

OSEK soll sicherer werden

Das OSEK-OS (Offene Systeme und deren Schnittstellen für die Elektronik im Kraftfahrzeug) wurde in den 90er-Jahren von Automobilherstellern und Zulieferern auf breiter Front eingeführt. Mit der Weiterentwicklung der Kfz-Elektronik gehen neue Anforderungen an die Leistungsfähigkeit des Betriebssystems einher. Schwerpunkte künftiger Implementierungen sind Sicherheit und Zuverlässigkeit.

Die Merkmale der künftigen OSEK-Systeme orientieren sich wesentlich an den Vorgaben der verschiedenen Standardisierungsgremien wie der HIS (Hersteller-Initiative-Software) oder dem AUTOSAR-Konsortium (Automotive Open System Architecture). Die wichtigsten aktuellen Forderungen sind, zeitkritische Tasks überwachen zu können sowie erweiterte Schutzmaßnahmen beim Speicherzugriff. „Beide Eigenschaften spielen künftig insofern eine Rolle, da die Funktionalität elektronischer Komponenten im Auto einerseits weiter steigt und andererseits die Anzahl der Steuergeräte begrenzt bzw. reduziert werden soll“, erklärt Peter Liebscher, Business Development Manager bei Vector Informatik. „Bei einer intensiven Nutzung der Multitaskingfähigkeiten von OSEK, insbesondere wenn Applikationen verschiedener Zulieferer auf demselben Steuergerät laufen, sind erweiterte Schutzfunktionen unabdingbar.“ AUTOSAR-konforme Betriebssysteme werden in Zukunft die wohl fortschrittlichste Möglich-



„Der zusätzliche Aufruf für OSEK ‘Non-trusted Functions’ bietet ein Maximum an Zuverlässigkeit“, Peter Liebscher, Vector Informatik

keiten für die Überwachung des Verhaltens von Software hinsichtlich Timing und Speicherzugriff bieten. Um das Zeitverhalten unter Kontrolle zu halten, wird mit Methoden wie „Execution Time Enforcement“ und „Arrival Rate Enforcement“ auch niedrigprioritäre Tasks ein Minimum an Zeitbudget zwingend zur Verfügung gestellt. So lassen sich Fehler nicht nur entdecken, sondern auch deren Quellen eindeutig identifizieren. Ein HIS-Protected-OSEK dagegen setzt für Laufzeitüberwachungen das weniger leistungsfähige Dead-

line-Monitoring ein, mit dem sich zwar Laufzeitüberschreitungen detektieren, nicht jedoch die Ursachen aufdecken lassen. Bei der Erweiterung des Speicherschutzes geht es vor allem darum, Zugriffe auf fremde Datensegmente zu verhindern, Stack-Überläufe zu entdecken und das Ausführen von falschem Code zu unterbinden. „Da es sowohl „Trusted Applications“ mit vollen Zugriffsrechten als auch „Non-trusted Applications“ mit begrenzten Zugriffsmöglichkeiten gibt, sollten in den Applikationen wo immer möglich Non-trusted Functions eingesetzt werden, die keinen Schaden anrichten können“, ergänzt Liebscher. „Daher bieten wir OSEK-Implementierungen an, die zusätzlich den Aufruf von Non-trusted Functions erlauben. Sie bieten ein Maximum an Zuverlässigkeit und sind somit für sicherheitskritische Anwendungen prädestiniert.“

(Peter Liebscher/mh)

Vector Informatik

Tel. +49(0)711 806700

InfoClick

166676