Fraunhofer IESE

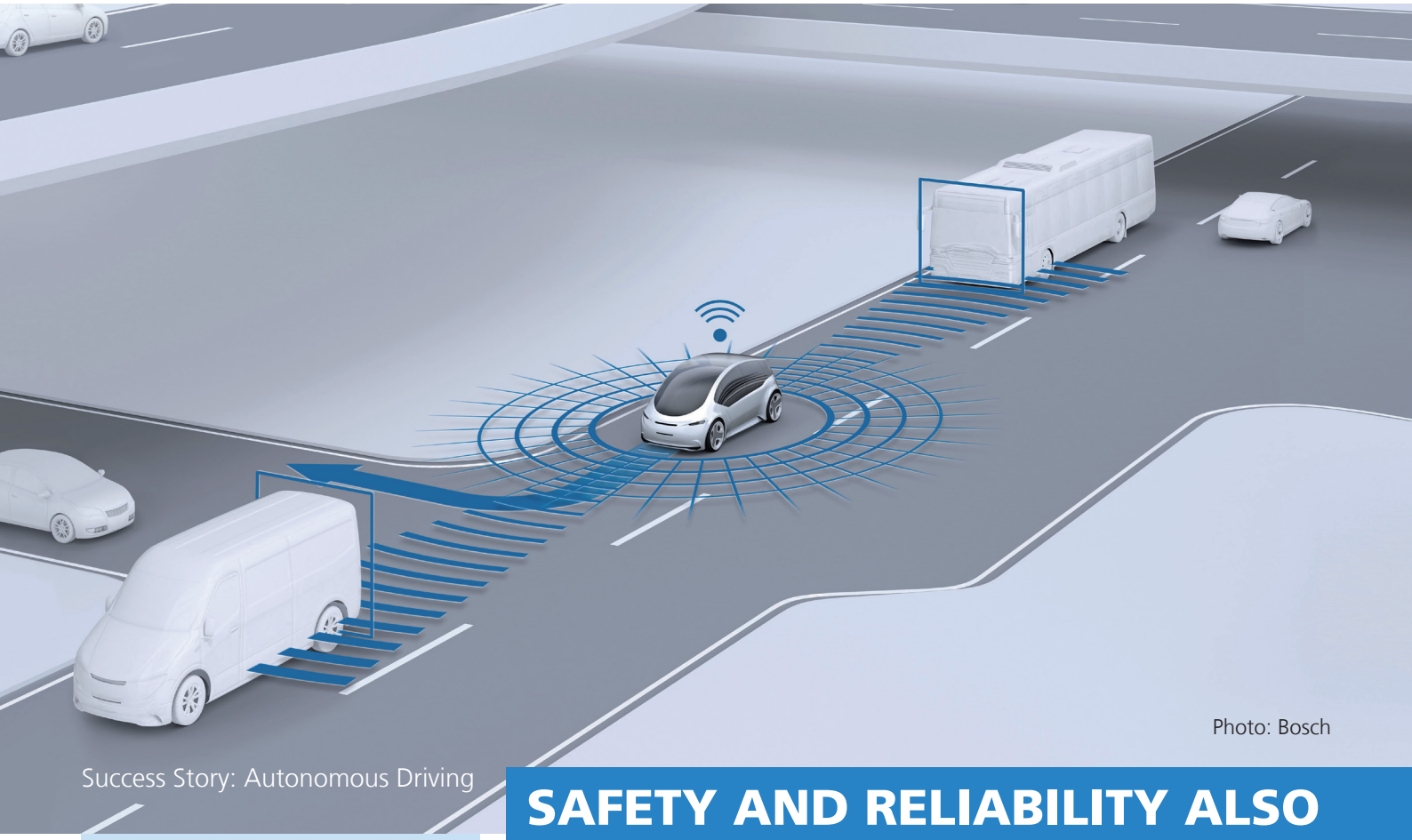

Photo: Bosch

Success Story: Autonomous Driving

SAFETY AND RELIABILITY ALSO FOR NON-AUTOMOTIVE HARDWARE

Name:
Robert Bosch GmbH

Website Bosch Mobility Solutions:
www.bosch-mobility-solutions.de/de/

Domains:
Automotive supplier, consumer goods (electrical tools, domestic appliances), industrial and building technology

Headquarters:
Gerlingen, Germany

Employees:
389,281 (2016)

Revenue:
73.129 billion EUR (2016)

BOSCH
Invented for life

Our Competencies and Solutions

- Safety Engineering and Safety Architectures
- Virtual Engineering, Simulation, FERAL, safeTbox

Your Benefits

- Flexible SW safety architecture enables use of non-automotive HW for safety-relevant applications
- Expensive special HW can be significantly reduced

What It Is about

In the area of autonomous driving, providers of automotive solutions are facing major challenges, as the complexity and the resource requirements of the systems used continue to increase enormously. Robert Bosch GmbH, one of the best-known suppliers in the automotive domain, also needs to address many challenges in the development of functions for highly automated and autonomous driving. One of the most important ones is to ensure safe and reliable functions, which is indispensable in this area – because human lives are at stake, after all. Bosch therefore decided to rely on the expertise of the Fraunhofer Institute for Experimental Software Engineering IESE. The institute has comprehensive competencies and project experience in the areas of embedded systems, safety, and virtual engineering. Together the project partners developed a flexible software safety architecture that enables the use of non-safety hardware for safety-relevant applications.

»Thanks to the solution realized together with Fraunhofer IESE to safely detect sporadic defects, we can now make do without expensive special hardware and still achieve safety. We are so much convinced by the results of our collaboration with Fraunhofer IESE that we will transfer them into series production.«

Markus Schweizer, Project Manager, Central Research; Robert Bosch GmbH

The Challenge

The challenges for providers of solutions in the area of autonomous driving are very diverse. For example, huge processing power is required to enable the necessary environment detection and the control of highly automated driving functions. In order to make it possible to rapidly respond to defects or to offer "functions on demand", future software architectures must enable, e.g., flexible over-the-air updates via a wireless interface.

However, neither the required processing power nor the required flexibility can be realized with established automotive components. There are also financial reasons why components from the area of consumer electronics will soon play an ever greater role. But whereas automotive components are already equipped with numerous safety mechanisms on the hardware side, this is not the case for consumer electronics. In order to be able to provide higher processing power and flexibility paired with the indispensable requirements on safety and reliability, the experts of Fraunhofer IESE have developed novel concepts in the context of a software safety architecture together with a research team from Bosch. These concepts now implement redundancy concepts realized at the software level that are otherwise realized at the hardware level.

The Solution

The focus of the joint research work was on the development of system components for the detection of runtime defects in the hardware. The twist: The use of expensive special hardware can be reduced significantly. The solution centers on the redundant execution of safety-critical functions at the software level. The challenge in this regard was to design the system in such a flexible manner that it is able to fulfill its task for the application function transparently on a wide variety of execution platforms. Central properties such as the physical distribution, the degree of redundancy, the alignment of extensive input data, the process for comparing the results, as well as the response to defects had to be taken into account.

The resulting solution is a flexible software safety architecture that enables the use of non-safety hardware for safety-relevant requirements. The project team demonstrated its realizability with the help of a prototype implementation, taking extensive safety considerations into account. Among other things, the experts used the tool **safeTbox** developed by Fraunhofer IESE to examine the degree of diagnostic coverage of a selected architecture configuration. For the safety analysis they used integrated component fault trees to identify possible defect patterns and demonstrate the suitability of the implemented measures. In addition, the research team employed robustness tests through simulation in a virtual execution environment using the IESE tool **FERAL**. This allowed the researchers to assess further influences, which may result, for instance, from complex operating system functionalities or communication channels.

The solution will enter series production – an indication that Bosch is convinced of usefulness of the results. In addition, the research team will jointly register the concept as a patent.

The Result

In the future, Bosch will be able to work with a solution that safely recognizes sporadic defects even in non-automotive hardware. High-performance hardware can thus be integrated safely and the use of expensive special hardware can be reduced to a significant extent.

Contact:

Ralf Kalmar | Business Unit Manager
Autonomous & Cyber-Physical Systems

Phone: +49 631 6800-1603
ralf.kalmar@iese.fraunhofer.de

www.iese.fraunhofer.de

Products and Downloads:

FERAL: feral.iese.fraunhofer.de

safeTbox: safetbox.iese.fraunhofer.de