

Mit AUTOSAR zu zertifizierter Sicherheit

Erfolgsgeschichte von Beijing New Energy Automobile

AUTOSAR setzt sich auf dem Automobilmarkt zunehmend als Referenz für die Entwicklung kompletter Steuergeräte-Software-Stacks durch. Die Vorteile höherer Effizienz, kürzerer Markteinführungszeiten und vollständiger Funktionsabdeckung werden in vielen Bereichen immer deutlicher, da AUTOSAR zu einem ausgereiften, rundum einheitlichen Standard für die Entwicklung von Embedded-Anwendungen wird - einschließlich der schnell wachsenden Domäne Elektrofahrzeug (EV). Beijing New Energy Automobile (BJEV) vertraut bei der Einführung von AUTOSAR für seine Steuergeräte auf ETAS.



Über BJEV

Beijing New Energy Automobile Co., Ltd., ein Tochterunternehmen von Beijing Automotive Group Co., Ltd., ist Chinas größter Elektrofahrzeughersteller. Das Unternehmen produzierte im Jahr 2017 über 100.000 Fahrzeuge – bald dürften es sogar über 230.000 sein. Als OEM für alternativ angetriebene Fahrzeuge trägt BJEV maßgeblich zu Chinas staatlichem Modernisierungsfahrplan „Made in China 2025“, einer Initiative zur Aufwertung der chinesischen Industrie.

Die Herausforderung

In den vergangenen Jahren hat sich die Automobilbranche tiefgreifend verändert. Zu den Hauptfaktoren zählen zweifellos die neuen Normen für funktionale Sicherheit, also ISO 26262 für Personenwagen bzw. ISO 25119 für Landmaschinen, welche die Prozesse und Verfahren in der Software-Entwicklung wesentlich beeinflussen.

Für das Projekt mit BJEV mussten Steuergeräte wie das E-Motor-Steuermodul (MCU), das Fahrzeugsteuergerät (VCU) und das Batteriemanagementsystem (BMS) gemäß ISO 26262 für ASIL-C entwickelt und zertifiziert werden. Besonders komplex wurde die Aufgabe durch die parallele Einführung etwa von AUTOSAR und mehreren Sicherheitsmaßnahmen.

Die sicherheitstechnisch größte Herausforderung bestand in der effizienten Umsetzung des Konzepts der Rückwirkungsfreiheit („Freedom of Interference“). Dieses ermöglicht es, gleichzeitig sicherheitskritische und -unkritische Softwarefunktionen im selben Ausführungskontext, also auf einem einzigen Steuergerät, auszuführen. Übliche Strategien für Rückwirkungsfreiheit sind:

- Speicherschutz, um sicherheitskritische von -unkritischer Software abzugrenzen
- Schutz vor korrupten Daten etwa mittels End-to-End-Signaturen, um zu erkennen, ob Dateninhalte gültig sind und in der richtigen Reihenfolge empfangen werden
- Sequenzielle Programmausführung mittels Ablaufüberwachung, um die Ausführung unerwarteter Sequenzen zuverlässig zu erkennen

Das Vorhaben erforderte neben den Maßnahmenpaketen detailliertes, präzises Projektmanagement in verschiedenen Bereichen. Dank der Beratungs- und Engineering-Services von ETAS konnte BJEV sich ganz auf seine Innovationsthemen konzentrieren.

Projekttablauf

Das Projekt verlief in drei Schritten: Zunächst benötigte BJEV Know-how zu AUTOSAR und insbesondere zur VCU-Entwicklung. Dabei unterstützte ETAS den Kunden durch Schulungen, beim Engineering mit dem RTA Basic

Software Release Package (RTA-BSW), der Integration der Mikrocontroller-Abstraktionsschicht (MCAL/CDD), dem Feinschliff der Basissoftwarekonfiguration, der Fehlerbehebung vor Ort und mit Beratung rund um die Integration von Softwarekomponenten. In der entscheidenden Anfangsphase konnte BJEV so einen konkreten Zukunftsplan für Steuergeräte auf AUTOSAR-Basis schmieden und die Weichen für ein effizienteres, hochwertigeres Endprodukt stellen.

Anschließend übertrug BJEV die AUTOSAR-Architektur auf BMS und MCU. Dazu musste unter anderem RTA-OS (Betriebssystem) auf die Mikrocontroller TI TMS570 und IFX TC234 portiert werden.

Abschließend folgte die Qualifizierung sämtlicher Steuergeräte-Software-Stacks für funktionale Sicherheit, bei der TÜV, BJEV und ETAS gemeinsam an der ASIL-C-Konformität arbeiteten. ETAS unterstützte BJEV mit dem ganzheitlichen Functional Safety Qualification Package dabei, die Anforderungen der ISO 26262 zu erfüllen. Dieses enthält Sicherheitshandbücher und -nachweise sowie Assessment-Berichte und Sicherheits-Reviews.

Fazit

Sich ändernde Automotive-Normen und -Vorgaben sowie der immer restriktivere, stärker regulierte und komplexere Markt erschweren es OEMs zusehends, mit innovativen Fahrzeugen Erfolge zu landen. Besonders wichtig ist es für die Hersteller, Kosten vertretbar zu halten und Neuheiten trotz steigender Komplexität schneller auf den Markt zu bringen. Die Produkte und Erfahrung von ETAS brachten BJEV schnell und reibungslos zum Ziel: Dank standardisierter AUTOSAR-Komponenten von ETAS und modernster Verfahren erforderte die vollständige Unterstützung der ISO-Norm 26262 für ASIL-C nur minimalen Entwicklungsaufwand.

„Die AUTOSAR-Lösungen von ETAS bringen unsere Projekte rasant voran“, freut sich Yu Jun, stellvertretender Leiter der Strategie-Entwicklung bei BJEV. „Mit dieser soliden Basis können wir uns voll und ganz auf unsere Innovationen konzentrieren. Auch die gute Zusammenarbeit und der kompetente Support von ETAS haben maßgeblich zum Projekterfolg beigetragen.“

Autoren

Tang Yi ist Hub Manager RTA Solutions bei ETAS in Shanghai, China. **Daniele Garfalo** ist Global Head of Product Management RTA Solutions bei ETAS Ltd. in York, Großbritannien.