AT A GLANCE

COMPETENCIES

- Design of system architectures
- System on Chip (SoC)
- Field Programmable Gate Array (FPGA)
- Parallel architectures (Multi-Core)
- Operating systems ARINC 653, AUTOSAR
- Evaluation, Review, Testing of test concepts and architectures
- Model-based testing and test automation
- Formal methods
- Norms (e.g. DO178B, ISO 11073, EN 62061, ISO 26262)

SERVICES

- Technology consulting and evaluation
- Signal Integrity Simulation
- Improvement of testing and validation processes
- Consulting on quality control and certification
- Implementation of hardware and software prototypes

INDUSTRIES

Aerospace, Medical technology, Railroad technology, Engineering and Automation technology, Automotive

making
cities smart

CONTACT

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

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

Fraunhofer FOKUS
Kaiserin-Augusta-Allee 31
10589 Berlin
Germany

www.fokus.fraunhofer.de/en/sqc

bad | 1402 (Photos: iStockphoto, Fraunhofer FOKUS)

Fraunhofer
FOKUS

FRAUNHOFER INSTITUTE FOR
OPEN COMMUNICATION SYSTEMS FOKUS

QUALITY CONTROL FOR SAFETY-CRITICAL SYSTEMS

CHALLENGE

Whether in satellites, airplanes, vehicles, medical technology or production facilities – embedded systems take on key control functions in an increasing number of various industrial applications. Particularly safety-critical areas with high risk potentials for man or environment require a maximum degree of reliability from these high integrity systems. The technologies will have to satisfy increasing safety standards and certification requirements.

Fraunhofer FOKUS counsels clients on the development and quality control of hardware and software components of safety-critical systems. Our aim is the optimal implementation of complex system architectures and development processes according to the individual needs of our clients.

FROM THE IDEA TO

THE FINISHED PRODUCT

COMPETENCIES

Fraunhofer FOKUS is an established expert for the development and quality control of safety-critical systems and has been active in numerous projects in industry and with public clients.
Our consulting combines know-how of hardware architectures and software methods with extensive knowledge of quality control processes.

In this way we can offer our clients comprehensive consulting services: we develop concepts and architectures and implement them in software and hardware, utilizing our long-standing expertise in the application of technologies such as System on Chip (SoC), Field Programmable Gate Array (FPGA), and Signal Integrity Simulation. This enables our clients to generate and realize practicable concepts from innovative product ideas in short periods of time. We also offer consulting and provide methods and tools for risk analysis. Specifically, we use code analysis and inspection, testing and verification, modeling and model checking, as well as refactoring of source code. Additionally, we test software systems regarding compliance with established norms and standards for our clients and assist them in the preparation for international certifications.

INDUSTRIES

Aerospace
A particular challenge in the aerospace industry is cost-efficient development despite high safety requirements and low quantities. We already support clients in both fields with FOKUS drafts of new control units and assist during complete development. FOKUS has for instance developed the satellite bus computer (SBC) and its operating software for the satellite project TET-1. Within the scope of the national innovation alliance 'Software Platform Embedded Systems' (SPES 2010), solutions for cross-industry and model-based development of embedded software were working out. FOKUS has devised a tool for safe time partitioning of operating systems according to ARINC 653. This offers the opportunity to significantly ease the development and qualification of complex multi-processor systems according to DO178B.

Railroad Technology
Safety standards in railroad technology usually lead to lengthy design phases for new developments, for instance of signaling installations. Our consulting begins in these early phases and accompanies the client from working on hardware and software architectures all the way to the industrial application, while observing conformity with the certification process according to EN 50128. Traditional test methods have proven to be costly in order to validate the reliability of embedded software. It is very expensive to attain the necessary high test coverage. Additionally, the size and complexity of embedded software will increase in the future. Mathematic methods that formally check the desired safety components offer an alternative. In the context of the project DEVICE-SOFT, researchers at FOKUS were working on making deductive verification methods usable for industrial railroad applications.

Automation Technology
In automation technology, intelligent control systems not only have to ensure that various controls work together. Additionally, the control units themselves are built in modular fashion in order to realize small quantities, as well. Small units that are composed of modules can be realized with reasonable effort and offer a chance for market entry for small and medium-sized companies, too. However, quality, reliability, and safety requirements regulated by norms such as IEC 61508, EN 13849, or EN 62061 are being refined evermore. This leads to a steady increase in cost for proving and licensing, which represents a serious challenge for small and medium-sized companies. Within the scope of the VaKoMo project, efficient methods for the validation and certification of modular architectures are developed.

Medical Technology
The error-free operation of systems has to be ensured in medical technology particularly. Manufacturers thus have to meet high safety standards and norms, such as IEC 60601, EN 62304, or ISO 11073 for the certification of their systems. We already support our clients in the early development phases by ensuring the compliance with norms through automatic test case generation. Within the scope of the 'Smart Senior' project sponsored by the Federal Ministry of Education and Research (BMBF), FOKUS were creating a testbed for the validation of functions regarding intelligent assistance and telemedical emergency services.

Automotive
The development of complex control units in the automotive industry is increasingly being affected by the reference architecture AUTOSAR and ISO norm 26262. It defines a process model as well as the applicable methods. In the VirtuOS project, FOKUS and partners from the automotive industry were researching and developing necessary processes, methods, and tools for AUTOSAR-based embedded software in order to meet future safety and security requirements during certification. FOKUS and the involved partners were analyzing how the required safety-critical functions can be integrated on a common platform.