

Potential von FlexRay optimal nutzen

Echtzeit-Fähigkeit im verteilten Regler-Entwurf – Teil 1

Zu den gängigsten Argumenten für den Umstieg von CAN nach FlexRay gehören eine höhere Bandbreite, Ausfallsicherheit sowie deterministisches Timing. Aber auch bei FlexRay treten an der Schnittstelle zwischen Bus und ECU unerwünschte zeitliche Effekte mit hoher regelungstechnischer Relevanz auf, z.B. Frequenzumsetzungen, Verzögerungen und ECU-seitige Signal-Jitter, verursacht durch das ECU-Scheduling. Das Echtzeit-Potential von FlexRay optimal nutzen wird nur derjenige, der die Effekte versteht und kontrolliert und damit auch die ECU-Zulieferer mit systematisch erarbeiteten Anforderungen versorgt.

Von Dr. Kai Richter

Im ersten Teil dieses Artikels werden die komplexen Timing-Effekte unter die Lupe genommen und die besonderen Herausforderungen im Detail dargestellt. Im zweiten Teil wird gezeigt, wie das Werkzeug SymTA/S

zur Scheduling-Analyse und Optimierung die zeitlichen Effekte des Gesamtsystems sichtbar macht. Dies gibt System-Architekten und Vernetzern die notwendige Kontrolle, um die Vorteile FlexRay-basierter Architekturen

systematisch zu bewerten, das Echtzeit-Potential von FlexRay optimal zu nutzen und präzise Timing-Anforderungen an die ECU-Zulieferer zu spezifizieren. Und auch die ECU-Anbieter profitieren durch die Möglichkeit, das ECU-Timing frühzeitig gegen die OEM-Anforderungen abzusichern.

Heutige Regelungsaufgaben im Automobil sind überaus komplex, und der Entwurf fordert die Kompetenz verschiedener Disziplinen, insbesondere Regelungstechnik, Signalverarbeitung, Fahrdynamik, aber auch Systementwurf. Die Betrachtung des Zeitverhaltens spielt bei allen Disziplinen eine wichtige Rolle. Die klassische (analoge) Regelungstechnik (Bild 1) geht von einer idealisierten Abtastregelung aus, von kontinuierlichen Werten und einer nahezu verzögerungsfreien Reaktion. Für eine digitale Realisierung

in Hardware und Software sind dann geeignete Ausführungs-Frequenzen (Sample Rates) für den Regelalgorithmus zu wählen, und zwar so hoch wie nötig für eine schnelle und stabile Regelung, aber so niedrig wie möglich, um Rechenleistung nicht unnötig zu verbrauchen, denn dies erhöht die Kosten. Genauso unterliegen die maximal zulässigen Reaktionszeiten der Regelfunktionen gewissen Beschränkungen, die ebenfalls die Qualität der Regelung beeinflussen: je „älter“ die Daten (als Latenz entlang des Signalpfades vom Sensor zum Aktor), desto schlechter die Vorhersage der geeigneten Regelmaßnahmen. Auch hier gilt: so schnell wie nötig und so langsam wie möglich. Mindestens sollten die erreichbaren Frequenzen oberhalb der Eigenfrequenz des zu regelnden Prozesses liegen. Für die Anforderungen an Frequenz und Reaktionszeit haben alle OEMs mittlerweile langjährige Erfahrungswerte, einige Timing-Daten von Audi finden sich z.B. in [1]. Fazit: Gesucht ist der beste Kompromiss zwischen Sicherheit, Qualität und Kosten.

Mit der Anbindung von Sensoren und Aktoren über das Netzwerk oder gar die Verteilung von Regelfunktionen auf mehrere ECUs kommt eine weitreichende Neuerung hinzu. Denn Kommunikation bedeutet zusätzliche Verzögerungen (Bild 2), die das Zeitverhalten der gesamten Regelung signifikant verändern können. Eine gemeinsame Taktbasis für alle ECUs ist bei FlexRay-Systemen zwar möglich, Kostengründe und Einschränkungen bei der Erweiterbarkeit sprechen aber häufig dagegen.

■ Herausforderung beim Systementwurf

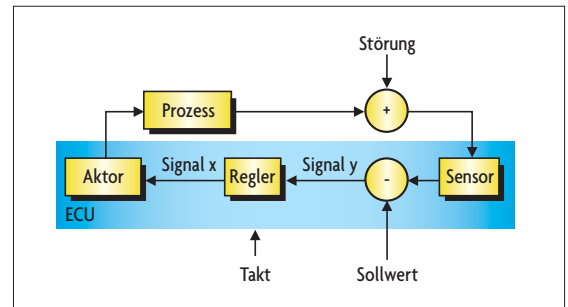
Nach dem klassischen Ansatz wird oftmals die gesamte Regelfunktion inklusive der Echtzeit-Anforderungen

vom OEM zur Implementierung an den Zulieferer übergeben (oder vom Zulieferer selbst entwickelt und dem OEM angeboten, z.B. ABS von Bosch). Der Zulieferer ist so für die Einhaltung der Vorgaben verantwortlich. Dies funktioniert, weil der Zulieferer über die Informations- und Entscheidungs-hoheit über das gesamte Regelsystem verfügt.

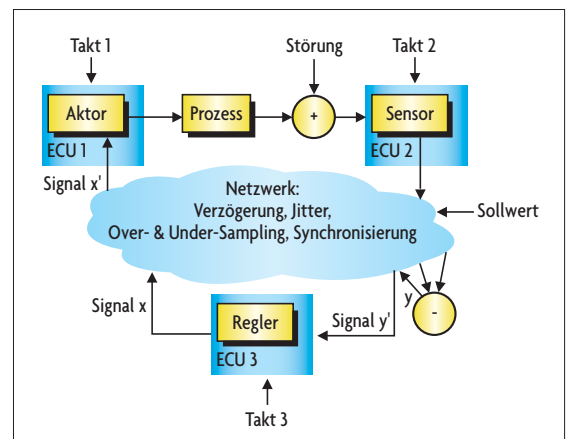
Mit der Einführung von verteilten Funktionen muss der OEM heute zunächst die Gesamtfunktion modularisieren und auf mehrere ECUs verteilen, bevor er Aufträge an ECU- und Software-Zulieferer vergibt. Eine zusätzliche technische Herausforderung besteht darin, dass das System während der Entwicklung nicht mehr „als Ganzes“ testbar ist, denn jeder Partner implementiert nur einen Teil des Systems. Das korrekte Zusammenspiel erst beim Integrationstest zu prüfen, ist offensichtlich zu spät, da Korrekturen hohe Kosten verursachen und ggf. sogar Entwicklungszeitpläne gefährden. Daraus ergibt sich eine Reihe neuer Fragen:

- ▶ Wie kann man das Timing von Software- und Hardware-Subsystemen gezielt vorhersagen und verifizieren?
- ▶ Wie können die geforderten Frequenzen und die Gesamtverzögerung in lokale Anforderungen für jede Komponente im Netzwerk bestimmt werden?
- ▶ Wer verantwortet welchen Teil der Gesamtverzögerung? OEM, Tier 1, BSW & OS-Konfigurator?
- ▶ Wie kommuniziert man dies zwischen den beteiligten Partnern möglichst „schmerz-frei“ im Rahmen bestehender Prozesse?
- ▶ Wie kann man das Zeitverhalten des Gesamtsystems optimieren?

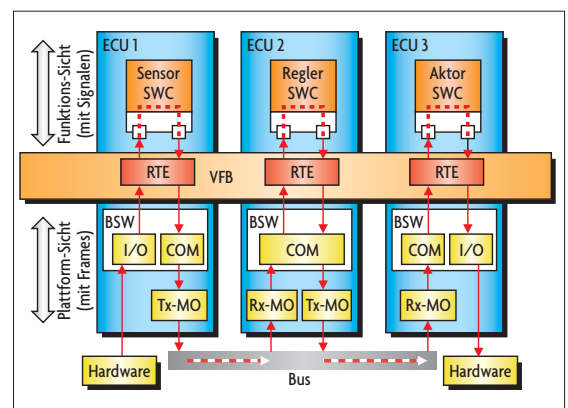
Die Beantwortung dieser (und weiterer) Fragen erfordert zunächst ein



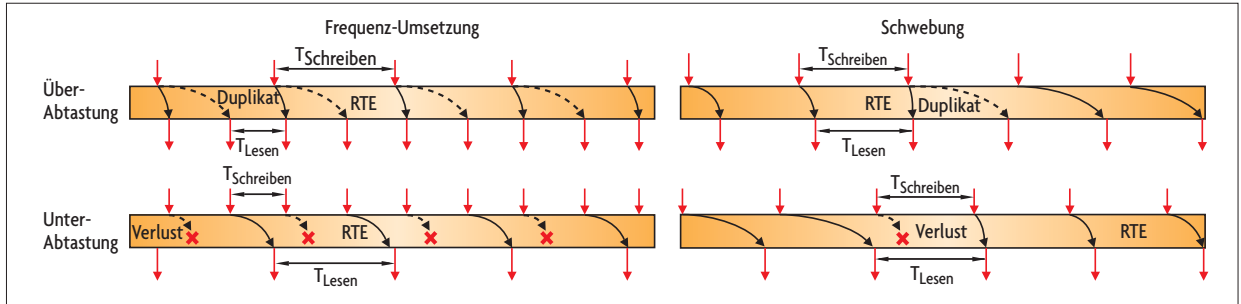
! Bild 1. Bei der klassischen Regelung gibt es konstante Signalverzögerungen und feste Taktung auf einer ECU.



! Bild 2. Bei der verteilten Regelung gibt es zusätzliche und häufig zeitlich schwankende Netzwerk-Verzögerungen und eventuell mehrere asynchrone Taktgeber.



! Bild 3. Die Software-Architektur eines verteilten Systems: Sensor, Aktor und Regler sind auf drei über FlexRay verbundene ECUs verteilt. Jedes neue Signal vom Sensor durchläuft die Komponenten: I/O – RTE – SWC – RTE – COM – FlexRay – COM – RTE usw.



! Bild 4. Auswirkung von Frequenzumsetzungen: Bei Über-Abtastungen werden Signale häufiger gelesen als geschrieben, es kommt zu Duplikaten. Bei der Unter-Abtastung ist es umgekehrt, es kommt zu Datenverlust durch Überschreiben.

Verständnis des Zeitverhaltens verteilter Systeme und dann einen systematischen Umgang damit. **Bild 3** zeigt den Signalfluss des Beispielsystems, diesmal unter Einbeziehung der Software-Architektur bei Verteilung auf drei ECUs. Die Abbildung orientiert sich am AUTOSAR-Standard, die Effekte existieren jedoch in vergleichbarer Form auch heute schon in nahezu allen verteilten Systemen. Im Idealfall durchlaufen alle Signale von der Sensor-Hardware alle Komponenten immer in derselben zeitlichen Folge, analog einem Fließband. D.h., alle Stufen haben dieselbe Frequenz und sind perfekt synchronisiert, so dass die zweite Stufe genau dann beginnt, wenn die erste Stufe fertig mit der Berechnung ist usw. In heutigen „zeitgesteuerten Systemen“ bedient man sich dazu gerne einer Taktung. In der Realität ist das Timing jedoch komplizierter, insbesondere durch die Einflüsse der Plattform bestehend aus Basis-Software, Bus-Kommunikation und Betriebssystem. Das hat mehrere Ursachen.

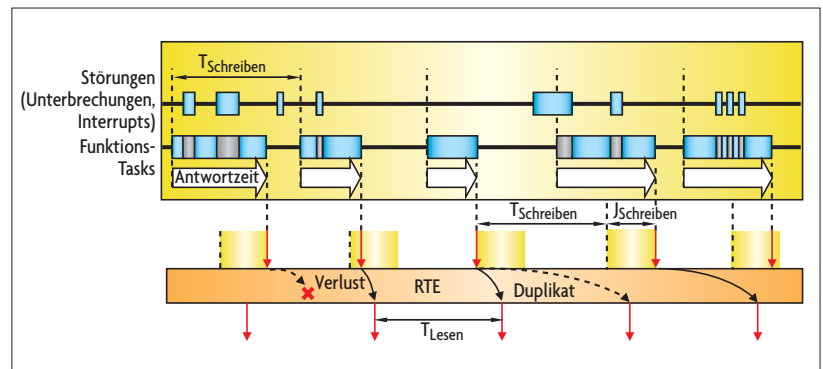
■ Über- und Unterabtastung

Nur selten haben alle Komponenten dieselbe Frequenz – teilweise aus Kostengründen (Unter-Abtastung, um die CPUs zu entlasten), teilweise weil nicht alle Frequenzen auf allen Komponenten technisch möglich (oder sinnvoll) sind. Zur Aktivierung von Software-Funktionen werden fast ausschließlich ganzzahlige Vielfache eines „Basistaktes“ verwendet; typische Werte sind 10, 20, 50, 100, . . . ms. Für FlexRay-Frames stehen meist nur Zweierpotenzen, d.h. 1, 2, 4, 8, 16 etc., der „Cycle Time“ zur Verfügung. Das führt zwangsläufig zu Frequenzumsetzungen zwischen den Signalen der An-

wendung (ECU-Software) und den Frames der Kommunikation (FlexRay).

Als Resultat findet man Komponenten einer Gesamtfunktion, die z.B. im Idealfall in einem Raster von 33,33 ms laufen soll, oftmals in mehreren Rastern wieder, z.B. 20, 30 und 40 ms. Derartige Frequenzumsetzungen werden in der Regelungstechnik als Über- und Unter-Abtastungen gezielt für Filterfunktionen eingesetzt. Hier handelt es sich hingegen um einen unbeabsichtigten Effekt mit der

Table“ auf einer ECU mit dem „Start of FlexRay Cycle“ auf dem Bus zu synchronisieren. Dadurch können die oben genannten Frequenzumsetzungen nicht gänzlich vermieden, deren dynamischer Einfluss (Schwankungen) jedoch eng begrenzt werden. Diese globale Synchronisation zwischen allen Software-Funktionen wird oft als besonderer Vorteil von FlexRay-Netzwerken propagiert. Ein Blick in die Entwicklungsprozesse der Automobilindustrie lässt jedoch erahnen, dass ein derartig radikaler Umstieg nicht über



! Bild 5. Zeitlicher Ablauf der Antwortverzögerung einer ECU. Die Software-Tasks werden zyklisch aktiviert, erfahren aber variierende Unterbrechungen. Dadurch werden die Ergebnis-Signale nicht mehr rein zyklisch an die RTE übergeben, sondern mit einem Jitter. In der Folge kann es zu Datenverlust und Duplikaten kommen.

Folge, dass einige Signale mehrfach übertragen werden, während andere „verloren“ gehen. Darüber hinaus implizieren Frequenzumsetzungen auch zusätzliche (und meist schwankende Verzögerungen) in den Puffern (in RTE und COM). **Bild 4** zeigt die Auswirkungen von Frequenzumsetzungen. Diese Verzögerungen gilt es möglichst frühzeitig zu erkennen und in die Auslegung des Reglers einzubeziehen.

Bei FlexRay besteht die Möglichkeit, mittels einer speziellen Service-Funktion den Start der „OS Schedule

Nacht zu erwarten ist. Vielmehr wird er sukzessive angegangen, indem ausgewählte Steuergeräte vom CAN auf den FlexRay-Bus verschoben werden. Oftmals wird dabei lediglich der COM-Layer ausgetauscht, Funktions-Software sowie OS werden aus Kostengründen wiederbenutzt. Als Folge werden sowohl synchrone als auch asynchrone ECUs an einem FlexRay-Bus zu finden sein. In solchen asynchronen Systemen kommt es mangels einer globalen Zeitbasis zu Schwebungen, die in ihren Auswirkungen denen der

Frequenzumsetzung gleich kommen (Bild 4).

Der dritte große Einfluss auf das Echtzeit-Verhalten ist das Betriebssystem-Scheduling (typisch OSEK, künftig auch AUTOSAR-OS), dem die Software-Komponenten (SW-C) unterliegen. Die Ausführung der enthaltenen Routinen (Runnables) innerhalb von Tasks wird durch höherpriorige SW-Tasks oder durch Interrupts verzögert oder unterbrochen. In der Folge werden die Signale verzögert an die Laufzeitumgebung (Run-Time Environment, RTE) übergeben. Da die Verzögerungen in der Praxis kaum konstant sind, weisen die Signale einen Jitter auf, so dass es auch ohne die o.g. Frequenzumsetzung zu doppelten und verlorenen Signalen kommen kann (Bild 5). Dieser Effekt kann nur auf Kosten zusätzlicher „Sicherheits-Wartezeiten“ wirksam verhindert werden. Natürlich liegt dieser Effekt mehr in der Verantwortung des ECU-Zulieferers, aber auch ein OEM tut gut daran, diese zu kennen, um in der Spezifikation von Anforderungen an Zulieferer die Weichen richtig zu stellen.

■ Zukünftige FlexRay-Systeme

Voll-synchron getaktete und verlustfrei kommunizierende Systeme sind, von physikalischen Fehlern abgesehen, mit FlexRay zwar möglich, haben aber ihren Preis. Die Einschränkungen bei der Wahl der Frequenzen wurden schon genannt. Hinzu kommt, dass auf den ECUs Leistungs-Reserven vorzuhalten sind, um auch in vorübergehenden Spitzenlast-Situationen das feste Zeitraster einhalten zu können. Das erhöht die Kosten für den Prozessor. Alternativ kann nur die Reaktionszeit verlängert werden, um auch mit weniger leistungsstarken Prozessoren ein voll-deterministisches System zu entwickeln.

Außerdem geht der so gewonnene Determinismus immer auch zu Lasten der Flexibilität, weitere Funktionen aufzunehmen und dadurch den FlexRay- und/oder ECU-Schedule erneut „durcheinanderzubringen“. Denn wenn auf dem FlexRay-Bus kein geeigneter Slot mehr frei ist, muss der Schedule geändert werden. Dies erfordert die Anpassung der Synchronisation und der Schedules aller betroffenen ECUs und ist mit weiteren Kosten verbunden.

In der Praxis ist daher auch mit Kompromissen zu rechnen, und OEMs und Zulieferer müssen mit Effekten von Über- und Unter-Abtastung, Asynchronität und Jitter leben, auch im Zeitalter von FlexRay und zeitgesteuerten Systemen. Wie auch immer – ob synchron oder asynchron, monolithisch oder verteilt getaktet: Wer erfolgreich und ohne späte (und teure) Überraschungen ein FlexRay-System aufsetzen möchte, tut gut daran, sich dieser Effekte bewusst zu sein und entsprechende Analyse- und Verifikations-Schritte im Prozess vorzusehen. Dies ist allerdings nicht so einfach, denn in Tests kann man den Signalen ihr Alter nicht ansehen. Vielmehr äußern sich „zu alte Daten“ in einer Reduzierung der Reglerqualität, die möglicherweise vom Fahrer als Qualitätseinbuße bemerkt wird, zum Beispiel, wenn das ESP „zu ruckeln beginnt“. Schlimmstenfalls schaltet sich ein elektronisches System ab.

Der zweiten Teil des Artikels zeigt auf, wie derartige Fehler zuverlässig vermieden werden können, wenn es heißt: „Scheduling-Analyse zur FlexRay-Optimierung bei OEMs und Zulieferern“. Es wird gezeigt, wie diese Effekte mittels Scheduling-Analysen zuverlässig kontrolliert und bereits beim Entwurf und in der Zusammenarbeit zwischen OEM und den Zulieferern

berücksichtigt und optimiert werden können. *fr*

Literatur

- [1] Reif, K.; Schmidt, K.: Vernetzte Regelsysteme im Kraftfahrzeug, ATZelektronik 2008, H. 4.
- [2] Richter, K.; Bartels, M.: Analyse des Zeitverhaltens von ECUs und Controller-Netzwerken. ATZ Elektronik 2007, H. 2.
- [3] Jersak, M.; Bartels, M.; Heckmann, R.; Franzen, B.: Sicher, nicht träge – Software in sicherheitskritischen Systemen. Design & Elektronik 2007, H. 1.
- [4] Richter, K.: Scheduling-Analyse zur optimalen und sicheren Auslegung der HW/SW-Zielplattform dynamischer Regelungssysteme. 4. VDI-Fachtagung „Steuerung und Regelung von Fahrzeugen und Motoren“, AUTOREG 2008.
- [5] Jersak, M.: Timing-Modell und Methodik für AUTOSAR. Elektronik Automotive Sonderausgabe AUTOSAR 2007, S. 9f.



Dr. Kai Richter

hat Elektrotechnik an der Technischen Universität Braunschweig studiert und promoviert (2004). Als anerkannter Experte im Bereich der Timing- und Performance-Analyse verteilter, eingebetteter Systeme hat er mehr als 50 Veröffentlichungen für international renommierte Zeitschriften und Konferenzen verfasst und weitaus mehr Vorträge zu diesem Thema gehalten. Seit 2005 ist er in der von ihm mit gegründeten Symtavigation GmbH als Geschäftsführer und Chief Technical Officer (CTO) für Technologie und Forschung verantwortlich. Symtavigation bietet Lösungen und Analyse-Werkzeuge einschließlich SymTA/S zur systemweiten Scheduling-Analyse von Echtzeitsystemen an.
info@symtavigation.com