Safety and security for automated driving

Future mobility in road and freight transport is shaped by a new quality of data, the currency and range of data as well as by a higher level of exchange of information. Information and communication systems within the vehicle as well as the connection of vehicles to other vehicles and/or with infrastructure will completely and durably relieve drivers of many driving tasks in the future.

Advanced driver assistance systems are already making automated driving possible. These systems take over driving subtasks on behalf of the driver in a wide variety of situations and alert the driver to dangers on the road. Automated driver assistance systems are the key to the individual mobility of the future.

Automation and connectivity facilitate greater safety in road transport and make an important contribution to the target of notably reducing the number of road fatalities and serious injuries (Vision Zero). They ultimately improve the quality of life by reducing the stress that traffic places upon people and the environment as well as open the door for older people and those from physical impairments to better participate in road traffic.

The Association of Technical Inspection Agencies (VdTÜV e.V.) and its members will shape this process of innovation and development for safe and secure automated driving. The issues of the vehicle's IT security and the protection of the driver/owner's data need to be of paramount importance in developing and promoting automation and connectivity in mobility. In addition, the classic environmental and safety targets of the vehicle during the type-approval process as well as when being placed on the market and into operation must also be considered. In developing these systems, it is pivotal that norms and standards are adapted to the latest state of the art in science and technology.

> **The national and international set of rules for digitally connected vehicles must be adapted and harmonised in order to promote a common European transport policy for automated vehicles and future autonomous vehicles in the connected mobility sector. Drivers need legal certainty when using assistance and/or automated systems!**

The rules of the 1968 Vienna Convention on Road Traffic still follow the basic principle that every vehicle in motion must have a driver. Technical systems which assist the driver, such as driver assistance systems or automated driving functions, must be designed in such a way that the driver can overrule or turn them off at any given time.

The provision of the Vienna Convention therefore needs to be adapted in order to facilitate the usage and authorisation in the future of highly automated and autonomous vehicles as well. To

this end, the agreement must set out the different levels of automated driving. In its present form, the regulatory framework does not provide any information upon the point of time at which the driver can hand over control of the vehicle – partially or fully – to the autonomous system. Various technical standards such as UN/ECE Regulation 79 concerning steering need to be revised. Clear, new regulations concerning the interface of human/machine are also required.

Intelligent connectivity and digitalisation inside and outside of the vehicle will play a more important role in the future. This shall ultimately contribute to an improvement in road safety. Connectivity means that vehicles communicate with one another (vehicle to vehicle – V2V) as well as with the infrastructure (vehicle to infrastructure – V2I), e.g. with traffic lights, traffic management systems or other road users. This technology, collectively referred to as "car-to-x communication", warns and informs the driver of hazardous situations along the route within fractions of a second, even if such situations are not yet visible to the driver. During highly-automated or fully-automated (autonomous) journeys, the vehicle will in such cases even independently apply its brakes or change lanes in order to circumnavigate the hazard area at a sufficient distance without the driver needing to take action. Various communication technologies can be used to provide the connectivity required for this. These include, for example:

- Standardised short distance technologies for general purposes (BluetoothTM, WiFi, wireless power, NFC, etc.)
- Technologies specifically developed to connect vehicles (IEEE 802.11p, a short distance communication method for V2V and V2I similar to Wi-Fi)
- Mobile communication (GSM, UMTS, LTE and all associated variants)

Inspection concepts and testing technologies used in the vehicle type-approval and periodic technical inspection of automated vehicles must be continuously developed further. Digitally connected transport infrastructure must be consistently and permanently operational!

Periodic inspection of vehicles

The provision on the periodic technical inspection of vehicles (Directive 2014/45/EU) needs to be revised. Vehicles must be designed in such a way that modern electronic vehicle systems can also be inspected via the electronic vehicle interface within the scope of the periodic technical inspection.

The examination criteria "type", "condition", "function" and "performance" for safety-related electronic functions must be supplemented with the criteria "IT security" and "data protection" and be clearly defined.

In order to be able to assess deviations from the approved status of the software of safety-related functions in the future, differentiated test findings for software versions, safety-related software updates and functional changes are required, among other things.

A functionality test, during which the electronic vehicle interface (on-board diagnostics) and/or future wireless interfaces are used, remains essential. At present, some vehicle manufacturers are refusing to release the diagnosis data that is to be delivered under EU Regulation 715/2007 due to ambiguously worded legislative norms. The relevant legislation must be adapted so that non-discriminatory access to all the relevant diagnosis data is possible.

Type-approval of vehicles (adaptation of Directive 2007/46/EC and Regulation (EC) No. 661/2009)

The mode of action and operation of safety-related and environment-related systems and components as well as the integrity of the vehicle software must be documented during the vehicle type-approval. Only by doing so will it be possible to make reliable statements upon road safety and environmental compatibility at a future time during vehicle inspections.

The legislation for the type-approval of vehicles needs to include requirements for concrete test procedures which describe tests of the IT security and the observance of the data protection requirements in an automated and connected vehicle.

The technical service must have access to the vehicle's software and algorithms. The transparency of the software and algorithms must be ensured at all times. Corresponding provisions should be added for a replicable test to the effect that – with standardised documentation – the functionality, interface and safety concept of all the safety and emissions-related components within the vehicle is disclosed.

This information must be provided for the periodic technical inspection and for market surveillance in order to ensure the safety and environmental compatibility of vehicles over their entire life cycle.

Digital infrastructure

The transport infrastructure necessary for the automated driving functions must be consistently and permanently operational.

All of the infrastructure installations for car-to-x communication must be permanently available and require periodic technical inspection in the future. The established principle of independent third-party testing by an inspection organisation makes an important contribution to protecting connected driving functions and improving road safety.

Trust: In digitally connected mobility, data relating to the vehicle and the vehicle owner must be protected and protection against cyberattacks must be ensured. The digital interfaces of vehicles in the future must provide secure, open and interoperable access for all market players.

As a result of a growing level of automation and interconnection of cars, data relating to the vehicle and its user must be protected and the protection against cyberattacks increased. Equal conditions, too, for all competitors with innovative data-based services are required.

The challenge is to adequately inform consumers so that they are in a position to understand the data flow and to personally decide upon the data that they wish to make accessible to be used and processed – and at what time, for what purpose, under which conditions and by which provider.

The future data processing in the vehicle has to take the principles of "privacy by design" (data protection performed by the implemented technology) and "privacy by default" (data protection being set as the default) into account. In this future, this requirement regarding the processing of data could be replaced by a highly secure communication platform which is installed in all vehicles as standard. This platform creates an interoperable security and safety standard and technologically implements the data and consumer protection of the vehicle occupants in a flexible manner. At the same time, it shall serve as the communication basis for the differing requirements and services of third parties. These requirements regarding data processing and protection must be assessed during the type-approval of the vehicle.

In addition, independent "trust centres" can be established to act as data custodians between the data owners/affected parties and authorised third parties, such as police authorities and municipalities. These trust centres shall manage, process and provide the relevant vehicle and traffic data.

It must equally be a political priority though to making publically available the social and economic potential of data. However, due to numerous uncertainties relating to the usage of data in commercial trade and the associated barriers to the free movement of data, there is currently no uniform market for data. As a result, economic, social and business opportunities cannot be pursued. Policy makers need to make sure that data can flow across borders and sectors and that data can be accessed and re-used in an optimal and secure way.

"Security by design" standards and interoperability are the prerequisites **for the digitalisation of mobility to succeed. Uniform European standards for digital connectivity need to be comprehensively defined for this purpose.**

Digital connectivity in mobility offers numerous possibilities for attacks and misuse and therefore requires uniform IT security concepts and solutions.

While today's vehicles meet the highest standards in terms of their functional safety (ABS, ESP, ACSF, etc.), too little attention is paid to the vehicle's IT security. Vehicle manufacturers usually develop their own IT security systems and mechanisms which are neither interoperable nor

sufficiently protected against misuse and manipulation. For this reason, it would make sense to specify a uniform standardised solution in the form of a communication platform in order to create a uniform and interoperable standard of security and safety in the vehicle. This communication platform would control the necessary security standards (including those relating to access and/or authorisation and encryption) and, in addition, the flow of information in the vehicle. This would allow manipulation and remote attacks on the vehicle – particularly those on safety-related subsystems – to be detected, reported/stopped and prevented.

Driving training and testing in the future must take the increasing number of modern assistance systems in vehicle into account in the curricula. Drivers must be proficient in all the basic driving skills at all times even without the aid of automated driving functions!

Intelligent connected road traffic and automated driving functions can cover the increasing demand for mobility and transport. In view of an ageing society, connectivity and automation make individual mobility easier and thereby also make it easier for people to participate in social life despite possible age-related physical deficiencies.

The increasing usage of assistance systems in vehicles dictates that both the training of drivers as well as the theoretical and practical driving test must be continually adapted to developments. In connection with this, training and testing requirements need to be developed and evaluation and decision-making criteria based on these must be defined. Here, novice drivers must – at least until vehicles are actually active on the roads in a driverless mode – be put in the position of being able to steer highly-automated vehicles and also, in case of need, be proficient in the essential driving skills without the aid of assistance systems.

A central aspect of preparing novice drivers in the future will be to convey the skills that enable the driver to regain full awareness of the driving situation and have stable control of the vehicle after the deactivation of the driving functions.

Drivers who have long held a driving license should also be able to safely control both highly-automated vehicles as well as those without any – or with only limited – assistance systems for the rest of their life.

Facilitate automated driving using real test drives

The electronics in modern vehicles are continually taking on more and more functions in the handling of complex vehicle situations. With each new generation of vehicles, the level of connectivity between sensors, drive technology (actuator technology) and electronic control devices is increasing.

Test drives under real conditions on trunk roads and in an urban environment are therefore essential as an addition to bench tests and simulations. Highly complex driving conditions and situations arise here which cannot be tested under laboratory conditions. Furthermore, in-depth findings on the durability and reliability of systems and components used for automated driving

can be gained from real test drives. Corresponding test specifications for real test drives and capacities for bench tests in a laboratory setting need to be further developed and expanded by using the latest scientific and technological knowledge.