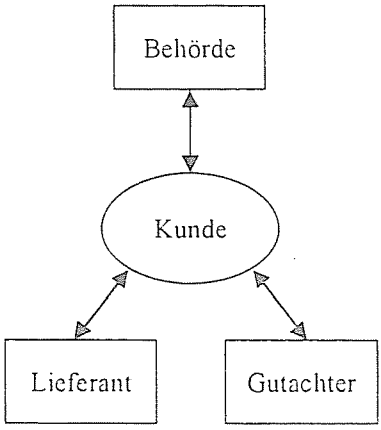

Abb. 1.

chen Aspekten. Es ist notwendig, einen Nachweis der Konsistenz und Widerspruchsfreiheit zu erstellen.

Die Ansprüche an o.g. Kommunikation können nur durch geeignete Beschreibungen erfüllt werden, wobei die Anforderungen ohne Interpretationsspielraum eindeutig formuliert werden müssen.

Qualifizierte und verifizierbare Beschreibungen sind erforderlich, mit denen Simulationen schon vor der technischen Realisierung durchgeführt werden können, die sich zur Herleitung von Testfällen eignen und mit denen die Kommunikation an den Verbindungsstellen zwischen neuen und alten Teilsystemen verbindlich notiert werden kann. Die Simulation kann ein gutes Mittel zur Kommunikation zwischen dem Kunden und dem Entwickler/Hersteller sein [13].

Die Frage der Eindeutigkeit und Vollständigkeit der Spezifikationstechnik beschäftigt die europäischen Bahnen und deren Lieferanten seit langer Zeit. Im Interesse der Ausfilterung der verbalen Ungenauigkeiten und der eindeutigeren Formulierung der funktionellen Zusammenhänge wurden zahlreiche Versuche durchgeführt [4].

Die ERRI-Arbeitsgruppe A201 hat das funktionelle Anforderungssystem der europäischen Bahnen untersucht, welches zur Zeit vereinheitlicht wird. Zu dieser Tätigkeit werden formale Techniken weitverbreitet angewandt [3].

Wegen der funktionellen und sequentiellen Komplexität der Eisenbahnsicherungsanlagen steht aber ein beweisbar vollständiges formales Funktionssystem noch nicht zur Verfügung. Eine vollständige formale Funktionsbeschreibung ist die Voraussetzung zur Gestaltung eines beweisbar verifizierbaren Systems.

In diesem Artikel wird dargelegt, daß die geschilderte Problematik der Kommunikation zur Entwicklung, Begutachtung und Zulassung durch die

sogenannten formalen Methoden teilweise gelöst werden kann. Im ersten Abschnitt wird der grundsätzliche Teil der Kundenkommunikation und der Systementwicklung von den Kundenanforderungen bis zur Systemspezifikation behandelt. Anschließend werden die Vorteile der Anwendung der formalen Techniken in der Systementwicklung geschildert. Da Tests und Simulation im Produktlebenszyklus eine hervorragende Bedeutung haben, wird der Einsatz der formalen Methoden in diesen Bereichen ausführlicher, auch durch realisierte Beispiele, vorgestellt. Abschließend wird ein kurzer Überblick über den heutigen Stand der Anwendung formaler Methoden in der Eisenbahnsicherungstechnik bzw. die zukünftigen Erwartungen gegeben.

1. Von Kundenanforderungen bis zur Systemspezifikation

Die Kundenanforderungen sind informale Beschreibungen der Eigenschaften eines neuen Systems oder eines solchen Systems, das an ein schon existierendes angepaßt werden muß. Das Dokument, das die Anforderungen enthält, heißt Lastenheft. Lastenhefte werden meistens in natürlicher Sprache formuliert und benutzen anwenderspezifische, nicht mathematische Ausdrücke.

Die Kundenanforderungen können in mehrere Klassen eingestuft werden:

- funktionelle Anforderungen, die bestimmen, was das System tun soll;
- nichtfunktionelle Anforderungen, die Direktiven sind, nach denen sich der Entwickler während der nachfolgenden Aktivitäten richten sollte;
- Zielsetzungen, die dem Entwickler helfen, wenn eine Wahlmöglichkeit besteht;
- Anforderungen an die Daten;
- Projektierungsdirektiven, Vorschriften für die Implementation und Ausstattung. Aus den Projektierungsdirektiven resultieren oft nicht optimale Systeme, weil sie den Entwickler unnötig einschränken.

Die Sicherheitsanforderungen an sicherheitsrelevante Systeme können entweder in einer selbständigen Klasse oder als Teil der funktionellen und nichtfunktionellen Anforderungen erscheinen.

Das Leben wäre für den Entwickler sehr einfach, wenn die Anforderungen im Lastenheft (und natürlich in der Spezifikation) auch in der Praxis in die oben erwähnten Anforderungsklassen immer eindeutig eingestuft wären. Die häufigsten Abweichungen von dem idealen Dokument sind:

- Ungenauigkeit/Ungewißheit,
- Widersprüche,
- Unvollständigkeit,
- Anforderungen verschiedener Klassen gemischt,

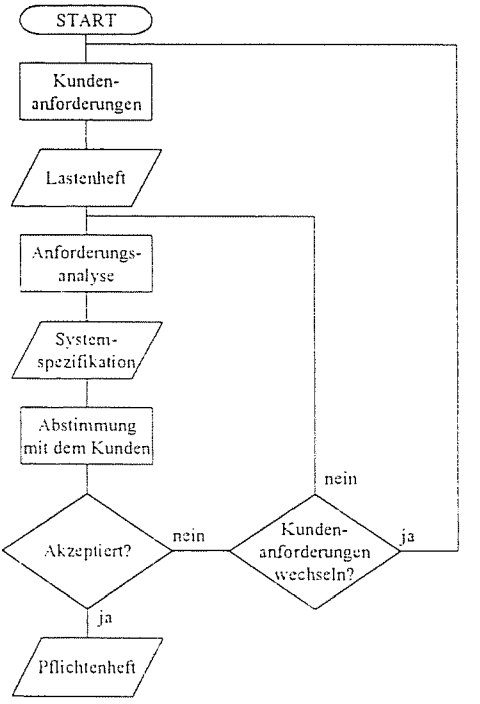

Abb. 2.

- Anforderungen verschiedener Abstraktionsebenen gemischt,
- Naivität des Kunden – der Kunde unter- oder überschätzt die Fähigkeiten des zukünftigen Systems,
- Zweideutigkeit, Mißverständnis – die natürliche Sprache ist ein schwaches Medium, wenn es um Präzision geht.

Durch eine Anforderungsanalyse muß der Entwickler aus dem Lastenheft eine Systemspezifikation erstellen (Abb. 2). Da die Systemspezifikation, bzw. das daraus zu erstellende Pflichtenheft als Grunddokument die Referenz für alle nachfolgenden Entwicklungsphasen ist, muß sie klar, konsistent und eindeutig sein. Dazu müssen alle oben aufgelisteten Mängel der Kundenanforderungen beseitigt werden.

Die Spezifikation beschreibt das zu entwickelnde System so, wie der Entwickler die Kundenanforderungen interpretiert hat. Für die Korrektheit der Spezifikation muß die Analyse der Kundenanforderungen durchgeführt werden, wobei das ausführliche Befragen des Kunden (mit vom Entwickler vorbereiteten Kontrollantworten) praktisch unvermeidlich ist.

Anschließend ist die Spezifikation an den Kunden zur Überprüfung (und Zulassung) zu übergeben.

Akzeptiert der Kunde die Spezifikation und läßt sie zu, kann der Entwickler auf Basis der Spezifikation das Pflichtenheft für den internen Gebrauch erstellen.

2. Formale Techniken zur Systementwicklung

Ein Großteil der Probleme bei der Systementwicklung entsteht daraus, daß für die einzelnen Entwicklungsphasen unterschiedliche und außerdem nicht vollkommen adäquate Beschreibungsmittel benutzt werden.

Ein typisches Beispiel ist eine Softwareentwicklung, wobei der Prozeß mit der Zusammenstellung eines in natürlicher Sprache geschriebenen Lastenheftes beginnt. Davon wird eine Systemspezifikation, z.B. in grafischer Darstellungsweise erstellt. Diese wird verfeinert und ein detaillierter Systemplan wird erstellt, z.B. als ein Satz von Steuerkonstruktionen, teilweise in Programmiersprache, teilweise in natürlicher Sprache. Endlich wird das Programm in einer Programmiersprache kodiert.

Es ist schon seit langer Zeit bekannt, daß durch die Programmiersprachen die Algorithmen und deren Implementationen genauer als durch die natürlichen Sprachen beschrieben werden können. Es wurde versucht, diese Eingenschaft auch für die Beschreibung der Hardware digitaler Systeme zu benutzen. So haben sich im letzten Jahrzehnt mehrere Hardware-Beschreibungssprachen herausgebildet. Die bekannteste und akzeptierteste ist VHDL, die durch gleiche Syntax ermöglicht, die Systeme sowohl im sog. Verhaltensbereich als auch im sog. strukturellen Bereich zu beschreiben. Das gilt für alle Elementebenen, d.h. von den Schaltern/Gattern bis zu Prozessoren/Speichern, sogar für die eindeutige Spezifikation auf der abstrakten Ebene.

Es ist aber wünschenswert, ebenfalls eine korrekte Beschreibung für alle Entwicklungsphasen der Gesamtsysteme zu haben. Eine Möglichkeit ist dazu der Einsatz eines formalen Beschreibungsmittels, das eine vollständige, integrierte Beschreibung ermöglicht, die alle Aspekte eines Systems umfaßt [9].

Die formalen Methoden haben ihre Wurzeln in den Forschungen für die automatische Funktionsprüfung in den späten 60-er/frühen 70-er Jahren. Die Forschungen in den letzten zehn Jahren haben sich auf die mathematischen Sprachen und die anschließenden Methoden für die Systemspezifikation und -entwicklung konzentriert.

Die formalen Methoden wenden mathematische (z.B. logische, mengentheoretische) Zeichnungen zur Beschreibung der Systeme in den einzelnen Entwicklungsphasen an. Die Anwendung der Mathematik in der Systemspezifikation hat eine Vielzahl von Vorteilen. Dies sind:

- Es ist leicht, unterschiedliche Abstraktionsebenen darzustellen.
- Es ist leicht, mathematisch zu argumentieren.

- Mathematik ist kompakt.
- Mathematik ist eindeutig.
- Mit Mathematik kann die Realität modelliert werden.

Im Vergleich ist es festzustellen, daß die Syntax und die Semantik bei den informellen Beschreibungsmitteln intuitiv, bei den formalen Techniken dagegen formal sind. Das heißt, daß die formalen Techniken strenge Konventionen und syntaktische Regeln/Vorschriften haben. Eine informelle Beschreibung ist leicht zu lesen, aber sie ist oft mehrdeutig. Die Lesbarkeit einer formalen Beschreibung ist viel schlechter, aber sie ist immer eindeutig. Wegen der strengen Syntax und Semantik ist es möglich die formalen Techniken völlig zu automatisieren, was bei informellen Techniken kaum vorstellbar ist.

Für die Entwickler wäre sehr günstig, die Spezifikation schon in formaler Sprache zu erstellen, was aber wegen der Kundenkommunikation nur relativ selten möglich ist. Diese Schwierigkeit kann aber dadurch beseitigt werden, daß der Entwickler aus der formalen Spezifikation ein durchführbares Simulationsmodell zur Visualisierung für den Kunden erstellt [9].

Da die Kundenanforderungen nach wie vor in natürlichen Sprachen formuliert werden, eliminieren die formalen Methoden die Benutzung der natürlichen Sprachen nicht, aber sie spielen eine kleinere Rolle.

Nicht nur die Kundenkommunikation braucht ein Modell. Zur Systementwicklung werden ebenfalls formale Modelle benötigt, die jedoch implementierungsfähig und phasenübergreifend durchgängig sein müssen.

Ein Modell ist die Abbildung eines für uns relevanten Teils der Realität. Natürlich sind die nicht relevanten Details zu verkürzen. Es muß auch die Systemumwelt mindestens vereinfacht modelliert werden. Das Umweltmodell muß alle weiteren, über Schnittstellen des Systems angebundenen Systeme enthalten.

Zur Erstellung eines Modells braucht man in allen Phasen der Systementwicklung ein Beschreibungsmittel, eine Methode und ein Werkzeug (BMW Prinzip).

Unter einem Beschreibungsmittel verstehen wir die einzelnen Darstellungselemente und die Konventionen über deren Kombinationen. Beschreibungsmittel dienen zur Beschreibung der Aufgabe, der Anforderungen, der Lösung und ihrer Vorgehensweisen sowie der resultierenden Ergebnisse und ihrer Dokumentation.

Eine Methode ist eine auf einem Regelsystem aufbauende, planmäßige Vorgehensweise zur Formulierung der Anforderungen, zur Integration verschiedener Aspekte, zur Überprüfung und Qualitätssicherung.

Zur effizienten Handhabung werden schließlich Werkzeuge gebraucht, die zur Unterstützung der Beschreibung und der methodischen Vorgehensweise, Prüfung, bei Test, Simulation, Dokumentation, usw. benutzt werden. Das Werkzeug ist heute fast immer ein Rechensystem.

Mit dem erstellten Modell hat man eine formale Beschreibung der Spezifikation. Ein solches Modell bietet eine Vielzahl von Möglichkeiten. Das Modell kann ausführbar sein, so ist es möglich eine Simulation der betrieblichen Abläufe durchzuführen. Mit Hilfe einer Simulation lassen sich die Projektierungsprobleme noch in der Spezifikationsphase zu zeigen und zu beheben. Auf Basis der Simulation können verschiedene Tests durchgeführt werden. Das Modell kann zur Qualitätssicherung des Systems und auch zum Sicherheitsnachweis verwendet werden. Endlich ist es auch möglich, aus dem ausführbaren Modell einen Quellencode und auch einen ausführbaren Code zu erstellen.

3. Tests, Simulation und formale Methoden

Grundlegende Komponente der Systementwicklung sind die Verifikation und die Validation. Durch die Verifikation wird festgestellt, ob die Ergebnisse einer Entwicklungsphase der vorangegangenen Phase entsprechen. Durch die Validation wird geprüft, ob die Ergebnisse einer Entwicklungsphase den Kundenanforderungen entsprechen.

Durch die Erhöhung der Komplexität der Systeme wurde die Verifikation des implementierten Systems eine der größten Probleme. Bei sicherheitsrelevanten Systemen muß neben der Funktionalität die Sicherheit ebenfalls verifiziert werden. Die Sicherheitsanforderungen können meist im Rahmen der Funktionsspezifikation angegeben werden. So sind die Methoden zur Verifikation des sicheren Verhaltens gleich oder ähnlich, wie die Methoden der Funktionsverifikation. Es gibt aber spezielle Komponenten der Sicherheit, deren Spezifikation durch die Funktionsspezifikation nicht möglich ist (z.B. die Spezifikation der Fehlertoleranz).

Beide Aktivitäten, Verifikation und Validation werden durch Tests unterstützt. Bei Tests werden die auf eine bestimmte Eingangssequenz folgenden Ausgangszustände (Istreaktionen) und die Sollreaktionen (Testreferenz) eines Systems (Testobjekt) verglichen.

Auf Basis der Testziele, mit Berücksichtigung des ökonomischen/zeitlichen Rahmens sind die Testanforderungen zu bestimmen. Während der Testplanung werden die den Testanforderungen entsprechenden Testfälle, bzw. die dazu benötigten Eingangssequenzen generiert. Die Testreferenzdaten werden durch die auf die Eingangssequenzen folgenden Reaktionen eines Simulationsmodells des Testobjektes erstellt.

Nach der Vorbereitungsphase kann der Test durchgeführt werden. Die Ergebnisse des Soll-/Istreaktion-Vergleiches werden bewertet und in der Testdokumentation eingetragen.

Traditionell muß man Tests zur Verifikation nach jeder Entwicklungsphase bzw. in jeder Phase des Produktlebenszyklus durchführen lassen. So geht es um

- Modultest
- Integrationstest
- Funktionstest
- Systemtest
- Abnahmetest
- Wartungstest.

Formale Beschreibungsmittel und der Einsatz von rechnergestützten Werkzeugen vereinfachen einige der grundlegenden Probleme des Tests [14].

- Sind die formalen Modelle ablauffähig, so kann deren Verifikation schon als erster Test angesehen werden, was die nachfolgenden Tests des implementierten Systems stark verkürzt.
- Der Horizont der Systemspezifikation ist die Basis für Festlegung der Testumgebung. Formale Modelle schon entwickelter Nachbarsysteme (Umweltmodell) bieten uns eine erweiterte und validierte Testumgebung an.
- Wird das System mit formalen Beschreibungsmitteln beschrieben und stehen verifizierte Entwicklungswerkzeuge zur Verfügung, kann man die Menge der konventionellen Tests bedeutend vermindern. Formale Methoden an sich helfen schon in der Spezifikation- und Entwurfsphase eine Vielzahl von Fehlern zu vermeiden, die dann später nicht mehr durch Tests gefunden werden müssen.

Die formalen Methoden eliminieren nicht die Notwendigkeit der Testierung. Der Kunde braucht immer eine Demonstration mit realen Daten vor der Inbetriebnahme um sicher zu sein, daß das System richtig funktioniert. Analog müssen Wartungstests durchgeführt werden.

Die automatische Testgenerierung und -durchführung ist einer der Bereiche der Eisenbahnsicherungstechnik, in dem formale Beschreibungsmethoden und die formale Modellbildung schon relativ früh angewandt wurden.

So wurde z.B. an der TU Budapest am Lehrstuhl für Verkehrsautomatik eine formale Beschreibungssprache RETES (RElais TESt) zur Beschreibung der Relaissätze (Relaisgruppen) verschiedener Bauart von Stellwerksanlagen mit der Zielsetzung der Testgenerierung in den 70-er Jahren entwickelt.

Das System RETES und dessen weiterentwickelte Version VIPERA ist aber nicht nur eine Beschreibungssprache, sondern es bildet mit der dafür entwickelten Testmaschine gemeinsam ein geschlossenes und automatisches Testsystem von der Beschreibung des Testobjektes, ü ber die automatische Erzeugung der Testsä tze bis zur Durchführung und Auswertung der Tests mit dem Ziel der Produktionsendkontrolle.

Die Komplexität der Aufgabe kann man sich durch die Anzahl der Relais in einer Relaisgruppe (über 30) und der Anschlußpunkte (über 300) vorstellen. Dazu kommt noch die Vielfältigkeit der Relais (die Anzahl und die Funktion der Wicklungen eines Relais, spezielle Mechanik, usw.). Die

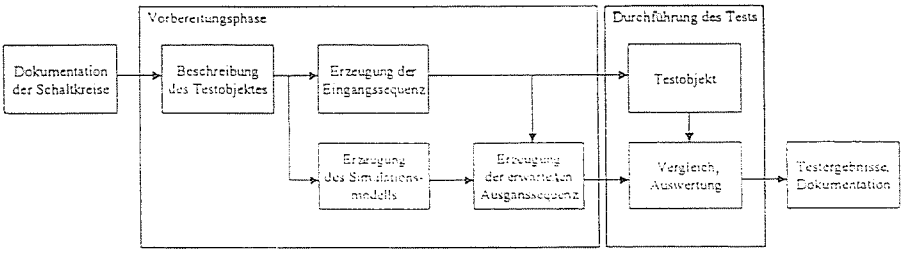

Abb. 3.

Ausgangsdokumentation für die Beschreibung sind die Schaltungspläne, die vorherig zweckmäßig präpariert wurden (Spezifikationsphase). Nach der sorgfältigen und überprüften Beschreibung findet alles folgende automatisch statt. Bei Relaisgruppen, die solche Besonderheit haben, die nur sehr selten vorkommen und deren Berücksichtigung bei der automatischen Erzeugung der Testeingangssequenz nicht zu empfehlen ist, braucht man eine fachmännische Mitwirkung, aber die Erzeugung der Ausgangssequenz erfolgt auch in diesen Fällen schon vollautomatisch. In 10 Jahren wurden Beschreibungen von mehr als 60 unterschiedlichen Typen von Relaissätzen erstellt und mehrere Tausende von Relaisgruppen getestet [17, 18, 19, 20].

Die Simulation kann nicht nur für Kundenkommunikation und Verifikation/Testgenerierung, sondern auch als selbständiges Trainingssystem oder Projektierungswerkzeug angewandt werden. Die formalen Methoden spielen bei Entwicklung dieser Anwendungen ebenfalls eine wichtige Rolle. Die zu simulierenden Objekte und die Simulationsumgebung sind in formaler Sprache zu beschreiben.

Beispielsweise wurde an der TU Budapest, Lehrstuhl für Verkehrsautomatik, in den frühen 80-er Jahren ein Trainingssystem entwickelt. Dieses System basiert auf Echtzeitsimulation eines Stellwerks bestimmter Bauart und dessen Umgebung umfaßt Bedienoberfläche/Anzeige, Außenanlagen und Zugverkehr. Das Modell kann nicht nur den Normalbetrieb, sondern durch vom Ausbilder eingegebene Fehler, technische und/oder betriebliche Unregelmäßigkeiten simulieren. Es wurden in Ungarn 7 solche Schulungssysteme in Betrieb genommen [15]. Eine stark weiterentwickelte Version SESAM hat bei der Deutschen Bahn AG eine verbreitete Anwendung gefunden: 28 Schulungszentren mit je 5 vernetzten Arbeitsplätzen benutzen das System [16]. Das SESAM-Projekt wurde von einer deutschen Firma DST und deren Tochterfirma Tran-Sys GmbH in mehrere Richtungen erfolgreich fortgesetzt, so z.B. im Rahmen des Projekts BEST-ESTW für die Simulation elektronischer Stellwerke [7].

Nicht nur als Trainigssystem sondern auch als Projektierungswerkzeug kann das neuartige Simulationssystem RailCAD benutzt werden, das von der 'Stellwerk' GmbH, Budapest entwickelt wurde. RailCAD benutzt eine formale Beschreibungssprache für jedes zu simulierende Teilsystem. Dadurch

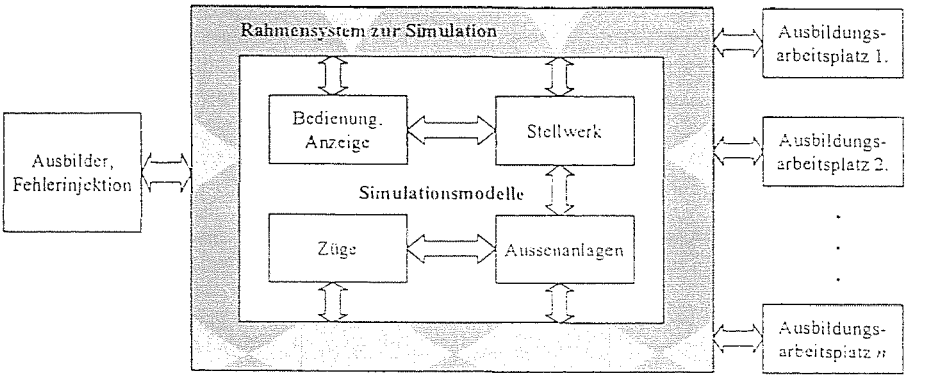

Abb. 4.

und durch die natürlichsprachliche Benutzerkommunikation kann eine beliebige Stellwerkslogik und die anderen Teilsysteme eindeutig und relativ leicht auch vom Kunden selbst beschrieben und/oder geändert werden [1].

Das Schema eines Trainingssystems wird auf *Abb. 4* dargestellt.

4. Die formalen Methoden heute und morgen

Anhand einiger Beispiele soll im folgenden Abschnitt der heutige Stand der Anwendung formaler Methoden in der Eisenbahnsicherungstechnik dargestellt und ein kurzer Ausblick in deren zukünftige (mögliche) Bedeutung gewagt werden.

BERNARDESCHI u. a. stellen einige Abstraktionstechniken vor, die Problematik der Validation der Sicherheitsanforderungen mit den vorhandenen Werkzeugen zu behandeln [2]. Die Abstraktionstechniken und deren Anwendungsmethodik wurden im Falle der Spezifikation eines elektronischen Stellwerksystems geprüft.

In Zusammenhang mit der Einleitung des einheitlichen europäischen Zugbeeinflußungssystems ETCS wird eine umfassende Forschungs-/Entwicklungstätigkeit auch im Bereich der Anwendung von formalen Techniken durchgeführt. Die bisherigen Ergebnisse wurden im Rahmen der internationalen Konferenz FORMS '98 an der TU Braunschweig veröffentlicht und diskutiert. In der Einleitung hat Professor SCHNIEDER die ganze Palette der Problematik und einige Fragen der Zukunft geschildert [13].

Ausgehend von der Relevanz formaler Methoden für modulare Softwaresysteme, kommunikationsbasierte und eingebettete Systeme hat Professor EHRIG einen kurzen Überblick über verschiedene formale und semiformale Methoden in der Informatik gegeben. Die gegenseitige Beeinflußung von Methoden der Ingenieurwissenschaften und der Informatik wurde am

Beispiel des DFG-Schwerpunktprogramms "Integration von Techniken der Softwarespezifikation für Ingenieurwissenschaftliche Anwendungen" demonstriert [5]. Im Schwerpunktprogramm wurden sechs verschiedene Integrationen von Spezifikationstechniken diskutiert und im Hinblick auf verschiedene anwendungsorientierte und technische Aspekte verglichen. Wie es festgestellt wurde, sind dabei neben der Universellen Modellierungssprache UML als semi-formale Methode High-Level-Petrinetze als formale Spezifikationstechnik von besonderer Bedeutung.

Auf der Basis der informellen Spezifikation von ETCS wurde im Auftrag der Deutschen Bahn AG im Institut für Regelungs- und Automatisierungstechnik der TU Braunschweig ein formales Modell erstellt [11]. Die gesamte Modellierung umfaßt drei Modelle: Fahrzeuggerät, Streckengerät und ein stark vereinfachtes Modell der Umwelt. Das Umweltmodell enthält alle weiteren, über Schnittstellen des Systems angebundene Systeme. Für den Systementwurf wurden nach ausführlichen Vergleichen als Beschreibungsmittel Petrinetze ausgewählt. Sie bieten die Möglichkeiten der in allen Entwicklungsphasen durchgängigen Verwendung, des Einsatzes unterschiedlicher Methoden und der formalen Analyse. Als Methode wurde ein integrierter Ansatz aus Ereignis- und Datenorientierung entwickelt, der aus spezifischen Netzebenen unterschiedliche Aspekte des Systems abbildet. Die Modellierung des Systems wurde mit dem Werkzeug Design/CPN unterstützt, das nach sorgfältigen Vergleichen ausgewählt wurde.

Ein weiteres rezentes Beispiel ist eine der Anpaßentwicklungen im Rahmen der Modernisierung der Eisenbahnstrecke Budapest–Wien, wobei die Funktionen einer elektronischen Stellwerksanlage (eStw) von Siemens mit der zusätzlichen Funktion der 75 Hz Signalübertragung/Zugbeeinflussung ergänzt werden sollten. Diese Funktion konnte am besten als externe Steuerung durch ein PLC (Speicherprogrammierbare Steuerung - SPS) gelöst werden. Um die informale Spezifikation eindeutig zu machen wurde eine neue, formale Beschreibungsmethode eingesetzt, deren Form auch für die Fachleute der Relaisstellwerke leicht lesbar und eindeutig interpretierbar ist. Anderseits können die Software-Entwickler diese Form ohne Umsetzung zur Implementation in der Programmiersprache STEP5 benutzen. Dadurch werden sowohl die Kundenkommunikation als auch die Verifikation des implementierten Systems bedeutend erleichtert [6].

Durch die obigen Beispiele wurde es gezeigt, daß die formalen Methoden in einigen Teilbereichen der Sicherungstechnik schon vorteilhaft eingesetzt werden. Die zukünftigen Erwartungen betreffen die Erweiterung der Anwendung auf den ganzen Produktlebenszyklus. Eine Voraussetzung dafür ist die Akzeptanz der neuen Technik bei allen Beteiligten am Sicherheitsvorgang.

Literatur

[1] ARANYOSI, Z. – MOSÓCZI, L. – RÁCZ, G. – TARNAI, G.: 'Training the Personnel Using Simulator and Training System', *World Congress on Railway Research WCRR'97 Proceedings*, Firenze 1997, Vol. A, pp. 745–751.

[2] BERNARDESCHI, C. : 'Proving Safety Properties for Embedded Control Systems' *EDCC-2* Taormina, Italy, October 1996, pp. 321–332.

[3] BOWIE, M. – INGLEBY, M.: 'ERRI A201 Committee: Harmonisation of European Interlocking Specification', *IRSE Proceedings*, 1997.

[4] BROWNBRIDGE, D.: Specifying BR Signalling Rules, *IRSE Proceedings*, 1997.

[5] EHRIG, H.: Relevanz, Integration und Vergleich formaler Spezifikationstechniken *FORMS '98*, 12-13 May 1998, Braunschweig, Germany.

[6] GÖRÖG, B. – SZABÓ, G. – TARNAI, G.: Sicherheits- und Zuverläßigkeitsanalyse von auf PLC-Basis realisierten Sicherheitsfunktionen, *Fachzeitschrift Vezetékek Világa*, Budapest 3/98, pp. 6–10 (ungarisch).

[7] HALL, W. – PARÁDI, F.: BEST-ESTW – Neues Simulationssystem zur Schulung von Fahrdiensleitern. *Signal+Draht*, 1996, H. 7/8.

[8] INCE, D.: An Introduction to Discrete Mathematics and Formal System Specification, and Z, Oxford University Press Inc., New York 1995.

[9] JAHNSEN, A.: Anwendung von Modellen zur Unterstützung der Kommunikation und Klarheit von Spezifikationen, *FORMS'98*, 12-13 May 1998, Braunschweig, Germany.

[10] KERESZTES, P.: Theoretische Fragen der Funktional- und Sicherheitsverifikation digitaler Systeme, *Fachzeitschrift 'Vezetékek Világa*, Budapest, 96/2, pp. 16–19 (ungarisch).

[11] MEYER ZU HÖRSTE, M.: Die formale Modellierung und Simulation von ERTMS/ETCS mit Petrinetzen *FORMS '98* 12-13 May 1998, Braunschweig, Germany.

[12] NELLI, M.: 'Dependability Modelling and Analysis of Complex Control Systems: An Application to Railway Interlocking, *EDCC-2 Second European Dependable Computing Conference*, Taormina, Italy, October 1996, pp. 93–110.

[13] SCHNIEDER, E.: Zum Geleit *FORMS '98 International Workshop Formal Specification of Train Control Systems in Europe, 12-13 May* 1998, Braunschweig, Germany.

[14] SCHULZ, H.-M.: Komplexität des Tests technischer Systeme mit Blick auf Leitsysteme im Schienenverkehr *FORMS '98*, 12-13 May 1998, Braunschweig, Germany.

[15] TARNAI, G. u.a.: Die Simulierung des Eisenbahnvehrkehrsprozesses mit Hilfe von Mikroprozessoren *Materialy na IV. Konferencje Naukova* Politechnika Warszawska Instytut Transportu, Warszawa, 1985. 3. k. pp. 193–201.

[16] TARNAI, G. – PARÁDI, F.: Unterstützung von bahnspezifischen Projektierungs- und Testverfahren durch Modellierung *Zeszyty Naukowo-Techniczne Oddzialu Krakowskiego SITK*, Zakopane 1992, Nr. 24. pp. 229–239.

[17] TARNAI, G.: Automatische Prüfung der Relaissätze in Stellwerkstechnik Dissertation für Grad Kandidat der Wissenschaften, Ung. Akademie der Wissenschaften, Budapest, 1984. pp. 152 (ungarisch).

[18] TARNAI, G.: Ein algebraisches Modell für Relaiseinheiten von Eisenbahnsicherungsanlagen, *Periodica Polytechnica, Transport*, Budapest, 12/1984/1.

[19] TARNAI, G.: Safety Verification for Train Traffic Control Communications *IEEE Journal on Selected Areas in Communications SAC-4*, October 1986. No 7. pp. 1118–1120.

[20] TARNAI, G.: Testing Microprocessor Equipment for Railway Safety, *Sixth Symposium on Reliability in Electronics*, Budapest, August 1985. pp. 539–545.