Mit ISO 26262 Hand in Hand

ETAS AUTOSAR-Basissoftware ist konform für ASIL-D:2018-Anwendungen

Je mehr Funktionen im Fahrzeug von Software übernommen werden, desto wichtiger wird funktionale Sicherheit. Die steigende Komplexität der E/E-Architekturen stellt eine weitere Herausforderung in der Entwicklung sicherer Software dar. Eine bewährte und zuverlässige Basissoftware ist dabei entscheidend für den Erfolg. TÜV SÜD hat die AUTOSAR-Softwareprodukte von ETAS auf ihre Eignung für den sicheren Einsatz in ISO 26262 ASIL-D-Anwendungen geprüft – und ihre Konformität bestätigt.

Funktionale Sicherheitsnormen wie ISO 26262 konzentrieren sich auf Maßnahmen zur Abwehr von Gefahren, die durch fehlerhafte E/E-Systeme verursacht werden. Diese Maßnahmen umfassen Indikatoren zur Qualifizierung von Soft- und Hardware. Aber reichen diese Indikatoren aus, damit Automobilhersteller und Tier 1s die Sicherheit ihrer Systeme qualifizieren können? Die Antwort lautet: sicherlich nicht, und das aus guten Gründen.

Komplexität beherrschen, Zeit und Geld sparen

Betrachtet man ein durchschnittliches, modernes Oberklassefahrzeug, so kann dessen Software leicht bis zu hundert Millionen Zeilen Code erreichen, mehr als das Vierfache der gesamten Software in einem F-35 Fighter-Jet von 2013. Angetrieben durch Elektrifizierung und autonomes Fahren sind die Automobilhersteller zu einer beispiellosen Welle von Veränderungen der E/E-Fahrzeugarchitekturen gezwungen. Diese Änderungen schmälern jedoch nicht das Sicherheitsbedürfnis der Fahrzeugnutzer. Im Gegenteil – die Verantwortung, die elektronische Systeme übernehmen, wird immer größer. Eine sichere Funktion ist daher essenziell.

Sicherheitsanforderungen über alle Systeme im Fahrzeug hinweg erfordern eine klare Strategie sowie Komponenten, die durch ihr Design sicher sind. Sicherheitsnormen definieren, was zu tun ist, sagen aber nicht wie. Hier können zertifizierte Komponenten helfen, den Aufwand zu reduzieren und die Strategie für eine größere Systemqualifikation zu unterstreichen.

Darüber hinaus stellen die immer kürzeren Entwicklungszyklen für Plattformen und der steigende Kostendruck die Automobilhersteller vor neue Herausforderungen. Jeder einzelne Prozessschritt, von der Beschaffung über die Software-Entwicklung bis zur Produktion, steht aus diesem Grund immer wieder auf dem Prüfstand.

Implementierung, Review und Auditierung sicherheitsrelevanter Software ist eine sehr teure, aufwendige und dennoch unvermeidliche Aufgabe. Aus diesem Grund ist es in vielen Fällen wichtig, auf bereits zertifizierten Komponenten aufzusetzen.

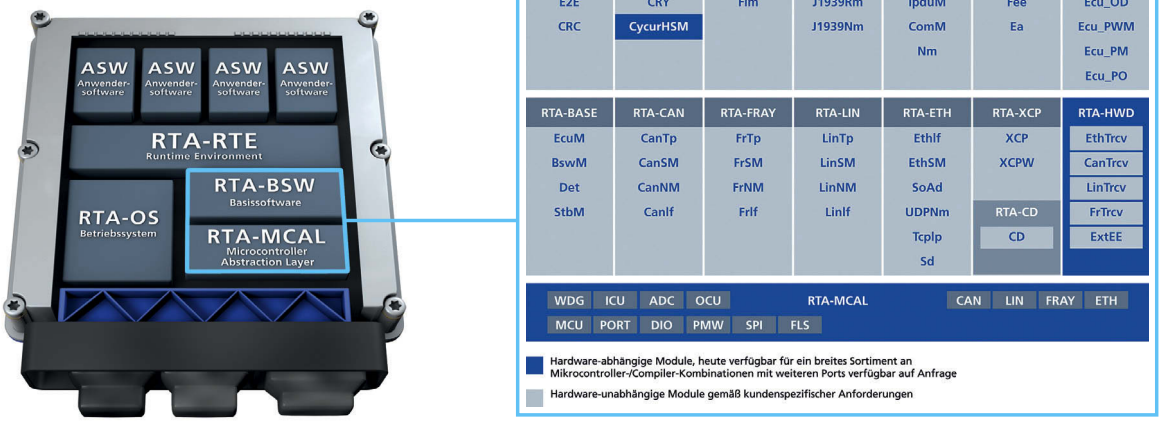
Das Projekt

Um Kunden bei der Entwicklung sicherheitsgerechter Systeme zu unterstützen, hat ETAS TÜV SÜD beauftragt, die AUTOSAR-Basissoftware RTA-BSW zu überprüfen. TÜV SÜD ist eine weltweit führende technische Service-Organisation und anerkannter Vertrauenspartner im Bereich der funktionalen Sicherheit. Die Überprüfung umfasste die Bewertung auf Konformität mit der Zertifizierung nach dem TÜV SÜD Smart Software Program einschließlich der Konformität mit den Anforderungen an die funktionale Sicherheit. RTA-BSW wurde hinsichtlich seiner Qualitäts- und Sicherheitseigenschaften bewertet:

- Allgemeines Sicherheitsmanagement
- Softwarespezifische Anforderungen in Bezug auf den Umfang der Software-Deliverables
- Software-Entwicklungsprozess

Was ist RTA-BSW?

RTA-BSW ist die serienreife AUTOSAR-Classic-Basissoftware von ETAS und Kern des RTA Classic-AUTOSAR-Produktportfolios RTA-CAR. Die Software enthält die Erfahrung von über 20 Jahren Einsatz im Automobil mit fast 2 Milliarden ECUs, die bisher ohne Fehler im Feld im Einsatz auf der Straße sind. RTA-BSW unterstützt AUTOSAR-R4.x-Funktionen und besteht aus einem umfassenden Satz von AUTOSAR-Stacks (Sammlung von Modulen), wie Kommunikation, Speicher, Diagnose und Sicherheit. Die Module der Basissoftware ermöglichen zentrale ECU-Kommunikationsfunktionen, die allgemein als gemeinsame Grundlage für die Entwicklung spezifischer Fahrzeugfunktionen angesehen werden.



RTA-BSW enthält alles, was Kunden für funktional sichere Anwendungen benötigen.

Der Umfang des Projekts umfasste mehrere Sicherheitsnormen, um PKWs, Motorräder, LKWs und Off-Highway-Maschinen abzudecken. Bei der Konformitätsbewertung wurden die folgenden Sicherheitsnormen verwendet:

- ISO 26262:2018
- IEC 61508:2010
- ISO/DIS 19014:2018
- ISO 25119:2018

Zusammenfassend zeigte die Bewertung, dass RTA-BSW die geltenden Anforderungen des TÜV SÜD Smart Software Program einschließlich des Moduls Funktionale Sicherheit erfüllt. Ein großer Erfolg für das RTA-Team von ETAS in Großbritannien, Deutschland und Italien. ETAS-Kunden steht durch RTA-BSW somit eine Basis zur Erfüllung hoher Sicherheitsanforderungen zur Verfügung.

Zusammenfassung

Die Automobilindustrie erlebt derzeit zahlreiche Veränderungen, die jeden einzelnen Schritt im Entwicklungsprozess der Automotive Software betreffen. Besonderer Schwerpunkt liegt dabei auf sicherheitsrelevanter Embedded Software. Der dringende Bedarf an neuen Einsparungen schafft die Notwendigkeit, sich auf differenzierende Faktoren zu konzentrieren und für die anderen Bereiche Standardkomponenten, wie beispielsweise AUTOSAR-Plattformen, einzusetzen. ETAS sorgt hierbei mit zertifizierten AUTOSAR-Basissoftware-Produkten für höchste Sicherheitsanforderungen, sodass ETAS-Kunden die anstehenden Herausforderungen erfolgreich meistern können.

Autoren

Luca Baldini ist Produktmanager für RTA-BSW bei ETAS Ltd. in York, Großbritannien. **Daniele Garofalo** ist Global Head of Product Management RTA Solutions bei ETAS Ltd. in York, Großbritannien. **Jonathan Manktelow** ist Projektmanager für die Safety-Zertifizierung bei ETAS Ltd. in York, Großbritannien.