Challenges and Approaches for Testing of Highly Automated Vehicles

Conference Paper · December 2014

DOI: 10.1007/978-3-319-19818-7_11

CITATIONS
15

READS
650

1 author:

Hans-Peter Schoener
"Insight from Outside" - Consulting
66 PUBLICATIONS **296** CITATIONS

SEE PROFILE

Challenges and Approaches for Testing of Highly Automated Vehicles

Dr. Hans-Peter Schöner

Daimler AG, D-71059 Sindelfingen

Abstract: Testing of highly automated vehicles has new challenges with respect to the questions to answer, the test cases, and the testing procedures. Main questions arise from the fact that highly automated vehicles are required to achieve high levels of availability and effectiveness of the vehicle functions; after all, their performance has to be compared to the performance of human drivers. Testing of such vehicles requires international consensus on the required level of safety and on the metrics to be applied. The main challenges for such testing are discussed and some new approaches are presented.

Keywords: Testing, highly automated vehicles, simulation

1. Towards highly automated vehicles (HAV)

In the past years, several companies and institutions have shown quite well functioning technologies for detecting the environment, algorithms for path planning and collision avoidance. On the other hand, more and more semi-automated functions are readily available in vehicles in the market place, like adaptive cruise control and lane keeping. These functions take over tasks which traditionally have been done by the driver. The driver's task is reduced to judging when to turn the system on and off, and to monitoring constantly whether the current conditions are still adequate for the function to work; but he also has to serve as a fall-back solution, when the system by itself judges that it can no longer safely manage the situation.

It seems a very small step to release the driver completely out of the vehicle control loop, at least temporarily during boring driving conditions, be it during a traffic jam or for continued constant speed driving on long journeys. But on closer inspection, this step entails considerable challenges.

2. Specific challenges of HAV

In case of a take-over request in a semi-automated vehicle, the driver is required to take over vehicle control more or less instantaneously. If the driver is out of the loop in a highly automated vehicle, response times will be longer in average. Although in simulator experiments drivers respond very fast on intense take-over signals (like a warning sound with simultaneous brake impulse), response times of several seconds have to be considered in designing highly automated vehicles. This requires that any complicated traffic situation and any emergency situation during continuous highly automated driving must be handled by the vehicle itself, at least for the duration of this take-over time. 99% is definitively not enough! Testing of highly automated vehicles means to prove that the vehicle can handle any driving situation in a sufficiently safe way by itself. In other words:

Before a highly automated vehicle will drive you anywhere, it has to prove that it does not drive you into trouble.

3. Safety benchmark for HAV

A new technology generally does only make sense, if it is safer than the state of the art. For highway driving, which will be one of the first steps towards highly automated driving, the accident statistics is a quite clear benchmark. Table 1 shows the accident rates on the "Autobahn" in Germany for the 4 severity levels S0 (material damage only) to S3 (persons killed) [1]. Highly automated vehicles should not increase this accident rate, but rather help in reducing those rates to even smaller values.

4. Safety assessment of HAV

When it comes to testing for very small occurrence rates, there is the general problem that a straight forward approach based on statistical analysis of the complete system would lead to extremely high and thus impracticable testing efforts [2]. Other systems with very high reliability requirements (aircraft control systems [3],

electrical power distribution systems, etc.) are designed and certified by a functional analysis approach, essentially comprising the following steps:

- system design for fault tolerance (with self-monitoring and redundant subsystems),
- logical modelling of the fault tree of the complete system in order to calculate the failure rate from better known subsystems,
- verifying the failure rates of components,
- avoiding and assessing common mode failures of redundant functional subsystems.

This allows calculating reliability and safety of the complete system based on the proven properties of the subsystems, which are verified in component and subsystem tests. In the final stages, the complete system is tested especially in order to verify the assumptions with respect to functional redundancy, single failure detection and common mode failure rejection.

Understanding the driving task as a safety system and using analogous methods for functional analysis allows assessing the safety of highly automated vehicles.

Table 1: Accident rates on freeways in Germany [1]

Severity level	Average distance between two accidents of this level	Accident rate (probability of accident per km driven)
S3	$660 \cdot 10^6$ km	$1.52 \cdot 10^{-9}$/km
S2	$53.2 \cdot 10^6$ km	$1.88 \cdot 10^{-8}$/km
S1	$12.5 \cdot 10^6$ km	$8.00 \cdot 10^{-8}$/km
S0	$7.5 \cdot 10^6$ km	$1.33 \cdot 10^{-7}$/km

5. Accident types and testing approaches

One important step in a functional analysis of the driving task is looking at the reasons for accidents. There are several categories which lead to significantly different testing and verification tasks.

5.1 Failure of components

Assessing the failure of components is well known in automotive industry. According to ISO 26262, ASIL (automotive safety integrity level) classes are defined which are required for certain critical parts. Typically failure rates between 10^{-8}/h and 10^{-7}/h are required for crucial systems. At a highway driving speed of 100 km/h this translates to distance related failure rates between 10^{-10}/km and 10^{-9}/km.

Designing components for this safety level is appropriate for the expected safety requirement level according to chapter 3. There will be more components necessary with high ASIL requirements than before.

Some critical functions, such as keeping the lane after a substantial component failure, have to be designed at least for slow degradation; after the take-over time (which is an important design parameter for this purpose) the driver will have the task to bring the vehicle to a safe stop, as he has to do with conventional vehicles for similar rare, but critical cases.

Testing and verification of components does not ask for new methods. It has to verify the environmental robustness, has to inject failures to check functional redundancy, verify common cause failure rejection – to name some typical tasks.

5.2 Behaviour-dependant accidents

Inattentiveness, sleepiness, distraction are reasons for many accidents with human drivers. Such reasons will be surely avoided by highly automated vehicles. Inadequate speed, leaving the lane unintentionally and other accidents without outer influences are other candidates for significant reductions in highway accidents.

However, also highly automated vehicles have to detect the environment in order to act adequately in all cases. This includes knowing rules like speed limits, warning traffic signs (e.g. construction sites), but also weather conditions. Most of this information can be detected on the fly by sensors, but also by using previous knowledge (from maps or maintained online data bases, serving as an additional independent detection channel) the detection rate can be significantly increased.

Testing for avoidance of behaviour-dependant accidents has to verify the detection ability for rules – through at least one channel – and the adaptation to the rules. Reliabilities in all single channels have to be assessed and an overall detection and adaptation rate has to be derived.

5.3 Deficiencies in environment sensing

Road, traffic and environment conditions have to be monitored constantly for safe driving. Detecting lane markings, seeing all relevant other traffic participants or other relevant objects and knowing the exact position of the vehicle with respect to a knowledge base (map) are crucial. Weather and light conditions have to be checked continuously, in order to assess whether highly automated driving is still adequate or must be suspended, i.e. the driving task should be handed over to the driver. For this end, a measure gauging the overall quality of the environment sensing should be established.

From system design aspects it is quite clear that environment sensing has to be done with several functionally redundant and technologically diverse sensors. The functional deficiencies of the different sensors have to be verified not only with respect to the failure rates, but also for common causes. As in many other safety systems, the relatively high failure rate of a single sensor allows for much shorter testing time than verifying the failure rate of the combined system in one step.

For testing of environment sensing, driving around in the world in order to experience many different environmental conditions (lighting, weather, locally different infrastructure, traffic conditions) is indispensable. Many of those conditions have been seen before during testing of semi-automated driving functions; thus typical detection rates of different sensor types are already known. From these values it can be deduced that a testing distance of around 500,000 km should be enough to both verify the sensing failure rates of the single sensors and to validate the acceptable rate of common causes.

5.4 Deficiencies in control algorithms

The knowledge of the environment, as detected from the sensors, has to be analysed and interpreted by algorithms in order to understand the situation and to deduce appropriate control actions. The algorithms have to cope with a multitude of different complex and critical situations. In contrast to environment detection, such situations can be simulated and don't need to be tested in real world. However, a sufficient set of real world benchmark test have to be performed under the same test conditions in order to validate the computer simulations.

Since there is a vast number of possible situations as input for the control algorithms, smart methods to search and find critical situations have to be established. As for the environment sensing, a measure gauging continuously the overall quality of the situation understanding (especially with respect to criticality awareness) and of the resulting control output must be established as well.

Prerequisite of a complete testing of algorithms is a good modelling of the sensor output generated by the combined sensor set. This model needs to reproduce the sensor output with respect to key performance indicators, like timing or stability of object tracking. These parameters of the sensor model should be taken from sensor signal monitoring during real world tests (see chapter 5.3). The sensor model has to allow for specific fault simulation, according to failure injection of component tests.

5.5 Faulty driver and vehicle interaction

Finally, there is a further reason for accidents, which had been dubbed "mode confusion" in the early days of autopilots in aircraft. It has to be guaranteed that both vehicle and driver are always aware of who controls the vehicle. Faulty commanding of an automated system by a human operator must be avoided by sufficient plausibility checks within the system. A badly designed user interface can cause a new reason for accidents, which has to be avoided and verified.

For testing the user interface, driving simulator test are adequate, especially to check hand-over situations, and prove that the driver understands vehicle interaction even in critical situations.

6. Driving risk scenario

For the assessment of operational safety of automated driving, a risk scenario consisting of a complete set of traffic situations must be evaluated; these situations in total should represent any relevant condition a vehicle may experience during automatic driving. For each type of traffic situation the exposure value (how often does this situation occur) and the severity of accident (if it occurs from this situation) is estimated. Completeness should be assessed based upon the knowledge about reasons for accidents as mentioned in chapter 5; situations with a (in comparison to other accident situations) negligible product of exposure and severity are irrelevant and can be omitted. Table 2 shows a list of situation categories and some examples.

Table 2: Categories of traffic situations in a risk scenario, with examples for situation, exposure and severity, here for simplicity on a scale from 1 to 3

Category	**Example:** Situation	Exposure	Severity
continuous control	keep vehicle in the lane, for any curve radius	3	3
predictable end of automated driving	planned exit of highway	3	1
obstacles on the road	sudden evasive manoeuver of vehicle ahead	2	3
unexpected infrastructure deficits	lane marking not obvious	3	3
traffic partner behaves "against the rules "	vehicle ahead drives too fast	3	1
weather-related challenges	sudden glare from sun	3	3
driver related misbehaviour	driver not ready for take-over	2	2
Hardware problems	complete sensor failure	1	3

This situation scenario should be generic for any vehicle, be it automated or driven by a human driver. It describes the driving risk scenario for the vehicles.

7. Controllability

Controllability of the situation by the driver (or by a HAV, respectively) is a measure for how probably this situation in the risk scenario will lead to an accident. Some traffic situations are not easy to judge whether they are controllable or not. Examples are the lost cargo which falls from a truck just ahead, or the wrong-way driver which appears in opposite direction. In such situations human drivers and HAV face the same problem, because some physical limitations cannot be overcome.

Human ability to avoid accidents in a specific situation can be tested in a driving simulator. Fig. 1 [4] shows how a criticality parameter (time to collision, TTC, at first sight of an obstacle in the lane) influences the ability to avoid an accident for a group of drivers, and how this can be improved by a warning system or by autonomous braking. A similar experiment can be made with highly automated vehicles on a test track, measuring the ability to avoid the accident statistically. This method can prove that highly automated vehicles can control a given situation better or at least as well as most human drivers, even if they cannot avoid an accident completely.

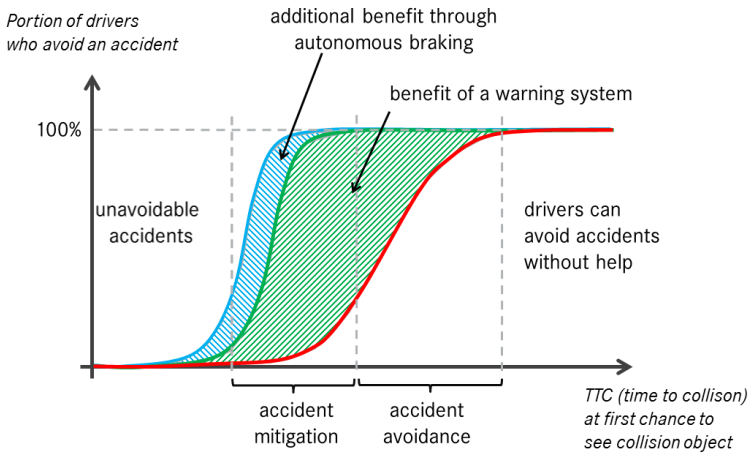

Figure 1: Controllability of a collision situation [4]

Controllability can be divided into the two steps “ability of detection” and “ability of reaction” for critical situations. This concept can help in better understanding and eliminating the deficits if controllability fails in an early design phase.

Each situation of the driving risk scenario contributes with its product of exposure E, severity S and controllability C to the overall risk R of driving: $R = \Sigma \{ E \cdot S \cdot (1-C) \}$. This allows comparing the total risk of highly automated driving with the well-known statistical risk of human driving.

8. Establishing testing standards

On national level and on the EU level, several projects will help to establish standards in testing. These projects are needed to establish a “state of the art” for verification of reliability and validation of safety of highly automated vehicles.

8.1 How safe is safe enough ?

In Germany, the project "PEGASUS" (Project for establishing generally accepted scenarios and simulation methods for highly automated, cooperative vehicle functions) is in preparation, in order to define the set of traffic situations which defines the risk scenario. This should be the base for a generally accepted method to assess the safety of highly automated vehicles. The project should also define methods to measure the controllability of the different traffic situations. For situations with unavoidable accidents the project will define thresholds for a sufficiently high controllability level.

8.2 How to validate the safety requirements ?

"AdaptIVe - Response 4" focusses on the safety validation and technical system limits as well as on legal aspects for the introduction of automated driving.

8.3. How to measure and test efficiently ?

Other projects are in preparation,aiming at improving testing methods and testing automation for highly automated vehicles.

9. Conclusion

This paper describes the outline of a concept for safety assessment and testing approaches for highly automated vehicles. The work on the details of this method is still ongoing, but validated and generally accepted methods for safety assessment of highly automated vehicles will be defined within the next coming years. A world-wide consensus on such methods and testing procedures needs to be established.

The author thanks his colleagues for many fruitful discussions on this topic, particularly Axel Blumenstock and Dr. Gert Volk.

10. References

[1] DESTATIS (German Federal Statistics Agency): "Verkehrsunfälle 2013"

[2] US FAA: "*System Safety Handbook*". Washington, DC, 2000

[3] Rausand, M.; Høyland, A.: "*System Reliability Theory: Models, Statistical Methods, and Applications*", Wiley & Sons, 2004

[4] Schöner, H.P.: "*Erprobung und Absicherung im dynamischen Fahrsimulator*", SIMVEC-Conference, Baden-Baden, 2014