



Bilder: Vector

Komplexität sinnvoll entzerren

Die **EMBEDDED-ENTWICKLUNG** schreitet zügig voran. Vor allem leistungsfähige Tools zur Entwicklung, zur Datenverwaltung und zum Übertragen der Software-Module in die Flash-Speicher der Steuergeräte gewinnen zunehmend an Bedeutung.

Ohne weitergehende Standardisierungen lässt sich die zunehmende Komplexität in der Automobilelektronik nicht mehr beherrschen. Fahrzeughersteller, wie etwa DaimlerChrysler, haben schon in den 90er Jahren mit erheblichem

Aufwand das Embedded-Betriebssystem OSEK (Offene Systeme und deren Schnittstellen für die Elektronik im Kraftfahrzeug) für Inhouse-Entwicklungen und für Zulieferkomponenten als verbindlichen Standard durchgesetzt.

Heute ist bei Fahrzeugherstellern und Zulieferern das echtzeit- und multitaskingfähige Betriebssystem die Basis für verbesserte Code-Qualität, gute Strukturierung und die Integration der Komponenten verschiedener Zulieferer. Auch in der 'Hersteller Initiative Software' (HIS) haben sich die großen Automobilhersteller auf einheitliche Standards verständigt.

Dazu wurden Arbeitskreise für die Bereiche Software, Software-Test, Process Assessment, Simulation und Tools sowie Flash-Programmierung eingerichtet. Für die Standards der künftigen Fahrzeuggenerationen ist das AUTOSAR-Konsortium (Automotive Open System Architecture) verantwortlich.

Zertifizierte OSEK-Implementationen gibt es von verschiedenen Herstellern. Die Einsatzbereiche der OSEK-Implementation 'osCAN' zum Beispiel erstrecken sich vom normalen Steuergerät über Multi-Bus-Gateways bis hin zu Schnittstellen-Hardware.

Kurze Reaktionszeiten

In dem Vector Interface für MOST VN2600 stellt 'osCAN' seine Leistungsfähigkeit mit einem 133-MHz-Altera-Excalibur-Controller durch die Verarbeitung von bis zu 35 000 Events/s unter Beweis. Dies entspricht einem Datendurchsatz von 1,7 MByte/s. Bei dem Gateway-Hersteller K2L haben sich Lösungen mit 'osCAN' aufgrund ihrer kurzen Reaktionszeiten und ihres genauen Timings bewährt.

Summary

Embedded Systems sind in nahezu allen Komponenten die Grundlage für die Entwicklung kostengünstiger, hochwertiger vernetzter Elektroniksysteme. Aufgrund des weiter steigenden Kostendrucks in den Elektronik wird ihre Bedeutung sogar noch steigen.

Zu den aktuellen Trends in der Automobilvernetzung zählt, die Anzahl der Steuergeräte in einem Fahrzeug zu reduzieren. Bis zu 40 Steuergeräte arbeiten heute in einem Oberklasse-Pkw. Um immer mehr Funktionen zu implementieren, müssen konsequenterweise künftig möglichst viele Applikationen auf dem selben Steuergerät laufen.

Das Multitasking Betriebssystem OSEK wurde für diesen Zweck spezifiziert. Für die Verwendung in sicherheitskritischen Systemen oder zur Integration von Software verschiedener Hersteller werden jedoch weitere Eigenschaften im Betriebssystem benötigt. Zum Beispiel darf keine Applikation parallel laufende Applikationen stören.

Timing im Mittelpunkt

Einer der Schwerpunkte bei der Weiterentwicklung der Embedded-Betriebssysteme in zukünftigen OSEK-Versionen beziehungsweise unter AUTOSAR liegt deshalb auf den notwendigen Überwachungsmöglichkeiten des Softwareverhaltens hinsichtlich Timing und Speicherzugriff. Die fortschrittlichsten Methoden zur Timing-Überwachung stellen AUTOSAR-konforme Implementierungen zur Verfügung.

Mit Methoden wie ‚Execution Time Enforcement‘ und ‚Arrival Rate Enforcement‘ wird auch niedrigprioritären Tasks ein Minimum an Zeitbudget zwingend zur Verfügung gestellt, so dass sich Fehler nicht nur entdecken,

sondern auch deren Quellen eindeutig identifizieren lassen.

Durch Speicherschutzfunktionen werden in Zukunft Zugriffe von Tasks auf den ihnen zur Verfügung gestellten Speicherbereich begrenzt. Dabei gilt es insbesondere, Schreibzugriffe auf fremde Datensegmente zu verhindern, Stack-Überläufe zu entdecken, aber auch das Ausführen von falschem Code zu unterbinden. Für Tasks, die zur selben Applikation gehören, braucht man andererseits Zugriffsmöglichkeiten auf dieselben Speicherbereiche.

Spezielle Systemfunktionen wie Treiber können darüber hinaus aber völlig unbegrenzten Speicherzugriff benötigen. Man unterscheidet zwischen so genannten ‚Trusted Applications‘ mit vollem Zugriffsrecht und ‚Non-trusted Applications‘ mit begrenzten Zugriffsmöglichkeiten. Dabei kann die Namensgebung zu Verwirrung führen: Auch ‚Non-trusted Applications‘ sind gesicherte Programme, die keinen Schaden anrichten können.

Gutes Design wird deshalb Funktionalitäten wo immer möglich in ‚Non-trusted Applications‘ legen. Vector Informatik bietet Implementierungen an, die zusätzlich den Aufruf von ‚Non-trusted Functions‘ erlauben. Sie sind prädestiniert für sicherheitskritische Anwendungen und bieten ein Maximum an Zuverlässigkeit. Ein entsprechender Vorschlag, dies in AUTOSAR ebenso zu handhaben, wird in einer Arbeitsgruppe zur Zeit diskutiert.

Die Überwachungsfunktionen für Timing und Speicher sind nur mit entsprechender Hardwareunterstützung effizient umsetzbar. Zum Speicherschutz braucht man Memory Protection Units (MPUs), deren Verwaltungsmöglichkeiten hinsichtlich Zahl und Größe der Speicherblöcke auf die Bedürfnisse der Automotive-Anwendungen zugeschnitten sind.

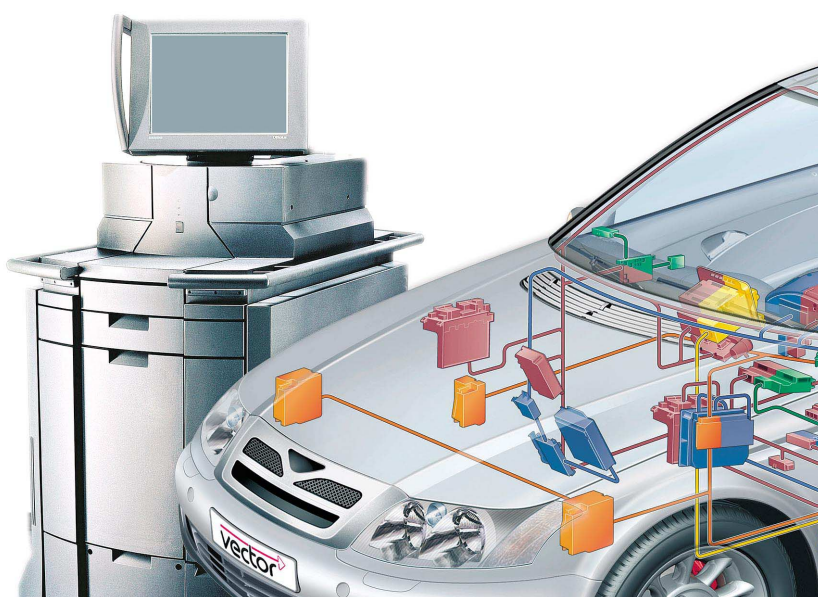
Kleinere Speichereinheiten

Vielfach lassen sich heute als kleinste Einheiten nur Blöcke mit 16 kByte Größe verwalten. Im Automotive-Embedded-Bereich werden jedoch deutlich kleinere Speichereinheiten benötigt.

Grundsätzlich sind die Anforderungen aktueller und künftiger OSEK-Echtzeitsysteme an die Hardware nur durch ein komplettes Redesign der aktuellen Prozessorkerne zu erfüllen. Über die Wünsche wird mit Halbleiterherstellern aktuell verhandelt.

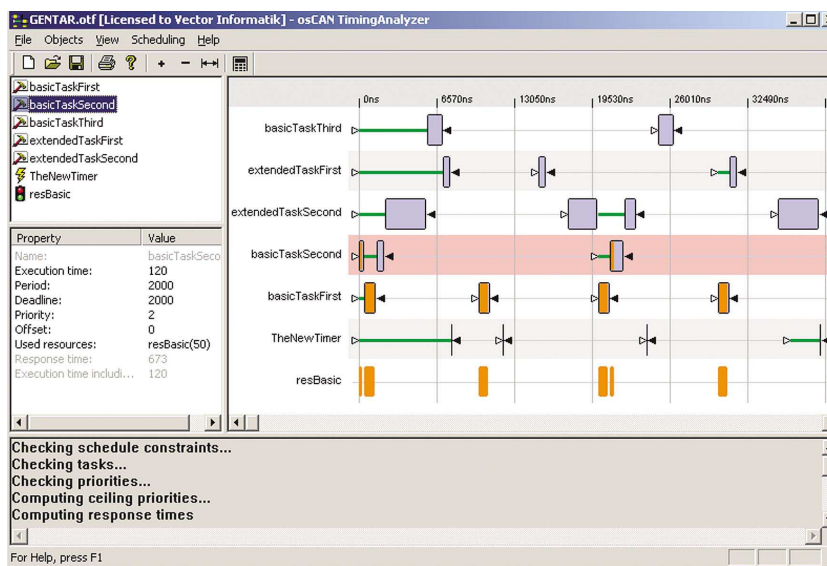
Zu den wichtigsten Forderungen zählen darüber hinaus auch ein Interrupt-Controller für verschiedene Interrupt-Level mit niedrigen Latenzzeiten, Hardware-Unterstützung beim Taskwechsel und Prozessorkerne mit möglichst kleiner Registerzahl.

Interessante Möglichkeiten zur Beherrschung der industriellen Komplexität liefern aktuelle Projekte durch den intensiven Einsatz der Mathematik in den Ingenieurwissenschaften. Mit systematischen Analyseverfahren lassen sich in Echtzeitsystemen Fehler aufdecken, die man mit



Autor Peter Liebscher betreut als Business Development Manager bei der Vector Informatik GmbH die Produktlinie Embedded Software Components.

Diagnose von Steuergeräten: Zur Funktionserweiterung müssen künftig mehr Anwendungen auf demselben Steuergerät laufen.



Richtiges Timing: Der ‚osCAN‘ TimingAnalyzer erlaubt die Simulation von Scheduling Tabellen (Fahrplänen) und die Berechnung der Schedulability.

Charakteristika. Zu den wesentlichen Unterscheidungsmerkmalen nichtflüchtiger Speichertypen zählen die Größe des Schreibsegments, die Größe des Löschesegments, die maximale Anzahl der Programmierzyklen sowie die zum Programmieren und Löschen benötigten Zeiten.

Die gegenwärtigen Flash-Speicher basieren auf den Technologien NOR Stacked Gate und MONOS (Metal Oxide Nitride Oxide Silicon). Ab circa 2008 rechnet die Branche mit neuen Speichertechnologien auf Basis von FeRAM (ferro-electric) oder MRAM (magneto-resistive), die gegebenenfalls unbegrenzt viele Schreib/Lösch-Zyklen erlauben.

HIS-standardisiertes Memory-driver-interface

Mit dem Ziel einer einheitlichen Speicherverwaltung wurde von der HIS-Automotive-Gruppe ein Standard für das Memory-driver-interface definiert, das zunehmende Unterstützung von Seiten der Halbleiterhersteller findet. Das Interface stellt die Funktionen zum Initialisieren, De-Initialisieren, Löschen, Programmieren und Lesen der Daten zur Verfügung.

Auf der Basis des HIS-Interfaces kann durch einen Multiple Memory Type I/O Manager der Zugriff auf unterschiedliche Speichertypen realisiert werden. Die Speicherkonfiguration lässt sich komfortabel über das Vector Tool Geny konfigurieren. Damit gewinnt man maximale Flexibilität beim Zugriff auf verschiedene Speichertypen, der sogar den Zugriff über das SPI (Serial Peripheral Interface) erlaubt.

Je nach Zahl der Steuergeräte dauert die Übertragung der Daten in der Serienproduktion eine volle Stunde und mehr. Fahrzeughersteller und Tool-Lieferanten denken deshalb über eine höhere Bandbreite der Übertragungsmedien und Datenkompression nach. Nach wissenschaftlichen Untersuchungen würde sich zur Kompression eine Kombination des LZ77-Verfahrens mit einer arithmetischen Kodiermethode am besten eignen und die Datenmenge bis auf die Hälfte reduzieren. *Peter Liebscher* ←

umfangreichen Tests kaum gefunden hätte.

Einen Schritt weiter gehen die Wissenschaftler des Verisoft-Projekts mit der Behauptung, dass es möglich sei, absolut fehlerfreie Embedded-Systeme und Elektronikkomponenten zu entwickeln. Mit den Methoden der formalen Verifikation lassen sich Gesamtsysteme, bestehend aus Hardware, Software, Betriebssystem, Kommunikation und Anwendung durchgängig verifizieren.

Die Rahmenbedingungen für die Flash-Programmierung variieren von Projekt zu Projekt

Immer größere Aufmerksamkeit erfordert die Reprogrammierung der Steuergeräte durch eine flexible Flash-Programmierung. Dabei wirft weniger die eigentliche Technik des Flashens Fragen auf, als vielmehr die Organisation und Behandlung des Gesamtprozesses.

Die Randbedingungen variieren von Projekt zu Projekt, wobei neben hersteller- und baureihenspezifischen Vorgaben unter anderem Hardware-Eigenschaften (Bootloader, Flash-Initiation), Flash-Formate, Transport- und Diagnoseprotokolle zu berücksichtigen sind. Passieren Flash-Daten beispielsweise diverse Gateways, muss sichergestellt sein, dass dort keine Daten verloren gehen können.

Diese und ähnliche Fragen müssen für jede Situation beantwortet werden. In der Praxis ist deshalb ein Automatis-

mus nicht einfach zu realisieren. Vor diesem Hintergrund gewinnt eine rationelle Handhabung der Flash-Prozesse immer größere Bedeutung.

Einer der Trends führt deshalb in Richtung einer einheitlichen Verwaltung in standardisierten Formaten. Die Werkzeuge von Vector Informatik speichern zu diesem Zweck die Flash-Daten zusammen mit Referenzen auf die Flash-Jobs in einem ODX-Flashdaten-Container.

Unter Umständen sollen Flash-Daten im Nachhinein durch einen Post-Build-Prozess verändert werden können. Wichtig ist in diesem Zusammenhang, dass neben den veränderten Parametern auch Checksummen und Signaturen neu zu berechnen sind und beim Flash-Update an den Flash Bootloader zu schicken sind. Mit den Tools CANape Graph und CANDito lassen sich sowohl Online als auch Offline Post-Build-Prozesse elegant beherrschen, wobei eine auf Flash- und Diagnoseaufgaben optimierte Script-Sprache sehr hilfreich ist.

Ein wichtiges Thema beim Reprogrammieren ist die Verwaltung verschiedener Speichertypen auf einem Steuergerät. Steigende Komplexität, zum Beispiel in Multiprozessor- oder verteilten Systemen, geht einher mit größeren Speicheranforderungen und einer Verwendung unterschiedlicher Speichertypen.

Die gebräuchlichen nichtflüchtigen Speichereinheiten haben teils sehr unterschiedliche physikalische