

Das EB tresos Safety OS - ein AUTOSAR kompatibler Microkernel für sicherheitsrelevante Anwendungen

Dr. Horst Laschinsky
Elektrobit Automotive GmbH
Erlangen, Germany

Funktionale Sicherheit stellt ein integrales Merkmal heutiger Software im Automotive-Umfeld dar. Auch die Elektrobit Automotive GmbH (kurz „EB“), einer der Marktführer im Bereich AUTOSAR basierter Lösungen für Steuergeräte im Automobil, bietet mit ihrem „EB tresos Safety OS“ ein Echtzeit-Betriebssystem an, welches höchsten Sicherheitsanforderungen gerecht wird.

Nach einer kurzen Übersicht über den AUTOSAR Standard wird das von EB entwickelte Safety OS präsentiert. Hierbei handelt es sich um eine Microkernel-basierte Implementierung des AUTOSAR-OS Moduls (dem eigentlichen Betriebssystemkern), welche für sicherheitsrelevante Anwendungen bis hin zu ASIL-D geeignet ist. Der Vortrag stellt die Probleme dar, die sich bei einer ASIL-D tauglichen Umsetzung der AUTOSAR-OS Spezifikation ergeben und zeigt die Vor- und Nachteile verschiedener möglicher Lösungsansätze auf. Anschließend werden die Design-Entscheidungen der EB-Lösung im Detail vorgestellt. Hierbei werden im Speziellen die Kernel-Eintritts- und Austrittspunkte, die Fehlerbehandlung und die Schnittstellen zu den nicht-sicherheitsrelevanten Funktionen („QM-Teil“) beleuchtet.