

Technical report 03-005

VEHIL: Test Facility for Fault Management Testing of Advanced Driver Assistance Systems*

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

To cite this work, please refer to the published version:

O. J. Gietelink, J. Ploeg, B. De Schutter, and M. Verhaegen, "VEHIL: Test facility for fault management testing of advanced driver assistance systems," *Proceedings of the 10th ITS World Congress*, Madrid, Spain, 13 pp., Nov. 2003. Paper 2693.

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://dpub.eu/03-005>

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

Olaf J. Gietelink & Jeroen Ploeg

TNO Automotive, P.O. Box 756, 5700 AT Helmond, The Netherlands,

Phone: +31 (0)492 566 507, Fax: +31 (0)492 566 566,

E-mail: {gietelink,ploeg}@wt.tno.nl, <http://www.automotive.tno.nl/>

Bart De Schutter & Michel Verhaegen

Delft Center for Systems and Control, Delft University of Technology, Mekelweg 2,
2628 CD Delft, The Netherlands, Phone: +31 (0)15 27 85119, Fax: +31 (0)15 27 86679,

E-mail: {b.deschutter,m.verhaegen}@dcsc.tudelft.nl, <http://www.dcsc.tudelft.nl/>

SUMMARY

This paper presents the latest developments of the VEHIL facility, which aims to make the development process of intelligent vehicles safer, cheaper and more manageable. The main feature of VEHIL is that a complete intelligent vehicle can be tested in a hardware-in-the-loop simulation environment. The use of VEHIL will be illustrated by preliminary test results of a Pre-Crash System. Furthermore, a methodological approach will be presented for the validation of fault management systems for Advanced Driver Assistance Systems by fault injection in VEHIL.

INTRODUCTION

The increase of mobility by passenger car over the past decades has brought many benefits to society, but also has negative effects on:

- **Accessibility:** traffic jams are not only a source of driver discomfort, but also cause a large financial loss in terms of lost man hours.
- **Sustainability:** passenger cars are responsible for a large amount of air pollution, an effect that is further amplified by traffic jams.
- **Safety:** every year in Europe alone, more than 40,000 casualties and 1.4 million injuries are caused by vehicle-related accidents, raising the costs in both human and financial terms.

Advances in technology have made passenger cars ever safer, but in the area of passive safety systems many possibilities for improvement have now been exhausted. However, 'intelligent' control systems for assisting the driver, so-called Advanced Driver Assistance Systems (ADASs),

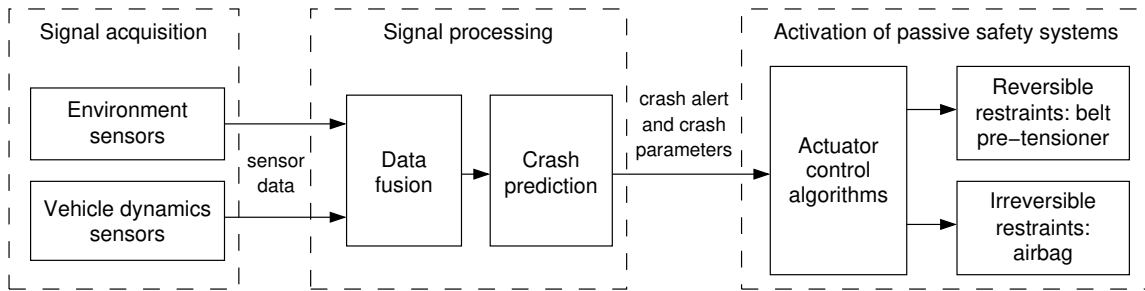


Figure 1: Components of a Pre-Crash System.

offer possibilities for improving traffic safety by active means, and at the same time contribute to accessibility and sustainability.

Examples of ADASs that have recently been introduced on the market are Adaptive Cruise Control and Lane Departure Warning Assistant (LDWA). Forthcoming developments include Collision Warning and Avoidance Systems (7) and Pre-Crash Systems (PCSs) (5). A PCS uses environment sensors (e.g. radar, laser, vision) and electronic control functions to improve the effectiveness of passive safety devices, such as airbags and seat belt pre-tensioners, by activating them before a collision occurs. A schematic representation of a PCS is shown in Figure 1.

However, in the development process of these ADASs a number of challenges still lie ahead, which will be discussed next. Then the latest developments of the VEHICLE Hardware-In-the-Loop (VEHIL) facility are presented, which aims to overcome these challenges. The use of VEHIL is illustrated by a case study with a PCS in a preliminary VEHIL setup. Finally, a methodological approach is proposed for the design and validation of fault management systems for ADASs and the use of VEHIL as a tool in this methodology.

CHALLENGES IN THE DEVELOPMENT OF ADVANCED DRIVER ASSISTANCE SYSTEMS

Increasing complexity of the vehicle 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 (11). This figure is expected to rise even further, as the increasing trend towards automatic safety systems implies a growing number of sensors, actuators and control systems implemented in embedded systems. The integration of several ADASs and the interaction with other vehicle control systems creates ever more *complex* systems. The interaction with the human driver and the traffic environment adds yet another level of complexity to the development of these systems. These interactions may introduce unforeseen failure modes and complicate the design and validation of ADASs.

User requirements for dependability

Apart from the usual desire for low cost and high performance, the user has ever higher requirements regarding *dependability*, i.e. the trustworthiness of a *safety-critical* computer system (6, 12). The dependability of an ADAS can be expressed in terms of *reliability* and *safety*. Reliability can be defined as the probability of a component, or 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 ADAS encounters. Safety is a property of a system that it will not endanger human life or the environment and in the automotive industry is usually quantified using Safety Integrity Levels.

The demand for safety and reliability naturally increases with increasing automation of the vehicle's driving task, since the driver must be able to depend on the ADAS. Failure of an automatic safety system simply cannot be tolerated, e.g. automatic deployment of an airbag or a belt pretensioner 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 requirements. In addition, it is often difficult to define these requirements and validate if the ADAS conforms to them.

Increased need for fault management

Failure modes that can occur during operation of a PCS and that may degrade dependability are:

- environment-related, such as deterioration of sensor signals due to weather conditions;
- equipment-related, such as faults in sensors, actuators, computer hardware and communication systems;
- vehicle-related, such as faults in drive-train, suspension or other vehicle subsystems; and
- software faults, such as incorrect algorithms or software bugs.

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. Various approaches for fault tolerant control of automotive mechatronic systems are described in (4). In order to prove reliability and safety, *validation* of the fault management system is meant to verify that the faults are handled correctly. Furthermore, faults must be identified that have not yet been found during the design process.

It is however difficult to validate the performance of these fault management systems against the dependability requirements. Firstly, it is very time-consuming to identify all potential failure modes and especially their interactions. Secondly, it is difficult to reproduce the test conditions and failure modes under which the control system operates. Hence, the design and validation of fault management systems represents a difficult problem.

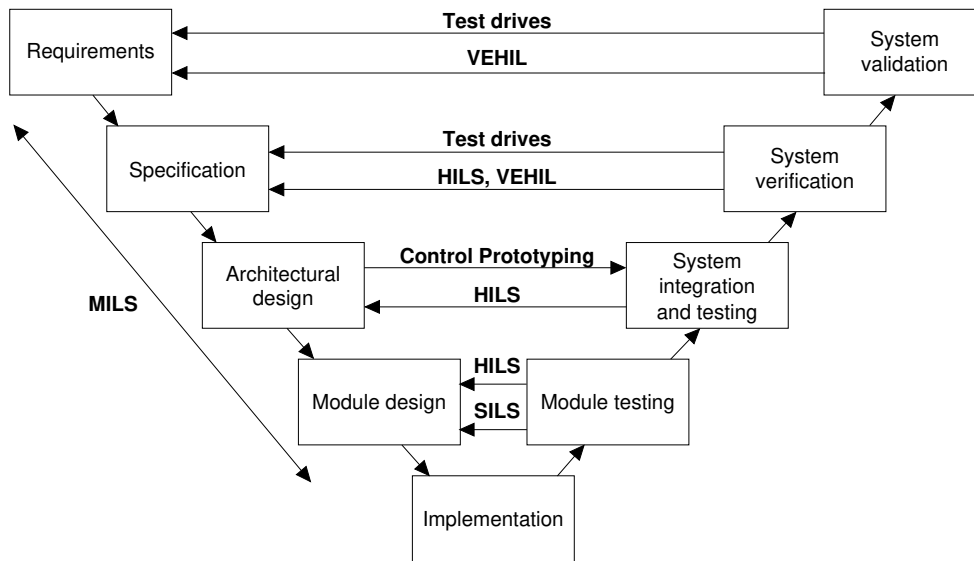


Figure 2: A diagrammatic representation of the development process for a safety-critical computer system and the tools for design and validation in different phases.

Difficulties in the design and validation of complex systems

Consequently, the following difficulties arise in the design and validation process of ADASs:

- Manufacturers are facing longer development times, whereas they have an increasing desire for a shorter time-to-market of their products.
- The costs for the validation process increases. It is estimated that testing and evaluation of an automotive control system may take up to 50% of the total development costs (2).
- Simulation tools are increasingly employed for design and validation of complex systems.

An efficient and reliable methodology for the design and validation of ADASs, especially regarding fault management, is thus desired. A popular way to represent the development cycle for embedded systems is the 'V' diagram (12), as displayed in Figure 2. In this process, the system to be developed is integrated from subsystems and components when moving up the right-hand side of the V, while activities related to requirements, specifications, as well as software design and implementation occur while moving down the left-hand side of the V.

The development process of an ADAS begins with the identification of the user requirements. From the user requirements a specification is produced, which in turn forms the basis for the design of the modules of which the system is composed. In every phase *verification* is performed to determine that a module meets its specification. When the separate modules (sensors, actuators, controllers) are integrated, *validation* of the complete system is necessary to determine that the system is appropriate for its purpose and that it conforms to the requirements. Because the

system design is changed according to the verification and validation results, the ‘V’ diagram represents an iterative process on every level.

Various tools are used for verification and validation, as indicated by Figure 2. Model-In-the-Loop Simulation (MILS), Control Prototyping and Software-In-the-Loop Simulation (SILS) are employed for control system design in an early stage. As hardware and software modules become integrated, use of Hardware-In-the-Loop Simulation (HILS) becomes necessary, where the hardware component is tested in real-time in a simulated environment (3).

HILS plays an important role in validation of automotive mechatronic components, such as ABS and suspension systems. For these components it is relatively easy to simulate the environment. However, validation of an ADAS, integrated with environment sensors and actuators, is difficult, because of the complexities in modeling sensors, actuators, vehicle dynamics and the traffic environment. ADASs are therefore currently tested by test drives on a test track, 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 must be taken to ensure the safety of test drivers and prototypes. Especially a PCS is difficult and safety-critical to test, due to the need for a collision to validate the performance of the system.

Consequently, the validation phase is the most expensive and time-consuming part of the development process of an ADAS. To overcome these difficulties, TNO Automotive has developed a laboratory specifically for the design, verification and validation of intelligent vehicles: VEHIL. The VEHIL concept makes it possible to conduct laboratory experiments with full-scale intelligent vehicles, where the complete vehicle is tested in a HILS. In this way the use of HILS for validation is extended from the component level to the vehicle system level, see Figure 2.

VEHIL (VEHICLE HARDWARE-IN-THE-LOOP)

The feasibility of the VEHIL concept was first described in (13). This section will therefore present an overview of the working principle, the latest developments, and the application of VEHIL for testing PCS and fault management systems.

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.

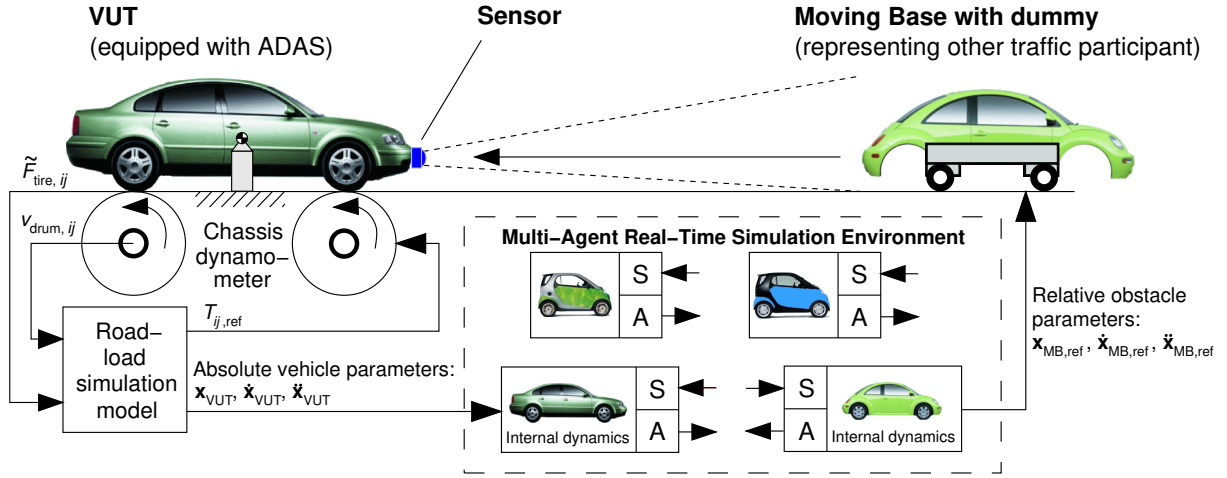


Figure 3: Schematic representation of the VEHIL working principle.

The so-called Vehicle Under Test (VUT) can be equipped with a PCS to sense an imminent collision and activate pre-crash restraints. The VUT is placed on a chassis dynamometer, 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 states $\mathbf{x}_{VUT} = [x \ y \ \psi]^T$, $\dot{\mathbf{x}}_{VUT}$ and $\ddot{\mathbf{x}}_{VUT}$ are changed in the simulation, where (x, y) is the absolute position, ψ the orientation, \dot{x} the velocity v and \ddot{x} the acceleration a . From the defined interactions between road users in the simulation environment the position of the VUT relative to other road users can be calculated.

In the VEHIL laboratory one or more of these surrounding traffic participants are represented by so-called Moving Bases (MBs). 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 the MBs still represent a dynamic 'real' environment for the VUT. The environment sensors of the VUT receive realistic sensor input, as if the VUT was 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 VEHIL simulation is closed, as shown schematically in Figure 3.

The VEHIL facility

The VEHIL facility is built in Helmond, the Netherlands by TNO Automotive and will be operational from November 2003 on. It has an effective test area of 200 m by 40 m and the effective height of the hall is 5 m. Figure 4 presents an artist impression of the facility. The components of the facility will be further described below.

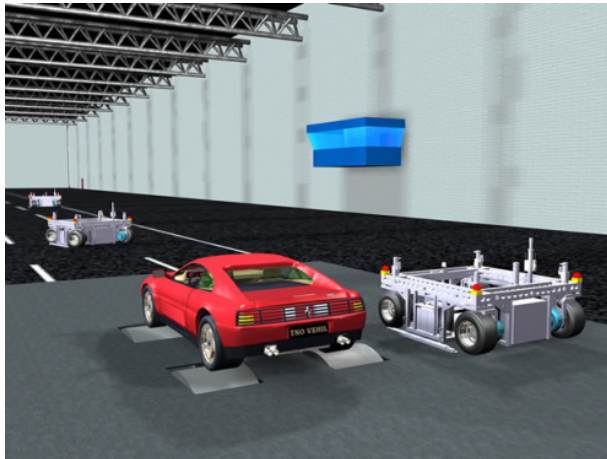


Figure 4: Artist impression of the VEHIL facility.

Multi-agent real-time simulator

The Multi-Agent Real-time Simulator (MARS) is the heart of VEHIL and generates a traffic scenario with multiple vehicles and other objects of the infrastructure in real-time, from which the relative motions between the MBs and the VUT are calculated. The main feature of the MARS is the fact that the interactions between the *entities* (vehicles and other objects in the virtual world) are dynamical in nature. These entities are controlled by their internal dynamics (a vehicle model) and communicate via abstract sensors (S) and actuators (A), as indicated in Figure 3. More information on the MARS can be found in (8, 9).

Chassis dynamometer

The dynamic response of the applied chassis dynamometer to driving actions of the VUT needs to be at a realistic level in terms of delay times and phase lag. In practice, an emergency stop of a passenger vehicle corresponds to 10 m/s^2 deceleration maximum. Consequently, the chassis dynamometer has to achieve this maximum deceleration as well. This is realized by a concept with four individual electric motor driven drums. The drums have a diameter of 1.6 m and are adjustable, such that they can accommodate a vehicle with a wheel base of 1.8 – 4.0 m and a track width of 1.2 – 2.4 m. The maximum velocity of the dynamometer is 250 km/hr.

The load simulation on each wheel (i, j) is a result of the drum inertia force and the electric motor torque T_{ij} . A vehicle mass between 800 and 3500 kg can be simulated fully. The reference signals $T_{\text{ref},ij}$ for the control units of the drums are calculated on the basis of a road-load simulation model with the observer estimated tire forces $\tilde{F}_{\text{tire},ij}$ taken as the input signal, see Figure 3. The chassis dynamometer control system takes care of the correct correlation between the drum speeds $v_{\text{drum},ij}$. Advantageously, this concept also enables the simulation of different wheel speeds that typically occur at μ -split conditions or while driving through bends.

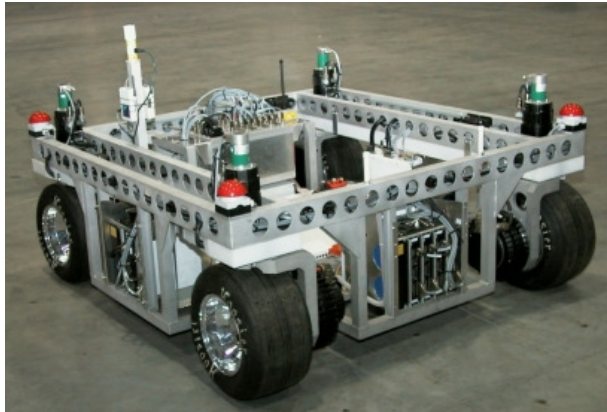


Figure 5: The moving base.

Moving bases

In order to emulate a vehicle motion relative to the VUT, the MB must be able to perform any arbitrary movement. The MB has been specifically designed for this purpose and features independent control of its position in the x and the y direction, as well as of its yaw angle ψ . Such maneuvering flexibility is accomplished through a vehicle platform equipped with independent all-wheel steering, and consequently independent all-wheel drive.

The objective of the trajectory controller of the MB is to realize a certain desired trajectory $\mathbf{x}_{\text{MB,ref}}(t) = [x_{\text{MB,ref}}(t) \ y_{\text{MB,ref}}(t) \ \psi_{\text{MB,ref}}(t)]^T$, i.e. position and orientation in the (x,y) plane parameterized with respect to time. To this end, the controller determines the drive torques and steering angles so as to minimize the difference between the actual and desired MB position.

Similar to the required dynamic performance of the chassis dynamometer also the dynamic response of the MB should correspond to the bandwidth of a normal passenger vehicle. 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. In addition, the MB should be capable of accelerating with 10 m/s^2 in order to simulate an emergency stop of the VUT. Finally, the top speed, which in view of the relative VEHIL world corresponds to the maximum speed difference Δv between two cars, should at least be equal to 50 km/h. These requirements are met by the MB, which is depicted in Figure 5 and further described in (10).

Applications for VEHIL

In VEHIL several types of ADASs can be tested, e.g. Adaptive Cruise Control, Stop & Go, Collision Warning and Avoidance Systems, Vehicle-to-Vehicle Communication (7), and PCS. But also fully Automatic Guided Vehicles for passenger or cargo transport can be investigated.

More specifically, VEHIL can be used for the design and validation of these ADASs in the following ways: development of the control algorithms in terms of the functional performance and driving comfort, sensor development, actuator development and fault management testing by injecting faults in the HILS.

Advantages and limitations of VEHIL

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

- Costs are reduced, because only one prototype vehicle is needed and no test drivers are required. Furthermore, a large number of tests can be performed in a short time frame.
- Test can be performed very safely, because no persons are physically present during the test and because of the absence of high absolute velocities.
- VEHIL provides the opportunity for quick and flexible variation of the desired traffic scenarios.
- Because the traffic environment is controlled from a simulation, tests can be performed accurately and in a reproducible way. All vehicle parameters can be easily monitored during the test. In this way it is possible to investigate the influence of specific parameters and failure modes, which can be injected to the VUT.

The possibilities for testing in VEHIL are limited by the testing area and the performance of the chassis dynamometer and MBs. Testing vision based systems and control systems that use the information from inertial sensors (e.g. lateral acceleration and yaw rate) is also limited to the extent to which these sensor signals can be reproduced. Furthermore, full-scale test drives will always be necessary to evaluate the system's performance on the road. But still, VEHIL provides a successful tool for the development of safety-critical ADASs, because it enables a better transition between simulations and test drives. This will be illustrated by the application of VEHIL for testing a PCS.

Application of VEHIL for validation of a PCS

As the VEHIL facility is not yet in operation, its feasibility will be demonstrated by a test with a vehicle equipped with a PCS in a preliminary VEHIL setup. A test vehicle is used as the VUT and positioned in the test area, equipped with a SICK laser sensor, a controller and a pre-crash seat belt pre-tensioner. This VEHIL test was performed without the chassis dynamometer, but with the rest of the VEHIL components, such as the MARS and the MB.

During the experiment the MB follows a crash trajectory, such that it is recognized by the laser scanner as a potential obstacle. When the controller estimates that a collision is imminent and unavoidable (taking conventional vehicle dynamics into account), it activates the belt pre-tensioner.

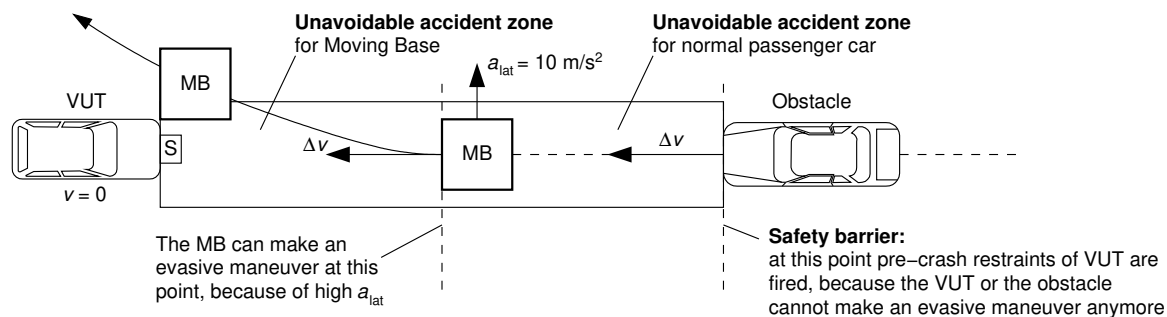


Figure 6: Testing a Pre-Crash System in a preliminary VEHIL setup.

However, an actual collision in this VEHIL setup is avoided, because the MB can achieve a much higher dynamic lateral acceleration than a normal passenger car, and is thus able to make an evasive manoeuvre at the latest moment. This test sequence is illustrated in Figure 6.

Further test results and movies of this VEHIL test are available at the project website (1). The first demonstration in the final VEHIL facility (due in November 2003) will focus on the validation of a PCS in a more complicated scenario. The simultaneously published paper on an integrated Design and Validation Environment (DVE) for PCS further describes the use of VEHIL as a tool in this DVE for testing sensors and actuators. In the next section we will consider the use of VEHIL for validation of fault management systems.

VALIDATION OF FAULT MANAGEMENT SYSTEMS

One of the current research objectives is to develop a methodology for validation of fault management systems of ADASs, such that errors in the processes of specification, design, development, and integration can be revealed in order to prevent hazardous consequences. Therefore, the possibilities for application of fault injection techniques in the VEHIL facility are investigated.

Identification of critical failure modes and scenarios

When the potential failure modes of the system have been identified, a suitable test coverage must be defined before testing the fault management system. 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 to deal with this problem is to take a *white-box* approach, where the system's internal states and their cause-and-effect relations are considered. Fault modeling may also be used to assist in the design of the test scheme. Efficient tests can then be devised to look at individual potential failures or at a combination of failure modes if it can be predicted in which way the system might fail, and by narrowing down the fault space of interest, using e.g. a *finite*

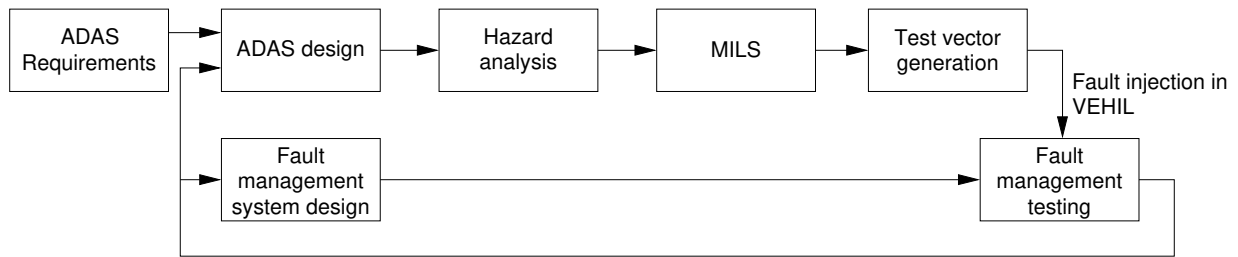


Figure 7: Process of validation of fault management systems using VEHIL.

state machine approach (14). It is then possible to reduce the number of necessary VEHIL tests, but still have sufficient test coverage for assessment of the system’s dependability.

In addition to the safety-critical failure modes, the critical operating scenarios must be identified, because certain faults may only evolve into failures under specific conditions. The most relevant combinations of scenarios and failure modes, in terms of criticality and frequency, can first be identified from hazard analyses and off-line simulations (MILS). The performance of the fault management system in response to these faults can then be assessed in the VEHIL facility by fault injection. This process is illustrated in Figure 7.

Fault injection in VEHIL

Fault injection covers a variety of techniques for inducing faults in systems to measure their response to those faults. In particular, it can be used in both hardware and software systems to measure the fault tolerance of the system. In VEHIL faults can be injected from the simulation environment and by physical injection, as shown in Figure 8.

Fault injection contributes to the dependability assessment of an ADAS in a number of ways. It can be used to assess the effectiveness of fault tolerance mechanisms built in the ADAS control system. Furthermore, fault injection may reveal potential failure modes that were not previously discovered. In VEHIL errors can be introduced in a controlled and reproducible way, which allows to determine the effect of a single fault or a combination of faults under specific conditions.

CONCLUSIONS AND FUTURE RESEARCH

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

- Preliminary tests show that the VEHIL concept is feasible and that it provides significant advantages for testing. VEHIL experiments can be performed quickly, safely, accurately, under near-realistic operating conditions, and at low cost. Initialization of a test sequence

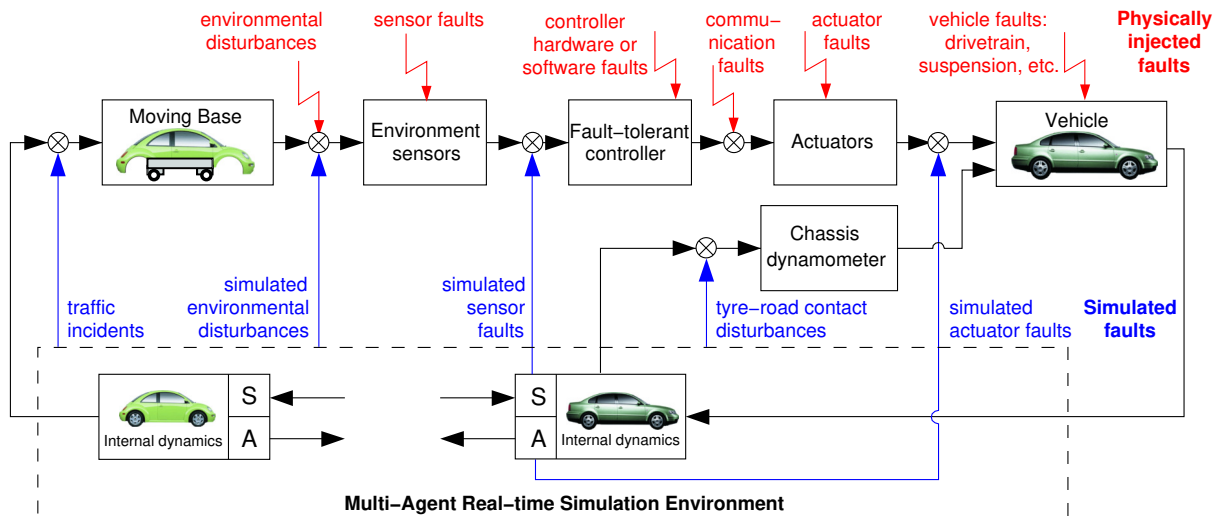


Figure 8: Validation of fault management systems by fault injection.

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.

- Within the development process of an ADAS, the VEHIL facility can provide the tool for efficient verification and validation of the performance of the ADAS control system. Reproducible experiments make it possible to isolate the performance of a single system parameter and thereby accurately determine the performance of specific characteristics.
- Especially the application of VEHIL for testing fault management systems has advantages, because of transparent techniques for fault injection and clear interpretation of test results. In VEHIL errors can be introduced in a controlled and reproducible way, which allows to determine the effect of a single fault or a combination of faults under specific conditions.
- Future research will focus on further development of the application of VEHIL for testing fault management systems. It is the objective to develop *test vectors* that capture the essential scenarios and failure modes in an efficient way. In this way the process in Figure 7 can be refined and applied for an efficient development of ADAS fault management systems using a white-box approach. This may form the basis for future *black-box* testing and certification of ADASs.

Acknowledgments

Research partially sponsored by TNO and TRAIL Research School.

REFERENCES

- (1) <http://www.automotive.tno.nl/smartsite.dws?id=1263>.
- (2) C. Hôte. Abstract interpretation techniques for software testing. *Business briefing: Global automotive manufacturing & technology*, pages 1–7, 2002.
- (3) R. Isermann. Modeling and design methodology for mechatronic systems. *IEEE/ASME Transactions on Mechatronics*, 1(1):16–28, Mar 1996.
- (4) R. Isermann, R. Schwarz, and S. Stölzl. Fault-tolerant drive-by-wire systems. *IEEE Control Systems Magazine*, 22(5):64–81, October 2002.
- (5) K. Labibes. An integrated design and validation environment for pre-crash sensing and collision avoidance system. In *Proc. of the 10th World Congress on Intelligent Transport Systems and Services (ITS)*, Madrid, Spain, 2003. Session PS 060, Paper 2731.
- (6) J.C. Laprie, editor. *Dependability: Basic Concepts and Terminology*. Springer, Vienna, Austria, 1992.
- (7) P. Morsink and O.J. Gietelink. Preliminary design of an application for CBLC in the CarTALK2000 project: Safe, comfortable and efficient driving based upon inter-vehicle communication. In *Proc. of the E-Safety Conference*, September 2002.
- (8) Z. Papp. HIL testing with virtual sensors. In *Proc. of the 10th World Congress on Intelligent Transport Systems and Services (ITS)*, Madrid, Spain, 2003. Session PS 093, Paper 2669.
- (9) Z. Papp and H.J. Hoeve. A multi-agent based modeling and execution framework for complex simulation, control and measuring tasks. *Proc. of the IEEE-IMTC*, pages 1561–1566, 2000.
- (10) J. Ploeg, A.C.M. van der Knaap, and D.J. Verburg. ATS/AGV, design, implementation and evaluation of a high performance AGV. In *Proc. of the IEEE Intelligent Vehicle Symposium (IV)*, Versailles, France, June 2002.
- (11) S. Poledna and G. Kroiss. TTP: Towards drive-by-wire. *Elektronik*, (14):36–43, 1999.
- (12) N. Storey. *Safety-Critical Computer Systems*. Addison Wesley Longman Ltd., Essex, U.K., 1996.
- (13) D.J. Verburg, A.C.M. van der Knaap, and J. Ploeg. VEHIL, developing and testing intelligent vehicles. In *Proc. of the IEEE Intelligent Vehicle Symposium (IV)*, Versailles, France, June 2002.
- (14) M. Yannakakis and D. Lee. Testing finite state machines: Fault detection. *Journal of Computer and System Sciences*, 50:209–227, 1995.