Analyse des Antwortzeitverhaltens netzbasierter Automatisierungssysteme

Jürgen Greifeneder und Georg Frey, Technische Universität Kaiserslautern

Netzbasierte Automatisierungssysteme (NAS) sind das Ergebnis der zunehmenden Dezentralisierung von Automatisierungssystemen mittels neuerer Netzwerkstrukturen. Eine ganze Fülle von Einflussfaktoren führt jedoch zu einem Spektrum von nicht-deterministischen Verzögerungen, die direkten Einfluss auf Qualität, Sicherheit und Zuverlässigkeit der Automatisierungsanlagen haben. Eine genaue Analyse dieser Einflussfaktoren ist somit nicht nur Voraussetzung für den verantwortungsbewussten Einsatz dieser Technologie sondern ermöglicht es auch, bereits im Vorfeld von Umstrukturierungen oder Erweiterungen Fragen der Verlässlichkeit zu klären. In diesem Beitrag wird gezeigt, welchen Einfluss einzelne Komponenten sowie netzbedingte Verhaltensmodi wie Synchronisation und die gemeinsame Nutzung von Ressourcen auf die Antwortzeiten des Gesamtsystems haben. Zur Analyse wird die wahrscheinlichkeitsbasierte Modellverifikation (PMC) verwendet. Umfangreiche Messungen wurden zur Validierung der Ergebnisse durchgeführt.

Netzbasierte Automatisierungssysteme (NAS) / Verteilte Steuerungen / Netzwerke / Antwortzeit / Wahrscheinlichkeitsbasierte Modellverifikation / Fehler / Informationsverlust / Zugriffskonflikte

Response time analysis for Networked Automation Systems

Networked Automation Systems (NAS) result from the increasing decentralization of automation systems using new network structures. However, a bounteousness of influencing factors leads to a spectrum of non-deterministic delays which directly influence quality, safety and dependability of automated plants. Therefore, a detailed analysis of those influencing factors not only is prerequisite for a responsible application of this technology but also enables to check dependability related questions prior to restructuring, reengineering or expansion. This article details how single components as well as network induced behaviors like synchronization and the shared use of components influence the response times of the overall system. The analysis uses Probabilistic Model Checking (PMC) Measurements are presented to validate the results.

Networked Automation Systems / Distributed control systems / Distributed control / networks / Response time / Probabilistic model checking / Failure / Loss of information / Access conflict

Einleitung

Die Verlässlichkeitsanalyse von Automatisierungssystemen erfordert das aus Hard- und Software bestehende Gesamtsystem zu betrachten. Diese Herausforderung wird durch die Ausbreitung von Netzbasierten Automatisierungssystemen (NAS) erschwert, da bei NAS der Einfluss des Netzwerkes zusätzlich zu dem der einzelnen Komponenten für die Verhaltensbestimmung Berücksichtigung finden muss, denn das Netzwerk bringt nicht nur (anzunehmender Maßen nicht-deterministische) Verzögerungen in das System ein, sondern auch weitere zu berücksichtigende Arbeitszyklen und ausfallgefährdete Komponenten.

Unterschiedliche Arten von Verzögerungen müssen ebenso berücksichtigt werden wie ein möglicher Informationsverlust. Die damit einhergehenden neuen Problemstellungen lassen sich wie folgt kategorisieren:

1. werden manche Komponenten (z. B. Sensoren, Switches) von mehreren Benutzern verwendet. Hierdurch können Wartezeiten (und somit zusätzliche Verzögerungen) entstehen.
2. überlagern sich nicht synchronisierte zyklische Verhaltensmodi zu einem komplexen Gesamtverhalten.
3. bildet das Netzwerk eine eigenständige Quelle von Verzögerungen und potentiellen Informationsverlusten.
4. müssen auch die von herkömmlichen Systemarchitekturen bekannten Problemquellen, wie Ausfälle und Informationsinkonsistenzen berücksichtigt werden.

Moyne und *Tilbury* bedauern in [1], dass die Wissenschaft sich fast ausschließlich um die Analyse und Verbesserung der Netzübertragung kümmert, wobei die durch die einzelnen Komponenten verursachten Verzögerungen meist als vernachlässigbar angenommen werden. Die im vorliegenden Beitrag präsentierte Analyse zeigt jedoch analog zu Messungen in [1] und Simulationen in [2], dass in AT-Systemen das Komponentenverhalten entscheidend ist. Wichtig für das Verständnis des Systemverhaltens ist es demnach,

den Einfluss der einzelnen Komponenten auf das Gesamtsystem zu analysieren, wobei im Rahmen dieser Arbeit der Fokus auf SPS, Netz und I/O-Karten gelegt wird. Neben diesen tendenziell eher statischen Betrachtungen ist es von großem Nutzen, detaillierte Kenntnisse über den Einfluss des Ressource-Sharings (Netz, I/O-Karten, Sensoren, …) einerseits, als auch im Gesamtverhalten sich überlagernder, nicht synchronisierter, zyklischer Bearbeitungsvorgänge andererseits, zu besitzen.

In dem diesem Artikel vorangestellten Co-Beitrag (atp 9/2007 [3]) wurde die Beschreibungssprache DesLaNAS eingeführt sowie der zugehörige Modellierungsprozess kurz umrissen und ein kleines Anwendungsbeispiel präsentiert. DesLaNAS wurde entwickelt, um den speziellen an die Modellierung und Analyse von NAS gestellten Ansprüchen umfassend gerecht werden zu können. Zur Validierung der gewonnenen Ergebnisse wurde auf messtechnische Verfahren zurückgegriffen. Hierdurch konnte die Vergleichbarkeit der Ergebnisse dokumentiert und die Verwendung des vorgestellten Ansatzes gerechtfertigt werden.

Dieser Beitrag ist wie folgt gegliedert: Im folgenden Abschnitt wird noch einmal kurz auf die zu analysierenden und zu modellierenden Eigenschaften eingegangen. In Abschnitt 3 wird dann ein Anwendungsbeispiel eingeführt, mit dessen Hilfe in den folgenden Abschnitten die unterschiedlichen Artefakte diskutiert und analysiert werden. Abschnitt 4 diskutiert zunächst die Einflüsse zyklischen Verhaltens einzelner Komponenten auf das Gesamtsystem. In den Abschnitten 5 und 6 wird darauf aufbauend der Einfluss von Fehlern und Zugriffskonflikten analysiert. Abschnitt 7 erörtert den Aspekt des Informationsverlustes. Stochastisches Komponentenverhalten wird im 8. Abschnitt untersucht. In Abschnitt 9 werden schließlich unterschiedliche Zykluszeiten der SPS und ihres I/O-Boards analysiert und die Ergebnisse mit Labormessungen verglichen. Der Beitrag schließt mit einer kurzen Zusammenfassung und einem Ausblick auf zukünftige Arbeiten.

Temporale Eigenschaften

Ähnlich der in [4] vorgestellten Korrektheitsklassen lassen sich die mit Sicherheit und Performanz in Beziehung stehenden Fragestellungen auf wertbasierte (reagiert das System korrekt) und zeitbasierte (reagiert das System innerhalb der zulässigen temporalen Grenzen) Eigenschaften aufteilen. Während für die Untersuchung von wertbasierten Eigenschaften schon umfangreiche Analysemethoden zur Verfügung stehen, ist der temporale Bereich in der Automatisierungstechnik bisher wenig erforscht. Ein wichtiges Charakteristikum temporaler Fragestellungen ist es, dass nicht das System selbst analysiert wird, sondern die auf einem solchen System laufenden Prozesse. Der Wunsch nach Analyse eines Prozesses induziert jedoch, dass dieser selbst Mittelpunkt der Betrachtung werden muss und somit eine Mitverfolgung des Prozessablaufes auf dem System notwendig ist (Signal-Tracking). Zur Analyse temporaler Eigenschaften ist es daher einerseits notwendig, Modelle zu verwenden, die mit den unterschiedlichen Aspekten eines NAS umgehen können, wie z. B. Zeitverzögerungen, Nebenläufigkeit, deterministische Abhängigkeiten oder Stochastik. Andererseits bedarf es einer Methodik, die Antworten auf temporale Eigenschaften betreffende Fragen liefern kann. Charakteristisch daran ist, dass sich all diese Fragestellungen auf eine Kopplung von zeitlichen (reagiert das System innerhalb vorgegebener Zeitschranken) und stochastischen (mit welcher Wahrscheinlichkeit geschieht dies) Aspekten zurückführen lassen.

Stochastische Effekte treten in NAS in vier verschiedenen Formen auf:

1. erfordert in NAS auftretendes unvorhersagbares Verhalten, wie z.B. Paketverluste und Ausfälle, die Einbeziehung stochastischer Beschreibungsformen in die Modellierung.
2. gibt es in einem NAS Komponenten, wie z. B. das Netzwerk, dessen Abläufe zwar im Detail bekannt sind und daher problemlos modellierbar wären, in ihrer eigentlichen Funktion jedoch kaum vom betrachteten Prozess abhängig sind. Konsequenterweise lässt sich das Verhalten solcher Komponenten am besten durch stochastische Zeitverteilungen abstrahiert ins System einbringen.
3. finden stochastische Beschreibungsformen auch dort Anwendung, wo Konflikte auftreten. Dies ist z. B. der Fall, wenn zwei Komponenten nahezu gleichzeitig einen Dienst einer dritten Komponente anfordern.
4. kommt man auch dann nicht ohne stochastische Anteile aus, wenn keiner der vorgenannten Aspekte in der Modellierung berücksichtigt werden muss. Dies liegt daran, dass der Beginn einer Prozessbeobachtung selten mit dem Systemstart zusammenfällt, das System also schon am Laufen ist, wenn der zur Analyse anstehende Prozess beginnt. Da einerseits die einzelnen Komponenten eines NAS in der Regel nicht miteinander synchronisiert sind und andererseits Abläufe meist durch Sensoren physikalischer Prozesse (wie z. B. Bewegung, Temperatur) ausgelöst werden, ergibt sich der Systemzustand zum Auslösezeitpunkt als stochastische Größe, die bei der Analyse berücksichtigt werden muss. Aus diesem Grunde ist es – auch für Systeme, in denen die drei erstgenannten Effekte nicht auftreten – unerlässlich, stochastische Modelle wie DesLaNAS zu verwenden.

Anwendungsbeispiel

Als Anwendungsbeispiel soll ein aus mehreren Sensoren, Aktuatoren und SPSen bestehendes NAS Verwendung finden. Bild 1 zeigt schematisch den Aufbau des Systems. Die SPSen kommunizieren mit ihren SPS-I/O-Boards über einen Backplane-Bus. Die SPS-I/O-Boards ihrerseits fragen zyklisch (1: 17 ms, 2: 19 ms, 3: 17 ms) die zugewiesenen Anlagen-I/Os ab. In diesem Abfragetelegramm werden auch die neuen Stellwerte übermittelt. Die in Bild 1 verwendeten Farben – rot für die SPS, gelb für die SPS-I/O, grün für die Anlagen-I/O, blau für Sensoren und Stellglieder und grau für das Netzwerk – werden in den folgenden Bildern wieder aufgegriffen.

Die zu untersuchende Eigenschaft ist die Antwortzeit des Systems, wobei diskutiert werden soll, welchen Anteil die

unterschiedlichen NAS-Verhaltenseigenschaften Bearbeitung, Netzübertragung, Synchronisationseffekte, Zugriffskonflikte und Fehler haben. Als *Antwortzeit* gilt die Verzögerung zwischen einem Signalwechsel an einem Eingang des Systems und der Reaktion am Ausgang. Hierbei wird angenommen, dass der neue Signalwert am Eingang des Systems mindestens so lange ansteht, wie es zur Erfassung durch das System erforderlich ist.

Für die *Netzübertragung* wird eine Ethernet-UDP/IP-Übertragung angenommen, welche – wie Messungen am Lehrstuhl der Autoren gezeigt haben [5] – im Mittel 2 ms benötigt, wobei die Messwerte zwischen 1,5 und 2,5 ms streuen. Für die Analyse wird daher jede Netzwerkpassage mit 2 ms berücksichtigt. Da die in der Automatisierungstechnik eingesetzten Netzwerkkomponenten in der Regel sehr schnell und selten überlastet [6] sind, ist es zulässig jede der zu modellierenden Datenübertragungen als unabhängiges Modul zu instanziieren und Störeinflüsse wie Verlust, Stau und andere Übertragungsverzögerungen als getrennte Prozesse zu modellieren.

Als *Bearbeitungszeiten* gelten die Reaktionszeit der Anlagen-I/O (2 ms) sowie die Zykluszeiten der beteiligten SPSen (SPS1: 10 ms, SPS2: 11 ms und SPS3: 13 ms). Hierbei wird angenommen, dass die SPS in den untersuchten Szenarien die Reaktion auf einen geänderten Eingangswert innerhalb eines Zyklus berechnet (z. B. O1: = I1).

Synchronisationsverzögerungen werden durch die Überlagerung nicht synchronisierter Arbeitszyklen der SPSen sowie der SPS-I/O-Boards verursacht und ergeben sich als Differenz der berechneten Verzögerung des ungestörten und zugriffskonfliktfreien Falls („Grundzeit“) und der Summe aus Netzübertragung und Bearbeitungszeit.

Zugriffskonflikte kommen zustande, weil in NAS mehrere Komponenten auf ein und dieselbe Ressource zugreifen. Im Beispiel tritt ein Ressourcenkonflikt an jenen Anlagen-I/Os auf, die von verschiedenen SPS-I/Os angefragt werden. Der zugehörige Verzögerungsanteil wurde als Differenz aus der für den konfliktbehafteten Fall ermittelten Verzögerung und der Grundzeit ermittelt. Selbstverständlich unterscheidet sich diese Differenz von der tatsächlich auftretenden durchschnittlichen I/O-Wartezeit, da durch die erhöhte Wartezeit vor der Anlagen-I/O auch der Ankunftszeitpunkt an der SPS und folglich derjenige an der SPS-I/O verschoben wird (in den analysierten Beispielen war diese Größe stets etwas kleiner). Die hierbei zusätzlich auftretenden Verzögerungszeiten werden jedoch immer durch „Warten auf eine Ressource“ hervorgerufen. Somit ist die Unterscheidung zwischen Zugriffskonflikt und Synchronisation eher didaktischer Natur, um den Effekt einer Mehrbenutzerumgebung demonstrieren zu können.

Ähnliches gilt für durch *Fehler* hervorgerufene Verzögerungen. Diese werden insofern analog zu Zugriffskonflikten behandelt, als dass die durch Fehler im Mittel zusätzlich zur Grundzeit auftretende Verzögerungszeit als Fehlerverzögerung benannt wird.

Synchronisation zyklischer Prozesse

Im Folgenden soll zunächst das Grundsystem betrachtet werden. Dieses bestehe lediglich aus einer SPS, der zugehörigen SPS-I/O, dem ungestörten Netzwerk und einer Anlagen-I/O samt Sensor und Stellglied. Die Antwortzeit ergibt sich aus dem in Bild 2 gezeigten GANTT-Chart, welches statt nach Komponenten nach den zuvor eingeführten Anteilsklassen aufgeteilt ist. Nachdem sich der Sensorwert ändert, wartet die Anlagen-I/O zunächst auf die nächste Anfrage der SPS-I/O. Trifft diese ein, erstellt die Anlagen-I/O ein Antworttelegramm. Dieses geht über das Netz zur SPS-I/O und wird von dort über den Backplane-Bus direkt in den Eingangspuffer der SPS geschrieben. Nun wird auf den nächsten Lesevorgang der SPS gewartet. Nach dem Lesen wird der Wert in der SPS verarbeitet und eine Reaktion berechnet. Diese geht wieder zur SPS-I/O und wartet dort auf den nächsten Sendevorgang. Danach erfolgt ein erneuter Netzdurchgang und eine Bearbeitung des Telegramms in der Anlagen-I/O. Das

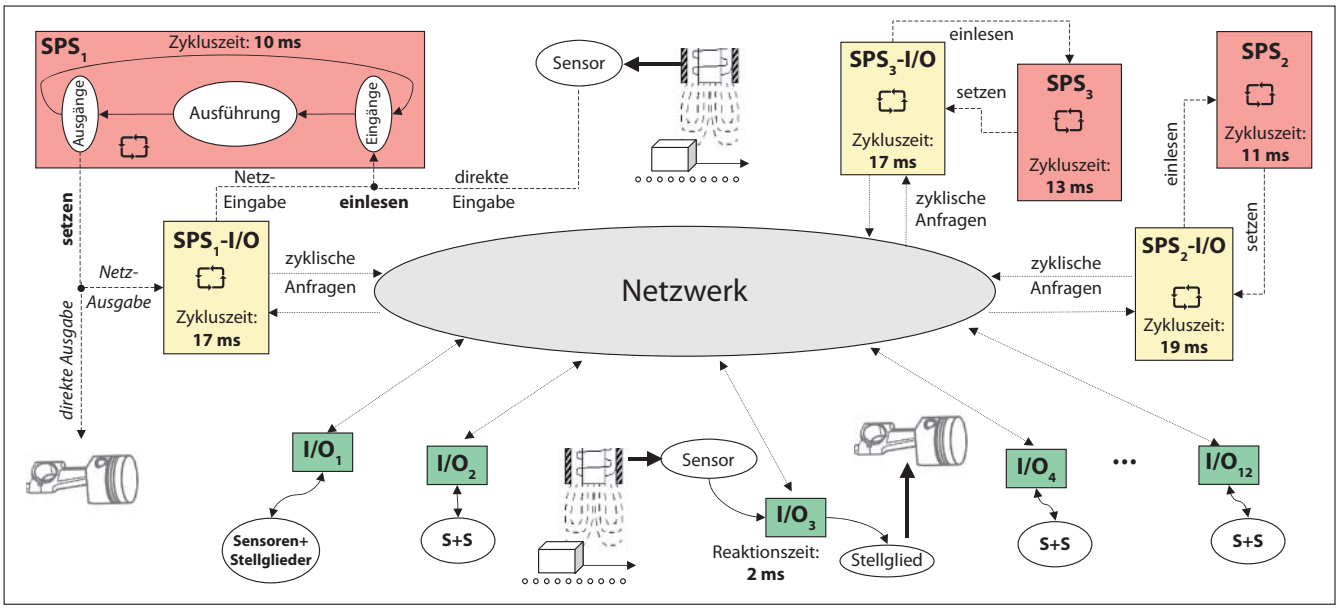

Bild 1: Anwendungsbeispiel.

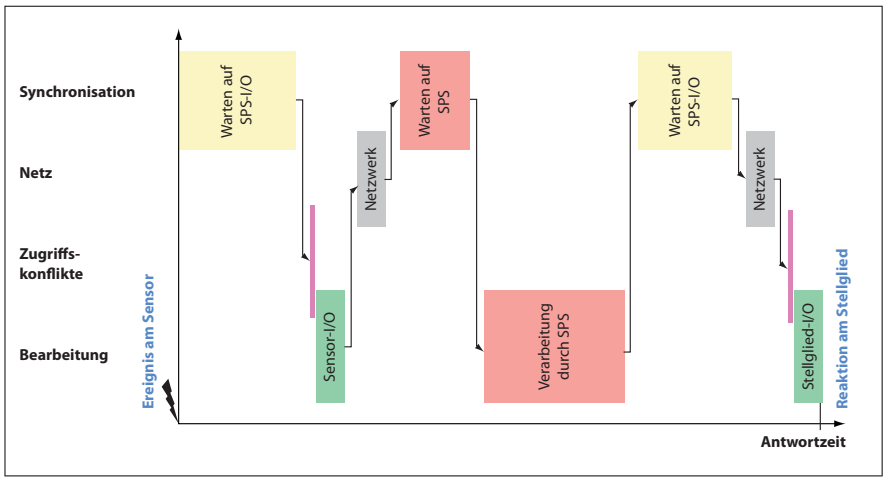

Bild 2: GANTT-Chart der betrachteten Antwortzeitenanalyse.

hier dargestellte Verhalten entspricht in der Funktionalität einem Schneider SPS-System mit MODBusIP [6].

Die Beobachtung des beschriebenen Prozesses resultiert in dem in Bild 3 dargestellten Signal-Tracking. Hierunter versteht man ein Modul im System, welches sämtliche Ereignisse mitprotokolliert. Aufgrund des Zustandes des Signal-Tracking-Moduls ist also feststellbar, ob der Prozess vollständig durchlaufen ist; eine Information die anders – aufgrund des einerseits zyklischen Verhaltens des Gesamtsystems und andererseits zufälligen Auftretens des Signalwechsels – nicht oder nur mittels zusätzlicher Variablen im System ermittelbar wäre.

Die DesLaNAS-Module der in diesem Beispiel auftretenden Grundfunktionalitäten (SPS, SPS-I/O, Anlagen-I/O, Netzübertragung) wurden bereits im Co-Beitrag [3] ausführlich diskutiert. Die zugehörige Antwortzeitverteilungsfunktion findet sich als blaue Trajektorie in Bild 9. Die Aufteilung der mittleren Antwortzeit nach Ursachen ist in Tabelle 1 jeweils als absoluter sowie prozentualer Anteil (bezogen auf die Summe) dargestellt. Bereits in diesem einfachen Beispiel ist zu erkennen, dass die Zeit, die durch Warten eines Teilprozesses auf die Synchronisation mit einem anderen in NAS verbracht wird, deutlich über der Bearbeitungszeit liegt, und die eigentliche Übertragungszeit nur eine untergeordnete Rolle spielt. Die dargestellten Ergebnisse wurden unter Verwendung der Software PRISM [7], einem Probabilistic Model-Checker der University of Birmingham errechnet.

Fehler

Im System wurden zwei Fehlerquellen vorgesehen: Zum einen kann mit einer (diskreten) Wahrscheinlichkeit von $p_{IOF}=10^{-3}$ ein Sensorwert ungültig sein (Anlagen-I/O-Fehler). Dies bedeutet, dass dieser Wert erst bei der nächsten Anfrage durch die SPS-I/O korrekt gelesen werden kann. Zum zweiten kann die Netzübertragung mit einer Wahrscheinlichkeit von $p_F=10^{-4}$ für eine Dauer von $F_t=4$ ms ausfallen (Netzfehler), wobei ein sofortiger Wiederausfall erneut mit $p_F=10^{-4}$ möglich ist. Alle zu übertragenden Pakete werden aber übertragen sobald das Netzwerk wieder zur Verfügung steht. Während sich die Anfangsverteilung des I/O-Fehlerfalles direkt aus der Ausfallwahrscheinlichkeit ermitteln lässt (aktuelle Ausfallrate ist stets $p_{IOF}=10^{-3}$), muss diese im Netzfehlerfall erst analytisch bestimmt werden. Dies ist jedoch relativ einfach, da aufgrund der Zyklizität des Ausfallautomaten der stationäre Fall gilt. Zuverlässigkeitsdaten wie sie hier Verwendung finden, können nach IEC EN 61508-6:2001, Teil B3 [8] ermittelt werden, welcher die Wahrscheinlichkeit eines Ausfalls je Stunde (für die Betriebsart mit hoher Anforderungsrate oder kontinuierlicher Anforderung) beschreibt.

Tabelle 1: Aufteilung der Antwortzeit in der Ausgangskonfiguration.

Gesamt		Anteile		
Wertebereich	Mittelwert/ Streuung	Netzanteil	Bearbeitung	Synchronisation
20–53 ms	39,9 ms/9,2 ms	4 ms/10,0 %	14,5 ms/36,3 %	21,4 ms/53,7 %

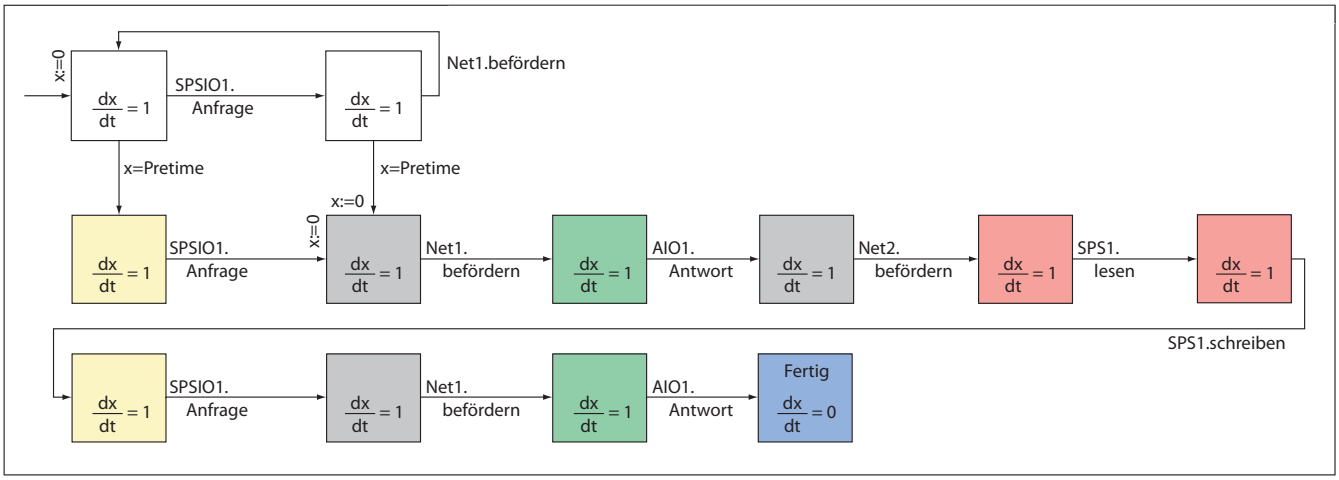

Bild 3: Signal-Tracking des Grundbeispiels.

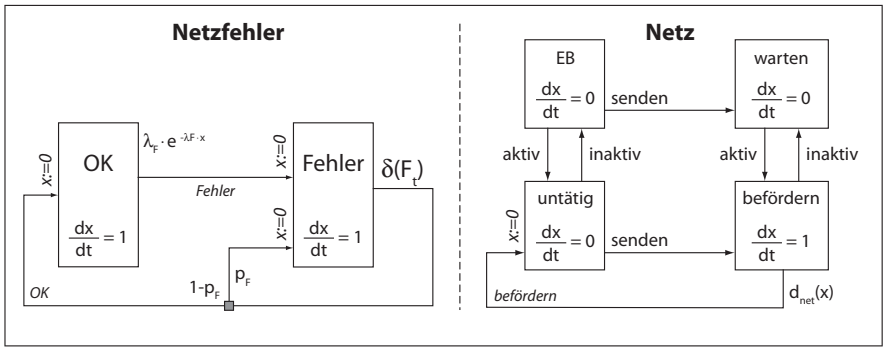

Bild 4: Netzfehlermodul (links) und Netzmodul, das einen solchen Fehler berücksichtigt.

Der Fehlertypus des Netzfehlers lässt sich als separates Modul modellieren, auf welches dann sämtliche Netzmodule synchronisieren (Bild 4, links). Dies macht insbesondere dann Sinn, wenn der auftretende Fehler mehrere Module beeinflusst, wie das hier für die beiden Netzübertragungen der Fall ist. Ein solches separates Fehlermodul hat zwei Zustände, nämlich OK und Fehler, wobei die Übergangswahrscheinlichkeiten durch entsprechende Dichtefunktionen gegeben sind.

Um den Fehlerfall repräsentieren zu können, muss das Netzmodul um zwei weitere Zustände ergänzt werden (Bild 4, rechts), wobei sich der Automat bei normalem Betrieb in einem der beiden ursprünglichen Zustände befindet. Ereignet sich ein Fehler (Ereignis: inaktiv), so wechselt der Automat vom aktuellen (unteren) in den direkt oberhalb des aktuellen befindlichen Zustand. Sobald der Fehler behoben wurde (Ereignis: aktiv) wechselt der Automat in den jeweils darunter liegenden Zustand. Selbstverständlich ist es möglich, dass eine Anfrage eingeht, während sich der Automat im Zustand „EB" (empfangs- aber nicht beförderungsfähig) befindet. In diesem Fall wechselt der Automat in den Zustand „warten". Die umgekehrte Richtung ist nicht möglich, da ein Komplettverlust des Datenpakets nicht vorgesehen ist. In Bezug auf die Initialisierung dieser Module ist anzumerken, dass die fehlerbehafteten Netzmodule nun natürlich nicht mehr unabhängig initialisiert werden können, da ihr Initialzustand von dem des Netzfehlermoduls abhängt.

Der für die Anlagen-I/O angenommene Fehlertyp ist von lediglich lokaler Wirkung, d. h. er beeinflusst nur ein einziges Modul und führt außerdem zum Komplettverlust der Information (ohne jedoch das übergeordnete Zeitverhalten des Moduls zu verändern). Dies lässt sich wie in Bild 5 gezeigt als Automat darstellen.

Während die Verwendung eines nicht zum Informationsverlust führenden Fehlertyps (z. B. Netzwerk) sich nicht im Signal-Tracking-Modul niederschlägt, muss hier das Signal-Tracking-Modul entsprechend erweitert werden (Bild 6), da ein Zurückkehren zu einem bereits passierten Zustand erforderlich wird.

Schlussendlich müssen die Module noch instanziiert, verbunden und parametriert werden. Dies erfolgt, wie in [3] gezeigt, grafisch (Bild 7), kann aber auch in textueller Form vorgenommen werden. Zum besseren Verständnis soll hier nochmals kurz die grafische Notation erläutert werden. Jeder Block repräsentiert ein eigenständiges Modul. In der Kopfzeile finden sich der Name des Moduls sowie die Modulklasse. Darunter werden auf der linken Seite die Systemparameter und auf der rechten die Initialzustandsparameter angegeben. Letztere teilen sich in P^0 auf, welches angibt, mit welcher Wahrscheinlichkeit ein gegebener Zustand der zum Zeitpunkt 0 aktive Zustand ist, und X^0, das die Verteilung der Uhrvariable(n) in einem gegebenen Zustand zum Zeitpunkt 0 angibt. GV(a,b) steht hierbei für gleichverteilt zwischen (a,b] und δ(a) für einen Dirac-Impuls zum Zeitpunkt a. Schlussendlich zeigt f(NF.OK) an, dass dieser Anfangszustand abhängig vom Zustand OK des Moduls NF ist. An die Verbindungslinien wird der Name des Ereignisses gesetzt, wobei kursive Schrift für den Namen im erzeugenden Modul und normale Schrift für den Namen im aufnehmenden Modul steht. Sind diese identisch, kann letzterer weggelassen werden (z. B. am Signal-Tracking).

Tabelle 2 zeigt, welche zusätzliche Verzögerung sich im (nicht zugriffskonfliktgestörten) System durch die unterschiedlichen Fehlerarten einstellt. Als dritte Spalte („Anteil

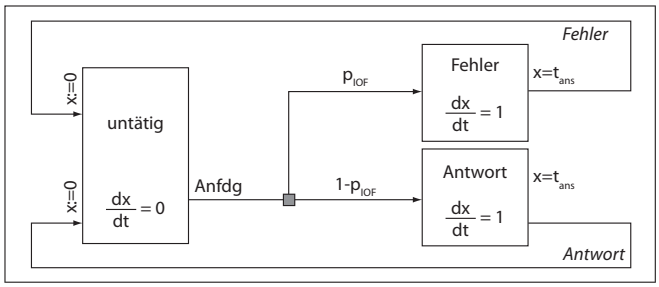

Bild 5: Automatendarstellung einer Fehler berücksichtigenden Anlagen-I/O.

Tabelle 2: Änderung der mittleren Antwortzeit unter Berücksichtigung von Ausfällen.

Fehlertyp	absoluter Zuwachs	relativer Zuwachs	Anteil über Max
Sensor	17,0170 µs	0,0426 %	0,07003 %
Netzwerk	2,5295 µs	0,0063 %	0,00412 %

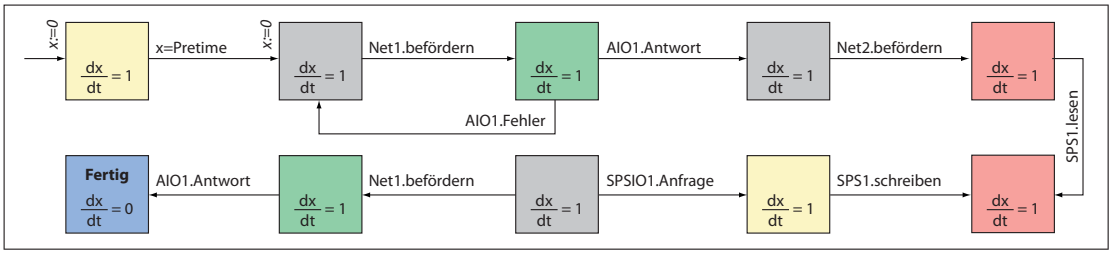

Bild 6: Signal-Tracking unter Berücksichtigung eines Anlagen-I/O-Fehlers.

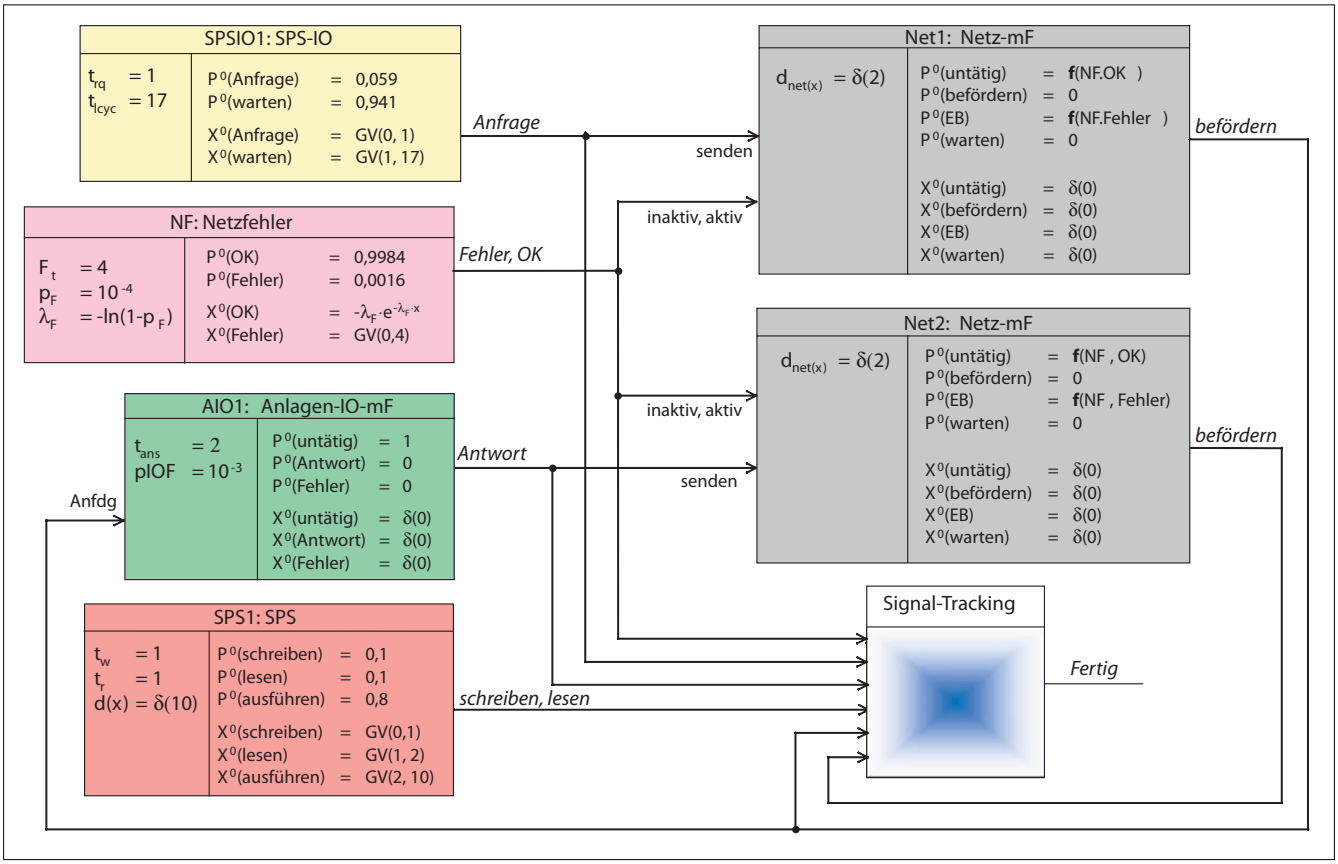

Bild 7: Instanziierung und Parametrisierung des NAS unter Berücksichtigung von Fehlern.

über Max“) wurde hierbei noch der Anteil der Fälle aufgetragen, in denen die Verzögerung größer als die maximale Verzögerung des nicht fehlerbehafteten Vergleichssystems ist. Die zugehörigen Verzögerungsdistributionen sind in Bild 8 gezeigt (logarithmischer Maßstab). Obwohl die Reaktion durch einen Fehler teilweise erheblich verzögert werden kann, muss dies natürlich stets in Relation mit der sehr niedrigen Auftretenswahrscheinlichkeit gesehen werden.

Zugriffskonflikte

Die bisher betrachtete Situation eines alleinigen (oder zumindest priorisierten) Zugriffs der SPS auf die anzufragende Anlagen-I/O taucht in der Praxis selten auf. Stattdessen finden sich mehrere SPSen, die unabhängig voneinander diese Anlagen-I/O anfragen. Dies ist auch insbesondere unter dem Erweiterungsaspekt interessant, da es in NAS möglich ist, dynamisch unterschiedlich viele Teilnehmer vorzufinden. PMC ist dabei eine Möglichkeit die Konsequenzen derartiger Veränderungen fundiert beurteilen zu können.

Ist die Anlagen-I/O beim Eintreffen einer Anfrage gerade mit der Bearbeitung einer anderen Anfrage beschäftigt, so wird zunächst diese, sich bereits in Bearbeitung befindliche Anfrage abgearbeitet und erst anschließend alle später eingetroffenen Anfragen (in der Reihenfolge ihres Eintreffens). Zur Abbildung dieses Verhaltens muss das DesLaNAS-Modul der Anlagen-I/O um einen Anfrage-Puffer erweitert werden. Die Struktur des Signal-Tracking-Moduls ändert sich für die Berücksichtigung von Zugriffskonflikten nicht. Die Instanziierung der weiteren SPS-I/O erfolgt wie für

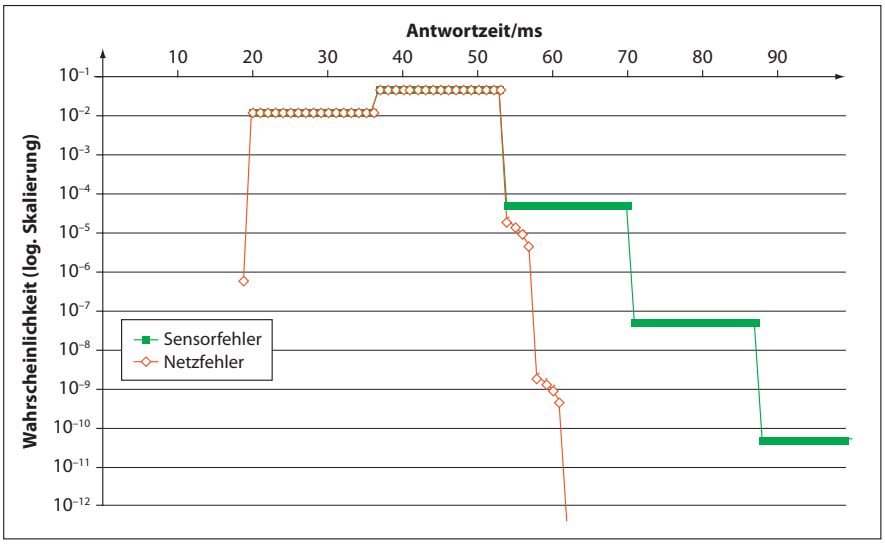

Bild 8: Diskrete Wahrscheinlichkeit dafür, dass die Antwortzeit des Systems im Bereich eines bestimmten Zeitintervalls der Länge einer Millisekunde liegt; für ein aus einer SPS bestehendes fehlerbehaftetes (aber zugriffskonfliktfreies) System.

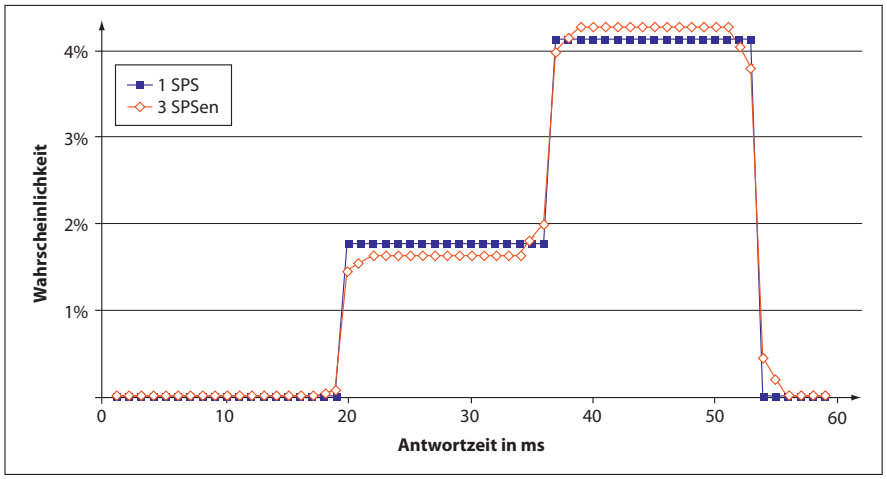

Bild 9: Diskrete Wahrscheinlichkeit dafür, dass die Antwortzeit des Systems im Bereich eines bestimmten Zeitintervalls der Länge einer Millisekunde liegt; für ein aus einer SPS bestehendes (zugriffskonfliktfreies) sowie ein aus drei SPSen bestehendes (zugriffskonfliktbehaftetes) System.

die bereits vorhandene SPSIO1, mit dem Unterschied, dass für die zweite SPS-I/O eine Zykluszeit von 19 ms angenommen wurde. Darüber hinaus wird noch ein weiteres Netzmodul benötigt, um den Datentransport von der zweiten SPS-I/O zur Anlagen-I/O zu beschreiben. Der Rücktransport spielt indes für den betrachteten Ablauf keine Rolle und wird daher nicht modelliert.

Ein Vergleich der Häufigkeitsverteilungen der Antwortzeiten (Bild 9 für eine und drei SPSen) zeigt in welchem Zeitbereich zusätzliche Verzögerungen in welchem Umfang auftreten. Eine genaue Analyse ergibt, dass die maximale Antwortzeit in den drei betrachteten Szenarien von 53 über 55 auf 57 ms steigt. Die prozentuale Anzahl der Antworten die um mehr als 53 ms (max bei einer SPS) verzögert werden, beträgt hierbei 0,43 % für zwei und 0,67 % für drei SPSen (vgl. Tabelle 3).

Im Hinblick auf Sicherheitsaspekte sollte hierbei besonders beachtet werden, dass Zugriffskonflikte nicht nur die maximale Antwortzeit erhöhen, sondern auch die minimale erniedrigen können. Dies liegt daran, dass die Anlagen-I/O beim Eintreffen einer Anfrage gerade mit der Bearbeitung der Anfrage einer anderen SPS-I/O beschäftigt sein kann und somit die betrachtete Anfrage warten muss, bis die früher eingetroffene abgearbeitet worden ist. Erfolgt nun eine Änderung des Sensoreinganges während dieser Warteperiode, so wird diese noch vor der Bearbeitung der gerade wartenden Anfrage registriert, wohingegen diese Anfrage im zugriffskonfliktfreien Fall noch den alten Wert zurückgemeldet hätte. In Bezug auf den Zeitpunkt der Sensorsignaländerung erhält die SPS also früher Bescheid, als dies im konfliktfreien System der Fall wäre. Dieser Effekt tritt zwar selten ein (im betrachteten Beispiel nur mit einer Wahrscheinlichkeit von ca. 0,1 %), senkt aber die minimale Antwortzeit 20 auf 18 ms (Bild 9 und Tabelle 3).

Der Zuwachs des Maximalwertes hängt von einer ganzen Reihe Parameter ab. So findet sich in Tabelle 3, dass der Einfluss einer Wartezeit vor dem Sensor aufgrund der Zyklen von SPS und SPS-I/O keinen Einfluss auf den Maximalwert (wohl aber auf die Verteilung) hat. Erhöht man jedoch die Antwortzeit der Anlagen-I/O von 2 ms auf 5 ms so ergibt sich ein deutlicher Unterschied, wie Tabelle 4 zeigt. Während zunächst der gleiche Effekt wie zuvor auftritt (ein Plus von 5 ms), steigt die Differenz von der zweiten zur dritten Spalte um 17 ms an. Dies entspricht einem kompletten Zyklus der ersten SPS-I/O. Als Ursache kommen zwei Dinge ins Spiel: Der Gangunterschied zwischen SPS und SPS-I/O kann bei den gewählten Parametern eine Anlagenbearbeitungszeit von 13 ms abfangen. Kommen jedoch alle drei SPS-I/O-Anfragen zusammen, so addiert sich die zugehörige Warte-/Bearbeitungszeit auf 15 ms und das Signal muss einen kompletten SPS-I/O-Zyklus abwarten.

Verlustwahrscheinlichkeit

Nimmt man für das an der Anlagen-I/O anliegende Sensorsignal eine fest vorgegebene Haltezeit an [9], so kann der Sensorwert beim Eintreffen der Anfrage schon nicht mehr anliegen und somit nicht mehr ausgelesen werden, falls die Anlage nicht entsprechend robust ausgelegt wurde. In diesen Fällen ist es interessant zu wissen, mit welcher Wahrscheinlichkeit ein (mindestens) *n* Millisekunden lang anlie-

Tabelle 3: Aufteilung der Antwortzeiten unter Berücksichtigung von Zugriffskonflikten.

	Eine SPS	Zwei SPSen	Drei SPSen
Netzanteil	4 ms / 10,0 %	4 ms / 9,97 %	4 ms / 9,92 %
Bearbeitung	14,5 ms / 36,3 %	14,5 ms / 36,16 %	14,5 ms / 35,94 %
Synchronisation	21,4 ms / 53,7 %	21,4 ms / 53,37 %	21,4 ms / 53,05 %
Zugriffskonflikt	–	0,2 ms / 0,50 %	0,44 ms / 1,09 %
Summe bzw. Zunahme	39,9 ms	40,1 ms / + 0,5 %	40,34 ms / + 1,1 %
Min. / Max / über Max	20 / 53 ms	18 / 55 ms / 0,43 %	18 / 57 ms / 0,67 %

Tabelle 4: Aufteilung der Antwortzeiten unter Berücksichtigung von Zugriffskonflikten bei geänderter Anlagen-I/O-Antwortzeit

	Eine SPS		Zwei SPSen		Drei SPSen	
Netzanteil	4 ms	8,639 %	4 ms	8,452 %	4 ms	8,172 %
Bearbeitung	20,5 ms	44,276 %	20,5 ms	43,318 %	20,5 ms	41,880 %
Synchronisation	21,8 ms	47,084 %	21,8 ms	46,065 %	21,8 ms	44,538 %
Zugriffskonflikt	–	–	1,024 ms	2,163 %	2,647 ms	5,408 %
Summe	46,3 ms		47,324 ms	+ 2,21 %	48,947 ms	+ 5,7 %
Max / über Max	**56 ms**	–	61 ms	**3,56 %**	78 ms	10,3 %

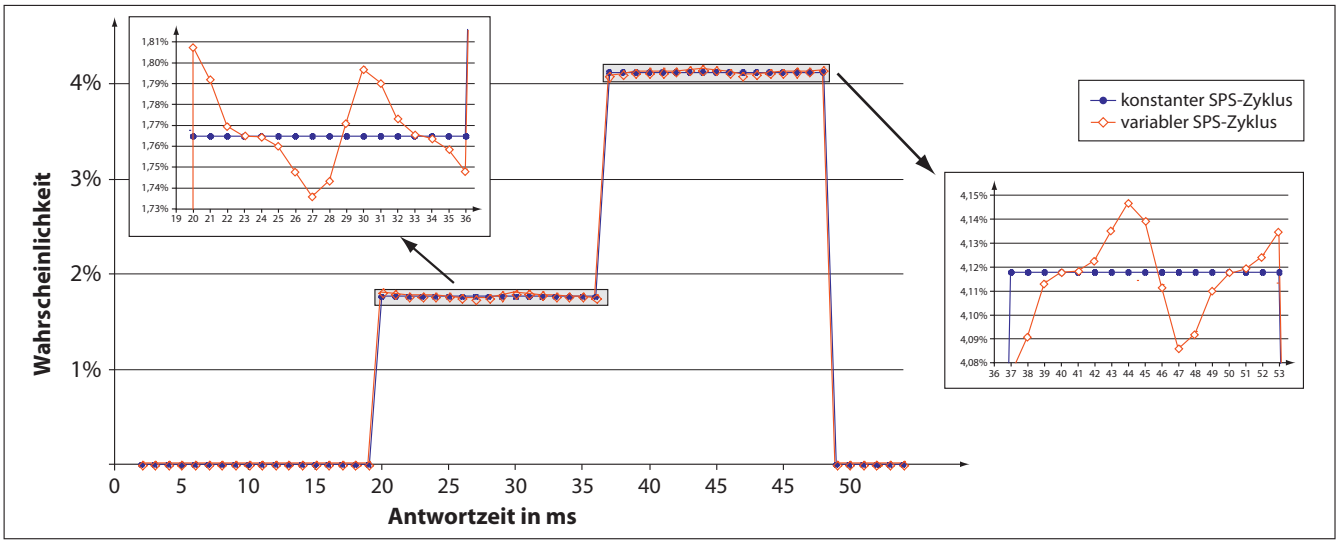

Bild 10: Vergleich der Antwortzeitverteilungen von variabler und konstanter SPS-Zyklusdauer. Die beiden Ausschnitte zeigen eine Vergrößerung des Verlaufs an den Plateaus.

gendes Signal erkannt wird, bzw. wie lange ein Signal mindestens anliegen muss, damit es mit einer bestimmten Wahrscheinlichkeit erkannt wird. Die Analyse dieses Problems ist verhältnismäßig einfach, da das Signal-Tracking auf die Elemente SPS-I/O, Anlagen-I/O und für den fehlerbehafteten Fall auf das Netzwerk, verkürzt wird. Tabelle 5 zeigt die Ergebnisse der zugehörigen Analyse für das bisherige Beispiel. In den Zeilen aufgetragen sind die Werte für verschiedene Settings, bei denen sowohl die Antwortzeit der Anlagen-I/O, als auch die Anzahl anfragender SPS-I/Os verändert wurde. In den Spalten findet sich zunächst die minimale Haltezeit im ungestörten Fall, d. h., jene Zeit, die das Signal mindestens anliegen muss, damit es im ungestörten Fall garantiert erkannt wird. Die folgenden vier Spalten geben hingegen jene Zeit an, die das Signal anliegen muss, um mit mindestens 99,999 % bzw. 99,9999 %-iger Wahrscheinlichkeit erkannt zu werden. Diese Werte entsprechen den über den Spalten angegebenen Verlustwahrscheinlichkeiten von 10^{-5} und 10^{-6}. Angegeben sind jeweils die Fälle eines Ausfalls der Anlagen-I/O (Sensorfehler usw.) als auch eines Ausfalls des Netzwerkes (beide Fehlerarten wie zuvor eingeführt). Erwartungsgemäß verringert sich die Verlustwahrscheinlichkeit mit steigender Haltezeit, bzw. erhöht sich die notwendige Haltezeit um unterhalb einer maximalen Verlustwahrscheinlichkeit zu bleiben.

Tabelle 5: Verlustwahrscheinlichkeiten in Abhängigkeit von Zugriffskonflikten, Anlagen-I/O-Antwortzeit und Fehlerquellen.

Anlagen-I/O Antwortzeit	Anzahl SPSen	minimal erforderliche Haltezeit				
		ungestört	Fehler im Netzwerk		Anlagen-I/O-Fehler	
			$p \leq 10^{-5}$	$p \leq 10^{-6}$	$P \leq 10^{-5}$	$p \leq 10^{-6}$
2 ms	1	20 ms	23 ms	24 ms	37 ms	37 ms
2 ms	2	22 ms	23 ms	24 ms	37 ms	39 ms
2 ms	3	24 ms	24 ms	25 ms	38 ms	40 ms
5 ms	1	23 ms	26 ms	27 ms	40 ms	40 ms
5 ms	2	28 ms	28 ms	30 ms	43 ms	45 ms
5 ms	3	30 ms	33 ms	33 ms	45 ms	49 ms

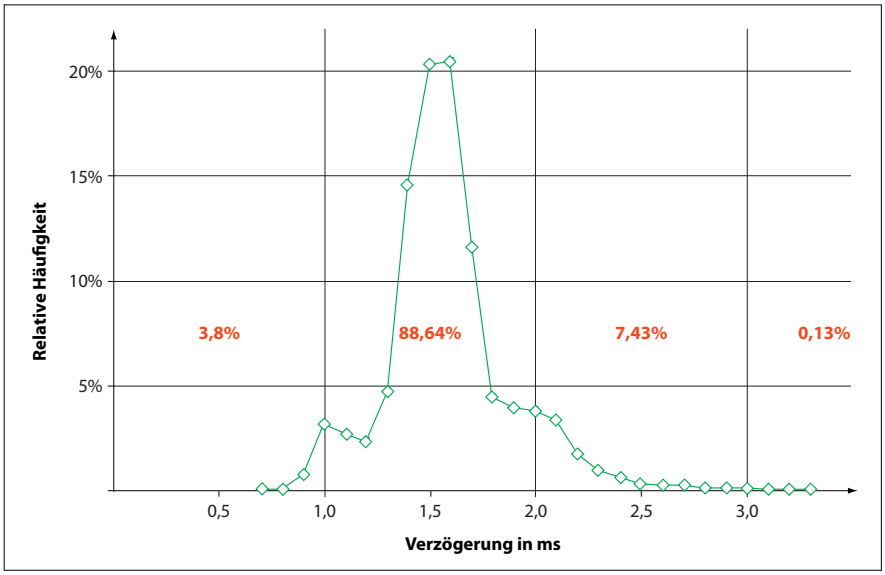

Bild 11: Verzögerung durch WLAN-Übertragung.

Stochastisches Komponentenverhalten

In diesem Abschnitt wird eine weitere Erscheinungsform stochastischen Verhaltens diskutiert, nämlich die Verhaltensabstraktion durch Verzögerungsver-

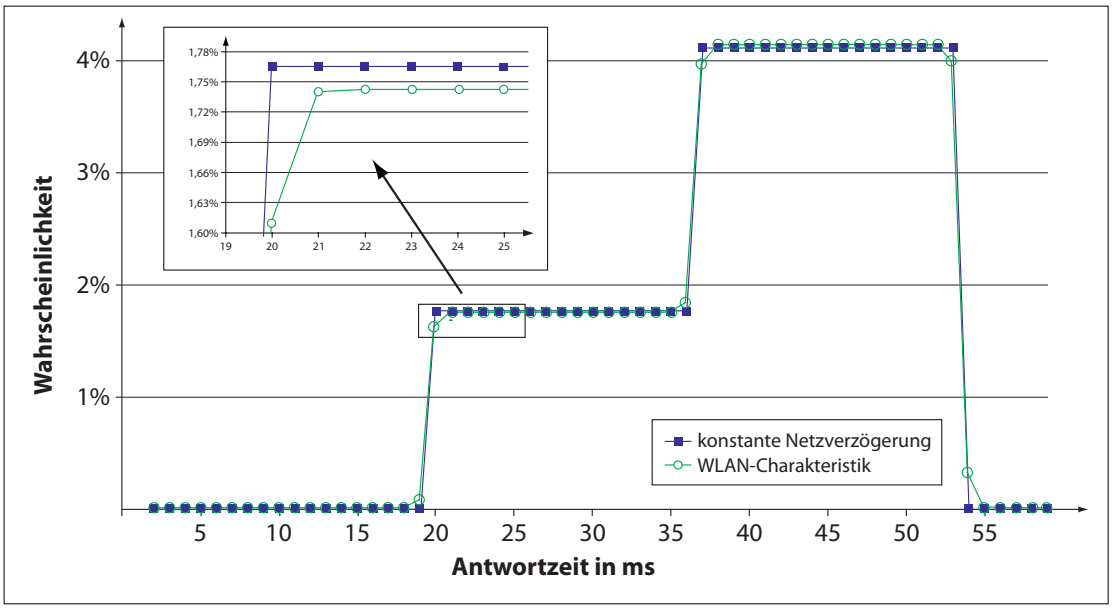

Bild 12: Vergleich der Antwortzeitverteilungen des Grundsystem unter Verwendung einer variablen Netzlaufzeit mit WLAN-Charakteristik gegenüber einer konstanten Netzlaufzeit von 2 ms.

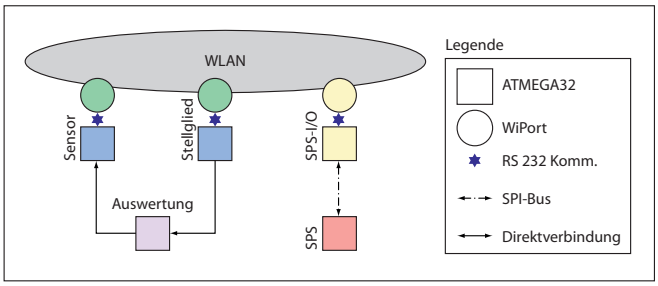

Bild 13: Struktureller Aufbau der Versuchsanlage.

teilungsdichten. Beispielhaft werden ein flexibler SPS-Zyklus und eine variierende Netzübertragungsdauer besprochen.

Bild 10 zeigt die Antwortzeitverteilung für ein NAS mit einer SPS, für deren Zyklus die folgenden Längen angenommen wurden: 9 und 11 ms mit je 20 %-iger Wahrscheinlichkeit und 10 ms mit 60 %. Da der Effekt des variablen SPS-Zyklus eher gering ist, wird im Weiteren (wie zuvor) von einem konstanten Zyklus ausgegangen.

Bisher wurde die Netzwerkverzögerung als konstant angenommen, da die Bandbreite von ± 0,5 ms kaum ins Gewicht fällt und der Einfluss der gesamten durch das Netzwerk verursachten Verzögerung bei lediglich 10 % liegt (vgl. z. B. Tabelle 1). Im Folgenden wird jedoch statt eines LANs ein WLAN verwendet, das, wie Messungen am Lehrstuhl der Autoren ergeben haben [10], die in Bild 11 dargestellte Übertragungszeitverteilung aufweist. Da das System mit einer Schrittweite von 1 ms diskretisiert wurde, ergeben sich die in rot angegeben prozentualen Verzögerungsanteile für 1, 2, 3 und 4 ms.

Während sich im DesLaNAS-Modell nur die Parametrierung ändert, entsteht bei der Umsetzung in ein diskretes PMC-Modell eine veränderte Übertragungscharakteristik. Diese erzeugt die in Bild 12 dargestellten Unterschiede zwischen einem Verlauf mit konstanter und variabler Netzverzögerung.

Zur Validierung der Ergebnisse wurde das System im Labor aufgebaut [11], wobei die Zykluszeiten von SPS und SPS-I/O softwaremäßig vorgegeben wurden. Dies wurde dadurch erreicht, dass das prinzipielle Verhalten von SPS und SPS-I/O jeweils auf einem eigenen ATMEGA32 Microcontroller der Firma Atmel implementiert wurde. In gleicher Weise wurden auch der Sensor, das Stellglied und die Auswertungslogik, auf eigenständigen Boards aufgebaut. Die Auswertungslogik umfasste dabei die Signalerzeugung und die Antwortzeitmessung. Aus Vergleichbarkeitsgründen wurde ein Aufbau ohne Zugriffskonflikte, d. h. mit lediglich einer SPS, verwendet, so dass sich die in Bild 13 gezeigte Struktur ergab.

Die Kommunikation wurde mittels WLAN realisiert, wobei als Sendebausteine WiPorts der Firma Lantronix Verwendung fanden. Angeschlossen wur-

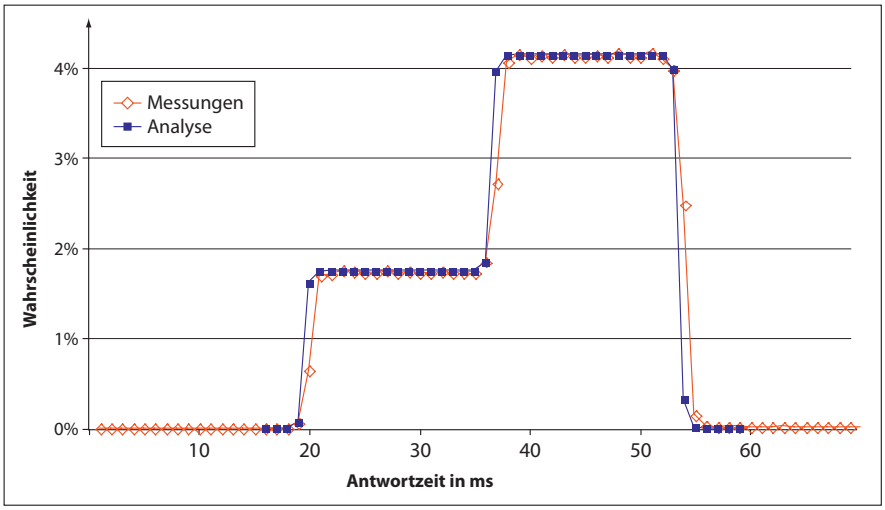

Bild 14: Relative Häufigkeiten von 1 Million, auf der Versuchsanlage nach [11] gemessenen, Antwortzeiten im Vergleich mit den analytisch bestimmten Wahrscheinlichkeitswerten (SPS-Zyklus: 10 ms, SPS-I/O-Zyklus: 17 ms).

den die Wiports an die ATMEGA32 über eine serielle Schnittstelle. Die Kopplung von SPS-I/O und SPS erfolgte mittels SPI-Bus. Die Messergebnisse sind in Bild 14 grafisch dargestellt.

Die Messungen zeigen eine hohe Übereinstimmung mit den analytisch ermittelten Werten. Dies bestätigt nicht nur die erstellten Modelle, sondern bildet auch die Grundlage für eine vertrauenswürdige Verwendung von PMC in komplexeren Strukturen und Fragestellungen.

Einfluss der Zykluszeit von SPS und SPS-I/O

Die bisherigen Ergebnisse zeigen deutlich den Einfluss des zyklischen Arbeitsverhaltens von SPS und SPS-I/O, weshalb sich die Frage stellt, was passiert, wenn man diese Zyklen verändert. In einer ersten Untersuchung werden dabei die Zykluszeiten von SPS und ihrer I/O vertauscht (SPS: 17 ms, SPS-I/O: 10 ms). Hierdurch wird erreicht, dass die SPS am Beginn eines Zyklus immer aktuelle Werte vorfindet. Der Preis hierfür liegt allerdings in einer Erhöhung der mittleren Verzögerungszeit von 40 ms auf 42,3 ms. Der zugehörige Graph findet sich in Bild 15.

Hieraus resultierte die Frage, was passieren würde, wenn SPS und SPS-I/O sehr schnell (SPS: 1 ms, SPS-I/O: 3 ms) wären. Da derart kurze SPS-I/O-Zyklen mit obigem Messaufbau nicht möglich sind, wurde auf Werte aus [12] zurückgegriffen, welcher lediglich ein Anlagen-I/O-board verwendete und somit kürzere Zyklen fahren konnte (Minimum 3 ms). Die zugehörige Verteilung findet sich in Bild 16. Während sich der Einfluss der SPS hier auf einen konstanten Faktor von 1 ms reduzieren lässt, sind SPS-I/O und die Netzwerkübertragung für die Gestalt der entstehenden Verteilung maßgeblich.

Zusammenfassung und Ausblick

Vernetzte Automatisierungssysteme (NAS) erlauben völlig neuartige, flexible Architekturen in der Automatisierungstechnik. Die Sicherstellung von Antwortzeiten stellt sich dabei als eine wichtige Entwurfs- und Analyseaufgabe heraus. In diesem Beitrag wurde mit der Methode des Probabilistic Model Checking der Einfluss verschiedener Faktoren auf das Zeitverhalten eines NAS analysiert.

Im ersten Teil dieser aus zwei Beiträgen bestehenden Arbeit wurde ein kurzer Überblick über Methoden zur Verzögerungsbestimmung gegeben. Hierauf aufbauend wurde die auf die besonderen Bedürfnisse bei der Modellierung von netzbasierten Automatisierungssystemen entwickelte Beschreibungssprache DesLaNAS schrittweise vorgestellt und der zur Anwendung gekommene Modellierungsprozess diskutiert.

In diesem zweiten Teil wurden nun anhand eines typischen NAS-Beispieles schrittweise die verschiedenen Einflussfaktoren eines NAS diskutiert und bewertet (Bild 17a,b). Zur Validierung der Ergebnisse wurden umfangreiche Labormessungen durchgeführt.

Zusammenfassend lässt sich sagen, dass der Netzwerkeinfluss selbst eher gering ist. Allerdings ermöglicht das Netzwerk erst jene Architekturen, die – insbesondere durch Synchronisationseffekte – erhebliche zusätzliche Verzögerungszeiten aufweisen.

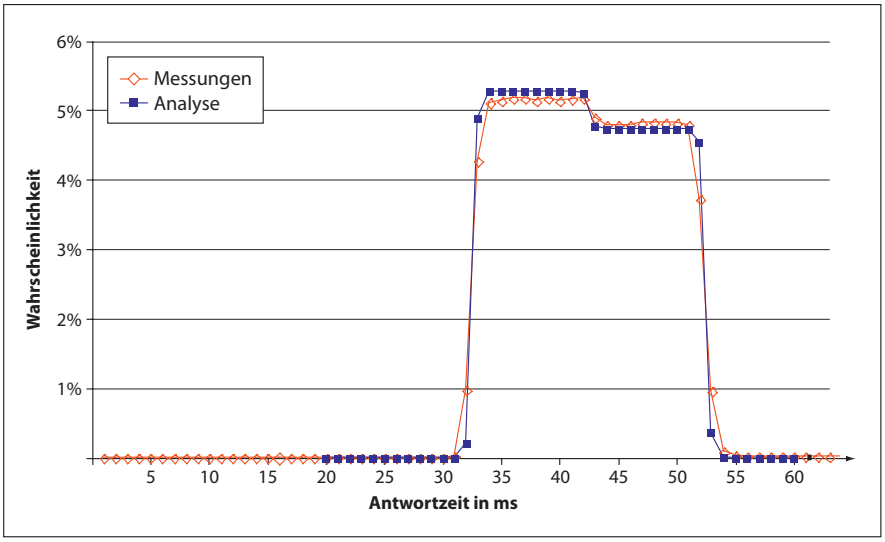

Bild 15: Relative Häufigkeiten von 1 Million, auf der Versuchsanlage nach [11] gemessenen, Antwortzeiten im Vergleich mit den analytisch bestimmten Wahrscheinlichkeitswerten (SPS-Zyklus: 17 ms, SPS-I/O-Zyklus: 10 ms).

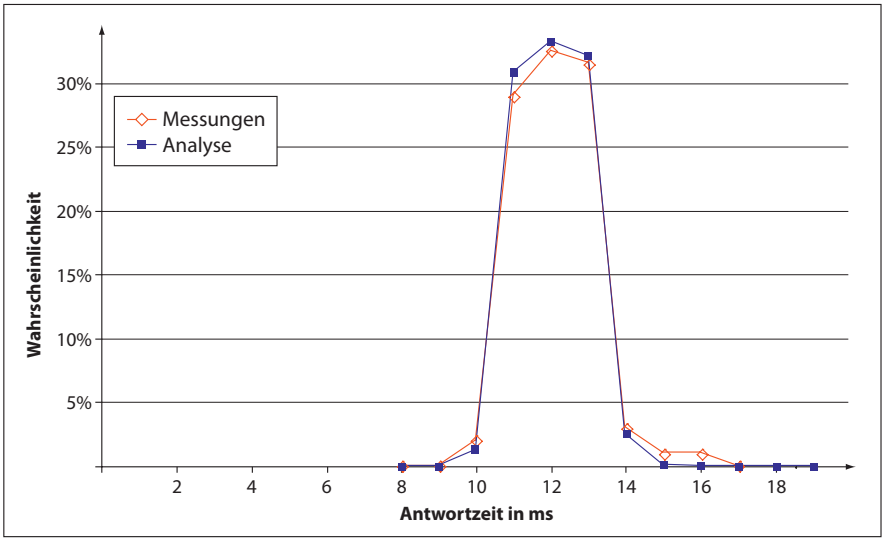

Bild 16: Relative Häufigkeiten von 200, auf der Versuchsanlage nach [12] gemessenen, Antwortzeiten im Vergleich mit den analytisch bestimmten Wahrscheinlichkeitswerten (SPS-Zyklus: 1 ms, SPS-I/O-Zyklus: 3 ms).

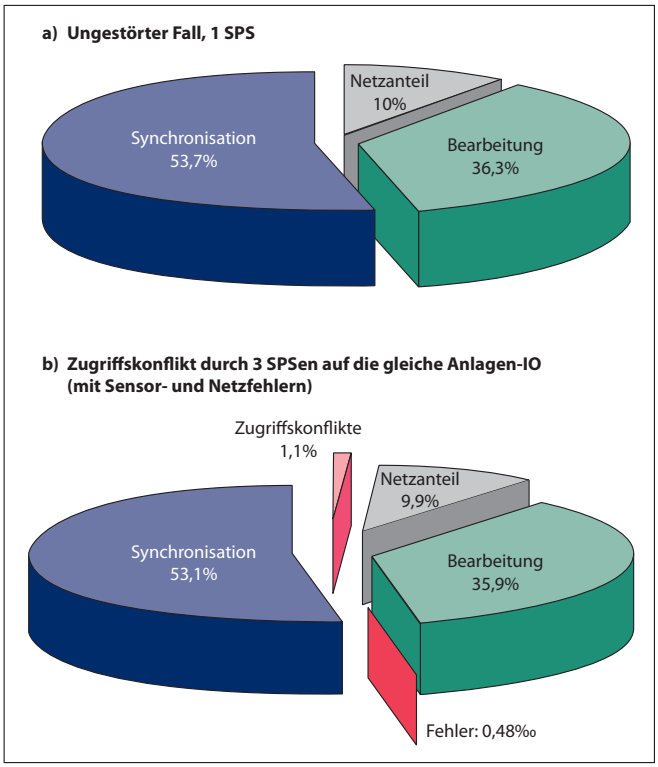

Bild 17: Prozentuale Aufgliederung der Antwortzeiten nach Einflussgrößen.

Obwohl Zugriffskonflikte und Fehler nur einen verhältnismäßig kleinen Einfluss auf die Antwortzeit haben (vgl. Bild 17), können sie im Einzelfall zu Antwortzeiten führen, die nicht nur deutlich über dem Maximal-, sondern auch unter dem Minimalwert der Antwortzeitverteilung des ungestörten Systems liegen. Da Zugriffskonflikte und Fehler jedoch eher selten auftreten ist es – gerade unter Sicherheitsaspekten – wichtig, ein Verfahren verwendet zu haben, dass auch die Auswirkungen seltener Effekte zuverlässig wiedergibt.

Aufbauend auf diesen Ergebnissen soll ein Designprozess zur automatischen Modellierung, Berechnung und Auswertung erarbeitet und implementiert werden.

Literatur

[1] *Moyne, J. R., Tilbury, D. M.*: The Emergence of Industrial Control Networks in Manufacturing Control, Diagnostics, and Safety Data. Proc. of the IEEE, Band 95, Nr. 1, S. 29–47, (2007).

[2] *Liu, L., Frey, G.*: Simulation Approach for Evaluating Response Times in Networked Automation Systems, Proc. 12th IEEE Int. Conf. Emerging Technologies and Factory Automation (ETFA), Patras, Griechenland (2007).

[3] *Greifeneder, J., Frey, G.*: Modellierung des Zeitverhaltens netzbasierter Automatisierungssysteme. atp Automatisierungstechnische Praxis 49 (2007), H. 9, S. 76–84.

[4] *Kopetz, H.*: Time-triggered real-time computing, Annual Reviews in Control, Nr. 27, S. 3–13, (2003)

[5] *Gottheit, C.*: Experimentelle Bestimmung von Verzögerungen in verteilten Automatisierungssystemen. Studienarbeit SA017, JPA², Fachbereich EIT, Technische Universität Kaiserslautern (2006).

[6] *Denis, B., Ruel, S., Faure, J.-M., Marsal, G., Frey, G.*: Measuring the Impact of Vertical Integration on Response Times in Ethernet Fieldbusses. Proc. Emerging Technologies and Factory Automation (ETFA), Patras, Griechenland (2007).

[7] *Kwiatkowska, M., Norman, G., Parker, D.*: PRISM: Probabilistic symbolic model checker. Proc. TOOLS, Springer Verlag, LNCS Band 2324, S. 200–204 (2002).

[8] IEC EN 61508: Funktionale Sicherheit elektrischer/elektronischer/programmierbar elektronischer sicherheitsbezogener Systeme, Teil 6: Beispielhafte Vorgehensweise zur Bestimmung von Hardware-Ausfällen, Abschnitt B3: Wahrscheinlichkeit eines Ausfalls je Stunde (für die Betriebsart mit hoher Anforderungsrate oder kontinuierlicher Anforderung). International Electrotechnical Commission (2001).

[9] *Greifeneder, J., Frey, G.*: Analyse des Antwortverhaltens vernetzter Automatisierungssysteme mittels Probabilistic Model Checking. Proc. des 9. Symp. zu Entwurf komplexer Automatisierungssysteme (EKA), Braunschweig, Germany (2006).

[10] *Horbach, P.*: Messtechnische Untersuchung des Antwortverhaltens einer verteilten Steuerung. Studienarbeit SA020, JPA², Fachbereich EIT, Technische Universität Kaiserslautern, (2006).

[11] *Greifeneder, J., Liu, L., Frey, G.*: Methoden zur Antwortzeitanalyse in vernetzten Automatisierungssystemen. Proc. of the SPS/IPC/DRIVES, Nürnberg, Germany (2007).

[12] *Bohl, J.*: Experimentelle Bestimmung von Steuerungsgüte-Parametern am Beispiel einer Positioniersteuerung. Studienarbeit SA022, JPA², Fachbereich EIT, Technische Universität Kaiserslautern (2006).

Manuskripteingang: 23. April 2007.

Dipl.-Ing. *Jürgen Greifeneder* (32) arbeitet zurzeit unter der Betreuung von J.Prof. G. Frey an der TU Kaiserslautern an seiner Promotion. Sein Arbeitsgebiet umfasst Modellierung, Simulation und formale Analyse von Regelungs- und Steuerungssystemen, derzeitiger Schwerpunkt ist die Untersuchung Netzbasierter Automatisierungssysteme (NAS).

Adresse: TU Kaiserslautern, FB Elektro- und Informationstechnik, Erwin-Schrödinger-Str. 12, 67663 Kaiserslautern, Deutschland, Tel. +49 631 205-4549, Fax -4462, E-Mail: greifeneder@eit.uni-kl.de

J. Prof. Dr.-Ing. *Georg Frey* (37) ist seit 2002 Inhaber der Juniorprofessur Agentenbasierte Automatisierung an der Technischen Universität Kaiserslautern. Seine Hauptarbeitsgebiete sind Methoden zur Bereitstellung verlässlicher Automatisierungssysteme mit einem Fokus auf verteilten/vernetzten Systemen. Dies betrifft zum einen transparente, nachvollziehbare Entwicklungsmethoden (basierend auf UML und ereignisdiskreten Formalismen) sowie zum anderen Analyseverfahren (Model Checking und Simulation).

Adresse: siehe oben, Tel. +49 631 205-4455, E-Mail: frey@eit.uni-kl.de