István Péter

# Monitoring-Kalkül für feldbusbasierte Automatisierungssysteme

Herausgegeben von

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

in der Reihe

**Informationstechnik im Maschinenwesen**

Herbert Utz Verlag · München
2006

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.



ISBN 3-8316-0587-4

Printed in Germany

Herbert Utz Verlag GmbH, München
089-277791-00
www.utzverlag.de

# Vorwort

Die vorliegende Arbeit entstand während meiner Tätigkeit als wissenschaftlicher Mitarbeiter am Lehrstuhl für Informationstechnik im Maschinenwesen an der Technischen Universität München.

Diese Arbeit reflektiert die vielseitigen Erfahrungen, Ergebnisse des Projektes „Diagnose-Monitor“. In diesem Zusammenhang möchte ich mich meinem Doktorvater, Herrn Prof. Dr.-Ing. Klaus Bender, für die vielfältige Unterstützung im Vorfeld und bei der Erstellung dieser Arbeit bedanken. Auch für seine Bemühungen Firmenkontakte herzustellen, die zum Gelingen dieser Arbeit erheblich beigetragen haben, möchte ich Ihm danken.

Für die Übernahme des zweiten Gutachtens bin ich Prof. Dr.-Ing. habil. Martin Wollschlaeger von der Technischen Universität Dresden zu Dank verbunden.

Für hilfreiche Kommentare zu frühen Versionen dieser Arbeit gebührt besonderer Dank meinen Kollegen Martin Pöschl und Sven Dominka.

Auch den Mitarbeitern des PROFIBUS-Zertifizierungslabors, Johannes Werner und Maik Straßner, möchte ich für Ihre freundliche Unterstützung und für die Überlassung von Testkomponenten danken. Weiterhin für ihr reges Interesse und Zusammenarbeit an der Weiterentwicklung des gesamten Softwaresystems und den in Ihren Labors durchgeführten Tests.

Dank gebührt auch an dieser Stelle Herrn Andor Nagy, der mit Rat und Tat bei der Erstellung von ersten Hardware-Prototypen dabei war, sowie auch an allen meinen Kollegen und Kolleginnen, die mich direkt oder indirekt unterstützt haben.

Nicht zuletzt bedanke ich mich bei allen meinen Bekannten, meiner Mutter und meiner Tochter für die Geduld, die sie während der Erstellung dieser Arbeit mit mir hatten.

München, den 01.12.2005

István Péter

## Inhalt

# 1 Einleitung

Seit Mitte der 80er Jahren ist in der Automatisierungstechnik ein grundlegender qualitativer Sprung zu beobachten: die konventionelle Parallelverdrahtung kann dem Bedürfnis nach komplexer Kommunikation aufgrund zunehmend intelligent werdender Feldgeräte nicht mehr nachkommen. Deswegen wird sie Zug um Zug durch die modernere Feldbustechnik verdrängt. Als Schlüsseltechnologie der Automatisierungstechnik bietet die Feldbustechnik eine Reihe von Bussystemen, die durch die Offenlegung der Spezifikation die Voraussetzungen für die Entstehung von Anlagen schaffen, die aus intelligenten Feldgeräten von mehreren Herstellern aufgebaut sind und meist die Präsenz von mehreren Bussystemen erfordern (vgl. Abbildung 1).

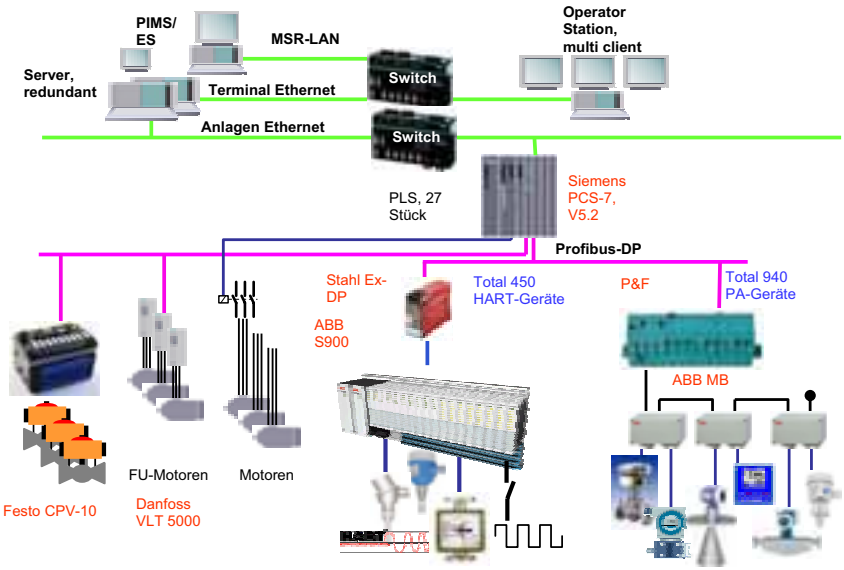


**Abbildung 1: Beispiel für eine moderne Anlage mit mehreren Bussystemen**

In solchen Anlagen werden die auf dem ersten Blick so überzeugend klingenden Vorteile der Feldbustechnik wie Flexibilität, vereinfachte Inbetriebnahme und Instandhaltung, größere Anlagenverfügbarkeit in der Praxis von einer aufwändigen Fehlersuche überschattet. Die häufigste Fehlerquellen sind dabei zum einen schwer reproduzierbare Fehler [RÖM04] in der hochkomplexen, kaum debugbaren Kommunikations-Software der Feldgeräte, die während der Zertifizierungsphase nicht erkannt wurden, zum anderen die Nichterfüllung der Anforderung an das Kommunikationssystem, die von immer komplexer werdenden technischen Prozessen gestellt werden. In diesem Kontext ist das etablierte Verfahren für die Fehlersuche im Kommunikationsverhalten der Einsatz von speziellen Werkzeugen für passive Messun-

gen/Aufzeichnungen im laufenden Betrieb, welche meist als Monitore bezeichnet werden. Die am Markt verfügbaren Monitore haben die Einschränkung, dass sie das beobachtbare Kommunikationsverhalten der Feldgeräte aus der Anlage nicht gegen das Sollverhalten, was meist in Form einer offen gelegten Spezifikation vorliegt, verifizieren können. Hierdurch entsteht ein beträchtliches Maß an manueller Prüfarbeit. Im Umkehrschluss besteht also ein gigantisches Potential, eine sehr ineffiziente manuelle Suchtätigkeit zu automatisieren. Im Mittelpunkt der vorliegenden Arbeit steht die Frage nach einer geeigneten Methodik zur Vereinfachung der Fehleranalyse mittels passiver Beobachtung unter der Berücksichtigung einer vorhandenen Protokollspezifikation. Die Aufgabenstellung dieser Arbeit, wird im folgenden Unterkapitel motiviert, Unterkapitel 1.2 stellt die Gliederung der Arbeit vor.

## *1.1 Motivation und Zielsetzung*

Das Auffinden und Beheben von Fehlern gehört zu den zeitraubendsten Tätigkeiten während der Entwicklung und in den späteren Phasen des Lebenszyklus der Kommunikationssoftware für die Feldgeräte. Die so genannte Fehleranalyse kann oft ein dominanter Kostenfaktor werden. Verschärft wird dieses Problem durch die eingeschränkte, passive Beobachtbarkeit der Feldgeräte, wenn diese nach einem erfolgreich bestandenen Konformitätstests als Teile einer hochkomplexen Automatisierungsanlage, deren Ausfall sehr schnell kostspielig werden kann, vorliegen. Weitere Probleme können durch die örtliche Verteilung des für die Fehleranalyse notwendigen Expertenwissens und durch eine sehr geringe Kooperationsbereitschaft entstehen, dessen Grund auf die Tatsache zurückzuführen ist, dass die heutigen Anlagen oft, wegen der eingesetzten offenen Feldbussysteme aus Feldgeräten von mehreren, örtlich entfernten Herstellern aufgebaut werden können. Trotz dieser ökonomischen Bedeutung sind in der Fehleranalyse im Bereich der Feldbuskommunikation nur wenige Fortschritte zu verzeichnen – wie vor 20 Jahren basiert die Praxis im Wesentlichen auf ineffizienten, händischen Verfahren der Fehlersuche und auf „Versuch und Irrtum“ in einem sehr großen Zustandsraum der heutigen Feldbusspezifikationen.

In dieser Arbeit werden zwei Hauptziele verfolgt, die jeweils einen Beitrag zur Automatisierung der Fehleranalyse der passiv beobachtbaren Kommunikationsabläufe leisten sollen. Zum einen wird die wesentliche Erweiterung der Funktionalität eines Monitors gegenüber dem derzeit verfügbaren Produkte um eine effiziente, einfach erlernbare Beschreibung der analysierenden Eigenschaften von beobachtbaren Kommunikationsabläufen angestrebt, die die Möglichkeit zur effizienten Ablegung und Wiederverwendung des Expertenwissens unterstützen soll. Eine solche Beschreibung ist unabdingbar für die Automatisierung der Fehleranalyse, und soll als Grundlage für ein möglichst effizientes Analyseverfahren dienen. Die grundsätzlichen Vorteile einer derartigen Erweiterung der Monitore gegenüber dem aktiven Test, in dem ein Testsystem die Rolle eines oder eventuell mehrerer Kommunikationspartners emuliert, sind:

- Ein erweiterter Monitor kann während der Entwicklung als Testorakel[1] verwendet werden. Damit kann die Auswertung der Testergebnisse effizienter durchgeführt werden.

- Ein passives, rückwirkungsfreies Analyseverfahren kann unter genau den Bedingungen eingesetzt werden, unter denen auch der Betrieb der Automatisierungsanlage stattfindet. Dadurch erhöht sich die Wahrscheinlichkeit sporadische Betriebsstörungen, die während des Langzeitbetriebes auftreten, zu erfassen. Wenn ein installiertes Feldbussystem zwar gelegentliche Störungen aufweist, seinen Betriebszweck aber noch im Großen und Ganzen erfüllen kann, ist es vorteilhaft, die Fehlersuche ohne kostspielige Betriebsunterbrechung durchführen zu können.

- In der Praxis kommt es oft vor, dass die Interoperabilität zwischen Komponenten verschiedener Hersteller gestört ist, obwohl beide Hersteller eine Zertifizierung ihrer Geräte vorweisen und zwischen Geräten desselben Herstellers keine Probleme auftreten. In solchen Situationen kann voraussichtlich die erweiterte Analysefähigkeit des Monitors zu einer Reduzierung der Ermittlungszeit der verursachenden Komponente beitragen.

- In Feldbusprotokollen müssen einige, vom Standard offen gelassene Parameter vom Anwender bei der Inbetriebnahme festgelegt werden, um die Anforderungen des technischen Prozesses erfüllen zu können. Durch solche Konfigurationseinstellungen können schwer nachvollziehbare Probleme auftreten, die auf die Interaktion verschiedener Komponenten zurückzuführen sind und beim aktiven Testen normalerweise unerkannt bleiben.

Das zweite Ziel der vorliegenden Arbeit, das als bedeutende technologische Unterstützung für das erste Ziel überlegt wurde, ist die Ableitung von verifizierenden Eigenschaften direkt aus der Protokollspezifikation mit Hilfe der heute verfügbaren fortschrittlichen Techniken aus dem Bereich der Constraint-Programmierung und der automatischen Invarianten-Generierung. Die so abgeleiteten Eigenschaften können als eine erste Überapproximation des erlaubten beobachtbaren Kommunikationsverhaltens betrachtet werden, die später, um eine größere Genauigkeit zu erreichen, manuell mit anderen, effizient beobachtbaren Eigenschaften ergänzt werden sollten, die teilweise aus der Protokollspezifikation und teilweise aus den Anforderungen des technischen Prozesses abzuleiten sind.

[1] Ein Testorakel ist eine (idealisierte) Informationsquelle, die bei Eingabe eines Testfalles die korrekte(n) Reaktion(en) bzw. Sollwerte liefert. Der Idealfall wäre ein vollständig rechnergestütztes Testorakel. In der Praxis muss diese Aufgabe oft ein Mensch erledigen, der dieses Wissen z.B. aus der Anforderungsdefinition ableitet.

## 1.2 Gliederung der Arbeit

Um das beschriebene Problemfeld wirkungsvoll bearbeiten zu können, wird im Kapitel 2 zunächst das Umfeld der Arbeit geschildert, die Problemstellung eingehend analysiert und auf die zugrunde liegenden technischen bzw. methodischen Defizite abgebildet. Ferner dient Kapitel 2 der Einführung der in der Arbeit verwendeten Terminologie. Im anschließenden Kapitel 3 werden die Funktionsmerkmale von kommerziell verfügbaren Feldbusmonitoren für die etablierten Feldbussysteme analysiert und bezüglich ihrer Tauglichkeit für die Aufgabenstellung bewertet. Ferner werden Methoden und Techniken aus dem Gebiet von Monitoring sowie von verwandten Gebieten vorgestellt und im Hinblick auf ihre Eignung zur Bearbeitung der Aufgabenstellung untersucht. Kapitel 4 stellt einen Lösungsansatz für das Monitoring von feldbusbasierten Automatisierungssystemen vor, gefolgt von einer exemplarischen Bewertung anhand des Feldbussystems PROFIBUS. Grundlage des Lösungsansatzes ist der datenflussorientierte Monitoring-Kalkül, dessen Ursprung in der linearen temporalen Logik liegt. Als technologische Hilfestellung zur praktischen Anwendung des Monitoring-Kalküls wird in Kapitel 5 ein constraintbasiertes Verfahren beschrieben, das zur Ableitung von effizient monitorisierbaren Sicherheitseigenschaften aus der Feldbusspezifikation dient. Ferner werden zwei fortschrittliche Techniken zur Invariantengenerierung bezüglich ihrer Eignung für die Ableitung von Sicherheitseigenschaften untersucht. Kapitel 6 fast anschließend die Ergebnisse zusammen und gibt einen Ausblick auf weitere Arbeiten, die auf den Erkenntnissen beruhen, die während der Durchführung dieser Arbeit entstanden sind.