AUF EINEN BLICK

Wir machen Städte schlau

Fraunhofer FOKUS

FRAUNHOFER-INSTITUT FÜR
OFFENE KOMMUNIKATIONSSYSTEME FOKUS

KOMPETENZEN

– Entwurf von Systemarchitekturen
– System on Chip (SoC)
– Field Programmable Gate Array (FPGA)
– Parallele Architekturen (Multicore)
– Betriebssysteme ARINC 653, AUTOSAR
– Bewertung von Testkonzepten und Architekturen
– Modellbasiertes Testen und Testautomatisierung
– Formale Methoden
– Normen (z. B. DO178B, ISO 11073, EN 62061, ISO 26262)

DIENSTLEISTUNGEN

– Technologieberatung und -evaluation
– Signal Integrity Simulation
– Verbesserung von Test- und Validierungsprozessen
– Beratung bei Qualitätssicherung und Zertifizierung
– Realisierung von Hard- und Software-Prototypen

BRANCHEN

Luft- und Raumfahrt, Medizintechnik, Bahntechnik, Anlagenbau und Automatisierungstechnik, Automotive

KONTAKT

Friedrich Schön
Abteilungsleiter
System Quality Center – SQC
Tel. +49 (0)30 3463-7453
friedrich.schoen@fokus.fraunhofer.de

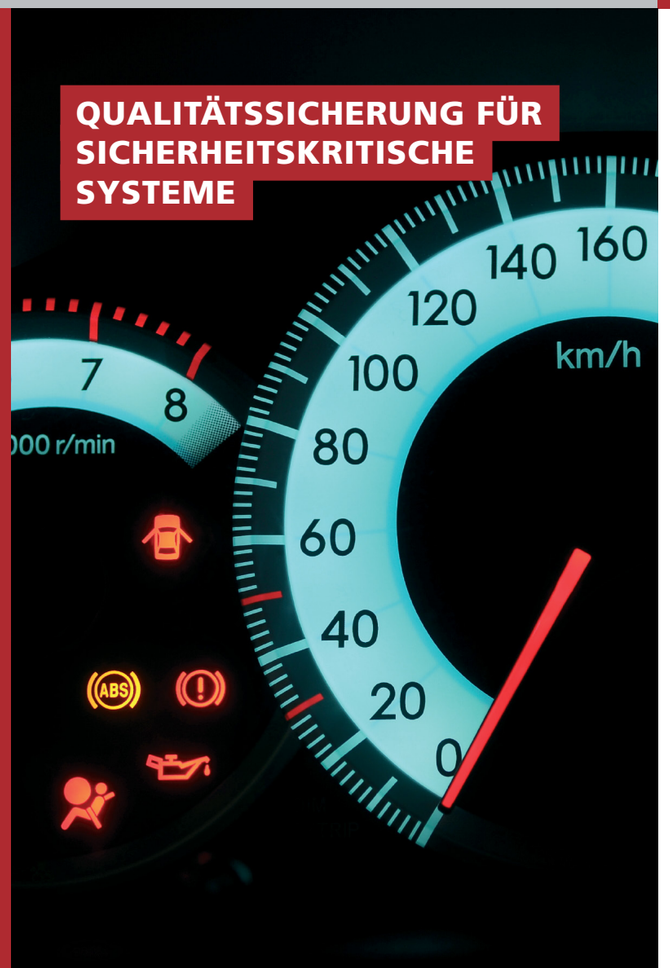
Prof. Dr. Holger Schlingloff
Stellvertretender Abteilungsleiter
System Quality Center – SQC
Tel. +49 (0)30 3463-7504
holger.schlingloff@fokus.fraunhofer.de

Fraunhofer FOKUS
Kaiserin-Augusta-Allee 31
10589 Berlin

www.fokus.fraunhofer.de/go/sqc

bad | 1402 (Fotos: iStockphoto, Fraunhofer FOKUS)

QUALITÄTSSICHERUNG FÜR SICHERHEITSKRITISCHE SYSTEME

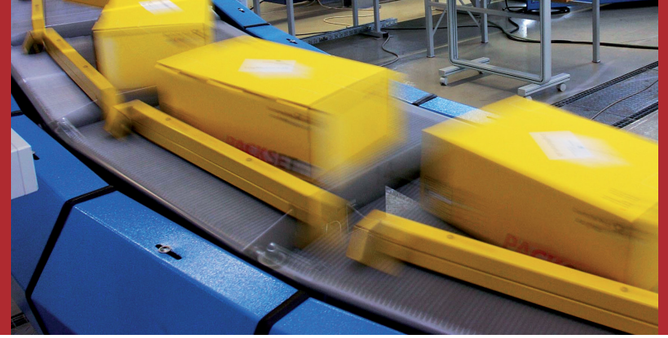


HERAUSFORDERUNG

In Satelliten, Flugzeugen, Fahrzeugen, der Medizintechnik oder in Produktionsanlagen – in zahlreichen industriellen Anwendungen übernehmen eingebettete Systeme immer mehr zentrale Steuerfunktionen. Insbesondere in sicherheitskritischen Bereichen mit hohem Gefährdungspotenzial für Mensch oder Umwelt wird von diesen high integrity systems ein Höchstmaß an Zuverlässigkeit verlangt. Die Technologien müssen dafür steigenden Sicherheitsstandards und Zertifizierungsanforderungen gerecht werden.

Fraunhofer FOKUS berät seine Kunden bei der Entwicklung und Qualitätssicherung von Hard- und Softwarekomponenten sicherheitskritischer Systeme. Das Ziel ist die optimale Umsetzung komplexer Systemarchitekturen und Entwicklungsprozesse nach individuellen Kundenanforderungen.

VON DER IDEE BIS ZUM
FERTIGEN PRODUKT



KOMPETENZEN

Fraunhofer FOKUS verfügt durch zahlreiche Projekte mit der Industrie und öffentlichen Auftraggebern über ausgewiesene Expertise bei der Entwicklung und Qualitätssicherung sicherheitskritischer Systeme. Unsere Beratung verbindet unser Know-how zu Hardware-Architekturen und Software-Methoden mit umfangreichen Kenntnissen im Bereich von Qualitätssicherungsprozessen. Auf diese Weise können wir unseren Kunden ein umfassendes Beratungsangebot anbieten: Wir erstellen Konzepte und Architekturen und setzen diese in Soft- und Hardware um. Dafür nutzen wir unsere langjährigen Erfahrungen beim Einsatz von Technologien wie System on Chip (SoC), Field Programmable Gate Array (FPGA) und Signal Integrity Simulation. Dadurch sind unsere Kunden in der Lage, aus innovativen Produktideen innerhalb kurzer Zeit praxistaugliche Konzepte zu erstellen und sie zu realisieren. Wir beraten zudem bei der Risikoanalyse und bieten dafür Methoden und Werkzeuge an. Im Einzelnen nutzen wir Codeanalyse und -inspektion, Test und Verifikation, Modellierung und Modellprüfung sowie Refactoring von Quelltexten. Außerdem überprüfen wir für unsere Kunden Softwaresysteme in Hinblick auf die Übereinstimmung mit gängigen Normen und Standards und stehen ihnen bei der Vorbereitung auf internationale Zertifizierungen zur Seite.

BRANCHEN

Luft- und Raumfahrt
Die besondere Herausforderung in der Luft- und Raumfahrt ist es, trotz hoher Sicherheitsanforderungen und geringer Stückzahlen kostengünstig zu entwickeln. In beiden Bereichen unterstützen wir unsere Kunden bereits bei den ersten Entwürfen neuer Steuergeräte und begleiten die vollständige Entwicklung. So hat FOKUS z. B. für den Technologie-Erprobungs-Träger TET-1 den Satellitenbuscomputer (SBC), einschließlich der Betriebssoftware entwickelt. Im Rahmen der nationalen Innovationsallianz Software-Plattform Embedded Systems (SPES 2020) wurden Lösungen für die branchenübergreifende und modellbasierte Entwicklung von eingebetteter Software erarbeitet. FOKUS hat z. B. ein Werkzeug zur sicheren Zeitpartitionierung von Betriebssystemen nach ARINC 653 entwickelt. Damit kann die Entwicklung und Qualifizierung komplexer Multiprozessor-Systeme nach DO178B erheblich vereinfacht werden.

Bahntechnik
Die in der Bahntechnik geltenden Sicherheitsstandards führen bei neuen Entwicklungen, z. B. Signalanlagen, meist zu langwierigen Entwurfsphasen. Unsere Beratung setzt in diesen frühen Phasen an und begleitet unsere Kunden von der Arbeit an den Hard- und Software-Architekturen bis hin zur industriellen Anwendung. Dabei wird die Konformität zum Zertifizierungsprozess gemäß EN 50128 berücksichtigt. Um die Verlässlichkeit eingebetteter Software zu überprüfen, haben sich traditionelle Testmethoden als teuer erwiesen. Es ist sehr aufwändig, die notwendige hohe Testabdeckung zu erzielen. Hinzu kommt, dass in Zukunft die Größe und Komplexität eingebetteter Software noch zunehmen wird. Eine Alternative stellen mathematische Methoden dar, die die erwünschten Sicherheitsbestandteile in der Software formal überprüfen. Im Rahmen des Projekts DEVICE-SOFT arbeiteten die Forscher bei FOKUS daran, deduktive Verifikationsmethoden für industrielle Bahnanwendungen nutzbar zu machen.

Automatisierungstechnik
In der Automatisierungstechnik müssen intelligente Steuerungssysteme dafür sorgen, dass viele Steuerungen koordiniert zusammenarbeiten. Zudem sind die Steuergeräte selbst modular aufgebaut, um auch kleine Stückzahlen realisieren zu können. Solche modular komponierbaren Geräte lassen sich mit überschaubarem Aufwand realisieren und bieten auch kleinen und mittleren Unternehmen die Chance auf einen Markteinstieg. Allerdings werden die Qualitäts-, Zuverlässigkeits- und Sicherheitsanforderungen, die in Normen wie IEC 61508, EN 13849 oder EN 62061 geregelt sind, immer mehr verfeinert. Dadurch steigen die Kosten für den Nachweis und die Zulassung, was gerade für KMUs eine ernstzunehmende Herausforderung darstellt. Daher wurden im VaKoMo-Projekt effiziente Methoden zur Validierung und Zertifizierung modularer Architekturen entwickelt.

Medizintechnik
Gerade in der Medizintechnik muss die einwandfreie Funktion von Systemen sichergestellt werden. Hersteller müssen daher bei der Zertifizierung ihrer Systeme hohe Sicherheitsstandards und Normen, wie IEC 60601, EN 62304 oder ISO 11073, erfüllen. Wir unterstützen unsere Kunden bereits in frühen Entwicklungsphasen, indem wir durch automatische Testfallgenerierung die Einhaltung von Normen überprüfen. Im Rahmen des vom Bundesministerium für Bildung und Forschung (BMBF) geförderten Projekts Smart Senior entstand bei FOKUS ein Testbed zur Validierung von Funktionen intelligenter Assistenz- und telemedizinischer Notfalldienste.

Automotive
Die Entwicklung komplexer Steuergeräte wird im Automobilbereich zunehmend von der Referenzarchitektur AUTOSAR und der ISO Norm 26262 beeinflusst. Sie definiert ein Vorgehensmodell sowie die anzuwendenden Methoden. Im Projekt VirtuOS erforschte und entwickelte FOKUS mit Partnern aus der Automobilindustrie notwendige Prozesse, Methoden und Tools für AUTOSAR basierte Embedded Software, um zukünftigen Safety und Security Anforderungen bei der Zertifizierung gerecht zu werden. FOKUS untersuchte mit den beteiligten Partnern wie die dazu benötigten sicherheitskritischen Funktionen auf einer gemeinsamen Plattform integriert werden können.