virtual vehicle

TÜV AUSTRIA

WhitePaper

Highly Automated Driving

The new challenges for Functional Safety and Cyber Security

Figure: shutterstock.com (zapp2photo)

Highly Automated Driving

The new challenges for Functional Safety and Cyber Security

Vienna, October 2018

TÜV AUSTRIA HOLDING AG
TÜV-Austria-Platz 1
A-2345 Brunn am Gebirge

Dipl.-Ök. Thomas Doms
Ing. Benedikt Rauch, MSc
DI Bernhard Schrammel
DI Christoph Schwald
DI Edvin Spahovic

VIRTUAL VEHICLE
Research Center
Inffeldgasse 21a
A-8010 Graz

DI Dr. Christian Schwarzl

Imprint

Abstract

Highly or even fully Automated Driving will have a deep impact on human´s social life, changing the way we perceive driving by its actual meaning and how the vehicle passengers will act during travelling between the desired destinations.

Future highly automated vehicles will have to be updated periodically to keep up with the enormous development speed of the entire Automated Driving ecosystem. This leads – already today – to a high risk of possible Cyber Security attacks over all kinds of internal and external electrical interfaces. By such attacks, information could be stolen or even the control of vehicles could be taken over. Such intention must be mitigated at all stages of the vehicle lifecycle including development, maintenance and disposal.

In addition, the functional correctness and safety of Automated Driving functions must be ensured and independently approved. This can only be achieved using novel verification and validation methods, which rely to a large extent on simulation methods, covering a wide range of critical and potentially dangerous test scenarios.

Currently, a well-defined and officially accepted approach to combine safety and security activities for testing and homologation is missing. This situation is reflected in the respective safety-related standards, which do not cover new development and verification paradigms needed for Automated Driving. Supplementary standards dealing with these new issues are currently in development but cannot be expected before end of 2020. Consequently, companies active in the automotive industry, are currently facing big challenges during development and approval of their products.

This White Paper by TÜV AUSTRIA and VIRTUAL VEHICLE discusses the challenges highly Automated Driving poses for human safety and demonstrates what kinds of aspects regarding Functional Safety and Cyber Security have to be considered already during development as per today.

The new challenges for Functional Safety and Cyber Security

Content

1 Introduction

The raising demand for safety in automotive mobility is one of the main reasons for the development of novel Automated Driving functions, which – at the same time – also provide additional comfort for the driver and other passengers. The newly won free time, enabled by allowing the driver to take the mind off driving, have brought a nearly endless flood of ideas on additional usages of the car, making it a family playground, multimedia centre or workplace. However, before this visionary vehicle utilizations and resulting new lifestyles can become reality, many technical questions have to be answered first to ensure the safety of passengers and other traffic participants during Automated Driving.

From a technical point of view a fully Automated Driving vehicle takes over all driving activities from the driver, especially longitudinal and lateral control of the vehicle, meaning accelerating, braking, and steering. The society of automotive engineers (SAE) defines five levels of automation in the J3016 standard [1], classifying the amount of driving activities performed by an Automated Driving function instead of the driver. In addition to these five levels, level zero (L0) refers to zero automation, where all driving activities are performed by the driver. On the other end of the scale is automation level five (L5), where the vehicle is fully automated and performs all driving activities on all kinds of roads and in any possible driving situation.

To make Automated Driving a success and to reach the ambitious goal of level five vehicles, also economical aspects and customer needs have to be considered. In a recently performed study *(Figure 1)*, the results clearly show that safety and quality of automated vehicles are of highest importance for buying decisions [2].

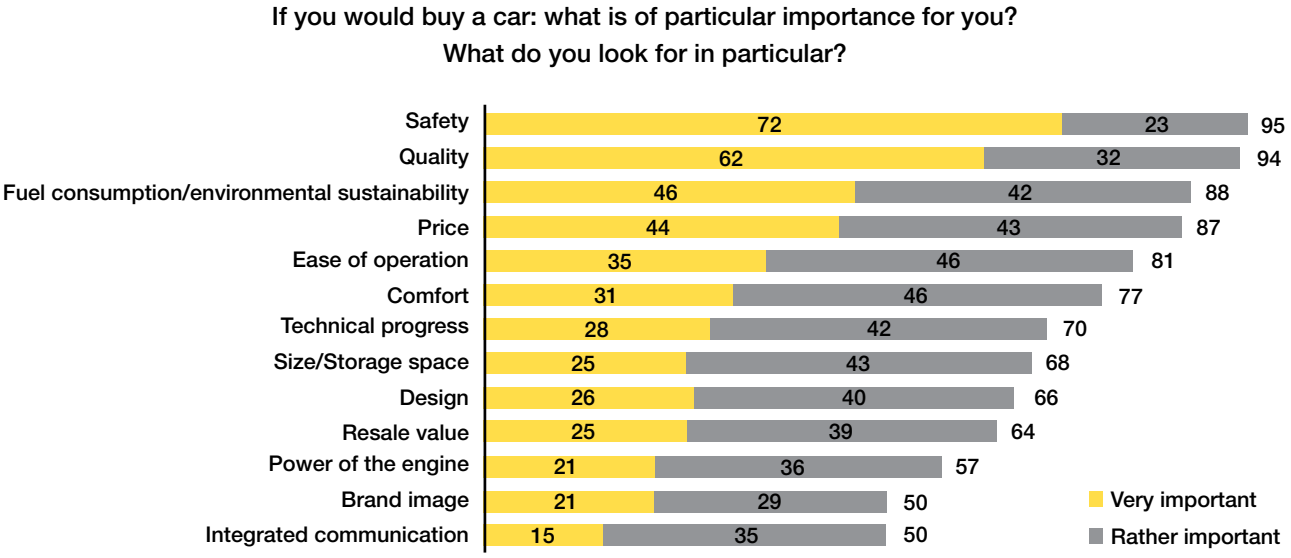


Figure 1: Study about importance of characteristics for buying decisions [2]

Based on this information it is self-evident that newly developed Automated Driving functions shall be thoroughly tested during development and type approval, to achieve the required quality level and to increase customer´s trust. A thorough testing of a complex Automated Driving function requires test drives for around 200M kilometres per vehicle model, as discussed in a scientific report [3]. This high amount of test drives is needed for achieving a similar accident probability for Automated Driving vehicles in comparison to manual driving. Since this large amount of test driving is economically infeasible and practically nearly impossible, new virtual testing and type approval techniques are inevitable. With these virtual type approval (also known as homologation) techniques it is possible to test the vehicle in critical driving situations (scenarios) within a simulated environment. The possibility to control the occurrence of critical scenarios in a virtual test environment, allows reducing the need for test drives enormously, while achieving the same occurrence probability we have currently on the streets.
Given the theoretical background, the main question remains: Why are there so many critical situations for Automated Driving vehicles? To answer this question, a closer look on the electric/electronic (E/E) system of the vehicle, which realizes the Automated Driving functionality, is needed.

1.1 Vehicle Electric/Electronic (E/E) Systems

In general, each Automated Driving function is split into three main tasks: sense, control and act. These three tasks are also reflected in the E/E system architecture *(Figure 2)* and will be described in more detail below.

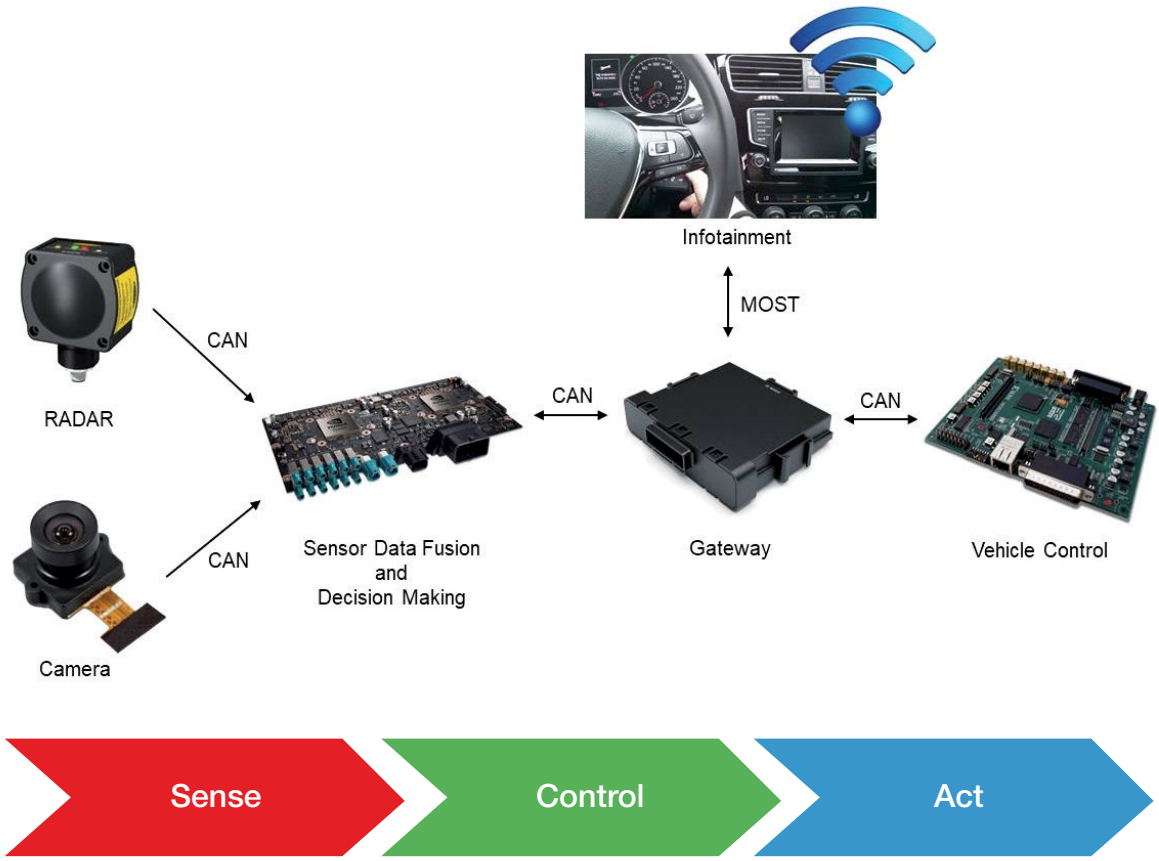


Figure 2: Vehicle E/E system showing the main components for an Automated Driving function and the infotainment system

1.1.1 Sense

The term sense refers in this context to all tasks needed to perceive the environment. The different object types, which must be perceived, require different sensor technologies *(Figure 3)*. A figurative example is the detection of street markings, which are only painted onto the street surface and are two-dimensional. For this reason, the usage of a camera is required because they cannot be detected by e.g. a RADAR or LiDAR sensor, which measure an electromagnetic wave or laser beam reflected by a three-dimensional object. However, it is difficult to calculate the distance of a three-dimensional object using just a single camera, because there is no unique relation between object size, focal length and the resulting object distance within the image.
In addition, the different sensor technologies perform differently under certain weather conditions, which make the environment perception part even more complex. For example, a camera and LiDAR sensor have a reduced performance if used in a foggy environment, whereas a RADAR sensor is not impaired. RADAR sensors on the other hand have functional limitations if metallic objects appear in the field of view, which can cause heavy distortions in the sensor data (e.g. aluminium beverage cans, or metal plates used at construction sites).

Recent developments in the use of artificial intelligence (AI) and in particular, the astonishing results obtained using deep-neural networks (DNNs, “Deep Learning”) for object detection and classification from camera images, opened the door for their application in the automotive industry.

There, they are often used to classify different object types into categories like cars, buses, trucks, pedestrians, streets, traffic signs, and so on and vastly outperformed solutions using standard software development techniques in terms of precision. However, due to the fundamental differences during development of DNNs, the well-established and elaborated software development processes in the automotive industry cannot be applied, making it very hard to ensure and verify that the Deep Learning functions work correctly in all different driving scenarios.

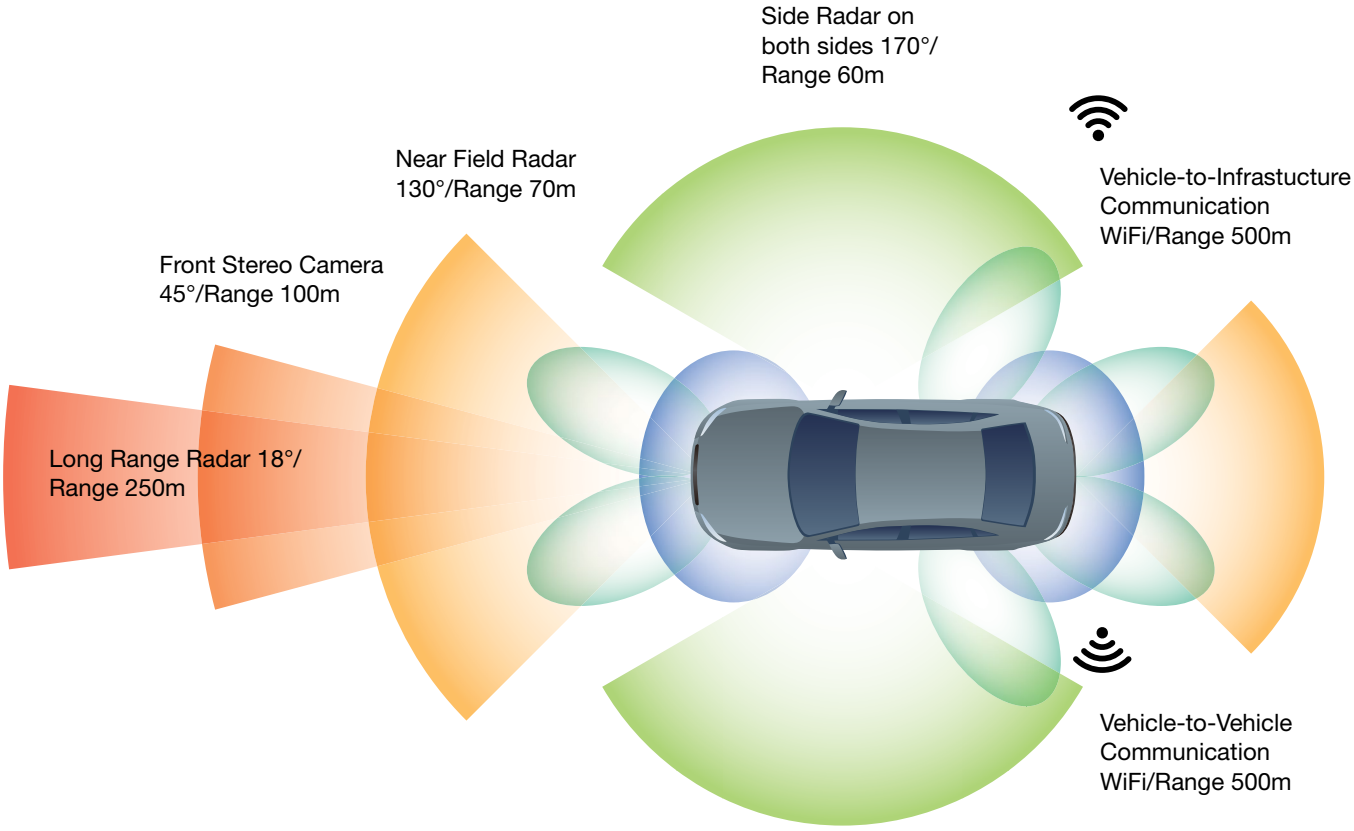


Figure 3: Multiple sensor technologies with their respective field of view and intended usage

1.1.2 Control

During the control part of the action chain, the detected environment objects are incorporated into an environmental model, capturing all collected information about the physical environment and the vehicle odometry. The vehicle odometry reflects the motion and location of the vehicle, obtained from vehicle sensors like inertial measurement units.

Using the different information in the environment model, a situation analysis and decision-making algorithms are used to define the next driving manoeuvre. The situation analysis algorithm refers to the environment model and identifies the free space on the road and the most likely behaviour of other traffic participants, to identify safe movement paths for the ego vehicle. The decision-making algorithms weighs the safe movement paths and decides on the next movement path to make, which is then executed during the act phase.

1.1.3 Act

In the act phase, a selected movement path is executed by the vehicle, meaning that steering, acceleration and brakes are controlled in such a way, that the given path will be followed by the ego vehicle. In order to inform other traffic participants about the planned driving manoeuvre, it has to activate the vehicle indicators for manual drivers and to communicate its decision over vehicle-to-vehicle communication to automated vehicles.

The different tasks and algorithms used in an Automated Driving vehicle have specific hardware requirements. The architectures of these E/E systems require fail-operational solutions if the driver is out of the loop. Therefore, a wide range of computing platforms are used within a vehicle E/E system, varying in computation power, electrical interfaces and safety concepts including measures like monitoring and diagnosis functions. The different software parts, realizing a vehicle function, are distributed over multiple computation platforms. In addition, on a single computation platform the software from different vehicle functions is executed. This means that the vehicle E/E system is a distributed system using shared hardware to maximize efficiency.

1.2 Testing: State-of-the-Art

The testing of such distributed systems is already a very complex task and usually performed on multiple test platforms. The test platform capabilities are typically aligned with the integration steps, where parts of the E/E system or functions are combined and tested. Test platforms with a high grade of simulation are a compromise between cost and closeness to reality. For example, rare situations can be cheaply tested using software tests running on an office PC, but these tests do not consider timing effects coming from bus communication or measurement errors contained in real sensor data. Thus, it is not possible to evaluate the entire vehicle functionalities and its correct behaviour by just applying software testing. On the other side of the spectrum is the test drive, where a vehicle is operated on public roads. These tests reflect the real implemented behaviour but are also very expensive, unpredictable and irreducible and are not suited to test critical or rare situations. For this reason, several test platforms are used in automotive testing, where the advantages of each test platform are leveraged to optimize the overall test results.

1.3 Testing: New Challenges

The high complexity of Automated Driving demands that a large testing part is performed in simulation and on test tracks, where a controlled environment allows the execution of reproducible tests. One of the main challenges is a coherent sensor stimulation, ensuring that all sensors detect the same environment. This becomes difficult especially in a simulated environment, where the environment objects have to be transformed into coherent sensor inputs. To achieve coherency, the different sensors need to perceive the same objects with comparable precision, ensuring the plausibility of measurements produced by different sensors. The coherent sensor stimulation must also consider different weather conditions, which can heavily influence the performance of real sensors.
The second big challenge in testing Automated Driving functions is the verification of the functions falling into the control category described above. Here, the biggest challenge is the definition of the needed test scenarios, ensuring that all critical scenarios are sufficiently covered with a minimal number of tests. Since an infinite number of tests for complex decision-making algorithms exists, the test selection will play a critical role in the development of Automated Driving functions.

1.4 Type Approval/Homologation: New Challenges

The complexity of Automated Driving and its functions stated above also pose severe challenges on the type approval/homologation of such functions, which must be done before a car is permitted to be brought onto the market. The type approval of a vehicle is performed by an independent party like TÜV AUSTRIA, which checks the functional correctness of the vehicle by testing. Consequently, the type approval/homologation procedure has to deal with the same challenges as stated above for testing and has to find general solutions applicable for all function variations coming from different OEMs (Original Equipment Manufacturer). The criticality of these testing activities is much higher than during function development. The reason is that if type approval/homologation is passed, the vehicle is deemed safe by the public authority and therefore the vehicle must perform according to public regulations and should reflect public expectations.

1.5 Security

The responsibility handover from the driver to the vehicle in Automated Driving further increases the importance of Cyber Security aspects within the development process of such functions. One of the main reasons is that security issues can directly impact the Functional Safety of the car, if a security breach is used to negatively impact implemented safety features. In addition, data privacy must be ensured, which requires secure technical solutions not only within the vehicle network but also for all other connections to e.g. back-end systems operated by OEMs and consumer electronics like tablets and smartphones.

A technical solution which is safe and secure at the same time, must fulfil mutual exclusive requirements regarding maintenance. A functional safe system is designed in such a way, that it can deal with internal system faults like hardware or software errors and incorrect stimuli from the environment without putting humans at unreasonable risk. For this reason, a safe system should not be changed over lifetime, ensuring that the safety measures are working as expected. In contrast, to maintain security, regular software updates are needed to remove newly found system vulnerabilities and to react to latest attacks. Consequently, a secure system has to be constantly adapted and changed (software updates and upgrades), which conflicts with the safety requirements regarding continuity. Moreover, updates (over the air or wired) need to be consistent and atomic. That means:

– **Consistent:** The compatibility of the versions shall be tested and versions that are not listed as compatible must be rejected. This requires every dealer/shop to use a standardized protocol and version repository.

– **Atomic:** A change to the system is done completely or not at all. If e.g. the Adaptive Cruise Control (ACC) ECU has been updated and the corresponding update of the engine ECU fails, a complete roll-back shall be performed. Otherwise the vehicle is left in an inconsistent state jeopardizing Functional Safety.

Thus, novel technical solutions as well as development processes maintaining safety and security of a constantly changing system shall be investigated and deployed.

2 Legal Constraints

The basic legal framework for developing vehicles, or more general safety critical systems, is defined by laws regarding product liability. Product liability requires that a product, which is brought onto the market, provides reasonable expectable safety and is developed according to the state-of-the-art. For example, an Automated Driving vehicle must not produce a rear-end collision, neither by driving into a vehicle in front nor by unreasonably strong braking causing another vehicle to collide with the automated vehicle.

The second requirement states that the product development is performed according to the state-of-the-art, which is roughly defined by the common methodologies employed at the time. These common methodologies are for example defined in national and international standards, maintained by standardization bodies like the International Standardization Organisation (ISO) and/or national standardization agencies. The main goal of the standardization work is to provide comparability and uniformity between analysis results independently performed in different companies.

For the development of Automated Driving functions and vehicles, especially the international standards ISO 26262, ISO PAS 21448 (under development) and ISO 21434 (under development) shall be considered, where ISO 26262 and ISO PAS 21448 focus on Functional Safety and ISO 21434 focuses on Cyber Security for road vehicles.

2.1 ISO 21434: Road Vehicles – Cyber Security

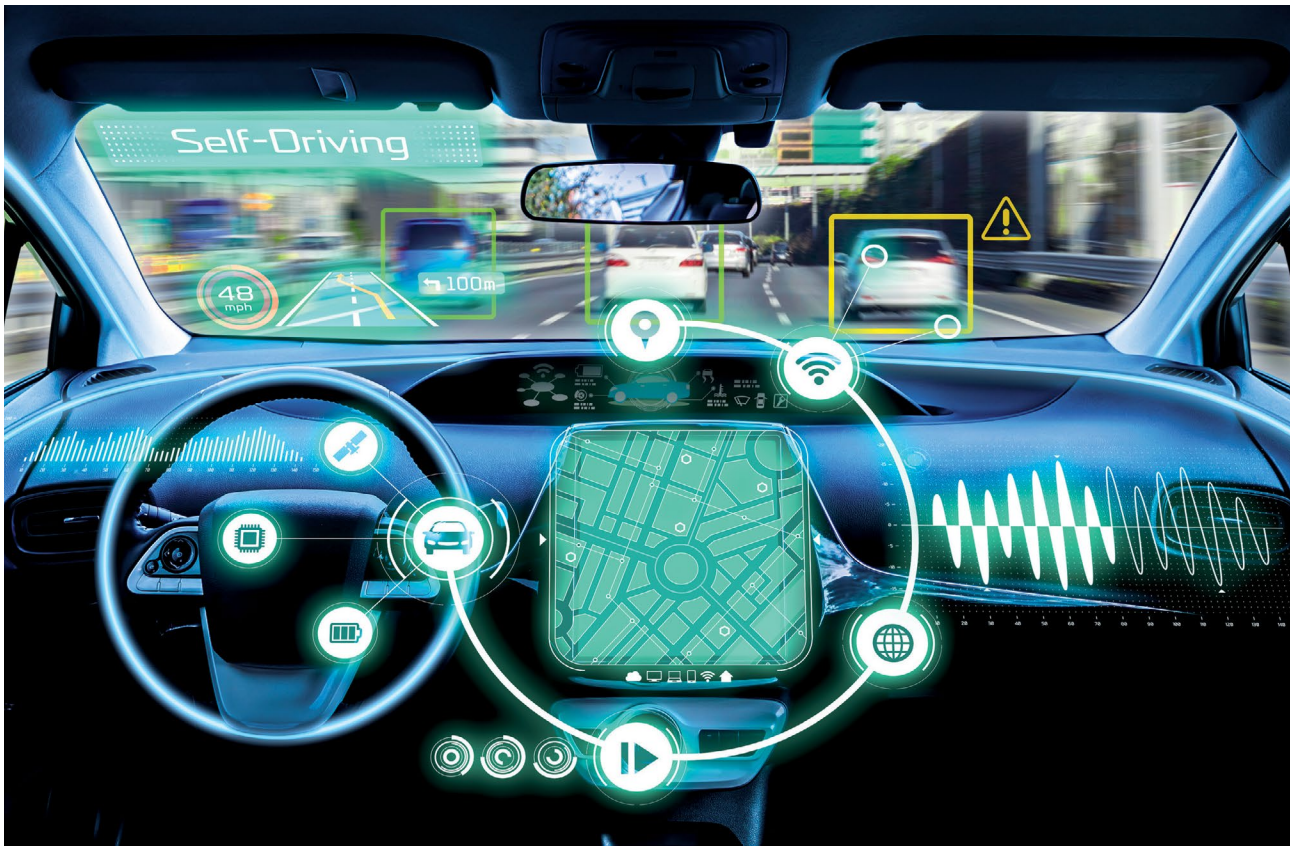
The automotive industry must address a wide range of challenges in order to make vehicles secure and consequently maintain Functional Safety. The main complexity driver is the large number of interfaces, which have been brought into the vehicle to communicate with consumer electronics and back-end services provided by the OEM and new integrated functions like the emergency call (eCall). Each of these interfaces offers an additional attack vector, where an attacker (hacker) can use a vulnerability to gain unauthorized access to the system. Once the system has been infiltrated, the attacker can steal information, take control over functionalities of the car (e.g. ransomware attacks) or disturb the proper functionality of the car. In all cases of possible attack scenarios, the OEM would suffer an image loss, which also might be one of the intentions of an attacker. It would be even more severe, if the personal safety of the driver and his passengers as well as other road users would be endangered by such attacks.

To avoid such scenarios, appropriate countermeasures have to be applied already during development of a vehicle (security by design) which is the intention of the ISO 21434.

The ISO 21434 Road Vehicles – Cyber Security Engineering is currently a draft and will be released in 2020. The goal of the standard is to harmonize the view on security among the different OEMs and suppliers to prevent unauthorized access and manipulations of the system. This will be achieved by regulating the development as well as the used methods. Consequently, the ISO 21434 defines requirements regarding the whole vehicle lifecycle with special emphasis on production and maintenance, including procedures for long-term security updates. In addition, it specifies methods and their corresponding work products to be used, providing evidence that the development has been performed according to the state-of-the-art. ISO 21434 recommends a Threat Analysis and Risk Assessment (TARA) during the concept phase of a vehicle. A possible method for risk identification can be done as in the Security Development Lifecycle (SDL) by utilizing Security Threat Modelling methods e.g. STRIDE. It is reasonable to list the identified risks in an expandable database, to be able to check e.g. known and new upcoming security threats for vulnerabilities of the components of the vehicle throughout the whole lifecycle. From the data generated by TARA a Cyber Security concept with mitigating measures can be developed (equivalent of the Safety Concept of ISO 26262), which leads to the security requirements for road vehicles, their components and interfaces throughout the engineering process.

2.2 ISO 26262: Road Vehicles – Functional Safety

The first version of the ISO 26262 has been released in 2011 and is already well integrated into current development processes in the automotive industry. The second edition has been released in 2018 improving clarity and has an extended scope including trucks, busses as well as motorcycles. The goal behind the required activities and work products is to ensure that no fault within the E/E system can cause a hazardous situation and potentially harm people. Therefore, this standard requires the development of a system, which can detect software and hardware errors and to mitigate the effect and reach a safe state.



2.3 ISO PAS 21448: Road Vehicles – Safety Of The Intended Functionality (SOTIF)

The ISO PAS 21448 – SOTIF is complementary to the ISO 26262 and focusses on the prevention of hazardous situations caused by technical shortcomings or misuse of the E/E system.
This standard is currently under development and is expected to be released in 2019.

The ISO PAS 21448 standard assumes that the system behaves as specified and no fault is present. However, technological shortcomings like incorrect behaviour caused by distorted sensor data will occur in practice. Such a sensor distortion can for example be a strong light source in the field of view of a camera or metal objects on the street in front of a RADAR sensor. An example for a potential technical shortcoming is shown in *Figure 4*, where an optical illusion might fool a camera-based perception system. The cross-walk marking, which is just painted onto the street and creates an optical 3D effect, might be incorrectly recognized as an obstacle and cause an evasive manoeuvre or an emergency brake of an automated vehicle. These reactions might cause a hazardous situation for the oncoming traffic or a following vehicle and is therefore within the scope of SOTIF.
SOTIF describes how to deal with such issues described above, that encompass the entire environment, including road conditions, surrounding landscape, object texture, weather, and potential misuse to minimize the risk.

Figure 4: Optical illusion which might fool a camera-based perception system

2.4 Situation for Companies

Different national regulations, applicable standards and technical challenges increase the development complexity of Automated Driving vehicles. For example, in the United States the National Highway Traffic Safety Administration (NHTSA) offers a nonregulatory approach for automated vehicles. This illustrates a guidance for the automotive industry and other key stakeholders for testing and safe deployment of Automated Driving Systems. The different standards for Functional Safety and Cyber Security have to be fulfilled at the same time and thus correspondingly considered in the (development) processes. However, the dependencies and synergies of the different analysis methods are currently investigated in the scientific community and automotive industry to find an efficient task- and review-alignment minimizing the overall effort. The result of these activities is a safety and security co-development approach, which fulfils the requirements of all relevant standards and precisely defines the interactions between the tasks and the content in the produced work products.

3 Safety

All safety activities in the automotive industry have the same goal, to avoid or at least to reduce harm to vehicle occupants and other traffic participants. In these activities technical measures are developed, which support the same goal but use fundamentally different approaches. These approaches can be roughly split into three categories: Passive Safety, Active Safety and Functional Safety.

3.1 Passive Safety

In the category of passive safety, primarily mechanical solutions are used to physically protect people. Some solutions in this category are for example the usage of improved materials providing higher stiffness at lower weight or novel body structures, increasing energy absorption and consequently reducing the effect on the vehicle occupants during a crash.

3.2 Active Safety

Active safety activities are focused on the development of assistant functions, which try to compensate human errors and to actively reduce harm. Prominent examples are the active bonnet to protect pedestrians and the automated emergency brake system, which actively initiates the braking system to avoid collisions. Future active safety systems used for Automated Driving will also include additional information from cloud-based services and obtained data from communication with other vehicles or the infrastructure. This received information will be used to update the environment model to increase its precision and to use data which cannot be obtained from vehicle sensors like cars hidden behind buildings.

3.3 Functional Safety

In contrast to the active safety activities mentioned above, which aim at limiting or avoiding harm by using additional features and technologies in the vehicle, Functional Safety ensures that no additional harm is caused by errors or technical shortcomings of the E/E system itself.

An example is a random hardware fault in an automated emergency brake system, which has been developed as an active safety measure, which could lead to an incorrect emergency braking manoeuvre. Due to the application of Functional Safety, the hardware fault is detected by the E/E system and the emergency brake is prevented. Thus, no additional harm is caused to other traffic participants.

The Functional Safety activities are supported by two international standards, ISO 26262 and ISO PAS 21448, where the first standard addresses faults within the system and the second, technical shortcomings if the system works as specified. Especially SOTIF is gaining importance with increasing vehicle automation level. The SAE J3016 defines five levels of automation, where the additional level zero refers to "no automation", as shown in *Figure 5*.

A big step, from a technical perspective, is the transition from level two to level three, where the responsibility for system monitoring is shifted from the driver to the vehicle. The driver acts as fall-back solution at level three and must retake control over the vehicle if the system cannot handle a situation. A typical hand-over scenario consists of the following steps: 1) the system identifies a situation it cannot handle, 2) the driver is notified beforehand to take over control, and 3) the driver takes control of the vehicle. In this scenario, the driver is notified before a critical section is reached, meaning that the system function must be guaranteed until the driver has retaken control. From an ISO 26262 perspective, this means that a random hardware or software fault occurring during the hand-over time shall not have an impact on the system functionality. A system fulfilling this property is called fail-operational. Safety measures for non-automated driving, assisted driving (level 1) and partial automation (level 2) of the vehicle usually ensure fail-silent operation, which guarantees that the driver can control the vehicle until a defined safe state is reached. However, to achieve fail-silent operation, a function can be disabled, which is not possible for fail-operational systems. For this reason, Automated Driving functions of level three and above shall be fail-operational to some extent, raising many technical questions about technical solutions and their costs.

The development of fail-silent systems is well known and covered by the ISO 26262, where faults within the system are analysed and corresponding mitigation strategies are defined. However, especially for upcoming fail-operational systems, technical shortcomings not addressed by the ISO 26262 – but in scope of the ISO PAS 21448 – must be considered additionally.

The main challenge in the SOTIF activities is, that not all technical shortcomings are known during development and in the worst case might be revealed during operation, after the vehicle has been brought onto the market. For this reason, the SOTIF activities explicitly includes tracking the vehicle performance in the field to identify unsafe scenarios not known during development.

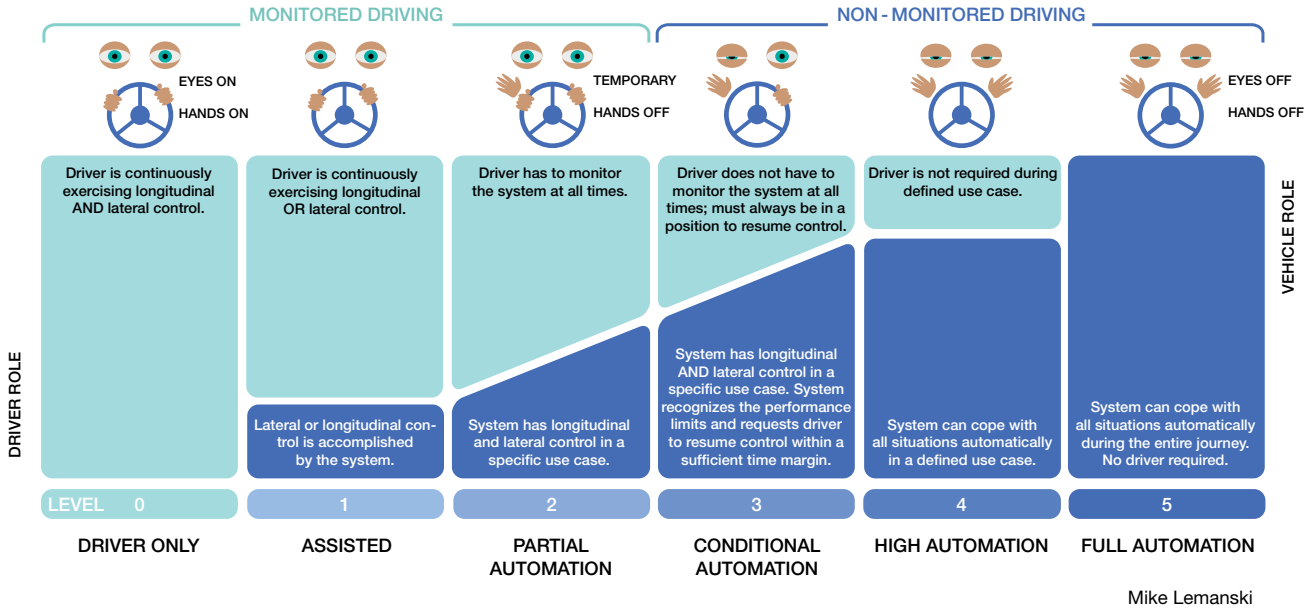


Figure 5: Vehicle automation levels

This evolution of the use case categories is shown in *Figure 6*, where the number of unknown and unsafe scenarios is minimized over time.

To ensure that the known technical shortcomings do not cause any hazardous situation, a rigorous verification and testing of the system is needed. During system verification, all known critical scenarios shall be tested under varying environment conditions, especially different weather conditions which can heavily impact the sensor performance. This approach allows identifying technical shortcomings before the vehicle is brought onto the market and enables a company internal learning to avoid unknown unsafe scenarios during development.

However, the absence of unknown and unsafe scenarios cannot be guaranteed and therefore criteria are defined, which provide evidence that the system causes no unreasonable risk. This is for example achieved by doing test drives – in simulation, on test tracks or public roads – and compare the residual risk based on occurring errors during validation with traffic statistics. If the comparison shows that the newly developed Automated Driving function is less likely to produce an accident or more general a hazard, then it can be considered as safe and enter the market.

In summary, the development of functional safe systems and the corresponding safety lifecycle builds on a sound basis defined in the ISO 26262 and new approaches to address issues caused by technical shortcomings are developed and introduced in the ISO PAS 21448. These safety activities do not explicitly address system changes during operation lifecycle, which are inevitable to allow e.g. software updates to maintain cyber secure operation. These issues are described in the next chapter.

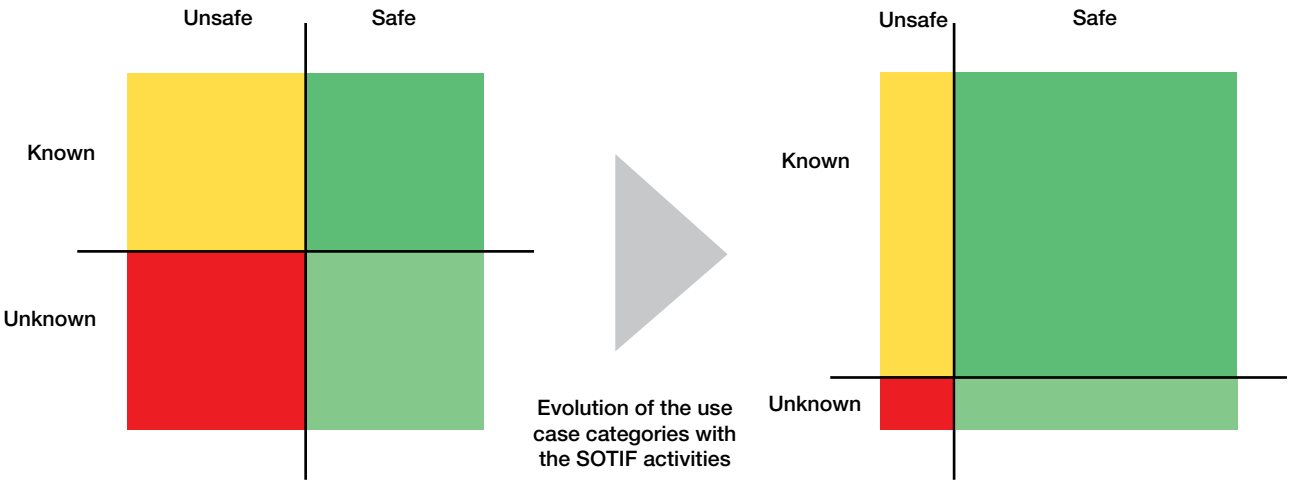


Figure 6: Minimization of the unknown and unsafe scenario number over time

4 Cyber Security

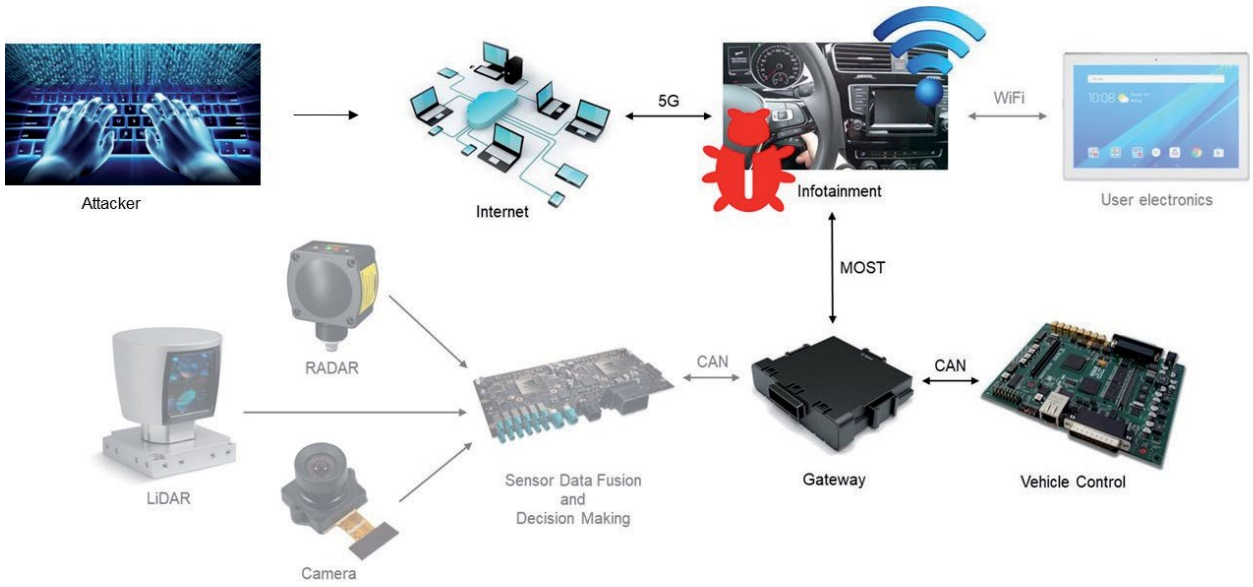


Figure 7: Manipulation of vehicle control using a software bug in infotainment system

Cyber Security has vastly gained attention within the industry and scientific communities with the arise of Automated Driving. The increasing interest was not only driven by successful cyber-attacks on a Jeep in 2015 [4], where complete control over the vehicle was gained due to a security vulnerability, but also because of the impact such vulnerabilities can have on the vehicle- and thus personal-safety. A lot of successful hacks are meanwhile well known.
One example is the Keyless Entry / Keyless Go feature of vehicles. Currently there is no way to detect the distance between a secure sender (key fob) and a secure receiver (car). Hence, attackers can relay the radio waves of a victim's key over several hundred meters to the car, which will in turn open and start. One fix would be to implement a push button on the key fob or to not use keyless entry at all.

In general, the success of a cyber-attack depends on three major categories:

1. remote attack surfaces
2. cyber physical features
3. and in-vehicle network architectures.

Although Cyber Security is a very wide topic including for example reduced safety, data theft, black mailing, fraud, damaging company reputations and so on. In this paper, we will only address issues regarding safety.

Example (security vulnerability impact)

Figure 7 shows the potential impact of a security vulnerability in the infotainment system on the vehicle control, allowing a remote attacker to steer, accelerate or brake. In this fictive example, it is assumed that the infotainment system has a security vulnerability caused by a software bug in the communication stack connecting the vehicle with the internet. An attacker finds the security vulnerability and uses a standard PC to connect to the vehicle and executes a specific code exploiting the security vulnerability to elevate its privileges within the vehicle E/E system. The gained privileges allow the attacker to upload and execute his own vehicle control code in the infotainment system. This code allows the attacker to send vehicle control messages over the Media Oriented Systems Transport (MOST) bus, which are forwarded to the vehicle control unit by the gateway.

The previous example outlines a potential attack scenario, which can be realized if no security measures are applied. It clearly highlights that Cyber Security affects the whole vehicle E/E system and cannot be achieved separately within single components or functions. It is also important to highlight that Cyber Security activities must consider all vehicle functions and shall not be limited to those which are critical from a Functional Safety perspective. This is also well illustrated in the previous example, where a completely uncritical vehicle function from the infotainment system was used as entry point and allowed a vehicle control takeover.

Such scenarios can be avoided if appropriate security measures are defined and implemented in the E/E system. There exist many security measures, which could have prohibited the remote vehicle control. For example, a firewall installed on the gateway can prevent the forwarding of the invalid vehicle control messages. Also, the use of message signing can ensure that the message sender can be verified by the receiver. However, since security must be achieved on system level, the different security measures must be carefully selected and aligned with each other to maximize their effectiveness.

As most Cyber Security attacks will be performed remotely, countermeasures should focus on different attack vectors. For example, by minimizing the attack surface and lock down remote services as much as possible to secure remote endpoints. Another idea often suggested is to cryptographically verify CAN (Controlled Area Network) messages to make CAN frame injection difficult. The idea is that only the ECUs (and authorized garage tools) have the keys and so a random attacker wouldn't be able to send valid CAN messages on the compromised automotive network. It is also widely discussed that manufacturers should design their automotive networks in such a way, that they isolate those ECUs with remote functionality from those that control safety critical features. However, these measures are all not panaceas and do not solve all the problems. Since mostly all types of remote attacks will necessarily be multi-stage, a defence in depth strategy that includes detection of frame/message injection as part of an overall security strategy is recommended by technical analysts [5].

Security measures can only be reasonably defined if the threats which must be mitigated are known. For this reason, a thorough system security analysis shall be performed, inspecting the system interfaces, dependencies between functions, used communication stacks, protocols and underlying bus system implementations. The results of the security analysis are potential threats, which can be executed. The well-known STRIDE method uses the following threat categorization:

- **Spoofing of user identity:** another user is impersonated
- **Tampering:** unauthorized modification of data
- **Repudiation:** break log data integrity
- **Information disclosure:** unauthorized retrieval of data
- **Denial of service (D.o.S):** prevent a function fulfilling its purpose
- **Elevation of privilege:** gain unauthorized access

The threat analysis is performed on the system architecture, where the components and interfaces are already defined. Each interface is also an attack surface, which can be exploited and accessed.

The methods and tools needed for system analysis and to define appropriate security measures are currently homogenized and aligned in the ISO working group crafting the ISO 21434 standard. In this standard, a security development process for the whole product lifecycle is defined. The described process starts with a thorough analysis of the system, its potential threats and vulnerabilities allowing the execution of a threat. The analysis results form the basis for the definition of security measures, which will then be implemented during product development. For the product development phase, primarily the management of security requirements and their verification and validation is specified, ensuring that no threat can be executed caused by mistakes made during development. In contrast to the Functional Safety standards, the ISO 21434 has also a strong focus on operation and maintenance, maintaining Cyber Security over the whole lifecycle. Particular requirements on the service and update procedures are defined in the standard, which are also potential attack surfaces and could allow an attacker to gain unauthorized access.

The different and partly mutual exclusive requirements for developing a safe and secure system requires a novel co-engineering approach, where the differences and synergies are precisely understood, and the applied analysis methods are most effectively used. Such a co-engineering approach must consider all the relevant standards and shall be reflected in the company internal development processes to minimize development cost.

5 Virtual Type Approval/Homologation

Before a new vehicle can enter the market, a thorough verification and validation of its functional correctness is necessary not only to ensure customer satisfaction in terms of comfort features, but also to avoid hazards to vehicle occupants and/or other traffic participants through an unsafe operational vehicle.

5.1 Automotive Test Platforms

The verification and validation (V&V) of the functional correctness is performed by OEMs & Tier 1 suppliers who use tests at different integration steps, where the individually developed functions or systems are integrated and tested using real or simulated environments. With increasing integration steps, the executed tests move from simulation to reality, where in the lowest step the function is tested using purely simulated inputs and in the highest step only real sensor data obtained during test drives on public roads is used. Additional regression test activities for functional changes and bug fix handling during development are considered for V&V activities.

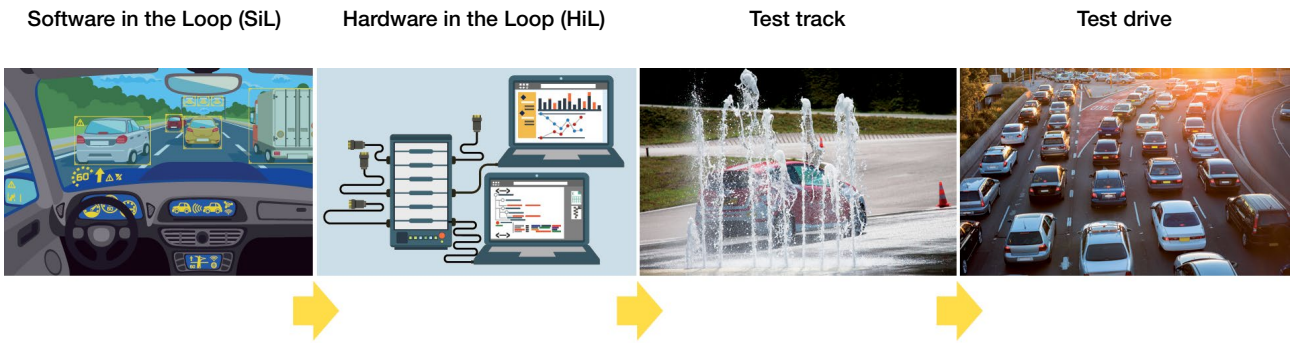


Figure 8: Common test platforms used in the automotive industry

The main test platforms considered in the automotive industry are shown in *Figure 8*, which are the Software-in-the-Loop (SIL), Hardware-in-the-Loop (HIL), proving ground and public roads. The shown test platforms reflect the integration steps of the developed function into the vehicle. On SIL and HIL platforms software and hardware parts are tested. On proving grounds and public roads functions are tested in the final vehicle.

For testing a sensor data fusion algorithm on a HIL platform, real sensors and software running on the target computation platform can be used. Although tests executed on the HIL can show that the individual sensors and algorithms perform as expected, but they cannot provide any evidence that they are appropriately used and integrated into the vehicle. In addition, especially the sensor performance under harsh environment conditions, typical for automotive applications, must be assured. Thus, the sensor needs to function under extreme temperatures ranging from -40°C to +85°C, heavy vibrations, electromagnetic interferences caused by the vehicle itself or passing vehicles, and must withstand water and ice coming from snow, fog and rain.

These issues are specifically addressed in tests executed on a proving ground or public roads, where the required components/systems are integrated into the vehicle and tested under real environmental conditions. On the proving ground, the vehicle is operated in a controlled environment, where reproducible tests in different weather conditions and driving situations are performed. Tests performed on public roads focus primarily on the validation of the developed function, where it is checked if the customer requirements are met. This is achieved by checking the behaviour in real life scenarios regarding usability and performance.

5.2 Type Approval/Classic Homologation

The main idea behind type approval, is the same as for verification, namely the execution of tests to ensure the vehicle meets its requirements and behaves as expected. However, type approval is done to get a "second opinion" about the functional correctness of a vehicle before it will be approved to enter the market. Since the type approval must be accompanied by an independent third it is performed by accredited companies like TÜV AUSTRIA.
For type approval typically the final, released for production, car is used for inspection and the execution of precisely defined driving manoeuvres. The main advantage of this approach is, that tests are executed under real environment conditions with the vehicle, preventing error masking. An error is masked if it is not revealed by a test due to differences in the test system in contrast to the original execution environment. For example, a simulation is an abstraction of the real world and therefore behaves differently. An error might not be detected by a test using a simulation but could be revealed in a test using the original execution environment, which is a vehicle in this case. The classic type approval approach works well for manual driven cars, where the focus was on ensuring that the mechanical parts of the system are functional safe. With the arise of Automated Driving the requirements for vehicle homologation are also increasing and include the whole E/E system, including all activities within the tasks sense, control and act. In future, considering automated operating vehicles, the type approval procedures and general inspections shall also ensure the operational safety of a vehicle entirely. However, this will increasingly be defined by software (assistance systems, comfort functions, etc.) and be more configurable during operation.
The large number of tests needed to verify an Automated Driving function of a vehicle, requires innovative virtual homologation approaches based on simulation like SIL and HIL platforms.

5.3 Challenges in Virtual Type Approval/Virtual Homologation

The term virtual type approval refers to V&V activities based on simulation techniques, which are used additionally to classic and established test methods during development and vehicle type approval. This addresses especially the needs for development of Automated Driving including the time to market requirements.
The use of simulation techniques means that inputs for the system under test or the vehicle under test are created by different tools for diverse V&V challenges. Two examples of V&V challenges are:

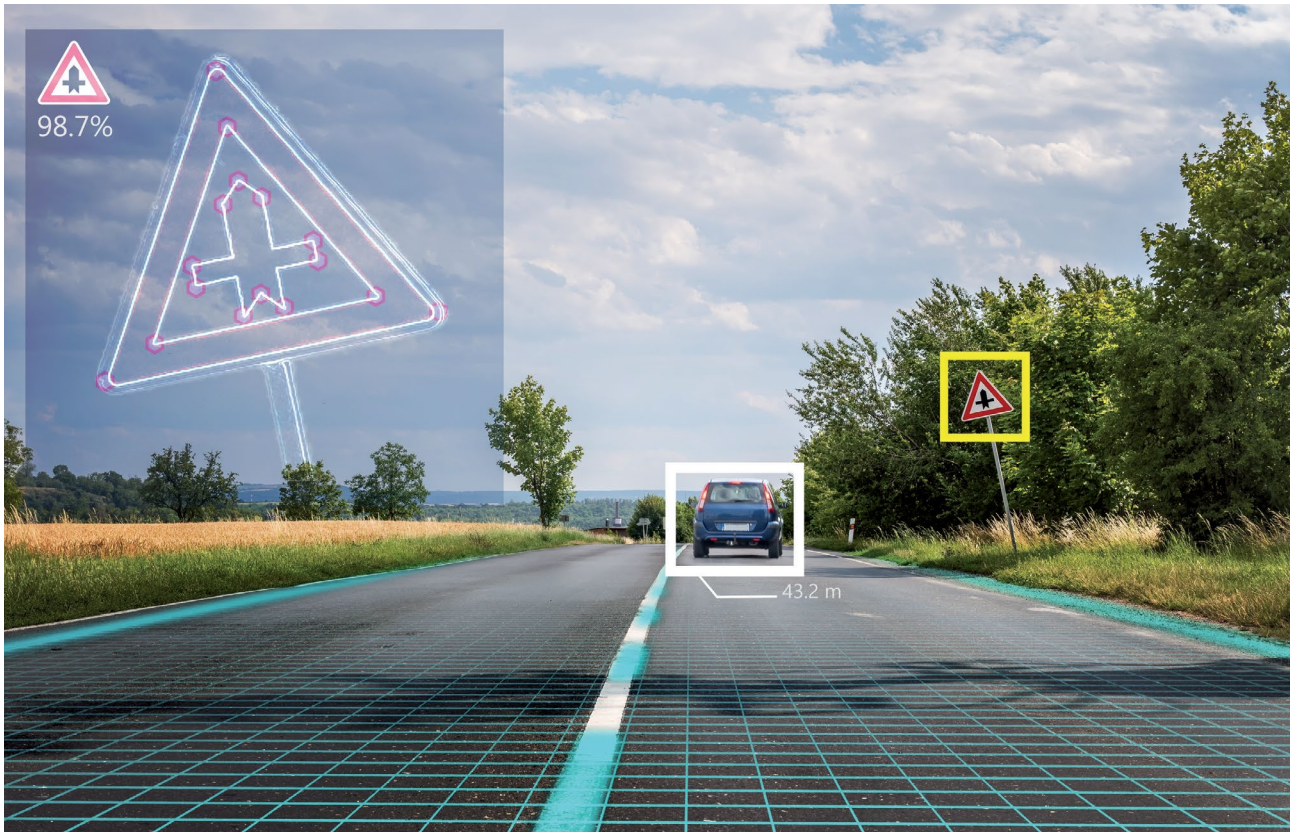
1) The simulation of cyber-attacks to systems consisting of infrastructure and vehicles
2) An environment simulation software for e.g. the sense task/SOTIF of vehicles, rather than by driving in a real environment like public roads

The use of environment simulation for the sense task raises, among others, two critical questions:

a) How to deal with error masking?
b) How can sensors with different physical measurement methods be coherently stimulated?

The first question regarding error masking was briefly discussed before and highlights the fact that a function or system under test can behave differently due to the abstractions made in the simulation. Knowing this fact, it is hard to decide if a passed test using simulation is sufficient to show that the system works under real environment conditions. This is of high importance for safety critical functions, where a wrong judgement can lead to human harm.
The second question addresses the challenge of creating sensor inputs with the same accuracy, allowing, for example, the tested perception system to recognize the simulated environment as plausible. Accuracy differences will lead, for example, to variations in the recognized object positions and sizes and might be identified as sensor error by the perception system, falsifying the test results. Consequently, to achieve the same data accuracy from an environment simulation, the underlying environment model needs to contain sufficient information for all needed sensor technologies, for which stimuli shall be generated. The reason is, that the different sensor technologies react differently to e.g. object materials, lighting and weather conditions, or structures like buildings, tunnels and bridges. Therefore, the additional sensor specific information must be explicitly defined in the model, making the creation of such a model an even more time-consuming task.
If solutions to both, the sense task and SOTIF questions stated above, can be provided, the credibility and reliability of the simulation and V&V test environment is a prerequisite for virtual type approval. For cost controlling and regression test planning for this kind of multi-party activities quality gates shall be implemented in all relevant development and V&V steps according to automotive quality guidelines from several standards.
For simulation of cyber-attacks to systems and V&V activities analogical questions with similar solutions need to be developed.

6 Summary and Outlook



Automated Driving functions raise a lot of technical questions regarding Functional Safety, Cyber Security, SOTIF, Human Machine Interfaces, testing in general and especially for type approval/homologation, which must be answered before accordingly equipped vehicles can enter the market. One of the main challenges is the harmonization of the different Functional Safety and Cyber Security standards in the company specific development processes. In these new safety and security co-engineering processes the specific analysis methods and resulting work products are aligned, leveraging their synergies to minimize the overall development effort.

A big challenge, from the technical perspective, is the V&V of Automated Driving functions and vehicles, which requires a very high number of tests. These tests cannot be performed without using novel environment simulation techniques, which raise questions about the confidence of test results, caused by the abstraction made in the underlying environment model.

These stated challenges need to be addressed in future work by both, the automotive industry and the scientific community, combining their respective strengths regarding practical implementation of development processes and tools, and profound investigations of analysis methods, simulation environments and test development.

In reaction to the identified prevailing uncertainties of the companies active in the automotive industry, especially concerning development and approval of components, systems and entire vehicles, having in mind all new challenges regarding safety and security issues for highly Automated Driving as outlined in this paper, TÜV AUSTRIA and VIRTUAL VEHICLE decided to join forces to develop novel solutions boosting Automated Driving.

About TÜV AUSTRIA and VIRTUAL VEHICLE

TÜV AUSTRIA Group

TÜV AUSTRIA is an international company with branches in more than 20 countries of the world. TÜV AUSTRIA employs about 1.600 employees.

The service competencies of the four business areas „Industry & Energy", „Infrastructure & Transportation", „Life, Training & Certification" and „Service Providers and Public" encompass the areas of testing, monitoring, certification, education and training and consulting.

TÜV AUSTRIA gives assistance to the automotive industry with development support for system safety solutions including Functional Safety, SOTIF, Cyber Security, electrical safety and further technical areas by type approvals, tests, inspections and with continuous online monitoring methods and processes.

From requirements analysis to integrated system security for ADAS, automated and connected systems, infotainment, secure transport infrastructures and e-mobility solutions, tailor-made services based on known standards or own test catalogues.

Moreover, TÜV AUSTRIA is working in several research projects amongst Automated Driving focussing on technology developments for public and urban transport, cybersecure infrastructures and the development of test regions.

Contact partner on the topic of Automated Driving:
Dipl.-Ing. Bernhard Schrammel – *bernhard.schrammel@tuv.at*

VIRTUAL VEHICLE Research Center

VIRTUAL VEHICLE is a leading international R&D center for the automotive and rail industries, located in Graz.
The center focuses on the advanced virtualization of vehicle development. This linking of numerical simulations and hardware testing leads to a powerful HW-SW system design.

VIRTUAL VEHICLE's international partner network consists of:
- 80+ international industrial partners (OEMs, Tier 1 & Tier 2 suppliers, software vendors)
- 40+ international scientific institutions

VIRTUAL VEHICLE is the largest COMET funded research center and is also active in 30+ EU-projects. Furthermore, VIRTUAL VEHICLE offers a broad portfolio of contract research for the vehicle development.

Contact partner on the topic of Automated Driving:
Dipl.-Ing. Dr. Christian Schwarzl – *christian.schwarzl@v2c2.at*

Bibliography

Sources

[1] SAE, "axonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems J3016_201401", 2014. [Online]. Available: https://www.sae.org/standards/content/j3016_201401/. [Accessed 20 6 2018].

[2] E. &. Young, "Autonomes Fahren – Die Zukunft des PKW Marktes?", 2013. [Online]. Available: http://www.ey.com/Publication/vwLUAssets/Autonomes_Fahren_-_die_Zukunft_des_Pkw-Marktes/$FILE/EY-Autopilot-2013-Praesentation.pdf. [Accessed 20 06 2018].

[3] W. Hermann, "(How) Can Safety of Automated Driving be Validated?", TU Darmstadt, 2016. [Online]. Available: https://www.fzd.tu-darmstadt.de/media/fachgebiet_fzd/publikationen_3/2016_5/2016_Wi_Wf_Ju_ViV-Symposium_Graz.pdf. [Accessed 6 20 2018].

[4] W. Curtis, "Hackers Remotely Kill a Jeep on the Highway – With Me in It", WIRED, 2015 7 1. [Online]. Available: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/. [Accessed 06 07 2018].

[5] C. M. &. C. Valasek, "A Survey of Remote Automotive Attack Surfaces", in DEF CON 22 hacking Conference, 2014.

Figures

Shutterstock (cover photo, P. 1, 2, 8, 9, 11, 12, 14, 19, 21, 24), E. & Young, „Autonomes Fahren – Die Zukunft des PKW Marktes?" (Fig. 1), VIRTUAL VEHICLE (Fig. 2, 6, 7), Shutterstock ©metamorworks (Fig. 3), ©Monika Skolimowska/dpa/picturedesk.com (Fig. 4), Shutterstock ©Tangam (Fig. 5), Shutterstock ©MSSA, ADE2013, Beate Panosch, e2dan (Fig. 8)

WhitePaper

Figure: shutterstock.com (Zapp2Photo)

TÜV AUSTRIA Group

DI Bernhard Schrammel
TÜV-Austria-Platz 1
2345 Brunn am Gebirge
Mail: *bernhard.schrammel@tuv.at*

www.tuv.at

VIRTUAL VEHICLE Research Center

DI Dr. Christian Schwarzl
Inffeldgasse 21a
8010 Graz
Mail: *christian.schwarzl@v2c2.at*

www.v2c2.at