SAFETY LAYER for INTELLIGENT TRANSPORT SYSTEMS

Benedikt Schonlau
Dr. Klaus Krumbiegel
David Seidel
IAV GmbH
Germany

Paper Number 15-0206

ABSTRACT

Intelligent Transport Systems are currently being developed in many different industry sectors.
These developments range from highly automated land vehicles, robots for mail delivery, agricultural drones up to ships automating vehicle ferry operations or automating the transportation of oil from the corresponding platforms.
Virtual drivers are a big challenge for implementation of these systems, and there is currently much activity in this area. But this is not the major challenge; which is making those systems safe and reliable. The following article shows an approach to realize safety and reliability of Intelligent Transport Systems by separating the functional components into a driver model with limited safety and reliability, and an additional safety layer.
In this approach, the driver model takes care of putting the required application case into practice and tries, similarly to a human driver, to continuously optimize the driving task. It is also possible to use training programs in productive operations for such driver models.
The driver model is supported by a static safety layer. This safety layer implements all safety targets that have been defined in the development phase and ensures that all safety targets are continuously being adhered to during the operation. This article shows an overview of the relevant safety targets for Intelligent Transport Systems and demonstrates strategies for implementing the security layer.

INTRODUCTION

Intelligent Transport Systems in combination with Highly Automated Driving are a frequent topic for research and development. IAV GmbH showed different use-cases with different speed levels of highly automated driving at the ITS World Congress in Detroit [1]. In Las Vegas the BMW Group presented technologies up to fully automated driving with the Remote Valet Parking Assistant [2]. Daimler AG introduced “The Truck of the Future”, an autonomously driving truck with the “Highway Pilot” system [3]. In Europe the first autonomous delivery flights of parcelcopters have been authorized for Deutsche Post DHL AG [4]. So compared to highly automated driving in Intelligent Transport Systems, there are also many similar technologies for automation and autonomous enabling of mechatronic systems in this area.
The objective of this technology is to provide a comfortable and safe future in all situations and numerous companies and institutions are putting a big effort into this [5]. But instead the big issue is to make these systems reliable and safe. The public acceptance of such high technology in their environment can only be achieved by a policy such as that aimed for in the “Vision Zero” initiative [6].
The goal of “Vision Zero”, introduced by the European Commission in 2011, aims for no fatalities or serious injuries by the year 2050. To accomplish a full acceptance it is necessary to put these goals into practice and familiarize the public with these technologies by continuous exhibiting [7].
Currently available assistance systems have a high level of safety, while their main features can be identified by availability and performance. These systems are primarily the basis of future highly automated or autonomous systems in Intelligent Transport Systems. The following article shows an approach to realize safety and reliability of Intelligent Transport Systems by separating the functional components into the comfort function with the main focus on availability and performance (i.e. assistance functions) and an additional safety layer as the safety function. (See Figure 1)

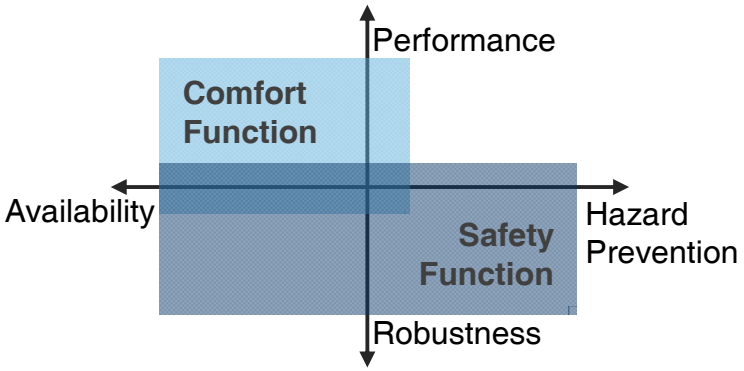

Figure 1: Characteristics of Comfort and Safety functions

CURRENT STATE OF ART

For a better comprehension of Intelligent Transport Systems (Abbr. ITS) and their safety issues, it is necessary to determine all essential system elements within the scope of this article. Starting in the lowest layer with assistance systems, followed by the Highly Automated Driving Systems (Abbr. HAD) and finally showing their part in ITS.
The "autonomous" character of driver assisting functions can be defined as decisions made by the car without the intervention of the driver [7].

Assistance Systems

Current driver assistance systems help drivers by way of a comfort function in standard situations as well as a safety function in critical situations [8]. Normally their function is limited to one problem and independent of other assistance systems [9]. There are two main types of systems: passive and active, not to be confused with categories of safety engineering. While the passive system works in background and the driver won't notice their assistance except for signaling, i.e. the Electronic Stability Control (ESC). The active system has to be turned on and/or adjusted by the driver. Situations the assistance function can't handle, the driver has to take over in around one to two seconds [11][15].
Input data can come from function-exclusive sensors. Shared input sources are a common way to distribute sensor data to the relevant functions. Objects already compiled from different input sources, e.g sensor data fusion, is also an increasingly popular method.
The function can be implemented as part of several functions on a control unit or alone on a control unit [10].

Highly Automated Driving

In contrast to assistance systems, here the car mostly operates by itself. The car controls the longitudinal and lateral directions. In first developments the driver sits in the loop with the automated system to intervene in situations the system can't handle. This take over action should have 8-10s to guarantee a smooth handover to the driver. With further research and development fully automated systems should be able to handle most situations. Then drivers won't be required and the handover request should give them several minutes time. The goal is an autonomous system which can handle every situation and where no drivers are necessary (See Figure 2) [5][11][15].

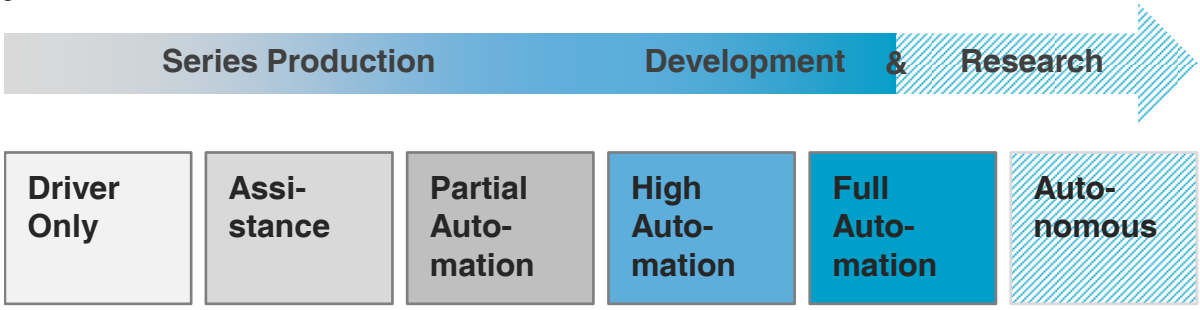

Figure 2: Levels of Automated Driving

Highly automated or autonomous systems require detailed environmental information, which can be achieved by data fusion of different sensor's data and information by communication between all participants. A verification of the presence of objects is possible with different sources of data.

Safety Functions & System Restrictions

Actual HAD Systems include state-of-the-art safety functions like redundancy, watchdogs etc. In addition the driver is sitting every time in the loop of the system [9]. When the automatic system fails, the driver has to take over. In emergency situations safety systems can support the driver or try by them self to bring the car into a safe state [8].

Moreover the German regulatory body doesn't support highly or fully automated driving systems, because the driver has to pay permanent attention to the traffic situation [12].

Fully Automated & Autonomous Systems

Furthermore highly automated or autonomous systems are more and more being introduced into ITS. They range from autonomous multicopters for parcel delivery [4] to fully automated public services [13] and unmanned cargo ships [14].

ANALYSIS OF APPLICATION

In the following illustration a scheme of different ITS participants and their interactions are characterized. It shows a possible example of a future application. Afterwards the limitations of highly automated and autonomous systems are demonstrated for the example with special focus on safety matters. The example also serves as the basis for practical application of the proposed safety concept.

Scheme of an ITS Interaction

The example is shown in Figure 3. It describes situations in an urban area with several participants such as pedestrians, cyclists, cars, public services and delivery services. The description is situation based. All cars are equipped with Highly Automated Driving. The public service and delivery service are also capable of autonomous or highly automated acting. Communication between most participants is possible.

Situation 1 Two cars are reaching an intersection at the same time. There is no direct visual contact between them. Because of car-to-car communications, the vehicles know each other's position, direction and velocity. The HAD System can handle this situation by cooperative actions, e.g. based on the most energy-efficient decision or the traffic rules.

Situation 2 A careless cyclist isn't paying attention to the traffic and just wants to reach the cycle path on the other side of the road. A car, equipped with HAD, is approaching the virtual crash point between these two participants. Even with the knowledge of the cyclist the car can't avoid a crash just by using emergency braking.

Situation 3 A car is approaching a crash site. The crash happened seconds before, so the car is entering a critical phase. Left of the car is a lane of oncoming traffic. On the other side is the sidewalk. The HAD System decides to brake and change to another lane.

Situation 4 A full autonomous delivery service distributes parcels by car and for the last meters to the house by multicopter. The multicopter drops off the parcel in a parcel box next to the house. On the way all sensors for obstacle detection fail.

Situation 5 A fully automated public bus is reaching a bus stop. Sensing an approaching passenger, the bus wants to pull over and stop, but a subsystem fails and is in danger of suffering damage.

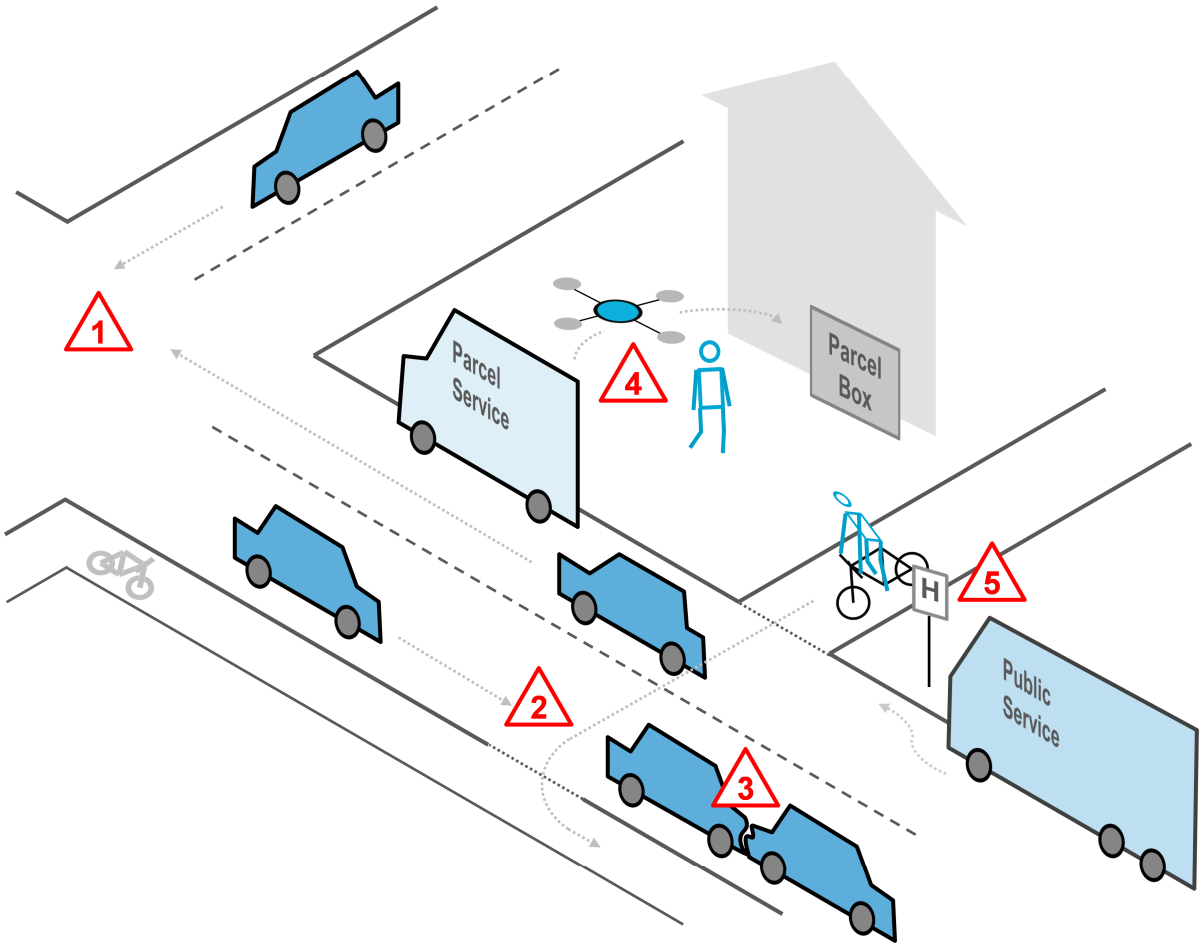

Figure 3: Scheme of danger situations in Intelligent Transport Systems

Limitations to Highly Automated Systems

To point out the limitations of highly automated systems, problems are explained for each proposed situations.

Situation 1 It might use a special implementation to detect other cars, their trajectory and a possible collision point. So for every unique situation like intersection crossing, turning or driving on the highway, there's a corresponding unique detection function for such problems.

Situation 2 The HAD System has to make a tough decision. The first objective is to avoid the crash or in the case it is unavoidable, to minimize the consequences of the accident. The HAD System chooses a process of avoidance, but can't guarantee a successful outcome with regard to the time-critical situation.

Situation 3 The car decides to change to another lane to avoid the crash. The system requests a steering angle, which exceeds the actual possible steering angle of the car. The HAD System thinks it's avoiding the crash, but actually it is not.

Situation 4 The multicopter's autonomous system still wants to deliver the package. It's actually possible, because of the knowledge of the position of the drop-off zone. But it is not safe to go there, because of the failure of the detection sensors.

Situation 5 The fully autonomous bus' system tries to reach the bus stop, but it doesn't recognize the failing system. If it keeps going, it may result in damaged subsystems.

CONCEPT PROPOSAL

This section introduces the Safety Layer Concept. This includes a theoretical explanation of the concept and a detailed description of all components. The concept is then applied to the proposed situations from the above section and the advantages are pointed out.

Safety Layer Concept

If assistance, automated and autonomous systems have a system failure, there is a probability for human or object damage. The concept aim is making these systems safer by separating the functions or subsystems in a comfort part and a safety part as fallback layers (See Figure 1). These fallback layers serve as basis to transfer the system with the failure condition into a safe state. The fallback layer initiates a plan of actions to achieve the safe state.

The procedure can be applied to different assistance functions and automated or autonomous systems, especially in situations where the function or system leads to undefined states, guides into accidents or where components and functions aren't executable. Furthermore the multiple variants of applied applications will be summed up as *functions*.

So the main purpose of monitoring the *functions* is to evaluate their output for regularity, check for possible hazard outcomes and verify for operability of relevant components. The input data can contain condition parameters of the vehicle and environment parameters, which may include information of mobile and stationary objects. The output contains the original output of the *function* or the corrected output in the case that one or more safety functions take control.

Plausibility Layer The first layer of the concept evaluates the output data of the *function* for their plausibility. If the output data exceed a defined interval, the plausibility of the data is not fulfilled.

If the plausibility of the data is not performed, plausible or none data will be forwarded. The check for plausibility can be performed on the basis of defined faults, tables, characteristic diagrams, functional relations, look-up tables or similar methods. The usage of more than one method is also possible.

A feedback to the *function* allows a recalculation for the next period or the deactivation of the *function*. If the *function* is deactivated, a notification to the driver can be given to take over, or another assistance function tries to bring the system into a safe state.

Accident Layer The second layer checks for possible hazard outcomes of the performed action of the *function*. This layer calculates on the basis of the new trajectory of the car and all objects in the environment, a value of accident risk. If the value exceeds a threshold, measures will be initiated to prevent or to reduce the consequences of the accident. This layer can be used for the whole system, even when there is no *function* in use.

Objects can be all other transport systems and users as well as infrastructure elements. So hazard outcomes are defined as damages to people and inanimate objects. Along with the calculated value of accident risk, it is also possible to include the expected hazard or the criticality of the accident in the calculation.

Function Layer The third layer verifies the operability of all relevant components, which are used in context with the *function*. If components are not functional, the layer tries to replace them or deactivates the relevant one.

Relevant components are sensors, actuators, control units, computing resources and algorithms which are used by the *function*. The replacement can be an adequate component or a substituted function by emulation or simulation, where the output data of the component is determined by other components data. If the component is deactivated, the driver should be informed to take over.

Complete Concept All layers are displayed in Figure 4. They are working constantly and monitor the *function* the whole time. It is possible to prioritize all layers differently, but to release output data all layers have to consent. The advantage of this concept is the provision of three independent layers to localize all cause-specific failure sources and eliminate them. All layers can adjust the output data of the function or execute a special action plan to reach a safe state.

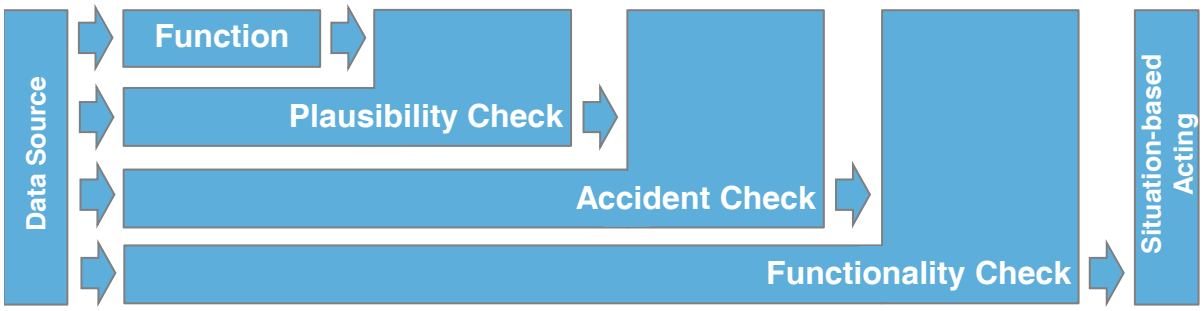

Figure 4: Scheme of Safety Layer Concept

To apply the concept to multiple systems, it is advisable to develop a configurable variant to adapt the layers to a specific system. So the development effort covers several systems and the costs can be divided between them. Also the development effort on the *functions* is a far less, because failures originating from systems, algorithms, undefined conditions or correlation of *functions* don't have any hazard-relevant effects. Further tests on the *functions* and defined threshold values are not necessary. So *functions* can be developed as platform-independent. With an already developed Safety Layer Concept it is easier to test *functions* and re-fit them in running systems.
It is possible to deactivate all relevant components which are associated with a failed component, to suppress false system activity and the usage of unnecessary system resources. After substituting a component, the system should assign a lower confidence value to it, maybe because of inaccuracy, to accomplish a higher safety in the system by adding additional safety tests based on this value.

Implementation in Scheme
In the following, the capabilities of the Safety Layer Concept are shown by applying it to the proposed situations. Application possibilities and advantages are presented.

Situation 1 The *Accident Layer* can operate as the detection function for external objects like other cars. So there is no need for multiple functions to detect outside objects. The HAD System can handle the longitudinal and lateral direction. If the *Accident Layer* detects a possible accident, it handles the specific situation on the basis of regulations and cooperative acting, and reports the takeover to the HAD System.

Situation 2 The HAD System has to handle a time-critical situation. The *Plausibility* and *Accident Layer* work in parallel with it. The layers can support the HAD System, which can only work as a comfort function, by monitoring steering angle and braking force plus adding more braking force. It is also possible to let the layers control the mechanical system, while the HAD System has more system resources to calculate the best avoidance procedure.

Situation 3 The *Plausibility Layer* detects a limit exceedance of the steering angle by the subsystem "Lane Change". By overwriting it to the maximum value, the *Accident Layer* detects a possible crash and decides to steer into the other lane, which is reachable with the maximum steering angle and also free of objects. The layers initiate an action plan to bring the car to a safe state by avoiding a crash with the cyclist.

Situation 4 The *Function Layer* detects the failing sensors. The layer decides to bring the multicopter into a safe state, because it is not safe for the environment to continue the flight. It initiates an action plan and overrules the autonomous system.

Situation 5 The system may end up with damaged parts. Instead the *Function Layer* also detects the failing subsystem and the consequences of its breakdown. The layer executes an action plan to reach a safe state with no further usage of the failing subsystem. The system can call another bus for exchange and a service to make repairs.

CONCLUSIONS

Assistance functions as well as highly automated and autonomous systems may contain possible failure effects like exceeding limit values, going into unknown states, guiding into accident situations or experiencing function losses and suchlike. By introducing the Safety Layer Concept it is possible to counteract these failures based on several layers to evaluate the output of functions for regularity, check for possible hazard outcomes and verify for operability of relevant components. These three layers are designated as *Plausibility Layer*, *Accident Layer* and *Function Layer*.
The concept can be applied to every level of a system, to monitor and control functions, subsystems or the whole system. With the possibility of feedback to the monitored element, overruling and deactivating, the layer concept includes several opportunities to act. By paralleling the layers themselves and to the *function*, it has high potential in time-critical situation to solve complex tasks by distributing the work between different methods. Also the concept can and should be used in every ITS participant, regardless to a possible superior functional unit, to improve the safety of all systems.
The introduction of highly automated and autonomous systems in daily life can only be achieved when these systems are totally reliable and do not present any hazards to people or objects. These goals are equal to the ones of the "Vision Zero" policy. Also the regulations in European States will only be adapted to this technology if sufficient activity on these features will be made. To fulfil such high standards in Intelligent Transport Systems, the use of the Safety Layer Concept is absolutely recommended.

REFERENCES

[1] IAV GmbH. (2014, September 3). *IAV bietet Testfahrten in eigenem hochautomatisierten Demofahrzeug an.* Press release.
[2] BMW Group. (2014, December 19). *BMW TO SHOWCASE INNOVATIONS INCLUDING HIGHLY & FULLY AUTOMATED DRIVING, DRIVER INTERFACE ADVANCEMENTS AND NEW LIGHTING TECHNOLOGIES AT THE LAS VEGAS CONVENTION CENTER SOUTH PLAZA DURING THE 2015 CONSUMER ELECTRONICS IN LAS VEGAS.* Press release.
[3] Daimler AG. (2014, July 3). *Weltpremiere für das Verkehrssystem von morgen – effizienter, sicherer, vernetzter – und autonomy.* Press release.
[4] Deutsche Post DHL. (2014, September 24). *DHL parcelcopter launches initial operations for research purposes.* Press release.
[5] Meyer, Gereon; Deix, Stefan. (2014). *Road Vehicle Automation. Research and Innovation for Automated Driving in Germany and Europe*. Springer International Publishing.
[6] European Commission. (2011, March 28). *White Paper: Roadmap to a Single European Transport Area - Towards a competitive and resource efficient transport system.*
[7] Özgüner, Ümit; Stiller, Christoph; Redmill, Keith. (2007). *Systems for safety and autonomous behavior in cars: The DARPA Grand Challenge experience.* IEEE (Vol. 95, No. 2), S. 397–412.
[8] Kämpchen, Dr.-Ing. Nico; Aeberhard, Kämpchen; Ardelt, Michael; Rauch, Sebastian. (2012). *Technologies for highly automated driving on highways.* ATZ worldwide (06/2012), S. 34–38.
[9] Cieler, Stephan; Konigorski, Ulrich; Lüke, Dr.-Ing. Stefan; Winner, Prof. Dr.rer.nat. Hermann. (2014). *PRORETA 3 Project-Aautomation. Safety with Assistance Systems.* autotechreview (Vol 3, Issue 11), S. 30–34.
[10] Winner, Hermann; Hakuli, Stephan; Wolf, Gabriele. (2012). *Handbuch Fahrerassistenzsysteme.* Wiesbaden: Vieweg+Teubner Verlag.
[11] Ebner, Hans-Thomas. (2013, December 11). *DVR-Kolloquium Automatisiertes Fahren. Motivation und Handlungsbedarf für Automatisiertes Fahren.* Deutscher Verkehrssicherheitsrat e. V. Bonn.
[12] Gasser, T. (2012). *Rechtsfolgen zunehmender Fahrzeugautomatisierung. Gemeinsamer Schlussbericht der Projektgruppe.* Bremerhaven: Wirtschaftsverlag NW (Berichte der Bundesanstalt für Straßenwesen, F 83). MA: C. ARZT, M. Ayoubi, A. Bartels, L. Bürkle, J. Eier, F. Flemisch et al.
[13] Siemens EOOD Bulgaria. (2007, July 3). *Another fully automatic metro system from Siemens goes into commercial.* Press release.
[14] Levander, Oskar. (2014). *Voyaging into the future.* Rolls-Royce. England.
[15] Petermann-Stock, I.; Hackenberg, L.; Muhr, T.; Mergl, CH. (2013). *Wie lange braucht der Fahrer? Eine Analyse zu Übernahmezeiten aus verschiedenen Nebentätigkeiten während einer hochautonmatischen Staufahrt.* TU München und TÜV Süd Akademie GmbH (Hg.): 6. Tagung Fahrerassistenz.