Chapter 18
Validation of Highly Automated Safe and Secure Systems

Michael Paulweber

18.1 Introduction

The increasing importance of advanced driver assistance systems is visible in the intensive development in this area of automotive OEMs as well as in research activities from nonautomotive companies. A well-known example of later activities is Google’s self-driving car project, which works successfully towards a fully automated vehicle.

The potential of advanced driver assistance systems to actively increase the safety of vehicles as well as the comfort of their passengers is currently discussed in many newspapers and reports in various TV programs. Therefore, it is likely that new passenger cars as well as heavy duty vehicles will be legally obliged to have certain Advanced Driver Assistance Systems (ADAS) installed in the coming next years. As a step in this direction, the EU has required new cars to be equipped with an Electronic Stability Program (ESP) from 2011 onwards. Five years later, in 2016, emergency braking assistant systems will be mandatory for new heavy duty vehicles in the European Union.

The OEMs have actively taken on this trend and equip new vehicle models with more and more advanced driver assistant systems. This development is driven by two main societal challenges: The increasing age of the population, especially in the western countries, and the continuing growth of the population on earth.

Mobility is one of the biggest values of the western countries. This can be seen in the fact that many families, after buying a house or an apartment for living, spend the second largest amount of money on vehicles. As people get older, they want to keep the personal mobility they have been used to all their life. In order to keep the trend of fatalities decreasing, it is necessary to support elderly people when driving
cars even at age of 80 and older. Without advanced driver assistance systems, elderly people have to stop driving or have an increased risk of fatal accidents. A statistics from [1] shows this trend, which can be reversed by the use of advanced driver assistant systems.

The growing global population makes space for one of the most precious goods especially in megacities such as London, Beijing, or New York. Traffic jams are normal in those cities. They do not only annoy the drivers but also increase the CO₂ and exhaust emissions, which contribute to global warming. As it is nearly impossible to build more or bigger streets in those cities, the only alternatives are public transportation or taking better advantage of the available space of existing streets for the personal mobility. Semi-automated vehicles which know where to park a car as well as jam pilots are first steps to keep personal mobility attractive also under the difficult environmental conditions of megacities. Vehicle-to-vehicle and/or infrastructure communication as well as the usage of map data allow to find energy optimal control schemes for vehicles, which can be implemented in (partially) automated vehicles. This can reduce the CO₂ emissions in the transport sector (especially in the transportation of goods using heavy duty trucks) significantly.

This indicates that the introduction of new and more sophisticated advanced driver assistant system up to fully automated vehicles will continue.

Depending on the degree of automation provided by ADAS, it partially or completely takes over the control of the transversal and/or longitudinal vehicle movement in many different situations, which may occur in the traffic environment. This requires the correct and reproducible reaction of those ADAS in all possible traffic scenarios, which might occur. Therefore, the validation of ADAS is already very complex and will get even more complicated when the degree of automation of the vehicles will continue to increase. Today, there are no test systems and validation methods available, which can guarantee the complete functional safety under all possibly traffic and environmental conditions. Current validation methods use catalogues of test scenarios, which define the traffic scenario as well as the expected correct reaction of the ADAS in this situation [2]. OEMs test vehicles with ADAS functions use scenarios of the catalogues either in proving grounds, in real traffic situations, or more and more in virtual (simulated) environments.

Testing on proving grounds or in real traffic does not require sophisticated simulation environments and is therefore often used at early functional prototypes of new ADAS or in partially or highly automated vehicles (in the remaining part of this chapter, ADAS shall also include the control systems of partially, highly, or fully automated vehicles). Unfortunately, those testing methods have severe drawbacks: Tests are difficult to reproduce. Therefore, it takes long testing times to check, if corrections in ADAS functions really solved identified problems of previous tests. Many traffic scenarios of the validation databases are difficult to reproduce or even dangerous for the test driver to execute. This also contributes to the high validation costs and long validation duration.

The development of simulation environments for validation in virtual traffic scenarios on the other hand is also very costly. A prominent company developing advanced driver assistant functions predicts the effort to develop validation
environments for highly automated vehicles 10–20 times higher than the effort to develop the vehicle automation function to be validated. The ratio increases for fully automated vehicles to 20–50 times higher.

This chapter tries to summarize the most promising upcoming trends in the validation of advanced driver assistant systems [2].

### 18.2 Complexity of Automated Vehicles

ADAS controllers offer unprecedented values to the drivers of vehicles: ADAS were initially introduced to improve the safety of vehicles (active safety measures compared to previously passive safety measures). But they also increase the comfort in releasing the driver from stressful situations such as driving in traffic jam. Additionally, they are used to decrease the negative impact of vehicles to the environment (e.g., traffic light assistant minimizes the energy consumption and exhaust emissions in optimizing the vehicle speed depending on the current and future status of the upcoming traffic signals on the route of the vehicle).

Figure 18.1 depicts the basic structure of ADAS. Contrary to conventional control units in automotive vehicles such as engine control units (ECU) or battery control units (BCU), ADAS control units (ACU) communicate with a significantly more complex environment using sensors which are new in the automotive industry.

Many of these sensors provide information about the outside world in object lists updated periodically (video sensors, radar sensors, LiDAR sensors, ultrasonic sensors). Vehicle-to-vehicle communication as well as vehicle-to-infrastructure communication also sends information about the environment around the vehicle. A third source of information for ADAS controllers is the information of accurate

![Fig. 18.1 Structure of ADAS](image-url)
maps together with GPS sensors. All these information together with classical online data in vehicles, e.g., engine speed, velocity, gear number, etc., are used to get an image of the world surrounding the car as accurate as possible.

Unfortunately, all these information sources have their insufficiencies. Therefore, sensor fusion is used to combine the information of various sources and improve the image of the outside environment. This sensor fusion increases the complexity of these systems significantly, as it requires the synchronized acquisition of data from many sensors to test or to reproduce the result of sensor fusion and the calculations in ADAS controllers.

The physical signals are in most cases already preprocessed in the sensor data acquisition subsystems and periodically sent to the sensor fusion algorithms. The results of the sensor fusion are used to generate an image (position, velocity, type of object, etc.) of the outside objects at the current instance of time as well as a projection into the future. The next step is the calculation of an optimal trajectory for the vehicle in order to fulfill the requested mission (e.g., driving from point A to point B or parking the car in a parking space). The controllers for the lateral and longitudinal movements of the vehicle calculate the set value for the various actuators in the vehicle as steering actuator, throttle value, brake pressure, etc.

The control strategies of ADAS controllers have to interact with many conventional cars around the vehicle which is steered by the ADAS (ego-vehicle), as well as with human beings, animals, and other objects such as traffic signs, road borders, stones, or objects flying in the wind.

Additionally, the accuracy and trustworthiness of the different ADAS sensors are heavily influenced by the environmental conditions (like rain, snow, fog, night, glaring sun light, etc.). These effects need to be simulated in virtual environments for validation of ADAS too.

An additional difficulty with ADAS are the increasing threads of security breaches from vehicle-to-vehicle or vehicle-to-infrastructure communication. Vehicles with ADAS, for example highly automated cars, have to be safe under every environmental condition. This requires sophisticated ADAS control algorithms as well as extensive validation of these systems.

### 18.3 Validation Challenges

Vehicles equipped with ADAS reach an unprecedented complexity. This has various reasons:

- There are a lot of new sensors such as video sensors, radar sensors, LiDAR sensors, ultrasonic sensors, vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication, GPS sensors, data from digital maps, etc. Many of these sensors are intelligent subsystems, which have significant data processing capabilities built in. Validation systems have to cope with streams of object lists generated by these sensors.
• As all of the new sensors have their weaknesses, sensor fusion is needed to create an image of the outside world. This image includes information about surrounding objects as well as their most likely future trajectories, which has two impacts on validation: it is necessary to either simulate all sensors or stimulate them simultaneously. Especially, if applying physical signals to the sensors of the ADAS via stimulators, which are directly connected to data from an online simulation of the surrounding environment, all time delays of these different actuators have to be compensated. Otherwise, the sensor fusion algorithms might lead to wrong results as the data from the different sensors are not exactly time aligned.

• ADAS equipped vehicles interact with the external world. Other vehicles driven by human drivers change their trajectory based on the reaction of the ADAS automated vehicle (e.g., whether it brakes rapidly at a road crossing or it smoothly decelerates and stops). Therefore, it is necessary to take also different behaviors of human actors into account when validating ADAS.

• Weather conditions heavily change the behavior of ADAS sensors. This requires tests under many different environmental conditions.

• Vehicle security has to be tested too, as security breaches may lead to wrong images of the outside world, which creates unwanted trajectories and might even result in accidents.

Vehicles equipped with ADAS functionalities (e.g., fully automated cars) have to be safe under uncountable environmental conditions and scenarios. Therefore, most of the validation of automated research vehicles is currently done on the road. Prof. Winner from the Technical University in Darmstadt, for instance, estimated the distance that needs to be tested with validation vehicles on German roads in order to prove that an automated vehicle is as safe as a manual driven car [3]. The calculated distance of 100 million km takes into account the average number of fatal accidents on German more than roads and the average driving performance on these roads. Considering that OEMs develop up to 25 different variants of one vehicle model and the fact that complex software systems, such as ADAS, typically have a new software version update every few months, very large test vehicle fleets would be required. Even if not all variants have different ADAS software, some modifications will lead to additional validation effort. The test vehicles would have to perform more than 100 million km testing several times a year.

When trying to perform validation road testing in short periods of time, it is difficult to ensure that almost all possible environmental conditions (hot, cold, low or high altitude, snow, rain, fog, ice, etc.) occur within this time frame. Additionally, many validation sequences require dangerous maneuvers, which are safety critical to test drivers piloting vehicles with new ADAS versions. Also costs of the additional objects (other vehicles, test robots, etc.) needed to validate ADAS systems in different scenarios are significant.

The replacement of pure road testing by validation in a virtual environment can reduce the validation time significantly, if eliminating those portions of test time on the road, where no safety relevant events occur, in the tests executed in the simulated
environments. Currently, several projects deal with the collection of databases of safety relevant scenarios for the validation of ADAS-based vehicles with many control units as transmission control unit (TCU), vehicle control unit (VCU), engine control unit (ECU), and many more.

In order to cope with the unrealistic required test time on roads discussed so far, it is common agreement that validation of ADAS require testing in simulated environments (see Fig. 18.2), which allow to perform testing faster than wall clock time and provide the possibility to stimulate different environmental conditions during the validation sequences. Currently, the required complex simulation models, which can simulate realistically “all” safety critical traffic and environment scenarios for ADAS equipped vehicles, do not yet adequately exist.

In order to get a better understanding if validation in a virtual environment can solve the problem, the following rough calculation is done:

- Road testing: The duration to perform 100 million km road testing with 100 test vehicles assuming 18 hours per day driving lead to a test duration of 8 years
- Virtual environment testing: Assuming testing of 300 safety relevant scenarios on 25 test beds under all combinations of environmental conditions will lead to test duration of 2 years (see Fig. 18.3)

This indicates that validation in a simulated environment is clearly a way to investigate in more detail; nevertheless, 2 years of testing is too long to perform validations for several variants of vehicles and several new ADAS software versions per year. The validation of highly automated systems is therefore still an unsolved
Fig. 18.3 Rough estimation of duration of validation in virtual environment

| Test duration per safety relevant scenario | 5 min |
| Number of safety relevant validation scenarios | 300 scenarios |
| Number of virtual validation testbeds used | 25 testbeds |
| Number of testing hours per day | 18 h |

| Number of variations of environmental conditions |
| # of vehicle variants | 1 variants |
| Clear / Rain / Snow | 3 variations |
| No fog / Fog | 3 variations |
| Day / night | 3 variations |
| warm / cold | 3 variations |
| low altitude / high altitude | 3 variations |
| Driver type | 3 variations |
| heavy traffic / low traffic | 3 variations |
| Low GPS reception | 2 variations |
| Vehicle load | 3 variations |

| Number of scenarios under different env. conditions | 3,936,600 scenarios |
| Time to test all scenarios in all conditions | 2.0 years |

problem; the “state-of-the-art” validation methods and tools are not sufficient anymore.

Safety means the absence of unacceptable or unreasonable risk. Validation is the activity to determine that the requirements are the right requirements and that they are complete. Verification checks ensure that a developed systems fulfills all defined requirements. Therefore, it is necessary to foresee all potential dangerous situations during the requirement phase of a new product. As ADAS heavily interact with the outside world, an uncountable number of safety critical situations can occur. It is very likely that many of them are not foreseen at specification time of a new system. Therefore, the most difficult validation challenge in highly automated vehicles is the functional insufficiency [4]. It results from unknown requirements, which are consequently neither implemented nor verified. As validation shall ensure that all relevant requirements are foreseen, it is necessary to think about concepts to handle functional insufficiencies.
18.4 Validation Concepts

In order to reduce the validation time even further, concepts from combinatorial testing together with validation in a virtual environment should be applied. This leads to the validation tool chain depicted in Fig. 18.4.

Validation scenarios derived from several sources:

- Test vehicles record data from ADAS sensors, environment and road data, and vehicle data (e.g., engine speed, vehicle velocity). These data are then analyzed and checked whether safety critical events occurred and whether these events are already part of a data base of safety critical ADAS scenarios. If it is not already existent, a new validation scenario is generated from the recorded data and added to the data base.
- Scenarios defined from official bodies (e.g., consumer organizations as EURO-NCAP) are also added to the data base of safety critical ADAS scenarios.
- Safety analysis of ADAS will also lead to additional validation scenarios.

Especially the first source, which derives validation scenarios from data recorded on the road, allows to create a learning cycle over time, which helps to overcome the problem of functional insufficiency. It is thinkable to extend this learning cycle also over data recorded during operation of ADAS equipped vehicles as long as the buyers of those vehicle agree to this procedure.

Fig. 18.4 Validation tool chain for ADAS equipped vehicles
The test infrastructure components in Fig. 18.5 allow to set up ADAS validation environment to reduce the validation time to a reasonable length. In order to allow the use of combinatorial testing concepts, all ADAS scenarios need the possibility to execute them in different combinations of environmental conditions. They are described by different sets of values of the scenario parameters as amount of rain (0–100%), fog (0–100%), daylight (0–100%), etc. All ADAS scenarios contain a test maneuver sequence with external inputs for the scenario parameters and a procedure to calculate, if an executed validation scenario has successfully passed.

When preparing the test sequence for the validation, those ADAS validation scenarios are taken from the ADAS scenario database, which are relevant for the ADAS function to be validated. An intelligent test generator based on methods of design of experiments (e.g., combinatorial testing methods as described in [5]) defines a set of values for the scenario parameters used during the execution of the scenario. Not all scenarios are tested with all possible combinations of scenario parameters. This reduces the number of necessary tests significantly.

In order to execute the test sequences, simulation models for the non-existing components of the ADAS equipped vehicle and the outside environment are needed. They are taken from the data base of environment models. The environment model components can also have the additional scenario parameter inputs (similar to the scenario sequences).

The last step to reduce the validation effort is the reuse of test sequences in different steps of the development V-process. This requires, on the one hand, a standardized scenario sequence description and, on the other hand, a simulation environment, which always provides the same functionality in combination with the unit under test components available in reality. The standardized scenario description language can be based on well-established standards as ASAM-ODX.
Fig. 18.6 HIL (HW in the loop) validation environment

[6] or Open Scenario [7], which will require extensions to cover the needs of ADAS validation.

The test sequences are reused during the development process:

- In MIL (model in the loop) environment during functional development in early phases of the V-model (see Fig. 18.2)
- In SIL (software in the loop) environment during ADAS software development in early phases of the V-model (see Fig. 18.2) MIL (Model in the loop) or SIL (Software in the loop) validation environment
- In HIL (hardware in the loop) environment during ADAS development in early phases of the V-model (see Fig. 18.6)
- In power in the loop (xIL) environment during ADAS vehicle integration and validation in early phases of the V-model (see Fig. 18.7)
- Potentially also in vehicle in the loop (VIL) environment during vehicle validation when using remotely controllable platforms as described in [8].

18.5 Virtual Validation Environment

The accelerated validation procedure described in the previous chapter requires a complex simulation environment. It combines real components with simulated components in different variations. The real components shall be equivalent in the behavior of the simulated components functionally as well as in its timing behavior.
Fig. 18.7 PIL (Power in the loop) validation environment

| Component                                 | Testbed type | MIL (Model in the loop) | SIL Software in the loop | HIL HW in the loop | xIL (Powertrain in the loop) | Proving ground | Road |
|------------------------------------------|--------------|-------------------------|--------------------------|-------------------|----------------------------|----------------|------|
| Vehicle                                  | Simulated    | Simulated               | Simulated                | Simulated         | Real                       | Real           |    |
| Powertrain                               | Simulated    | Simulated               | Real                     | Real              | Real                       | Real           |    |
| Driver                                   | Simulated    | Simulated               | Simulated                | Simulated         | Real                       | Real           |    |
| Stimuli needed                           | no           | no                      | yes / no                 | yes / no          | no                         | no             |    |
| Sensors                                  | Simulated    | Simulated               | Real / Simulated         | Real / Simulated  | Real                       | Real           |    |
| Sensor fusion                            | Simulated    | Real                    | Real                     | Real              | Real                       | Real           |    |
| Trajectory building                      | Simulated    | Real                    | Real                     | Real              | Real                       | Real           |    |
| Controllers                              | Simulated    | Real                    | Real                     | Real              | Real                       | Real           |    |
| Actuators                                | Simulated    | Simulated               | Real / Simulated         | Real / Simulated  | Real                       | Real           |    |
| Road                                     | Simulated    | Simulated               | Simulated                | Simulated         | Real                       | Real           |    |
| Traffic and environment objects (pedestrians etc.) | Simulated    | Simulated               | Simulated                | Real / Simulated  | Real                       | Real           |    |
| Environmental conditions (rain, snow, fog, night, ice, etc.) | Simulated    | Simulated               | Simulated                | Simulated         | Simulated                  | Simulated      | Real |

Fig. 18.8 Simulated/real components in ADAS validation environments

Figure 18.8 shows the combination of real, simulated, and emulated objects, which are used at the different test bed types described above. The table also
indicates where a conversion from simulated values to real physical quantities such as ultrasonic signal reflections, torque, GPS satellite signals, etc., exists. These connectors between the simulated world and the real world are called stimuli. They have to introduce energy into the real world according to the current values in the simulated world. An example are GPS coordinates indicating the current position of a simulated world driving on a simulated road via simulated satellites. Navigation units in vehicles but also on mobile phones can receive these emulated satellite signals and show the correct position of the simulated vehicle when using navigation software packages.

ADAS validation systems can need the following stimuli:

- Ultrasonic stimuli, which send the reflection of an ultrasonic signal from a parking sensor back according to the distance to objects next to the ego-vehicle and according to the current situation in the simulated virtual world
- Radar stimuli: same function as ultrasonic stimuli for radar sensors. This stimuli are very difficult to build and currently not adequately available
- LiDAR stimulus
- Video camera stimuli, which show video cameras of ADAS equipped vehicle the image of the currently surrounding environment via replayed or artificially created video sequences on video screens
- GPS stimulus, which convert simulated GPS coordinates in a simulated environment to HF signal, which an antenna of a navigation system would receive from one or several GPS satellites.
- Vehicle-to-infrastructure and vehicle-to-vehicle communication stimuli, which simulate the communication between ego-vehicle and infrastructure control center and surrounding vehicles
- Torque stimulus as used in powertrain test beds
- Steering system stimulus, which emulates the mechanical feedback from the wheels on the road to the steering system sensor of a vehicle even if the wheel is not turning (either on a chassis dyno test bed or a powertrain test bed)
- Climatic stimulus (climatic chamber)

Stimuli need to ensure that the simulated output of a component matches the real measureable input of a physical component. Therefore, a lot of energy is needed in many cases to minimize the control error of a stimulus.

The connection between different simulated components requires a co-simulation framework, the combination of different simulated and real components needs a special co-simulation framework which is for example described in [9]. In order to mix and match the vehicle components, the environmental components, and the components to build ADAS controller and the driver models, it is necessary to define several interfaces:

- Inputs and outputs of real/simulation components. They connect the outputs of simulated components with the inputs of other simulated components. In case of a connection to a real component, a stimulus is needed in between the output of the simulated components and the physical input of the real component.
Fig. 18.9 Validation simulation environment

- Inputs of scenario parameters. Scenario parameters are changed at the beginning of a test scenario, but stay unchanged during the test sequence of the scenario. Also stimuli must react to scenario parameters (e.g., modification of a video image in case a scenario is tested in simulated rain).

In order to allow also ADAS function development on MIL systems, the main function blocks of ADAS are also needed as simulation components (e.g., sensor fusion block). Figure 18.9 shows these main building blocks in a simulated environment. It also indicates that the simulated ego-vehicle model interacts with the traffic and environment simulation (outside upper gray connection between left and right side of the figure).

The last validation building block is an executor of the test sequence. It is of advantage, if the test sequence is stored in a standardized format, which allows easily to reuse test sequences in different phases of the development process of ADAS. This saves significant costs as the creation of validation environments, and test sequences is 5–25 times more expensive than the development of the ADAS function itself.

18.6 Conclusion

This chapter presented a summary of the challenges to validate the functionality and especially the safety of ADAS for vehicles. It explained why new approaches are required to allow the validation of ADAS in reasonable time frames and at
reasonable costs. Only then it is possible to achieve the full potential of ADAS and consequently to ensure personal mobility to ageing society and a reduction of CO₂ and exhaust emission of traffic at a growing population. In transport, automated vehicles offer an excellent solution to meet the societal challenges due to their capability to increase safety by avoiding human errors, to improve efficiency by better usage of road space, and especially to significantly reduce emissions in mobility applications. In addition, automated driving can also enable handicapped or elderly people to participate in social life self-determined.

References

1. J. Oxley, B. Fildes, E. Ihsen, J. Charlton, R. Day, Differences in traffic judgements between young and old pedestrians, Accid. Anal. Prev. 26–29(6), 839–847 (1997)
2. H. Winner, S. Hakuli, G. Wolf, *Handbuch Fahrerassistenzsysteme: Grundlagen, Komponenten und Systeme für aktive Sicherheit und Komfort* (Vieweg+Teubner, Wiesbaden, 2011)
3. H. Winner, W. Wachenfeld, Absicherung automatischen Fahrens, in *6.FAS Tagung*, Munich, Germany, 2013
4. Müller, Bernd; Robert Bosch AG, Challenges in Demonstrating Safety for Highly Automated Systems, in *Safetrans Industrial Day 2015*, Renningen, 2015
5. L. Yu, Y. Lei, N. Kacker, R. Kuhn, ACTS: A Combinatorial Test Generation Tool, in *IEEE 6th International Conference on Software Verification and Validation*, Neumunster Abbey, Luxembourg, 2013
6. A. eV, ASAM Connects—Standard Details, ASAM eV, May 2015, [Online] http://www.asam.net/nc/home/standards/standard-detail.html?tx_rwbmasamstandards_pi1%5BshowUid%5D=525. Accessed 10 08 2015
7. V.S. GmbH, OPen Scenario Bringing Content to the Road, VIERES Simulationstechnologie GmbH (2015), [Online] http://www.openscenario.org/. Accessed 10 08 2015
8. M. Schmidl, H. Steffan, ADAS Testing with UFO Test System, in *Autonomous Vehicle Test & Development 2015*, Stuttgart, 2015
9. G. Stettinger, J. Zehetner, H. Kokal, M. Paulweber, M. Wierse, B. Toye, Control of an Engine Test-Bench via Hardware-Software-Co-Simulation, in *14.Internationales Stuttgarter Symposium Automobil- und Motorentechnik*, Stuttgart, 2014