OSPERT 2015 Keynote Talk

Software Architectures for Advanced Driver Assistance Systems (ADAS)

Robert Leibinger
Elektrobit Automotive GmbH

In recent years, the demand for electronic control units (ECUs) has been rapidly growing along with the number and complexity of functions these ECUs help to realize. The criticality of functions from a functional safety point of view is also increasing, which has lead to a demand for standards for safety-critical systems such as IEC 61508 or ISO 26262. At the same time, the underlying software architecture has also been standardized by committees such as AUTOSAR.

Traditionally, most automotive systems have been constructed as fail-safe systems, i.e., the failure of a system is detected with high confidence and the system degrades or is simply shut down. Every driver is nowadays aware of such diagnostic functions in the form of yellow or red warning signs telling them to visit the garage or even to stop the car immediately.

However, with the advent of supported, assisted, or even autonomous driving, the focus shifts from fail-safe systems to fail-operational systems. Such systems need to detect an error or even the fault leading to an error before the error leads to the failure of the system. Such systems are well established in other domains such as nuclear, where failure is not an option, or avionics, where many systems simply can't be shut down during flight operation.

As the automotive market is cost sensitive, different patterns need to be applied depending on the functionality, criticality, and reliability requirements of the system. To identify which pattern needs to be implemented, error scenarios as well as their effect on the reliability of the system need to be analyzed.

Reliability engineering shows that these solutions must use some form of redundancy, e.g., a degraded function on a different core of a multi-core processor or a different ECU or even a fully redundant function on a different ECU. Real-time requirements of the system as well as network latency and bandwidth are important factors for the selection of the optimal pattern. Such constraints often have a large impact on the implementation and can even influence the selection of algorithms that are used in advanced driver assistance systems, e.g., object recognition.

The keynote will show with examples how established concepts can be integrated into the automotive domain using both well-known approaches such as AUTOSAR or standard diagnostic functions, as well as new approaches such as service-oriented architectures based on automotive Ethernet.

Robert Leibinger studied Communication Electronics at Georg Simon Ohm University of Applied Sciences in Nuremberg, Germany. After graduating as Diplom-Ingenieur he started at 3SOFT (now Elektrobit, EB) in 2001 as Software Engineer for medical systems. In 2002, he switched to the automotive team, working on the OSEK operating system introduction at Daimler and serving as a consultant for several tier-1 suppliers regarding OSEK software architectures.

Starting in 2007, Robert became team leader of the AUTOSAR MCAL driver integration team and main contact to the microcontroller vendors. In 2011, he took over as the Product Manager responsible for the EB Safety Products and Operating Systems. Since 2014, he is part of the Solution Manager Team. The team defines and manages OEM-specific solutions using EB products and services. Robert is responsible for Daimler, JLR, and Functional Safety Solutions from Elektrobit.