Einblicke in die Zertifizierung eines AUTOSAR-Betriebssystems

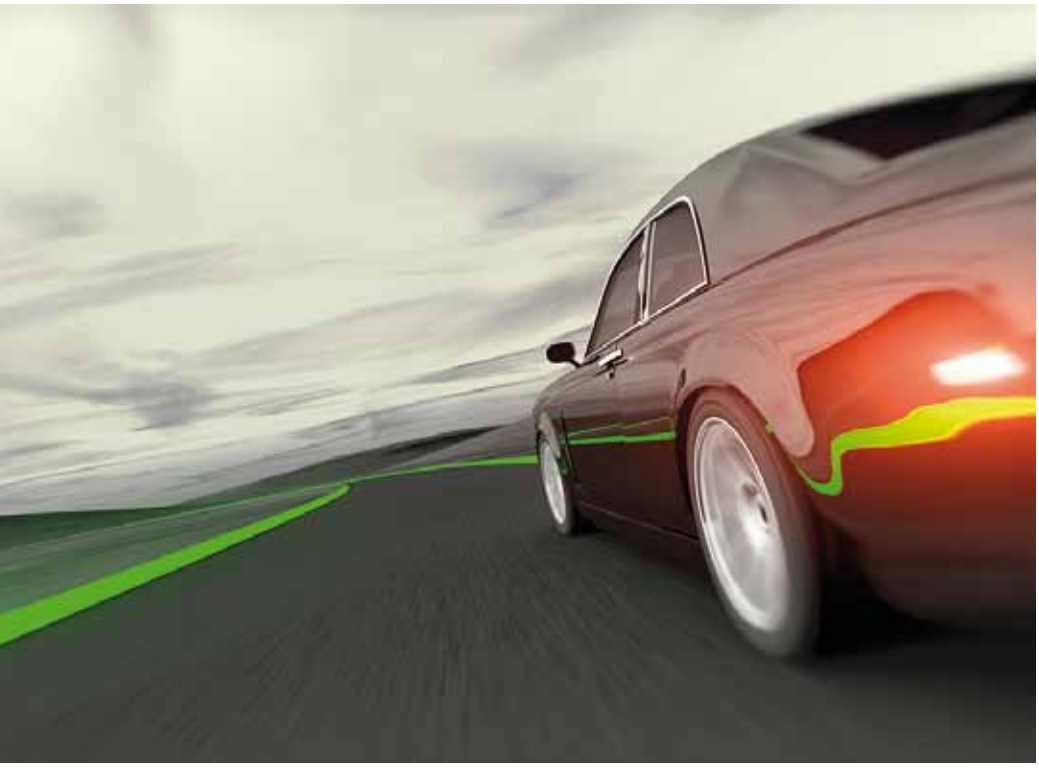
Das AUTOSAR-Betriebssystem EB tresos Safety OS von Elektrobit wurde von exida gemäß ASIL D und SIL 3 zertifiziert. Experten beider Unternehmen stehen Rede und Antwort zum Zertifizierungsprozess.

Als einer der ersten Automobil-Zulieferer bietet Elektrobit (EB) ein gemäß ASIL D zertifiziertes AUTOSAR-Betriebssystem an. Dabei handelt es sich zudem um das einzige auf dem Markt, das gleichzeitig für das Safety Integrity Level 3 (SIL 3) für Anwendungen außerhalb des Automobilbereichs zertifiziert ist. ASIL D und SIL 3 gehören zu den höchsten Sicherheitsstandards für funktionale Sicherheit gemäß den Normen ISO 26262 und IEC 61508 für elektrische und elektronische Komponenten. Die Zertifizierung für funktionale Sicherheit führte die unabhängige Prüfstelle exida Certification SA durch. Damit ist bestätigt, dass das EB tresos Safety-Betriebssystem für den Einsatz in Anwendungen des Automotive Safety Integrity Levels D (ASIL D) geeignet ist, zum Beispiel für elektrische Servolenkungen. Rainer Faller, Principal Partner bei exida, und Robert Leibinger, Produktmanager Software & Tools bei EB geben Einblicke in den Zertifizierungsprozess.

ELEKTRONIKPRAXIS: Warum sollten Zulieferer ihre Produkte zertifizieren lassen?

Rainer Faller: Funktionale Sicherheit ist ein zentrales, anspruchsvolles Thema und dementsprechend komplex sind die Produkte. Daher schreiben alle Sicherheitsstandards für höhere Sicherheitsniveaus vor, dass die Entwicklung der Produkte und die dabei angewandten und dokumentierten Sicherheitsmaßnahmen einer unabhängigen Beurteilung (Assessment) unterzogen werden muss. Exida Assessments decken darüber hinaus die technischen Sicherheitseigenschaften des Produktes ab. Zertifikate sind dabei eine freiwillige Bestätigung der erfolgreichen Assessments.

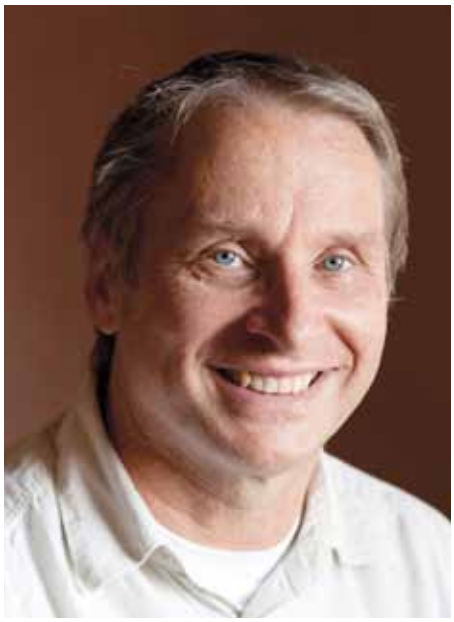
Die Basisnormen zur funktionalen Sicherheit, wie ISO 26262, sind bewusst sehr allgemein verfasst und bedürfen der Interpretation für die jeweiligen Produktkategorien. Die Umsetzung der Anforderungen wird durch eine Vielzahl von Dokumenten belegt. Assessments bedürfen neben dem großen Zeitaufwand auch eines hohen Kenntnisstands über die Produkte und Normen. Sie liefern dem Anwender des Produkts einen unabhängigen Beleg über die erreichte Sicherheit. Deshalb ist es sinnvoll, die funktionale Sicherheit einmal beurteilen zu lassen, statt dies von jedem Anwender neu durchführen zu lassen. Die Anwendbarkeit der Assessment-Ergebnisse muss vom Anwender natürlich für jeden Anwendungsfall beurteilt werden.



Funktionale Sicherheit: *Gemäß ASIL D der Norm ISO 26262 zertifizierte Komponenten eignen sich für den Einsatz in sicherheitsrelevanten Anwendungen wie elektrische Servolenkungen*

Was sollten Unternehmen wie Elektrobit bei einem Safety-Zertifikat beachten? Gibt es Unterschiede und woran erkennt man diese?

Rainer Faller: Der genaue Umfang des Assessment und die Betrachtungstiefe sind wichtige Informationen für den Anwender. ISO 26262 beispielsweise erlaubt auch Assessments von Teilen der Entwicklung: Ein Assessment der Entwicklungsprozesse und Maßnahmen gegen die zutreffenden Normenanforderungen ist möglich, ohne die technischen Sicherheitseigenschaften des konkreten Produktes zu beurteilen. Auch sind Assessment-Aussagen immer mit bestimmten Annahmen verbunden, die der Anwender natürlich kennen muss. Assessment-Berichte enthalten diese wichtigen Informationen, die allein aus dem



Rainer Faller: *„Unsere Assessments beurteilen sowohl die Entwicklungsabläufe als auch die technischen Sicherheitseigenschaften des Produktes."*

Zertifikat nicht ersichtlich sind. Zertifikate ohne aussagekräftige Berichte sind daher nicht normenkonform und für die Anwender nicht belastbar.

EB entwickelt Software für Infotainment und ECU. Warum wurde gerade das Safety-Betriebssystem als erstes Produkt zertifiziert?

Robert Leibinger: Im Vergleich zu den meisten Infotainment-Geräten müssen Funktionen wie Bremsen oder Airbags deutlich höhere Sicherheitsstandards erfüllen, um eine Gefährdung für den Straßenverkehr auszuschließen. Daher müssen die entsprechenden Steuergeräte, die Aufgaben bis zum höchsten „Automotive Safety Integrity Level" (ASIL) D erfüllen, nachweislich sicher sein. Das Betriebssystem ist innerhalb einer Sicherheitsarchitektur die zentrale Komponente und die Basis für alle anderen in der Software implementierten Sicherheitsmechanismen. Deshalb muss auch bei einer Zertifizierung hier als allererstes angesetzt werden.
Die Einflussmöglichkeiten, die die Basiskomponente Betriebssystem auf das gesamte Steuergerät nehmen kann, ist nicht zu unterschätzen. Aufgabe des Betriebssystems ist ja nicht nur, die Speicherpartitionierung vorzunehmen, sondern den kompletten Programmablauf inklusive der Sicherheitsmechanismen zu steuern. Aus diesem Grund haben wir bei EB schon vor über zwei Jahren entschieden, einen neuen, rein auf Sicherheit optimierten Kernel zu entwickeln. Es wurden keine Ergänzungen in ein bestehendes System eingebaut, sondern es von Grund auf neu konzipiert. Von den Requirements über Design und Implementierung bis zu den Tests wurde alles auf funktionale Sicherheit ausgerichtet. Das Ziel war von Beginn an, ein verlässliches Safety-Betriebssystem zu entwickeln, das sich nahtlos in AUTOSAR integrieren lässt.

Die Zertifizierung eines Produktes kann sich sehr unterschiedlich gestalten. Wie geht exida an eine solche Aufgabe heran?

Rainer Faller: Unsere Assessments beurteilen sowohl die Entwicklungsabläufe als auch die technischen Sicherheitseigenschaften des Produktes. Das Assessment erfolgt in mehreren Schritten. Nach einer genauen Abstimmung des Umfangs des Assessments erfolgt eine Beurteilung der Umsetzung der Sicherheitsanforderungen anhand der Dokumentation - unbeeinflusst von den Managern, Entwicklern und Testern des Produktes. Aufkommende Fragen werden in Meetings geklärt, und die praktische Umsetzung der vom Hersteller definierten Prozesse und Prozeduren werden in einem Audit beim Hersteller hinterfragt.
Das Assessment berücksichtigt alle zutreffenden ISO 26262-Zielsetzungen („Objectives") und Arbeitsergebnisse. Startpunkt der Beurteilung ist der vom Hersteller vorgelegte Safety Case und die darin referenzierten Entwicklungsdokumente. Da die Zielsetzungen sehr allgemein gehalten sind, wählt der Assessor weitere wichtige Normenanforderungen aus. Bei exida wird dies durch ein Safety-Case-Datenbank-Tool unterstützt, das auch abgestimmte Interpretationen enthält. Bei der Auswahl von Anforderungen aus der technischen Anforderungsspezifikation des Produktes wird insbesondere auf die für den Anwender wichtigen Sicherheitsfeatures und Fehleraufdeckungsmaßnahmen und Fehlerreaktionen geachtet. Diese sind im Assessment-Bericht beschrieben.

Wie lief die Zusammenarbeit zwischen exida und EB ab?

Robert Leibinger: Die Zusammenarbeit war äußerst konstruktiv. Zunächst wurde ein gemeinsames „Vor-Assessment" durchgeführt. Hier haben wir die Strategie für die Safety OS-Entwicklung in Hinblick auf funktionale Sicherheit sowie die Pläne und Requirements genauer betrachtet. Somit konnten wir die Anforderungen, die das Assessment an uns stellt, bereits sehr früh

in unseren Entwicklungsprozess mit einbinden.

Im nächsten Schritt legten wir den technischen Umfang der Zertifizierung fest, also welche Funktionalitäten des Betriebssystems sicherheitsrelevant sind und somit auch bewertet werden müssen. Für ein sogenanntes „Safety Element out of Context" bieten diese Funktionalitäten dann die Grundlage, auf die unsere Kunden ihre Safety-Argumentation aufbauen können. Exida konnte mit diesen Daten dann einen Assessment-Plan aufstellen, in dem Art und Umfang des Zertifizierungsprozesses definiert wurden.

Dann erst begann das eigentliche Assessment, in dessen Rahmen in regelmäßigen gemeinsamen Meetings intensiv diskutiert wurde. Auf hohem technischem Niveau wurden alle relevanten Themengebiete wie die Umsetzung der Requirements, des Designs und der Tests bis hinein in den Quellcode betrachtet. Es fand also neben der Prozessevaluation auch eine Betrachtung der Architektur und der Umsetzung der Sicherheitsaspekte des Betriebssystems statt.

Bei den Assessment Meetings waren neben unserem Assessor Herrn Faller alle an der Entwicklung des Betriebssystems beteiligten Entwicklungs-, Test- und Qualitätsingenieure sowie der Safety Manager von EB involviert. Eine große Herausforderung war dabei, aus der Fülle an Material die benötigten Informationen in der geeigneten Form aufzubereiten, um die Argumentation zu unterstützen. Die von Beginn an auf funktionale Sicherheit ausgerichtete Entwicklung des Betriebssystems war dabei äußerst hilfreich.

In einem iterativen Prozess ist dann schließlich der Assessment-Bericht entstanden, der Ende 2012 fertig war.

Betriebssysteme wie Safety OS sind die Basis für Steuergeräte, die höchste Sicherheitsstandards erfüllen müssen. Wie kann die Zertifizierung des Betriebssystems bei der Zertifizierung der Steuergeräte helfen?

Robert Leibinger: Auf Basis des Betriebssystems werden Sicherheitsmechanismen implementiert, die den höchsten Sicherheitsstandards genügen müssen. Diese Mechanismen müssen sich auf gewisse grundlegende Funktionalitäten verlassen können. Das exida-Zertifikat garantiert dem Steuergeräte-Hersteller, dass diese Funktionen entsprechend des höchsten Standards geprüft wurden. Kommt es also beim Steuergeräte-Hersteller selbst zum Safety-Assessment, kann er beim Nachweis der Sicherheitseigenschaften des Betriebssystems nach der ISO 26262 auf das Zertifikat verweisen. Er hat also keinen weiteren Aufwand, um die Grundfunktionalität des Betriebssystems abzusichern und kann diese Nachweise aus dem Gesamt-Steuergeräte-Test ausklammern. In gewisser Weise teilen wir uns die Arbeit mit unseren Kunden, indem wir den Nachweis für die Grundfunktionalität des Systems übernehmen.

Robert Leibinger: *„Im Vergleich zu den meisten Infotainment-Geräten müssen Funktionen wie Bremsen oder Airbags deutlich höhere Sicherheitsstandards erfüllen, um eine Gefährdung für den Straßenverkehr auszuschließen."*

Rainer Faller: Die größte Hilfestellung geben die zugesicherten Sicherheitsfeatures des Safety OS. Besonders wichtig für eine zielgerichtete Entwicklung sicherheitsrelevanter Software ist der Schutz der Ausführung von nebenläufigen Software-Teilen und des logischen Partitioning sowie der gesicherte Ablauf der µC-Konfiguration beim Startup. Dies wird vom Safety OS durch das Zusammenwirken mit Hardware-Funktionen wie Memory und Hardware Resource Protection (Freedom from Interference) erreicht. Das Safety OS ist damit das Fundament für die Umsetzung der logischen Architektur, die durch die funktionalen und technischen Sicherheitskonzepte nach ISO 26262 spezifiziert ist. Dies umfasst sowohl die Anwendungssoftware als auch die AUTOSAR-konforme Basissoftware.

Welchen Mehrwert haben Kunden durch das zertifizierte Betriebssystem?

Robert Leibinger: Unsere Kunden können ihr Augenmerk ganz auf ihre Kernkompetenzen legen. Die grundlegenden Funktionen für ihre Software stellen wir nach ASIL-D abgesichert in unserem Betriebssystem zur Verfügung. So bieten wir neben einem sicheren Kontext-Wechsel auch sicherheitsrelevante Funktionen wie Task-Scheduling, Event-Handling oder Locking-Mechanismen. AUTOSAR-Systeme setzen über die RTE oft für den Anwender unbemerkt auf diese Mechanismen auf. Des Weiteren erlaubt dies den Einsatz dieser Funktionen direkt im Safety-Mechanismus, um Teile der Software über Events zu entkoppeln oder vor gegenseitigem Zugriff auf gemeinsame Ressourcen zu schützen. Unser Ziel war dabei, alle grundlegenden Funktionen mit dem Zertifikat abzudecken. Dies ermöglicht eine verlässliche Entwicklung von Steuergeräten bis zum höchsten Sicherheitslevel.

Bei der Auswahl der sicherheitsrelevanten Funktionen haben wir uns ganz bewusst dafür entschieden, nur den grundlegenden Funktionssatz in die Zertifizierung mit aufzunehmen. Die Komplexität der Software sollte so gering wie möglich sein, um die Safety-Analyse so einfach wie möglich zu gestalten. Gleichwohl ist es uns gelungen, auch die nicht-zertifizierten Elemente durch eine geschickte Architektur ohne Einflussmöglichkeit auf die restlichen Funktionen zu gestalten. Somit bietet das Safety OS verlässliche Sicherheitsfunktionen und ist gleichzeitig AUTOSAR-kompatibel.

Was ist bei EB im Bereich Functional Safety noch geplant?

Robert Leibinger: Neben dem reinen Betriebssystem-Kern werden noch weitere Komponenten in der Entwicklung sicherheitskritischer Software benötigt, so zum Beispiel eine Programm-Ablaufkontrolle oder eine abgesicherte Kommunikation. Deshalb konzentrieren wir bei EB uns darauf, auch unsere weiteren Produkte aus der EB tresos Safety-Produktfamilie zertifizieren zu lassen, um ein unabhängig bestätigtes, vollständiges Safety-Paket anbieten zu können. So werden demnächst auch unsere Lösungen zum sicheren Management der Laufzeitumgebung (EB tresos Safety RTE), der geschützten Zeit- und Ausführungskontrolle (EB tresos TimE Protection) sowie der geschützten Übertragung von sicherheitsrelevanten Daten zwischen mehreren Steuergeräten (EB tresos Safety E2E Protection) von exida zertifiziert sein. // **TK**

Elektrobit
+49(0)9131 77010