

Matthias Römer

**Rechnergestützte Analyse des
Kommunikationsverhaltens
feldbusfähiger Automatisierungsgeräte**

Herausgegeben von

**Prof. Dr.-Ing. Klaus Bender
Technische Universität München**

in der Reihe

Informationstechnik im Maschinenwesen



Herbert Utz Verlag · Wissenschaft
München 2004

Bibliografische Information Der Deutschen Bibliothek

Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.ddb.de> abrufbar.

Dieses Werk ist urheberrechtlich geschützt. Die dadurch begründeten Rechte, insbesondere die der Übersetzung, des Nachdrucks, der Entnahme von Abbildungen, der Wiedergabe auf photomechanischem oder ähnlichem Wege und der Speicherung in Datenverarbeitungsanlagen bleiben – auch bei nur auszugsweiser Verwendung – vorbehalten.

Copyright © Herbert Utz Verlag GmbH · 2004

ISBN 3-8316-0331-6

Printed in Germany

Herbert Utz Verlag GmbH, München

089-277791-00

www.utzverlag.de

Inhalt

1	EINLEITUNG	1
1.1	Motivation der Arbeit	1
1.2	Gliederung der Arbeit	3
2	DIE FEHLERANALYSE BEIM KONFORMITÄTSTEST FELDBUSFÄHIGER AUTOMATISIERUNGSGERÄTE	5
2.1	Offene Feldbussysteme in der Automatisierungstechnik	5
2.1.1	Einordnung des Feldbusses in die Domäne der Automatisierungstechnik	5
2.1.2	Strukturierung offener Kommunikation nach dem ISO/OSI-Referenzmodell	9
2.1.3	Offene Feldbussysteme und ihre Einordnung in das ISO/OSI-Referenzmodell	12
2.1.4	Nutzen und Verbreitung offener Feldbussysteme	13
2.2	Der Konformitätstest feldbusfähiger Automatisierungsgeräte	14
2.2.1	Der Begriff des Konformitätstests	15
2.2.2	Die Bedeutung des Konformitätstests aus Anwender- und Herstellersicht	15
2.2.3	Vergleich paarweiser Test und Test gegen Testreferenz	17
2.2.4	Klassifizierung des Konformitätstests nach den durchführenden Parteien	18
2.2.5	Der Konformitätstest durch unabhängige Prüfinstitutionen	20
2.3	Methoden und Grenzen des Konformitätstests	21
2.3.1	Formaler Ablauf des Konformitätstests	21
2.3.2	Standardisierte Methoden des Konformitätstests	22
2.3.3	Grenzen des Konformitätstests	24
2.4	Die Analyse von Kommunikationsverhalten	27
2.4.1	Motivation für eine Analyse von Kommunikationsverhalten	27
2.4.2	Eingrenzung des Anwendungsbereichs der Fehleranalyse	28
2.4.3	Anforderungen an das Ergebnis der Fehleranalyse	29
2.4.4	Voraussetzungen für den Durchführenden der Fehleranalyse	30
2.4.5	Begriffsdefinitionen und Zusammenfassung	31
2.5	Resultierende Problemstellung	34
2.5.1	Mangelnde Verfügbarkeit von Prüfexpertise	34
2.5.2	Auswirkungen mangelnder Verfügbarkeit von Prüfexpertise	35
2.5.3	Bedarf nach einer einheitlichen Fehlerbeschreibung	36

2.5.4	Aufgabenstellung	37
3	METHODEN FÜR SPEZIFIKATION, TEST UND FEHLERANALYSE ZUSTANDSAUTOMATENBASIERTER PROTOKOLLE	39
3.1	Modellierungskonzept und Spezifikationsform von Protokollen	39
3.1.1	Abgrenzung zwischen Modellierungskonzept und Spezifikationsform	40
3.1.2	Das Modellierungskonzept der erweiterten endlichen Zustandsautomaten	41
3.1.3	Formale Spezifikationsformen für zustandsautomatenbasierte Protokolle	44
3.1.4	Nutzen und Anwendung formaler Spezifikationsformen	46
3.1.5	Modellierungskonzept und Spezifikationsform bei der Fehleranalyse	47
3.2	Test zustandsautomatenbasierter Kommunikationsprotokolle	48
3.2.1	Verfahren der Testfallermittlung	48
3.2.2	Methoden des Konformitätstests nach IS 9646	51
3.2.3	Realisierung von Konformitätstest und Fehleranalyse mit Prüfsystemen	54
3.2.4	Nutzen von Testmethoden für die Fehleranalyse	56
3.3	Formale Beschreibungstechniken beim Konformitätstest	56
3.3.1	Formale Beschreibungssprachen für Testfälle	57
3.3.2	Techniken zur formalen Datenbeschreibung	59
3.3.3	Kodierungsregeln und ihre formale Beschreibung	61
3.3.4	Bewertung der untersuchten formalen Beschreibungstechniken	63
3.4	Bewertung von Analyseverfahren	63
3.4.1	Analyseverfahren	64
3.4.2	Strukturmodelle und Funktionale Modelle bei Test und Fehleranalyse	65
3.4.3	Fehlermodelle bei zustandsautomatenbasierten Kommunikationsprotokollen	67
3.4.4	Anwendung von Analyseverfahren bei Feldbussystemen	68
3.5	Zusammenfassende Bewertung	69
4	EINE METHODE FÜR DIE RECHNERGESTÜTZTE FEHLERANALYSE	71
4.1	Ein Modellierungskonzept für Kommunikationsverhalten	71
4.1.1	Erweiterte endliche Zustandsautomaten	71
4.1.2	Ableiten endlicher Zustandsautomaten aus erweiterten Automaten	72
4.1.3	Definition endlicher Zustandsautomaten	77
4.1.4	Eigenschaften endlicher Zustandsautomaten	81
4.1.5	Fehlermodell für indeterministische endliche Zustandsautomaten	83
4.1.6	Grenzen einer Fehleranalyse und Zusammenfassung	84

4.2	Anforderungen an eine Fehlerdiagnose	86
4.2.1	Fehlerdiagnose bei Beobachtbarkeit von Zuständen	86
4.2.2	Eine Fehlerdiagnose mit günstiger Annahme von Zuständen	88
4.2.3	Identifizierbarkeit der zutreffenden Fehlerdiagnose	91
4.2.4	Kritische Bewertung der Ergebnisse und weiteres Vorgehen	94
4.3	Das Konzept einer vollständigen Fehlerdiagnose	95
4.3.1	Vollständige Fehlerdiagnose bei einer Eingabe und einer Ausgabe	96
4.3.2	Vollständige Fehlerdiagnose bei einer Folge von Ein- und Ausgaben	99
4.3.3	Graphische Beschreibung der vollständigen Fehlerdiagnose	101
4.3.4	Erweiterung um erwartetes Kommunikationsverhalten	103
4.4	Eine Fehleranalyse auf Basis von Testfällen	104
4.4.1	Motivation für eine testfallbasierte Fehleranalyse	105
4.4.2	Ermittlung der vollständigen Fehlerdiagnose aus einem Testfall	105
4.4.3	Ausführbarkeitsbedingung von Testfällen mit Zustandsangaben	108
4.4.4	Ein Verfahren für die Reduktion von Testfällen	109
4.4.5	Ermittlung der Folge beobachteter Ausgaben	109
4.4.6	Übersicht über das Lösungskonzept und weiteres Vorgehen	110
4.5	Formalisierung von Fehlerdiagnose und Testfall	111
4.5.1	Definition elementarer Bestandteile von Fehlerdiagnose und Testfall	111
4.5.2	Der Bezeichnungsoperator	114
4.5.3	Der Schritt als elementarer Bestandteil von Fehlerdiagnose und Testfall	115
4.5.4	Aggregation von Schritten	117
4.5.5	Definition der vollständigen Fehlerdiagnose	120
4.5.6	Definition des vollständigen Testfalls	123
4.5.7	Definition von reduziertem Testschritt und reduziertem Testfall	124
4.6	Algorithmen für eine testfallbasierte Fehleranalyse	127
4.6.1	Definition der Ausführbarkeitsbedingung	127
4.6.2	Algorithmus zur Ermittlung des reduzierten Testfalls	128
4.6.3	Algorithmus zur Ermittlung der Ausgabefolge y	130
4.6.4	Algorithmus zur Ermittlung der vollständigen Fehlerdiagnose	132
4.7	Zusammenfassung	133
5	DEFINITION UND ANWENDUNG EINER FORMALEN SPRACHE FÜR DIE FEHLERANALYSE	135
5.1	Bewertung formaler Beschreibungstechniken	135
5.1.1	Formale Sprachen	135

5.1.2	Anforderungen an die Beschreibungssprache und ihre Metasprache	137
5.1.3	Bewertung formaler Beschreibungstechniken	138
5.1.4	Motivation für die erweiterbare deklarative Sprache XML	141
5.2	Definition einer XML-basierten Beschreibungssprache	142
5.2.1	Syntaxdefinition mit XML-Schemas	143
5.2.2	XML-Schemadefinition von Schritten und ihrer Aggregation	146
5.2.3	XML-Schemadefinition von Fehlerdiagnose und vollständigem Testfall	150
5.2.4	XML-Schemadefinition von reduziertem Testfall und Testschritt	152
5.2.5	XML-Schemadefinition einer Testreihe	154
5.2.6	XML-Schemadefinition für schichtenorientierte Feldbussysteme	155
5.2.7	Strukturierung der XML-Schemadefinition	158
5.3	Konzept der Feldbusadaption	160
5.3.1	Herausforderungen bei der Realisierung von Test und Fehleranalyse	160
5.3.2	Der Upper Tester beim Konformitätstest feldbusfähiger Geräte	161
5.3.3	Der Lower Tester beim Konformitätstest feldbusfähiger Geräte	164
5.3.4	Konzept der Feldbusadaption bei der Erzeugung ablauffähiger Testfälle	166
5.3.5	Konzept der Feldbusadaption bei der Fehleranalyse	168
5.4	Konzept der Prüfsystemadaption	170
5.4.1	Erzeugung ablauffähiger Testfälle	171
5.4.2	Unvollständig spezifizierte PDUs	172
5.4.3	Erzeugung ablauffähiger Testfälle mit Behandlung unvollständiger PDUs	174
5.4.4	Informationsbereitstellung für die Erzeugung der Fehlerbeschreibung	176
5.5	Zusammenfassung	178
6	PROTOTYPISCHE REALISIERUNG EINER RECHNERGESTÜTZTEN FEHLERANALYSE	181
6.1	Realisierung von Algorithmen zur Fehleranalyse	182
6.1.1	Einführung in das Document Objekt Model (DOM)	182
6.1.2	Realisierung Algorithmus zur Ermittlung des reduzierten Testfalls	186
6.1.3	Realisierung Algorithmus zur Ermittlung der Folge beobachteter Ausgaben	188
6.1.4	Realisierung Algorithmus zur Ermittlung der vollständigen Fehlerdiagnose	190
6.2	Realisierung der Feldbusadaption	191
6.2.1	Kodier- und Dekodierfunktionalität auf Basis formaler Beschreibung	191
6.2.2	Herausforderungen aus einer beschreibungsbasierten Kodierfunktionalität	194
6.2.3	Erzeugung von feldbusspezifischen XML-Schemadefinitionen aus ASN.1	195
6.2.4	Zusammenfassender Überblick über die Realisierung der Feldbusadaption	196

6.3	Realisierung der Prüfsystemadaption	197
6.3.1	Konzept für die Erzeugung ablauffähiger Testfälle	197
6.3.2	Verarbeitung eines reduzierten Testfalls	199
6.3.3	Verarbeitung eines reduzierten Testschritts	201
6.4	Rechnergestützte Fehleranalyse am Beispiel PROFIBUS	203
6.4.1	Übersicht über die Durchführung der rechnergestützten Fehleranalyse	203
6.4.2	Ausschnitt aus dem erweiterten endlichen PROFIBUS-Zustandsautomaten	205
6.4.3	Ableiten von endlichen Zustandsautomaten	207
6.4.4	Beispiel eines Testfalls für einen indeterministischen Zustandsautomaten	210
6.4.5	Fehleranalyse bei einem indeterministischen Zustandsautomaten	211
6.4.6	Beispiel eines Testfalls für einen deterministischen Zustandsautomaten	214
6.4.7	Fehleranalyse bei einem deterministischen Zustandsautomaten	215
6.5	Abschließende Bewertung der prototypischen Realisierung	217
7	ZUSAMMENFASSUNG UND AUSBLICK	219
7.1	Zusammenfassung	219
7.2	Ausblick	221
ANHANG A 1 :	LITERATUR	223
ANHANG A 2 :	XML-SCHEMA TESTSUITE.XSD	239
ANHANG A 3 :	XML-SCHEMA TESTCASE.XSD	240
ANHANG A 4 :	XML-SCHEMA DIAGNOSIS.XSD	241
ANHANG A 5 :	XML-SCHEMA STEP.XSD	242
ANHANG A 6 :	XML-SCHEMA RTESTCASE.XSD	243
ANHANG A 7 :	XML-SCHEMA RSTEP.XSD	244
ANHANG A 8 :	ASN.1-BESCHREIBUNG DER PROFIBUS-ASPS	245
ANHANG A 9 :	XML-SCHEMA DER PROFIBUS-ASPS	246
ANHANG A 10 :	ASN.1-BESCHREIBUNG VON ASP-TYPEN	247

ANHANG A 11 : XML-SCHEMA DER PROFIBUS-ASP-TYPEN	248
--	------------

ANHANG A 12 : ECN-BESCHREIBUNG DER KODIERUNG VON PDUS	249
--	------------

1 Einleitung

Die Feldbustechnik hat sich in den vergangenen Jahren zur Schlüsseltechnologie in der Automatisierungstechnik entwickelt. Dabei kommt insbesondere den offenen Feldbussystemen, die dem Anwender der Technologie die freie Wahl des Lieferanten von Automatisierungsgeräten ermöglichen, eine herausragende Bedeutung zu. Die Kommunikation in offenen Feldbussystemen stellt eine besondere Herausforderung dar, weil die Verantwortung für die Funktionalität einer automatisierungstechnischen Anlage nicht bei einem Gerätehersteller allein, sondern bei der Gesamtheit aller Hersteller liegt, deren Produkte gemeinsam eine Automatisierungsaufgabe erfüllen. Eine wichtige Voraussetzung zur korrekten Kommunikation im Sinne der Kommunikationsspezifikation besteht darin, dass jedes mit anderen Automatisierungsgeräten über den Feldbus in Kommunikation tretende Gerät über eine Feldbusschnittstelle verfügt, welche die Anforderungen der Kommunikationsspezifikation erfüllt.

Für die Prüfung dieser sogenannten *Konformität* zur Kommunikationsspezifikation kommt dem *Konformitätstest* eine hohe Bedeutung zu, weil bei seiner Durchführung ein von der Kommunikationsspezifikation abweichendes Kommunikationsverhalten (*inkonformes* oder *fehlerhaftes Kommunikationsverhalten*, auch kurz als *Fehler* bezeichnet) erkannt werden kann. Der Konformitätstest kann bereits während der Geräteentwicklung (*entwicklungsbegleitender Konformitätstest*) oder am Ende der Geräteentwicklung (*entwicklungsabschließender Konformitätstest*) durchgeführt werden. Während der entwicklungsbegleitende Konformitätstest typischerweise durch den Entwickler selbst durchgeführt wird, wird der entwicklungsabschließende Konformitätstest häufig von speziell dafür eingerichteten Prüfinstitutionen wahrgenommen. Im Fall, dass ein inkonformes Kommunikationsverhalten beobachtet worden ist, soll das Resultat des Konformitätstests gleichzeitig Grundlage für eine Korrektur des getesteten Geräts sein.

Die Frage nach der Gestaltung des Konformitätstests, damit dieser nicht nur dazu dient, ein inkonformes Kommunikationsverhalten zu erkennen, sondern gleichzeitig eine geeignete Grundlage für die Korrektur des getesteten Automatisierungsgeräts bildet, steht im Mittelpunkt dieser Arbeit. Die Aufgabenstellung der Arbeit wird im folgenden Unterkapitel motiviert, Unterkapitel 1.2 stellt die Gliederung der Arbeit vor.

1.1 Motivation der Arbeit

Grundlage für eine Korrektur der Kommunikationsschnittstelle ist eine detaillierte Erklärung dafür, warum ein fehlerhaftes Kommunikationsverhalten beobachtet worden ist. Dazu ist das tatsächliche Kommunikationsverhalten des zu prüfenden Geräts einer Analyse zu

unterziehen, die zu einer Gegenüberstellung von beobachtetem und erwartetem Kommunikationsverhalten führt und so die Abweichungen zwischen beidem deutlich macht.

Voraussetzungen für eine derartige *Analyse von Kommunikationsverhalten* sind einerseits detaillierte Kenntnisse der Kommunikationsspezifikation, durch die das geforderte Kommunikationsverhalten definiert wird, und andererseits ein genaues Wissen über den Konformitätstest selbst, der festlegt, welches Detail der Kommunikationsspezifikation auf welche Weise getestet wird. Beide Voraussetzungen werden in der Regel nur von ausgewiesenen Prüfexperten erfüllt, was zur Folge hat, dass die auf einer Analyse basierende Korrektur der Kommunikationsschnittstelle in den meisten Fällen nur mit Unterstützung durch Prüfexperten möglich ist.

Prüfexperten sind typischerweise in speziellen Prüfinstitutionen tätig, in denen ein entwicklungsabschließender Konformitätstest angeboten wird. Während der Geräteentwicklung, bei welcher der entwicklungsbegleitende Konformitätstest der Kommunikationsschnittstelle nur eine von vielen Aufgabenstellungen ist, kann in der Regel eine entsprechende Prüfexpertise nicht aufgebaut werden. Somit wird der Geräteentwickler bei der zur Korrektur des getesteten Geräts notwendigen Analyse des Kommunikationsverhaltens in den meisten Fällen auf externe Prüfexpertise angewiesen sein, auch wenn er zur Durchführung des Konformitätstests allein in der Lage ist. Dies führt dazu, dass Geräteentwickler den Konformitätstest meist erst am Ende einer Geräteentwicklung durch Prüfexperten durchführen lassen. Auf entwicklungsbegleitende Konformitätstests in frühen Phasen der Geräteentwicklung, durch die fehlerhaftes Kommunikationsverhalten frühzeitig erkannt und korrigiert werden könnte, wird häufig verzichtet.

Unzureichend vorab getestete Geräte zeigen beim entwicklungsabschließenden Konformitätstest eine Vielzahl von Fehlern, was wiederum zu erheblichem Aufwand für Nachbesserungen beim Geräteentwickler führt. Nachgebesserte Geräte werden erneut durch Prüfexperten dem Konformitätstest unterzogen, wodurch zusätzlich Aufwand durch wiederholte Konformitätstests entsteht.

Selbst für erfahrene Prüfexperten ist die Analyse von Kommunikationsverhalten ein sehr arbeits- und zeitintensiver Vorgang. Geräte mit vielen Fehlern führen zwangsläufig zu hohem zeitlichen und personellen Aufwand seitens der Prüfexperten. Bei gleichzeitig knapper Verfügbarkeit von Prüfexpertise ergeben sich bei den entsprechenden Prüfinstitutionen lange Wartezeiten bis zur Durchführung eines Konformitätstests. Der entwicklungsabschließende Konformitätstest, der typischerweise am Ende des kritischen Pfades eines Entwicklungsprojekts liegt, kann damit die Markteinführung eines Automatisierungsgeräts in gravierender Weise verzögern.

Durch das skizzierte Szenario wird die Aufgabenstellung dieser Arbeit motiviert, die darauf fokussiert, eine neue Form der Analyse des Kommunikationsverhaltens felddbusfähiger

Automatisierungsgeräte zu finden, die mit Hilfe von Rechnerwerkzeugen erfolgt und damit weitgehend unabhängig von Prüfexpertise ist.

Damit ergeben sich neue Szenarien beim entwicklungsbegleitenden und beim entwicklungsabschließenden Konformitätstest: Der Entwickler eines Automatisierungsgeräts ist für die zur Korrektur notwendige Analyse eines fehlerhaften Kommunikationsverhaltens nicht mehr auf Prüfexperten angewiesen. Damit bietet der entwicklungsbegleitende Konformitätstest verbunden mit der rechnergestützten Analyse einen weitaus größeren Nutzen für den Geräteentwickler als der Konformitätstest allein. Dieser Nutzen lässt erwarten, dass vermehrt entwicklungsbegleitende Konformitätstests durchgeführt werden und die Anzahl der im Rahmen des entwicklungsabschließenden Konformitätstests erkannten Fehler sinkt. Weniger Fehler beim entwicklungsabschließenden Konformitätstest wiederum verringern die Anzahl von Nachbesserungen und wiederholten Konformitätstests einerseits und die Zeitdauer eines Testvorgangs andererseits. Beim entwicklungsabschließenden Test wird der Prüfexperte durch eine rechnergestützte Analyse des Kommunikationsverhaltens entlastet, wodurch zusätzlich eine Reduzierung von zeitlichem und personellem Aufwand bei den Prüfinstitutionen verbunden ist.

Als Konsequenz der skizzierten Szenarien verringern sich Wartezeiten bei Prüfinstitutionen, und das Risiko einer durch fehlerhaftes Kommunikationsverhalten bedingten Verzögerung bei der Markteinführung eines Automatisierungsgeräts sinkt.

1.2 Gliederung der Arbeit

Die Arbeit ist wie folgt gegliedert: Kapitel 2 ordnet die Feldbustechnologie in die Domäne der Automatisierungstechnik ein, zeigt die Bedeutung des Konformitätstests feldbusfähiger Automatisierungsgeräte und motiviert die rechnergestützte Analyse des Kommunikationsverhaltens als Aufgabenstellung dieser Arbeit. Ferner dient Kapitel 2 der Einführung der in der Arbeit verwendeten Terminologie. Im anschließenden Kapitel 3 werden unterschiedliche Methoden und Technologien aus den Gebieten Spezifikation, Test und Fehleranalyse von Kommunikationsprotokollen vorgestellt und im Hinblick auf ihre Eignung zur Bearbeitung der Aufgabenstellung bewertet.

Kapitel 4 stellt den Lösungsansatz für die rechnergestützte Analyse des Kommunikationsverhaltens feldbusfähiger Automatisierungsgeräte vor. Grundlage des Lösungsansatzes sind Testfälle, die im Rahmen des Konformitätstests bei Automatisierungsgeräten mit zustandsautomatenbasierten Feldbusprotokollen durchgeführt werden. In Kapitel 5 wird die konzeptionelle Umsetzung des Lösungsansatzes mit Hilfe von Techniken der formalen Sprachen erarbeitet. Dazu wird einerseits eine Sprache definiert, mit der erwartetes wie auch beobachtetes Kommunikationsverhalten beschrieben werden können, und andererseits die Integration des Lösungsansatzes in die Methoden des Konformitätstests erläutert.

Die prototypische Realisierung des Konzepts wird in Kapitel 6 exemplarisch anhand des Feldbussystems PROFIBUS gezeigt. Abschließend fasst Kapitel 7 die Ergebnisse zusammen und gibt einen Ausblick auf weitere Arbeiten.

Textpassagen in kleiner Schriftgröße dienen einer vertiefenden Betrachtung, indem ein Sachverhalt ausführlich und häufig unter Zuhilfenahme von Beispielen diskutiert wird. Zusammenfassungen von Ergebnissen, die für die Arbeit von besonderer Bedeutung sind, werden durch kursive Schrift und in grauem Rahmen hervorgehoben.