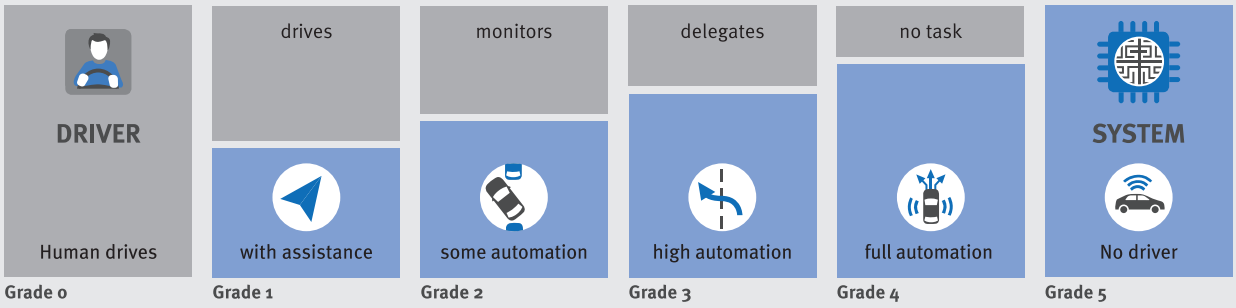
AUTOMATED AND CONNECTED DRIVING NEEDS TO BE REGULATED

Driverless vehicles communicating between one another and with their environment? It may sound like science fiction, but is already being trialled – and will be part of everyday life before long. For consumers, automated and connected driving promises a more comfortable, more flexible, and far safer way of getting from A to B; but the downside of connected driving is that traffic and driving data will be collected and analysed.

In 2014, the European Commission's Directorate-General for Mobility and Transport – as well as the German Federal Ministry of Transport and Digital Infrastructure (Bundesministerium für Verkehr und digitale Infrastruktur, BMVI) – moved early and created the so-called C-ITS platform (in Germany the "Automated Driving Round Table"), two stakeholder groups working on connected driving, to investigate the potential of this development. Participants included representatives from national, regional and local authorities, the car, telecommunications and insurance industry, service providers, user representatives and academia. Working groups have been set up to discuss a range of challenges such as how to go about authorising technology, who is liable for it, and where further research is required. The first phase of the C-ITS platform concluded in January 2016 with a report[1].

On top of the overall technological framework, there are also important legal issues which need to be solved before highly automated, connected vehicles can take to the streets. Road traffic law will need to be adapted to situations in which autonomous systems have taken over full control of vehicles.

LEVELS OF VEHICLE AUTOMATION



Source: Classification of levels of automation as produced by the Federal Highway Research Institute, Bundesanstalt für Straßenwesen (BASt)

VZBV'S POSITION

Limiting data snooping in cars: In the era of connected transport, fundamental principles of consumer protection and data privacy are crucial. There must be genuine transparency and high levels of data protection. Carmakers and dealerships must, together, be under a legal obligation to inform car buyers comprehensively about which data is generated how, for what reason is it collected, and where it is stored. Consumers must be told who has access to this data and for how long it will be stored before deletion. A holistic approach is needed for data protection and data security from the moment the car is licenced all the way through subsequent regular vehicle inspections.

Defining legal liability: Law must clarify that a driver who delegates the task of manoeuvring their vehicle to an autonomous system is no longer responsible. Drivers must not be prosecuted neither under criminal law nor be liable under civil law for driving errors which occur in highly automated modes of driving. A precondition must thus be the documentation of who is driving the vehicle and when. For vehicles no longer requiring driver involvement liability as such will have to be rethought completely as, in this situation, the driver becomes a user. Discussion is needed to determine whether manufacturers, operators, or a wholly new legal person must be held responsible for errors.

FACTS AND FIGURES

A representative survey commissioned by vzbv revealed that a majority of consumers in Germany is unaware that a new car comes with up to 70 control devices which collect data.[2]

There are already several new cars which are equipped with functions for autonomous driving: these vehicles can automatically avoid others, apply brakes independently, or park themselves.

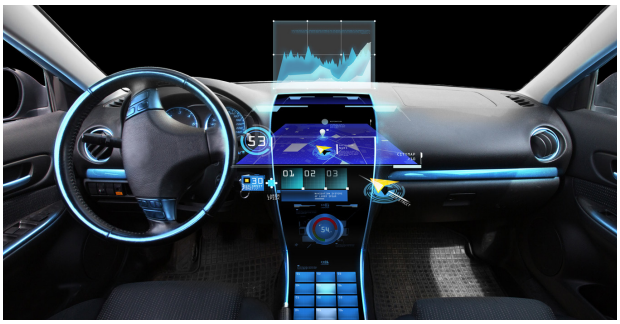
Google is testing its own self-driving cars in California and Texas and has, since 2015, also been testing them in everyday traffic. The German Federal government, too, has set up a digital motorway testing area to test connected and automated driving on the road.[3]

In February 2016, a Google self-driving car steered straight into the front of a bus. For the first time, the corporation blamed its software for the collision.[4] Automated driving means placing a huge amount of trust in the developers behind the technology.

A majority of consumers in Germany is sceptical of connected cars, as showed by a survey commissioned by vzbv. 63 per cent are concerned about liability issues, 62 per cent about data protection.[5]

A survey carried out by vzbv showed that 80 per cent of consumers in Germany see hacking of automated vehicles from outside as the greatest threat to the protection and security of their data.[6]

EVERYDAY TRANSPORT IN 2035



Vehicles will soon have a variety of functions which go far beyond moving people and goods from one place to another. Kitted out with networking software, the cars of tomorrow will automatically select the most efficient route while turning on the heating at home on the way back and offering mobile office space. The following scenarios could be utterly unremarkable by 2035.

Scenario 1 In city centres, the only vehicles allowed are autonomous, networking electric cars, trucks, and busses; apart from that, only bicycles and pedestrians are permitted. Most cars on the road now are part of either company or car-sharing fleets (bookable by users); other vehicles are part of the municipal transport infrastructure. Individual motorised travel has otherwise become a luxury by toll rings drawn around urban centres.

Scenario 2 Outside of cities, too, public transportation services consist of self-driving shuttles, with various levels of comfort and flexibility according to the price the user pays. Depending on the route and distance involved, users choose between road and rail; sleeping pod vehicles whisk people off on holiday overnight.

Scenario 3 On motorways, completely autonomous and connected vehicles share the lanes with highly-automated and partially automated cars. In the slow lane, up to ten trucks are connected into convoys, following the speed set by the first and braking in unison. For vintage vehicles, motorways are only accessible in exceptional cases following prior authorisation.

Before any of the scenarios sketched out above comes true, there is a broad range of questions which need to be answered. Privacy, data security and the safety of users must be prioritised. Opportunities for society as a whole and for individuals must regularly be weighed up against the risks.

1 http://ec.europa.eu/transport/themes/its/doc/c-its-platform-final-report-january-2016.pdf
2 TNS Emnid, Digitalisierung des Verbraucheralltags, Oktober 2014
3 http://energyload.eu/elektromobilitaet/elektroauto/google-car-tests-bei-nassem-wetter-autonomes-fahren-kirkland/
4 http://www.zeit.de/mobilitaet/2016-03/google-auto-selbstfahrend-unfall-technik
5 TNS Emnid, Sorgen beim automatisierten Fahren, August 2015
6 http://www.zeit.de/mobilitaet/2016-03/google-auto-selbstfahrend-unfall-technik

Verbraucherzentrale Bundesverband e.V. (vzbv)
Federation of German Consumer Organisations
Rudi-Dutschke-Straße 17, 10969 Berlin – Germany
Phone +49 30 258 00-0

mobilitaet@vzbv.de
Responsible for the content:
Klaus Müller, vzbv Executive Director
Copy and Design: construktiv GmbH
Infographic, p. 1: vzbv/INFOGRAFIK PRO GmbH,

verbraucherzentrale Bundesverband