Delft University of Technology

Delft Center for Systems and Control

Technical report 03-010

VEHIL: A test facility for validation of fault management systems for advanced driver assistance systems*

O. Gietelink, J. Ploeg, B. De Schutter, and M. Verhaegen

If you want to cite this report, please use the following reference instead:
O. Gietelink, J. Ploeg, B. De Schutter, and M. Verhaegen, "VEHIL: A test facility for validation of fault management systems for advanced driver assistance systems," *Proceedings of the 1st IFAC Symposium on Advances in Automotive Control*, Salerno, Italy, pp. 410–415, Apr. 2004.

Delft Center for Systems and Control
Delft University of Technology
Mekelweg 2, 2628 CD Delft
The Netherlands
phone: +31-15-278.24.73 (secretary)
URL: https://www.dcsc.tudelft.nl

* This report can also be downloaded via https://pub.bartdeschutter.org/abs/03_010.html

VEHIL: A TEST FACILITY FOR VALIDATION OF FAULT MANAGEMENT SYSTEMS FOR ADVANCED DRIVER ASSISTANCE SYSTEMS

O. Gietelink [*,**] **J. Ploeg** [*] **B. De Schutter** [**] **M. Verhaegen** [**]

[*] *TNO Automotive, P.O. Box 6033, 2600 JA Delft, The Netherlands, email: {gietelink,ploeg}@wt.tno.nl*
[**] *Delft Center for Systems and Control, Delft University of Technology, Mekelweg 2, 2628 CD Delft, The Netherlands, email: {o.gietelink,b.deschutter,m.verhaegen}@dcsc.tudelft.nl*

Abstract: We present a methodological approach for the validation of fault management systems for Advanced Driver Assistance Systems (ADAS). For the validation process the unique VEHIL facility, developed by TNO Automotive and currently situated in Helmond, The Netherlands, is applied. The VEHIL facility provides the opportunity to make the entire development process of intelligent vehicles safer, cheaper, and more manageable, and to make simulation more reliable. The main feature of VEHIL is that a complete intelligent vehicle, including its sensors and actuators, can be tested in a Hardware-In-the-Loop simulation environment. In this way VEHIL can be applied in the design phase for fast and easy optimization of the sensor configuration. Moreover, due to its ability for providing very accurately controllable testing conditions, VEHIL can also be used for the validation of the performance of intelligent vehicle control and fault management systems. In this paper, we particularly focus on the use of VEHIL for the validation of fault management systems for Advanced Driver Assistance Systems.

Keywords: automotive control, fault-tolerant systems, advanced driver assistance systems, fault management, hardware-in-the-loop simulation

1. INTRODUCTION

Passenger transport by car has increased rapidly over the past decades, bringing many benefits to society, but also having negative consequences regarding:

- Accessibility: traffic jams are not only a source of discomfort for the driver, but also cause a large macro-economic loss in terms of lost man hours.
- Sustainability: passenger car transport is responsible for a large amount of air pollution, which is amplified by traffic jams.
- Safety: every year in Europe alone, more than 40 000 casualties and many more injuries are caused by vehicle-related accidents.

Advances in technology have made passenger cars ever safer, but in the area of passive safety many possibilities for improvements have now been exhausted. However, "intelligent transport systems" offer the possibilities to improve traffic safety by active means, while at the same time improving accessibility and sustainability. The development of intelligent control systems for assisting the driver, so-called Advanced Driver Assistance Systems (ADAS), are therefore of major interest to the automotive industry. Examples of ADAS that have recently been introduced on the market are Adaptive Cruise Control, Parking Assistant, and Lane Departure Warning Assistant. Future developments include Collision Warning, Collision Avoidance, and Pre-Crash Systems (PCS). Although the use of environment sensors and electronic control

functions improves the effectiveness of passive and active safety devices in ADAS, a number of challenges still lie ahead in the development process of ADAS, especially in the area of fault management.

2. CHALLENGES IN ADAS DEVELOPMENT

Today, control systems in the automotive industry are characterized by an increased complexity of the system and its environment, an ever increasing user requirements for dependability, and an increased need for fault management, which have a significant impact on the design process (in particular, that of ADAS).

2.1 Increased complexity of the system and its environment

Within the automotive industry the importance of electronic control functions is increasing rapidly. Today, software and electronics account for more than 25 % of the total development costs of a passenger car (Poledna and Kroiss, 1999). The increasing trend towards automatic safety systems implies a growing number of sensors, actuators and control systems implemented in embedded systems, causing ever more *complex* systems. Moreover, the interaction with the human driver and the traffic environment adds yet another level of complexity to these systems.

2.2 User requirements for dependability

Apart from the desire for low cost and high performance, the user has ever increasing requirements regarding *dependability*. Dependability can be defined as the trustworthiness of a safety-critical computer system, such that reliance can justifiably be placed by the user on the service it delivers (Laprie, 1992).

The demand for dependability, especially in terms of *reliability* and *safety* (which will be defined below, in Section 5.1), increases with increasing automation of the vehicle's driving task. The failure of an automatic safety system simply cannot be tolerated. E.g., automatic deployment of an airbag or a belt pre-tensioner in a PCS should be executed if, and only if, a crash is imminent and unavoidable. However, the increasing complexity of automated vehicle control systems and their environment is often in contradiction to these high safety and reliability requirements. In addition, it is difficult to even define the requirements themselves, and to assess whether the system conforms to them. In this paper the PCS will be used to illustrate the validation of the user requirements.

2.3 Increased need for fault management

Key means for increasing the dependability of a complex control system are *fault prevention*, *fault tolerance*, *fault removal* and *fault forecasting*.

Fault prevention aims to detect and remove faults during the design process. However, not all faults can be prevented, which stresses the need for fault removal. If faults cannot be removed during operation, fault tolerance techniques are necessary, e.g., using redundant components. For both approaches fault forecasting is crucial in order to estimate size and location of the fault.

During the development of a PCS, possible faults that can occur should be identified, before the dependability can be assessed. It is however difficult to validate the capabilities of the fault management system against the dependability requirements. Moreover, it is impossible to identify all potential failure modes and their interactions. And even if this would be possible, the large number of possible failure modes under various operating conditions make *exhaustive testing* impractical. Furthermore, it is usually difficult to reproduce the test conditions and failure modes under which the control system operates.

2.4 Design and validation of complex systems

The issues mentioned above have consequences for the design and validation process of ADAS:

- Longer development times, whereas manufacturers have a desire for a shorter time-to-market of their products.
- Higher costs for the validation process: it is now estimated that testing and evaluation may take up to 50 % of the total development costs of an ADAS. This figure will likely increase with the introduction of more safety-critical applications.
- Simulation tools are increasingly employed for design and validation of complex systems. However, due to the complexity in modeling environmental conditions, sensor and actuator behavior, and other electronic equipment, not all situations can be tested reliably with simulations.

As a consequence, design and validation of ADAS, especially regarding fault management requires a growing effort in the product development process of these systems, and highlights the need for cost-efficient, time-efficient, and more reliable validation methods for the design and validation of complex systems.

Hardware-In-the-Loop (HIL) simulations play an important role in validation of automotive mechatronic components. However, with regard to validation of the integrated vehicle system, it is difficult to validate the safety and reliability requirements and to assess the performance. Currently, test runs on a proving ground are used to test a complex ADAS, but this has a number of disadvantages:

- It is impossible to perform exhaustive testing to cover every possible operating scenario and failure mode.

- Due to disturbances, test results can be unreliable, and difficult to analyze and reproduce.
- Extensive safety precautions have to be taken to ensure the safety of test drivers and prototypes.
- Due to the high system complexity, the limited controllability of testing conditions and the necessary safety precautions, the validation phase is the most expensive and time-consuming part of the development process.

To overcome these difficulties, TNO Automotive has developed a laboratory specifically for the design and validation of intelligent vehicles: VEHIL (VEhicle Hardware-In-the-Loop). The VEHIL concept makes it possible to conduct experiments with full-scale intelligent vehicles in a laboratory, where the complete vehicle is tested in a HIL simulation.

3. VEHIL FACILITY

3.1 Working principle of VEHIL

In the VEHIL laboratory a virtual environment is defined in which the vehicles, the infrastructure and their interactions are simulated in real-time, but where part of the simulation is performed with hardware (see Figure 1).

The Vehicle Under Test (VUT) is placed on a chassis dynamometer (roller bench), which provides a realistic load for the vehicle's actuators (throttle, brake, steer) and is interfaced with its counterpart in the virtual environment. Accordingly the VUT's state (position, orientation, velocity, acceleration) is changed in the simulation. In the VEHIL laboratory one or more surrounding traffic participants are represented by so-called Moving Bases (MBs), see Figure 2. The MB is an autonomous positioning platform that responds to position commands of the simulator and emulates the motions of the other road users relative to the VUT. In this way, the dynamics of the experiment are restricted to the relative motion as seen from the point of view of the VUT, but still exhibit a dynamic "real" environment for the VUT.

The VUT is instrumented with sensors, actuators and equipped with an on-board control system to implement intelligent control actions, such as sensing an imminent collision and activating pre-crash restraints. The environment sensors of the VUT (e.g., radar, laser, vision) receive realistic sensor input, as if the VUT were driving on the road. The on-board controller is fed by a mixture of real sensor readings and virtual sensor readings (generated by the simulator). On the basis of these sensor inputs the control system takes action and sends command signals to the actuators. In this way the loop in the HIL simulation is closed, as shown schematically in Figure 1.

In Figure 3 a photograph of the VEHIL facility is presented. The VEHIL facility has an effective test area of 200 m by 40 m. The effective height of the facility hall is 5 m. The hall has an elevated control room near the chassis dynamometer placing. This ensures a maximum test area and gives a good overview of the hall.

Now we discuss the most important components of the VEHIL facility in more detail:

- Multi-agent real-time simulator:
  The complex traffic scenario with multiple interacting road users is controlled by the Multi-Agent Real-time Simulator (MARS). This multi-agent based framework decomposes the traffic simulation into a number of autonomous entities. These entities are controlled by their internal dynamics and communicate via abstract sensors and actuators as shown in Figure 1. More information can be found in (Papp and Hoeve, 2000).
- Moving bases:
  The MBs used to represent other road users in the VEHIL facility are specifically designed for this purpose. In order to emulate a vehicle motion relative to the VUT, the MB must be able to perform any arbitrary movement, not hindered by the conventional motion constraints of a car. Therefore, the MB has been built with four independently steered wheels. The MB is controlled by a so-called *generic controller*, which transforms the desired vehicle motion from the simulation into the command signals for the separate wheel drives and steering motors (Ploeg *et al.*, 2002).

  In practice, an emergency stop of a passenger vehicle corresponds to $10\,\mathrm{m/s^2}$ deceleration maximum. As a consequence, the MB has been designed such that it is capable of accelerating with $10\,\mathrm{m/s^2}$ in order to simulate an emergency stop of the VUT. The dynamic maneuvering behavior of conventional passenger cars can be described in terms of yaw response to steer inputs and speed response to throttle/brake input. The corresponding transfer functions typically show a bandwidth in the 1 Hz frequency range. This implies that the MB must at least have a bandwidth of about 5 Hz in order to minimize positioning phase lag. Finally, the top speed of the MB, which in view of the relative VEHIL world corresponds to the maximum speed difference between two cars, is equal to 50 km/h. This covers about 95 % of all collision scenarios (Moritz, 2000).
- Chassis dynamometer:
  The chassis dynamometer consists of four independently driven rolls, such that road curves can also be simulated. Similar to the required dynamic performance of the MBs also the dynamic response of the chassis dynamometer to the driving actions of the VUT needs to be at a realistic level in terms of delay times and phase lag. Therefore, the coupling of the four drums

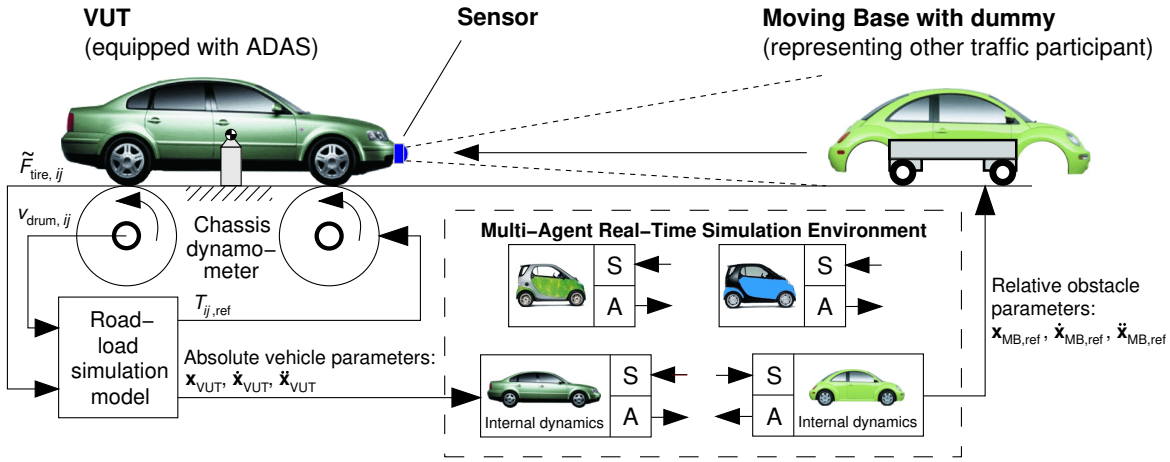

Fig. 1. Schematic representation of the VEHIL working principle.

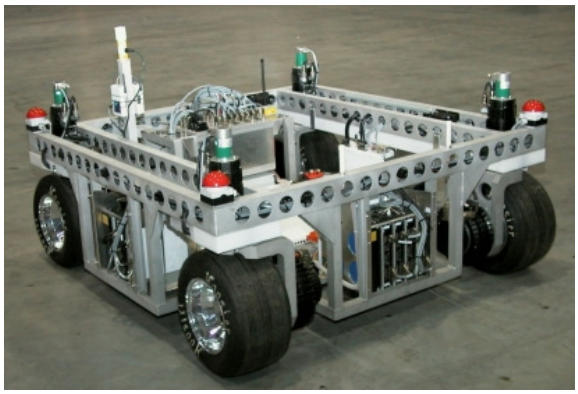

Fig. 2. The moving base (MB).

has a high correlation with the real world driving conditions, even at transient behavior.

3.2 Applications for VEHIL

In the VEHIL laboratory several types of ADAS can be tested, such as automatic guided vehicles, vehicle-to-vehicle communication (Morsink and Gietelink, 2002), Adaptive Cruise Control and Stop&Go applications, Collision Warning and Avoidance Systems, and PCS (Labibes *et al.*, 2002). More specifically, VEHIL can be used for the design and validation of these ADAS in the following ways:

- Development of the control algorithms in terms of the functional performance of the ADAS and real-time behavior, i.e., control prototyping.
- Sensor development, i.e., testing sensor characteristics and sensor modeling.
- Fault management testing by injecting faults in the HIL simulation.

3.3 Advantages for the customer

The VEHIL approach offers a number of distinct advantages as opposed to conventional design and validation tools:

- Lower costs, because only one prototype vehicle and no test drivers are required for the tests. Furthermore, a large number of tests can be performed in a short time frame.
- Since the traffic environment is controlled from a simulation, tests can be performed accurately and reproducibly. In this way it is possible to investigate the influence of specific system characteristics on the performance.
- Test can be performed very safely, since no persons are physically present during the test and because of the absence of high absolute velocities.
- VEHIL provides the opportunity for a quick and flexible variation of the desired traffic scenarios.
- Faults can easily be injected to the VUT, since all of its inputs and outputs are linked to the simulation environment. This link between hardware components and the simulation environment also allows all vehicle parameters to be easily monitored during the test.

4. ILLUSTRATION OF THE VEHIL FACILITY: TESTING PCS IN VEHIL

As the VEHIL facility is not yet fully operational, its feasibility will be demonstrated using a test with a vehicle equipped with a PCS in a preliminary VEHIL set-up (Labibes *et al.*, 2002).

Testing PCS in a reliable way is very difficult using conventional test methods, since it is unsafe, costly and not reproducible to actually perform a crash with a prototype vehicle. An alternative would be to test on a track with a dummy vehicle. However, these tests are also not reproducible and may cause damage to the prototype vehicle (Alessandretti *et al.*, 2002).

For the experimental set-up the VUT is equipped with a laser sensor, a controller and a pre-crash seat belt pre-tensioner. During the experiment the MB follows a crash trajectory, such that it is sensed by the laser scanner as a potential obstacle. When the controller estimates that a collision is unavoidable (taking nor-

Fig. 3. VEHIL hall.

mal vehicle behavior into account), it activates the belt pre-tensioner. However, an actual collision in this VEHIL-like set-up is avoided, because the MB can reach a much higher dynamic lateral acceleration than a standard passenger car, and thus makes an evasive maneuver at the latest moment, as shown in Figure 4.

The preliminary tests show that the concept is feasible and that the VEHIL concept provides significant advantages for testing. Using the HIL set-up in the VEHIL laboratory, experiments can be performed quickly and accurately and under near-realistic operating conditions. Initialization of a test sequence is a matter of seconds, whereas on a test track this would bring about extensive test procedures. Especially with regard to testing PCS the prototype vehicle is not damaged during the tests.

5. METHODOLOGY FOR VALIDATION OF FAULT MANAGEMENT SYSTEMS

As can be seen from the analysis above, VEHIL has a number of distinct advantages. Because this facility is under active further development and improvement, there is much ongoing research and development in connection with the simulation environment, MB control, sensor models, and scenario development. One of the main research issues is focused on the application of fault injection techniques in the VEHIL facility in order to test the fault management systems of ADAS, and on the development of a methodology for validation of fault management systems. Based on the preliminary experience with VEHIL, an outline of this methodology is described below.

5.1 Definition of dependability requirements

The development process of an ADAS begins with the identification of the user requirements, which for safety-critical applications such as ADAS can be specified as follows (Storey, 1996):

- *Reliability* can be defined as the probability of a component or a system functioning correctly over a given period of time under a given set of operating conditions. A measure for reliability is the false alarm and missed alarm rate that the system encounters.
- *Safety* is a property of a system that it will not endanger human life or the environment and can be quantified using Safety Integrity Levels (SIL).

Although safety and reliability have sometimes conflicting requirements, one aspect that contributes to both is fault-tolerant behavior, i.e., to maintain operational behavior in spite of faults. In order to prove reliability and safety, *validation* is meant to verify that the faults are handled correctly without interrupting the system operation. Furthermore, faults must be identified that have not yet been found during the design process. From the user requirements test specifications and acceptance criteria can be identified.

5.2 Modeling of the complex vehicle system and its failure modes

From a safety analysis, such as a Failure Modes, Effects and Criticality Analysis (FMECA) or a Fault-Tree Analysis, the critical failure modes can be identified. For a PCS various fault types can be identified:

- environment-related, such as deterioration of sensor signals due to weather conditions,
- equipment-related, such as errors in the human-machine interface, sensor failures, actuator failures, hardware failures, or software failures,
- incidents, such as complicated vehicle maneuvers reaching the system limitations, possibly resulting in *false positives*.

When the potential failure modes of the system have been identified, a suitable *test coverage* must be defined. An ideal test scheme might provide complete coverage, but unfortunately exhaustive testing in terms of investigating all possible failure patterns is almost always impossible. An alternative way of looking at the problem is to explicitly consider the system's internal states and their cause-and-effect relations, and use fault modeling to assist in the design of testing methods.

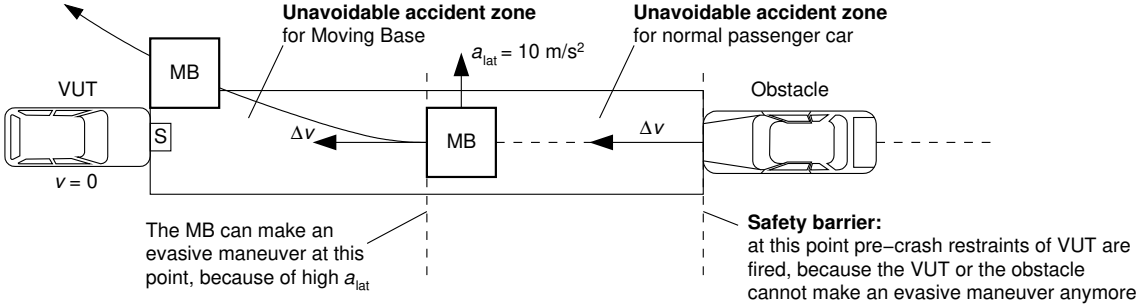

Fig. 4. Testing a PCS in VEHIL.

5.3 Fault injection

Fault injection is a phrase covering a variety of techniques for inducing faults in systems to measure their response to those faults. In particular, it can be used in both electronic hardware systems and software systems to measure the fault tolerance of the system. The contribution of fault injection to dependability assessment of ADAS encompasses both fault removal and fault forecasting. With respect to the former, fault injection is primarily used to estimate the distribution of the coverage achieved by the fault tolerance mechanisms built into the ADAS control system. With respect to the latter, fault injection may reveal potential failure modes that were not previously discovered. In VEHIL failure modes or *errors* can be introduced in a controlled and reproducible way, thus allowing to estimate the influence of a single fault type.

The next step is to generate *test vectors* that capture the essential scenarios and failure modes in an efficient way. It is the objective of ongoing research to develop a methodology to design a minimal (or as small as possible) set of test vectors that cover the fault space.

6. CONCLUSIONS

We have presented the VEHIL concept and explained how it can be incorporated in the design and validation process of ADAS, especially regarding dependability requirements and their consequences for validation of fault management systems. The main conclusions are:

- Fault management in terms of fault prevention, fault removal, and fault tolerance, is crucial for the success of safety-critical ADAS applications. For cost-efficient and time-efficient testing, it is however necessary to correctly identify the safety requirements, the acceptance criteria, the critical failure modes, and the critical scenarios. VEHIL provides a development and validation environment that supports these steps in the development process.
- Within the development process of an ADAS, the VEHIL facility provides an excellent tool for easy validation of the performance of the ADAS control system in terms of functional behavior, driving comfort and fault management.
- The application of VEHIL to the development process saves time, because of transparent techniques for fault injection and clear interpretation of test results. Furthermore, reproducible experiments make it possible to single out the performance of a single system parameter and thereby to accurately determine the performance of specific characteristics. VEHIL supports an "optimum" design of the ADAS, such that the right amount and performance characteristics of sensors and actuators and adequate levels of redundancy are applied. In this way, costs can be minimized, both for the design phase and the testing phase.

Acknowledgments
Research partially sponsored by TNO-TRAIL.

REFERENCES

Alessandretti, G., P. Baraud, C. Domsch and G. Sala (2002). A European activity on pre-crash application: The CHAMELEON project. In: *Proc. E-Safety Conf.* Lyon, France.

Labibes, K., D. Verburg and P. Lemmen (2002). AV3 — Automatische veiligheid in verkeer en vervoer, Work package 1: Survey and system specifications. Tech. rep. D01. TNO. Delft, The Netherlands.

Laprie, J.C. (Ed.) (1992). *Dependability: Basic Concepts and Terminology*. Springer. Vienna.

Morsink, P. and O.J. Gietelink (2002). Preliminary design of an application for CBLC in the CarTALK2000 project: Safe, comfortable and efficient driving based upon inter-vehicle communication. In: *Proc. E-Safety Conf.* Lyon, France.

Papp, Z. and H.J. Hoeve (2000). A multi-agent based modeling and execution framework for complex simulation, control and measuring tasks. *Proc. IEEE-IMTC,* pp. 1561–1566.

Ploeg, J., A.C.M. van der Knaap and D.J. Verburg (2002). ATS/AGV, design, implementation and evaluation of a high performance AGV. In: *Proc. IV 2002*. Versailles, France.

Poledna, S. and G. Kroiss (1999). TTP: Towards drive-by-wire. *Elektronik* **14**, 36–43.

Moritz, R. (2000). Pre-Crash Sensing – Functional evolution based on short range radar sensor plat-

form. *Society of Automotive Engineering*, SAE Paper 2000-01-2718.
Storey, N. (1996). *Safety-Critical Computer Systems*. Addison Wesley Longman Ltd. Essex, U.K.