

Petrinetzbasierte Spezifikation und Analyse operationaler Prozesse am Beispiel Eisenbahnsicherung

**Von der Gemeinsamen Fakultät für Maschinenbau und Elektrotechnik
der Technischen Universität Carolo-Wilhelmina zu Braunschweig**

zur Erlangung der Würde

eines Doktor-Ingenieurs (Dr.-Ing.)

genehmigte Dissertation

von: Dipl.-Ing. Stefan Einer
aus: Hamburg

eingereicht am: 25.04.2003
mündliche Prüfung am: 20.06.2003

Referenten: Prof. Dr.-Ing. Eckehard Schnieder
Prof. Dr. Hans-Dieter Ehrich
Vorsitzender: Prof. Dr.-Ing. Karsten Lemmer

2003

Inhaltsverzeichnis

1 Einleitung	1
1.1 Problemstellung.....	2
1.2 Ziel	4
1.3 Stand der Technik und Ansätze.....	4
1.4 Vorgehen.....	5
1.5 Gliederung der Arbeit	6
2 Ein Entwicklungsrahmen für formale Techniken.....	7
2.1 Systemtheoretische Grundlagen.....	7
2.1.1 Der allgemeine Systembegriff.....	7
2.1.2 Allgemeine Klassifizierung von Systemen	9
2.1.3 Modellbildung.....	10
2.1.4 Verifikation und Validation	10
2.2 Strukturmerkmale des Entwicklungsrahmens.....	11
2.2.1 Das BMW-Prinzip.....	11
2.2.2 Ebenenmodell der formalen Systembetrachtung	12
2.3 Elemente des Entwicklungsrahmens.....	16
2.3.1 Der Formalismus.....	16
2.3.2 Metamodelle.....	16
2.3.3 Beschreibungsmittel auf systemtheoretischer und anwendungsspezifischer Ebene.....	17
2.3.4 Methoden auf systemtheoretischer und anwendungsspezifischer Ebene.....	18
2.3.5 Konkrete Modelle, Modellbildung und –prüfung.....	18
2.4 Praktische Anwendung des Entwicklungsrahmens in der vorliegenden Arbeit	18
3 Spezifikation von operationalen Prozessen der Automatisierungstechnik.....	20
3.1 Der Begriff des Betriebsverfahrens.....	20
3.1.1 Ganzheitliche Betrachtung des Verhaltens von Automatisierungssystemen	21
3.1.2 Das Betriebsverfahren in der Verfahrens- und Fertigungstechnik.....	21
3.1.3 Das Betriebsverfahren in der Verkehrstechnik	22

Inhaltsverzeichnis

3.2 Die Begriffe Spezifikation und Spezifizierung	23
3.3 Wesentliche Merkmale der Spezifikation von Betriebsverfahren	26
3.4 Ansatz der formalen Spezifikation von Betriebsverfahren	27
4 Der Formalismus Coloured Petri Nets (CPN)	31
4.1 Petrinetz-Formalismen	31
4.2 Basis der CPN	32
4.2.1 Basis eines CPN-Grafen	32
4.2.2 Basis der Dynamik eines CPN	33
4.3 Gefährtheit der CPN	34
4.4 Zeitkonzept der CPN	35
4.5 Strukturierungskonzepte der CPN	36
4.5.1 Das Hierarchie-Konzept der CPN	37
4.5.2 Global Fusion Plätze der CPN	37
4.6 Methoden der CPN	38
5 Das Beschreibungsmittel von STOP	41
5.1 Ansätze der Pragmatik	41
5.2 Metamodelle der Pragmatik	42
5.2.1 Metamodell der Struktur von Modellsystemen nach STOP	43
5.2.2 Metamodell der Dekomposition von Modellsystemen nach STOP	44
5.2.3 Metamodell der Kausalität von Modellsystemen nach STOP	46
5.2.4 Metamodell der Temporalität von Modellsystemen nach STOP	49
5.2.5 Zusammenfassung der Metamodelle	49
5.3 Dem Ansatz nach mit Petrinetzen vergleichbare Formalismen	52
5.4 Entwurfsmuster der Modellsysteme nach STOP	54
5.4.1 Entwurfsmuster zur globalen Struktur der Modellsysteme nach STOP	56
5.4.2 Entwurfsmuster zur detaillierteren lokalen Struktur der Modellsysteme nach STOP	58
5.4.3 Entwurfsmuster zur lokalen Kausalität der Modellsysteme nach STOP	61
5.4.4 Entwurfsmuster zur lokalen Temporalität der Modellsysteme nach STOP	62
5.4.5 Entwurfsmuster zur Szenariokoordination	67
5.4.5.1 Problem	67
5.4.5.2 Konzept	68

5.4.5.3	Realisierung	70
5.4.6	Entwurfsmuster zur Beschränkung des Zustandsraumes	72
5.4.6.1	Problem	72
5.4.6.2	Konzept	75
5.4.6.3	Realisierung	77
5.4.7	Zusammenfassung der Entwurfsmuster	80
5.4.7.1	Entwurfsmuster zur globalen Struktur der Modellsysteme nach STOP	80
5.4.7.2	Entwurfsmuster zur detaillierten lokalen Struktur der Modellsysteme nach STOP	81
5.4.7.3	Entwurfsmuster zur lokalen Kausalität der Modellsysteme nach STOP	81
5.4.7.4	Entwurfsmuster zur lokalen Temporalität der Modellsysteme nach STOP	81
5.4.7.5	Entwurfsmuster zur Szenariokoordination	81
5.4.7.6	Entwurfsmuster zur Beschränkung des Zustandsraumes	82
6	Methoden von STOP	83
6.1	Methoden der Modellbildung	83
6.1.1	Modellierung von Szenarien	83
6.1.2	Modellierung von Restriktionen	86
6.1.3	Modellierung von Abweichungspotenzial	86
6.2	Methoden der Modellprüfung	88
6.2.1	Prüfung der Zulässigkeit aller Zustände	89
6.2.2	Prüfung der Korrektheit des Verhaltensabschlusses	89
6.2.3	Prüfung der temporalen Korrektheit von Reaktionen	90
6.3	Vorgehensmodell	94
6.3.1	Verifikation des Modells hinsichtlich der Modellanforderungsspezifikation	96
6.3.2	Validation des Modells hinsichtlich des operationalen Prozesses	97
7	Anwendung von STOP am Fallbeispiel der Bahnübergangssicherung	99
7.1	Das Konzept der funkbasierten Bahnübergangssicherung	100
7.1.1	Überblick über die funkbasierte Bahnübergangssicherung	100
7.1.2	Abstraktion hinsichtlich des Betriebsverfahrens	102
7.2	Spezifikation des Sollszenarios	103
7.2.1	Natürlichsprachliche Erläuterung des Szenarios	103
7.2.2	Modellbildung des Sollszenarios	104
7.2.2.1	Entwicklung des Petrinetzgraphen	104
7.2.2.2	Modellbildung der Prozesszustandsdauern	110

Inhaltsverzeichnis

7.2.2.3 Zusammenfassung.....	112
7.2.3 Verifikation des Sollszenarios.....	114
7.2.4 Validation des Sollszenarios.....	116
7.3 Spezifikation des temporalen Potenzials der Zugbewegung.....	116
7.3.1 Modellierung des temporalen Potenzials der Zugbewegung.....	116
7.3.2 Verifikation des um das temporale Potenzial der Zugbewegung erweiterten Modells.....	117
7.4 Spezifikation der restriktiven Einfahrt in den Bahnübergang.....	118
7.4.1 Modellbildung der restriktiven Einfahrt.....	118
7.4.2 Verifikation des um die restriktive Einfahrt erweiterten Modells.....	119
7.4.3 Validation des um die restriktive Einfahrt erweiterten Modells.....	119
7.5 Spezifikation des temporalen Potenzials der Einschaltung.....	121
7.5.1 Modellierung des temporalen Potenzials der Einschaltung.....	121
7.5.2 Verifikation des um das temporale Potenzial der Einschaltung erweiterten Modells.....	121
7.6 Spezifikation des Szenarios „Status ungesichert“.....	122
7.6.1 Natürlichsprachliche Erläuterung des Szenarios „Status ungesichert“.....	122
7.6.2 Modellbildung des Szenarios „Status ungesichert“.....	122
7.6.2.1 Entwicklung des Petrinetzgrafen.....	122
7.6.2.2 Modellbildung der Prozesszustandsdauern.....	128
7.6.3 Verifikation des um das Szenario „Status ungesichert“ erweiterten Modells.....	130
7.6.4 Validation des um das Szenario „Status ungesichert“ erweiterten Modells.....	130
7.7 Zusammenfassung der beispielhaften Anwendung.....	130
8 Zusammenfassung und Ausblick.....	133
Anhang – Ausführbare Modelle und Verifikationen.....	137
A Spezifikation des Sollverhaltens.....	138
A.1 Ergebnismodell.....	138
A.1.1 Teilnetze auf anwendungsspezifischer Ebene.....	138
A.1.2 Hierarchie.....	138
A.1.3 Deklarationen.....	144
A.1.4 Teilnetze auf anwendungsneutraler Ebene.....	145
A.1.4.1 Zugbewegung.....	145
A.1.4.2 Zugüberwachung.....	147
A.1.4.3 Bahnübergangsüberwachung.....	148

A.1.4.4 Bahnübergangssicherung	150
A.1.5 Netz der Initialisierung und globalen Synchronisation	152
A.2 Verifikation	152
A.2.1 Report zum Erreichbarkeitsgraphen	153
A.2.2 Durchführung der Verifikation	153
A.2.3 Funktionen zur Prüfung des korrekten Verhaltensabschlusses	153
A.2.4 Funktionen zur Prüfung der Zulässigkeit aller Zustände	154
A.3 Analyse der Prozesszustandsdauern	155
A.3.1 Die anwendungsspezifischen Teilnetze vor der analytischen Bestimmung der Prozesszustandsdauern	155
A.3.2 Die anwendungsneutralen Teilnetze vor der analytischen Bestimmung der Prozesszustandsdauern	155
A.3.3 Analyse der Prozesszustandsdauern	164
A.3.3.1 Durchführung der Analyse der Prozesszustandsdauern	165
A.3.3.2 Erweiterung des Global Declaration Node	165
A.3.3.3 Funktionen zur Analyse der Prozesszustandsdauern	167
B Temporales Potenzial der Zugbewegung	171
B.1 Modell	171
B.1.1 Veränderung der anwendungsspezifischen Teilnetze	171
B.1.2 Veränderung der Hierarchie	171
B.1.3 Veränderung der Deklarationen	171
B.1.4 Veränderung der anwendungsneutralen Teilnetze	171
B.1.5 Veränderung des Netzes der Initialisierung und globalen Synchronisation	171
B.2 Verifikation	174
B.2.1 Report zum Erreichbarkeitsgraphen	174
B.2.2 Durchführung der Verifikation	174
C Spezifikation der restriktiven Einfahrt	175
C.1 Modell	175
C.1.1 Veränderung der anwendungsspezifischen Teilnetze	175
C.1.2 Veränderung der Hierarchie	175
C.1.3 Veränderung der Deklarationen	175
C.1.4 Veränderung der anwendungsneutralen Teilnetze	175
C.1.5 Veränderung des Netzes der Initialisierung und globalen Synchronisation	175
C.2 Verifikation	179

D Temporales Potenzial der Einschaltung.....	180
D.1 Modell	180
D.1.1 Veränderung der anwendungsspezifischen Teilnetze	180
D.1.2 Veränderung der Hierarchie	180
D.1.3 Veränderung der Deklarationen	180
D.1.4 Veränderung der anwendungsneutralen Teilnetze	180
D.1.5 Veränderung des Netzes der Initialisierung und globalen Synchronisation	180
D.2 Verifikation	182
D.2.1 Report zum Erreichbarkeitsgraphen	182
D.2.2 Durchführung der Verifikation	182
D.2.3 Funktionen der Prüfung der temporalen Korrektheit der Reaktionen.....	183
D.2.3.1 Überprüfung der Notwendigkeit der Alternative des Prozesszustandswechsels „BÜ-Sicherung wird aktiviert“ (t1 im Prozess Bahnübergangssicherung).....	184
D.2.3.2 Überprüfung der Notwendigkeit der Komplementbildung der verbleibenden relevanten Reaktionen	184
E Spezifikation des Szenarios „Status ungesichert“	188
E.1 Ergebnismodell.....	188
E.1.1 Veränderung der anwendungsspezifischen Teilnetze.....	188
E.1.2 Veränderung der Hierarchie	188
E.1.3 Veränderung der Deklarationen.....	188
E.1.4 Veränderung der anwendungsneutralen Teilnetze	188
E.1.5 Veränderung des Netzes der Initialisierung und globalen Synchronisation.....	195
E.2 Verifikation.....	199
E.2.1 Report zum Erreichbarkeitsgraphen.....	199
E.2.2 Durchführung der Verifikation.....	200
E.2.3 Funktionen zur Prüfung des korrekten Verhaltensabschlusses	200
E.3 Analyse der Prozesszustandsdauern	201
E.3.1 Die anwendungsspezifischen Teilnetze.....	201
E.3.2 Die anwendungsneutralen Teilnetze.....	201
E.3.3 Analyse der Prozesszustandsdauern	201
E.3.3.1 Durchführung der Analyse der Prozesszustandsdauern	201
E.3.3.2 Funktionen zur Analyse der Prozesszustandsdauern.....	204
Literaturverzeichnis.....	206