Zugeschnittene Entwicklungsprozesse für die Nutzfahrzeugbranche

TÜV-zertifizierte generische ASIL-C Steuergeräte nach ISO26262 und ISO21434

In den letzten Jahren hat die Entwicklung von elektronischen Fahrzeugfunktionen in der Nutzfahrzeugindustrie enorm an Bedeutung gewonnen. Um sicherzustellen, dass diese Funktionen sicher und zuverlässig sind, hat die International Organization for Standardization (ISO) den Standard ISO 26262 entwickelt. Dieser Standard etabliert sich zunehmend als Norm für die Entwicklung von Fahrzeugfunktionen und hat weitreichende Auswirkungen auf kleine und mittlere Unternehmen in der Nutzfahrzeugbranche. Darüber hinaus gewinnen Anforderungen an die Cybersicherheit der EE-Architektur gemäß ISO 21434 in immer mehr Anwendungsfällen an Bedeutung.

Frank Steinert, Roland Mader und Daniel Magnus

Die Normen ISO 26262 und ISO 21434 sind speziell für die Entwicklung sicherheitskritischer elektronischer Systeme in Fahrzeugen konzipiert. Diese Standards umfassen den gesamten Entwicklungsprozess von der Konzeptphase bis zur Serienproduktion und legen detaillierte Anforderungen für die einzelnen Schritte fest.

Die Einführung dieser Standards erfordert von kleinen und mittleren Unternehmen in der Nutzfahrzeugbranche erhebliche Anstrengungen. Diese Unternehmen müssen ihre Entwicklungsprozesse neu ausrichten und sämtliche Entwicklungsphasen sorgfältig dokumentieren. Oftmals übertreffen die Anforderungen an die bestehenden Prozesse der Hersteller oder Zulieferer in der Nutzfahrzeugbranche die tatsächliche Praxis bei weitem.

Die Anwendung der Normen wirkt sich auch auf die Hardwareentwicklung elektronischer Steuerungen aus, die dadurch sehr viel aufwendiger wird, als dies bisher der Fall war. Die Entwicklung von generischen Steuergeräten, die unabhängig von der Zielanwendung alle Voraussetzungen für die Steuerung sicherheitskritischer Funktionen erfüllen, ist auf dem Markt selten, da die Entwicklung mit erheblichen Kosten und Aufwänden verbunden ist.

Um die Aufwände aus Prozess, Hardwareentwicklung und Softwareentwicklung einzelner Fahrzeugfunktionen für typische Kunden aus der Nutzfahrzeugbranche handhabbar zu gestalten, haben die Unternehmen ECUtronic GmbH und Sontheim Industrie Elektronik GmbH eine durchgängige Prozesskette inklusive generischem

© Sontheim Industrie Elektronik GmbH

Steuergerät erstellt. Hierbei werden die Anforderungen an einen durchgängigen Entwicklungsprozess gemäß ISO 26262 erfüllt und auch Lösungen gemäß ISO 21434 berücksichtigt, ohne dass eine aufwendige anwendungsspezifische Hardwareentwicklung erforderlich ist.

Das zentrale Element ist ein TÜV-zertifiziertes, generisches Steuergerät der Sontheim Industrie Elektronik GmbH mit einer Vielzahl von sicheren Ein- und Ausgängen auf ASIL-C-Niveau sowie prozesstechnisch abgetrennten QM-Bereich für weniger sicherheitsrelevante Funktionen. Parallel zur zertifizierten Hardware wurde auch die sogenannte Middleware – die Softwareschicht zwischen Hardware und kundenspezifischer Applikation – in die Zertifizierung eingeschlossen. Dadurch entfallen die sehr zeitaufwändigen Arbeiten für diese Punkte in der kundenspezifischen Anwendung.

Um die gewünschten kundenspezifischen Funktionen auf der Zielhardware gemäß ISO 26262 zu implementieren, sind eine Vielzahl von konzeptionellen und gestaltenden Prozessschritten erforderlich, die der Umsetzung vorgeschaltet sind. In diesem Bereich hat sich ECUtronic auf die spezialisiert.

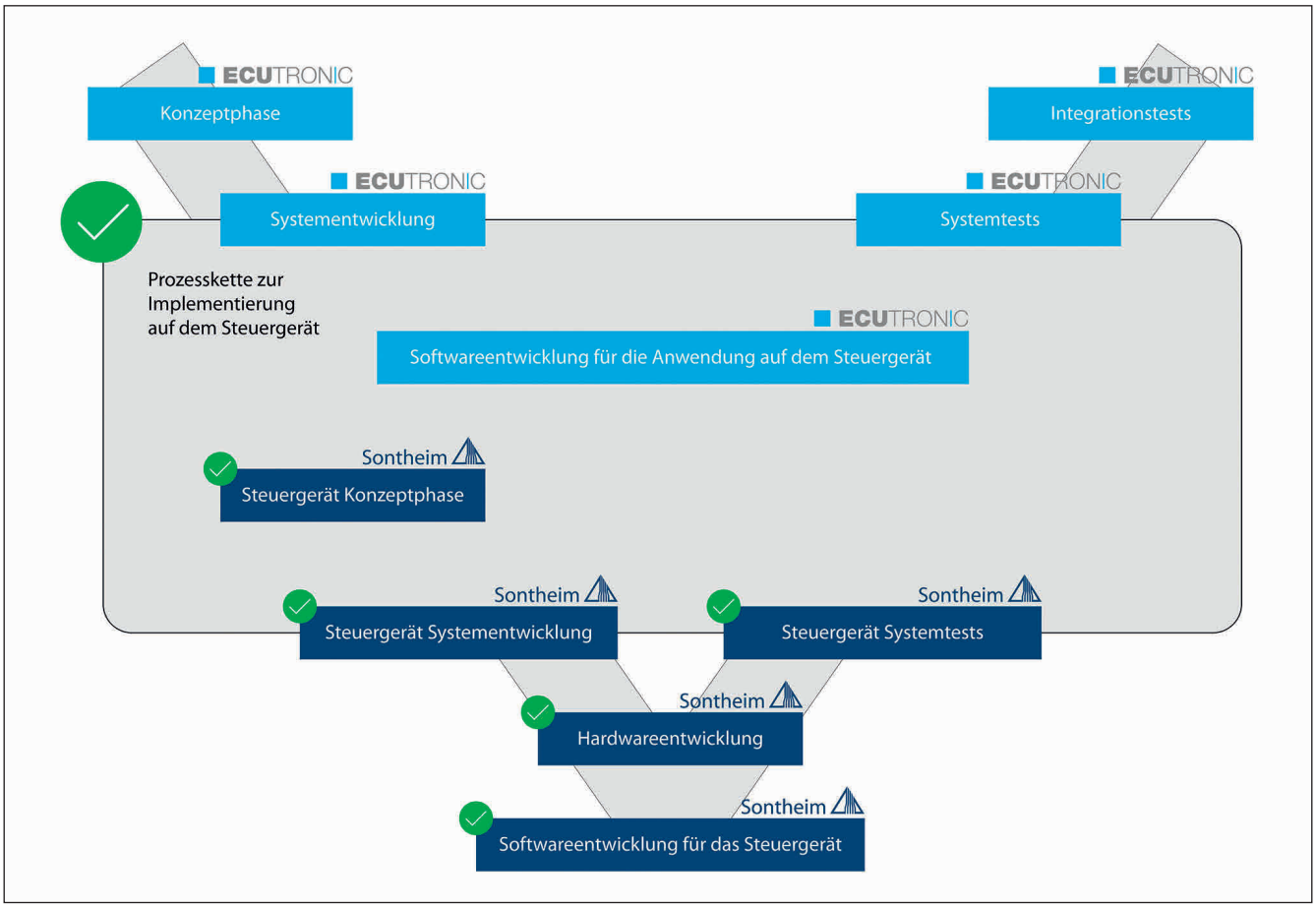
Durch die intensive Zusammenarbeit zwischen ECUtronic und Sontheim können Kunden von optimierten und synchronisierten Werkzeugketten profitieren. Dabei reduzieren etablierte Schnittstellen und Abstimmungsprozesse die Komplexität bei Entwicklungsprojekten. Dies ermöglicht eine gesteigerte Effizienz und Entwicklungsgeschwindigkeit für den Kunden.

Konzeptphase und Anforderungsmanagement:

Die Entwicklung neuer elektrischer/elektronischer Funktionen gemäß ISO 26262 und ISO 21434 starten mit der Konzeptphase. In diesem Prozessschritt legt ein Unternehmen die Grundlagen für die Entwicklung eines sicheren Produkts. Dabei müssen zunächst die sicherheitsrelevanten Anforderungen definiert werden. Dies umfasst die Identifikation potenzieller Gefahren und die Festlegung der Sicherheitsziele. In dieser Phase werden auch die Architektur und das Systemdesign entwickelt

In dieser Phase empfiehlt sich die Unterstützung durch Partner, die mit dieser Randbedingung vertraut sind und Fachwissen sowohl im Bereich der ISO 26262 als auch in den typischen klein- und mittel volumigen Anwendungsfällen im Bereich Truck, Bus, Trailer, Agrar- und Baumaschinen sowie Sonderfahrzeugen vorweisen können.

Als zentrale unterstützende Tätigkeiten stehen hier das formale Safety Management sowie die Einführung und



Durchgängige ISO26262-konforme Prozesskette – vom Konzept über eine generische Hardware bis zum Test © ECUtronic GmbH

Begleitung bei der Umsetzung eines Anforderungsmanagements für das zu entwickelnde Produkt im Fokus, wenn dies im Produktentwicklungsprozess des Unternehmens bisher keine Rolle gespielt haben sollte.

Oft ist das Ergebnis der Konzeptphase, dass elektronische Steuerungen zur Umsetzung von Funktionen benötigt werden. Im Bereich geringer bis mittlerer Stückzahlen sollten dafür möglichst generische, vorentwickelte Steuerungen zum Einsatz kommen, um den Zeit- und Kostenrahmen der Projekte einhalten zu können. Dies ist im Bereich mobiler und stationärer Maschinen Stand der Technik und weit verbreitet. Innerhalb des Normbereichs von ISO 26262 und ISO 21434 stellen derartige Steuerungen jedoch noch eine Seltenheit dar.

Zentrales Element – die sichere Steuerungshardware nach ISO 26262

Bei der Verfolgung des Ziels, eine sichere ECU zu entwickeln, die einen möglichst breiten Anwendungsbereich abdeckt, wurde besonderes Augenmerk auf eine möglichst große Anzahl verschiedener Schnittstellen gelegt, die auch im Sicherheitskontext belastbar sind.

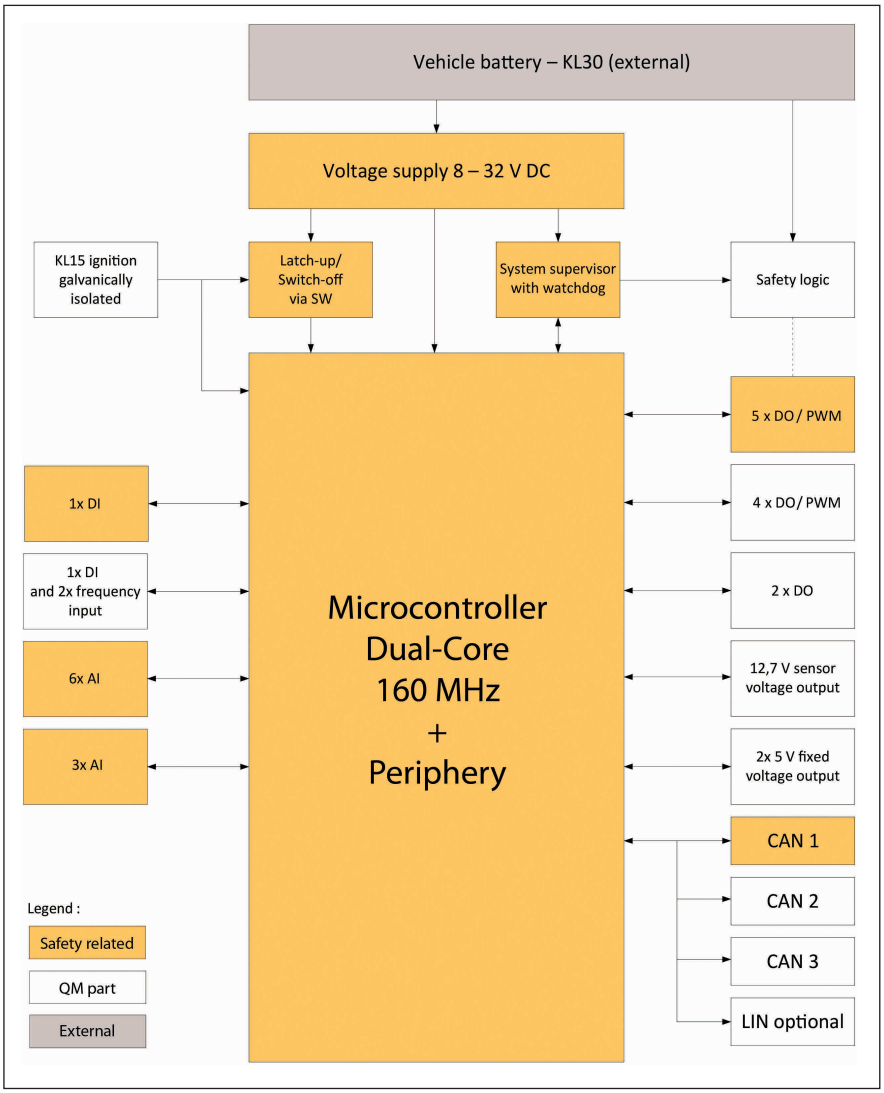
Besonders viel Wert wurde auch auf Schnittstellen zur Steuerung von Hydraulikventilen mit hoher Strombelastbarkeit gelegt, die bei sonstigen ISO 26262 Steuerungen nicht vorgesehen sind. Die Auslegung für sehr raue Einsatzbereiche betont den universellen Ansatz. Die Steuerung ist gemäß ISO 26262:2011 ASIL C zertifiziert.

Die Sicherheitsprinzipien für das Steuergerät bestehen in der Verwendung eines Sicherheits-Mikrocontrollers mit Überwachungsfunktion, einschließlich Watchdog (dem sogenannten Companion-Chip), die alle vorzertifiziert sind. Der Sicherheits-Mikrocontroller verfügt über eine eingebaute Selbstdiagnose, die ebenfalls von der Firmware aktiviert und zurückgelesen wird. Ein grundlegendes Sicherheitskonzept liegt darin, dass das Steuergerät im Falle eines Ausfalls selbst sicher stummgeschalten wird. In diesem Fehlerfall werden die ECU-Ausgänge deaktiviert und die Kommunikation zu den umliegenden Systemen unterbrochen. Darüber hinaus ist die ECU-Architektur für die sicheren IOs redundant und mit Diagnose ausgestattet. Die sicheren digitalen Ausgänge sind in Kombination mit einem High- und Low-Side-Schalter mit Strommessung und Diagnosefunktionen wie Überstrom-, Übertemperatur- und Open-Load-Erkennung aufgebaut. Redundante elektronische Ventile (High-Side- und Low-Side-Schalter) sorgen dafür, dass das Abschalten der Ausgänge auch im Falle eines Ausfalls eines der elektronischen Ventile möglich ist. Durch die redundante Ausführung ist sichergestellt, dass sicherheitskritische Zustände (z. B. ein Ausfall eines elektrischen Ventils oder ein Ausfall der Diagnose selbst) auch im Falle eines Diagnosefehlers erkannt werden können.

Die Analogeingänge werden als 2-Kanal-Eingänge für Diagnosezwecke genutzt.Der digitale Eingang ist redundant aufgebaut, mit einem digitalen Eingang und einem analogen Eingangskanal zur Diagnose.

Gemäß dem Anspruch, möglichst schnell kundenspezifische Projekte mit dem Steuergerät realisieren zu können, wurde besonderer Wert daraufgelegt, die unteren Softwareschichten weitgehend projektunabhängig zu gestalten und abzuschließen.

Das grundlegende Sicherheitskonzept der ECU besteht in einer Trennung in der Firmware zwischen einer sicheren Partition mit erweiterten recht strikten Kontrollmechanismen und einer QM-Partition mit weniger strikten Softwarevorgaben. Diese werden durch die Memory Protection Unit (MPU) getrennt und vom Echtzeitbetriebssystem unterstützt. Die sicheren Treiber der Ein- und Ausgänge sind bereits Bestandteil der Basissoftware. Es existieren Realisierungsvarianten gemäß Au-



Übersichtsblockdiagramm des Steuergerätes eSYS SCV3 XT © Sontheim Industrie Elektronik GmbH

tosar-Standard oder als sogenannter Complex Device Driver (CDD), falls die kundenspezifischen Anforderungen an die Ein- und Ausgänge über den Autosar Standard hinausgehen sollten. Für die externe Kommunikation gehört eine E2E-Bibliothek zum Lieferumfang der Steuerung.

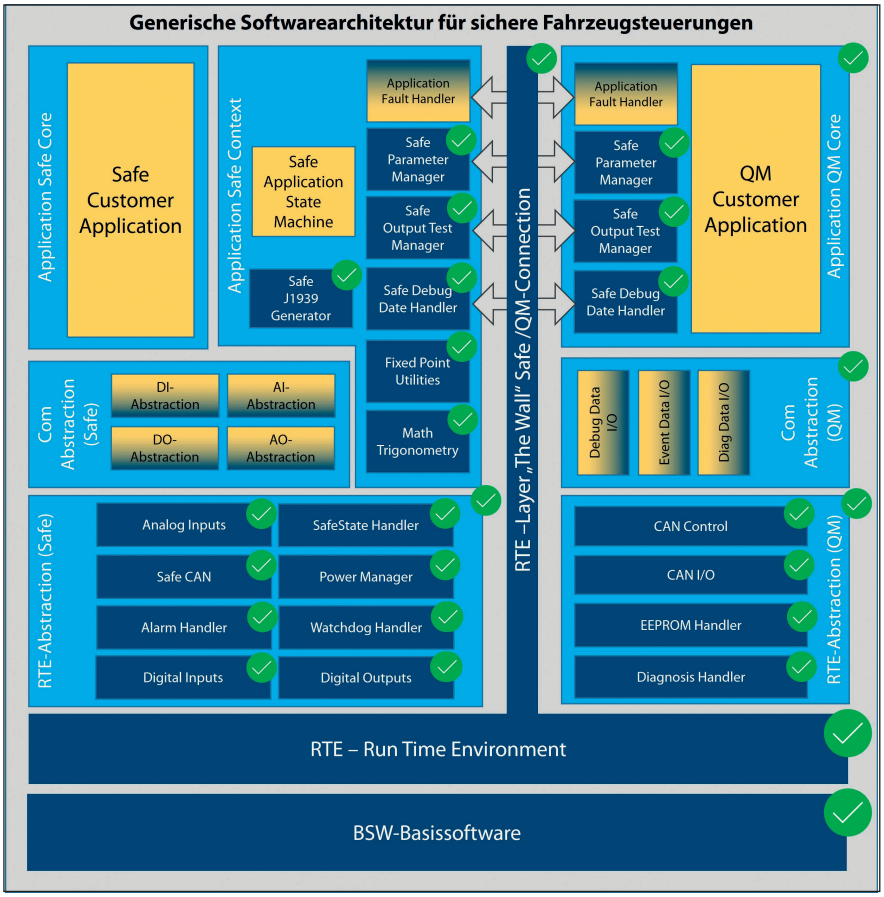
Entwicklung und Test der kundenspezifischen Applikationssoftware

Bei der Entwicklung der kundenspezifischen Applikationssoftware stellt die enge Vernetzung zwischen Steuerungshardware, deren Funktionalitäten und Eigenschaften, dem Betriebssystem sowie der vom Entwickler des Betriebssystems vorgesehenen Software- und Sicherheitsarchitektur eine besonders komplexe und potenziell aufwändige Herausforderung dar. Durch die etablierte Zusammenarbeit zwischen den Partnern Sontheim und ECUtronic wurden alle Schnittstellen und Verfahren für ein gemeinsames Leistungsangebot abgestimmt und die Vernetzung der Softwaremodule über Projekte hinweg etabliert. Im Ergebnis ist es möglich, sich bei der funktional sicheren Softwareentwicklung auf die konkrete kundenspezifische Applikation mit einigen Anpassungen bei den umgebenden Softwaremodulen zu konzentrieren.

Die konkrete Applikationsentwicklung erfolgt nach einem definierten Entwicklungsprozess. Dieser beginnt mit der Entwicklung der Softwarearchitektur für die Applikation unter Berücksichtigung der bereits vorhandenen Architekturmerkmale der Steuergerätelösung (blauer Bereich). Im nächsten Schritt werden die Modulspezifikationen aller an der Applikation beteiligten Komponenten erstellt. Diese Spezifikation verknüpft die Anforderungen aus der Funktionsbeschreibung mit den Bedingungen der Hard- und Softwarekomponenten.

Mit der Modulspezifikation können sowohl das eigentliche Programmieren und Implementieren der Software erfolgen als auch Testfälle abgeleitet werden, die die implementierten Module nach Abschluss bestehen müssen. Nach der Implementierung erfolgt die Integration, bei der die einzelnen Softwarekomponenten zusammengeführt und im Zusammenspiel getestet werden. Sowohl funktionale als auch nichtfunktionale Tests werden durchgeführt, um sicherzustellen, dass die Software den spezifizierten Anforderungen entspricht. Anschließend erfolgt die Verifikation, bei der die Korrektheit und Sicherheit der Software im Zusammenspiel mit der Steuerungshardware überprüft wird. Dafür kommen z.B. Hardware-in-the-Loop-Tests zur Anwendung. Schließlich erfolgt die Freigabe der Software in Kombination mit der Hardware, nachdem alle sicherheitsrelevanten Anforderungen erfüllt sind und die zu Beginn identifizierten Cyber- und funktionalen Risiken auf ein akzeptables Maß reduziert wurden.

Dank der generischen ECU, inklusive zugeschnittener Entwicklungsprozesse fällt es gerade OEMs in der Nutzfahrzeugbranche leicht, sich den neuen Themen rund um ISO 26262 und ISO 21434 anzunehmen und mit minimierten Aufwand und auch mit kleineren bis mittleren Stückzahlen ihre Applikationen erfolgreich abzubilden. ECUtronic und Sontheim sind hierbei die idealen Partner um sich jetzt diesen Herausforderungen zu stellen und sich im ECU-Bereich zukunftssicher aufzustellen. Dank des generischen Prinzips können verschiedenste Applikationen bedient werden, sei es in der Agrar-, Bau-, LKW-, Trailer- oder auch Busbrache. ■



Darstellung der generischen Softwarearchitektur: gelb: zu entwickelnde kundenspezifische Module; blau: existente vorentwickelte Module; gelb-blau: Module mit kundenspezifischem Anpassungsbedarf © ECUtronic GmbH und Sontheim Industrie Elektronik GmbH

Sontheim Industrie Elektronik GmbH
www.s-i-e.de
ECUtronic GmbH
www.ecutronic.de

Frank Steinert ist Geschäftsführer bei ECUtronic GmbH
© ECUtronic GmbH

Roland Mader ist Safety Manager bei Sontheim Industrie Elektronik GmbH
© Sontheim Industrie Elektronik GmbH

Daniel Magnus ist Marketing Manager bei Sontheim Industrie Elektronik GmbH
© Sontheim Industrie Elektronik GmbH