Software steuert immer mehr sicherheitskritische Funktionen im Fahrzeug

Gefragter Sicherheitsstandard

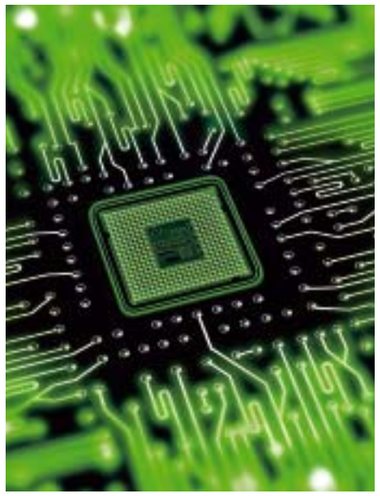
Realisierung softwarerelevanter Funktionen im Automobil

Software spielt eine immer wichtigere Rolle bei der Entwicklung von Fahrzeugen. Ob Infotainmentsystem, Einparkhilfe, Abstandswarner, ESP oder ABS – ein Großteil aller Funktionen im Auto wird inzwischen von Software gesteuert. Das bedeutet aber, dass die Kontrolle der Sicherheitsanforderungen für Autos immer komplexer wird.

Der Autor Dr. Alexander Mattausch ist Project Manager bei der Elektrobit Automotive GmbH, Erlangen

Selbst kleinste Bauteile, wie zum Beispiel Steuergeräte, die das reibungslose Zusammenspiel der Komponenten im Fahrzeug regeln, müssen daher strengste Sicherheitskriterien erfüllen. Dies gilt umso mehr, als die zunehmende Anzahl elektronischer Bauteile im Fahrzeug dazu führt, dass die Autohersteller immer mehr Funktionen in einer immer geringeren Anzahl von Steuergeräten bündeln.
Wichtig ist dabei zunächst die Unterscheidung zwischen zwei verschiedenen Sicherheitskonzepten, die im Englischen mit den Begriffen „Security“ und „Safety“ bezeichnet werden. Im ersten Fall geht es um ein System, das gegen Angriffe und Manipulationen von außen geschützt ist, also um Themen wie Softwareintegrität, Verschlüsselung, Digital Rights Management oder Zugangskontrolle. Die sogenannte funktionale Sicherheit hingegen befasst sich mit der Ausfallsicherheit eines Systems, sie soll gewährleisten, dass ein System stets sicher und zuverlässig arbeitet oder im Fall von eventuellen Problemen automatisch in einen sicheren Zustand zurückversetzt wird, damit keine Menschenleben gefährdet werden. Die Richtlinien, Prozesse und Grenzen, die Softwareentwickler für Automobilanwendungen erfüllen und einhalten müssen, um diese Ausfallsicherheit zu garantieren, beschreibt der Standard ISO 26262.
So legt die Richtlinie zum Beispiel bereits für die Konzeptphase fest, dass das Gesamtsystem sowie alle zu entwickelnden Einzelkomponenten auf potenzielle Risiken geprüft werden. Diese Risikoanalyse umfasst eine Grundsatzanalyse, die verschiedenen Arbeitsmodi, die Ermittlung eventueller Gefahren, Fehlermöglichkeits- und Einflussanalyse, Fehlerbaumanalyse, Gefahreneinstufung sowie die Einschätzung der jeweiligen Auswirkungen. Dann werden Sicherheitsziele definiert und den einzelnen Komponenten zugeordnet.

Das EB-tresos-Safety-Betriebssystem ermöglicht die Entwicklung von Steuergeräten bis zum höchsten Sicherheitslevel ASIL D



Autohersteller bündeln immer mehr Funktionen in einer immer geringeren Anzahl von Steuergeräten

Schließlich überprüfen die Entwickler das Konzept erneut und fassen alle Ergebnisse in einem Dokument zusammen.

Bedeutung von Autosar
Um die Komplexität zu verringern und eine Wiederverwendung von Softwarekomponenten auch über Herstellergrenzen hinaus zu ermöglichen, greifen die meisten Automobilhersteller bei der Entwicklung von Steuergeräten auf die Autosar-Architektur zurück. Die einzelnen Komponenten unterscheiden sich dabei hinsichtlich ihrer Sicherheitsrelevanz und werden daher mit verschiedenen ASIL-Leveln (Automotive Safety Integrity Level) bewertet. Werden verschiedene Komponenten zusammengefasst, gilt der jeweils höchste ASIL-Level. Für ASIL-Projekte schreibt der Standard ISO 26262 zudem vor, dass neben dem Projektmanager auch ein Safety Manager zur Verfügung steht, der sicherheitsrelevante Aktivitäten plant, koordiniert und überwacht.
Für die Erfüllung der Sicherheitskriterien gemäß ISO 26262 sind verschiedene Ansätze möglich. Zum einen, dass sämtliche Komponenten des Systems die Kriterien einlösen. Ein zweites Konzept ist die Redundanz, was in diesem Fall bedeutet, dass sicherheitsrelevante Hard- und Softwarekomponenten jeweils mehrfach zur Verfügung stehen. Ein dritter Weg ist die Aufteilung in sicherheitsrelevante und nicht sicherheitsrelevante Softwarekomponenten. Hierzu werden die einzelnen Komponenten voneinander isoliert, um Rückwirkungsfreiheit zu gewährleisten – ein Fehlverhalten einer Komponente darf auf keinen Fall andere Komponenten beeinflussen. Sicherheitsrelevante Bestandteile werden zudem mit einer speziellen Prüffunktion versehen, um Fehlfunktionen oder Ausfälle auszuschließen.
Auf den ersten Blick scheinen sich Autosar und funktionale Sicherheit nur schlecht miteinander zu vertragen. Während sicherheitskritische Anwendungen möglichst einfach gehalten sein sollten, bietet Autosar mit seinen über 6000 Konfigurationsparametern und weit mehr als 100 000 Zeilen Code einen fast unendlichen Variantenreichtum. Durch eine geschickte Kapselung und Verwendung der Speicherschutz-Funktionalitäten moderner Prozessoren ist es jedoch möglich, Sicherheitsmechanismen auf einzelne Autosar-Module aufzusetzen. So reduziert sich der nach dem höchsten ASIL-Level zu entwickelnde Code, während gleichzeitig ein Sicherheitsgewinn durch die Reduzierung der Komplexität erreicht wird.
Die Entwicklung eines innovativen Betriebssystems für Autosar-Steuergeräte, das höchsten Sicherheitsansprüchen genügt, erfordert daher viel Zeit und Aufwand. Als einer der ersten Zulieferer bietet Elektrobit (EB) jetzt ein ASIL D zertifiziertes Autosar-Betriebssystem an. Als einziges System auf dem Markt ist es sogar für zwei Sicherheitsstandards zertifiziert. Die Zertifizierung für Funktionale Sicherheit der Bewertungsagentur Exida bestätigt, dass das EB tresos Safety Betriebssystem für den Einsatz in sicherheitskritischen Anwendungen, wie zum Beispiel elektrischen Servolenkungen, des Automotive Safety Integrity Levels D (ASIL D), geeignet ist. Gleichzeitig ist das Betriebssystem auch für das Safety Integrity Level 3 (SIL 3) für Anwendungen außerhalb des Automobilbereichs zertifiziert. ASIL D und SIL 3 zählen zu den höchsten Sicherheitsstandards für funktionale Sicherheit für elektrische und elektronische Komponenten.
Das Betriebssystem schützt sich selbst vor möglichen Fehlern, die von anderer Software auf dem Steuergerät verursacht werden können. Es stellt eine sichere Ausführungsumgebung zur Verfügung, die komplett unabhängig von nicht-sicherheitsrelevanter Software läuft. Für die Entwicklung dieser sicheren Umgebung übertrug EB bewährte Technologien auf die Autosar-Welt, wie beispielsweise das Mikrokernel- und das System Call-Konzept, die auch in der Luftfahrtindustrie und der Automatisierungstechnik eingesetzt werden. Neben einem sicheren Kontext-Switch schützt das EB tresos Safety OS auch sicherheitsrelevante Funktionen für Autosar-Systeme wie Task Scheduling, Event-Handling und Locking-Mechanismen. Das ermöglicht die Entwicklung von Steuergeräten bis zum höchsten Sicherheitslevel. Gleichzeitig senkt die sichere Partitionierung der Steuergeräte-Software den Aufwand für Sicherheitsanalysen und beschleunigt die Entwicklung von sicherheitsrelevanten Steuergeräten. Das Autosar-Betriebssystem wird bereits von mehreren großen deutschen Automobilherstellern in verschiedenen Serienprojekten eingesetzt. Es ist verfügbar für Sicherheits-Mikrocontroller von Freescale, STM, Infineon, Texas Instruments und Renesas.

Elektrobit Automotive , Tel.: 09131 77010, E-Mail: info.automotive@elektrobit.com