Braunschweigische
Wissenschaftliche Gesellschaft

Jahrbuch 2016

Sonderdruck
Seiten 217–221

J. Cramer Verlag · Braunschweig
2017

Dependable Advanced Driver Assistance Systems by a Combination of Design Time Testing and Runtime Monitoring*

Andreas Rausch et.al.

TU Clausthal, Institute for Applied Software Systems Engineering,
Wallstr. 6, D-38640 Goslar, E-Mail: andreas.rausch@tu-clausthal.de

Institute for Applied Software System Engineering (IPSSE)

From coffee machines, through mobile phones and pacemakers, to aircraft – most products released these days include some kind of software element. The almost certainly complex programs hidden on the tiny microchips control all manner of processes, in a way acting as the brains behind the technology. A standard passenger car conceals around 100 million lines of code. If you printed this out onto standard paper and lined the pieces up end-to-end, then the line would stretch right across Europe. When it comes to the self-driving car of the future, the software will be even more complex and extensive.

Software developers of the future therefore don‘t just need ever greater knowledge, they also need innovative tools and systems that can deal with increasing complexity of requirements, while at the same time remaining affordable and flexible. This is the challenge addressed by the research association formed by the Institute for Applied Software Systems Engineering (IPSSE) at TU Clausthal and their expert colleagues at TU Braunschweig. The institute is supported and partially funded by notable companies from various sectors.

The research association carries out research in five fields: reliable reactive systems, adaptive and modular architectures, platform and development tools, hardware/software co-design, and continuing education. IPSSE Researchers investigate, e.g., the utilization of software components for sound and efficient modification of software systems, the optimization of task distribution and scheduling on multi-core systems, variable architectures for the integration of heterogeneous service into open adaptive systems, or the systematic identifica-

* Der Vortrag wurde am 08.04.2016 in der Klasse für Ingenieurwissenschaften der Braunschweigischen Wissenschaftlichen Gesellschaft gehalten.

tion of signal patterns in vehicle measurements for their analysis and usage in offline tests.

The research results are demonstrated and validated in practical applications in the environment of industrial partners and with their close cooperation. Within the research, demonstrators, prototypes or full-featured tools suitable for industrial programmers and engineers are developed incorporating innovate methods and latest academic results. Seamless tool support is realized within demonstrating scenarios.[1]

It is important to the Institute to also support budding researchers in all of these important fields. Students can benefit from a practical master's program alongside a tailored program of instruction. What is more, the graduates have a good chance of getting an attractive job in industry.

Research Project: Dependable Advanced Driver Assistance Systems

In the following, one of our current research projects is described in more detail. In the project Dependable Advanced Driver Assistance System (DADAS), we currently investigate the verification and validation of Advanced Driver Assistance System (ADAS) under the infinite quantity of possible situations these system will encounter in the real world. It is necessary to systematically verify the safety of ADAS in such highly dynamic environments in order to exclude any for the drivers, the vehicles and any persons or objects in their environments.

Research Problem: Verification and Validation of ADAS

Driver assistance systems, (semi-)autonomous mobility systems and mobility management systems are gaining more and more importance in mobility carriers, such as vehicles, aircraft or rail- transport systems. They greatly assist the driver in his controlling task or replace it partly or even completely. For example, they assist in critical situations, help to counteract a possible malpractice and minimize the risk of accidents.

Such assistance systems are, however, extremely complex. The size of the systems continuously increases with the set of functions with which they support the driver and results in a higher degree of autonomy for the assistance systems. ADAS has to independently plan and execute appropriate measures based on the

[1] see http://www.ipsse.de/

current environmental situation. Therefore the ADAS has to consistently monitor and interact with the highly dynamic environment, leading to a complex reactive system with distributed components and complex algorithms. Furthermore, the environmental complexity makes it not feasible to exhaustively consider every possible environmental situation in which the assistance system may have to work. This leads to a certain degree of uncertainty with which these systems have to be developed.

Despite the increasing influence of driver assistance systems, the highest road safety must be maintained. ADAS has to safely operate in highly dynamic environments and to exclude any harm for the drivers, the vehicles and any persons or objects in their environments. Developers are required to sufficiently prove the system's dependability.

Today's conventional engineering methods are not able to provide such dependability guarantees for the steadily increasing complex ADAS with its (semi-) autonomous functionalities and inherent uncertainty. Currently, mainly statistical quality assurance techniques are used. The ADAS is observed along a large number of actually driven miles. If no accident occurs within this distance, the ADAS is judged to be safe. However, if the functionality and complexity of ADAS increase, actually driving the Dependable Advanced Driver Assistance Systems (DADAS) vehicle for long distances is infeasible if not impossible. Also, it will be unclear if all relevant situations can be encountered by randomly driving the vehicle, even for longer distances.

New approaches have to be developed to ensure the availability, reliability, safety and accuracy of these complex driver assistance systems. An idea is to transfer quality assurance effort from tests on real roads to offline simulations in order to reduce the costs and time needed for failure search and correction. In these simulations, the ADAS has to be tested for a comprehensive set of common and uncommon – critical- traffic scenarios which the automated vehicle will encounter in the real world.

Even though the set of possible scenarios, in which an ADAS is required to behave as expected and needs to be simulated (tested) is vast - if not unlimited -, the set of scenarios, considered in simulations and tests, still has to be constructed systematically. With current state-of-the-art quality assurance approaches from computer science and systems engineering, ADAS cannot be verified appropriately through simulations and tests. A systematic approach for determining all relevant scenarios for the correct and safe behavior is missing. The uncountable amount of possible scenarios is unlikely to be exhaustively simulated and tested. Furthermore, a sufficient coverage criterion for the reduction of the considered set of scenarios, as known from traditional software testing, is not yet defined for ADAS and its variety of vast scenarios.

Research Objectives: System Dependability by a Combination of Design Time Testing and Runtime Monitoring

In our research we intend to devise novel methods in order to ensure the safety, robustness and dependability of ADAS by detecting critical and unsafe driving situations and initiating appropriate counter measures. We aim at a synergetic combination of design time analysis and runtime monitoring (cf. Figure 1: Overview about the combination of design time testing and runtime monitoring. Figure 1) in order to determine behavioral deviations of ADAS and/or environments, as well as failures of sensors, under quality-related costs.

Using design time testing in x-in-the-loop simulations, the correctness and dependability of ADAS is verified for a pre-defined manageable subset of relevant traffic scenarios. These can be the most relevant or most dangerous scenarios known at design time. It is impossible to test all possible real scenarios, ADAS is likely to encounter in the real world, because of its exponential combinatorial. We can only exhaustively test a well-defined subset of all possible scenarios at design time. This subset of relevant traffic scenarios has to be systemically assembled. Each scenario is used in the simulations as environmental model.

The set of test qualified scenarios is adopted as foundation for the runtime monitoring within the vehicle. All traffic situations merging from the simulations of these scenarios are recorded and used as knowledge for the runtime monitors. If those situations are the only ones encountered at runtime, the ADAS is known to be safe. If a non-secured behavior is monitored in one or more situations, no guarantees can be given for the correctness and dependability of the vehicle in

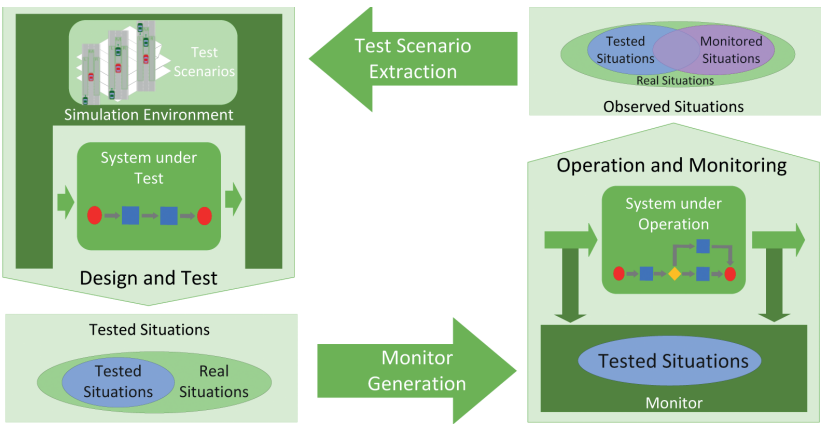

Figure 1: Overview about the combination of design time testing and runtime monitoring.

these situations. For instance, the driver can be warned or the ADAS functionality can be disabled. Further, the behavioral deviations of the ADAS and/or the environment from the behaviors of the qualified scenarios allow estimations about failures of the ADAS, its sensors or the assumed scenarios.

An iterative feedback process can be used to extend the set of verified scenarios by adding missing, scenarios from the in-vehicle monitoring to the test set of scenarios or altering existing faulty scenarios. With each iteration the maturity level of the DADAS test and the simulation framework will improve. After several iterations the behavior of the ADAS in the most likely driving situations is tested and qualified. This approach will iteratively eliminate unsafe behavior from ADAS and enhance the dependability and safety of these systems, which will result in an improvement of the overall traffic safety by reducing the number of accidents.

Our concept and implementation of this approach – combining design time testing in simulation and runtime monitoring to improve the dependability of complex Advanced Driver Assistance Systems – can be found in the following peer-reviewed publications:

[1] MAURITZ, M., A. RAUSCH & I. SCHAEFER (2014): Dependable ADAS by Combining Design Time Testing and Runtime Monitoring. – In FORMS/FORMAT 2014, 10th Int. Symp. on Formal Methods.

[2] MAURITZ, M., F. HOWAR & A. RAUSCH (2015): From Simulation to Operation: Using Design Time Artifacts to Ensure the Safety of Advanced Driving Assistance Systems at Runtime. – International Workshop on Modelling in Automotive Software Engineering.

[3] MAURITZ, M., F. HOWAR & A. RAUSCH (2016): Assuring the Safety of Advanced Driver Assistance Systems Through a Combination of Simulation and Runtime Monitoring. – In Leveraging Applications of Formal Methods, Verification and Validation: Discussion, Dissemination, Applications.