Die zeitgesteuerte Architektur und FlexRay

Einleitung

Elektronische Systeme in Kraftfahrzeugen haben in den letzten Jahren enorm an Komplexität zugenommen. Aufgrund der beschränkten Übertragungsbreite in heute eingesetzten Bussystemen werden im Fahrzeug mehrere CAN-Busse nebeneinander eingesetzt. Jede neue Fahrzeuggeneration weist eine höhere Datenrate als der Vorgänger auf, was den Einsatz weiterer Busse unvermeidlich macht. Um dieser Tendenz gerecht zu werden, wurden in den letzten Jahren unterschiedliche Bussysteme entwickelt. Darunter auch das zeitgesteuerte Busprotokoll FlexRay™. Da es für deterministische und schnelle Datenübertragung sorgt und den wachsenden, sicherheitsrelevanten Anforderungen der Industrie, beispielsweise für X-By-Wire, gerecht wird, hat FlexRay das Potenzial zu einem wichtigen Kommunikationssystem im Automobil zu werden. Derzeit wird FlexRay nur zur Datenübertragung eingesetzt, die Möglichkeiten zur Synchronisation von Regelfunktionen bleiben ungenutzt. Nämlich den Betrieb verschiedener elektronischer Steuereinheiten (Electronic Control Units, ECUs) zu synchronisieren und somit eine höhere Ausfallssicherheit, Robustheit, Echtzeitfähigkeit und Determinismus zu erreichen.

In weiterer Folge soll dieser Artikel die zeitgesteuerte Architektur (Time-Triggered-Architecture, TTA) im Kontext von FlexRay erläutern.

Die zeitgesteuerte Architektur

Die Zeitsteuerung ist ein weit verbreitetes und erprobtes Konzept im Bereich der Embedded Systeme und kommt auch im Alltagsleben vor, wenn eine Steigerung der Effizienz auf Kosten der „Laufzeit-Flexibilität“ – also der Freiheit zur spontanen Entscheidung – sinnvoll oder notwendig ist, z.B. bei Fahrplänen von öffentlichen Verkehrsmitteln, Flugzeugen, oder für die Terminplanung für eine Gruppe von Personen.
Zeitgesteuerte Systeme zeichnen sich dadurch aus, dass wesentliche Aspekte ihres Verhaltens nicht durch „äußere Einflüsse“, sondern durch einen statisch vorgegebenen Ablaufplan gesteuert werden, wobei dieser Ablaufplan nach einem strikten zeitlichen Raster abgearbeitet wird. Somit sind der zeitliche Rahmen und die Zeitbedingungen von Anwendungen wichtige Kerneigenschaften von Echtzeitsystemen. Für ein verteiltes System (Programme und Daten werden auf verschiedenen Rechnern verteilt und von diesen arbeitsteilig bearbeitet) – um solche handelt es sich im Bereich der Automobilelektronik – bedeutet dies, dass wesentliche Aspekte des Gesamtsystems nur auf einem globalen Ablaufplan beruhen und mittels einer globalen Zeitbasis abgearbeitet werden. Unter wesentlichen Aspekten sind einerseits funktionale Eigenschaften wie z.B. Steuerungen, Regelungen usw., andererseits „strukturelle“ Aspekte wie beispielsweise Mechanismen zum Systemmanagement, verteiltes An- und Abschalten, Niederfahren, Fehlererkennung und Rekonfiguration, Redundanzmanagement usw. zu verstehen. Eine möglichst strikte Trennung dieser beiden Seiten hat entscheidende Vorteile für die Testbarkeit und Wiederverwendbarkeit von Modulen.
Idealerweise haben die zugrunde gelegten Technologie und der gewählte Entwicklungsansatz die Eigenschaft der Zusammensetzbarkeit: Bei der Integration von Teilsystemen kommt es zu keinerlei Änderungen an den Eigenschaften der Teilsysteme; die Eigenschaften sind somit „invariant bezüglich der Vollständigkeit des Systems“.
Die zeitgesteuerte Architektur ermöglicht diese Zusammensetzbarkeit nicht nur auf der Ebene des Kommunikationsprotokolls, sondern auch auf der Ebene der verteilten Algorithmen.

Die Gesamtfunktion des Systems verteilt sich auf Teilsysteme, die durch ein zeitgesteuertes Netzwerk miteinander verbunden sind .Die zeitgesteuerte Kommunikation benötigt keine spezielle CPU, erfordert allerdings einen eigenständigen Kommunikations-Controller. Dabei reduziert die TTA die Komplexität, die in ereignisgesteuerten Systemen durch die steigende Zahl an miteinander kommunizierenden Funktionen entsteht. Die nach wie vor schwierige Aufgabe, die unterschiedlichen Funktionen exakt zu koordinieren, kann und muss bereits in der Entwicklungsphase gelöst werden; dafür sind das Verhalten der Funktionen und ihre Koordination in der Integrationsphase stabil.

Ein FlexRay Ablaufplan weist allen Subsystemen voneinander getrennte Slots zu, während derer die jeweiligen Subsysteme exklusiven Zugriff auf den Bus haben. Die Slots wiederholen sich in einem vorher festgelegten Zyklus. Dieser Ablauf sorgt im Bussystem für Zusammensetzbarkeit auf der Ebene des Kommunikationssystems. Eine Überlastung des Kommunikationssystems ist deshalb praktisch ausgeschlossen, da die Verarbeitung von Eingabedaten, ihre Berechnung und Datenausgabe immer zu festen Zeiten erfolgen. Das ist aber keine hinreichende Voraussetzung für funktionale Zusammensetzbarkeit, denn diese erfordert sowohl die Softwaremodule als auch die Datenkommunikation. Aus diesem Grund ist es notwendig, den Entwicklungsprozess von Software und Kommunikation für viele Zulieferer systematisch, d.h. ausgehend von der globalen und dann zur lokalen Ebene hin, durchzuführen: zuerst die globale Planung, danach die lokale Validierung, die strikt auf der globalen Planung beruht. Diese Vorgehensweise wird als zweistufiger Entwicklungsansatz (Two-Level Design Approach) bezeichnet.

In Embedded Systemen ist die Zeitsteuerung ein seit längerem etabliertes Konzept. Sie wird nicht nur in der Automobilindustrie, sondern beispielsweise auch in der Luftfahrtindustrie (Fly-By-Wire- Cockpit von Honeywell) in einer Reihe von Serienprojekten eingesetzt.

Der zweistufige Entwicklungsansatz

Eine Architektur, die den zweistufigen Entwicklungsansatz unterstützt, unterscheidet zwischen Cluster- und Knotendesign:

- Die Entwicklung des physischen Cluster-Layouts, der Subsysteme und der Schnittstellen zwischen den Subsystemen erfolgt durch den Systemintegrator auf der Ebene des Clusters.
- Die Entwicklung und Implementierung der Subsysteme erfolgt durch die Zulieferer auf der Ebene der Rechnerknoten, ECUs, und beruht genau auf den Wechselwirkungen, die im Clusterdesign spezifiziert wurden.

Subsysteme in einem zeitgesteuerten Netzwerk

Der zweistufige Entwicklungsansatz sorgt für die Zusammensetzbarkeit der Subsysteme, die durch ein zeitgesteuertes Netzwerk miteinander verbunden sind. Subsysteme sind Einheiten, die Signale senden. Jedes Signal ist durch den Datentyp (Bit-Layout) und dem genauen Slot, in der es versendet wird, spezifiziert. Alle Subsysteme werden auf den elektronischen Steuereinheiten – das sind die Rechnerknoten, auf denen sie ausgeführt werden sollen – abgebildet. Ein Subsystem stellt gleichzeitig auch die kleinste Replikationseinheit dar und kann auf mehr als einem Knoten abgebildet werden. Wird ein Subsystem auf zwei ECUs abgebildet, so sind die durch das Subsystem erzeugten Signale im Netzwerk doppelt vorhanden. So können Störungen eines Subsystems toleriert und eine entsprechende Ausfallsicherheit gewährleistet werden.

Schnittstellen zum Kommunikationsnetzwerk

In einer zeitgesteuerten Architektur werden alle Subsysteme synchron ausgeführt. Dieser Vorgang wird von einer globalen, über das gesamte Netzwerk verteilten Zeitbasis gesteuert. Die Signale werden nach einem periodischen Ablaufplan ausgetauscht. Alle Rechnerknoten sind über eine Schnittstelle (Communication Network Interface, CNI) mit dem (zeitgesteuerten) Netzwerk verbunden. Die Schnittstelle „kennt" den Kommunikationsablaufplan und „weiß" von der Replikation gewisser Signale. Da die Schnittstelle die implementierten Subsysteme mit Signaldaten versorgt, muss die Applikation selbst weder den Ablaufplan „kennen" noch von Replikation „wissen" (*vgl. Abbildung 1*).

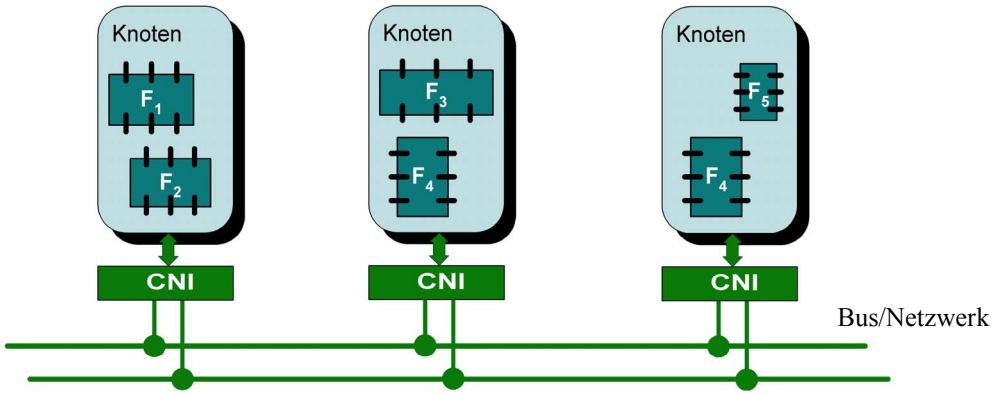

Abbildung 1: Knoten, Subsysteme und Schnittstellen zum Kommunikationsnetzwerk, F_y = repliziertes Subsystem

Wiederverwendbarkeit und Zusammensetzbarkeit

Ein wichtiger Aspekt der Software-Entwicklung für Automobilanwendungen ist die Wiederverwendbarkeit von Modulen und die Möglichkeit zur Einbindung von hardware-unabhängigen Modulen in das Steuergerät. Um Software-Module zu erstellen, die standardmäßig (off-the-shelf) verwendet und nach Anpassung gemeinsam mit anderen Modulen auf einer mehr oder weniger beliebigen Hardware-Plattform integriert werden können, sind Entwicklungskonzepte notwendig, die die Stabilität der Schnittstellen garantieren.

Im Bereich verteilter Systeme kommen Kommunikationsschnittstellen, Koordination von Ein- und Abschaltung, koordinierte Rekonfiguration und Reihenfolgeprobleme bei zyklischen Abhängigkeiten hinzu, und im Fall von Redundanzanforderungen ein entsprechendes Redundanzmanagement sowie gegebenenfalls Reintegration von Knoten nach temporären Fehlern. All diese Anforderungen müssen in stabile Schnittstellen umgesetzt werden, damit ein Modul bei der Integration in ein System entsprechend stabiles Verhalten zeigt.
In einem zeitgesteuerten System können Module mit konkreten, vom Hersteller getesteten und garantierten Werten für zeitliche Eigenschaften entsprechend diesen Anforderungen eingesetzt werden. Die Vorhersagbarkeit eines solchen Systems erlaubt eine Überprüfung der Gültigkeit dieser Werte noch in der Entwicklungsphase

Der zweistufige Entwicklungsansatz sorgt auch für die Zusammensetzbarkeit der Subsysteme. Ein System wird dann als zusammensetzbar bezeichnet, wenn kleinere, weniger komplexe Subsysteme entwickelt und dann ohne Nebeneffekte integriert werden können. Jedes Subsystem lässt sich unabhängig von anderen Subsystemen gemäß einer genau spezifizierten Signalschnittstelle entwickeln. Danach wird das Subsystem in den jeweiligen Cluster integriert. Diese Integration wirkt sich nicht auf andere, bereits im Cluster vorhandene Subsysteme aus, weil sich ein jedes Subsystem an das von der CNI bereitgestellte Signal-Netzwerk-Abbild hält. Somit macht die Integration von Teilsystemen keine Änderungen an den