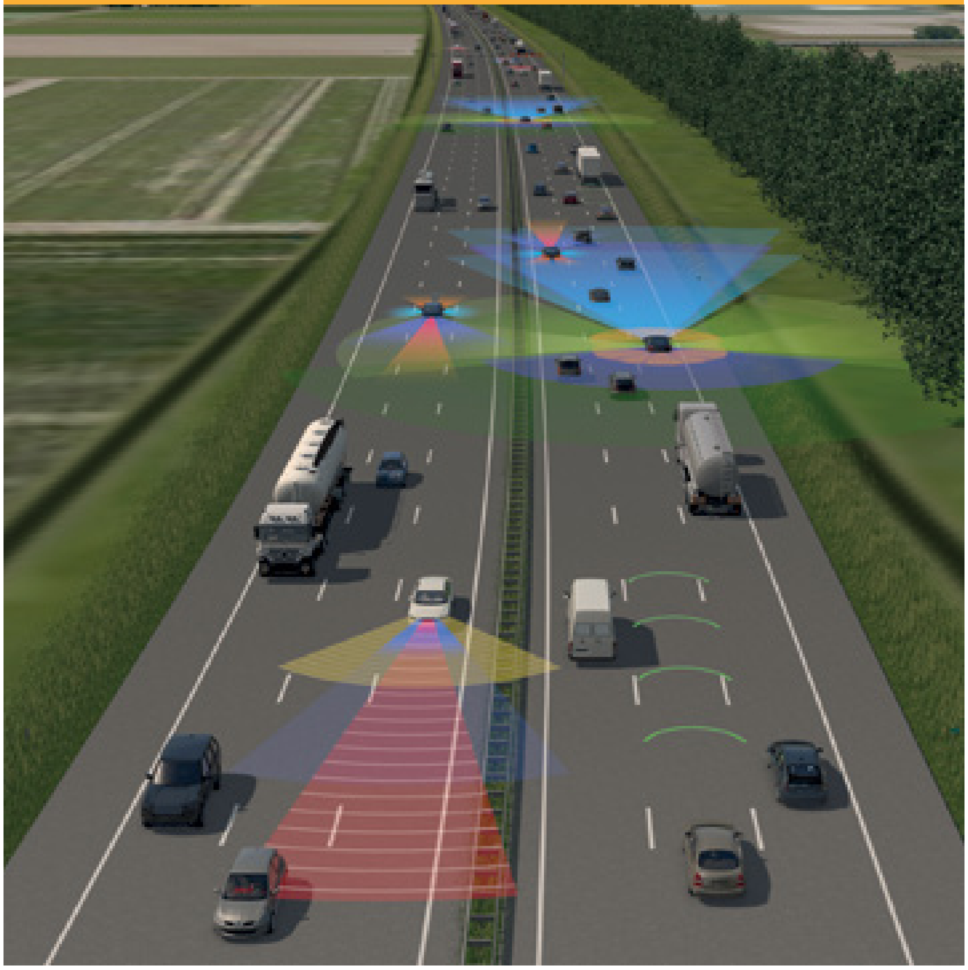
DUTCH
SAFETY BOARD

# Who is in control?

## Road safety and automation in road traffic



# Who is in control?

## Road safety and automation in road traffic

*The Hague, November 2019*

*Photo cover: Dutch Safety Board*

Content
Considerations
Summary
Recommendations
Abbreviations
1 Introduction
2 Reference framework
3 Managing safety risks
4 Bottlenecks in the safe introduction and deployment of ADAS
5 Bottlenecks in monitoring and adjustment
6 Conclusions
7 Recommendations
References
Appendices

## The Dutch Safety Board

When accidents or disasters happen, the Dutch Safety Board investigates how it was possible for these to occur, with the aim of learning lessons for the future and, ultimately, improving safety in the Netherlands. The Safety Board is independent and is free to decide which incidents to investigate. In particular, it focuses on situations in which people's personal safety is dependent on third parties, such as the government or companies. In certain cases the Board is under an obligation to carry out an investigation. Its investigations do not address issues of blame or liability.

|  |  |
|---|---|
|  | **Dutch Safety Board** |
| Chairman: | J.R.V.A. Dijsselbloem<br>M.B.A. van Asselt<br>S. Zouridis |
| Secretary Director: | C.A.J.F. Verheij |

Visiting address:
Lange Voorhout 9
2514 EA The Hague
The Netherlands

Postal address:
PO Box 95404
2509 CK The Hague
The Netherlands

Telephone: +31 (0)70 333 7000

Website: safetyboard.nl
E-mail: info@safetyboard.nl

N.B. This report is published in het Dutch and English language. If there is a difference in interpretation between the Dutch and English version, the Dutch text wil prevail.

# CONTENT

# CONSIDERATIONS

### Safer cars thanks to innovation

The history of the car is one of technological innovation. As a consequence, over time, cars have become more reliable, more comfortable and safer. Partly thanks to such innovations as crumple zones and airbags, road safety has improved drastically since the 1970s. Over the past few years, however, the improvement in road safety has stagnated: every year, there are more than 600 deaths on the roads in the Netherlands and around 21,000 serious injuries. In the face of this worrying situation, both national and European governments have announced the ambition of 'zero deaths' on the roads by the year 2050, starting with a reduction to not more than 500 road fatalities in 2020. The expectation is that innovation - and more specifically automation - will make a contribution in the form of advanced driver assistance systems (ADAS) such as emergency braking systems and adaptive cruise control.

### Fundamental change in the character of the car

It is important to realize that modern cars equipped with ADAS are incomparable in technical terms with their predecessors of just a few decades ago. New cars can already take over numerous tasks from the driver, for example steering, braking and accelerating. The ADAS in fact carry out these actions on the basis of their own observations and their own decisions, coordinated by algorithms. Vehicles of this kind are equipped with so much hardware and software that they are effectively computers on wheels. This fact has far-reaching consequences for drivers, other road users and the infrastructure. It effectively implies a fundamental change in the character of the car: a transformation which, as is the case for any innovation, delivers not only progress but also new safety risks.

### Driving is becoming more difficult and easier at the same time

Automation means that relatively simple tasks can be taken over and executed at a constant and higher level of safety. The difficult tasks (for the time being tasks that are too difficult to solve with automation) are left to human drivers. Automation is changing the human task because drivers are required to remain 'constantly alert' just in case the computer does not know what to do, or intervenes wrongly. This represents an additional difficulty since automation in fact reduces the level of alertness. In just a few short seconds, drivers are required to understand that intervention is necessary, before making the adequate response. After all, the margins on the roads are minimal. The outcome is a paradoxical situation in which ADAS that are intended to make the life of the driver easier in fact make it specifically more difficult.

Content
Considerations
Summary
Recommendations
Abbreviations
1 Introduction
2 Reference framework
3 Managing safety risks
4 Bottlenecks in the safe introduction and deployment of ADAS
5 Bottlenecks in monitoring and adjustment
6 Conclusions
7 Recommendations
References
Appendices

### The autonomous car is still a long way off

When the discussion turns to the automation of cars, the focus is often on the future vision of autonomous cars, in which the driver if superfluous. The car drives itself, while the people it is carrying are busy with something entirely different. This distant-future vision appeals to the imagination of policy makers, engineers, town and city planners and philosophers. But we are still a long way from reaching that stage. Certainly in built-up areas where cars and vulnerable traffic participants come together, the future with fully autonomous cars is still a long way away, if it can ever in fact be achieved.

### Urgent attention for the current hybrid situation

Over the next few years, we will find ourselves in a hybrid situation in which vehicles are controlled both by humans and machines. This is a risky combination because of the growing interaction between human and vehicle, the extent of which can also vary depending on the type of ADAS and can further change over time, as a result of software updates. In a vehicle equipped with ADAS, the driver is no longer continuously actively driving, but increasingly fulfils the role of 'process controller'. On occasion, the system surprises the driver with sudden interventions, or indeed unexpectedly failing to intervene. 'Who is in control?' then literally becomes a crucial question.

### Towards responsible innovation

The automotive industry, governments and experts switch to 'fast forward' in respect of a distant future with autonomous cars. To take control in the current hybrid situation, it is vital that the automotive sector achieves a turnaround, towards responsible innovation. The central focus of that innovation must be that road safety is demonstrably improved. In other words, manufacturers must assess the risks of new innovations and be transparent about the outcomes. Increasingly, manufacturers must take account of the role of humans and the interaction between humans and machines. In addition, the learning capacity of the sector must be improved by learning from incidents and accidents and by actively including the experiences of users in future developments. The Dutch Safety Board is not convinced that all manufacturers will be able to achieve this turnaround of their own volition and considers it essential that legislation be introduced to embed responsible innovation in practice. It is vital that these tasks be not exclusively the role of manufacturers but that the government also considers its own role and guarantees the public interests that are at stake because of automation in road transport.

### Pioneering role for the Netherlands

The Netherlands is well positioned to play a pioneering role when it comes to innovation in road transport. The Netherlands is an active proponent of innovation in general and responsible innovation in particular, in international forums. The Netherlands is therefore ideally positioned to call for international regulations for responsible innovation in the automotive industry. In this way, the potential contribution of innovation to road safety can be utilized to the full, in the interests of zero road traffic fatalities by 2050.

# SUMMARY

As the name suggests, Advanced Driver Assistance Systems (ADAS) are systems that assist the driver in carrying out the primary driving task. ADAS observe the environment using sensors and are able to take over control of speed or driving direction, subject to the responsibility of the person at the wheel. Systems of this kind are also able to warn the driver in situations that the system considers dangerous.

Automation in road traffic can help improve road safety, but also engender new road safety risks. On the basis of accident investigations, a literature review and discussions with experts, the Dutch Safety Board has identified a number of types of new risks that are not yet sufficiently recognized or managed. When they are placed on the market, ADAS are not yet fully mature. This means that following permission for use on public roads, they undergo further development. Together with the lack of knowledge among drivers, situations in which drivers fail to understand why the vehicle responds or indeed fails to respond in a particular way can quickly arise. In addition, drivers in vehicles fitted with ADAS play a different role than drivers in conventional cars, namely the role of operator. The range of tasks that this role engenders creates the risk that drivers become less alert and react too slowly. Automation makes us less alert. At the same time, in legal terms, the driver remains responsible and liable, even if the vehicle intervenes and/or if the driver is driving under the assumption that the vehicle is in fact driving itself. This is a point of conflict and results in risks.

The advances in automation also mean that cars with ADAS have increasingly become computers on wheels. As a consequence, the risks inherent in computers have been increasingly introduced to cars fitted with ADAS. These include cybersecurity risks and the risk that essential safety and security updates are not carried out. Updates themselves can in fact represent a specific risk, if they change the functioning of the ADAS and as a consequence the driving behaviour of the vehicle, without the driver being fully aware of this change.

**Responsible innovation**

In all its investigations, the Dutch Safety Board operates a reference framework. This framework lays out the standards with which the various stakeholders are expected to comply, in order to manage safety risks in a given field. Essentially, this reference framework is a question of responsible innovation.

To arrive at responsible innovation, right from the start of the design phase, it is essential that safety issues be taken into account. It is also vital that attention is not focused exclusively on the safety of the technological innovation itself, but also the combination of technology and the user. We must prevent innovation being seen as a purely technological issue: the human aspect is certainly just as important. This in turn means that manufacturers of any new technology have a responsibility towards the users to inform them of the risks.

New risks must be estimated in advance and mitigated as far as possible. Safe innovation is a gradual process with constant fine tuning on the basis of monitoring and evaluation. Manufacturers must demonstrate that their innovations are safe (transparency) and data about accidents must be made available. The government must be willing and prepared to intervene whenever the use of a new technology on balance entails potential unsafe situations.

Based on this framework, the Dutch Safety Board has identified bottlenecks in terms of design, policy, regulation and supervision, data availability and learning capacity.

### Design

Manufacturers introduce new systems because technology makes it possible and to make their cars more attractive for their customers. Road safety is not a basic principle in the design process right from the start and insufficient account is taken of the driver who is required to operate the innovation. Moreover, vehicles today are not designed in such a way that safety is maintained throughout their lifecycle. The exchange of knowledge and transparency are not common practices within the sector.

### Policy

Dutch and European policy are aimed at encouraging and indeed making the installation of ADAS obligatory. This is based on the ambition of reducing the number of road traffic accident victims. However, there is no elaborated vision on the required level of safety in relation to the desired extent and direction of innovation. There are no systematic risk analyses and no determination has been made of how the risks can be mitigated or what is needed to arrive at mitigating measures. Furthermore, within the policy, there is insufficient focus on the current generation of systems. Government attention is above all aimed at the distant future in which vehicles may be able to operate fully autonomously. Current measures from the Ministry of Infrastructure and Water Management aimed at filling the knowledge gap among drivers are a step in the right direction, but are not sufficiently binding.

### Regulation and supervision

In many areas, legislation follows social developments. In that sense, it is no surprise that technological changes in the automotive industry are outpacing the related regulations. However, the problem is greater than simply a question of phasing. The rules are lagging behind in respect of a number of safety aspects - for example human factors and the training of users - because manufacturers and government simply pay less attention to these aspects. Regulations are not geared to the fact that following permission for use on public roads, cars are subject to further changes as a result of updates. Vehicle regulations do state that new systems are not permitted to make traffic 'less safe', but in no way specify how the safety level of ADAS or other innovations can be assessed. As a result, there is no monitoring of the way in which manufacturers estimate risks and consider scenarios; systems are approved while their effect on road safety is unknown and there is no systematic monitoring of the effects of these innovations.

### Black box

At a whole number of levels, ADAS are something of a 'black box'. Following an accident, the police are often unable to access the data and there is no knowledge at all of which cars are equipped with precisely which ADAS and whether the systems were activated. It is also unclear for all types of ADAS what effect they have on road safety. There is a lack of sound monitoring and evaluation following the introduction of these new technologies. The monitoring of accidents involving ADAS could be integrated in regular accident investigations. One positive development in this connection is that from now on Rijkswaterstaat (Directorate-General for Public Works and Water Management) has commissioned the SWOV Institute for Road Safety Research to investigate fatal accidents on national highways. This offers a basis for investigating the role of ADAS in the occurrence of fatal accidents, thereby boosting overall learning capacity.

### Learning capacity

Manufacturers undertake no systematic investigation into accidents. As a consequence, they are unable to learn from any shortcomings in their products. Any accident investigations that are carried out are very fragmented. A proportion of the risks related to ADAS are only revealed in practice, no matter how carefully they are designed and tested in advance. The fact that actual practice functions as a 'living lab' is an unavoidable consequence of any innovation, but innovation must nonetheless take place in a responsible manner. It is vital that the industry investigates the potential lessons from accidents and near accidents as broadly as possible, so that those lessons can be learned by the entire automotive industry.

### Uncertain effect on road safety

Both the Dutch government and the European Commission are striving to achieve zero road fatalities by 2050. To achieve this ambitious target, much hope rests on technological developments in general, and vehicle automation in particular. However, the introduction and use of ADAS leads to new risks, many of which are as yet insufficiently recognized, monitored and managed. ADAS can potentially have a positive influence on road safety, but as yet there are no guarantees that that potential will be truly fully utilized.

# RECOMMENDATIONS

*To the automotive manufacturers and the OICA and ACEA umbrella organizations:*

1. Demonstrate that the development and introduction of ADAS is taking place according to the principles of responsible innovation.

*To the BOVAG and RAI Association:*

2. Ensure that BOVAG members fully instruct their customers on the possibilities and limitations of their vehicles equipped with ADAS. And make sure that BOVAG members are able to do this.

*To the Minister of Infrastructure and Water Management:*

3. Take the initiative within the UNECE to place human factors and responsible innovation on the agenda.

4. Support the initiatives of Euro NCAP to make human factors and consumer information about ADAS an integral part of the vehicle safety assessment (Euro NCAP star system).

5. Improve the possibilities for learning from road traffic accidents in general and the role of ADAS in particular, and take measures aimed at improving road safety on the basis of the study results.

6. Within the European Commission, argue that vehicle regulations must tie in with the current generation of ADAS (SAE level 2 and lower). Responsibility for demonstrating that new ADAS improve safety must be placed clearly in the hands of the manufacturers. Moreover, attention should be focussed on the introduction of requirements relating to human factors, user training, access to data from ADAS following accidents and accident investigation by manufacturers.

J.R.V.A. Dijsselbloem
Chairman Dutch Safety Board

C.A.J.F. Verheij
Secretary Director

Content
Considerations
Summary
Recommendations
Abbreviations
1 Introduction
2 Reference framework
3 Managing safety risks
4 Bottlenecks in the safe introduction and deployment of ADAS
5 Bottlenecks in monitoring and adjustment
6 Conclusions
7 Recommendations
References
Appendices

# ABBREVIATIONS

| | |
|---|---|
| AAA | American Automobile Association |
| ABS | Anti-lock Braking System |
| ACC | Adaptive Cruise Control |
| ACSF | Automatically Commanded Steering Functions |
| ACEA | European Automobile Manufacturers’ Association |
| ADAS | Advanced Driver Assistance System(s) |
| ADASS | Advanced Driver Assistance Steering Systems |
| AEBS | Advanced Emergency Braking System, also called Autonomous Emergency Braking System or Automatic Emergency Braking System |
| AI | Artificial Intelligence |
| ANWB | Royal Dutch Touring Club (Automobile Association) |
| ASS | Autonomous Steering Systems |
| Auto-ISAC | Automotive Information Sharing & Analysis Center |
| CBR | Central Office for Motor Vehicle Driver Testing |
| CIECA | International Commission for Driver Testing |
| CSF | Corrective Steering Functions |
| CSMS | Cyber Security Management System |
| CS/OTA | Cyber Security/Over The Air (updates/communication) |
| DL | Deep Learning |
| DSSAD | Data Storage System for Automated Driving |
| ECU | Electronic Control Unit |
| EDR | Event Data Recorder |
| ENISA | European Union Agency for Cybersecurity |
| ESC | Electronic Stability Control |
| ETSC | European Transport Safety Council |
| Euro NCAP | European New Car Assessment Programme |
| EVA | Equality for Vehicle Advancement |
| FCW | Forward Collision Warning |
| FOT | Field Operational Test |
| GDPR | General Data Protection Regulation |
| GRVA | UNECE Working party for Automated/Autonomous and Connected Vehicles |
| GSR | General Safety Regulation |
| HMI | Human Machine Interaction |

| | |
|---|---|
| IenW | Ministry of Infrastructure and Water Management |
| ISA | Intelligent Speed Assistance or Intelligent Speed Adaptation |
| ISO | International Organization for Standardization |
| LDA | Lane Departure Avoidance, also called Lane Departure Alert or Lane Departure Assistance |
| LDW | Lane Departure Warning |
| LKA | Lane Keeping Assist |
| LKS | Lane Keeping System |
| ML | Machine Learning |
| MoT | Periodic Vehicle Inspection |
| NHTSA | National Highway Traffic Safety Administration |
| NTSB | National Transportation Safety Board |
| OEDR | Object and Event Detection and Response |
| OTA | Over-The-Air (communication or update) |
| RDW | National Vehicle and Driving Licence Registration Authority |
| RWS | Rijkswaterstaat is the Directorate-General for Public Works and Water Management |
| SAE | Society of Automotive Engineers |
| SWOV | Institute for Road Safety Research |
| TACC | Traffic Aware Cruise Control, synonym for ACC |
| TCU | Telematics Control Unit |
| TNO | The Netherlands Organization for Applied Scientific Research |
| UNECE | United Nations Economic Commission for Europe |
| V2I | Vehicle to Infrastructure (communication) |
| V2V | Vehicle to Vehicle (communication) |
| V2X | Vehicle to everything (communication) |
| VDLF | Vehicle Drivers' License Framework |
| VSSF | Vehicle Safety and Security Framework |

Content
Considerations
Summary
Recommendations
Abbreviations
1 Introduction
2 Reference framework
3 Managing safety risks
4 Bottlenecks in the safe introduction and deployment of ADAS
5 Bottlenecks in monitoring and adjustment
6 Conclusions
7 Recommendations
References
Appendices

# 1 INTRODUCTION

## 1.1 Road safety and automation

Road safety in the Netherlands has improved considerably since the 1970s, but in recent years that trend has reversed. Since 2010 there has been an average of more than 600 fatalities and some 21,000 severe injuries per year, while in 2018 there were 678 fatalities: the highest number since 2010.[1] This is in spite of the ambition of the Dutch government and the European Commission to achieve zero road fatalities by 2050.[2, 3] Automation is seen as one of the means to improve road safety[4, 5] , which is why the EU Member States, the European Commission and the automotive industry are all committed to the development of automated vehicles.[6] The first step in this process is the introduction of Advanced Driver Assistance Systems (ADAS), and this technology is developing rapidly. But the introduction and implementation of new technologies can also entail new risks. In fact, these risks have already manifested in practice: ADAS played a role in several recent accidents on public roads.

In light of these developments, car manufacturers and other stakeholders are faced with the challenge of maximizing the opportunities and minimizing the risks so that the innovations can make a real contribution to improving road safety. The automation in road traffic also affects the regulatory and supervisory role of the government and calls for a different interpretation of these responsibilities. To what extent are the parties responsible for road safety aware of the new risks associated with the introduction and deployment of ADAS? A characteristic of the current generation of technology is that the systems are continuously under development, including in vehicles that are already on the road. This dynamism is characteristic of the ICT systems which are increasingly being used in vehicles. The concern is that the parties involved are not paying sufficient attention to fundamental changes in the characteristics of vehicles (and road traffic), and that existing legislation and regulations may no longer sufficiently guarantee safety.

[1] SWOV, *Factsheet Verkeersdoden in Nederland*, 2019.
[2] Ministerie van IenW et al., Veilig van deur tot deur; *Het Strategisch Plan Verkeersveiligheid 2030: Een gezamenlijke visie op aanpak verkeersveiligheidsbeleid*, 2018.
[3] Europese Commissie, *Annex 1: Strategic Action Plan on Road Safety,* in Europe on the move; Sustainable Mobility for Europe: safe, connected and clean, 2018.
[4] ETSC, *Prioritising the safety potential of automated driving in Europe*, 2016.
[5] Minister van Infrastructuur en Milieu, *Kamerbrief 31305 Mobiliteitsbeleid*, 2014.
[6] EU-lidstaten, *Declaration of Amsterdam; Cooperation in the field of connected and automated driving*, 2016.

Technical interventions over the years have made a significant contribution to the reduction of traffic accident victims. Familiar examples are seat belts, crumple zones, rigid occupant compartments, airbags, anti-lock brakes (ABS) and Electronic Stability Control (ESC). The first four are forms of passive safety, providing more protection to car occupants in case of an accident. According to the car manufacturers, there is little room for further development of these passive safety technologies, because this can only lead to heavier cars. Although these would provide better protection for the car's occupants, they would pose a greater threat to the safety of other more vulnerable road users and produce higher emissions. ABS and ESC are forms of active safety that intervene in the vehicle's control systems in order to prevent accidents or limit their consequences. Car manufacturers still see scope for the further development of active safety in the form of ADAS. Passive safety measures typically only affect the car itself, while many active safety measures also involve far-reaching interaction with the driver and the road infrastructure. The deployment of ADAS to increase active safety will therefore require a different approach.

## 1.2 Aim and research questions

The Dutch Safety Board aims to contribute to improving road safety in the Netherlands in the dynamic environment that is road traffic. To fulfil its role, the Board must respond to evolving safety issues such as those that arise from the automation of road traffic. The aim of this theme investigation is to improve road safety by providing the parties responsible for road safety with insight into ways they can identify and manage the new risks that follow from the introduction and deployment of ADAS. The research questions below are central to this study.

**Research questions**

- How do users, the automotive industry, sector parties and the government manage the risks associated with the introduction and deployment of Advanced Driver Assistance Systems (ADAS)?
- To what extent can this risk management be improved?

The investigation focuses on the management of the risks associated with the introduction and deployment of ADAS in vehicles by manufacturers, suppliers, importers, dealers, regulators, legislators, interest groups, etc. This thus concerns risk management, rather than the risks themselves. The risks described in this report mainly serve as examples to illustrate the various parties' approaches to this risk management; the report does not provide a comprehensive overview of all risks. This is important, because this field of study is still only in the early stages of development, and so new risks will gradually be identified as the technologies evolve.

## 1.3 Working method

The investigation described in this report comprised four phases. After an exploratory phase (phase 1), a study was conducted into new forms of safety risks and the way they are managed (phase 2, first research question). To this end, six accidents were investigated, a large number of interviews were conducted (both formal and informal), a literature review was carried out and discussions were held with subject-matter experts. Because this is a thematic investigation, the range of risks described is broader than those identified in the accidents. The accidents illustrate the kinds of risks involved and do not comprise a comprehensive overview of all the types of ADAS accidents that can occur. The investigation focussed on risk management, and is hence not a risk assessment. New risks will be identified in the short term as the technologies develop.

Most of the accidents described involved Tesla cars, which is explained by the fact that Tesla is at the forefront of ADAS implementation and builds this technology into all its cars as standard. ADAS is implicated in accidents involving Teslas more often than in other makes of car, as a result of which the latter are reported less frequently to the Dutch Safety Board. The accidents described in this report are therefore not a representative sample of accidents in which ADAS plays a role.

To answer the second research question, a reference framework was drawn up (phase 3) and used to identify bottlenecks for the safe introduction and deployment of ADAS (phase 4).

More information about the working method can be found in Annex A: Explanation of the investigation.

## 1.4 Terms of reference and definitions

This section defines a number of key concepts in the investigation. These key concepts simultaneously comprise the terms of reference.

Automation in road traffic is a broad concept which covers a wide range of developments (see Figure 1) that may involve both vehicles and the infrastructure they use. This investigation focuses on the automation of the primary driving task.

**Automation of the primary driving task**
The primary driving task involves the longitudinal and lateral control of the vehicle (i.e. steering, accelerating and braking). In case of partial or full automation of the primary driving task, the driver is supported in the execution of the driving task, or the driving task is taken over completely (permanently or temporarily).

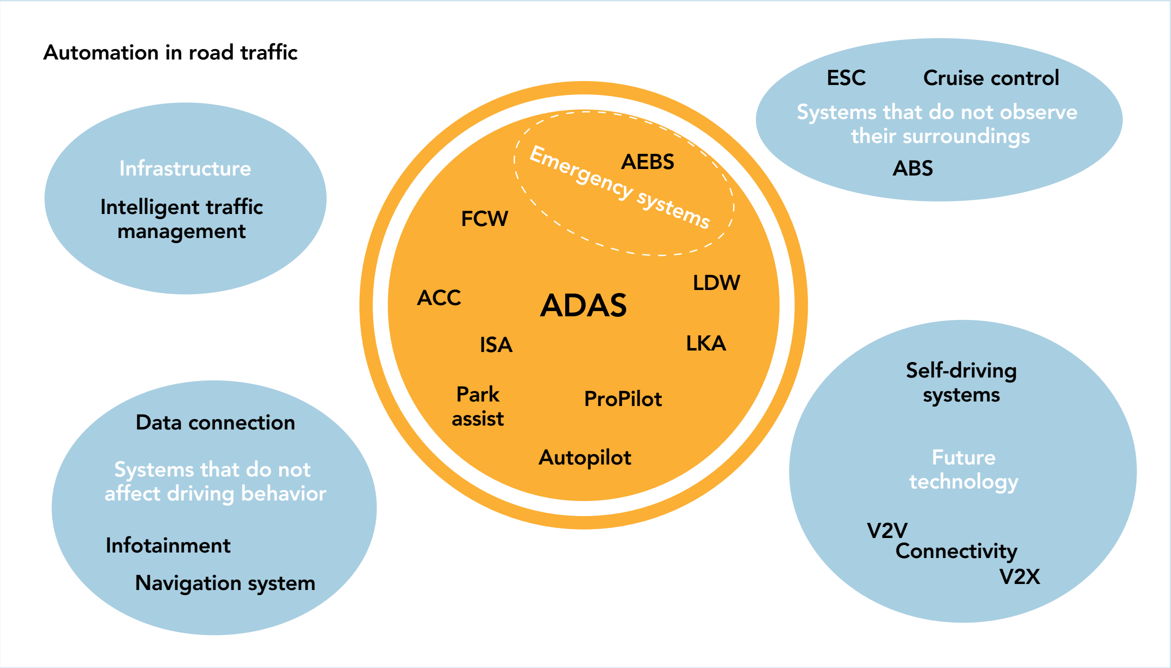


*Figure 1: The investigation focuses on the current generation of ADAS (orange circle). Other aspects of road traffic automation fall outside the scope of this report.*

*ADAS*

Automated systems in vehicles assist the driver, based on observations of the environment. These systems can provide the driver with information and warnings about hazardous situations. Furthermore, they can also take over control of the speed and/or direction of the vehicle. These automated systems are known as Advanced Driver Assistance Systems (ADAS). An example of an ADAS is Lane Keeping Assist (LKA)[7]. This system is intended to prevent the vehicle from unintentionally leaving a road lane and can intervene automatically with a steering correction. It is also known as Lane Departure Avoidance (LDA). A more far-reaching form of Lane Keeping Assist is Lane Centering, whereby the car is continuously kept in the middle of the lane. Lane Departure Warning (LDW) does not intervene, but warns the driver if the car is about to leave the lane unintentionally. Another example is the emergency braking systems, which were introduced around 2010. An Advanced Emergency Braking System (AEBS) can temporarily take over control of the vehicle in order to apply the brakes to prevent a collision, for example with the vehicle in front, a cyclist, a pedestrian or any other object. Forward Collision Warning (FCW) produces only a warning of an imminent collision.

[7] There are different types of lane assistance systems on the market, There are many different names and classifications (see box on diversity ADAS in section 3.3, appendices D.4 and E.4), so it is not always clear which system is involved. Therefore, in this report, all these systems are referred to as Lane Keeping Assistance (LKA).

**Definition of ADAS**
Advanced Driver Assistance Systems (ADAS) support the driver in performing the primary driving task. These systems observe their surroundings using sensors and can take over control of the speed and/or direction of the vehicle under the responsibility of the driver. Such systems can also alert the driver to situations that the system estimates to be dangerous.

With this definition, the Dutch Safety Board places the emphasis on the driver. This is broadly the same definition used by the ADAS Alliance[8] but different to the definitions used by the European Automobile Manufacturers' Association (ACEA) and the Society of Automotive Engineers (SAE).[9, 10, 11] Systems such as ABS and standard cruise control are not covered by this definition of ADAS and therefore fall outside the scope of the study (these systems do not observe their surroundings using sensors).

Fully self-driving cars are currently not allowed on public roads. The current generation of ADAS (which may be called various other names by manufacturers) usually comprise a combination of Adaptive Cruise Control (ACC)[12], Lane Keeping Assist (LKA) and an Advanced Emergency Braking System (AEBS). On certain roads and under certain conditions, the system enables the car to steer, brake and accelerate independently, however the driver must stay alert to take back control of the vehicle if necessary.

New systems are constantly being developed, such as evasive steering (an emergency system that can conduct evasive manoeuvres). In future systems, the exchange of information with the infrastructure and other vehicles (so-called connectivity) will play an increasingly important role. These systems of the future also fall outside the scope of the study.

Table 1 provides an overview of standard ADAS-equipped models of various makes of car. This list is probably incomplete and mainly serves as an illustration of the widespread application of ADAS. The market share of ADAS has increased significantly over the last three years (see Figure 2).[13]

[8] ADAS Alliance, ADAS Convenant, 2019.
[9] ADAS Alliance, *Website ADAS Alliantie*, https://www.adasalliantie.nl, accessed August 23, 2019
[10] Knapp et al., *Code of Practice for the Design and Evaluation of ADAS*, 2009.
[11] SAE International, *Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles - Surface Vehicle Information Report*, 2014.
[12] Also sometimes referred to as traffic aware cruise control (TACC).
[13] VMS on behalf of BOVAG, Het effect van ADAS op schadeherstel , onderhoud en reparatie, 2019.

| | | | | |
|---|---|---|---|---|
| Alfa Romeo Stelvio | Honda Civic | Land Rover Discovery | Peugeot 508 | Toyota C-HR |
| Audi A6 | Hyundai i30 | Lexus ES | Peugeot Rifter | Toyota Yaris |
| Audi Q3 | Hyundai Nexo | Mazda 6 | Range Rover Velar | Toyota Corolla |
| BMW 5 series | Hyundai Santa Fe | Mercedes-Benz A-Class | Renault Koleos | Toyota RAV4 |
| BMW X5 | Jaguar E-pace | Mercedes-Benz C-Class | Subaru Impreza | Volvo S60 |
| Citroën Berlingo | Jaguar F-pace | Mercedes-Benz X-Class | Subaru XV | Volvo S90 |
| DS 7 Crossback | Jaguar I-pace | Mitsubishi Eclipse Cross | Suzuki Jimny | Volvo V60 |
| Ford Focus | Jeep Compass | Nissan Leaf | Tesla Model 3 | Volvo V90 |
| Ford Mustang | Kia Stinger | Opel Combo | Tesla Model S | Volvo XC40 |
| Ford Tourneo Connect | | Opel/Vauxhall Ampera-e | Tesla Model X | Volvo XC60 |
| | | Opel/Vauxhall Insignia | | VW Arteon |
| | | | | VW Touareg |
| | | | | VW T-Roc |

*Table 1: Overview of cars equipped with ADAS as standard (as of April 2019).*

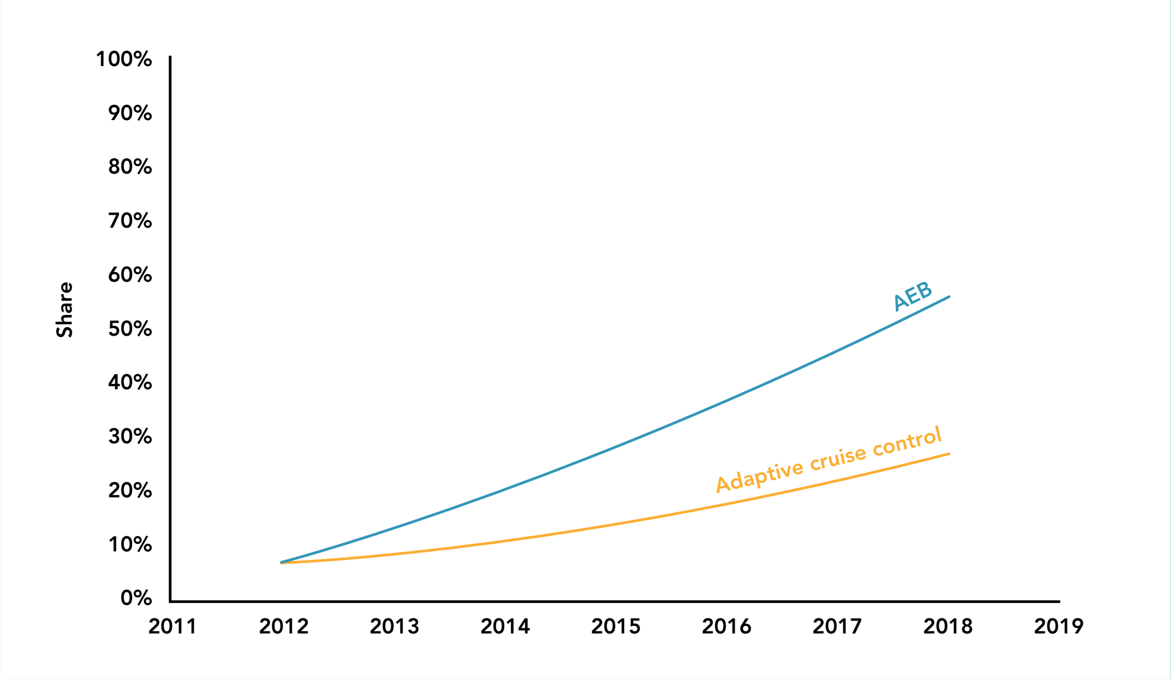


*Figure 2: Two versions of ADAS in new cars. (Source: BOVAG)*

Content
Considerations
Summary
Recommendations
Abbreviations
1 Introduction
2 Reference framework
3 Managing safety risks
4 Bottlenecks in the safe introduction and deployment of ADAS
5 Bottlenecks in monitoring and adjustment
6 Conclusions
7 Recommendations
References
Appendices

*Cybersecurity*

The deployment of ADAS has also introduced risks at the interface where digital technologies meet conventional 'physical' road traffic. Security is becoming increasingly important as a means of ensuring physical safety. Cars are transforming into driving computers, as it were, so that problems that used to be typical of the IT sector are now also affecting road traffic. Moreover, the opportunities for malicious attacks on cars are growing due to the increasing number of digital connections in and between vehicles. These two developments combined are responsible for the rise of cybersecurity risks in cars.

**Definition of cybersecurity**

Cybersecurity involves all measures to prevent or repair the damage caused by the disruption, failure or misuse of ICT. Such damage may consist of detrimental effects on the availability, confidentiality or integrity of information systems and information services and the information stored in them[14]. Damage may also occur in the physical world, for example in road traffic.

This investigation focuses on misuse of cybersecurity vulnerabilities that results in safety risks.

*Privacy*

In addition to road safety, there are other public interests at stake due to the introduction and deployment of ADAS. In particular, personal information (and the right to privacy) could be compromised if, for example, data on driving behaviour becomes widely available (either to the public or third parties). However, such interests fall outside the scope of this report. This subject received plenty of attention at both the European and national level in the spring of 2019. At the European level, this has culminated in the adoption of the General Safety Regulation (GSR) which in its turn refers to the General Data Protection Regulation (GDPR), while at the national level, the Minister of Infrastructure and Water Management discussed the issue in response to questions from the House of Representatives.[15]

[14] National Cyber Security Center, *Cybersecuritybeeld Nederland CSBN 2018*, 2018.

[15] Minister of Infrastructure and Water Management, *Letter to Parliament Answering Parliamentary Questions by Members Schonis and Verhoeven (both D66) on the Article "Wie Temt Het Datamonster in de Auto-Industrie?"*, 2019.

Content
Considerations
Summary
Recommendations
Abbreviations
1 Introduction
2 Reference framework
3 Managing safety risks
4 Bottlenecks in the safe introduction and deployment of ADAS
5 Bottlenecks in monitoring and adjustment
6 Conclusions
7 Recommendations
References
Appendices

## 1.5 Involved parties

The parties involved in the management of the risks associated with the introduction and deployment of ADAS can be divided into three groups:

1. Industrial and sector parties
2. Users
3. Government

The industry comprises the car manufacturers, who are ultimately responsible for the product they put on the market, and their suppliers. In addition to the traditional car manufacturers and suppliers, new manufacturers have appeared on the scene who have a greater affinity with ICT (e.g. Tesla). Some suppliers produce complete systems, while others only focus on chips or software, for example. Combinations of manufacturers and suppliers also occur. Traditional car manufacturers usually buy ADAS systems 'off the shelf' or develop them together with suppliers, while new car manufacturers on the market often develop the systems in-house. Sector parties are importers, dealers and car repair shops. These parties make the products available to the users and maintain and repair the systems.

Any member of the public can use an ADAS. No additional training is required, which means that the driver of a car equipped with ADAS may operate the system without any prior knowledge of it (compare with drivers of conventional cars who have received training and have proved that they can drive a car safely during a driving test). Users of cars fitted with ADAS are hence not always adequately informed of how the system works.[16] The ANWB (Dutch travellers' association) is the primary interest group for ADAS users in the Netherlands. The deployment of ADAS also has consequences for other road users, e.g. drivers of cars without ADAS and vulnerable road users such as cyclists and pedestrians. These groups are faced with new traffic risks. Further automation in road traffic will have potentially far-reaching consequences for society as a whole, as it will affect almost all citizens.

The government comprises the national government and the EU. The EU has entrusted a large part of the implementation of the regulations to a special UN commission, the United Nations Economic Commission for Europe (UNECE). The implementing bodies of the Dutch government separate road traffic affairs into the traditional division of 'humans', 'vehicles' and 'roads'. The CBR (Central Office for Motor Vehicle Driver Testing) tests the driving skills of drivers. The RDW (National Vehicle and Driving Licence Registration Authority) and its sister organizations in Europe test vehicles against a harmonized set of requirements (of which safety is an important aspect) and authorizes approved vehicles to use public roads throughout Europe. Various road authorities such as Rijkswaterstaat (Directorate-General for Public Works and Water Management) and provincial and municipal authorities are responsible for road design and maintenance. The Ministry of Infrastructure and Water Management is responsible for policy and legislation not

[16] Harms and Dekker, ADAS: *From Owner to User; Insights in the Conditions for a Breakthrough of Advanced Driver Assistance Systems*, 2017.

covered internationally. This Ministry is also responsible for the Dutch contribution to the EU and UNECE. The Ministry commissions RDW to conduct a large part of the activities preparatory to forming policies and legislation. Vehicle safety is promoted by Euro NCAP, which provides insight into the safety of cars (and some ADAS) by means of a star rating system.

## 1.6 Guide for readers

*Chapter 2* outlines how the Dutch Safety Board expects parties to fulfil their responsibility for the safe introduction and deployment of new technology in road traffic.

*Chapter 3* focuses on the management of safety risks associated with automation in road traffic. This chapter provides an overview of the risks and the extent to which these risks have been identified and managed. It also describes a number of accidents to illustrate the risks.

The risks of automation in road safety originate in bottlenecks at the system level. We distinguish between bottlenecks in the design and approval of new ADAS (*Chapter 4*) and bottlenecks in monitoring and legislative and regulatory adjustment (*Chapter 5*).

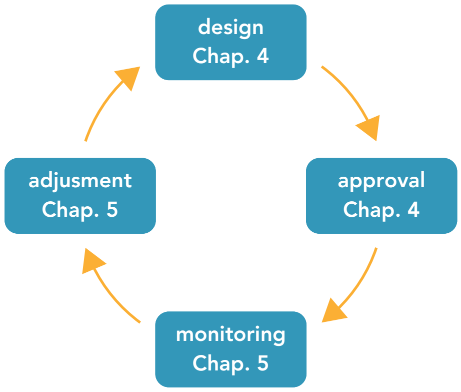


*Figure 3: The structure of the report.*

The report ends with conclusions and recommendations in chapters 6 and 7 respectively.

# 2 REFERENCE FRAMEWORK

The Dutch Safety Board applies a reference framework to all its investigations and studies. This reference framework outlines the standards that the parties involved should meet in order to manage safety risks in a given area. By identifying deviations from the reference framework, it becomes clear where improvements can be made. The development of the reference framework for the safe introduction of new technology and cybersecurity was an important part of the investigation that the Dutch Safety Board conducted to produce this report.

## 2.1 Safe introduction of new technology

Safety risks associated with innovation are characterized by uncertainty, and this uncertainty increases as innovations become more radical. This is why parties must take account of these uncertainties in all their manifestations as the starting point for all their activities.[17, 18] This requires them to assess risks based on more than only empirical data; they also need to consider the feasibility of each scenario. They need to understand that a given set of scenarios will usually be incomplete and hence they must also take measures to cover insufficiently understood risks (precautionary principle).[19]

*Safety principles*
Safety is an important social value. The Dutch Safety Board's safety principles for the introduction of new technology are based on existing literature on public values and ethics in innovation and Artificial Intelligence.[20, 21, 22, 23, 24, 25, 26] These safety principles are generic for innovation and are specifically applied to the introduction and deployment of ADAS in chapters 4 and 5.

1. New technologies must demonstrably improve safety and certainly not compromise it, and this must remain the case throughout the service life of a product.

[17] WRR, *Onzekere veiligheid: Verantwoordelijkheden rond fysieke veiligheid*, 2008.
[18] Onderzoeksraad voor Veiligheid, *Opkomende voedselveiligheidsrisico 's*, 2019.
[19] Onderzoeksraad voor Veiligheid, *MH17 Crash*, 2015.
[20] Floridi et al., *An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations*, Minds and Machines 28, number 4, 2018.
[21] Van de Poel, *An Ethical Framework for Evaluating Experimental Technology*, Science and Engineering Ethics 22, number 3, June 14, 2016.
[22] Future of Life Institute, *AI Principles*, https://futureoflife.org/ai-principles, accessed January 7, 2019.
[23] PBL, *Mobiliteit en elektriciteit in het digitale tijdperk. Publieke waarden onder spanning*, 2017.
[24] Santoni de Sio, *Ethics and Self-Driving Cars; A White Paper on Responsible Innovation in Automated Driving Systems*, number October, 2016.
[25] Rathenau Instituut, *Samenvatting rapport mensenrechten in het robottijdperk*, 2017.
[26] Von Schomberg, *A vision of Responsible Research and Innovation*, in Responsible Innovation, 2013.

Content
Considerations
Summary
Recommendations
Abbreviations
1 Introduction
2 Reference framework
3 Managing safety risks
4 Bottlenecks in the safe introduction and deployment of ADAS
5 Bottlenecks in monitoring and adjustment
6 Conclusions
7 Recommendations
References
Appendices

2. Safe designs of new technology in relation to road safety must meet the following conditions:
    - they take safety into account right from the start of the design phase (*safety by design*)
    - the technology will safely shut itself down in case of a failure (*failsafe*)
    - they do not only assure the safety of the technological innovation itself, but also of the combination of the technology and the user (*foolproof design*[27]): this is a standard term in safe design and means that the design is protected against any intentional or unintentional incorrect or improper use
    - the designers can explain how a system arrives at certain decisions or actions, i.e. the behaviour of the system is understandable and predictable for humans (*explainability*)
    - the designers can explain under which conditions and circumstances the system has control and under which the user has control; this should be clear to the user and also influenceable to a certain extent (*autonomy*)

3. Manufacturers must provide insight into the technology such that others (users, the government) can make an assessment of it (transparency). In addition, empirical data on the consequences for safety must be publicly available and accessible in order to allow assessments of the negative impact of the innovation on safety. There must also be adequate transparency about cybersecurity risks and incidents (see section 2.2).

4. It is important to examine and assess various scenarios and risks. When using new technology, new risks must be monitored and mitigation measures must be taken at the operational, tactical and strategic levels if necessary.

5. New technologies must be introduced in road traffic as part of a carefully controlled process that allows for continuous adjustment based on monitoring and evaluation. These technologies can be gradually scaled up, or the terms and conditions of use can be gradually broadened.

6. The government must be prepared to intervene and temporarily or permanently stop the use of a new technology, or have it modified, if it compromises safety. Such situations must be taken into account in advance, for example by establishing criteria and process agreements for the assessment of risks.

7. The government must protect vulnerable groups or groups who cannot afford the new technology.

8. Legislation and regulations must be adapted to the maturity of the technology and the speed at which it is developing:
    - Rules for using mature technologies, that have been in use for a long time and are tried and tested in practice, can be established in requirements, preferably after a broadly supported process of harmonization and standardization. The manner in which compliance with these rules is assessed must be clearly defined.

[27] Onderzoeksraad voor Veiligheid, *Koolmonoxide: Onderschat en onbegrepen gevaar*, 2015.

- Technology that is still in development must be governed by legislation in the form of performance requirements. Such performance-based regulations must prescribe the level of performance and the associated test methods.
- If the technology is changing rapidly and is not yet mature, qualitative, functional and preferably adaptive regulations will be most appropriate. This applies all the more if the technology is subject to changes while already in use. Assessments are mainly conducted at the process level and the responsibility for demonstrating soundness and safety lies more with the manufacturer and less with the assessment bodies.

*Social embedding and responsibilities of parties*

Responsible innovation[28] can be characterized as a balance between efforts to maximize the positive contributions of the technology and efforts to minimize its negative impact.[29] It is important that innovators, manufacturers, government authorities and social parties (such as representatives of users) share responsibility for the social embedding of the innovation. Innovation must never be seen as a purely technological issue and this implies that broader consultation is needed, including with parties who are not directly involved.

Shared responsibility for safety is part of responsible innovation. A transparent, interactive process in which all actors respond to each other adequately is necessary for the development of safe new technologies. The interactive process is necessary in order to identify safety targets, manage expectations and adapt designs to meet social safety needs. Technology and risk assessments form part of this process.[30, 31]

Manufacturers bear primary responsibility for the safe design of a new technology. Suppliers also have an important contribution to make, because they are the ones who develop a large part of the innovative technology. A precondition for their role is that they can obtain information about the use of the systems and the risks that occur in practice. To this end, manufacturers must facilitate communication within the supply chain and actively collect practical experience of the new technology from consumers. Sellers and importers may also have a role to play here. The manufacturers' responsibility for the product also makes them responsible for the interactive process, in which all actors respond to each other on the same footing.

The government must consider, at an early stage, what its roles are or what roles it wants to play in innovative developments (e.g. user, client, financier, regulator, supervisor or guardian of public interests) and the potential risks it will face.[32] Without government involvement, new technological developments may have negative consequences for important public values.[33] The government can therefore be expected to make an effort

[28] Responsible Research and Innovation (RRI) is an important area of Horizon 2020, the European Framework Programme to stimulate research and innovation.
[29] Rip, *The Past and Future of RRI*, Life Sciences, Society and Policy 10, number 1, 2014.
[30] Van Wezel et al., *Risk Analysis and Technology Assessment in Support of Technology Development: Putting Responsible Innovation in Practice in a Case Study for Nanotechnology*, Integrated Environmental Assessment and Management 14, number 1, January 1, 2018.
[31] Borup et al., *The Sociology of Expectations in Science and Technology*, Technology Analysis and Strategic Management 18, 2006.
[32] Rathenau Instituut, *Met beleid vormgeven aan sociotechnische innovatie*, 2016.
[33] PBL, *Mobiliteit en elektriciteit in het digitale tijdperk. Publieke waarden onder spanning*, 2017.

Content
Considerations
Summary
Recommendations
Abbreviations
1 Introduction
2 Reference framework
3 Managing safety risks
4 Bottlenecks in the safe introduction and deployment of ADAS
5 Bottlenecks in monitoring and adjustment
6 Conclusions
7 Recommendations
References
Appendices

to identify and monitor the opportunities and the risks of innovations and to share information on the risks with parties with the capacity to mitigate them.

Users of innovative technologies often suffer from a lack of knowledge, especially when they are citizens with no specific training rather than professionally trained users. A manufacturer may be expected to inform customers and users about the risks of a new technology and the possible mitigation measures they can take. At the same time, it is important for users (and user collectives) to report the risks they identify to manufacturers and/or the authorities (whereby both manufacturers and authorities must provide the opportunity to do so).

## 2.2 Cybersecurity

Fully and semi-automated cars do not only involve safety risks, but security risks too. Cybersecurity can have an impact on physical safety in road traffic. In cyber-physical systems such as (partially) automated cars, digital and physical systems are connected and cybersecurity risks hence also pose risks to physical safety.[34] In critical safety systems, cybersecurity risks must be managed to ensure this safety.[35]

Different approaches are required to mitigate safety and security risks. Safety risks arise from external factors that cause unintentional damage. These risks can be managed by establishing an adequate set of requirements that can be adapted based on new insights, but that are essentially constant in nature. Such requirements may also be established to manage security risks, but they must then also take account of deliberate intent. This requires prior knowledge of the threat actor's intentions and their capacity to cause harm, their techniques, and their knowledge of system weaknesses that can be abused (vulnerabilities). These variables will change over time and so estimates of cybersecurity risks will also be subject to change. The cybersecurity risks during the design and production of a car can differ significantly from the risks involved when the car is several years old. As a result, cybersecurity must be a continuous process throughout the service life of the car. Specific measures and a control structure will be required to deal with these dynamic risks. In addition, it is important to always assume that every computer system can be hacked if an attacker really wants to.

Various bodies have documented how cybersecurity should be organized for IT systems in general and for IT in vehicles in particular.[36, 37, 38, 39, 40, 41, 42] Eight cybersecurity principles

[34] British Standards Institution, *Connected automotive ecosystems – Impact of security on safety – Code of Practice*, vol. PAS 11281, 2018.
[35] Bloomfield et al., *Security-Informed safety: Integrating security within the safety demonstration of a smart device*, 10th International Topical Meeting on Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies, 2017.
[36] ISO and IEC, *ISO/IEC 15408-1:2009*, ISO, 2009.
[37] ISO, *The ISO/IEC 27000 Family of Standards helps organizations keep information assets secure.*, https://www.iso.org/isoiec-27001-information-security.html, accessed August 23, 2019.
[38] NIST, *NIST Special Publication 800-Series*, https://csrc.nist.gov/publications/sp800, accessed January 24, 2019.
[39] SAE International, *Cybersecurity Guidebook for cyber-physical vehicle systems - J3061*, SAE, 2016
[40] SAE International, *Requirements for hardware-protected security for ground vehicle applications - J3101*, 2012.
[41] NIST, *Framework for improving critical infrastructure cybersecurity, Version 1.1*, 2018.
[42] In addition, the ISO/SAE 21434 - Automotive Cybersecurity Standard is being developed.

Content
Considerations
Summary
Recommendations
Abbreviations
1 Introduction
2 Reference framework
3 Managing safety risks
4 Bottlenecks in the safe introduction and deployment of ADAS
5 Bottlenecks in monitoring and adjustment
6 Conclusions
7 Recommendations
References
Appendices

have subsequently been drawn up for car manufacturers and their suppliers which cover three areas of security:[43, 44]

*Control structure:*

1. Within an organization, the management is responsible for cybersecurity policy. This means that management is engaged and controls cybersecurity. In addition, the management promotes the importance of cybersecurity for the organization and ensures that there is clear communication about what this means for the working process.
2. Manufacturers, including subcontractors, suppliers and potential third parties, must cooperate to improve the system's cybersecurity.
3. Cybersecurity risks must be assessed and managed appropriately and proportionately, including the risks that arise in the supply chain. The measures should take into account the intentions and expertise of the threat actors.

*Design:*

4. The system must be designed to withstand attacks and to respond appropriately when defence mechanisms or sensors fail (failsafe).
5. Systems must be designed according to the defence-in-depth strategy[45]. Security-by-obscurity[46] must not be tolerated.
6. The storage and transmission of data must be secured and controllable.

*Service life:*

7. Software protection measures must be traced throughout the service life of the vehicle.
8. Manufacturers must ensure adequate aftercare and incident response services, so that any vulnerabilities that arise throughout the service life of the vehicle are resolved as quickly as possible and the vehicle remains safe.

*Transparency and cooperation*

Transparency and cooperation between car manufacturers, subcontractors and suppliers is necessary so they can share information on vulnerabilities, incidents and threats and accordingly adhere to the above principles.

Regulators and legislators must be informed of the number and type of cybersecurity incidents so they can make informed adjustments to regulations and regulatory supervision and enforcement where necessary.

To the owner of the car it must be clear what software support and cybersecurity measures are provided by the manufacturer during the service life of the vehicle. It must also be clear to the owner of the car whether they are also the owner of the software installed in it.

[43] GOV.UK, *The key principles of vehicle cyber security for connected and automated vehicles*, 2017.
[44] British Standards Institution, *The fundamental principles of automotive cyber security*, vol. PAS 1885, 2018.
[45] A security strategy in which multiple layers of defense are placed in and around the system to be protected. The failure of one layer of defense is therefore compensated for by the next layer.
[46] Security that relies on the unfamiliarity of the potential attacker with the system design.

For lease companies and fleet managers, transparency in cybersecurity related issues is important so that they can make their own risk assessments.

**Key points**

For a safe design of a new technology it is necessary to take safety into account from the beginning of the design phase. Furthermore, it is necessary to assure safety of the combination technology and user and not only the technological innovation itself. The vision that innovation is a purely technological matter should be prevented. In addition, manufacturers have a responsibility to users to inform them about the risks of a new technology.

New risks must be assessed in advance and mitigated as much as possible. Safe innovation entails a gradual process that allows for continuous adjustments based on monitoring and evaluation. Manufacturers must show that they are innovating safely (transparency) and accident data must be available.

The government must be prepared to intervene if the use of a new technology compromises safety.

Cybersecurity risks must be managed to ensure the safety of interconnected physical and digital systems.

# 3 MANAGING SAFETY RISKS

The introduction and deployment of ADAS entails changes for automobiles and road traffic in general. These changes may introduce new types of safety risks. Risks are inherent to innovation, but risks must be managed. This chapter describes how various types of risks are currently managed by the parties involved.

*Fundamental changes to the nature of cars*
The consequence of technological developments in semi-automated vehicles is that some decisions in vehicles that participate in traffic are now taken by technology. This gives rise to new interactions between computers, drivers and other road users, see Figure 4. The roles and tasks of drivers change substantially when ADAS is deployed in vehicles. The driver becomes more of an 'operator' than an 'active driver', and has to deal with many more interactions than in a non-automated car. The changes in roles and tasks become more far-reaching as the car is equipped with more and more complex ADAS.

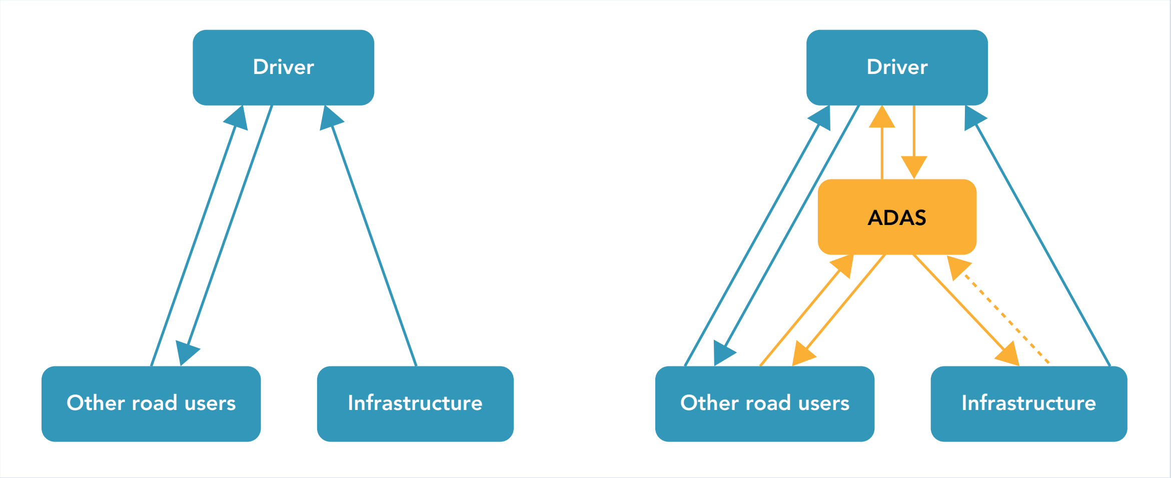


Figure 4: Interactions between drivers and their environments when driving a conventional car (left) or a car equipped with ADAS (right).

*Risk clusters*
Automation in road traffic goes hand in hand with the introduction of new road safety risks. We identified five risk clusters based on accident investigations, literature studies and interviews with experts:

- immaturity of systems
- drivers as operators
- interaction between vehicles and drivers
- dynamic development of automation (updates)
- cybersecurity

In this report, we do not describe all potential risks, but instead provide examples for each cluster. Where possible, these examples are made concrete based on investigated accidents (see Table 2). Because they concern a new type of accident from which much can be learned, these accidents are described in detail in the main document. More information, including the data from the vehicles investigated, can be found in Appendix C:. The involved parties' risk management measures are then discussed for each risk category.

| Accident | Description | Example in section |
|---|---|---|
| **1** | Truck collides into tail end of queue | 3.1 |
| **2** | Truck's emergency brakes engaged | - |
| **3** | Collision with merging truck | 3.1 |
| **4** | Car with Autopilot crashes into slow-moving traffic | 3.2 |
| **5** | Car drives straight ahead across roundabout | 3.2 |
| **6** | Head-on collision between two cars | 3.3 |

*Table 2: Accidents.*

## 3.1 Immaturity of systems

*Introduction*

There are high expectations of the deployment of the new generation of ADAS and its effect on road safety.[47, 48, 49, 50] These expectations are sometimes presented as safety claims in communication and marketing campaigns (see box below). The expectations are based on qualitative studies involving accidents that could potentially be prevented by ADAS in combination with the frequencies of certain types of accidents. They are subject to various preconditions, including the full implementation of ADAS in all vehicles, and take little account of the fact that the deployment of ADAS also entails new risks.[51, 52] In addition, these studies assume that ADAS will work perfectly under all circumstances.

[47] Minister of Infrastructure and the Environment, *Letter to Parliament 31305 Mobiliteitsbeleid*, 2014.
[48] EU Member States, *Declaration of Amsterdam; Cooperation in the field of Connected and Automated Driving*, 2016.
[49] AAA Foundation for Traffic Safety, *Potential Reductions in Crashes , Injuries, and Deaths from Large-Scale Deployment of Advanced Driver Assistance Systems*, 2018.
[50] Aon Risk Solutions, *Whitepaper: Als de auto autonoom wordt; Verkennende analyse van de verzekeringsmarkt en nieuwe risico's bij zelfrijdende auto's*, 2015.
[51] ETSC, *Road Safety Priorities for The EU 2020-2030; Briefing for the European Parliamentary Elections*, 2018.
[52] ETSC, *BRIEFING | EU Strategy for Automated Mobility*, 2018.

Content
Considerations
Summary
Recommendations
Abbreviations
1 Introduction
2 Reference framework
3 Managing safety risks
4 Bottlenecks in the safe introduction and deployment of ADAS
5 Bottlenecks in monitoring and adjustment
6 Conclusions
7 Recommendations
References
Appendices

**Safety claims by car manufacturers**

Nissan expressly describes a relationship between ADAS and safety on its website: 'These technologies form the basis of Nissan's acclaimed ProPILOT system for safer, more confident driving'.[53] A brochure for the Nissan Leaf states: 'We work with our intelligent driving systems to constantly look out for you and help you avoid any mishaps.' ACEA, the umbrella organization of European car manufacturers, suggests that active safety measures are capable of reducing the number of accidents and their consequences.[54]

*Problem*

The current generation of ADAS does not always make the right decisions[55, 56], because the technology is not yet fully developed when the product is released to the market. This is known as system immaturity. Automation cannot (yet) cover all the situations that are actually possible. Although the current ADAS only support the driver from a legal point of view, in practice drivers experience that the ADAS occasionally take over control (see further section 3.2 and 3.3). Drivers sometimes experience that the car makes the wrong decision.

*Volvo truck collides into tail end of queue*

On 27 March 2017, there was a rear-end collision on the A29 near Den Bommel (Goeree-Overflakkee). A Volvo truck built in 2016 crashed into the rear of a stationary truck with a low loader. The Volvo was equipped with an Advanced Emergency Braking System (AEBS), which was made mandatory in 2015[57].

The AEBS was supposed to ensure that the Volvo braked in time, but this did not happen. The driver did not brake either. An analysis of the tachograph data revealed that the truck collided into the rear of the stationary low loader while driving 83 km/h and without the brakes being applied. As a result of the impact, the freight container came off the chassis and collided with the cabin from behind. The truck's cabin was crushed between the container and the bulldozer on the stationary low loader. The driver of the truck was killed in the accident.

[53] Nissan, *Nissan LEAF - Elektrische Auto - Elektrische Voertuigen*, 2019.

[54] ACEA, *ACEA Position Paper; General Safety Regulation Revision* Brussel, 2018.

[55] Gorter and Klem, *Markering en rijtaakondersteunende systemen* Amersfoort: Royal Haskoning DHV on behalf of the Province of Utrecht, 2016.

[56] Eykholt et al., *Robust Physical-World Attacks on Deep Learning Visual Classification*, in 2018 IEEE/CVF Conference on Computer Vision and Pettern Recognition IEEE, 2018.

[57] Commission Regulation (EU) No 347/2012 of 16 April 2012 implementing Regulation (EC) No 661/2009 of the European Parliament and of the Council with respect to type-approval requirements for certain categories of motor vehicles with regard to advanced emergency braking systems. This obligation only applies to trucks produced after the effective date.

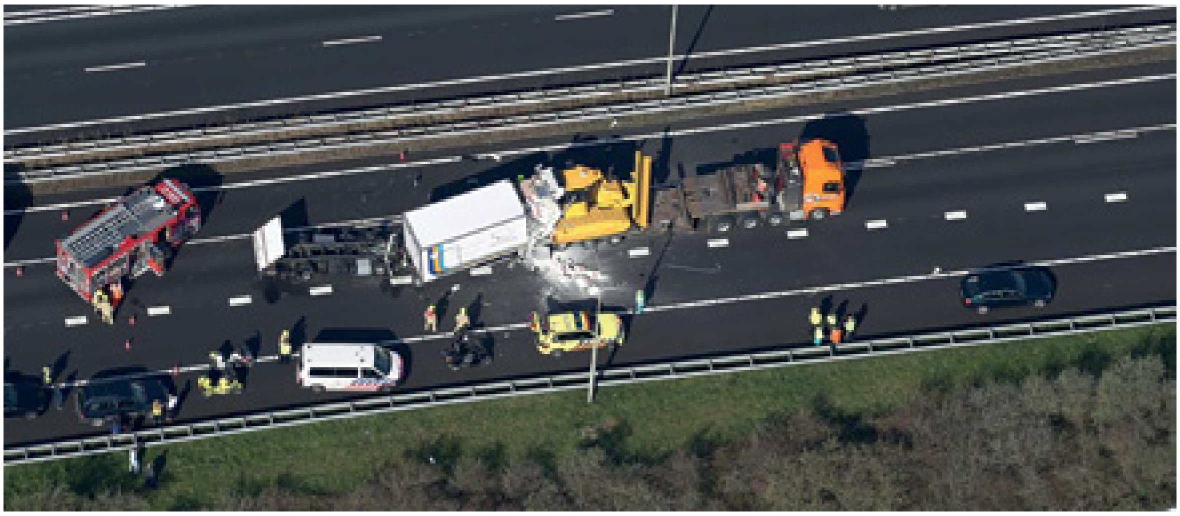


*Figure 5: Aerial view of the accident on the A29. The Volvo truck (white) collided with a low loader carrying a bulldozer. (Source: police)*

According to the truck manufacturer, the camera system probably did not recognize the low loader. The AEBS only recognizes the rear ends of the most common vehicles (see Annex C.2.1 for the technical details). Low loaders carrying a bulldozer do not fall under this category of common vehicles.

The generation of emergency braking systems used in this truck does not store any system data if there is a sudden loss of voltage, which is why no data is available from the moment the accident occurred.

*Immaturity of AEBS*

The accident with the Volvo truck reveals that AEBS does not work in all cases. Despite the fact that AEBS became mandatory for new trucks in 2015, there are still a number of scenarios in which the current generation of emergency braking systems will continue to have problems detecting other road users.[58] Moreover, AEBS in various models of trucks and cars do not, or only insufficiently, recognize temporary traffic measures (such as a traffic warning trailer used to warn of roadworks).[59] This can lead to dangerous situations when these temporary traffic measures are used to warn for roadworks and accidents.

In the approval procedure for vehicles with AEBS, the emergency braking systems are tested in three situations: when the vehicle in front is stationary, when the vehicle in front is moving slowly and when the vehicle in front suddenly brakes[60]. The response of AEBS to other stationary and moving objects, such as traffic warning trailers, is not tested as part of the approval procedure.

[58] Klem et al., *AEBS en vrachtwagens; Praktijktest herkenbaarheid vrachtwagens voor Advanced Emergency Braking Systems* Royal Haskoning DHV, 2017.

[59] Van Hattem, Klem, and Gorter, *AEBS en verkeersmaatregelen; Praktijktest zichtbaarheid verkeersmaatregelen voor Autonomous Emergency Braking Systems*, vol. BF1326 Amersfoort: Royal Haskoning DHV, 2017.

[60] Commission Regulation (EU) 2015/562 of 8 April 2015 amending Regulation (EU) No 347/2012 implementing Regulation (EC) No 661/2009 of the European Parliament and of the Council with respect to type-approval requirements for certain categories of motor vehicles with regard to advanced emergency braking systems.

*Collision with merging truck*

On 11 April 2017, a Tesla Model S on the A1 near Bathmen (a motorway with two lanes in each direction) was driving with the Autopilot system engaged (combination of Adaptive Cruise Control and Lane Keeping Assist[61]). The Tesla was driving in the left lane at high speed (the driver had set the ACC to 150 km/h).

A number of trucks were driving in convoy in the right lane. One of these trucks abruptly had to swerve into the left lane to make room for a merging vehicle. At that moment, the Tesla was overtaking the line of trucks at high speed.

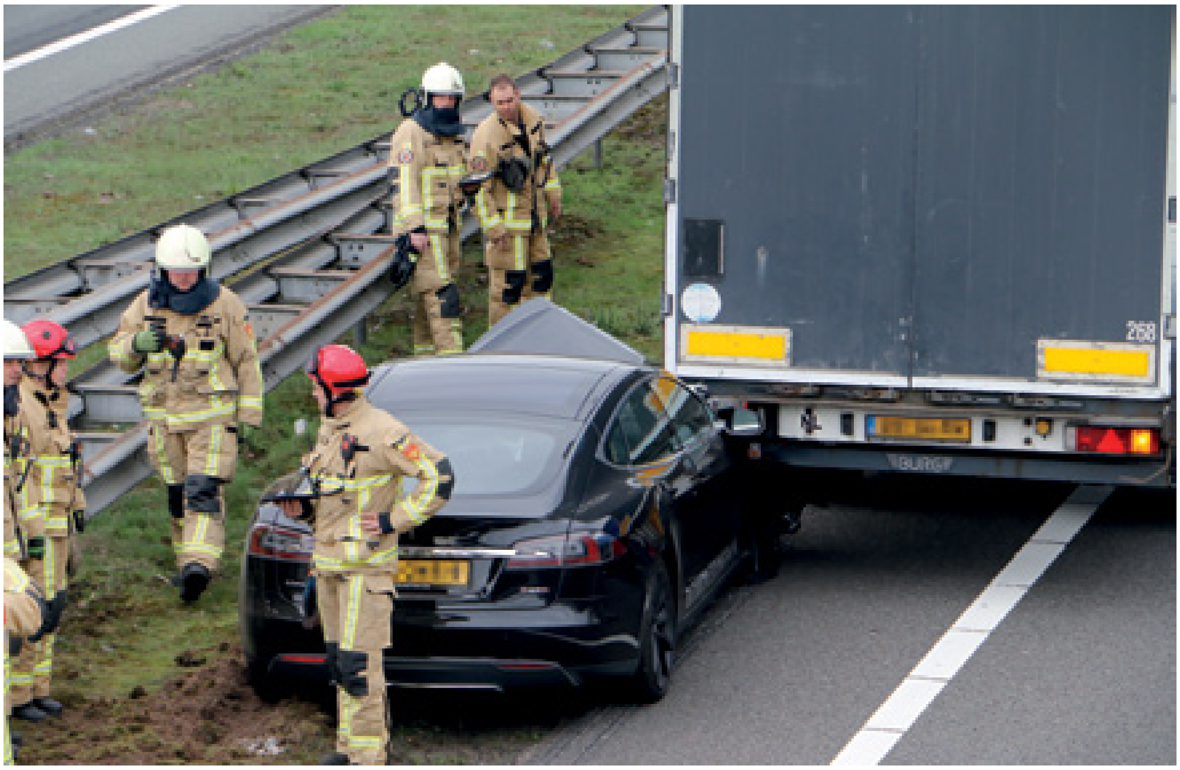


*Figure 6: The Tesla after it came to a standstill under the trailer of the truck. (Source: Hof van Twente fotografie)*

*Immaturity of adaptive cruise control*

The driver of the Tesla did not see the truck change lanes because he was looking briefly into his rear-view mirror at the time. Before the Tesla collided with the truck, its speed dropped to about 128 km/h because the Autopilot detected a vehicle in front and engaged the brakes. The speed of the truck was 98 km/h. The Tesla collided with the rear of the trailer travelling at this speed. The driver of the Tesla was not injured.

Although the Tesla in question was equipped with an emergency braking and warning system, both systems were activated very shortly before the impact; too short to allow the driver to intervene and to reduce the speed sufficiently. The manufacturer claims that the version of the emergency braking and warning system in the Tesla (2014) effectively detects vehicles in front of the vehicle but cannot yet detect vehicles that are changing lanes. Both the initial deceleration by Autopilot and the activation of the emergency warning and braking system functioned as designed.

[61] Tesla calls these systems TACC and Autosteer.

Euro NCAP has tested assistance systems (combinations of ACC and LKA, referred to as Autopilot or ProPILOT in some makes of car) in combination with the operation of emergency braking systems in ten different makes of cars in order to give consumers a realistic picture of the potential of the current ADAS.[62] The tests revealed, for all makes, that ACC has difficulty anticipating merging and diverging traffic, because the systems only recognize the rear ends of other vehicles; a vehicle at an angle will not be recognized. This was the case in the accident described above. In other situations, such as when approaching a stationary queue, the performance of the ACC in the various makes differed widely. While ACC in one vehicle gradually applied the brakes as it approached a queue, in another the emergency brake system was activated, and some cars did not respond at all.

*Other examples of immaturity*

Currently available technologies for ADAS that combine ACC, LKA and AEBS are really only intended for use on roads with clearly marked lanes, such as motorways. Another condition is that there must not be any roadworks, accidents or other disruptions on the motorway. However, these systems can also be engaged on roads for which they are not intended (according to the manufacturer) nor suitable.[63] For example, Tesla's Autopilot does not take roundabouts, traffic lights, traffic signs or priority for other motorists into account, but Autosteer can still be engaged on any road with lanes that the system recognizes as such (be it correctly or incorrectly). According to Tesla, drivers are aware of these limitations and like the Autopilot so much that they engage it wherever possible.[64] Other manufacturers also apply location-based restrictions (so-called *geo-fencing*) to the use of ADAS. For example, Volvo Cars says that its Pilot Assist is mainly intended for use on roads outside built-up areas, but the system can also be engaged in built-up areas. The same applies to Nissan's ProPILOT, for example. In addition to the unclarity about the precise area of application, these comfort systems can sometimes take drivers by surprise with unexpected and uncomfortable behaviour, such as sudden hard braking for no apparent reason, taking an unintended exit lane, or flying out of a curve because it is sharper than the system can handle.

*Identifying and managing the risks of immaturity*

As explained above, several ADAS are still immature systems and do not work properly in all situations, with the subsequent risk of accidents. 'Self-learning' is a common feature of the systems currently in use, as these systems only take a limited number of situations into account in the first instance. The system makes decisions based on automated decision rules and a large amount of data, such as the sensor data from cameras or radar. New decision rules can be loaded into the ADAS together with system updates. An example of a technological development is the expansion of a detection system that initially only recognizes cars to also recognize pedestrians.

[62] Euro NCAP, *2018 Geautomatiseerde Rijsystemen*, 2018.
[63] Provided that the system state is within the operational design domain.
[64] The precondition is that lines are present.

The deployment of immature systems on the road is seen as a necessary step to further develop these systems. This does not have to be a problem in itself, but it is a problem when the principles for safe innovation have not been sufficiently taken into account (see section 2.1). For example, drivers must be sufficiently equipped to understand and deal with such automated systems (see sections 3.2 and 3.3), but instead drivers are still insufficiently aware of the risks associated with immature systems.

These new risks are managed by car manufacturers in various ways. Some car manufacturers constantly modify their systems and others only include updates in new vehicles. An example of a manufacturer that constantly modifies systems is Tesla. Tesla states that developing technologies can only be managed adequately if a channel is created with which existing systems can regularly be updated. Tesla uses Over-The-Air (OTA) updates to this end (see also section 3.4). In addition, Teslas regularly send information back to the manufacturer, for example about dangerous situations and unexpected interventions made by the Autopilot. In addition to testing new software versions within a select test group, Tesla invites all its customers to provide feedback about any complaints, experiences or incidents. Tesla uses the feedback provided by the cars and drivers to develop the systems further. In order for the systems to become mature, the real world is used as a 'living lab'. In addition, risk management may entail extensive system testing before they release the systems to the market. For example, Daimler has its systems tested on various continents by non-technical staff, carries out a number of circuit tests, and also conducts driving simulation tests with different testers.[65]

There is no transparency about whether and how manufacturers improve their products and on the basis of what information, such as accident data. Manufacturers are not obliged to collect and analyse accident data. They learn from accidents involving their systems as they see fit. In early 2019, Volvo Cars published the results of more than 50 years of accident investigations online as part of its EVA (Equality for Vehicle Advancement) initiative. The EVA database contains information about the circumstances of accidents with Volvo cars, including any automated systems that may have been involved. Tesla has been publishing a quarterly Vehicle Safety Report since 2018.[66] These reports do not contain a lot of information as yet, but Tesla has plans to expand their content. Other car manufacturers only report internally on accidents and the safety performance of their ADAS. In the opinion of these manufacturers (as stated in various interviews) other manufacturers will not benefit much from these reports, because their vehicles are equipped with different systems and/or modules and hence there is little basis for comparison. However, it cannot be ruled out that competition considerations also play a role in this reluctance to share data.

[65] Many of these procedures are internal and therefore specific to the manufacturer, but are derived from ISO 26262 - an international standard for the functional safety of electronic systems in vehicles.

[66] Tesla, *Q3 2018 Vehicle Safety Report*, https://www.tesla.com/nl_NL/blog/q3-2018-vehicle-safety-report, accessed December 12, 2018.

Euro NCAP includes AEBS in its safety assessments, even if it does not yet fully function properly in all circumstances. The reason for this is that there is sufficient evidence that these systems improve safety. Adaptive Cruise Control is not yet included in the safety assessments, because Euro NCAP does not yet have adequate information about its limitations and safety benefits (see C.1).

*Managing risks through regulatory supervision and legislation*
ACC is widely used in the current generation of cars. No approval requirements apply to the use of ACC.[67] These systems are not considered to be unsafe by the various approval authorities in Europe and are therefore approved for use (see diagram in Appendix E:), while it is unclear to what degree they detriment or improve safety. There are also no regulations for AEBS in cars. These do exist for AEBS in trucks, with the specific objective of preventing collisions whereby a truck drives into the rear of a passenger car in a queue.

**Partial conclusions**
The current generation of ADAS is not yet fully mature in all respects. Systems that are known to improve road traffic safety, such as AEBS, can also be further improved. For other systems, such as ACC, it is not clear yet what the safety balance will be. Nevertheless, there are no type approval requirements for ACC.

The performance of ADAS with similar characteristics can vary significantly from make to make. ADAS do not recognize all types of vehicles or objects, have difficulties detecting merging and diverging traffic, and emergency braking systems do not brake for all types of vehicles. This has already led to accidents.

The systems are not designed to be used on every type of road, but they do not use location-based restrictions.

Drivers are insufficiently familiar with the operation and limitations of the systems but rely on them nevertheless.

Some of the current types of ADAS are regulated, while others are not.

Systems that continue to be developed while they are already in use are inherent to the current generation of technology. Some manufacturers modify their ADAS during the service life of the vehicle, while others only do so for newly produced cars. There is no transparency about whether and how manufacturers improve their products based on monitoring and evaluation.

Manufacturers are not required to learn from accidents involving their systems and can do so as they see fit. Most manufacturers do not share the results of accident investigations with each other. In this area, the first steps have been taken by Volvo Cars and Tesla.

[67] There is an ISO standard: 15622 about the performance requirements.

Content
Considerations
Summary
Recommendations
Abbreviations
1 Introduction
2 Reference framework
3 Managing safety risks
4 Bottlenecks in the safe introduction and deployment of ADAS
5 Bottlenecks in monitoring and adjustment
6 Conclusions
7 Recommendations
References
Appendices

## 3.2 Drivers as operators

*Introduction*
The roles and tasks of motorists change when ADAS is deployed in vehicles. The driver becomes more of an operator, i.e. a supervisor of the driving process rather than an active driver.[68] As the *operator* of the vehicle, the driver monitors whether the ADAS-equipped car is performing the driving tasks correctly and intervenes if necessary. In some cases, the driver will receive a warning from the car if human intervention is necessary, or if the system detects that the driver is insufficiently alert. The driver must then respond adequately, for example by correcting the steering or by braking.[69]

The role of the driver is changing due to systems that assume part of the driving task for long stretches of time, such as Adaptive Cruise Control and Lane Keeping Assist. This changing role does not apply to emergency systems such as AEBS.

In addition to this changing role, drivers are faced with another major change, namely the increased interaction with the vehicle. This interaction also involves risks, and these are discussed in section 3.3.

*Tesla with Autopilot crashes into slow-moving traffic*
On 25 August 2016, the driver of a Tesla Model S was driving on the A4 motorway near Leiden with the Autopilot function engaged (Autopilot is a combination of Lane Keeping Assist and Adaptive Cruise Control). Traffic on the motorway was moving slowly. Matrix signs above the road indicated a speed limit of 50 km/h. The driver had adjusted the ACC (Tesla calls this TACC) to 130 km/h, with the shortest distance headway.

The driver of the Tesla had noted that the system had correctly decelerated to a lower speed several times that afternoon. Approximately 5 minutes prior to the collision, the driver of the Tesla was given a warning of a possible collision with another vehicle in front by the Forward Collision Warning system (FCW). The driver immediately applied the brakes. After this he reengaged Autopilot.

The Autopilot system had been engaged for a period of approximately 5 minutes prior to the collision and one of the registered parameters revealed that the driver's hands had not been on the steering wheel during this period. No FCW warning was provided.

The vehicle was travelling at a speed of approximately 67 km/h just before the moment of impact. The driver of the Tesla started braking between 0.5 and 1.5 seconds before reaching the rear of the queue, at a distance of about 19 metres from the vehicle in front. He was unable to prevent the Tesla from colliding into this vehicle and setting off rear-end collisions between five other cars. No one was injured in this accident.

[68] Van Nes and Duivenvoorden, *Veilig naar het verkeer van de toekomst; nieuwe mogelijkheden, risico's en onderzoeksagenda voor de verkeersveiligheid bij butomatisering van het verkeerssysteem*, R-2017-2 Den Haag: SWOV, 2017.
[69] Kyriakidisa et al., *A Human Factors Perspective on Automated Driving*, Theoretical Issues in Ergonomics Science 18, number 1, 2017.

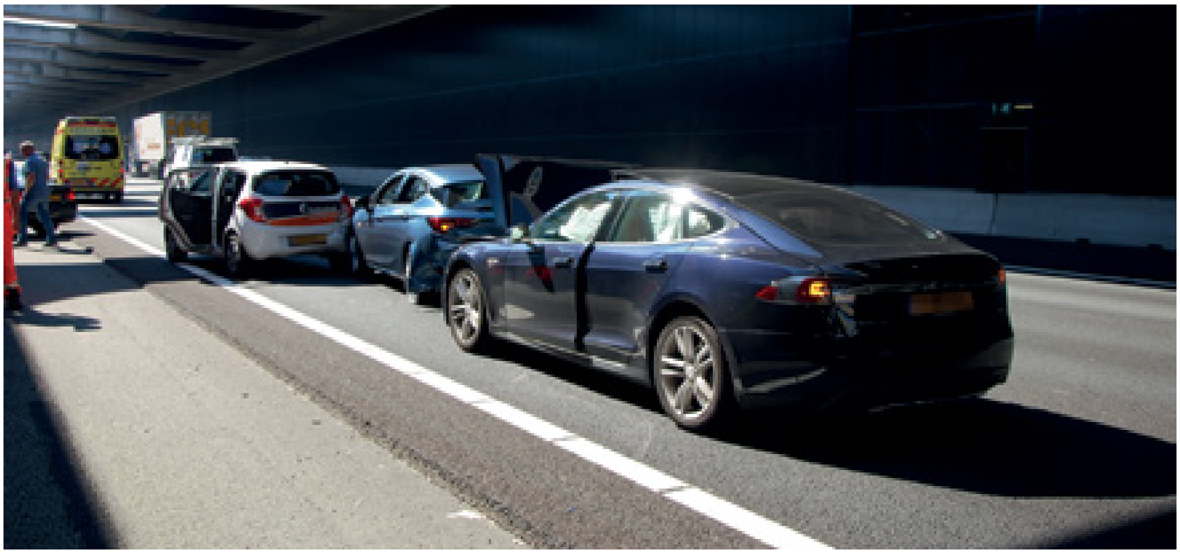


*Figure 7: Tesla Model S collides with the vehicle in front at a speed of 58 km/h. (Source: 112regioleiden.nl)*

Despite the fact that Autopilot was engaged, the system did not carry out any form of speed reduction measures and nor did it issue any warnings. Taking only the braking distance of the vehicle in front into account, this indicates that the driver responded adequately quickly. However, drivers need to anticipate much further ahead than only the vehicle in front of them. The investigation shows that it is conceivable that the driver was not aware of the traffic situation further ahead because of the low mental workload, or because he was distracted as a result.

This accident reveals that this driver had a lot of confidence in Autopilot. He had selected a high speed and he had chosen a short distance headway. The driver's confidence in Autopilot was strengthened by the fact that the FCW system had warned him again shortly before the accident. His alertness at the moment the vehicle in front started braking helped to ensure that the accident did not have more severe consequences, but he nevertheless failed to adequately anticipate the traffic ahead of him.

In the meantime Tesla has updated and decreased the hands-on detection time interval to 15 seconds. If the driver's hands have not been on the steering wheel for longer than this time, the system will issue a warning. By reducing this time span, Tesla complies with UNECE approval requirements in R79.03. Tesla also later introduced the '3 strikes you're out' rule, requiring the driver to stop the vehicle to re-use Autopilot after the system has detected three times that the driver did not have his hands on the steering wheel for more than 15 seconds.

*Longer response times and reduced alertness*

Monitoring the driving process in the role of operator, as is the case when driving with ACC in combination with LKA, involves risks that do not affect conventional vehicles with active drivers. This is because operators have longer response times than active drivers

Content
Considerations
Summary
Recommendations
Abbreviations
1 Introduction
2 Reference framework
3 Managing safety risks
4 Bottlenecks in the safe introduction and deployment of ADAS
5 Bottlenecks in monitoring and adjustment
6 Conclusions
7 Recommendations
References
Appendices

(more than six seconds in some cases[70, 71, 72, 73] in comparison to about two seconds for active drivers) and they also miss more information.[74] Operators are also likely to be more easily distracted and less alert than active drivers.

In October 2017, Waymo (a subsidiary of Google) decided to stop developing systems that require human intervention, because dangerous situations arose during testing. The specially-trained drivers of the test vehicles were easily distracted: they did their makeup, checked their phones or even fell asleep.[75]

Research reveals that 29% of ADAS users at least occasionally feel they are able to engage in other activities than driving the car if they are using Adaptive Cruise Control.[76] The risks involved in longer response times and missing information are exacerbated by the fact that some drivers of automated vehicles tend to rely on this automation to drive the vehicle, while it does not function adequately in all situations (see section 3.1).

Users report that ADAS relieves them of some driving tasks, which makes driving more relaxed. A few also say that this makes their driving safer. However, it has not been scientifically established whether the current generation of ADAS leads to a lower mental workload for drivers.[77] A driver of a car equipped with a current generation ADAS has to perform a wider range of tasks (in particular monitoring) than a driver without ADAS.[78] In the role of operator, motorists are required to monitor more and more information and, for example, adjust the speed manually in the system instead of releasing the accelerator pedal or braking. This continuous monitoring of the status of the system can also cause a risk, because it requires drivers to take their eyes off the road.

*Identifying and managing the risks of reduced alertness*

Manufacturers are aware of the risk of drivers being insufficiently alert when using assistance systems. They sometimes label this improper use of the systems, rather than a logical consequence of the low mental workload. Manufacturers try to mitigate these risks, for example by installing systems that monitor driver alertness. One way of doing this is by monitoring whether the driver has their hands on the steering wheel and by alerting them with visual and/or audio signals if they have their hands off the wheel for a

[70] Vlakveld et al., *An Empirical Exploration of the Impact of Transition of Control on Situation Awareness for Potential Hazards;An Experiment about the Hazard Perception Capabilities of Drivers after Interruption in a Video-based Scanning Task*. The Hague: SWOV, 2015.

[71] Endsley and Kaber, *Level Of Automation Effects on Performance, Situation Awareness and Workload in a Dynamic Control Task*., Ergonomics 42, number 3, 1999.

[72] Wright et al., *Experienced Drivers are Quicker to Achieve Situation Awareness than Inexperienced Drivers in Situations of Transfer of Control within Level 3 Autonomous Environment*, in Proceedings of the Human Factor and Ergonomics Society 2016 Annual Meeting, vol. 60, 2016.

[73] Zhang et al., *Determinants of Take-Over Time from Automated Driving: A Meta-Analysis Of 129 Studies*, Transportation Research Part F: Traffic Psychology and Behaviour 64 2019.

[74] Vlakveld et al., *Situation Awareness Increases when Drivers Have More Time to Take Over the Wheel in a Level 3 Automated Car: A Simulator Study*, Transportation Research Part F: Traffic Psychology and Behaviour, 2018.

[75] Dave, *Google Ditched Autopilot Driving Feature After Test User Napped Behind Wheel*, ed. Sam Holmes Atwater, California, USA: Reuters, 2017.

[76] AAA Foundation for Traffic Safety, Vehicle Owners' *Experiences with and Reactions to Advanced Driver Assistance Systems*, 2018.

[77] Zhang et al., *Determinants of take-over time from automated driving: A meta-analysis of 129 studies*, Transportation Research Part F: Traffic Psychology and Behaviour, 2019.

[78] Kyriakidisa et al., *A Human Factors Perspective on Automated Driving*, Theoretical Issues in Ergonomics Science 18, number 1, 2017.

given length of time. However, this is not a direct measurement of alertness, but rather a more convenient method for measuring behaviour that may indicate alertness. Renault has chosen a different route and introduced a system that detects driver fatigue based on driving behaviour. No EC or UNECE legislation or regulations have been established to govern such systems to date. The new General Safety Regulation (GSR) (see Annex E) requires the introduction of fatigue and alertness warning systems and 'advanced distraction warning' systems. These systems are subject to the EU's general technical and privacy requirements.

*Tesla drives over central island of roundabout*
In the early afternoon of 1 July 2016, a Tesla Model S drove at high speed straight over the central island of a roundabout. The Tesla collided with a pole on the other side of the roundabout and came to a standstill. The driver suffered major injuries in the accident.

At the time of the accident, the Tesla was driving on the N57 road with Autopilot engaged (ACC and LKA). The vehicle's time lapse log revealed that it had approached the roundabout at a constant speed of approximately 84 km/h. The speed decreased to 10 km/h in a period of approximately 3 seconds, and another 3 seconds later the vehicle came to a standstill. The driver only applied the brakes once the vehicle was crossing the central island of the roundabout. The Autopilot system did not give any warning and did not apply any form of braking. Upon receiving his car, the driver had a brief explanation of the systems in the vehicle. He also stated that he had taken most of the information about the functioning of Autopilot from the owner's manual. The manual states that Autosteer is intended for use only on motorways. At the same time, the manual provides explanation about the speed restriction when using Autosteer in built-up areas. This implies that the system can also be used there. The manual does not give any warning about roundabouts.

The current generation of ADAS is designed to be used on roads that are clearly marked, whereby there are no disruptions such as roadworks. Among other things, these systems are unable to control the car in bends with a radius below a certain value and on roundabouts. However, many of these ADAS are designed so that they can be engaged on roads with sharp bends and roundabouts nevertheless. The system does not produce a warning when approaching such a road situation. In effect, the system can only keep the car in its lane, maintain a preset speed and lower the speed if a vehicle in front is driving more slowly. In the meantime, Tesla has released an update in which Autopilot is enabled to use digital map data in order to allow preventive breaking and thus anticipating to, for example, sharp bends. The ADAS design is based on the assumption that the driver will take control if the system no longer recognizes the situation. The problem with this is that drivers as operators have a longer response time and miss more information than they would do when actively driving a car without ADAS. As a consequence, the driver may intervene too late. This was also the case in this accident where the car drove straight ahead over a roundabout.

Content
Considerations
Summary
Recommendations
Abbreviations
1 Introduction
2 Reference framework
3 Managing safety risks
4 Bottlenecks in the safe introduction and deployment of ADAS
5 Bottlenecks in monitoring and adjustment
6 Conclusions
7 Recommendations
References
Appendices

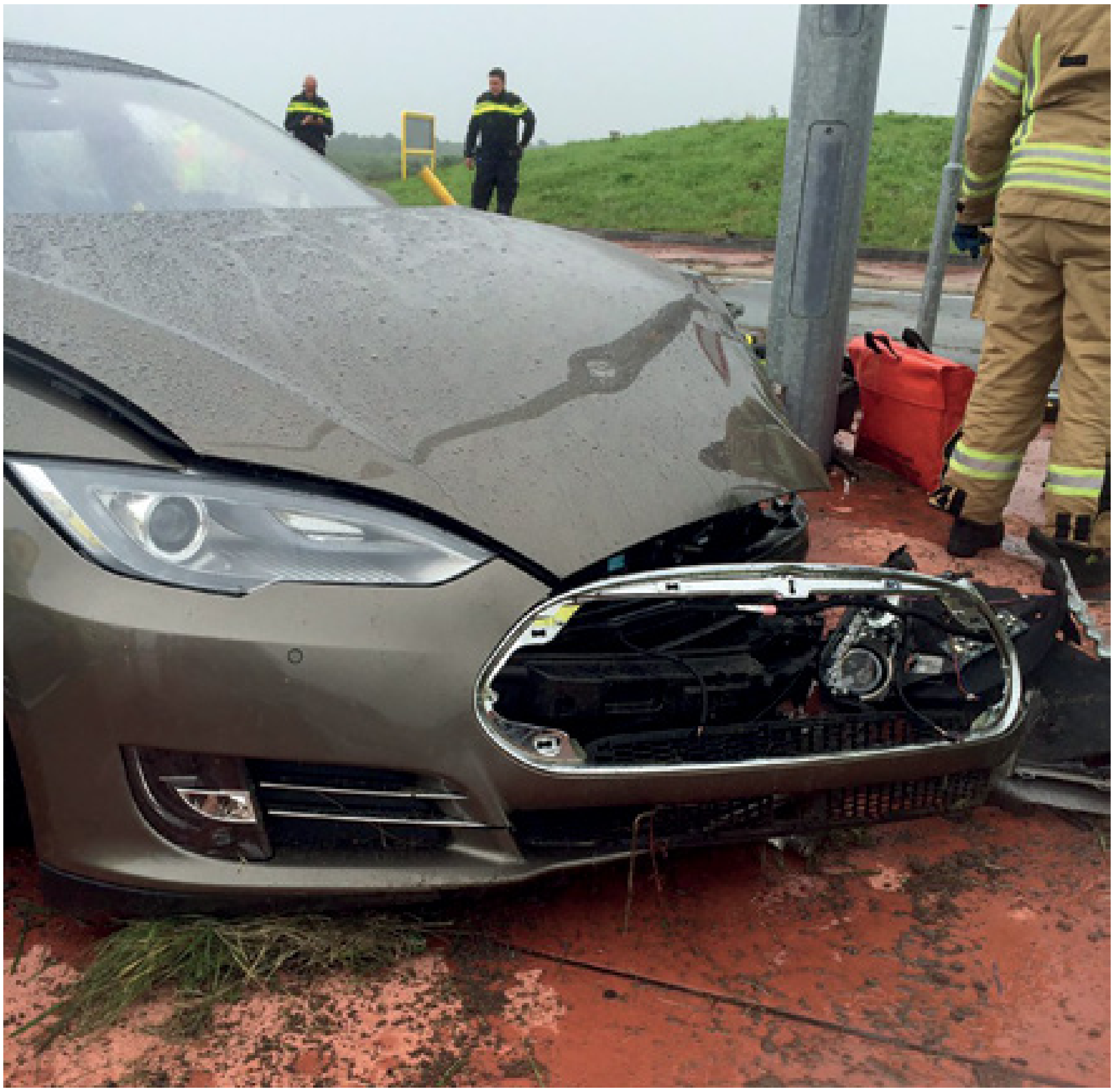


*Figure 8: The Tesla Model S after it collided with the pole on the other side of the roundabout. (Source: Twitter, posted by road inspector Jeroen of Rijkswaterstaat)*

*Lack of knowledge*

The safety of ADAS depends very much on how these systems are used. There are many misconceptions about ADAS among drivers. Some drivers overestimate the systems and rely too heavily on them. For example a system may be called an 'auto-pilot'[79], but the driver still has to remain alert. Drivers often do not know exactly which ADAS is installed in their car and the functionality of the system can change with a new update (see section 3.4). In addition, not all drivers are aware of the limitations of the ADAS in their car and it may be unclear why the system makes certain decisions. This can lead to misunderstandings and additional risks.[80]

[79] Abraham et al., *What's in a Name: Vehicle Technology Branding and Consumer Expectations for Automation*, AutomotiveUI 2017 - 9th International ACM Conference on Automotive User Interfaces and Interactive Vehicular Applications, Proceedings, September, 2017.

[80] Carsten and Martens, *How Can Humans Understand their Automated Cars? HMI Principles, Problems and Solution*s, Cognition, Technology and Work 21, number 1, 2019.

*Identifying and managing the risks of lack of knowledge*

Half of the drivers use Lane Keeping Assist systems without any prior knowledge of how they work.[81] An analysis of various online forums and social media reveals that the main sources of information are self-study and instructions provided by the dealer. Manuals are often very long and so are not carefully studied. Moreover, the manuals often contain descriptions of all optional systems, rather than only the systems that are actually installed in the vehicle. Many users are still unclear about the conditions under which the system can be used after reading the manual. Moreover, some users consider the information in the manual to be incomplete. Studies have also revealed that drivers do not adequately apply the information they read in the manuals in practice.[82] All this means that users are not receiving adequate instructions about the correct way to use ADAS.

Some manufacturers believe it is not necessary to provide information because the operation of the system should be intuitive and self-explanatory. They think an indication of a good system is that a driver can use it without reading the manual. This is not always the case, however, because drivers are not always fully informed about how the ADAS works and how they should use it.[83] Other manufacturers believe that the user should be given clear instructions about the systems and what can and cannot be expected of them. For example, Volvo Cars offers its Dutch customers an introductory course provided by a specialized company. No legislation has yet been developed on the instruction of drivers.

Euro NCAP is developing test protocols to determine whether manufacturers provide sufficiently clear and non-deceptive consumer information on ADAS.[84] These should explain, among other things, the functionality and limitations of the systems, so that drivers understand the functioning of the systems and have the right expectations. These test results will not affect the Euro NCAP star rating in the coming years (until 2025).

Although car manufacturers do encourage dealers to inform customers, there are apparently no requirements to provide customers with information about the use of ADAS. Those car dealers who do provide information to customers often do not provide enough, neither at the time of purchase nor in response to later enquiries. The reason being that the dealers themselves do not always have access to the right information. Studies revealed that only a quarter of lease drivers received instructions about ADAS from the dealer.[85] Dealers and importers currently often play no role in the provision of information to consumers. An important reason for this is that they themselves have little knowledge about ADAS in cars. BOVAG is investigating whether its members (the dealers) consider providing information to be their responsibility. The RAI association indicates that, alongside dealers, importers also have little knowledge of the ADAS in the cars they sell. Some manufacturers fail to make sure that their importers, dealers, and

[81] ANWB, *Verwachtingen werking Lane Assist nog te hoog gespannen; Onderzoek naar rijbaanhulpsysteem in auto's*, 2017.

[82] Boelhouwer et al., *Should I Take Over? Does System Knowledge Help Drivers in Making Take-over Decisions while Driving a Partially Automated Car?*, Transportation Research Part F: Traffic Psychology and Behaviour 60, 2019.

[83] ADAS Alliance, *ADAS Convenant*, 2019.

[84] Euro NCAP, *Euro NCAP 2025 Roadmap: in pursuit of vision zero*, 2017.

[85] Harms en Dekker, *ADAS: From Owner to User; Insights in the Conditions for a Breakthrough of Advanced Driver Assistance Systems*, 2017.

Content
Considerations
Summary
Recommendations
Abbreviations
1 Introduction
2 Reference framework
3 Managing safety risks
4 Bottlenecks in the safe introduction and deployment of ADAS
5 Bottlenecks in monitoring and adjustment
6 Conclusions
7 Recommendations
References
Appendices

ultimately the drivers of their vehicles are sufficiently informed, so they compensate for this with follow-up driving courses and training courses for dealers, importers and interested drivers. The ANWB considers the lack of knowledge among drivers to be a significant risk and provides general information about ADAS through its website.[86]

The current European legislation for driving tests is strict and unambiguous. There is little scope for Member States to modify the driving tests to meet their own requirements. The Ministry and CIECA are currently calling for new framework legislation. The current driving test that is conducted by the CBR does not assess the correct use of the various ADAS that are present in vehicles. In general, new technology is not included in the driving test until this technology has gained widespread use. For example, as of 25 March 2018, part of the route of the driving test must be followed using a navigation system. Because there are still many differences between the various ADAS, the CBR cannot yet require the use of ADAS in the practical driving test (however, it could include questions about ADAS in the theory test). Another reason is that many driving schools do not have ADAS-equipped vehicles and almost all of these vehicles have automatic gearboxes, which means that a driving licence obtained in such a vehicle does not permit the license holder to drive in a manual vehicle.

Until recently, only more expensive car models were equipped with ADAS. The large number of different versions and variants of ADAS poses a problem for developing competence in their use. Examiners benefit from uniformity; it is difficult to stay informed of the exact functioning and limitations of all the different systems. There are also concerns about the competence of driving instructors in the area of ADAS. The CBR is studying how ADAS can be integrated in driving tests together with the SWOV Institute for Road Safety Research and other parties.

In June 2019, 42 parties joined forces in the ADAS Alliance and established an ADAS Covenant (see section 4.2.3). Raising awareness of ADAS is one of the pillars of this covenant. One of the measures is an online community (slimonderweg.nl), where information is provided about the opportunities and risks offered by ADAS, among other things. The website emphasizes that self-driving cars are not yet a reality and that drivers must remain vigilant.

[86] ANWB, *Welke rijhulpsystemen zijn er?*, 2017.

**Partial conclusions**

The changing role of drivers from 'active drivers' to 'operators' leads to longer response times and drivers missing information from their surroundings. This is augmented by the fact that some drivers rely too heavily on ADAS. This overestimation of ADAS is in turn augmented by the manner in which car manufacturers communicate and by advertisements and the media.

Users have only limited insight into how ADAS works. Communication about how ADAS works and should be used is sometimes inadequate, and the provision of information and instruction is often lacking. The driving test does not include ADAS.

ADAS risks are mitigated by installing even more systems (alertness and fatigue monitoring systems), which are also still immature.

## 3.3 Interaction between vehicles and drivers

*Problem*

Although there is formally still only one driver in current ADAS-equipped vehicles (namely the human driver, who is fully responsible for the driving task), in practice there appear to be two drivers (the human driver and the automated system), which leads to new risks. Studies in another context (in this case accidents at work), have revealed that accidents occur mainly when several people are jointly responsible for a single process or when several people are responsible for various sub-processes that influence each other.[87] Problems particularly arise due to the ambiguity and conflicts that can occur in overlapping and intersecting areas. This also applies to vehicles with ADAS, for example because a human driver assumes that the automated system is controlling the process, or because a human driver does not know what their responsibility is in relation to the automated system. It is also possible that the driver is not sure whether or not the ADAS has been engaged. Cars with ADAS engaged sometimes respond differently than a human driver would. Conversely, ADAS may assume that the driver will intervene when necessary (see also section 3.2), either with or without a warning. So, the question arises as to who is actually in control.

*Fatal accident with Tesla Model S*

On 30 January 2019, a Tesla Model S was driving on the N277, a provincial road near the town of Zeeland (Noord-Brabant). Data from the vehicle revealed that it was travelling at a speed of approximately 83 km/h with ACC engaged.

To engage Autopilot, the driver must successively engage ACC and LKA[88] Autopilot only functions on roads with clear road marking that can be detected by the system.

[87] Leplat, *Occupational Accident Research and Systems Approach*, Journal of Occupational Accidents 6, number 1–3, 1984.

[88] Tesla uses the terms TACC and Autosteer for ACC and LKA.

Content
Considerations
Summary
Recommendations
Abbreviations
1 Introduction
2 Reference framework
3 Managing safety risks
4 Bottlenecks in the safe introduction and deployment of ADAS
5 Bottlenecks in monitoring and adjustment
6 Conclusions
7 Recommendations
References
Appendices

The driver of the Tesla was under the impression that the Autopilot system had been engaged and that the vehicle was maintaining its position in the lane.

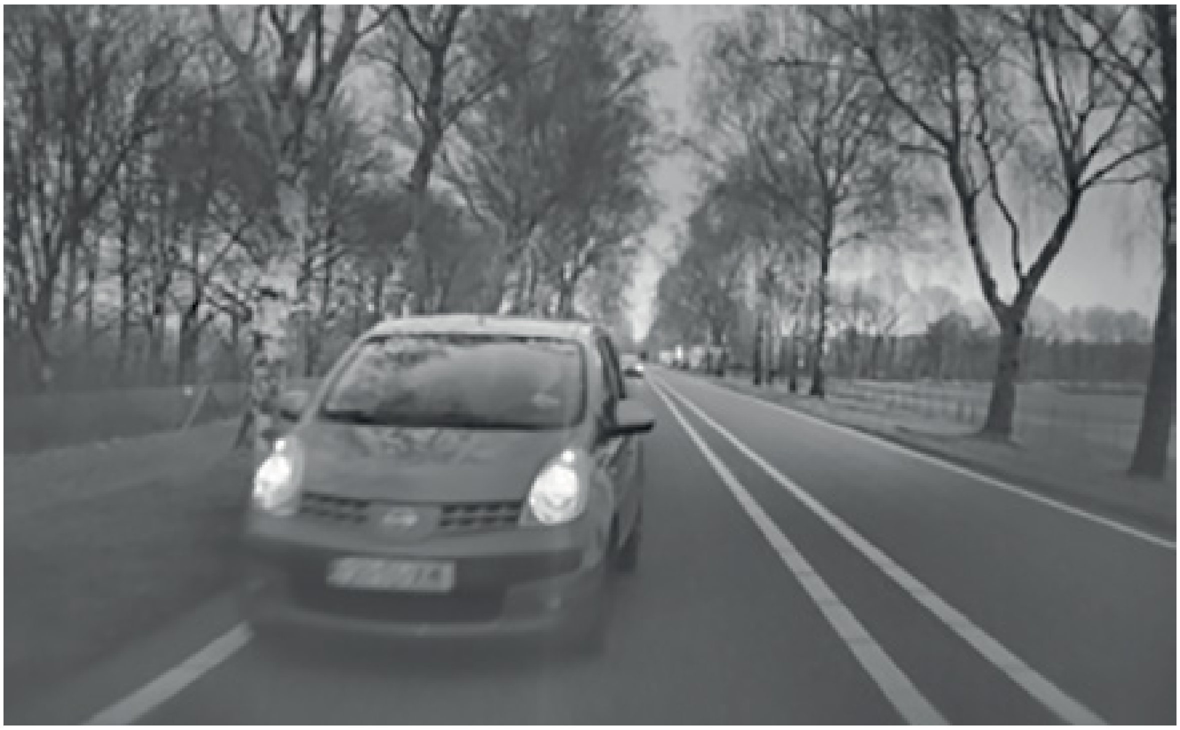


*Figure 9: Photograph taken by the camera in the Tesla just before the collision.*

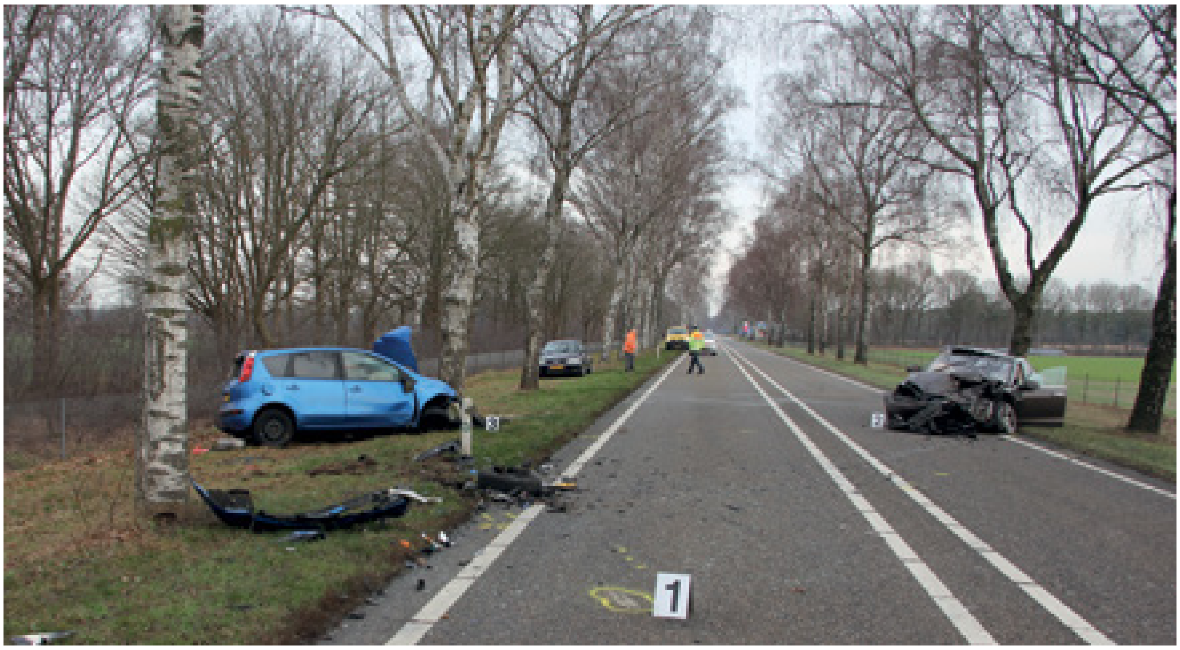


*Figure 10: Both vehicles after the collision. (Source: police)*

When the driver of the Tesla briefly turned his attention to the display in the centre console, he noticed that the vehicle had moved to the adjacent lane and was approaching an oncoming vehicle. The Tesla collided into the oncoming Nissan. The driver of the Nissan was killed; the driver of the Tesla was uninjured.

Data from the vehicle revealed that the Tesla's Autosteer (LKA) had not been engaged. The driver's hands had not been detected on the steering wheel for a period of 9 seconds prior to the collision. Approximately 23 seconds before the impact, the driver pressed the cruise control lever of the Autopilot system up twice in quick succession. The first time the lever was pressed up it adjusted the TACC pre-set speed to the current speed, the second time, the pre-set speed was increased to 85 km/h. The driver had made a mistake: pressing the cruise control lever up twice closely resembles the action of pulling the lever twice towards you (see blue box). The feedback on the display differs in colour, namely a grey or blue steering wheel icon to the right of the speed. In addition, the driver receives an audio signal as feedback when activating Autosteer.

The Tesla was equipped with an Advanced Emergency Braking System, but the current generation of this system does not function in collisions with oncoming vehicles.

**Activating Tesla's Autopilot**

The Tesla's Autopilot is engaged by means of a shift lever on the left rear of the steering wheel. Autopilot comprises a combination of TACC and Autosteer. TACC can be engaged in two ways. The current speed can be set and maintained by moving the cruise control lever up or down. By pulling the lever towards the driver, the speed limit or current speed of the vehicle is maintained. TACC can only be switched on when the system is available, as shown by the grey speedometer icon on the instrument panel.

If Autosteer is available, a grey Autosteer icon will appear on the display, and it can be engaged by pulling the lever towards the driver again. This must be done shortly after activating TACC. After activating Autosteer, the driver receives an audio signal and the Autosteer icon will turn blue. Moving the lever up or down adjusts the pre-set TACC speed incrementally but will not disengage Autosteer.

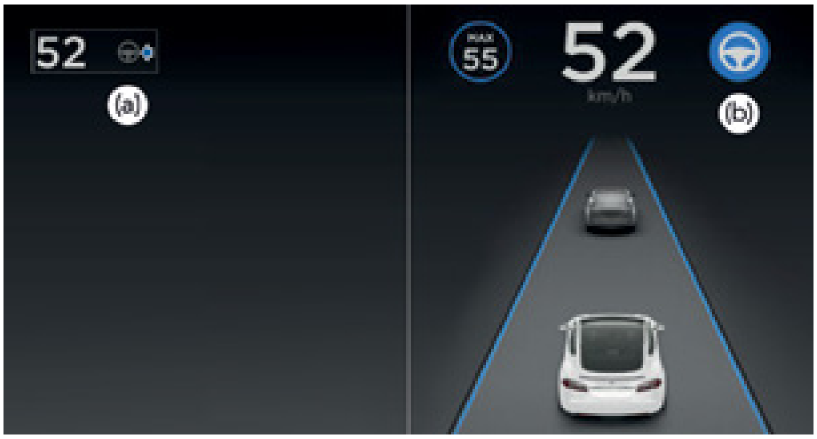


*Figure 11: (a) If Autosteer is available, a grey Autosteer icon is displayed on the dashboard, (b) the icon turns blue when Autosteer is engaged. (Source: Tesla Model S user manual[89])*

*Uncertainty about who is in control*
The driver involved in the frontal collision thought that he had engaged Autosteer, while this was not the case. Because of this mistake, he was paying less attention to the road. Many makes of car facilitate various states of the system and there are subtle differences in operation and (audio)visual feedback, so mistakes are easily made.

In dangerous situations, where a human is required to assume control, it is important that this is made clear to the driver so that they can do so in good time. In addition, it is important that the system can safely disengage in situations where the human driver fails to take control in time or if they are insufficiently alert. In practice, drivers of various makes of car experience that in common situations, e.g. approaching a roundabout or a sharp bend, the system fails to provide a timely warning that the driver needs to take control. Insufficient alertness on the part of drivers can lead to additional problems.

*Lack of a foolproof design*
The design was not sufficiently foolproof, because a driver's operating error could lead to a serious accident. Another factor was that the driver did not notice that the vehicle was not behaving as he expected because he was distracted by the car's dashboard. Drivers being distracted is a common issue when using ADAS (see section 3.2).

An ADAS can operate a vehicle under certain conditions. For example, the system must be able to detect road marking, it can only be engaged above or below a certain speed, and it can only corner safely in bends of a certain radius. The latter limitation often also depends on the speed, so that the driver may think, based on previous experience, that the system can handle a sharp bend at speed, while in fact this is not the case.

[89] Tesla, *Tesla Model S Owner's Manual*, 2018.

This could happen, for example, because the car took the turn at a lower speed on a previous occasion because the system automatically lowered the speed in response to a slower vehicle in front. In addition, circumstances such as the weather and the incidence of light sometimes play a role. Not all situations can be anticipated, but even in common situations – such as approaching a roundabout, or taking a tight bend – insufficient consideration has been given to the way an ADAS disengages and alerts the driver to take full control of the vehicle. This can result in unsafe situations.

*Identifying and managing the risks*

According to car manufacturers, it is absolutely clear that the driver must always stay alert with the current generation of ADAS. From a legal point of view, it is clear who is responsible in the current generation of ADAS. ADAS assists or supports the human driver to carry out the driving task. The driver formally drives the vehicle and is therefore always responsible. At the same time, the driver is insufficiently equipped. This is because the systems lead some human drivers to have different expectations of them (see section 3.2), while these systems are not yet mature (see section 3.1). These expectations are in part fed by the media and the marketing information provided by manufacturers. In addition, drivers are not always aware of the status (on/off) of the system in their car. This has to do with uncertainties in the operation of the vehicle, the provision of feedback (e.g. the status on the dashboard) and the wide variety of ADAS (see box). Manufacturers recognize the risk caused by the lack of clarity about who is driving. They try to manage this risk by referring to the liability principle and their disclaimers, rather than scrutinizing the safety of their systems in combination with the humans who use them.

The large variation in ADAS contributes to the lack of clarity about the status of the system. The partners in the ADAS Alliance (see section 4.2.3) intend to submit proposals to RDW (on European regulations) and Euro NCAP (the manufacturers) to develop generic names and symbols for ADAS and, where possible, to standardize their operation. The responsibility for implementing these proposals lies with the manufacturers, because there is no legal requirement for them to do so now. At present, manufacturers do not cooperate to this end, with the exception of the partnerships between Daimler and BMW[90] and between Volkswagen and Ford[91], who are cooperating in the development of ADAS and self-driving cars. A second exception is ADAS that temporarily take over control of the human driver. UNECE has laid down a number of harmonised requirements for this in Regulation R.79 (see Annex E4).

[90] Daimler, *BMW and Daimler. Plan to Headquarter Joint Venture in Berlin*, https://www.daimler.com/innovation/case/shared-services/jv-daimler-and-bmw.html, accessed August 22, 2019.

[91] Volkswagen, *Ford – Volkswagen Expand Their Global Collaboration to Advance Autonomous Driving, Electrification and Better Serve Customers*, https://www.volkswagen-newsroom.com/en/press-releases/ford-volkswagen-expand-their-global-collaboration-to-advance-autonomous-driving-electrification-and-better-serve-customers-5188, accessed August 22, 2019.

### Diversity of ADAS

There are differences between ADAS in different car makes and models, but also between different software versions. These ADAS all operate and respond differently and all have different operational limitations (for example the maximum speed they can operate at). Manufacturers use these systems to distinguish themselves from other makes and so use their own names to describe the systems. A study by the American Automobile Association (AAA)[92] revealed that there are as many as 19 different names for 'Lane Keeping Assist', such as: Active Lane Assist (Audi), Active Steering Assist (Mercedes-Benz), Lane Assist (Seat), Lane Keeping Alert (Ford) and Intelligent Lane Intervention (Nissan). Lane Keeping Assist is also often part of systems that can control the direction and speed of the vehicle, for example: Autopilot (Tesla), Pilot Assist (Volvo) and ProPILOT (Nissan). This is also the case for other ADAS.

Human machine interaction is not an explicit part of vehicle regulation and type approval. To the extent that this is included, it forms an integral part of the technical requirements. UNECE is not currently developing any new legal requirements in the field of human machine interaction involving ADAS of SAE level 1 and 2. The Ministry of Infrastructure and Water Management has mandated RDW to contribute to UNECE WP.29 (vehicle requirements, see Appendix E) on behalf of the Netherlands. In spite of efforts to develop knowledge, the RDW only has limited knowledge in the field of human machine interaction. As a result, Dutch contribution to UNECE in this area is also limited. The EC has made no requests to develop requirements to this end.

Furthermore, governments consider that HMI (Human Machine Interaction) legislation is less important for the current generation of ADAS because the driver is liable (see further section 4.2.2). From a legal point of view, ADAS only assist or support the human driver in the driving task. In practice, however, ADAS fully take control under certain conditions. Systems can accelerate, steer and brake until they find themselves in a situation for which they are not designed. This means that HMI legislation is also important for the current generation of ADAS.

UNECE[93] indicates that much research is still needed into human factors and ADAS, because only general principles have been described to date. It is suggested that the driver of a car with ADAS will function optimally if the driver:

- is *in the loop* and not *out of the loop;*
- has an average mental workload;
- always has good situational awareness when driving;
- has the appropriate level of confidence in the assistance system;
- does not display any negative change of behaviour in response to the assistance system.

[92] AAA, *Advanced Driver Assistance Technology Names*, 2019.
[93] Appendix to Annex 5 of the UN R.E.3

To make these general principles more concrete, UNECE recommends further investigation of the following points:

- Methods to measure situational awareness while driving, to understand how this varies, and to estimate the preferred level of awareness and how this can be maintained.
- Methods to measure mental workloads that are too low or too high, to prevent excessive reliance on ADAS by drivers and to prevent negative changes of behaviour by drivers in response to ADAS.
- Explore ways to ensure that drivers maintain responsibility as the level of in-car automation increases.

To learn more about human factors and ADAS, the first naturalistic driving study (5 makes, 20 test subjects) has been performed in the Netherlands for three years. This study is being carried out by TNO in collaboration with the SWOV Institute for Road Safety Research on behalf of the Ministry of Infrastructure and Water Management (IenW), RDW and Rijkswaterstaat. The first phase of this research (mainly data collection) has been completed. IenW assesses whether follow-up research is necessary and, if so, how the study questions will be defined. A large naturalistic driving study is also underway in the United States.[94] The first results of this study show that drivers use Autopilot in more than a third of the distance driven and appear to maintain a relatively high degree of vigilance.[95] A possible explanation for this is that Autopilot is not yet perfect and drivers intervene on average every 16 km. This could mean that as systems improve, drivers will be less alert.

The Ministry of Infrastructure and Water Management and the EC are aware of the existence of human machine interaction risks. For example, the risks are seen as a challenge for the development of automated driving.[96] Like any innovation, the current generation of ADAS has advantages and disadvantages. These advantages and disadvantages must be weighed against each other. The advantages must outweight the disadvantages. The advantage of ADAS is the constant and high safety level of the part of the driving task that is supported or taken over by the ADAS. A disadvantage is that the driver cannot always intervene if a system fails. In such circumstances, the human driver is hence regarded as a safety barrier. Accident investigations and studies have revealed that humans cannot function as a safety barrier when they are distracted. This also leads to the paradoxical situation that the driver ultimately has to guarantee safety, while the driver's role has actually been reduced by automation, partly in the interests of safety. Moreover, if humans are indeed the most important 'safety barrier' in certain circumstances, it is all the more salient that the question of how humans and machines interact has hardly been taken into account in the introduction and deployment of these systems and the approval process. All the more because the driver's role as operator (section 3.2) has made it more difficult for them to respond adequately.

[94] Fridman et al., *MIT Advanced Vehicle Technology Study: Large-scale Naturalistic Driving Study of Driver Behavior and Interaction with Automation*, IEEE Access 7, 2019.
[95] Fridman et al., *Human Side of Tesla Autopilot: Exploration of Functional Vigilance in Real-world Human-Machine Collaboration*, 2019.
[96] High Level Group on the Competiteness and Sustainable Growth of the Automotive Industry in European Union, *Gear 2030*, 2017.

**Partial conclusions**

It is sometimes unclear to drivers who is in control of the vehicle. This can lead to accidents, partly because the systems are not foolproof and mistakes made by the user are not always compensated, prevented or mitigated. This leads to the paradoxical situation that the technology has to make driving safer, but that the driver, as the ultimately responsible person, has been put in a more difficult position.

Manufacturers and government agencies often refer to the liability principle (the driver as safety barrier), rather than scrutinizing the safety of the systems in combination with the humans who use them. Human machine interaction is not an explicit part of the requirements for type approval.

More (scientific) research is needed into human factors and ADAS in practice, for example in the form of naturalistic driving studies.

## 3.4 Dynamics of automation

*Introduction*

There is a long history of digitization in cars. In 1977, the ECU[97] (Electronic Control Unit, see Figure 12), i.e. software, was introduced in the car. Since then, the amount of software has grown significantly (see Figure 13) thanks to automated systems such as ADAS, but also navigation and infotainment systems. ADAS observe their surroundings by means of sensors. These sensors generate large amounts of data that are processed by computer systems in the car. The computer system uses algorithms to determine how it should support the driver in the driving task. This may involve activating the brake or generating a warning.

[97] An ECU is a kind of mini-computer that can be found as a control unit in various systems within a vehicle. They are used, among other things, to adjust the climate control, infotainment system and advanced driving assistance systems.

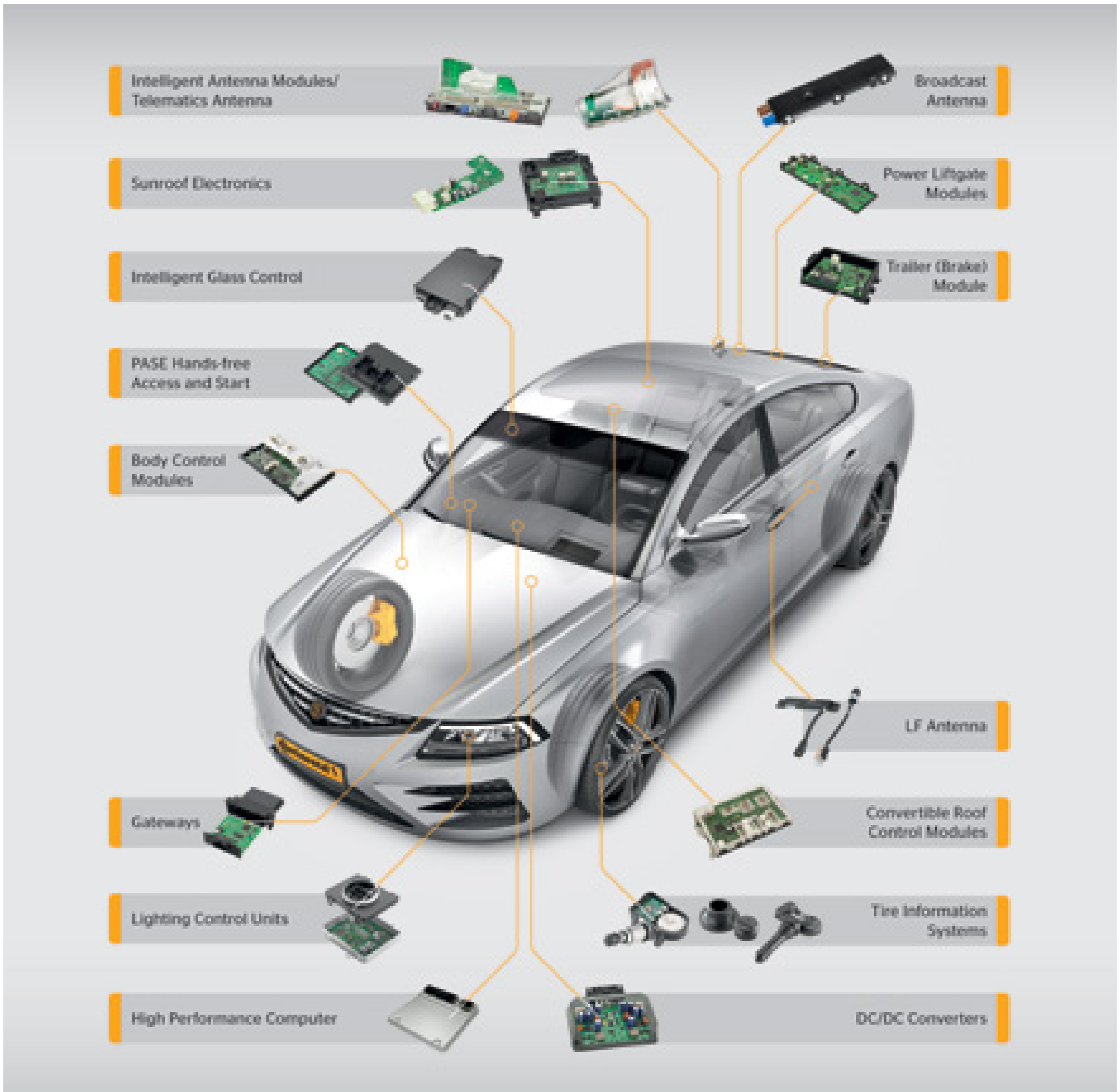


*Figure 12: Various Electronic Control Units (ECUs) used in vehicles. (Source: Continental[98])*

The amount of software in modern vehicles has increased enormously with the advent of modern ADAS (see Figure 13). To compare: there is more software in a modern car than in a Boeing 787 passenger airplane or an F-35 fighter plane[99, 100]. With the advent of 'connected cars' – vehicles that can communicate with each other and exchange information with the road infrastructure – it is expected that the amount and complexity of software in vehicles will only increase.

[98] Folda, *From Requirement to Standard Security Test; A Brief Introduction to the World of Security Testing*, Vector Cybersecurity Symposium 2019, 2019.

[99] McCandless, Doughty-White, and Quick, *Million Lines of Code*, https://informationisbeautiful.net/visualizations/million-lines-of-code/, accessed July 10, 2019.

[100] Charette, *This Car Runs on Code*, https://spectrum.ieee.org/transportation/systems/this-car-runs-on-code, accessed August 21, 2019.

Content
Considerations
Summary
Recommendations
Abbreviations
1 Introduction
2 Reference framework
3 Managing safety risks
4 Bottlenecks in the safe introduction and deployment of ADAS
5 Bottlenecks in monitoring and adjustment
6 Conclusions
7 Recommendations
References
Appendices

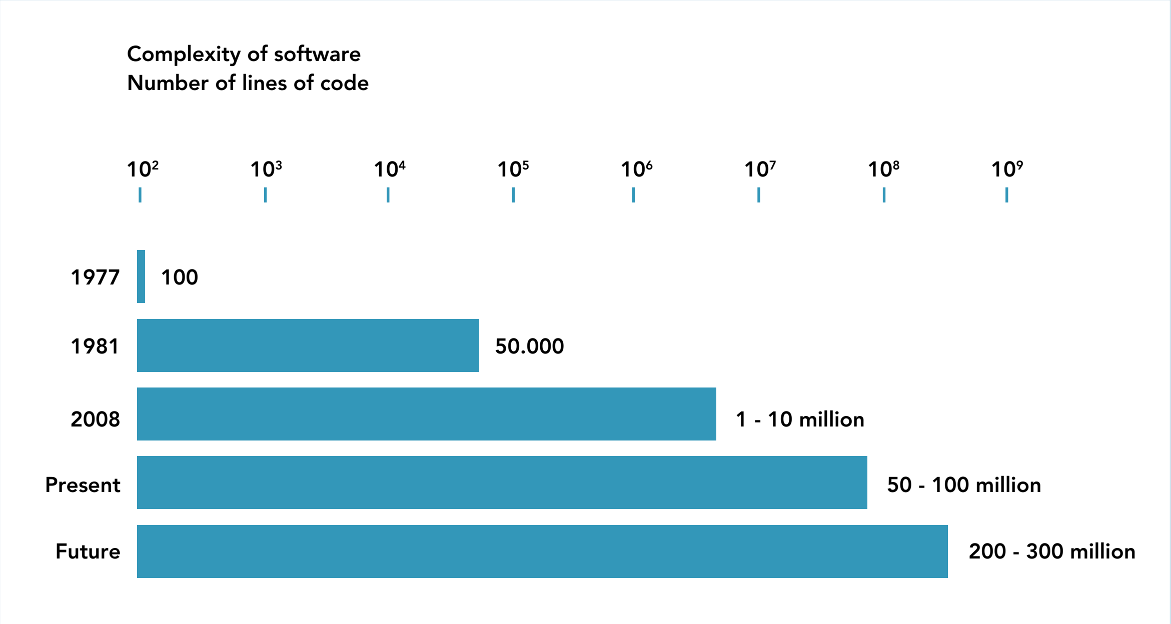


*Figure 13: Increase in the amount of software in cars. (based on data obtained from C't magazine[101])*

It takes a long time to develop a new model car, often requiring several years before the new model rolls off the production line. Software development, on the other hand, is usually an iterative development process, whereby the design, assembly, testing and roll-out phases are alternated and run partly in parallel. These two worlds have now come together in the automotive industry. On the one hand, there is the world of the static, mechanical car, which does not undergo any changes after production (with the exception of a few minor tweaks). On the other hand, there is the new reality of the driving computer, whereby software updates implemented while the vehicle is already in use can entail major changes to the functionalities of the vehicle, and thus to driving behaviour. The transition to driving computers has consequences for the automotive industry. Volkswagen currently works with 70 different operating systems that run on software provided by almost 200 different suppliers. It is now considering how to simplify this software landscape.[102]

All software code contains errors. To minimize these errors, the automotive industry applies various standards to ensure the programs are safe.[103] The ISO standard[104] requires that extra attention be paid to this in safety-critical software. Although manufacturers indicate that they comply with this standard, new software will inevitably contain errors (bugs) and vulnerabilities when it is introduced. If bugs or vulnerabilities are discovered after the introduction of the car, and they have an impact on its proper functioning or safety, they must be resolved as soon as possible. A prerequisite for easily accessible software updates is that the car must have an Over-The-Air (OTA)[105] update feature. This is currently only the case in the latest and more expensive models, but is being applied more and more.

[101] C't Magazine, *Connected Cars in de fout bij cybersecurity*, 2016.
[102] Volkswagen, *Volkswagen start car.software met 5.000 in-house ontwikkelaars*, 2019.
[103] British Standards Institution, *Connected Automotive Ecosystems – Impact of Security on Safety – Code of Practice*, 2018.
[104] ISO, *ISO 26262-6:2018 Road Vehicles - Functional Safety - Part 6: Product Development at the Software Level* Gene, 2018.
[105] OTA refers to the process of remotely adjusting software or configuration settings on electronic devices.

The majority of existing cars has no OTA update mechanism and in these cars the software can only be updated by a dealer or car repair shop. This is expensive and is only done in practice if it is necessary to comply with product responsibility[106] or to add new functionality.

*Problem*

There may be risks associated with updating the software in vehicles, or in fact failing to implement updates.

Older vehicles may be at risk if they do not receive important updates. The way software is updated is important for fixing bugs and for the continued proper functioning of the vehicle. Today's cars will be on the roads for at least 20 years, while computer systems and consumer electronics are usually supported by manufacturers for a maximum of five years.[107] It is unclear whether the software and hardware is supported for the entire service life of the vehicle. If this is not the case, the ADAS software in older cars will not be updated after a certain point and any remaining bugs will not be fixed.

Changes in human machine interaction gives rise to risks when updates are used to introduce new functionalities or to modify existing ADAS. The driving behaviour of the vehicle will change as a result, with the risk that it will respond differently than a driver expects and/or is used to. This potentially applies even more to OTA updates than to updates performed by a dealer, because the dealer has the opportunity to inform the driver about the changes. Drivers are often given only limited information about updates, while clear instructions for drivers are essential in cases where the driving behaviour of a car changes as a result of a software update. This information is currently often provided in the form of a pop-up on the dashboard display. This is not an effective way of informing drivers about a change in driving behaviour, because the pop-up appears at the moment the driver is about to drive off. Above all, it is often shown which functionality changes, but not what effect this has on the performance of the driving task. In addition, the driving task involves ingrained patterns in human machine interaction, so a driver may not respond as required to the changes in the car's driving behaviour even if they have been fully informed.

Using OTA for updates has several advantages but also introduces new cybersecurity risks (see section 3.5).

*Identifying and managing the risks*

Regular updates are required to maintain the computer systems in modern cars. Tesla is an example of a manufacturer that makes intensive use of OTA. In a Tesla, the driver has the choice to decide when and where to install updates. After the installation, the driver receives an overview on the dashboard screen that describes any changes to system regarding functionality or capabilities. It is also possible for the driver to receive a notification on the mobile phone, so that the driver knows when an update has taken place. Most cars currently on the road do not have OTA functionality. Manufacturers have

[106] In line with R79, Annex 6, UNECE 1958 agreement which indicates that software should be safe.
[107] An example of this is the software on smart TVs. Source: Van der Staak, *Verdwijnende apps op smart-Tv's*, 2018.

Content
Considerations
Summary
Recommendations
Abbreviations
1 Introduction
2 Reference framework
3 Managing safety risks
4 Bottlenecks in the safe introduction and deployment of ADAS
5 Bottlenecks in monitoring and adjustment
6 Conclusions
7 Recommendations
References
Appendices

so far been reluctant to install OTA systems because the technology is new and there are costs involved in its implementation. Resolving software errors in cars without OTA functionality is a relatively slow and costly process because this has to be carried out at a dealership. Drivers who do not regularly visit the dealer will not know whether the latest version of the software is installed in the vehicle. In addition, it is not always clear to the driver which errors have been solved in a particular software version. Regulators and investigation authorities have no insight into which cars have installed the latest software version. It is therefore unclear which vehicles this problem applies to and how big the problem is.

Manufacturers do not provide users with clear information about the service life of their product, so they do not know how long the manufacturer will continue to actively support the computer systems in different makes and models.

The way software is updated, which may potentially have an impact on driving behaviour, is not yet regulated and therefore unsupervised. There are also no specific requirements for maintaining software in ADAS. However, in general terms, the manufacturers are held to their duty of care and their cars must remain safe.[108] Regulations for software and software updates are under development (see section 4.2.2).

It should also be noted that there are no limits with regard to changing ADAS software during the service life of the vehicle. Changes to software that affect a vehicle's emissions have been subject to stricter supervision since the emissions scandal in 2015 (see box below).

**Emissions scandal**

Software is dynamic and affects the behaviour of the car. A well-known recent example is the emissions scandal involving the combustion behaviour of diesel engines. The on-board computer recognized when an emissions test was being conducted and altered the behaviour of the engine to keep it within the predefined emissions levels during the test. Millions of cars of various makes were recalled worldwide to replace this 'cheating software' and ensure that the cars met the required standards on the road too.[109]

RDW has reached agreements with an individual manufacturer on limits to changing software of existing cars before vehicles already bearing a licence plate have to undergo a new assessment in order to continue the type approval (see box below). This is a temporary and informal agreement for a specific case, and not a standard solution, among other reasons because it is unclear what will happen when the manufacturer stops producing this particular model and the cars still on the road require an update.

[108] Regulation (EU) 2018/858, Article 14.
[109] Teffer, *Dieselgate. Hoe de industrie sjoemelde en Europa faalde*, 2017.

**Gentlemen's agreement**
In order to gain some control of the risks associated with the dynamic nature of software updates, RDW has made agreements with a car manufacturer about updating software in their vehicles. Vehicles already in use receive the same updates as those applied to newly manufactured vehicles. The idea behind this is that if newly manufactured vehicles must comply with the approval requirements, then vehicles already in use will comply with them too.

**Partial conclusions**
Software affects the behaviour of cars. Software must be updated during the service life of a vehicle, in particular to correct bugs. ADAS can be improved during their service life by implementing software updates to incorporate new insights or the advantages of new models.

Safety risks can arise both when important safety updates are not implemented, and when updates are implemented that change the functionality of the vehicle.

Car manufacturers are not required to fix software errors during the service life of the car, but they are held to their duty of care and their cars must remain safe. Many existing car models do not have OTA functionality for efficiently performing software updates.

There is currently very little legislation governing the software in ADAS. As a result, it is impossible to supervise these dynamic automated systems.

## 3.5 Cybersecurity

ADAS comprises various sensors and computer systems installed in the vehicle. Automation technology has developed rapidly in recent years, which has led to an exponential increase in the amount of software and hardware installed in ADAS cars compared to conventional vehicles. This means the risks associated with computers are also increasingly being introduced in cars with ADAS.

*Problem*
The advent of advanced ADAS in vehicles entails cybersecurity risks. Today's vehicles equipped with ADAS have more external connections (i.e. a larger attack surface) and thus more digital inputs that need to be protected against deliberate misuse[110]. An ADAS also establishes a more direct link between the vehicle's computer systems and its control mechanisms, so that in theory, anyone with digital access to the ADAS could control the vehicle remotely. This means that someone with malicious intent who succeeds in gaining

[110] Examples include connections to the manufacturer's computer systems, wifi in the car and Bluetooth connections.

Content
Considerations
Summary
Recommendations
Abbreviations
1 Introduction
2 Reference framework
3 Managing safety risks
4 Bottlenecks in the safe introduction and deployment of ADAS
5 Bottlenecks in monitoring and adjustment
6 Conclusions
7 Recommendations
References
Appendices

this access could remotely control a car, or several cars, for example by braking, steering, accelerating or deactivating the brakes, with potentially disastrous consequences for road safety.

The connections between modern vehicles and the manufacturer's computer systems for delivering software updates, traffic information, maintenance warnings and general information means these systems also play an important role in the cybersecurity of the cars. If these systems were compromised, an attacker could gain digital access to multiple cars simultaneously without having to be physically present.

*Ethical hacks*

Several studies (ethical hacks[111]) have proven that systems in vehicles already on public roads today can be hacked; they contain vulnerabilities that can be exploited, thereby compromising road safety.

In 2014, American researchers were the first to demonstrate that they could remotely hack the computer systems of a Jeep Cherokee and a Toyota Prius[112, 113, 114]. They were able to take control of a number of ADAS and thus influence the driving behaviour of the car. When the researchers hacked the Jeep Cherokee, they were in a position to seriously endanger the lives of the driver and passengers. For example, they were able to switch off the engine, deactivate the brakes and control the steering wheel to influence the direction of travel. In response to this hack, Jeep decided to recall 1.4 million cars to fix the vulnerabilities.[115] The recall actually involved sending a USB memory stick to the owners of the cars so they could update the vehicle themselves. This means there was no guarantee that all vehicles were updated in good time.

[111] An ethical hack tests computer and network security systems to detect errors and security holes in the systems and networks and then reports them to companies or agencies.

[112] Greenberg, *Hackers Remotely Kill a Jeep on the Highway—With Me in It*, https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/, accessed August 17, 2018.

[113] Greenberg, *Hackers Reveal Nasty New Car Attacks--With Me Behind The Wheel (Video)* Forbes, https://www.forbes.com/sites/andygreenberg/2013/07/24/hackers-reveal-nasty-new-car-attacks-with-me-behind-the-wheel-video, accessed August 23, 2018.

[114] Greenberg, *The Jeep Hackers Are Back to Prove Car Hacking Can Get Much Worse*, https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks/, accessed August 23, 2018.

[115] Greenberg, *After Jeep hack, Chrysler recalls 1.4M vehicles for bug fix*, https://www.wired.com/2015/07/jeep-hack-chrysler-recalls-1-4m-vehicles-bug-fix/, accessed August 17, 2018.

Content
Considerations
Summary
Recommendations
Abbreviations
1 Introduction
2 Reference framework
3 Managing safety risks
4 Bottlenecks in the safe introduction and deployment of ADAS
5 Bottlenecks in monitoring and adjustment
6 Conclusions
7 Recommendations
References
Appendices

*Figure 14: During the experiment with the Jeep Cherokee, the braking system was deactivated such that the driver could no longer brake and the vehicle ended up in a ditch. (Source: Wired)*

In 2016, Chinese researchers at Keen Security Lab (part of Tencent, a Chinese internet company) carried out an ethical hack on all of Tesla's existing models at the time. They were able to remotely control and influence various components of the Teslas, such as folding in the side mirrors or opening the boot while the vehicle was driving. It was also possible to activate the brakes and disable the power steering and ABS.[116] Tesla solved these vulnerabilities within a few days with an OTA update, as was confirmed by the Keen Security Lab researchers.

More recently, Keen Security Lab spent a year researching the security of BMW cars (the research was completed in February 2018), which revealed several vulnerabilities. The findings were published and presented at the Blackhat USA security conference, after they were first reported to BMW so it could take mitigating measures.[117, 118] The identified vulnerabilities made various attack scenarios possible. Using a simulated mobile network, the researchers were able to access the Telematics Control Unit (TCU)[119]. It was also possible to manipulate the infotainment system by gaining local access to the vehicle and to take over the vehicle's communication system using BMW's ConnectedDrive service. Once an attacker had digital access to the car, it was possible to send messages to secure ECUs and hence control specific functions of the vehicle, despite the presence of domain isolation. By sending a text message through the simulated mobile network, it was also possible to mislead BMW's Remote Services and open the door of the vehicle or operate the climate control. Immediately after receiving the report of the problems, BMW blocked access through the simulated mobile network by implementing an OTA

[116] Nie, Liu, en Du, *Free-fall: Hacking Tesla from Wireless to CAN Bus*, in Blackhat Briefings USA, 2017.
[117] Tencent, *Experimental Security Assessment of BMW Cars: A Summary Report*, 2018.
[118] Cai et al., *0-Days & mitigations : Roadways to Exploit and Secure Connected BMW Cars*, White Paper Blackhat USA 2019 Conference, 2019.
[119] A TCU is an in-car computer system that collects data. The system can share this data with the manufacturer or the owner. Parameters include the position and speed of the vehicle.

update in the affected models. The vulnerabilities in the vehicles and the problems with the servers that connect to the cars have since been resolved. BMW's transparency in this incident and the fact that they shared their experiences serves as an example to the automotive industry.

*No accidents involving cybersecurity reported*
No accidents have been reported to date in which cybersecurity played a role. This does not mean that such accidents can be ruled out. Security researchers in various countries have been able to hack into cars from the outside and thereby influence the car's driving behaviour, demonstrating that it is possible. However, the vehicles and the manufacturers' data centres do not store sufficient information to be able to investigate whether a cybersecurity incident was the cause of an accident, nor is this actively monitored. As such, it is never certain whether cybersecurity played a role in the occurrence of an accident.

Requirements currently under development for the Event Data Recorder (EDR) (see also section 5.2.2) do not cover the storage of data that can provide insight into possible cybersecurity incidents.

*Identifying and managing the risks*
Government authorities, manufacturers and suppliers have been paying more attention to cybersecurity in recent years. The automotive industry has developed standards that a large proportion of manufacturers and suppliers already comply with, and the rest is following suit. For example, in 2016 the SAE (Society of Automotive Engineers) published a handbook to help organizations in the sector to identify and quantify cybersecurity threats and to take them into account in the development of their vehicles.[120] These standards relate to the points described in our reference framework (see section 2.2). The sector is currently developing an ISO/SAE standard for cybersecurity in the automotive industry[121] that will be published in 2020.

In addition to industry standards, various government agencies such as ENISA and NHTSA and the British government have published guidelines and best practices. [122, 123, 124, 125] Various European research projects have also been carried out in the field of connected car security.[126] However, there is no specific legislation as yet for cybersecurity in and around cars (developments in legislation are described in section 4.2.2). Cybersecurity is currently described as a guideline in an annex to the approval requirements.[127]

[120] AE International, *Cybersecurity Guidebook for Cyber-physical Vehicle Systems - J3061*, 2016.
[121] ISO/SAE 21434 - Automotive Cybersecurity Engineering Standard under development.
[122] NHTSA, *A Summary of Cybersecurity Best Practices*, 2014.
[123] NHTSA, *Cybersecurity Best Practices for Modern Vehicles*, 2016.
[124] ENISA, *Cyber Security and Resilience of Smart Cars; Good Practices and Recommendations*, 2016.
[125] British Standards Institution, *The Fundamental Principles of Automotive Cyber Security. Specification*, vol. PAS 1885, 2018.
[126] For example https://www.preserve-project.eu/, https://www.evita-project.org/.
[127] ECE/TRANS/WP.29/78/Rev.6 Annex 6

Manufacturers can incorporate new cybersecurity principles in the design process of new models as standard, but these are not mandatory. This is not the case for older vehicles that have been on the road for several years, because they were designed and produced at a time when there was less attention for cybersecurity. In older ECU models, it is sometimes impossible to modify the software due to a lack of storage capacity or the absence of an update mechanism.

Older models of cars are not designed to keep track of software security for the entire service life of the vehicle. Mitigating measures to limit the likelihood of abuse of a certain vulnerability may be possible when there are no technical solutions for vulnerabilities. This may be sufficient to limit the worst risks, but because the vulnerabilities remain unresolved, the defence-in-depth strategy (cybersecurity principle 5) is undermined.

In the automotive industry, it is unusual to publish information about issues related to cybersecurity, because it is assumed that transparency in this area may lead to more security problems. If a current vulnerability is made public this can have major consequences. Due to this lack of transparency, it is not known whether the vulnerabilities exposed by the ethical hacks are exceptions or whether similar problems occur in more vehicles. Independent cybersecurity experts investigate vehicles much less often than they hack regular software systems, because it is more expensive, there is less information available about the hardware and software, and there is usually no source code available. Inspection authorities, fleet owners and individual car owners therefore have very little information about potential vulnerabilities in the systems of a particular make of car.

**Partial conclusions**

The introduction of advanced ADAS in vehicles and the increase in the number of external connections entails cybersecurity risks. Car manufacturers are aware of the importance of cybersecurity and demonstrate this by their commitment to developing standards and best practices.

No accidents have been reported to date in which poor cybersecurity played a role. This does not mean such accidents can be ruled out. However, insufficient information is stored to be able to investigate whether a cybersecurity incident was the cause of an accident.

Independent cybersecurity tests are not often carried out, while these could make the sector more resilient to cyberattacks. Inspection authorities, fleet owners and individual car owners do not have access to much information about potential vulnerabilities. Existing vehicles may not comply with current cybersecurity standards and may therefore pose a permanent safety risk, while there are no systems in place to monitor this.

## 3.6 Conclusions

The ongoing development of automation in the vehicles on the road focuses on the benefits of technology and fails to give due attention to the importance of the driver. Systems are being introduced to the market that are not yet fully developed and hence immature. The current generation of ADAS (SAE Level 2) is based on the principle that the driver bears full responsibility and that the systems are only there to provide support. This means that the driver can, and must, always intervene when a system fails. Drivers experience this differently in practice, however. In their experience, they share the control of the vehicle with the systems installed in it. Moreover, drivers in the role of operator have more difficulty responding adequately than active drivers without ADAS. The systems are insufficiently tailored to the human user and humans are not trained to use these systems.

The car is gradually transforming into a driving computer. This increases cybersecurity risks and it is not known to what extent manufacturers have these risks under control. Automation is a dynamic process by definition, whereby the software in the car is adapted during use. This can have an impact on the vehicle's driving behaviour and thus on road safety. There are risks associated with both the implementation of updates and the failure to implement important security updates.

This study has revealed that the risks associated with automation in road traffic are not adequately controlled. This raises the question of the extent to which bottlenecks occur at the system level in the introduction and deployment of ADAS (Chapter 4), in the monitoring of ADAS, and in adjustments to control the use of ADAS (Chapter 5).

Content
Considerations
Summary
Recommendations
Abbreviations
1 Introduction
2 Reference framework
3 Managing safety risks
4 Bottlenecks in the safe introduction and deployment of ADAS
5 Bottlenecks in monitoring and adjustment
6 Conclusions
7 Recommendations
References
Appendices

# 4 BOTTLENECKS IN THE SAFE INTRODUCTION AND DEPLOYMENT OF ADAS

The introduction of new ADAS involves the design of the systems themselves and subsequently permission for use on the public roads. In both phases, a key question arises: what is the role of safety? This question is above all relevant because ADAS are deployed to reduce the number of road traffic victims; with that in mind, ADAS should certainly not be deployed if they negatively influence road safety. Precisely from this (policy) perspective, it is essential that road safety be a guiding principle in both design and type approval. This means that new risks must be identified and recognized and managed as far as possible. New risks may not be accepted in advance. Chapter 3 reveals how various types of new risks do arise, that are not managed. Moreover, as yet we do not know whether various ADAS on balance have a positive effect on road safety. In this chapter, we identify key bottlenecks in producing a safe design (section 4.1) and in supervision in the form of type approval (section 4.2). The principles for the safe introduction of new technology (reference framework, section 2.1) and the cybersecurity principles (section 2.2) are used for this purpose.

## 4.1 Design

### 4.1.1 Innovation not driven by safety

Many ADAS have been designed quite simply because the (technological) developments became available. Above all as a result of new technology becoming cheaper, more powerful and more compact, opportunities have arisen for developing functions that until recently were not possible. Car manufacturers and suppliers see these opportunities and the main aim of their response is to create market value. Improving safety is not always a central point of focus in developing a variety of systems such as LKA and ACC or combinations of these technologies such as Autopilot and ProPilot. Instead, these systems contribute to driver comfort and their development is technology driven. For that reason, the safety principle of *safety by design* has not been taken into account right from the start. It must be said, however, that there are differences between car manufacturers

### 4.1.2 Insufficient knowledge exchange in the supply chain

A limited number of car manufacturers develop these systems entirely in-house. As a result they are not dependent on external parties, and knowledge of ADAS is guaranteed within the organization. However, the vast majority of car manufacturers leave the development of systems like these to specialist parties, the so-called Tier-1 suppliers.

In many cases, in practice, car manufacturers who purchase sensors, system components and software from suppliers, do have sufficient knowledge of the functioning of these ADAS for integration in their vehicles. Nonetheless, they have less detailed knowledge of the functioning and limitations of the sensor hardware or the software version in the hardware. In many cases, these tasks are outsourced to the supplier, a fact that may have unforeseen consequences when it comes to integration in their vehicle (safety principle: transparency).

### 4.1.3 User not the central focus of design

Manufacturers view *failsafe* and *foolproof* design as being important and apply these principles in their design process. They recognize the importance of intuitive systems, and ensuring that after just a short period, users know how and under what circumstances the systems function. There is also attention for bringing the vehicle safely to a standstill when the user no longer delivers any input.[128] Accident investigations by the Dutch Safety Board (section 3.2 and 3.3) illustrate that attention for the combination of technology and user remains a bottleneck. This bottleneck is indeed also known to the car manufacturers. Chapter 3 demonstrates that the designs are not always *foolproof*. This does not necessarily mean that the general assumption is that the driver must be a 'fool', however in many cases drivers are untrained and inexpert with regard to ADAS. There are designs that can lead to unsafe situations, for example because the systems suddenly switch off or no longer function, as a result of which the driver no longer receives the support on which he otherwise relies. Examples of possible unsafe situations are sharp bends or approaching a roundabout with no vehicles in front. The ADAS alliance argues that the driver shares control over the vehicle with the vehicle, while at the same time adopting the position that the driver is in fact responsible.[129] For drivers, this is a difficult situation, because it is unclear to them who is actually in control (safety principle: autonomy).

**Design principles**

Failsafe is a design principle according to which a system must be designed in such a way that in the event of a technology failure, it is possible to fall back on the human driver, whereby the functioning of the vehicle is not less safe as a consequence.

Foolproof design means that systems are designed in such a way that things do not go wrong even if used incorrectly or inexpertly, for example by correcting an incorrect operation.

Clarity about control means that it must be clear to the driver under which circumstances and according to which conditions a system is in control and under which circumstances and in which conditions the driver is in control.

[128] There are differences between car manufacturers as to how bringing the vehicle to a safe standstill is achieved: in the vehicle's own lane, in the right-hand lane, on the hard shoulder, at the nearest carpark. Opinions on these issues also differ between government organizations. Within the UNECE, these subjects are under discussion, with the eventual aim of introducing regulations, in the long term.

[129] ADAS Alliance, *ADAS Covenant*, 2019.

Content
Considerations
Summary
Recommendations
Abbreviations
1 Introduction
2 Reference framework
3 Managing safety risks
4 Bottlenecks in the safe introduction and deployment of ADAS
5 Bottlenecks in monitoring and adjustment
6 Conclusions
7 Recommendations
References
Appendices

Because designs are not *foolproof*, information must be provided about their functioning. In practice, manuals are barely read, if at all. In addition, manuals offer insufficient clarity and dealers and importers currently have no role to play in terms of consumer information (see section 3.2). As a result, instructions on the correct and safe use of an ADAS do not reach the user (safety principle: transparency).

### 4.1.4 Uncertainty about whether a design is secure

Older car models sometimes demonstrate security-by-obscurity. The idea behind this principle is that a computer-controlled system is safe (secure) if the specific functioning of that system remains secret. It is uncertain whether this principle arose as a result of a deliberate choice or whether it is the consequence of lack of disclosure about specifications in a competitive market. On the other hand, building on existing (outdated) architecture does influence the continued existence of this security-by-obscurity situation, rather than ensuring a defence-in-depth approach. Although this situation does make it more difficult to hack cars, if the hacker is sufficiently motivated, at the end of the day, it does not prevent the risk of hacking. It is not possible to see from the outside whether the security of a car still relies on lack of knowledge by a potential attacker of the electronics used (security-by-obscurity) or whether it is the consequence of sound protective measures in the form of defence-in-depth. (Cybersecurity principles: design)

The systems that can influence the cybersecurity of a car go beyond the physical boundaries of the car itself. Take for example digital maps with up-to-date route information, communication between vehicles, communication with car manufacturers for updates and information collection, aftermarket telemetry devices, mobile telephones that can be linked to the entertainment system of the car and the apps according to which the owner can access data about his own vehicle, and which can be operated via his mobile telephone. These are all examples of systems outside the car, that can have a direct influence on the cybersecurity of the car as a whole. Because these systems are used by many vehicles, the impact in the event of misuse of these systems can be very considerable. It is not always known whether the design of these systems is in fact secure. At present there are no type approval requirements or permanent requirements for these auxiliary systems.

### 4.1.5 Maintenance during the lifecycle

For the maintenance of computer systems such as those employed in modern cars, software is updated during use. The aim of these updates is to solve bugs and vulnerabilities, so that the safety of the vehicle is not reduced during its lifecycle. However, it is often the case that updates are no longer released after a certain time. At certain manufacturers, no updates whatsoever are released for existing vehicles as long as no complaints arise. If problems do emerge with systems, at certain manufacturers, only those specific vehicles are provided with an update, while the same problem in fact still affects similar systems throughout the vehicle fleet. Manufacturers (and otherwise supervisors) only take action when necessary in order to satisfy their duty of care, for example with a recall programme for specific models. Clear regulations are currently being developed (see section 4.2.2). In addition, there is a whole range of practical problems when it comes to carrying out updates, because in the past, during the design phase, little account was taken of these options. (Cybersecurity principles: lifecycle)

Content
Considerations
Summary
Recommendations
Abbreviations
1 Introduction
2 Reference framework
3 Managing safety risks
4 Bottlenecks in the safe introduction and deployment of ADAS
5 Bottlenecks in monitoring and adjustment
6 Conclusions
7 Recommendations
References
Appendices

Almost all of the latest cars equipped with ADAS do have the option of wireless communication (OTA), for example with the car manufacturer, so system updates have become more simple. As a result, cybersecurity threats can be better managed. In older cars that are not yet equipped with OTA, software updates will have to be carried out by the dealer or garage. Various car suppliers are reticent in updating software to the latest version. In comparison with the IT sector, it requires greater efforts on the part of the car industry to correct vulnerabilities. This is because stricter demands are placed on functional safety[130] of the systems during development, production and maintenance. As a result, certification and validation must first take place before an update is actually rolled out. This in turn requires a complex process of registration, testing and management of all possible hardware and software combinations, to prevent new problems being introduced with an update. Moreover, over the course of years, different types of ECUs are often employed in the same model of car, as a result of which software maintenance becomes even more complex.

By allowing these vulnerabilities to exist, defence-in-depth is negatively influenced, and as a consequence newly discovered vulnerabilities can have even greater consequences. It is possible in practical terms that not all vulnerabilities can be rectified as a result of the costs and technical limitations. The problem is that it is unclear how manufacturers make their choices with regard to these issues and on the basis of which considerations. It is therefore also unclear whether there are vulnerabilities known to the manufacturer in specific earlier produced models or types of cars. As yet, there are no specific guidelines from government on these questions.

**Partial conclusions**

The design of ADAS is primarily driven by technical possibilities. As a consequence, in certain respects, the design of different ADAS is unsafe, and is not able in all cases to provide users with clarity on what the system can do and what it does, the role of the driver, and why. For drivers, in practice, it is also not always clear who is in fact in control. Manufacturers fail to ensure that it is sufficiently clear to drivers how ADAS work. Drivers are not always sufficiently at the focal point when it comes to designing ADAS.

In many cases, it is unclear whether the software in a certain earlier produced model or type of car is up-to-date, or contains vulnerabilities known to the manufacturer.

Cybersecurity during the entire lifecycle of the car is insufficiently guaranteed, and is dependent on the good intentions and professionalism of the manufacturer.

[130] ISO, *ISO 26262-6:2018 Road Vehicles - Functional Safety - Part 6: Product Development at the Software Level*, 2018.

## 4.2 Type approval and policy

In the vision of the Dutch government and the European Commission, ADAS should make an important contribution to reducing the number of road traffic accident victims, see section 1.1. With that in mind, safety should be a guiding principle in design and approval. This section describes the extent to which existing regulations for type approval and the underlying policy of the Netherlands and the European Commission with regard to ADAS tie in with the ambition of improving road safety.

We show that the existing regulations for type approval do not tie in with the vision that ADAS must make an important contribution to reducing the number of victims of road traffic accidents, because increasing safety is not a guiding principle in type approval (section 4.2.1) and because legislation is not suitable for cars as driving computers (section 4.2.2), because legislation was developed for 'mechanical' cars. Moreover, Dutch (section 4.2.3) and European policy (section 4.2.4) are aimed at encouraging ADAS, but barely if at all focus on mitigating the risks and adjusting the legislative framework.

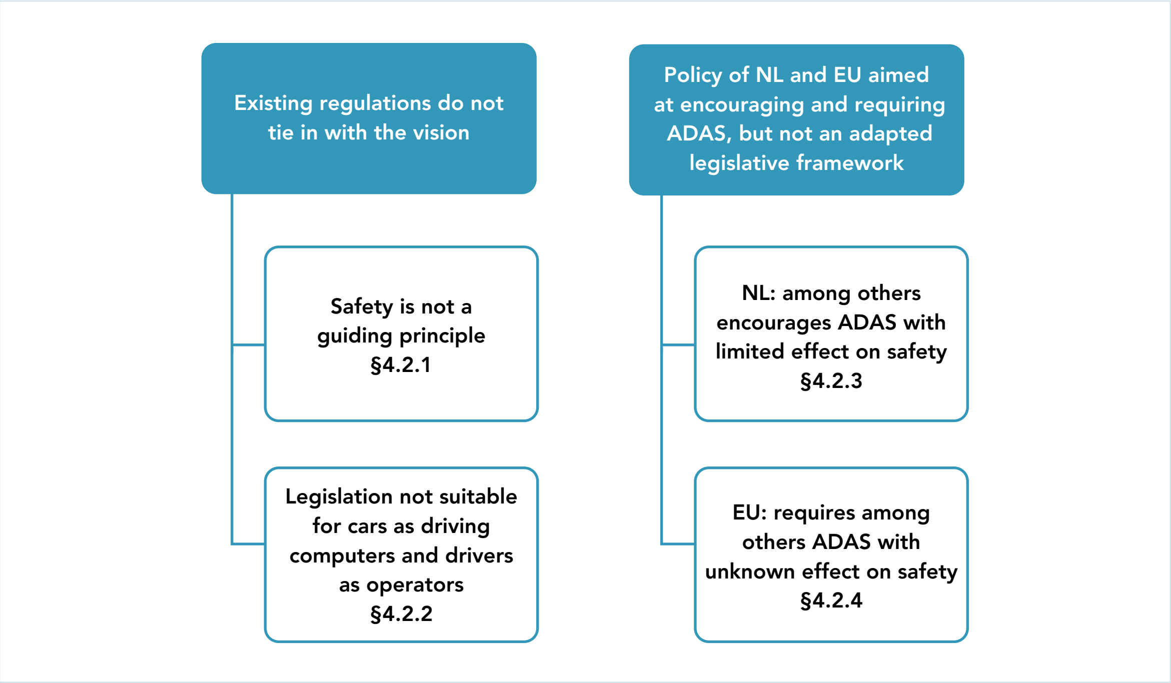

Existing regulations do not tie in with the vision
Safety is not a guiding principle §4.2.1
Legislation not suitable for cars as driving computers and drivers as operators §4.2.2
Policy of NL and EU aimed at encouraging and requiring ADAS, but not an adapted legislative framework
NL: among others encourages ADAS with limited effect on safety §4.2.3
EU: requires among others ADAS with unknown effect on safety §4.2.4

*Figure 15: Chapter breakdown.*

### 4.2.1 Safety is not a guiding principle

In order to ensure that ADAS make an important contribution to reducing the number of road traffic accident victims, improving safety should be a guiding principle in design and type approval. In current vehicle regulation, however, this operating principle is not consistently reflected.

In the type approval of new ADAS on the basis of Article 20 of Directive 2007/46/EC, the condition for granting exemption is that vehicles equipped with these systems must at least achieve an equivalent level of safety. This is less ambitious than increasing the level of road safety.

Content
Considerations
Summary
Recommendations
Abbreviations
1 Introduction
2 Reference framework
3 Managing safety risks
4 Bottlenecks in the safe introduction and deployment of ADAS
5 Bottlenecks in monitoring and adjustment
6 Conclusions
7 Recommendations
References
Appendices

Moreover, nowhere do vehicle regulations specify how the level of safety of an ADAS can be assessed. This lack of clarity in assessing the level of safety means that manufacturers are not required to provide any risk assessment or scenarios (safety principle 4). There are also often no scientifically supported statements on the safety of particular systems, because that would require better road traffic accident investigations, and greater understanding of the interaction between ADAS and drivers in practice, for example on the basis of naturalistic driving studies (see section 5.2.2.). At present, when assessing new ADAS, it is often stated that the effect on road safety cannot be demonstrated. It is then stated that it is not possible to say that the new ADAS negatively influences road safety. In this way, this ADAS meets the requirement of an at least equivalent level of safety. For ACC systems, for example, no type approval requirements have been set, a fact that merely implies (see Figure 38 in Appendix E) that at the time of introduction, there were no explicit indications that the system has a negative effect on road safety.

Specific requirements are either absent or not sufficiently tight. Manufacturers are not required to make their own risk assessments, despite the fact that such assessments are compulsory for experiments with automated and connected driving[131]. As a consequence, there is no guarantee that new ADAS are sufficiently tested for their risks and their contribution to improving road safety and the risk is clearly present that ambitious policy objectives will not go beyond the stage of well-intentioned plans.

### 4.2.2 Legislation not suitable for cars as travelling computers

Current vehicle regulations consist of a legislative framework and extensive technical requirements, see appendix E. The legislative framework regulates the extensive one-off testing (type approval) and the more broad-based MoT (Periodic Vehicle Inspection). This legislation is geared to the 'mechanical' car, but is less suitable for the recent development of a car as a 'computer on wheels', and the related development of the driver as an operator, because:

1. technological changes in the field of ICT are taking place faster than ever and, as a consequence, the legislative process is falling ever further behind than in the past;
2. legislation and regulations have until now been drawn up and applied by people with a background in automotive engineering;
3. the computer on wheels undergoes changes during its lifecycle as a result of updates;
4. wear to computer parts is not a gradual process.

*Fast-paced changes*

Internationally harmonized technical regulations are established on the basis of detailed international consultation between governments, car manufacturers and other stakeholders in the UNECE. The automotive industry plays a major role in this process, as they take part in many informal working groups. Technological changes in the field of ICT take place so rapidly that the system based on reaching agreement on technical

[131] In the CAD document (connected and automated driving, previously CAV), the Netherlands Vehicle Authority (RDW) elaborated the process for manufacturers/research institutes that apply for an exemption for an experiment. The assessment of the risk evaluation (for example an FMEA in accordance with the ISO 26262 standard) drawn up by the applicant is a key element of the procedure. The risk assessment deals with risks relating to vehicle, road and behavioural aspects, and mitigating measures. The mitigating measures then become part of the exemption.

requirements that until recently functioned well is no longer fast enough. As a result, uncertainties can arise as to which type approval requirements apply for a new ADAS. This turned out to be the case several years ago, when type approval bodies in different countries issued differing assessments in respect of similar new ADAS, namely a combined system of ACC and LKA. In the Netherlands, the system was approved within the existing type approval requirements, while in Germany, an Article 20 procedure was initiated because the type approval body in question suggested that the new system did not fit into the existing regulations. In respect of LKA, type approval requirements were only introduced in October 2018 in UN R.79 (see Appendix E). This was several years after the first LKA systems were placed on the market in 2014 and, in the absence of specific regulations, were approved without assessment. In 2018, the EU decided that new ADAS for which there were not yet any elaborated requirements had to be assessed via an Article 20 procedure.

**Article 20 procedure**

In an Article 20 procedure, a new technology can be approved via an exemption, if inconsistent with existing regulations. The precondition is that the manufacturer demonstrates that the new technology guarantees an equivalent level of safety. An Article 20 procedure is the lead-up to regulations (via Article 21). See appendix E for a more detailed explanation.

*Focus primarily on automotive engineering*

Until now, regulations have above all been made and applied by people with a background in automotive engineering, mechanical cars. As a result there has been less focus on new types of risks, and to date almost no requirements have been developed in the field of human machine interaction (section 3.3), software (section 3.4) and cybersecurity (section 3.5).

On the other hand, there are detailed and specific requirements for the mechanical components of the car. No such requirements exist for software because for the regulator it is impossible to check the huge number of lines of (ever changing) computer code. Moreover, with a fixed test programme, manufacturers can adapt to the type approval test (as was the case with the emissions scandal, see section 3.4). It is possible to evaluate software systems by validating the behaviour of the software (for example by means of computer simulations and test runs) and in that way to assess at process level whether the development of the software was carried out correctly.[132] The RDW argues that this is not necessary for the current generation of ADAS (up to and including SAE level 2), because these systems assist or support the driver, while it is formally up to the human to carry out the task of driving. At the same time, this is not the way in which the users perceive and use the systems and is not in line with how those systems are positioned in the real world, among others by the car manufacturers and the media. Here, in fact, the picture is created that cars with the current generation of ADAS are partially already autonomous vehicles. For the same reasons, there are no requirements for human machine interaction. And there is insufficient knowledge in this field (see section 5.3.2).

[132] For systems in which the car takes over control from people, legislation is currently being developed.

Because there are no specific requirements with regard to software and human machine interaction, and because manufacturers are not called upon to carry out a risk assessment (see section 4.2.1), new risks are not sufficiently taken into account in deciding whether to approve a particular vehicle or specific ADAS.

*Changes during the lifecycle*
Automation systems can also be regularly updated during the lifecycle of the car, resulting (partially) in potential changes to the function, see section 3.4. New functions can also be added to existing systems. These updates are not subjected to standard assessment and evaluation by the regulator, because the type approval is a one-time process. There is no such thing as 'continuous' or phased type approval. Such a process is currently being developed within the UNECE for future cars which will (partially) take over control from the driver (SAE level 3 and higher). Legislation is also being developed in the field of software updates (see further below).

*Abrupt loss of performance*
Digital components and systems do not suffer gradual loss of performance as a result of (mechanical) wear, but as a rule fail abruptly, without prior warning. As a result, problems with digital components are often not uncovered during a periodic inspection (MoT) and for that reason periodic inspection is not suitable for digital components. Some form of continuous monitoring would be more suitable for a computer on wheels, than an MoT. In its Annual Report[133], the RDW has talked in this framework about converting the MoT to a General Permanent Inspection as opposed to a General Periodic Inspection.

*Developments in legislation*
The field of tension between existing regulations developed for mechanical cars and the new questions and risks that emerge from the development of the car as a computer on wheels is recognized by the RDW and the UNECE.

The RDW is working to develop the VSSF (Vehicle Safety & Security Framework) and the VDLF (Vehicle Drivers' License Framework). Within the UNECE, work is also underway both on regulations for cars that are capable of (temporarily) taking over control from the driver, and regulations relating to software updates and cybersecurity for all new cars.

Within the Informal Working Group on Functional Requirements for Automated and Autonomous Vehicles (FRAV), a roadmap[134] has been drawn up that contains a vision on safety: automated or autonomous vehicle systems must not be permitted in automated mode to cause road traffic accidents that result in injury or death, that could reasonably be predicted or prevented. Based on this vision, a number of subjects have been identified in respect of which regulations need to be developed. These include functional requirements (such as those that exist for other automotive components), validation (new test methods, such as those also being developed within the VDLF) and quality assurance (including cybersecurity) as standard within the ICT domain, and which are aimed at the process of design, production, testing, monitoring and updating (as in the VSFF).

[133] RDW, *Jaarverslag 2018*, 2019.
[134] UNECE, *ECE/TRANS/WP.29/2019/34, Framework Document on Automated/Autonomous Vehicles*, 2019.

The roadmap describes a number of subjects which could form the foundation for future legislation. A large number of those subjects are however not only relevant for future systems but also for existing systems, for example the human machine interface (HMI), validation of system safety (including a risk analysis and risk assessment), data storage (EDR and DSSAD). Informal working groups have already been established for validation methods and for data storage, but not yet for HMI. With regard to the subject information provision and training for users, it has even been decided that this is not a priority within WP.29. Although the legislation is no longer appropriate, for the current generation of ADAS (as yet) no new legislation is being developed at UNECE level for either HMI or for validation (a series of tests carried out by the manufacturer in simulators, on test tracks and by specialist field test drivers).

The informal working group CS/OTA has issued a proposal for a regulation on cybersecurity, which is to be discussed in WP.29 in November 2019. The RDW is a leading player in this working group. The development of the VSSF has made a valuable contribution. The proposal calls upon manufacturers to have a compulsory certified cybersecurity management system (CSMS) at the moment of type approval. The CSMS must take account of the entire lifecycle of the vehicle. In addition, manufacturers must be able to demonstrate that they have evaluated the cybersecurity risks of the model in question, and have taken sufficient mitigating measures. The proposal does not specify precisely how this should be done, but refers to current standards because it is a constantly changing process. The informal working group CS/OTA has also issued a proposal for a regulation on software updates, that is also due to be discussed in WP.29 in November 2019. This proposal includes that software versions must be identifiable, and that changes to software via updates must be logged in a certified Software Update Management System.

At EU level, there are no current developments aimed at adjusting the legislation framework, despite the fact that it no longer matches the current generation of cars with ADAS. Elsewhere at EU level there are developments in respect of cybersecurity legislation, which could affect the automotive industry in the future. For example, there is a Network and Information Systems Directive (NIS; Directive (EU) 2016/1148) that imposes requirements on cloud service providers, and the successor to the Cyber Security Act (Regulation (EU) 2019/881) which describes the cybersecurity certification framework for ICT products, services and processes.

### 4.2.3 Dutch policy

*Encouraging ADAS*
There is much attention within Dutch policy for autonomous vehicles. The (distant) future picture of cars that drive fully automatically everywhere or only at specific locations (SAE levels 4 and 5; see Appendix D.4) is perceived by the Ministry of Infrastructure and Water Management (IenW) as very attractive, given the numerous potential advantages in respect of road safety, environment (emissions) and traffic flows. This was also the reason for launching a steering committee on Autonomous Cars in 2014. Economic advantages also played a role. The attention of that steering group is heavily future oriented. Within this steering group itself there is little attention for ADAS; the focus instead is on fully automatic driving or automatic driving subject to specific conditions.

One of the measures from the Road Safety Action Plan[135] published in 2018 is aimed at encouraging the safe use of ADAS, subject to specific conditions, see section 1.1. Since that time, a small group of staff at IenW has been working on the development of ADAS, under the auspices of the ADAS Covenant, that was signed in June 2019.[136] It is agreed within the ADAS Covenant that ADAS will be encouraged that have a positive effect on one or more of the policy priorities road safety, environment or traffic flow, while at the same time having no negative effect on road safety. The Covenant was signed by members of the so-called ADAS Alliance, which is made up of 42 parties, that have each drawn up their own ADAS implementation plan.

One key spearhead of the ADAS Covenant is raising awareness of ADAS and thereby tackling the lack of knowledge among drivers. The aim will be to inform both drivers and people employed in the automotive industry. Within that framework, together with BOVAG/RAI (sector organizations for garages and car importers), IenW will be informing car sellers and IenW, ANWB (Dutch car owners club), the RAI Association, the Province of Noord-Holland and the CBR (Driver's licence issuing authority) have created the website slimonderweg.nl ("smart on the road") to inform drivers. These measures are entirely non-binding and in no way guarantee that the lack of knowledge among all users will be rectified.

On behalf of IenW, the SWOV Institute for Road Safety Research has mapped out the safety effects of ADAS on the basis of various foreign studies, whereby a number of assumptions have been made because sufficient research was not available in all cases.[137] This literature study has revealed that three out of the fourteen investigated systems have a major positive effect on road safety. These are the combination of FCW and AEB, ISA that intervenes whenever the applicable maximum speed is exceeded, and an alcohol lock (Table 3). Of the systems investigated by the Dutch Safety Board, LKA and Autopilot, the effects on safety are unknown, and different studies into ACC have delivered contradictory results. The parties in the ADAS Covenant will be promoting those systems that have been identified by the SWOV as eligible for promotion, given the current state of technology. IenW will be investigating the possibilities for providing financial support for these ADAS. The systems in question mainly issue warnings or intervene in critical situations. LKA, Autopilot and ACC are not (currently) recommended by the SWOV. For certain systems, such as FCW, major discrepancies in effectiveness were identified between different models and makes of car. This may relate to the immaturity of the systems themselves, or the human machine interaction.

*Insight into the risks*
The work of the steering committee on autonomous cars, experiments with connected and automated driving (for example platooning experiments in which passenger cars or trucks travel 'in convoy') and the contacts with the RDW have given the Ministry of Infrastructure and Water Management an insight into the risks relating to current and

[135] Ministry of Infrastructure and Water Management, *Landelijk actieplan verkeersveiligheid 2019-2021: Veilig van deur tot deur*, The Hague, 2018.
[136] ADAS Alliance, *ADAS Covenant*, 2019.
[137] SWOV, Veiligheidseffecten van rijtaakondersteunende systemen; Bijlage bij het convenant van de ADAS Alliantie, 2019.

future ADAS. In the Letter to Parliament on Smart Mobility[138] various types of risks are identified. However, no risk analyses were carried out for existing ADAS and no future scenarios were drawn up, while risk analyses are being carried out with regard to automated and connected driving (see section 4.2.1). The risks engendered by existing ADAS are monitored to a limited extent (see section 5.3.2). What is more, the Ministry of Infrastructure and Water Management has not elaborated how the risks could be mitigated, or what is needed to arrive at mitigating measures. The Ministry of Infrastructure and Water Management assumes that the risks will themselves automatically decrease as technological developments advance, see box below. In addition, people at the Ministry have assumed that as the requirements for existing ADAS become stricter, many of these risks will be managed.

**From the Strategic Plan for Road Safety**
'Not only vehicles are changing but also the approach to traffic management. The growth in connectivity makes it possible to guide road users in their mobility behaviour in ever smarter ways. The developments in automation and connectivity also mean that growing volumes of data about infrastructure and vehicles are becoming available. On that basis, governments can better plan their road safety policy. Automation also offers new opportunities for (digital forms of) enforcement. Innovations offer new possibilities but also raise new questions about road safety policy. Because the developments are taking place so rapidly, constant adaptation is needed. That in turn requires a vision from government about the degree of innovation and how to tackle new developments.'

The government has sketched out a picture of very rapid, autonomous, technological developments. At the same time, the Strategic Plan for Road Safety underlines the importance of intervention whenever the development of risks deviates from the desired path. However, that means that a vision must be developed with regard to the desired level of safety in relation to the desired degree and direction of innovation, and that systematic risk analyses be undertaken, and that the influence of ADAS on road safety be monitored. Despite this, none of these conditions has yet been met.

### 4.2.4 EU policy

The new General Safety Regulation was adopted by the European Parliament in April 2019, and comes into effect in 2022. This GSR is aimed at contributing to reducing the number of traffic deaths ('Vision Zero') and introduces a compulsory requirement for additional systems for various types of motor vehicles. For passenger vehicles these include ISA (Intelligent Speed Assistant), AEBS (Advanced Emergency Braking System), pedestrian and bicycle detection (emergency braking system), a warning system for drivers who are at risk of falling asleep or who become distracted, reverse (driving) warning systems involving cameras or sensors, EDR (Event Data Recorder; a sort of 'black box' for motor vehicles) and LKA (Lane Keeping Assist), see Table 3. The specific details of the requirements on these systems must still be determined within the UNECE.

[138] Minister of Infrastructure and Water Management, *Letter to Parliament 205325 Smart Mobility Dutch Reality*, 2018.

In reaching agreement on the GSR, the EC has expressed real confidence in technical measures as remedies for tackling unsafe situations in road traffic.[139] This confidence is based on the reasoning that 90% of road traffic accident victims are due to human error, and that this percentage will fall if machines start to replace people. In this reasoning, however, the fact that human errors can also be made in designing and programming new technologies (immature systems) and the fact that humans are also responsible for preventing accidents, are ignored. In addition, in many cases, the driver continues to act as a safety barrier, even if the driver him or herself does not realize this fact (see chapter 3).

There are notable differences between the systems which the Dutch government wishes to encourage (ADAS Covenant) and the systems that will be introduced as compulsory according to the GSR.

- The ADAS Covenant currently only promotes ADAS that according to the SWOV have a positive effect on road safety, whereas the GSR has proposed the compulsory introduction of a number of ADAS, the effect of which on road safety is unknown, according to the SWOV.
- The ADAS Covenant promotes all three ISA variants (systems that advise on speed, that warn on speed violations and that limit speed) but expects the greatest positive effect on road safety from the variant that intervenes to a greater or lesser extent, while the GSR has made the informing variant of the ISA compulsory. According to the SWOV, this particular variant only has a minimal effect on road safety.
- The GSR makes systems that warn of fatigue and attention loss compulsory, as well as advanced systems for distraction warning. The ADAS Covenant considers the time not yet ripe for these systems, because their effect on road safety (according to the SWOV) is as yet unknown. The GSR deliberately opts to introduce mitigating measures to manage the risk of behaviour adaptation, thereby stacking system on top of system, which results in greater complexity, a situation that is clearly at odds with safety.
- The GSR promotes pedestrian and bicycle detection, while the ADAS Covenant does not consider the time ripe for these systems because their effect on road safety (according to the SWOV) is not yet known. It is remarkable that the recognition of bicycles and pedestrians by AEBS has been included in the new GSR partly as a result of Dutch efforts. Initial tests, however reveal that in many cases the system does not function well.[140, 141]

[139] European Commission, *Press release Road Safety: Commission Welcomes Agreement on New EU Rules to Help Save Lives*, https://europa.eu/rapid/press-release_IP-19-1793_en.htm, accessed August 23, 2019.
[140] Charlebois, Meloche, and Burns, *Detection of Cyclists and Pedestrians Around Heavy Commercial Vehicles*, in 26th International Technical Conference and Exhibition on the Enhanced Safety of Vehicles (ESV) Eindhoven, 2019.
[141] AAA, *Automatic Emergency Braking with Pedestrian Detection*, 2019.

| System | Informing/Warning/Taking over/Intervening | Accuracy | Behaviour change | Pre-conditions | Effect on traffic safety[142] | Timing of promotion[143] | GSR |
|---|---|---|---|---|---|---|---|
| **Longitudinal control (speed)** | | | | | | | |
| **Forward Collision Warning** | Warning | Fair | Minimal | | +/- | Now | |
| **Autonomous Emergency Braking** | Intervening | Fair | Minimal | | + | Now | Yes |
| **Combination of FCW and AEB** | Warning/Intervening | Fair | Minimal | | ++ | Now | |
| **Pedestrian and Bicycle detection** | Warning | Suspected still insufficient | Unknow | | Unknown | Potential | Yes |
| **Adaptive Cruise Control** | Taking over | Fair | Contradictory results | | Contradictory results | None | |
| **Intelligent Speed Adaptation** | Informing/Warning/Taking over | Good | Minimal | Navigation systems with speed limits; Accurate location determination | +/-<br>+<br>++[144] | Now | Yes Only Informing |
| **Emergency stop signal** | Warning[145] | | | | | | Yes |
| **Lateral control (steering and intended course change)** | | | | | | | |
| **Lane Departure Warning** | Warning | Fair | Minimal | Good road markings | +/- | Now | |
| **Lane Keeping System** | Taking over | Fair | Unknown | Good road markings | Unknown | Potential | Yes |
| **Blind spot warning** | Warning | Fair | Minimal | | +/- | Now | |

[142] minimal +/-, fair +, considerable ++

[143] Now = can already be promoted given current status of technology; Potential = effect on road safety in practice unknown but if demonstrated to be effective can make a major contribution to road safety and can then also be promoted; None = promotion has no priority because the safety effect (as yet unknown in practice) is estimated as relatively low.

[144] Depending on whether the ISA is informative, warning or intervenes to a greater or lesser extent

[145] Is somewhat beyond the definition of ADAS because it does not support the driver but informs his environment. Included because the GSR has made the emergency stop signal compulsory.

Content
Considerations
Summary
Recommendations
Abbreviations
1 Introduction
2 Reference framework
3 Managing safety risks
4 Bottlenecks in the safe introduction and deployment of ADAS
5 Bottlenecks in monitoring and adjustment
6 Conclusions
7 Recommendations
References
Appendices

| System | Informing/ Warning/ Taking over/ Intervening | Accuracy | Behaviour change | Pre-conditions | Effect on traffic safety[142] | Timing of promotion[143] | GSR |
|---|---|---|---|---|---|---|---|
| **Combined longitudinal and lateral control** | | | | | | | |
| **Autopilot** | Taking over | Fair | Considerable | | Unknown | Potential | |
| **Monitoring status of driver** | | | | | | | |
| **Fatigue detector** | Warning | Suspected still insufficient | Unknown | | Unknown | Potential | Yes |
| **Distraction detector** | Warning | Insufficient | Unknown | | Unknown | Potential | Yes |
| **Alcohol lock** | Intervening | Good | None | | ++ | Now | Yes[146] |
| **Support for special manoeuvres** | | | | | | | |
| **Rear-view camera** | Warning | Fair | Minimal | | +/- | Now | |
| **Accident data** | | | | | | | |
| **Data recorder for accidents**[147] | Informing | | | | | | Yes |

*Table 3: Overview of ADAS and global indication of the effect on road safety according to SWOV. An indication is also given of which ADAS are promoted according to the ADAS Covenant. The final column lists the measures from the GSR.*

[146] The GSR has only made support of the installation of an alcohol lock compulsory, not the alcohol lock itself. This equates to the installation of a standardized interface that facilitates the aftermarket fitting of an alcohol lock in a vehicle.

[147] This data recorder (EDR) is not ADAS but is made compulsory in the GSR.

Content
Considerations
Summary
Recommendations
Abbreviations
1 Introduction
2 Reference framework
3 Managing safety risks
4 Bottlenecks in the safe introduction and deployment of ADAS
5 Bottlenecks in monitoring and adjustment
6 Conclusions
7 Recommendations
References
Appendices

**Partial conclusions**
The policy ambition of only approving ADAS that improve road safety as demonstrated by scientific research is not reflected in vehicle regulations, which assume at least an equally high level of safety. There is a lack of clarity in assessing the level of safety and, as a consequence, manufacturers are not required to provide any risk assessment or scenarios, thereby not guaranteeing that no systems will be approved that have a negative effect on road safety.

The field of tension between existing regulations tailored to the mechanical car and new risks that emerge from the development of the car as a computer on wheels, as a result of which the role of the driver is increasingly shifting to that of operator, and in which the human machine interaction is becoming increasingly important, is recognized by the Dutch government, but has not yet led to any changes to vehicle regulations. Developments in the field of legislation are related mainly to vehicles that (temporarily) take over control from the driver, while legislation is in fact also no longer suitable for systems that assist or support the driver.

With regard to automation in road traffic, the Ministry of Infrastructure and Water Management is more interested in the long-term future than the present and the near future. Within Infrastructure and Water Management, there is a clear assumption that the large scale deployment of ADAS will in the long term, and on balance, result in fewer road traffic accident victims. This assumption is barely supported, if at all, by the lack of a vision on the desired level of safety, and the absence of systematic risk analyses.

In the ADAS Covenant that was signed in June 2019, it was agreed that ADAS would be encouraged that have no negative effect on road safety and that do have a positive effect on road safety, the environment and traffic flows. Non-binding information to drivers is an essential element of the implementation plans that are dealt with by the Covenant. The new General Safety Regulation has made a number of ADAS compulsory, by 2022, for which there is not yet any scientific supporting argument with regard to their effect on road safety.

## 4.3 Conclusions

It is inherent in any innovation that systems will be placed on the market that are not yet fully developed. Particularly in the case of information-based systems, what is needed to fully mature those systems can only be revealed in practice. This means that ADAS will undergo further development, once on the public roads. This reality is not ideal from a safety perspective. At the same time, innovation may improve safety if safety improvement is a requirement in the development of new systems. It is therefore essential to innovate in a responsible way. To this end, a number of safety principles should be respected in terms of design, type approval and policy (see the reference framework in Chapter 2).The Dutch Safety Board has concluded that there is room for improvement here.

Content
Considerations
Summary
Recommendations
Abbreviations
1 Introduction
2 Reference framework
3 Managing safety risks
4 Bottlenecks in the safe introduction and deployment of ADAS
5 Bottlenecks in monitoring and adjustment
6 Conclusions
7 Recommendations
References
Appendices

*Design*
In their design process, manufacturers are focused more on the technical functionality than on increasing road safety. As a result, the safety principles safety by design, foolproof design, secure design and clarity on who has control are not respected. In addition, cybersecurity is not sufficiently guaranteed throughout the entire lifecycle and there is a lack of transparency within the supply chain and to consumers.

*Type approval*
Existing regulations for type approval match poorly with the principle that innovation must improve safety, and the Dutch and European policy ambition that ADAS should make an important contribution to reducing the number of road traffic accident victims. The reasons for this are that safety is not a guiding principle in type approval and that existing legislation is not suitable for cars as computers on wheels, in which the driver is an operator, and that human machine interaction has increased. The influence of the automotive industry on the development of legislation also plays a role in maintaining this situation.

*Policy*
Dutch and European policy are aimed at encouraging and making ADAS compulsory. This is based on the ambition of reducing the number of road traffic victims. However, there is no elaborated vision on the desired level of safety in relation to the desired degree and direction of innovation. For example, there are no systematic risk analyses and no elaboration has been made of how risks can be mitigated, or what is needed to arrive at mitigating measures. Moreover, the policy is insufficiently focused on the current generation of systems, and attention within government is focused above all on systems that could (temporarily) take over control of the car in the (distant) future. Current mitigating measures of the Ministry of Infrastructure and Water Management aimed at tackling the lack of knowledge among drivers are all non-binding. Within the UNECE, there is no specific working group for HMI-related regulations.

# 5 BOTTLENECKS IN MONITORING AND ADJUSTMENT

## 5.1 Introduction

The introduction of new technology such as ADAS is always surrounded by uncertainty. Only once the new technology is in use in practice (the living lab situation), it will be possible to determine what is still needed in order to bring that technology to full maturity. Against that background, with regard to innovative technologies, it is essential to keep an ear to the ground (monitoring) and to feed back information about the performance of that technology to manufacturers and government (feedback). As a result, on the basis of an evaluation, any necessary mitigating measures can be taken by the manufacturer or the government in the form of adjustment or prohibition (safety principles carefully controlled process and government intervention, reference framework, section 2.1). By monitoring and taking measures, the feedback loop is closed. See Figure 16.

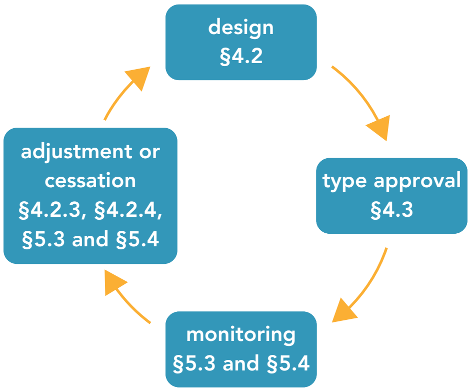


*Figure 16: Safe introduction and safe use of ADAS.*

In this chapter, we examine the bottlenecks in closing the feedback loop. These bottlenecks, in sequential order, are the lack of information for monitoring and adjustment (section 5.2), the learning capacities of parties in response to accidents and hazardous situations (section 5.3) and learning from cybersecurity incidents (section 5.4).

Content
Considerations
Summary
Recommendations
Abbreviations
1 Introduction
2 Reference framework
3 Managing safety risks
4 Bottlenecks in the safe introduction and deployment of ADAS
5 Bottlenecks in monitoring and adjustment
6 Conclusions
7 Recommendations
References
Appendices

## 5.2 Lack of information

The collection of empirical data is essential for the learning capacity of the automotive industry and government and for adjustment or intervention on the basis of monitoring.[148] Empirical data relate to insight into the number of cars with ADAS and data about accidents, hazardous situations and the prevention of hazardous situations.

### 5.2.1 No insight into the number of cars with ADAS

There are no statistics with data about the presence of the various ADAS in the Dutch vehicle fleet. The RDW does record a large volume of data in its vehicle registration systems, but that does not include the presence of ADAS. The reason for this is that it is difficult to provide a complete and clear picture of the ADAS in a vehicle within a limited number of parameters. Manufacturers, for example, offer a variety of systems that appear similar but that function and respond slightly differently, see section 3.3. It is also relevant which software version is installed. Because there are different software versions, the system variation is considerable.

The RDW is investigating the possibility of including ADAS in the vehicle registration record and accessing data about ADAS in vehicles (for example for car buyers via the website). This investigation is an initiative by the RDW itself, in response to discussions with stakeholders such as the RAI Association, BOVAG and the ANWB. Above all for the trade in second-hand cars, it is vital for buyers and sellers to know which systems are on board and to understand the specifications of those systems.

As part of the ADAS Covenant, the Ministry of IenW has started monitoring the degree of penetration by various ADAS in the Dutch vehicle fleet, and the level of knowledge and use of those systems among Dutch car drivers.

### 5.2.2 Lack of empirical data about accidents

Empirical data about accidents in which ADAS have played a role are often not available. This is firstly due to the design of ADAS and the way in which data are stored. Accident investigations and discussions with experts have revealed that the current generation of systems suffer a number of shortcomings with regard to the storage and collection of accident data:

1. Data are not always stored. Certain systems, for example, are designed in such a way that in the event of a sudden system interruption - as a result of a collision - the data for the last few seconds are not recorded. There are also cases in which no data at all are stored about the functioning of ADAS, either during driving or following accidents. It is also not always possible to ascertain whether the ADAS present in a car were actually switched on.
2. Data are stored in a proprietary format. As a result, those data cannot be read out without assistance from the manufacturer.
3. Data are stored encrypted. Here, too, the data cannot be read out without the assistance of the manufacturer.

[148] See the safety principles from the reference framework in section 2.1.

4. Data are stored distributed across various modules and it is not always clear where those data are stored. Because ADAS are purchased from suppliers, in many cases, in certain situations it is not even clear to the automotive manufacturer where what information is stored.

In addition, empirical data are not available because accidents are not registered. Generally speaking, the registration level is low (approx. 30% for accidents involving serious injuries).[149] As concerns fatal road traffic accidents, only those that have occurred on national highways have been systematically analyzed, in recent times.[150] Moreover, the presence of ADAS is not an element in accident registration because the presence of ADAS in vehicles is not registered, see section 5.2.1. In addition, there is often no investigation into whether ADAS was a factor in the accident. One reason for this is that the various parties (including the police) have no insight into the presence of ADAS in various vehicles (brands, types, software versions), see section 5.2.1. Furthermore, there is no generally prevalent awareness that ADAS may be present in all modern vehicles and as such could be a factor in an accident.

Partly with a view to facilitating accident investigations, the installation of an EDR (Event Data Recorder) will be made compulsory on all new cars, by 2022, see section 4.2.4. Precisely which data must be stored, who is authorised to read out these data and who is permitted to use these data for investigations are still subjects of debate within the UNECE and the EC.[151] The same applies to the data stored in ADAS, and which could in principle be read out.[152] Because of their limited storage capacity, EDRs are not the ideal device for storing ADAS-related or cybersecurity events. These events are generally stored on other data storage devices.

### 5.2.3 Missing empirical data about cybersecurity incidents

We cannot exclude the possibility that accidents occur due to misuse of vulnerabilities because today's cars are not equipped for digital investigation following an accident into whether the accident is potentially cybersecurity related. Data for determining whether a hack has taken place are not specifically stored, see section 3.5. As a consequence, the police and accident investigators have no possibility of recognising or excluding a cybersecurity incident, and as a result there are no further investigations.

[149] SWOV, *Ernstig verkeersgewonden 2017*, 2018.
[150] SWOV, *Dodelijke verkeersongevallen op rijkswegen in 2017*, 2019.
[151] EU-lidstaten, *Declaration of Amsterdam; Cooperation in the Field of Connected and Automated Driving*, 2016.
[152] European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee, the Committee of the Regions; On the Road to Automated Mobility: An EU Strategy for Mobility of the Future*, 2018.

Content
Considerations
Summary
Recommendations
Abbreviations
1 Introduction
2 Reference framework
3 Managing safety risks
4 Bottlenecks in the safe introduction and deployment of ADAS
5 Bottlenecks in monitoring and adjustment
6 Conclusions
7 Recommendations
References
Appendices

**Partial conclusions**
There is a lack of empirical data about accidents, hazardous situations and cybersecurity incidents involving vehicles with ADAS, despite the fact that these data are essential for the feedback loop. The absence of any registration of the presence of ADAS is a hindrance to the evaluation of ADAS.

The correct data for investigating accidents and cybersecurity incidents are not stored in the vehicle.

## 5.3 Learning from accidents and hazardous situations

### 5.3.1 Learning from (near) accidents by manufacturers

Manufacturers learn from accidents and near accidents in a number of different ways. Broadly speaking, there are five possibilities for collecting information:

1. Collecting the data generated by the computer systems in the vehicle. These data can be shared with the manufacturer via a wireless link. This not only creates the possibility of intervening - for example by issuing an update to improve the current generation of systems - but this information also offers the manufacturer an insight into further improving and designing new products more safely. Tesla applies this method to create a closed feedback loop.
2. Investigation on site by an investigation team or incident response team. This investigation could, for example, include collecting data originating from the vehicle, recording traces and replicating the system status.
3. Collecting complaints from car drivers and truck drivers.
4. Collecting sales details for spare parts such as front and rear bumpers, based on the assumption that these are often used in repairing vehicles following an accident.
5. Initiating or undertaking targeted (scientific) research, individually or in collaboration with research institutes.

There are few manufacturers that combine these five methods in arriving at the most complete possible picture of what occurred shortly before, during and following a (near) accident. Moreover, not all manufacturers offer good possibilities for receiving feedback from consumers, for example about the functioning of ADAS and (near) accidents. A number of automotive manufacturers have indicated that they do collect this feedback by entering into discussion with their customers, and holding public discussions, for example during conferences and at car events. Nonetheless, an analysis of online media has revealed that in many cases, users are simply passed on to the car dealer as their point of contact, despite the fact that car dealers are not always aware of all ADAS in the vehicle, and the fact that potential problems must first be known at the car dealership if the dealer is to go in search of a solution.

Suppliers are a key link, because in many cases manufacturers purchase ADAS from these parties. Just like manufacturers, suppliers can also learn from accidents in a number of different ways. Suppliers have little to no contact with end users. They receive feedback about the performance of ADAS, but mainly via the automotive manufacturers. This feedback has limited application because the suppliers are often already working on the next generation of ADAS when the feedback about the performance of the previous generation is received. Just like automotive manufacturers, in certain cases, suppliers do carry out on-site investigations. However, suppliers do not do this on their own initiative. If the manufacturer investigates an accident, they may opt to call in the supplier to provide assistance, if there is a suspicion that the ADAS played a role. In other cases, the supplier is generally left out of the loop.

As well as learning from their own accident investigations and information collection processes, manufacturers can also learn from case studies from fellow manufacturers. After all, many manufacturers work with systems from the same supplier, ADAS have similar functions, and also come up against the same technical limitations in the current generation of ADAS, both during the design and use phase. However, in practice, little information is shared between manufacturers. The most important reason put forward for this is the competitive interests and limited similarity of ADAS due to mutual differences in terms of functionality and operation. Manufacturers above all focus on improving their own products and pay less attention to improving the safety of ADAS in general.

At the start of 2019, Volvo Cars broke the silence of manufacturers by publishing its database with the results of investigations into accidents involving more than 40,000 cars, over the years. Volvo Cars referred to this as the E.V.A. (Equality for Vehicle Advancement) initiative, see also section 3.1.

### 5.3.2 Learning from accidents and hazardous situations by government

The shortcomings in accident registration, which also include a lack of information about in which cars ADAS are installed (section 5.2.2), means that the Ministry of Infrastructure and Water Management has no insight into how many accidents occur involving cars equipped with ADAS. The introduction of the GDPR has in fact made accident investigation even more difficult.[153]

[153] Minister of Infrastructure and Water Management, *Letter to Parliament Answering Parliamentary Questions from Members Dijkstra and Van Gent (both VVD) on the Reports ''De schrikbarende stijging die niemand kan verklaren' and 'Verkeersanalyse provincie nutteloos door privacywet')*, 2019.

**Partial conclusions**
Within the sector, there is insufficient learning at systemic level from (near) accidents, due to the absence of empirical data and lack of transparency. There is almost no information sharing between manufacturers; any learning that does take place is unique to the manufacturer, and it is up to the manufacturer itself to determine the extent to which anything is learned. As a result, each manufacturer has its his own learning process. There are no agreements and no statutory obligations to learn from incidents as is the case in aviation, shipping and at companies subject to the Major Accidents Risks Decree (BRZO - Besluit Risico Zware Ongelukken), where learning from incidents and sharing safety information are laid down in international conventions.

The Ministry of Infrastructure and Water Management is unable to assess the effect (be it positive or negative) of the introduction of ADAS on road safety. The necessary monitoring data are absent. The Ministry of Infrastructure and Water Management in no way ensures that it has access to sufficient empirical data about the safety of ADAS, while access to that information is in fact essential for the feedback loop.

## 5.4 Learning from cybersecurity incidents

### 5.4.1 No large-scale incidents

To date, in practice, the automotive industry has not faced any large-scale cyber threat. On the other hand, experience has been gained of misuse, for example of contactless car keys, whereby thieves are able to capture the signals from the key, and use those signals to steal the car. However, abuse of this vulnerability has no impact on the road safety of the vehicle. With the exception of car theft, a practically applicable earning model for the abuse of vulnerabilities has not yet been found. Other sectors have been far more affected by cyber threats, because attackers were able to earn money through hacks. Examples are hacking the security of picture material for pay TV and the abuse of Internet banking. In both cases, a cat and mouse game has arisen, aimed at staying one step ahead of the criminals. A major difference between these examples and the automotive industry is that in the above sectors, the negative effect is primarily financial, and has no safety impact.

The ability of the automotive industry to respond to hacks and to minimize its effects, remains unclear because the automotive industry has barely had to deal with any large-scale cyber threats. Initiatives such as the Auto-ISAC do contribute to the sharing of knowledge of these threats within the sector. To date, many digital attack scenarios have been estimated as unlikely[154] because no concrete examples are known in practice.[155] (Cybersecurity principles: Control structure)

[154] ENISA, *Cyber security and Resilience of Smart Cars; Good Practices and Recommendations*, 2016.
[155] In other investigations by the Dutch Safety Board, it has been noted that certain scenarios were considered unlikely, namely *MH17 Crash*, 2015 and *Emerging Food Safety Risks*, 2019

Content
Considerations
Summary
Recommendations
Abbreviations
1 Introduction
2 Reference framework
3 Managing safety risks
4 Bottlenecks in the safe introduction and deployment of ADAS
5 Bottlenecks in monitoring and adjustment
6 Conclusions
7 Recommendations
References
Appendices

### 5.4.2 Learning from vulnerabilities and incidents

No abuse of vulnerabilities is known which has had an effect on safety. On the other hand, as is the case with other computer systems, vulnerabilities have been identified (section 3.6). These security incidents were investigated by security investigators, whose aim is to assist in improving car security.

The responsible reporting of vulnerabilities by security investigators assists manufacturers in effectively structuring their internal handling process for identified vulnerabilities or the abuse of vulnerabilities (incident response). By applying this process in practice, the entire cybersecurity process will be raised to a higher plane, and a more rapid response to incidents actually involving the abuse of vulnerabilities will be achieved. This is reflected in the reference framework in the importance of cooperating with third parties with the aim of improving the cybersecurity of the system. (Cybersecurity principle: Control structure)

The majority of automotive manufacturers today operate bug bounty programmes, that offer external hackers the opportunity to earn money from identified vulnerabilities, at least if they are reported according to the conditions laid down. General Motors also makes use of the expertise of external security investigators via the bug bounty programme from HackerOne[156] and operates a security programme according to which researchers are given access to a GM car. Another example is Tesla, which was the first automotive manufacturer to make a vehicle available for the public hacker competition Pwn2Own. In this process, Tesla has followed the example of software companies like Microsoft and Apple.

Knowledge of vulnerabilities and the capacity to correct those vulnerabilities is primarily present among manufacturers and not among repair workshops or dealers. These are dependent on the manufacturers and as a rule are not capable of independently carrying out cybersecurity investigations. Because dealerships and car repair workshops often do not have a role to play in the chain of vehicle cybersecurity, there are no checks and balances in the chain, and greater responsibility is placed on the manufacturer.

In the statistics from the bug bounty programmes, the conclusion can be drawn that many reported vulnerabilities have been solved. In practice, car manufacturers differ in their response to solving identified vulnerabilities, as discussed in section 4.2.5. Most vehicle makes have no knowledge of the presence or past presence of vulnerabilities in a specific model. There is no overall control.

Car manufacturers do share threats and best practices and information about hacks and other incidents within the automotive information sharing and analysis centre (Auto-ISAC)[157]. The Auto-ISAC is a positive example of how an often mutually exclusive automotive industry is willing to cooperate in the field of cybersecurity.

[156] HackerOne, *How GM Works with Hackers to Enhance Their Security*, 2018.
[157] For more information, see https://www.automotiveisac.com/

**Partial conclusions**
As yet, there has been no large-scale abuse of vulnerabilities in vehicles thereby representing a risk to road safety. Cybersecurity will become an important issue if hackers find a practically applicable earning model. It is unclear whether the sector will be able to offer a suitable response.

Knowledge of vulnerabilities and choices made in response to those vulnerabilities (the cybersecurity risk estimation) are matters for the manufacturer and are only sparingly shared with other chain parties, such as dealers or repair workshops. Government and users also have no insight.

**Overview of findings with regard to cybersecurity**
The subject cybersecurity is discussed in chapter 3, chapter 4 and chapter 5. For that reason, we have made a summary of the key findings with regard to cybersecurity.

Over the past few years, cybersecurity has enjoyed a growing level of attention within the automotive industry. The need for this response has been made clear by the identification of a number of vulnerabilities. Manufacturers must balance how much they wish to invest in security in order to resist future threats. A complicating factor for the automotive industry as compared with other sectors, such as office automation, is the long development time, long service life and the complex system of components, suppliers and software. This makes it all the more relevant to ensure that the cybersecurity principles (reference framework, section 2.2) are applied universally.

As yet, there is no consensus on the cybersecurity measures needed for the design of existing cars and which cybersecurity measures need to be taken for cars produced in the past. Standards and best practices for cybersecurity are currently being developed. Requirements on cybersecurity in the form of legislation are also being developed.

Automotive manufacturers experience difficulty in effectively and correctly applying cybersecurity principles. The following bottlenecks have been identified with regard to the subject of cybersecurity:

- It is difficult to determine to what extent car cybersecurity is still the consequence of a lack of knowledge about the electronics in the vehicle (security-by-obscurity as opposed to defence-in-depth).
- In many cases, it is unclear whether the software in a certain earlier produced model or type of car is up-to-date, and whether those models and types contain vulnerabilities that are known to the manufacturer (lack of transparency).
- The software in cars is insufficiently updated, as a result of which cybersecurity is insufficiently guaranteed throughout the entire service life.
- There are no type approval requirements for systems linked to the car, such as digital maps and mobile telephones, nor are there any permanent requirements, despite the fact that these systems have a direct impact on the cybersecurity of the vehicle and hence possibly indirectly on vehicle safety.
- Existing cars are not equipped to permit accident investigation into the possible relevance of cybersecurity aspects. Due to the lack of empirical data, it is not possible to learn enough from cybersecurity incidents (lack of openness and access).
- Cybersecurity incidents will occur more regularly once hackers have identified a practically applicable earning model. It is unclear whether the sector will be able to respond adequately (unknown control structure).
- The cybersecurity risk assessment is currently only made by automotive manufacturers; users and governments are expected to trust that this is carried out in an adequate manner. This is contradictory to the safety principles described in section 2.1, for the introduction of new technology.

## 5.5 Conclusions

Above all for users and government at all levels, ADAS form something of a 'black box'. This is not of benefit for road safety. There is a lack of insight into the functioning of ADAS, and it is unclear in which vehicles ADAS are installed. In the same way, it is not clear for all types of ADAS what effect they have on road safety. As a result, the safety principles transparency and explainability are not satisfied, both of which are integral parts of socially responsible innovation. Furthermore there are no good gatekeepers governing the introduction of ADAS. And there are no structured evaluations into the reduction of accident numbers that should be brought about by ADAS. Innovation is moving forward without adjustment and without the necessary mitigating measures. Moreover, there is no sound monitoring following the introduction of these new technologies. Accidents involving ADAS are not monitored. All these aspects are further amplified by the limited willingness of the stakeholders to share data. Both transparency and the availability of empirical data are essential if the government is to make adjustments and intervene.

Content
Considerations
Summary
Recommendations
Abbreviations
1 Introduction
2 Reference framework
3 Managing safety risks
4 Bottlenecks in the safe introduction and deployment of ADAS
5 Bottlenecks in monitoring and adjustment
6 Conclusions
7 Recommendations
References
Appendices

# 6 CONCLUSIONS

*New risks*
Automation in road traffic can help improve road safety, but also engender new road safety risks. On the basis of accident investigations, a literature review and discussions with experts, the Dutch Safety Board has identified a number of types of new risks that are not yet sufficiently recognized identified or managed. When they are placed on the market, ADAS are not yet fully mature. This means that following approval to the public roads, they undergo further development. Together with the lack of knowledge among drivers, situations in which drivers fail to understand why the vehicle responds or fails to respond in a particular way can quickly arise. In addition, drivers in vehicles fitted with ADAS play a different role than drivers in conventional cars, namely the role of operator. The range of tasks that this role engenders creates the risk that drivers become less alert and react too slowly. The advances in automation also mean that cars with ADAS have increasingly become computers on wheels. As a consequence, the risks inherent in computers have been increasingly introduced to cars fitted with ADAS. These include cybersecurity risks and the risk that essential safety and security updates are not carried out. Updates themselves can in fact represent a specific risk, if they change the functioning of the ADAS and as a consequence the driving behaviour of the vehicle, without the driver being fully aware of this change.

*Driver not the central point of focus*
ADAS are often not fully matured. In combination with untrained drivers, this results in situations whereby drivers in cars fitted with ADAS feel the system regularly take over control of the car. On occasion, the system surprises the driver with sudden interventions, or indeed unexpectedly failing to intervene. ‘Who is in control?’ then literally becomes a crucial question. However, in the current generation of ADAS, automotive manufacturers and government consider this question irrelevant. They instead stick to the traditional, legal approach that the driver is liable, while that same driver is often insufficiently equipped to operate the ADAS under these circumstances. In their marketing and public information, automotive manufacturers reinforce the impression that ADAS are above all intended to enhance the safety and comfort of the driver, without pointing out the new safety risks that go hand in hand with automation.

*Safety not central to design*
Automation in cars is driven by technological possibilities. Certainly for ADAS that aim to increase driver comfort, those technological possibilities are the underlying principle for the development, while the requirement that safety levels are not allowed to decline is insufficiently operationalized. The user is not central to the design. Moreover, in the design process, insufficient attention is paid to safety during the lifecycle of the system. For example, cybersecurity is insufficiently guaranteed throughout the full lifecycle. It is often unknown whether car software in fact has vulnerabilities.

*Inappropriate legislation*
Technological changes are clearly outpacing the regulation of those changes. As a consequence, current legislation is no longer appropriate for modern cars, which have more or less become computers on wheels. In particular with regard to human factors the rules are lagging behind, because manufacturers and government pay little attention to these aspects. Moreover, regulations are not geared to the fact that cars are becoming increasingly dynamic and that following approval to the public roads, they continue to change as a result of updates. In addition to traditional detailed regulations, there are also laws that impose a minimum safety level. However, nowhere do these laws specify how the level of safety provided by ADAS can be assessed. As a result, there is no supervision of the way in which manufacturers estimate risks and consider scenarios. This means that systems are type approved without any knowledge of their effect on road safety.

*Insufficient learning capacity*
Both manufacturers and government learn insufficient lessons from accidents because:

- there is no record of which ADAS are fitted in which vehicle;
- accidents involving ADAS are not monitored;
- accident registration by the police is generally incomplete, and fatal accidents are at best counted (total numbers) but not analysed;
- the necessary data cannot be retrieved from a vehicle, or at least not without considerable difficulties;
- there is no structured evaluation into the reduction of accident numbers that should be achieved thanks to the deployment of ADAS.

As a result, there is no knowledge of how many accidents take place involving ADAS and how many are prevented by ADAS. Manufacturers learn insufficient lessons from accidents involving their own car makes. Indeed, they do not even investigate a large proportion of those accidents. Manufacturers do not learn from one another and that restricts the learning capacity of the entire sector. Moreover, suppliers are almost never involved in accident investigations with the aim of improving road safety.

*Insufficient attention for the current generation of ADAS*
The government, in particular the Ministry of Infrastructure and Water Management, is more interested in the (distant) future of autonomous cars than the introduction and use of today's generation of ADAS. The Ministry has limited vision on how ADAS can contribute to improving road safety and fails to proactively carry out systematic risk analyses. At the same time, the Ministry has started encouraging ADAS subject to certain conditions, but improving road safety is not one of those necessary conditions, as long as the effect on one of the three targets (road safety, the environment or traffic flows) is positive. New regulations currently being developed within the UNECE, for example with regard to human machine interaction and accessibility of data from ADAS to allow thorough accident investigation, relate only to future systems that (temporarily) take over control from the driver. Existing legislation is no longer appropriate for today's systems that assist or support the driver.

*Uncertain effect on road safety*

Both the Dutch government and the European Commission are striving to achieve zero road fatalities by 2050. To achieve this ambitious target, much hope rests on technological developments in general, and vehicle automation in particular. However, the introduction and use of ADAS leads to new risks, many of which are as yet insufficiently recognized, monitored and managed. Although ADAS can potentially have a positive influence on road safety, as yet there are no guarantees that that potential will be truly fully utilized.

# 7 RECOMMENDATIONS

*To the automotive manufacturers and the OICA and ACEA umbrella organizations:*

1. Demonstrate that the development and introduction of ADAS is taking place according to the principles of responsible innovation.

*To the BOVAG and RAI Association:*

2. Ensure that BOVAG members fully instruct their customers on the possibilities and limitations of their vehicles equipped with ADAS. And make sure that BOVAG members are able to do this.

*To the Minister of Infrastructure and Water Management:*

3. Take the initiative within the UNECE to place human factors and responsible innovation on the agenda.

4. Support the initiatives of Euro NCAP to make human factors and consumer information about ADAS an integral part of the vehicle safety assessment (Euro NCAP star system).

5. Improve the possibilities for learning from road traffic accidents in general and the role of ADAS in particular, and take measures aimed at improving road safety on the basis of the study results.

6. Within the European Commission, argue that vehicle regulations must tie in with the current generation of ADAS (SAE level 2 and lower). Responsibility for demonstrating that new ADAS improve safety must be placed clearly in the hands of the manufacturers. Moreover, attention should be focussed on the introduction of requirements relating to human factors, user training, access to data from ADAS following accidents and accident investigation by manufacturers.

# REFERENCES

AAA, Advanced Driver Assistance Technology Names, 2019, https://newsroom.aaa.com/2019/01/common-naming-for-adas-technology/.

AAA, Automatic emergency braking with pedestrian detection, 2019, https://www.aaa.com/AAA/common/aar/files/Research-Report-Pedestrian-Detection.pdf.

AAA Foundation for Traffic Safety, Potential Reductions in Crashes, Injuries, and Deaths from Large-Scale Deployment of Advanced Driver Assistance Systems, 2018, http://aaafoundation.org/wp-content/uploads/2018/09/18-0567_AAAFTS-ADAS-Potential-Benefits-Brief_v2.pdf.

AAA Foundation for Traffic Safety, Vehicle Owners' Experiences with and Reactions to Advanced Driver Assistance Systems, 2018, https://aaafoundation.org/vehicle-owners-experiences-reactions-advanced-driver-assistance-systems/.

Abraham, H., Seppelt, B., Mehler, B., and Reimer, B., What's in a Name: Vehicle Technology Branding and Consumer Expectations for Automation, AutomotiveUI 2017 - 9th International ACM Conference on Automotive User Interfaces and Interactive Vehicular Applications, Proceedings, number September, 2017.

ACEA, ACEA Position Paper; General Safety Regulation Revision. Brussel, 2018.

ADAS Alliance, ADAS Convenant, 2019.

ADAS Alliance, Website ADAS Alliantie, https://www.adasalliantie.nl. Accessed August 23, 2019.

Alvarez, S., Safety Benefit Assessment, Vehicle Trial Safety and Crash Analysis of Automated Driving: A Systems Theoretic Approach. PSL Research University, 2017, https://pastel.archives-ouvertes.fr/tel-01767563.

ANWB, Verwachtingen werking Lane Assist nog te hoog gespannen; Onderzoek naar rijbaanhulpsysteem in auto's, 2017, https://www.anwb.nl/auto/zelfrijdende-auto/rijbaan-hulp-lane-assist-onderzoek.

ANWB, Welke rijhulpsystemen zijn er?, 2017, https://www.anwb.nl/auto/zelfrijdende-auto/andere-systemen.

Aon Risk Solutions, Whitepaper: Als de auto autonoom wordt; Verkennende analyse van de verzekeringsmarkt en nieuwe risico's bij zelfrijdende auto's, 2015.

BCG, A Roadmap to Safer Driving through Advanced Driver Assistance Systems, 2015.

Bloomfield, R., Butler, E., Guerra, S., and Netkachova, K., Security-Informed Safety: Integrating Security within the Safety Demonstration of a Smart Device, 10th International Topical Meeting on Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies, 2017, http://openaccess.city.ac.uk/17724/1/pp9v01n_npic_cyber_smarts.pdf.

Boelhouwer, A., Beukel, A.P. van den, Voort, M.C. van der, and Martens, M.H., Should I Take over? Does System Knowledge Help Drivers in Making Take-over Decisions While Driving a Partially Automated Car?, Transportation Research Part F: Traffic Psychology and Behaviour 60, number December, 2019: 669–684, https://doi.org/10.1016/j.trf.2018.11.016.

Borup, M., Brown, N., Konrad, K., and Lente, H. van, The Sociology of Expectations in Science and Technology, Technology Analysis and Strategic Management 18, 2006: 285–298.

British Standards Institution, Connected Automotive Ecosystems – Impact of Security on Safety – Code of Practice, Vol. PAS 11281, 2018.

British Standards Institution, The Fundamental Principles of Automotive Cyber Security. Specification, Vol. PAS 1885, 2018, https://shop.bsigroup.com/ProductDetail/?pid=000000000030365446&_ga=2.267667464.704902458.1545217114-2008390051.1545217114.

British Standards Institution, The Fundamental Principles of Automotive Cyber Security, Vol. PAS 1885, 2018, https://shop.bsigroup.com/ProductDetail/?pid=000000000030365446&_ga=2.267667464.704902458.1545217114-2008390051.1545217114.

C't Magazine, Connected cars in de fout bij cybersecurity, 2016, https://www.ct.nl/achtergrond/connected-cars-fout-cybersecurity/.

Cai, Z., Wang, A., Zhang, W., Gruffke, M., and Schweppe, H., 0-Days & Mitigations : Roadways to Exploit and Secure Connected BMW Cars, White Paper Blackhat USA 2019 Conference, 2019: 1–37.

CAR, Technology Roadmaps: Intelligent Mobility Technology, Materials and Manufacturing Processes, and Light Duty Vehicle Propulsion, 2017, https://doi.org/10.1044/leader.ppl.22062017.20.

Carsten, O., and Martens, M.H., How Can Humans Understand Their Automated Cars? HMI Principles, Problems and Solutions, Cognition, Technology and Work 21, number 1, 2019: 3–20, https://doi.org/10.1007/s10111-018-0484-0.

Charette, R.N., This Car Runs on Code, https://spectrum.ieee.org/transportation/systems/this-car-runs-on-code. Accessed August 21, 2019.

Charlebois, D., Meloche, E., and Burns, P., Detection of Cyclist and Pedestrians Around Heavy Commercial Vehicles, In 26th International Technical Conference and Exhibition on the Enhanced Safety of Vehicles (ESV). Eindhoven: Transport Canada, 2019.

Daimler, BMW and Daimler. Plan to Headquarter Joint Venture in Berlin, https://www.daimler.com/innovation/case/shared-services/jv-daimler-and-bmw.html. Accessed August 22, 2019.

Dave, P., Google Ditched Autopilot Driving Feature after Test User Napped behind Wheel, Edited by Sam Holmes. Atwater, California, USA: Reuters, 2017.

Electrek.co, Tesla Increases Autopilot 2.0 Speed Limits with Latest Update, https://electrek.co/2017/03/08/tesla-autopilot-2-0-speed-limit-update/. Accessed May 21, 2018.

Electrek.co, Tesla Releases New Update to Enable Full Speed Automatic Emergency Braking for Autopilot 2.5 and More, https://electrek.co/2017/10/22/tesla-update-full-speed-automatic-emergency-braking-autopilot-2-5/. Accessed August 7, 2018.

Endsley, M.R., and Kaber, D.B., Level of Automation Effects on Performance, Situation Awareness and Workload in a Dynamic Control Task., Ergonomics 42, number 3, 1999: 462–492.

ENISA, Cyber Security and Resilience of Smart Cars; Good Practices and Recommendations, 2016.

ETSC, BRIEFING | EU Strategy for Automated Mobility, 2018.

ETSC, Prioritising the Safety Potential of Automated Driving in Europe, 2016.

ETSC, Road Safety Priorities for The EU 2020-2030; Briefing for the European Parliamentary Elections, 2018, http://etsc.eu/wp-content/uploads/2015_lux_pres_briefing_final.pdf.

EU Member States, Declaration of Amsterdam; Cooperation in the Field of Connected and Automated Driving, 2016.

Euro NCAP, Euro NCAP 2025 Roadmap: in pursuit of vision zero, 2017

Euro NCAP, 2018 Geautomatiseerde Rijsystemen, 2018, https://www.euroncap.com/nl/veiligheid-voertuig/veiligheidscampagnes/2018-geautomatiseerde-rijsystemen/.

European Commission, Annex 1: Strategic Action Plan on Road Safety, In Europe on the Move; Sustainable Mobility for Europe: Safe, Connected and Clean, 2018.

European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee, the Committee of the Regions; On the Road to Automated Mobility: An EU Strategy for Mobility of the Future, 2018.

European Commission, Press release Road safety: Commission welcomes agreement on new EU rules to help save lives, https://europa.eu/rapid/press-release_IP-19-1793_en.htm. Accessed August 23, 2019.

Eykholt, K., Evtimov, I., Fernandes, E., Kohno, T., Li, B., Prakash, A., Rahmati, A., and Song, D., Robust Physical-World Attacks on Deep Learning Visual Classification, CVPR, number 2018, 2017, https://arxiv.org/pdf/1707.08945.pdf.

Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., and Luetge, C., An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations, Minds and Machines 28, number 4, 2018: 689–707, https://doi.org/10.31235/OSF.IO/2HFSC.

Folda, C., From Requirement to Standard Security Test; A Brief Introduction to the World of Security Testing, Vector Cybersecurity Symposium 2019, 2019, https://assets.vector.com/cms/content/events/2019/vSES19/vSES19_08_Folda_Continental.pdf.

Fridman, L., Brown, D. Glazer, M. Angell, W., Dodd, S., Jenik, B., Terwilliger, J., Patsekin, A., Kindelsberger, J., Ding, L., Seaman, S., Mehler, A., Sipperley, A., Pettinato, A., Seppelt, B.D., Angell, L., Mehler, B., and Reimer B., MIT Advanced Vehicle Technology Study: Large-Scale Naturalistic Driving Study of Driver Behavior and Interaction With Automation, IEEE Access 7, 2019

Future of Life Institute, AI Principles, https://futureoflife.org/ai-principles. Accessed January 7, 2019.

Gorter, M., and Klem, E., Markering en rijtaakondersteunende systemen. Amersfoort: Royal Haskoning DHV on behalf of the Province of Utrecht, 2016.

GOV.UK, The Key Principles of Vehicle Cyber Security for Connected and Automated Vehicles, 2017, https://doi.org/10.1016/j.molcel.2010.01.018.

Greenberg, A., After Jeep Hack, Chrysler Recalls 1.4M Vehicles for Bug Fix, https://www.wired.com/2015/07/jeep-hack-chrysler-recalls-1-4m-vehicles-bug-fix/. Accessed August 17, 2018.

Greenberg, A., Hackers Remotely Kill a Jeep on the Highway—With Me in It, https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/. Accessed August 17, 2018.

Greenberg, A., Hackers Reveal Nasty New Car Attacks--With Me Behind The Wheel (Video). Forbes, https://www.forbes.com/sites/andygreenberg/2013/07/24/hackers-reveal-nasty-new-car-attacks-with-me-behind-the-wheel-video/. Accessed August 23, 2018.

Greenberg, A., The Jeep Hackers Are Back to Prove Car Hacking Can Get Much Worse. Wired, https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks/. Accessed Augustus 23, 2018.

HackerOne, How GM Works with Hackers to Enhance Their Security, 2018.

Harms, I.M., and Dekker, G.-M., ADAS: From Owner to User; Insights in the Conditions for a Breakthrough of Advanced Driver Assistance Systems, 2017.

Hattem, J. Van, Klem, E., and Gorter, M., AEBS en verkeersmaatregelen; praktijktest zichtbaarheid verkeersmaatregelen voor autonomous emergency braking systems, Amersfoort: Royal Haskoning DHV, 2017.

High Level Group on the Competiteness and Sustainable Growth of the Automotive Industry in European Union, Gear 2030, 2017.

Iriondo, R., Differences Between AI and Machine Learning, and Why It Matters, https://medium.com/datadriveninvestor/differences-between-ai-and-machine-learning-and-why-it-matters-1255b182fc6. Accessed August 23, 2019.

ISO, ISO 26262-6:2018 Road Vehicles - Functional Safety - Part 6: Product Development at the Software Level. Gene, 2018.

ISO, The ISO/IEC 27000 Family of Standards Helps Organizations Keep Information Assets Secure., https://www.iso.org/isoiec-27001-information-security.html. Accessed August 23, 2019.

ISO, and IEC, ISO/IEC 15408-1:2009, ISO, 2009.

Jong, R. De, Kool, L., and Est, R. Van, Zo Brengen We AI in de praktijk vanuit Europese waarden, 2019, https://www.rathenau.nl/sites/default/files/inline-files/Zo brengen we AI in de praktijk vanuit Europese waarden - Roos de Jong%2C Linda Kool en Rinie van Est_0.pdf.

Klem, E., Barten, N., Droogsma, J., Gorter, M., and Huisman, M., AEBS en Vrachtwagens; Praktijktest herkenbaarheid vrachtwagens voor Advanced Emergency Braking System. Royal Haskoning DHV, 2017.

Knapp, A., Neumann, M., Brockmann, M., Walz, R., and Winkle, T., Code of Practice for the Design and Evaluation of ADAS, 2009, https://www.acea.be/uploads/publications/20090831_Code_of_Practice_ADAS.pdf.

Kyriakidisa, M., Winter, J.C.F. de, Stanton, N., Bellet, T., Arem, B. van, Brookhuis, K., Martens, M.H., A Human Factors Perspective on Automated Driving, Theoretical Issues in Ergonomics Science 18, number 1, 2017: 1–27, https://doi.org/http://dx.doi.org/10.1080/1463922X.2017.1293187.

Leplat, J., Occupational Accident Research and Systems Approach, Journal of Occupational Accidents 6, number 1–3, 1984: 77–89.

McCandless, D., Doughty-White, P., and Quick, M., Million Lines of Code, https://informationisbeautiful.net/visualizations/million-lines-of-code/. Accessed July 10, 2019.

McKinsey&Company, Rethinking Car Software and Electronics Architecture, 2018: 1–15.
Michigan Tech Research Institute, Benchmarking Sensors for Vehicle Computer Vision Systems, https://mtri.org/automotivebenchmark.html. Accessed August 28, 2019.

Minister of Infrastructure and the Environment, Letter to Parliament 31305 Mobiliteitsbeleid, 2014.

Minister of Infrastructure and Water Management, Letter to Parliament Answering Parliamentary Questions by Members Dijkstra and Van Gent (both VVD) on the Reports "De schrikbarende stijging die niemand kan verklaren" and "Verkeersanalyse provincie nutteloos door privacywet", 2019.

Minister of Infrastructure and Water Management, Letter to Parliament 205325 Smart Mobility Dutch Reality, 2018.

Minister of Infrastructure and Water Management, Letter to Parliament Answering Parliamentary Questions by Members Schonis and Verhoeven (both D66) on The Article "Wie Temt Het Datamonster in de Auto-Industrie?", 2019.

Ministry of Infrastructure and Water Management, Ministry of Justice and Security, IPO, VNG, Vervoerregio Amsterdam, and Metropoolregio Rotterdam Den Haag, Veilig van deur tot deur; Het strategisch plan verkeersveiligheid 2030: Een gezamenlijke visie op aanpak verkeersveiligheidsbeleid, 2018.

Ministry of Infrastructure and Water Management, Landelijk actieplan verkeersveiligheid 2019-2021: Veilig van Deur Tot Deur. Den Haag, 2018, https://www.rijksoverheid.nl/documenten/rapporten/2018/12/05/bijlage-2-landelijk-actieplan-verkeersveiligheid-2019-2021.

National Cyber Security Center, Cybersecuritybeeld Nederland CSBN 2018, 2018.

National Instruments, Building Flexible, Cost-Effective ECU Test Systems, 2019, https://www.ni.com/nl-nl/innovations/white-papers/06/building-flexible--cost-effective-ecu-test-systems.html.

Nes, C.N. Van, and Duivenvoorden, C.W.A.E., Veilig naar het verkeer van de toekomst; Nieuwe mogelijkheden, risico's en onderzoeksagenda voor de verkeersveiligheid bij automatisering van het verkeerssysteem, R-2017-2. Den Haag: SWOV, 2017.

NHTSA, A Summary of Cybersecurity Best Practices, 2014.

NHTSA, Cybersecurity Best Practices for Modern Vehicles, 2016, http://www.nhtsa.gov/staticfiles/nvs/pdf/812333_CybersecurityForModernVehicles.pdf.

Nick Davis, Automotive Electronics: What Are They, and How Do They Differ from "Normal" Electronics? - Power Electronics, https://www.powerelectronicsnews.com/technology/automotive-electronics-what-are-they-and-how-do-they-differ-from-normal-electronics. Accessed August 23, 2019.

Nie, S., Liu, L., and Du, Y., Free-Fall: Hacking Tesla from Wireless to CAN Bus, In Blackhat Briefings. USA, 2017, https://www.blackhat.com/docs/us-17/thursday/us-17-Nie-Free-Fall-Hacking-Tesla-From-Wireless-To-CAN-Bus-wp.pdf.

Nissan, Nissan LEAF - Elektrische Auto - Elektrische Voertuigen, 2019, https://www.nissan.nl/voertuigen/nieuw/leaf.html.

NIST, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, 2018, https://doi.org/10.6028/NIST.CSWP.04162018.

NIST, NIST Special Publication 800-Series, https://csrc.nist.gov/publications/sp800. Accessed January 24, 2019.

NTSB, Collision Between a Car Operating With Automated Vehicle Control Systems and a Tractor-Semitrailer Truck - Highway Accident Report, 2017, https://doi.org/10.1093/jicru/ndl025.

NTSB, Preliminary Report: Highway HWY18FH011, 2018,https://www.ntsb.gov/investigations/AccidentReports/Reports/HWY18FH011-preliminary.pdf.

NTSB, Preliminary Report - Highway - HWY18MH010. Washington D.C., 2018, https://www.ntsb.gov/investigations/AccidentReports/Reports/HWY18MH010-prelim.pdf.

Onderzoeksraad voor Veiligheid, Koolmonoxide: Onderschat en onbegrepen gevaar, 2015.

Onderzoeksraad voor Veiligheid, MH17 Crash, 2015.

Onderzoeksraad voor Veiligheid, Opkomende voedselveiligheidsrisico's, 2019.

PBL, Mobiliteit en elektriciteit in het digitale tijdperk. Publieke waarden onder spanning, 2017.

Poel, I. van de, An Ethical Framework for Evaluating Experimental Technology, Science and Engineering Ethics 22, number 3, 2016: 667–686, https://doi.org/10.1007/s11948-015-9724-3.

Rathenau Instituut, Met beleid vormgeven aan sociotechnische innovatie, 2016.

Rathenau Instituut, Mensenrechten in het robottijdperk, 2017.

RDW, Jaarverslag 2018, 2019.

Rip, A., The Past and Future of RRI, Life Sciences, Society and Policy 10, number 1, 2014: 17, https://doi.org/10.1186/s40504-014-0017-4.

Russel, S., and Norvig, P., Artificial Intelligence – A Modern Approach, 2010, https://doi.org/10.1017/S0269888900007724.

SAE International, Cybersecurity Guidebook for Cyber-Physical Vehicle Systems - J3061, 2016.

SAE International, Requirements for Hardware-Protected Security for Ground Vehicle Applications - J3101, 2012, https://www.sae.org/standards/content/j3101/.

SAE International, Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles - Surface Vehicle Information Report, 2014.

Santoni de Sio, F., Ethics and Self-Driving Cars; A White Paper on Responsible Innovation in Automated Driving Systems, number October, 2016.

Schomberg, R. von, A Vision of Responsible Research and Innovation, In Responsible Innovation, edited by M. Heintz and J Bessant R. Owen. London: John Wiley, 2013.

Staak, B. Van der, Verdwijnende apps op smart-tv's, 2018, https://www.consumentenbond.nl/tv/honderden-meldingen-over-verdwijnende-apps-op-smart-tvs.

SWOV, Dodelijke verkeersongevallen op rijkswegen in 2017, 2019.

SWOV, Ernstig verkeersgewonden 2017, 2018, https://www.swov.nl/publicatie/ernstig-verkeersgewonden-2017.

SWOV, Factsheet verkeersdoden in nederland, 2019.

SWOV, Veiligheidseffecten van rijtaakondersteunende systemen; Bijlage bij het convenant van de ADAS Alliantie, 2019.

Teffer, P., Dieselgate. Hoe de industrie sjoemelde en europa faalde, 2017.

Tencent, Experimental Security Assessment of BMW Cars: A Summary Report, 2018.

Tesla, Q3 2018 Vehicle Safety Report, https://www.tesla.com/nl_NL/blog/q3-2018-vehicle-safety-report. Accessed December 12, 2018.

Tesla, Tesla Model S Owner's Manual, 2018, https://www.tesla.com/sites/default/files/model_s_owners_manual_europe_nl_nl.pdf.

Tricentis, AI Approaches Compared: Rule-Based Testing vs. Learning, https://www.tricentis.com/artificial-intelligence-software-testing/ai-approaches-rule-based-testing-vs-learning/. Accessed August 23, 2019.

UNECE, ECE/TRANS/WP.29/2019/34, Framework Document on Automated/ Autonomous Vehicles, 2019.

UNECE, ECE/TRANS/WP.29/78/Rev.6, Consolidated Resolution on the Construction of Vehicles (R.E.3), Revision 6, 2017, https://www.unece.org/fileadmin/DAM/trans/main/wp29/wp29resolutions/ECE-TRANS-WP.29-78r6e.pdf.

UNECE, ECE/TRANS/WP.29/GRVA/2019/2, Proposal for a Recommendation on Cyber Security, 2019, http://www.unece.org/fileadmin/DAM/trans/doc/2019/wp29grva/ECE-TRANS-WP29-GRVA-2019-02e.pdf.

UNECE, Proposal for Amendments to ECE/TRANS/WP.29/2019/34; Framework Document on Automated/Autonomous Vehicles (Levels 3 and Higher), 2019.

UNECE, World Forum For Harmonization of Vehicle Regulations (WP.29); How It Works, How to Join It, 2019, http://www.unece.org/fileadmin/DAM/trans/main/wp29/wp29wgs/wp29gen/wp29pub/WP29-BlueBook-4thEdition2019-Web.pdf.

Vetzo, M.J., Gerards, J.H., and Nehmelman, R., Algoritmes en grondrechten, 2018.

Vlakveld, W., Vissers, L., Hulleman, K., and Nes, N. van, An Empirical Exploration of the Impact of Transition of Control on Situation Awareness for Potential Hazards; An Experiment about the Hazard Perception Capabilities of Drivers after Interruption in a Video-Based Scanning Task. The Hague: SWOV, 2015.

Vlakveld, W., Nes, N. van, Bruin, J. De, Vissers, L., and Kroft, M. van der, Situation Awareness Increases When Drivers Have More Time to Take over the Wheel in a Level 3 Automated Car: A Simulator Study, Transportation Research Part F: Traffic Psychology and Behaviour, 2018, https://doi.org/10.1016/j.trf.2018.07.025.

VMS on behalf of BOVAG, Het effect van ADAS op schadeherstel, onderhoud en reparatie, 2019.

Volkswagen, Ford – Volkswagen Expand Their Global Collaboration to Advance Autonomous Driving, Electrification and Better Serve Customers, https://www.volkswagen-newsroom.com/en/press-releases/ford-volkswagen-expand-their-global-collaboration-to-advance-autonomous-driving-electrification-and-better-serve-customers-5188. Accessed August 22, 2019.

Volkswagen, Volkswagen start car.software met 5.000 in-house ontwikkelaars, 2019, https://www.volkswagen.nl/nieuws/volkswagen-start-carsoftware-met-5000-in-house-ontwikkelaars/.

Weiss, S.M., and Indurkhya, N., Rule-Based Machine Learning Methods for Functional Prediction, Journal of Artificial Intelligence Research 3 (1995): 383–403, https://arxiv.org/pdf/cs/9512107.pdf.

Wezel, A.P. van, Lente, H. van, Sandt, J.J. van de, Bouwmeester, H., Vandeberg, R.L., and Sips, A.J., Risk Analysis and Technology Assessment in Support of Technology Development: Putting Responsible Innovation in Practice in a Case Study for Nanotechnology, Integrated Environmental Assessment and Management 14, number 1, 2018: 9–16, https://doi.org/10.1002/ieam.1989.

Wright, T.J., Samuel, S., Borowsky, A., Zilberstein, S., and Fisher, D.L., Experienced Drivers Are Quicker to Achieve Situation Awareness than Inexperienced Drivers in Situations of Transfer of Control within Level 3 Autonomous Environment., In Proceedings of the Human Factor and Ergonomics Society 2016 Annual Meeting, 60:270–273, 2016.

WRR, Onzekere veiligheid: Verantwoordelijkheden rond fysieke veiligheid, 2008.

Zhang, B., Winter, J. de, Varotto, S., Happee, R., and Martens, M., Determinants of Take-over Time from Automated Driving: A Meta-Analysis of 129 Studies, Transportation Research Part F: Traffic Psychology and Behaviour 64, 2019: 285–307, https://doi.org/10.1016/j.trf.2019.04.020.

# APPENDIX A

## EXPLANATION OF THE INVESTIGATION

This annex describes the general investigation process, the most important quality assurance measures and the project organization.

### A.1 Aim, research questions and investigation phases

The aim of this investigation was to improve road safety by providing the parties responsible for road safety with insight into ways they can identify and manage the new risks that follow from the introduction and deployment of ADAS. The research questions below were central to this investigation.

- How do users, the automotive industry, sector parties and the government manage the risks associated with the introduction and deployment of Advanced Driver Assistance Systems (ADAS)?
- To what extent can this risk management be improved?

The investigation focuses on the management of the risks associated with the introduction and deployment of (semi-)automated vehicles by manufacturers, suppliers, importers, dealers, regulators, legislators, interest groups, etc. In other words, the focus is on risk management rather than the risks themselves.

*Sub questions*
To answer the first main question, we examined the current situation and the way stakeholders control new risks (safety control structure). To this end, we asked the stakeholders the following questions:

1. Which parties can, or should, take responsibility for safety during the introduction and deployment of ADAS?
   a. Who are these parties? What are their interrelationships? Which existing legislation and regulations apply?
   b. What are their current working methods and how do they interpret and fulfil their tasks?
   c. What is the historical background to this division of tasks and responsibilities?

2. How do these parties identify the risks? How do they respond to risks that have not yet arisen?
    a. How do the parties identify fundamental character changes in vehicles?
    b. How do the parties monitor the (potential) risks?
    c. What types of risks are identified?
    d. What is the level of detail?
    e. How is the severity or magnitude of the risks estimated?
3. How do the parties manage these risks?
4. What basic safety principles do the sector and the regulatory and supervisory system need to comply with (according to the Dutch Safety Board)?
5. To what extent are the risks adequately controlled?
6. Do the parties see opportunities to improve risk management (based on the reference framework drawn up by the Dutch Safety Board)?

*Phases*

The investigation comprised four phases.

| | |
|---|---|
| Phase 1: | Orientation and background |
| Phase 2: | Current situation: research questions 1 to 3 |
| Phase 3: | Reference framework: research question 4 |
| Phase 4: | Comparing the findings to the reference framework: research questions 5 and 6 |

Phase 1: In the orientation and background phase we formed a general picture of the sector (influence and interests) and defined the research questions more closely. This was a repetitious and simultaneous process. In addition, a global overview was drawn up of already existing new risks (based on a literature review and concerns voiced by various parties) and a number of relevant accidents were investigated. We also summarized the results of investigations of a number of accidents in the US (involving Tesla cars and an Uber experimental vehicle) conducted by the NTSB. For phase 1, a number of examples were selected that could be used to interview the involved parties about their current risk management methods. Phases 2 to 4 overlapped somewhat, and phase 2 and phase 3 were conducted partly in parallel.

## A.2 Data collection

Data was collected from a number of sources in order to answer the research questions of each of the various phases. The most important sources of information are described below.

### A.2.1 Interviews

Table 4 provides an alphabetical overview of the interviewed parties. To ensure the quality of the investigation, the Dutch Safety Board always conducts formal interviews with two investigators. The subjects for discussion during the interview are prepared in advance by a team based on the research questions and the results of the analysis (see 'Analysis'). A report of each interview was drawn up and submitted to the interviewed parties for verification.

It proved difficult to hold interviews with private parties such as car manufacturers because they were generally unwilling to participate in the investigation.

| Organization | Organization |
|---|---|
| ANWB | NXP |
| AON | Netherlands Environmental Assessment Agency (PBL) |
| BOVAG | Police (VOA) |
| CBR | PON |
| Computest | Radiocommunications Agency Netherlands |
| Continental | RAI association |
| Cruise automation | Rathenau Institute |
| Daimler | Risk Prosecution |
| DITSS | RLI |
| ENISA | RDW |
| ETSC | RWS |
| Euro NCAP | SWOV |
| Europese Commissie, DG GROW, Unit C.4 | Tesla |
| Science and Technology, Maastricht University | Netherlands Organisation for Applied Scientific Research |
| Ministry of Infrastructure and Water Management | Dutch Association of Insurers |
| Netherlands Forensic Institute (NFI) | Volvo Cars |
| NHTSA | Volvo Trucks |
| Nissan | Waag |
| NTSB | |

*Table 4: Overview of the interviewed organizations (formal and informal interviews).*

### A.2.2 Documents

A large number of documents were consulted as part of the investigation, including published scientific articles and theses on ADAS, legislation and regulations, parliamentary documents, ministerial letters, reports, newspaper articles and internal and/or confidential documents of the interviewed parties.

### A.2.3 Working visits

In order to gain experience with the subject matter, the investigation team organized a practical afternoon during which they tested various ADAS-equipped cars manufactured by Tesla, Volvo and Nissan.

### A.2.4 Conferences and meetings:

Relevant information was also gathered by attending conferences and meetings. The following conferences and meetings were attended:

- EVU Haarlem 2017 (European Association for Accident Research)
- AEBS test day, Lelystad, December 2017
- Humanist conference, The Hague 2018
- ADAS Conference, Rosmalen 2018
- Scandinavian safety boards meeting, 2019
- ESV2019 (International Conference on the Enhanced Safety of Vehicles), Eindhoven

### A.2.5 Investigation of accidents involving cars with ADAS

Nine accidents involving ADAS were investigated to help answer the research questions. Data collected for this purpose included digital tachograph data and data/log files from data recorders. As described in the report, it was not easy to extract the necessary digital information from the vehicles' data recorders after an accident (encryption, no or inadequate EDR storage, no data logging).

The Dutch Safety Board did not only investigate the possible contribution of ADAS to the occurrence or the severity of the investigated accidents. Other factors were also examined, such as the condition of the driver, the use of mobile phones, weather conditions and the condition of the road. These factors were not described in detail in the report. Annex C.3 shows investigated accidents in which ADAS did not have played a significant role.

## A.3 Analysis

### A.3.1 CAST and CASCAD

The CAST method (Causal Analysis using STAMP) was used to analyse the data. This method is based on systems theory (circular causality and feedback & control) rather than the traditional linear causality model. According to STAMP, accidents and/or unsafe situations occur when external disruptions, failing components or dysfunctional interactions between components are not adequately controlled by the hierarchical system of parties (control structure). Safety is thus seen as a control problem that must be managed by a control structure through the imposition and implementation of safety constraints. To this end, the parties need to receive feedback on the relevant process.

A specific version of CAST, developed for the analysis of traffic accidents with automated vehicles, was used for the analysis of the accidents. This method of analysis is called CASCAD (Causal Analysis using STAMP for Connected and Automated Driving[158]). CAST was used to analyse how the parties manage safety risks associated with road traffic automation.

### A.3.2 Analysis sessions

The CAST/CASCAD analysis was partly based on a number of team sessions. These team sessions were also used to systematically share, enrich and interpret data collected by the different team members during the various phases of the investigation. A total of six analysis sessions were held by the investigation team.

### A.3.3 Stakeholder analysis

In order to gain insight into the relevance of the theme and the spheres of influence of the parties, the communications department carried out two stakeholder analyses. This analysis was conducted in two steps: 1) identification of stakeholders and 2) assessing the interests of each stakeholder and to what extent they could influence it. The concrete outcome is an overview in which parties are plotted on a matrix (much/little influence, positive/negative attitude, and much/little interest). By combining these three factors in different ways, the team gained insight into which parties are for or against, what their interest in the investigation is, and which parties play an essential role in the sector. This helped the investigators to determine the most suitable template and sequence for conducting the formal and informal interviews.

### A.3.4 Social media analysis

A social media analysis was carried out to include the element 'user opinions' in the investigation. Four research questions, one general and three specific, were prepared for this purpose:

1. What do users of ADAS-equipped vehicles think about the presence of this technology in their cars?
2. How do users of ADAS-equipped vehicles experience the provision of information about the technology when purchasing a new or second-hand car?
3. To what extent do users of ADAS-equipped vehicles report risks or problems with the technology to the manufacturer, and how does the manufacturer respond to these reports?
4. Are users of ADAS-equipped vehicles aware of accidents involving these vehicles that have not yet included in our report?

An overview was drawn up of user groups and relevant social media, after which data were collected from discussion websites. This concerned 61 discussion topics, mostly on car forums. These data were processed based on a qualitative thematic analysis.

[158] Alvarez, *Safety Benefit Assessment, Vehicle Trial Safety and Crash Analysis of Automated Driving: A Systems Theoretic Approach* PSL Research University, 2017.

### A.3.5 Comparison with civil aviation

The discussion on the introduction and deployment of ADAS in cars often draws the parallel with the introduction of automated systems, such as autopilots, in civil aviation. We have analysed this possible parallel and have come across large differences between automation in civil aviation and in road traffic. Therefore, this analysis has not been included in the report. The main differences are as follows:

- Pilots are much better informed, trained and tested in the operation of automated systems, whereas car drivers are not.
- Automated systems in aviation are better tested and validated than ADAS in cars before they are applied in practice.
- In the design of automated systems in aviation, explicit account is taken of human factors, human machine interaction; in road traffic hardly ever.
- In aviation, a system of risk management and feedback of experiences is in place that structurally supports learning from incidents; in road traffic there is no such system.
- There is consensus in aviation industry about the great importance of safety that transcends commercial interests of individual manufacturers, whereas in the automotive industry commercial interests seem to prevail over road safety.
- Road traffic is more complex than air traffic due to differences in the number and heterogeneity of road users.
- The social impact of aviation accidents with fatalities is many times greater than the impact of road accidents with fatalities.

This does not mean that new automation systems in aviation always work flawlessly, but it does mean that problems are detected earlier and that measures are taken if, despite all the precautions taken, problems do occur in practice. There are also major differences between civil aviation, where selected and trained professionals operate aircraft, and road traffic, where everyone must be able to drive a car, as a result of which certain measures cannot be adopted in road traffic. As a result, we have decided not to give this analysis a prominent place in the report. However, this exploratory analysis has taught us that safety should receive more attention in the design of the ADAS, that car drivers should be better informed about the ADAS present in their cars and that car manufacturers and governments should jointly ensure a well-functioning and transparent system to provide feedback on experiences in practice for the design of the new ADAS and the modification of the existing ADAS.

Content

Appendix A. Explanation of the investigation

Appendix B. Responses to the draft report

Appendix C. Accidents

Appendix D. ADAS

Appendix E. Legislation and regulations

## A.4 Forming a judgement: comparing findings to the reference framework

This investigation paid much attention to activities aimed at establishing the reference framework. This reference framework had to be adjusted to new and changing risks involving new technology such as ADAS (Chapter 2 gives a detailed description of the reference framework). The Dutch Safety Board's general reference framework, based on the SMS concept (see section A.4.1), provided a good basis but was insufficiently flexible. It was necessary to establish basic principles of compliance for the parties responsible for safety in order to be prepared for current and future technological developments. The data for the reference framework was obtained from a literature review and interviews. Team sessions were held to consider which principles should be included in the reference framework. The team examined the differences between the current situation and the desired situation (as described in the reference framework) together with the stakeholders. This produced an answer to the second main question.

### A.4.1 General principles for safety management

The Dutch Safety Board's general reference framework comprises five principles that parties should comply with in order to manage safety. These principles are based on national and international legislation and regulations and widely accepted and implemented standards. These principles are:

1. Insight into risks as a basis for a safety strategy
   The starting point for achieving the required safety level is:
   - a system analysis
   - an analysis of the relevant risks
2. Demonstrably effective and realistic safety strategy
   In order to prevent and manage undesirable events, a realistic and practical safety strategy must be established, including the associated basic principles. This safety strategy must be adopted and managed at the highest organizational level and is based on:
   - legislation and regulations
   - standards, guidelines, best practices and the organization's own insights, experiences and specific safety objectives
3. Implementing and ensuring compliance with the safety strategy
   The safety strategy is implemented, compliance is monitored and the identified risks are managed by:
   - a description of how the safety strategy is implemented, with attention to the concrete objectives and plans, including the resulting preventive and repressive measures
   - a transparent, unambiguous division of responsibilities that is known to all parties
     a clear description of the deployment of human resources and expertise required for the various tasks
   - clearly defined and active centralized coordination of all safety activities

4. Fine-tuning the safety strategy
   The safety strategy must be continuously fine-tuned based on:
   - The performance of risk analyses, observations, inspections and audits, periodically and in any case every time the basic principles are altered (proactive approach).
   - A system for monitoring and investigating incidents, near misses and accidents, and analysing these (reactive approach), which forms the basis for evaluations and any necessary adjustments to the safety strategy.
5. Supervision, commitment and communication
   The supervision of the involved parties/organizations must:
   - Ensure clear and realistic expectations within the organization with regard to the safety ambitions, and a climate of continuous safety improvement on the work floor by in any case setting a good example and making sufficient manpower and resources available for this purpose.
   - Communicate clearly to the outside world about the general working methods, the manner in which they are evaluated, procedures in the event of deviations etc., all on the basis of clear agreements with the stakeholders.

## A.5 Quality control

*SWOT analysis:* A Strengths, Weaknesses, Opportunities & Threats (SWOT) analysis was carried out to control the project quality risks. Specific measures were taken to neutralize threats and exploit opportunities on the basis of this analysis.

*Critical feedback sessions:* At three points during the investigation, employees of the Dutch Safety Board (non-team members) assessed the interim results with ‘fresh eyes’. The results of these critical feedback sessions were used to improve the quality of the investigation.

*Guidance committee:* The investigation was discussed with a guidance committee. See under ‘Guidance committee’ for concrete details.

*Inspection:* In accordance with the Dutch Safety Board Kingdom Act, a draft version of this report was submitted to the involved organizations and persons, whereby they were asked to inspect the report for errors, omissions and inaccuracies and provide comments where applicable.

*Analysis methods:* Various analysis methods were used to reduce the likelihood of incorrect or irrelevant conclusions being reached (as described above).

## A.6 Guidance committee

The Dutch Safety Board established a guidance committee for the purposes of this investigation. This committee comprises external members with expertise relevant to the investigation and is chaired by a member of the Dutch Safety Board. The external members sit on the guidance committee in a personal capacity. The committee convened on two occasions during the investigation to discuss the purpose and results of the investigation with the Board member and the project team. A written consultation round also took place to collect interim feedback. The committee acted in an advisory capacity during the investigation. The Dutch Safety Board has final responsibility for the report and the recommendations. The committee is composed as follows:

| | |
|---|---|
| Prof. M.B.A. van Asselt | Chair of the guidance committee, member of the Dutch Safety Board |
| Prof. M.H. Martens | Professor of ITS & Human Factors at the University of Twente from January 2014 to May 2019. She has held the chair in Automated Vehicles & Human Interaction at TU Eindhoven since June 2019 and is an expert in the field of human interaction with intelligent transport systems. With a background in behavioural sciences, she specializes in human responses to smart mobility solutions in cars and on roads. She is a member of the Scientific Advisory Board of the SWOV Institute for Road Safety Research. She has also worked for TNO in this field for more than 23 years. |
| J.G.Hakkenberg MSc | Director of the National Vehicle and Driving Licence Registration Authority (RDW) from September 1995 to 1 October 2014. He now runs his own consultancy and sits on the advisory boards of ORMIT (ORMIT matches trainees with organizations) and BridgeHead (BridgeHead matches the needs of the government with solutions from the market). He was CFO of the Ministry of Transport, Public Works and Water Management from 1989 to 1995. |
| Prof. M.J. van den Hoven | Professor of Ethics and Technology at TU Delft. Founder and scientific director of the 4TU Centre for Ethics and Technology (2007-2013). In 2009, he won the World Technology Award for ethics and the IFIP Prize for ICT and Society for his work on ethics and ICT. Founder and, until 2016, programme manager of the Dutch Research Council for Responsible Innovation. Member of TU Delft's Blockchain Lab. |
| Prof. A.W. Bronkhorst | Principal Scientist at TNO Defence and Safety. He leads a large long-term programme on early technological research in the field of defence and security. This ranges from biotechnology, robotics, computer science and nanotechnology to cognitive sciences. |
| M.C. Stikker | Internet pioneer and founder of De Digitale Stad ('The Digital City'). Director and founder of the Waag Technology & Society cultural research and development lab, an institute that initiates technological experiments. Member of the European Horizon 2020 committee 'High-level Expert Group for SRIA on Innovating Cities'/ DGResearch and of the AcTI Dutch Academy of Technology & Innovation. |
| R.J. Prins MSc | Internet pioneer and founder of De Digitale Stad ('The Digital City'). Director and founder of the Waag Technology & Society cultural research and development lab, an institute that initiates technological experiments. Member of the European Horizon 2020 committee 'High-level Expert Group for SRIA on Innovating Cities'/ DGResearch and of the AcTI Dutch Academy of Technology & Innovation. |

## A.7 Project organization

Prof. M.B.A. van Asselt acted as portfolio manager for this investigation on behalf of the Dutch Safety Board. The investigation was carried out by the project team, which comprised the following members:

| | |
|---|---|
| Dr. A. Umar | Investigation manager |
| Dr. E.M. Berends | Project leader |
| M.A. van den Hoek MSc | Investigator and data specialist |
| F. van Leusden-Tamsma MSc | Digital investigator |
| J.D. Romkes MSc | External investigator (cybersecurity specialist) |
| Dr. W.M.M. Heijnen | Senior investigator |
| E. Mol MSc | Research and development advisor |
| Dr. E.M. de Croon | Methodology advisor (CASCAD/STAMP) |
| M. Amelink MSc | External investigator |
| C. Dielen MSc | External investigator |
| D.C. Ipenburg LLM MA | Senior secretary |
| S. Sewnath | Project office assistant |
| J. Demir | Project office assistant |

# APPENDIX B

Content

Appendix A. Explanation of the investigation

Appendix B. Responses to the draft report

Appendix C. Accidents

Appendix D. ADAS

Appendix E. Legislation and regulations

## RESPONSES TO THE DRAFT REPORT

In accordance with the Dutch Safety Board Act, a draft version (without considerations and recommendations) of this report was submitted to the parties involved for review.

The following parties have been requested to check the report for any factual inaccuracies and ambiguities:

- Minister of Infrastructure and Water Management
- Netherlands Vehicle Authority (RDW)
- Tesla, Inc.
- Volvo Trucks
- DAF Trucks N.V.

The responses received can be divided into the following two categories:

- Corrections and factual inaccuracies, additional details and editorial comments that were taken over by the Dutch Safety Board (insofar as correct and relevant). The relevant passages were amended in the final report. These responses have not been included separately.
- Where the Safety Board has not adopted responses, the reason for this decision is explained. These responses and the explanation are set out in a table that can be found on the Dutch Safety Board's website (www.onderzoeksraad.nl).

# APPENDIX C

## ACCIDENTS

### C.1 Introduction

Accidents involving cars equipped with ADAS where the driver assistance system may have played a role have prompted the Board to launch a study into the automation of road traffic. The Dutch Safety Board investigated a number of accidents that occurred in the period 2016-2019 in order to ascertain whether and how advanced driver assistance systems play a role in traffic accidents. These accidents, and a number of accidents in the US which were extensively investigated by the National Transportation Safety Board (NTSB), are described in this appendix.

### C.2 Accidents in the Netherlands

In this section, we will present a number of accidents that occurred in the Netherlands in the period 2016-2019. An advanced driver assistance system (ADAS) was involved in each case. The accident investigations were largely based on information collected by accident analysts of the police. Note that the accidents are not representative of all accidents with ADAS.

| Accident | Omschrijving | Example in section |
|---|---|---|
| 1 | Truck collides into tail end of queue | 3.1 |
| 2 | Truck’s emergency brakes engaged | - |
| 3 | Collision with merging truck | 3.1 |
| 4 | Car with Autopilot crashes into slow-moving traffic | 3.2 |
| 5 | Car drives straight ahead across roundabout | 3.2 |
| 6 | Head-on collision between two cars | 3.3 |

*Table 5: Accidents.*

### C.2.1 Collision with Volvo truck at tail end of queue

On 27 March 2017, there was a rear-end collision on the A29 near Den Bommel (Goeree-Overflakkee). A Volvo truck built in 2016 crashed into the rear of a stationary truck with a low loader. The Volvo was equipped with an advanced emergency braking system (AEBS), which was made mandatory in 2015.[159] The AEBS was supposed to ensure that the Volvo braked in time, but this did not happen. An analysis of the tachograph data revealed that the truck collided into the rear of the stationary low loader while driving 83 km/h and without the brakes being applied.

**Automatic Emergency Braking System**

AEBS is designed to automatically brake the vehicle in the event of an imminent collision. The system's sensors continuously monitor whether there is sufficient distance to prevent a collision with the vehicle in front. When a critical limit is exceeded, the system provides an audio-visual warning based on progressive warning levels. If the driver does not respond immediately, the AEBS is engaged. The truck will then automatically apply maximum braking pressure to avoid a collision or limit the consequences.

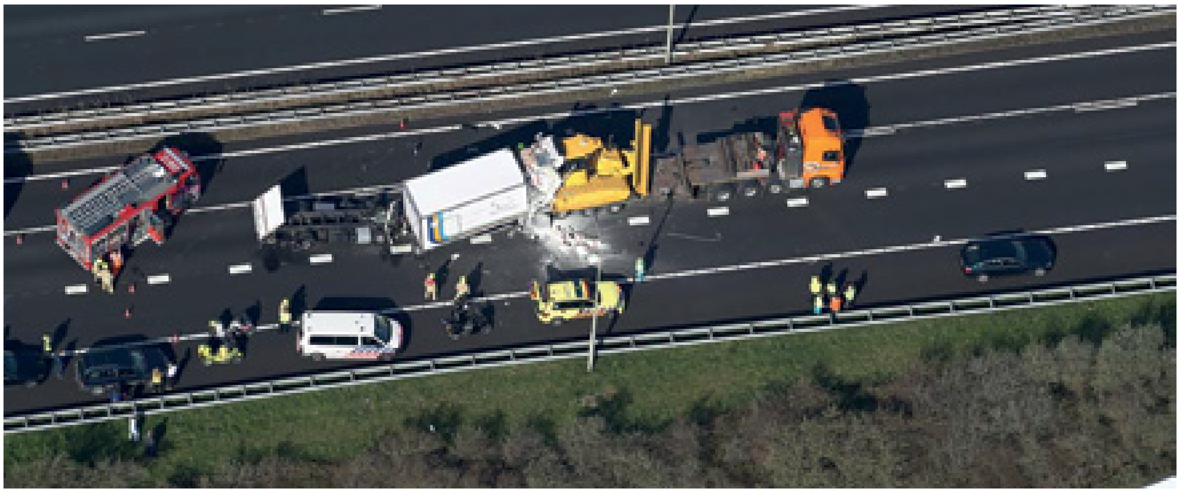


*Figure 17: Aerial view of the accident on the A29. The Volvo truck (white) collided with a low loader carrying a bulldozer. (Source: police)*

The driver of the Volvo truck was killed in the accident and the damage was enormous. It is clear from the aerial view in Figure 17 that the Volvo truck (white) drove into the rear of the stationary low loader carrying a bulldozer. The truck's cabin hit the low loader first. As a result of the impact, the freight container came off the chassis and collided with the cabin from behind. The truck's cabin was crushed between the container and the bulldozer on the stationary low loader.

[159] Commission Regulation (EU) No 347/2012 of 16 April 2012 implementing Regulation (EC) No 661/2009 of the European Parliament and of the Council with respect to type-approval requirements for certain categories of motor vehicles with regard to advanced emergency braking systems. This requirement only applies to trucks produced after the effective date of the Regulation.

The police examination of the tachograph data revealed that the truck was driving at a constant speed of 83 km/h during a period of 7 minutes and 12 seconds prior to the accident (see Figure 18). The Volvo slowed down from 83 km/h to 7 km/h in a timeframe of 0.50 seconds. The Volvo driver did not apply the brakes and crashed into the back of a stationary low loader at full speed during daylight and with sufficient visibility. The Dutch Safety Board was not able to determine why the driver did not brake.

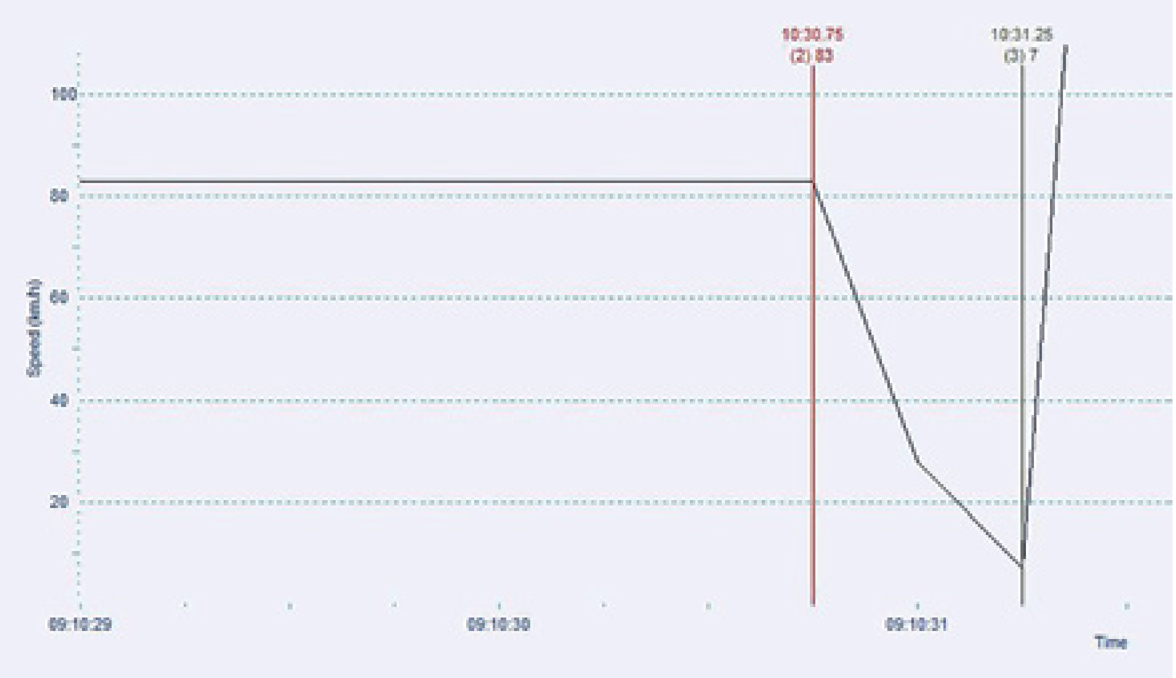


*Figure 18: Speed recording from the truck's tachograph. (Source: police accident report)*

The AEB system was examined to determine why it did not engage the emergency brake, which it should have done if switched on and in proper working order. It is possible that the driver switched off the AEBS (a system which is required by law). The Dutch Safety Board was unable to determine whether the AEBS was switched on because, in this model of truck, the data is only stored if the engine is switched off in the normal manner. In the event of a sudden power failure, as in the case of this accident, the system will not be able to transfer the data to the permanent memory in time.

Volvo's engineers have stated, based on the available knowledge of the operation of the camera system, that the camera system is unlikely to have recognized this low loader with load. Volvo obtained this camera system from a supplier and is only familiar with the general principle behind the system for recognizing vehicles in front of the truck. For example, the current generation of camera systems detects vehicles by monitoring the position of the vehicle's axle and wheels and taking into account its contours. Non-standard contours (such as a low loader with bulldozer or a traffic warning trailer) will not always be detected.

Content

Appendix A.
Explanation of
the investigation

Appendix B.
Responses to the
draft report

Appendix C.
Accidents

Appendix D.
ADAS

Appendix E.
Legislation and
regulations

**Object location determination with AEBS**
Every vehicle equipped with an AEB system is also equipped with a camera and radar module. By means of sensor fusion (a technique used by computers to combine information from multiple sensors) the computer can determine the distance from the vehicle to the object. The radar module helps the system to determine the direction of the object, while the camera module can accurately determine the distance between the vehicle and the object. Figure 19 provides a schematic representation of how the two modules jointly determine the location of an object. Once located, if the object is within a predefined distance (and depending on the speed of the vehicle), an emergency brake is engaged.

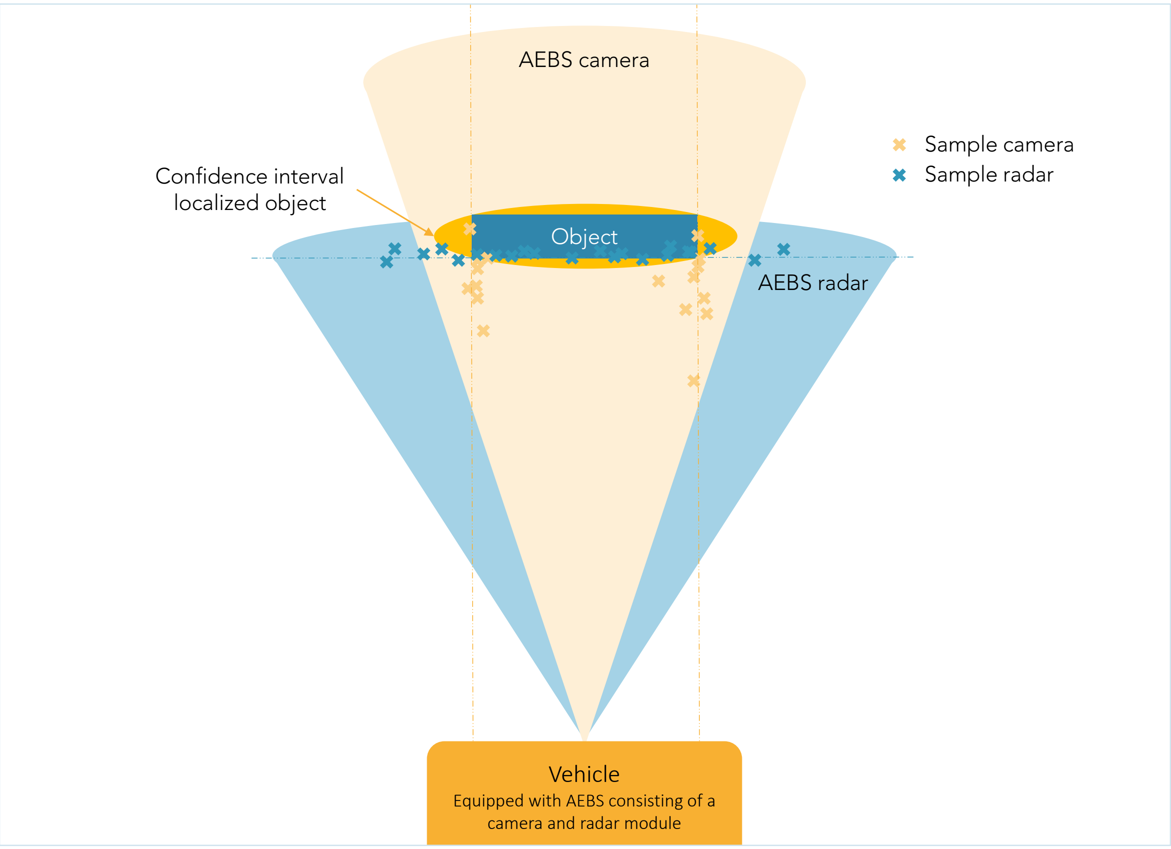

AEBS camera
Confidence interval localized object
Sample camera
Sample radar
Object
AEBS radar
Vehicle
Equipped with AEBS consisting of a camera and radar module

*Figure 19: Detection of an object in the direction of travel of a vehicle equipped with AEBS by means of the camera and radar module.*

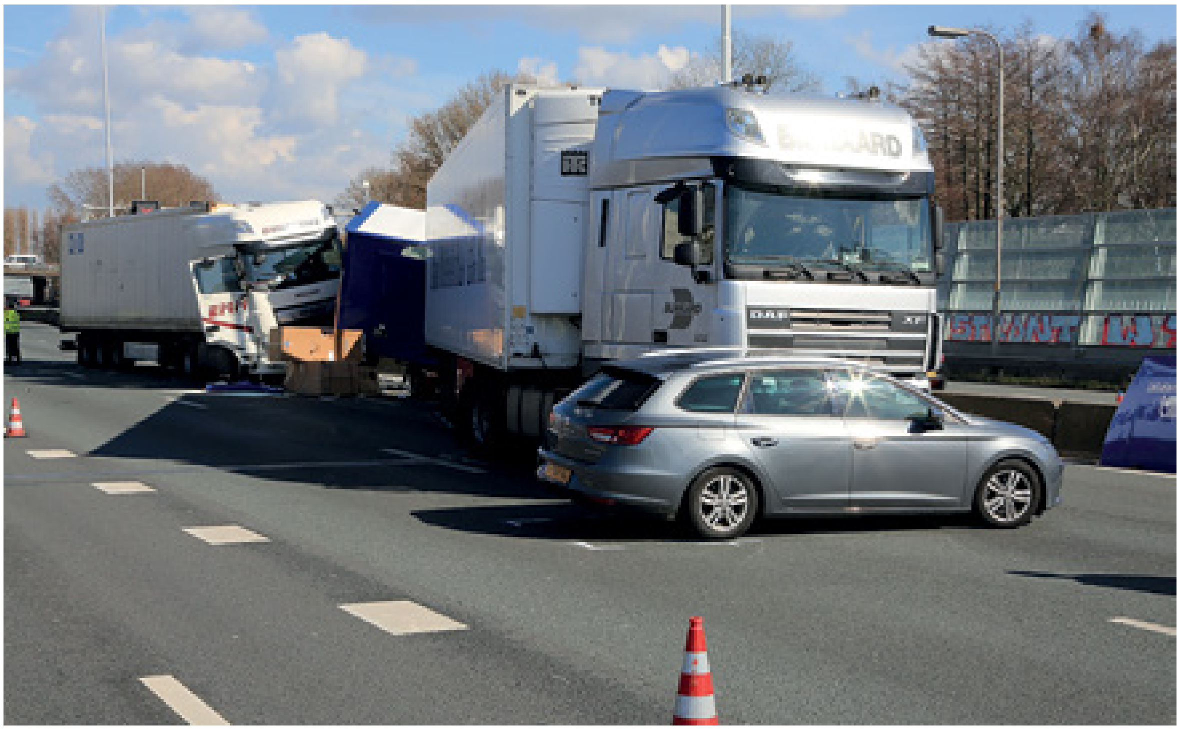
### C.2.2 Truck's emergency brakes engaged

On 29 March 2018, there was a rear-end collision involving two trucks, a delivery van, and a car. The rearmost tractor-semitrailer truck was a DAF XF produced in 2018. This vehicle was equipped with an advanced emergency braking system (AEBS) as required by the regulations for vehicles with a gross mass exceeding 3.5 tonnes.

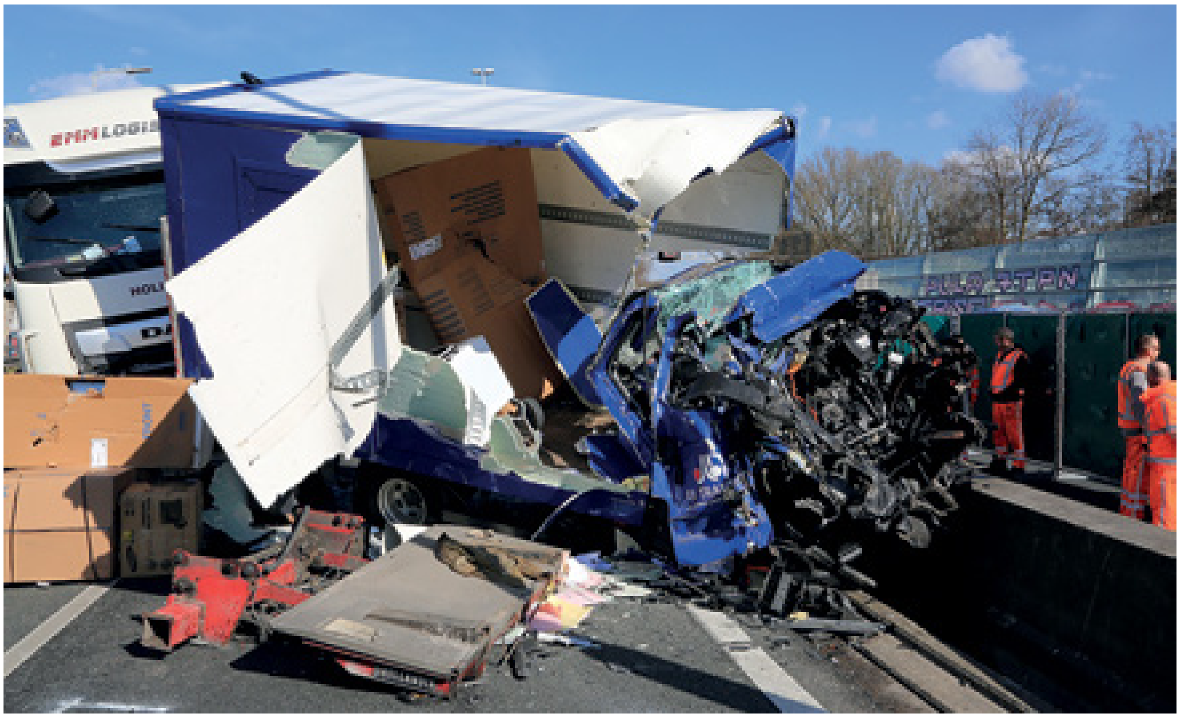
Following a collision between a car and a truck (see Figure 20 a), whereby these two vehicles had both come to a standstill in lane 2, a blue van and the aforementioned DAF truck collided into the rear of this stationary combination (see Figure 20 b). In his statement, the driver of the truck said that the van merged in front of him shortly before the accident and that the DAF responded by applying the emergency brake.

Despite the heavy damage to the other vehicles, the DAF at the rear of the collision remained reasonably intact. Two occupants of the other vehicles were rushed to hospital.

The police confiscated and analysed the digital tachograph data. However, this data did not reveal whether it was the driver or the AEB system that applied the brakes. The radar module was examined by the manufacturer and/or supplier, who reported that the AEB system was engaged at 12:12:27. At the time, the truck was travelling at a speed of 76 km/h. After the AEB system was engaged, the driver of the truck applied the brake pedal. Although the truck was too close to be able to come to a full stop (in combination with the speed of the vehicle), activation of the emergency braking system may have prevented more severe consequences.



*(a) The foremost truck (also a DAF, colour silver) collided with the car (Seat, colour silver).*



*(b) The van (blue) then collided with the stationary truck and was crushed by the truck behind it (DAF, colour white).*

*Figure 20: Two DAF trucks, a car and a van were involved in a rear-end collision. The DAF truck with the white cabin was equipped with an AEB system. (Source: police)*

### C.2.3 Car collides with merging truck

On 11 April 2017, a Tesla Model S on the A1 near Bathmen (a two-lane motorway) crashed into the rear of a truck. The Tesla was driving in the left lane at high speed and the Autopilot[160] function was engaged. The truck was in the right lane. Shortly before the collision, the truck changed lanes to make room for another truck that was merging. Both the Tesla's Autopilot and the driver failed to apply the brakes. However, the vehicle apparently did throttle back shortly before the impact, such that the Tesla slid under the trailer at a somewhat reduced speed and was dragged along for a few hundred metres. No one was injured in this accident.

[160] For more information on the functionalities of the Autopilot, see https://www.tesla.com/nl_NL/autopilot. Generally speaking, the Autopilot is considered to be active if both Autosteer and TACC are engaged, and this is the definition used in this appendix.

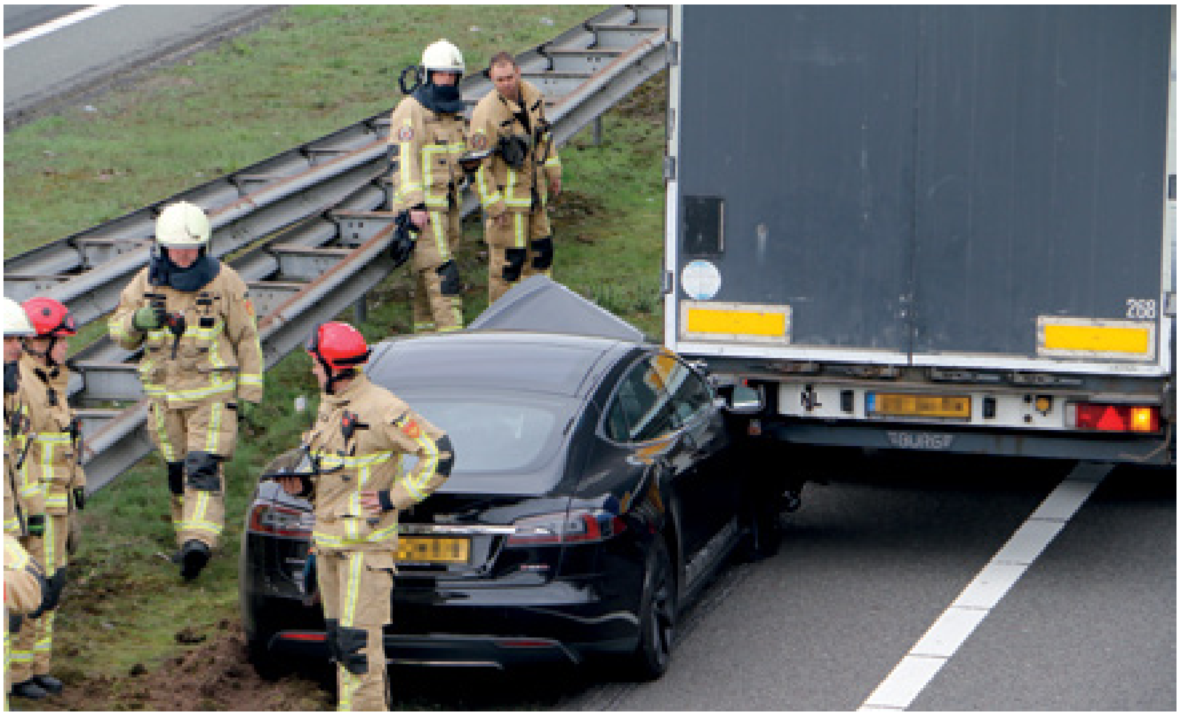


*Figure 21: A Tesla Model S drove into a truck changing lanes at a speed of approximately 127 km/h without braking. (Source: Hof van Twente fotografie)*

Figure 22 a to f display a time lapse recording of a number of parameters from the Tesla log files. Figure 22 a and b reveal that the vehicle was travelling at a speed of approximately 150 km/h just before the accident occurred (07:43:00) and that the Autopilot function was engaged (TACCC[161] and Autosteer[162]; the reported state was 'Active Nominal'). The cruise speed had been set to 145 km/h for some time and was increased to 150 km/h by the driver just before the accident (07:43:17) (Figure 22 f).

The Tesla crashed into the truck at 07:43:43, shortly after the truck had merged into the left lane in front of the Tesla. The Autopilot system remained engaged up until the moment of impact. The Tesla's speed had reduced somewhat to approximately 130 km/h. According to Tesla, this was because the TACC system throttled back and applied initial braking because it had detected a vehicle in front of it. The Tesla slid under the truck at a speed of 127 km/h. The driver immediately applied the brakes (see Figure 22 d), which disengaged the Autopilot system. The Tesla slid under the truck, became stuck, and was dragged along for a few hundred meters. Both vehicles came to a standstill at 07:44:00.

At the time of the collision, the Autopilot system reported 'hands required and detected', i.e. the driver appears to have had his hands on the wheel. The settings on the Tesla display indicate that the FCW and AEB system were probably both engaged. However, AEBS was only enabled for high speeds of 50-90 miles/hour (80-145 km/h) in a later software version (2.5) and so it appears the vehicle-specific AEBS was not operational at the time of the impact (with a speed of 127 km/h).

[161] Tesla's term for their own version of adaptive cruise control.
[162] Autosteer is an active form of lane keeping assistance and controls the position of the car on the road.

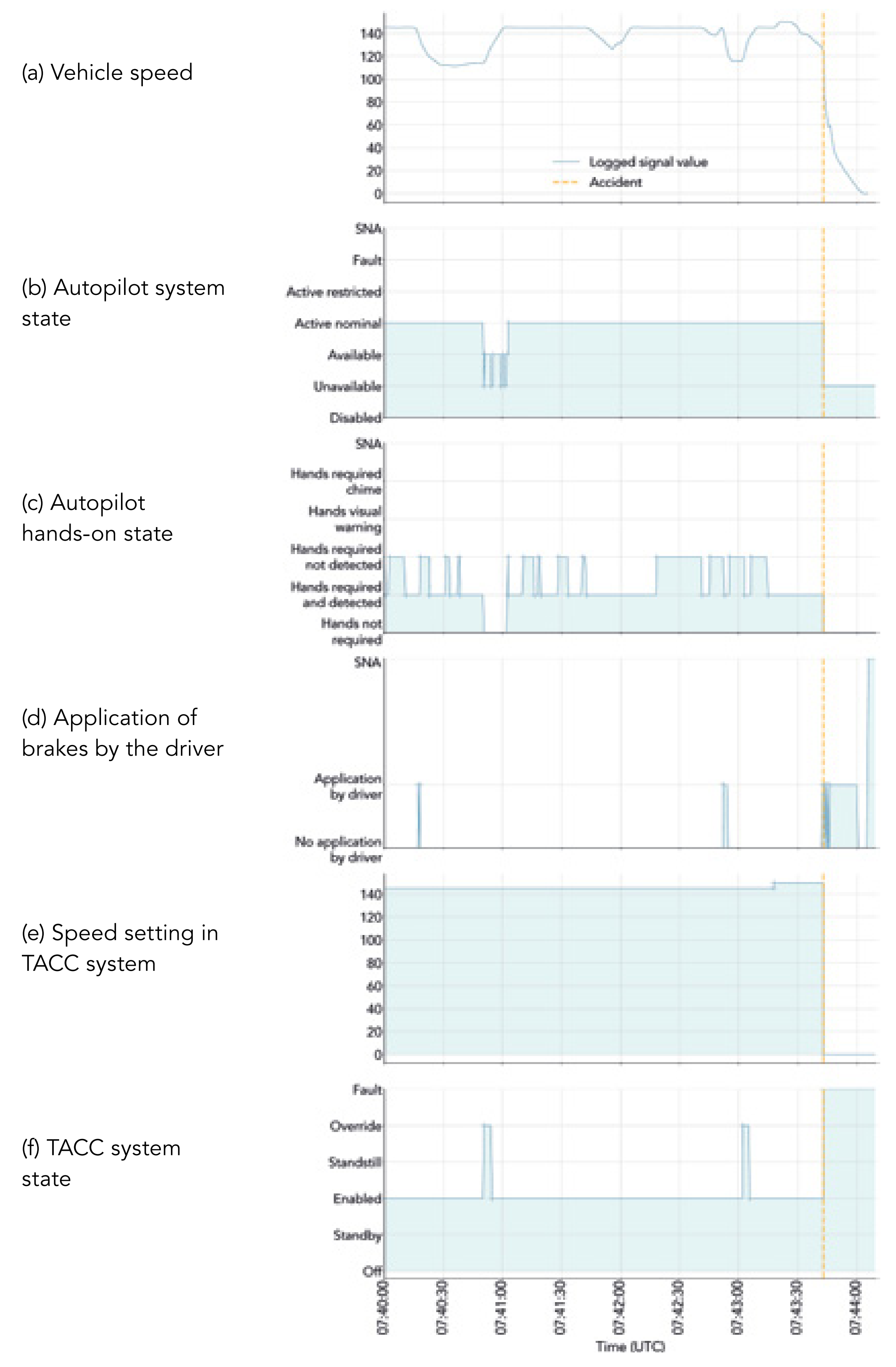
ACC systems have difficulty anticipating lane changes. According to Tesla, the TACC system did detect the vehicle in front and applied initial braking. It is unclear why the car did not try to brake more substantially. Both the initial deceleration by Autopilot and the activation of the emergency warning and braking system functioned as designed.

The data structure of the Tesla in question differs from the data structure of previously examined Tesla vehicles. A number of parameters are not included in the log files or have different locations (e.g. distance to vehicle in front, speed of vehicle in front, accelerator pedal log). As already mentioned, it is possible to change the way data is stored by performing an over-the-air software update.

Software updates make it easy to change the settings that control the system. For example, in software version 2.0, the speed limit of the TACC was changed and in 2.5 an emergency brake function was added that functions at speeds above 80 km/h (to a maximum of 145 km/h)[163, 164]. These software updates – and hence also additions or changes in functionality – occur when the vehicle is stationary for a longer period of time. In a Tesla, the driver has the choice to decide when and where to install updates. After the installation, the driver receives an overview on the dashboard screen that describes any changes to system regarding functionality or capabilities. It is also possible for the driver to receive a notification on the mobile phone, so that the driver knows when an update has taken place

[163] Electrek.co, *Tesla increases Autopilot 2.0 speed limits with latest update*, https://electrek.co/2017/03/08/tesla-autopilot-2-0-speed-limit-update/, accessed on 21 May, 2018.

[164] Electrek.co, *Tesla releases new update to enable full speed automatic emergency braking for Autopilot 2.5 and more*, https://electrek.co/2017/10/22/tesla-update-full-speed-automatic-emergency-braking-autopilot-2-5/, accessed on 7 August, 2018.



(a) Vehicle speed

(b) Autopilot system state

(c) Autopilot hands-on state

(d) Application of brakes by the driver

(e) Speed setting in TACC system

(f) TACC system state

*Figure 22: Time lapse recording of a number of parameters from the vehicle log files (Tesla Model S, Bathmen).*

### C.2.4 Car with crashes into slow-moving traffic

On 25 August 2016, there was a multiple collision on the A4 near Leiden involving six cars. Five of the cars involved were in a stationary queue. A Tesla Model S collided into these five cars from behind. The Tesla was equipped with the Autopilot system. The system was active at the time of the incident.

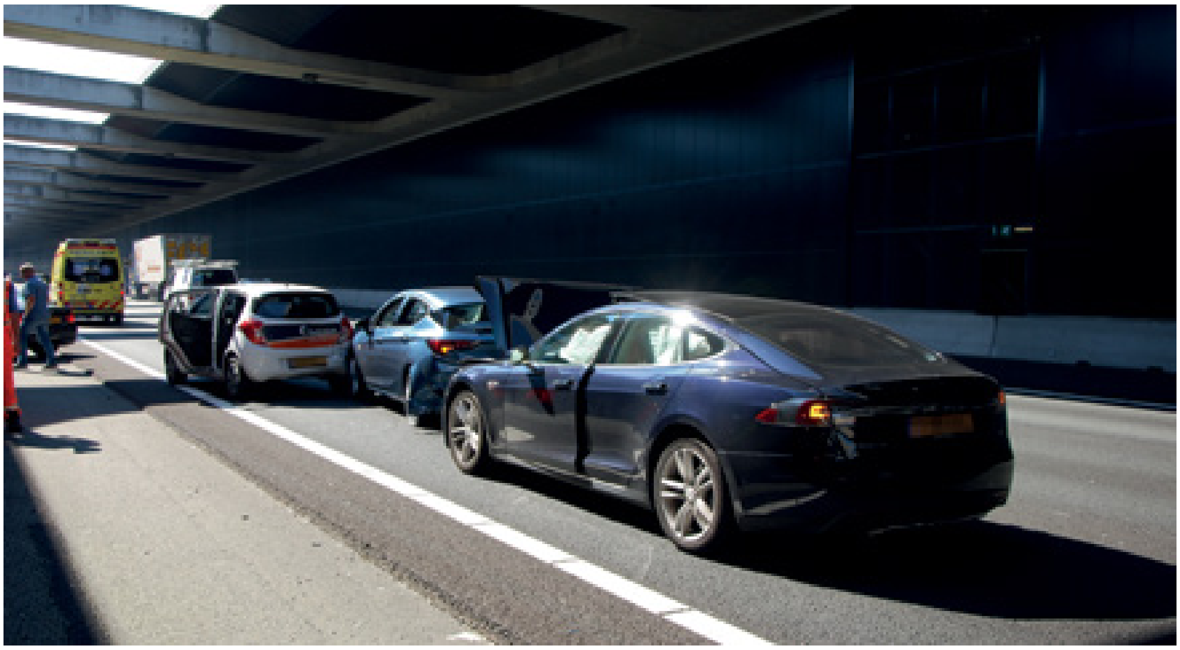


*Figure 23: The Tesla Model S collided with the vehicle in front at a speed of 58 km/h. (Source: 112regioleiden.nl)*

The collision between the Tesla and the vehicle in front set off rear-end collisions between the other five cars. None of those involved were injured.

The matrix signs indicated a speed of 50 km/h and it was clear that traffic was slow-moving. The driver had noted that the system had correctly decelerated to a lower speed several times that afternoon. Analyses of the Autopilot system and the TACC system conducted by Tesla (Figure 24 b and g) revealed that, during the 20 minutes prior to the collision, the TACC had been adjusting the speed of the car to the traffic conditions, and that approximately 5 minutes prior to the collision the driver was given an audio-visual warning of a possible collision with another vehicle in front by the Forward Collision Warning system (FCW system[165]). The driver immediately applied the brakes (see Figure 24 d; 13:12:09), which disengaged the Autopilot system. After this he reengaged the Autopilot. The driver further entrusted the driving to the Tesla's Autopilot function. The Autopilot was engaged and the TACC speed was set to 130 km/h with the shortest distance headway. The driver's confidence in the Autopilot was strengthened by the fact that the FCW system had warned him again shortly before the accident.

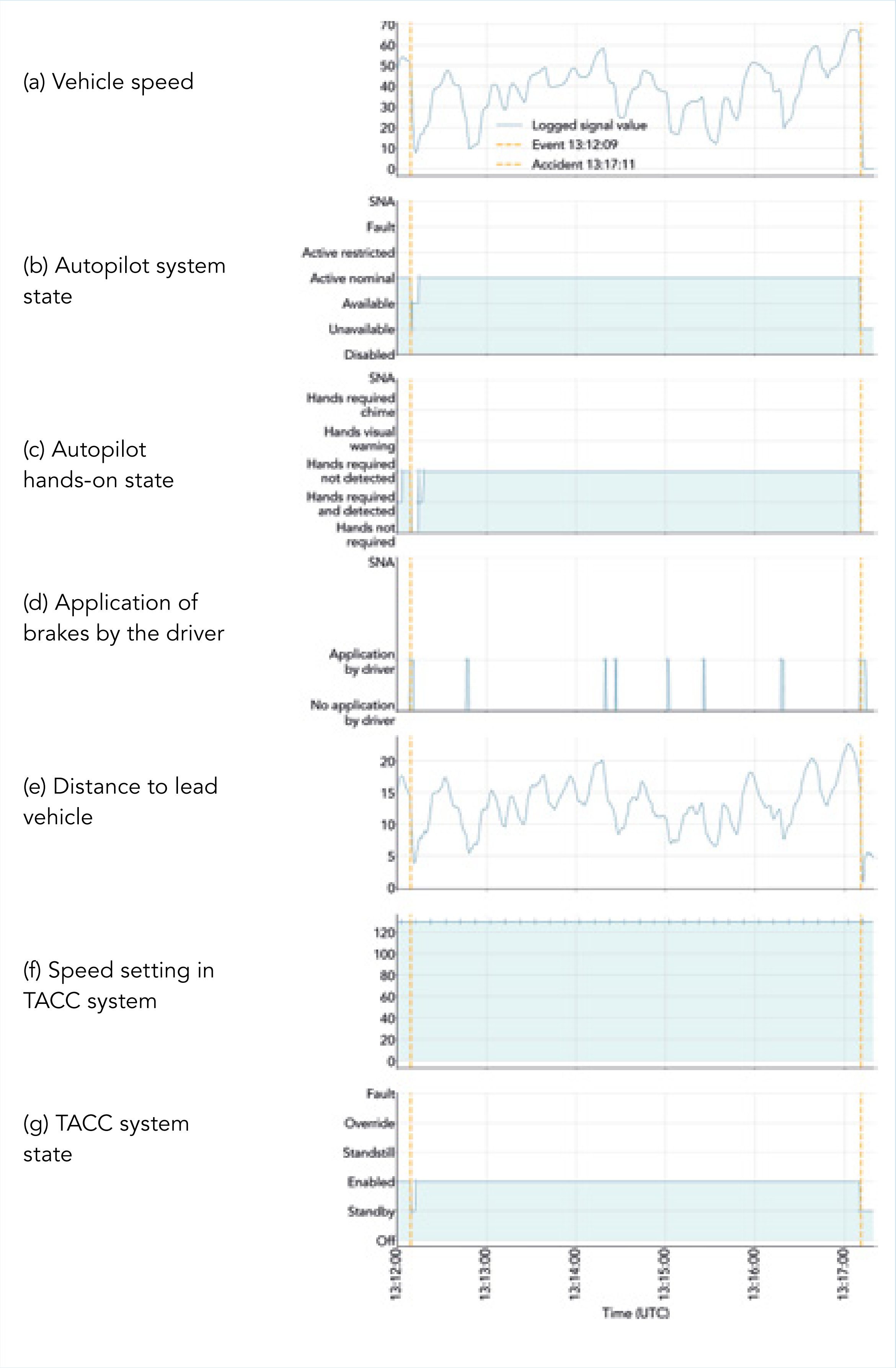
[165] Alle Tesla's zijn uitgerust met een Forward Collision Warning systeem. Dit systeem staat los van het Autopilot systeem en waarschuwt de bestuurder – zowel auditief als visueel – in het geval van een naderende botsing. Er zijn verschillende waarschuwingsniveaus (bijvoorbeeld eerst een visuele waarschuwing, daarna een geluidswaarschuwing). Het FCW heeft alleen de mogelijkheid om te waarschuwen en kan niet het remsysteem aansturen.

The parameters in the vehicle's log files (Figure 24) reveal that the vehicle was travelling at a speed of approximately 67 km/h just before the moment of impact (13:17:07). The driver of the Tesla started braking between 0.5 and 1.5 seconds before reaching the rear of the queue (13:17:10), at a distance of about 18 metres from the vehicle in front. This was insufficient to bring the vehicle to a standstill in time. The Tesla collided with the vehicle in front while travelling approximately 58 km/h. The driver applied his brakes between 0.5 and 1.5 seconds after the vehicle in front started braking. Taking only the braking distance of the vehicle in front into account, this indicates that the driver responded adequately quickly. However, drivers need to anticipate much further ahead than only the vehicle in front of them. The investigation shows that it is conceivable that the driver was not aware of the traffic situation further ahead because of the low mental workload, or because he was distracted as a result.

Figure 24 b shows that, at the time of the event, the Autopilot state was 'Active Nominal'. In this mode, the Autopilot deploys both Autosteer and TACC. This is confirmed by the state of the speed control system, which was 'enabled' and was set to a speed of 130 km/h (see Figure 24 f and g). Furthermore, the hands-on state parameter reveals that the system did not detect any hands on the steering wheel for a period of approximately 5 minutes, during which time Autopilot was engaged (see Figure 24 b and c). No FCW warning was provided.

Although the Autopilot system was engaged, the system did not take any action to maintain the car's distance from the vehicle in front. The driver of the Tesla applied the brake pedal approximately one second before the impact with the vehicle in front. Just before this, the vehicle applied regenerative braking; this entails a slight application of the brakes to charge the battery with kinetic energy and is unrelated to emergency braking.

The hands-on state parameter revealed that the system did not detect any hands on the steering wheel for a period of approximately 5 minutes, during which time Autopilot was engaged. No warning was provided.



(a) Vehicle speed

(b) Autopilot system state

(c) Autopilot hands-on state

(d) Application of brakes by the driver

(e) Distance to lead vehicle

(f) Speed setting in TACC system

(g) TACC system state

*Figure 24: Time lapse recording of a number of parameters from the vehicle log files (Tesla Model S, Leiden).*

Content

Appendix A. Explanation of the investigation

Appendix B. Responses to the draft report

Appendix C. Accidents

Appendix D. ADAS

Appendix E. Legislation and regulations

The data is logged in a manner that is proprietary to the car manufacturer; only the manufacturer has access to the exact key required to decipher the data. A small proportion of the parameters were deciphered due to the efforts of various bodies. However, the key could well be changed in a new software update[166]. The amount of work involved in deciphering the data structure and the variety of ways the data is logged make easy interpretation of the data impossible for third parties.

### C.2.5 Car drives straight ahead across roundabout

In the early afternoon of 1 July 2016, a Tesla Model S drove at high speed straight over the central island of a roundabout on the N57. The Tesla collided with a pole on the other side of the roundabout and came to a standstill. The driver suffered heavy injuries in the accident. At the time of the accident, there was little traffic; there were no vehicles directly in front of the Tesla.

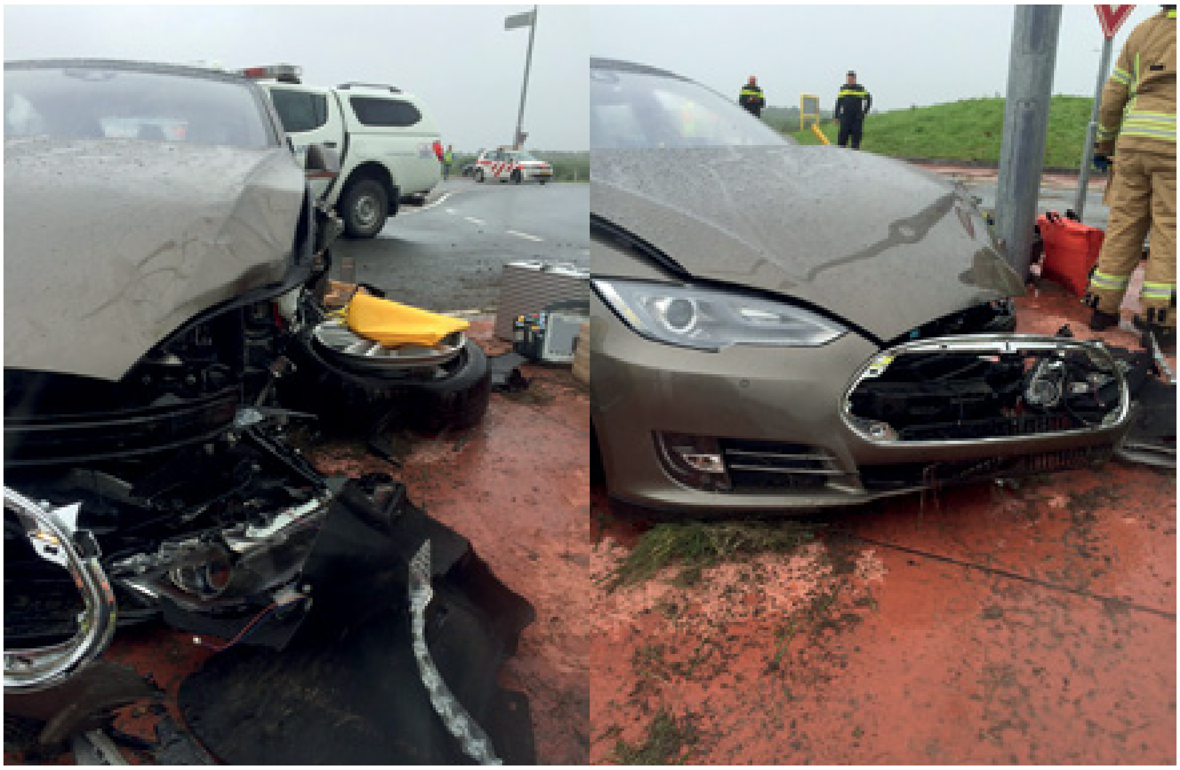


*Figure 25: The Tesla Model S after it collided with the pole on the other side of the roundabout (Source: Twitter, posted by Rijkswaterstaat road inspector Jeroen).*

A time lapse recording of a number of parameters from the vehicle log files is displayed in Figure 26. This information revealed that the vehicle had approached the roundabout at a constant speed of approximately 84 km/h. The vehicle had been driving at this speed for a period of approximately 3 minutes. At 12:12:03, the speed decreased to 10 km/h in roughly 3 seconds, and another 3 seconds later the vehicle came to a standstill.

[166] Tesla automobiles regularly receive over-the-air software updates (via the mobile network).

The Autopilot system reported the state as 'Active Nominal', which means the Autopilot was active prior to the accident. Figure 26 e and f reveal that the TACC state was normal and the cruise speed was set to 85 km/h. Figure 26 c also reveals that the Autopilot system was engaged; the driver had not applied the accelerator pedal during a period of approximately 3 minutes prior to the accident. The brake pedal (Figure 26 d) was not applied during this period either. The driver did attempt to stop the vehicle upon driving onto the central island of the roundabout, before the vehicle came to a standstill.

The FCW did not warn of the approaching roundabout, and nor did the emergency braking system intervene. In addition, the driver declared that he did not receive any warning from the FCW. Autosteer can be engaged even on roads for which it is not actually designed.

The driver has stated that he has taken most of the information about the functioning of Autopilot from the manual. He also received a brief explanation of the systems in the vehicle when he started using the car.

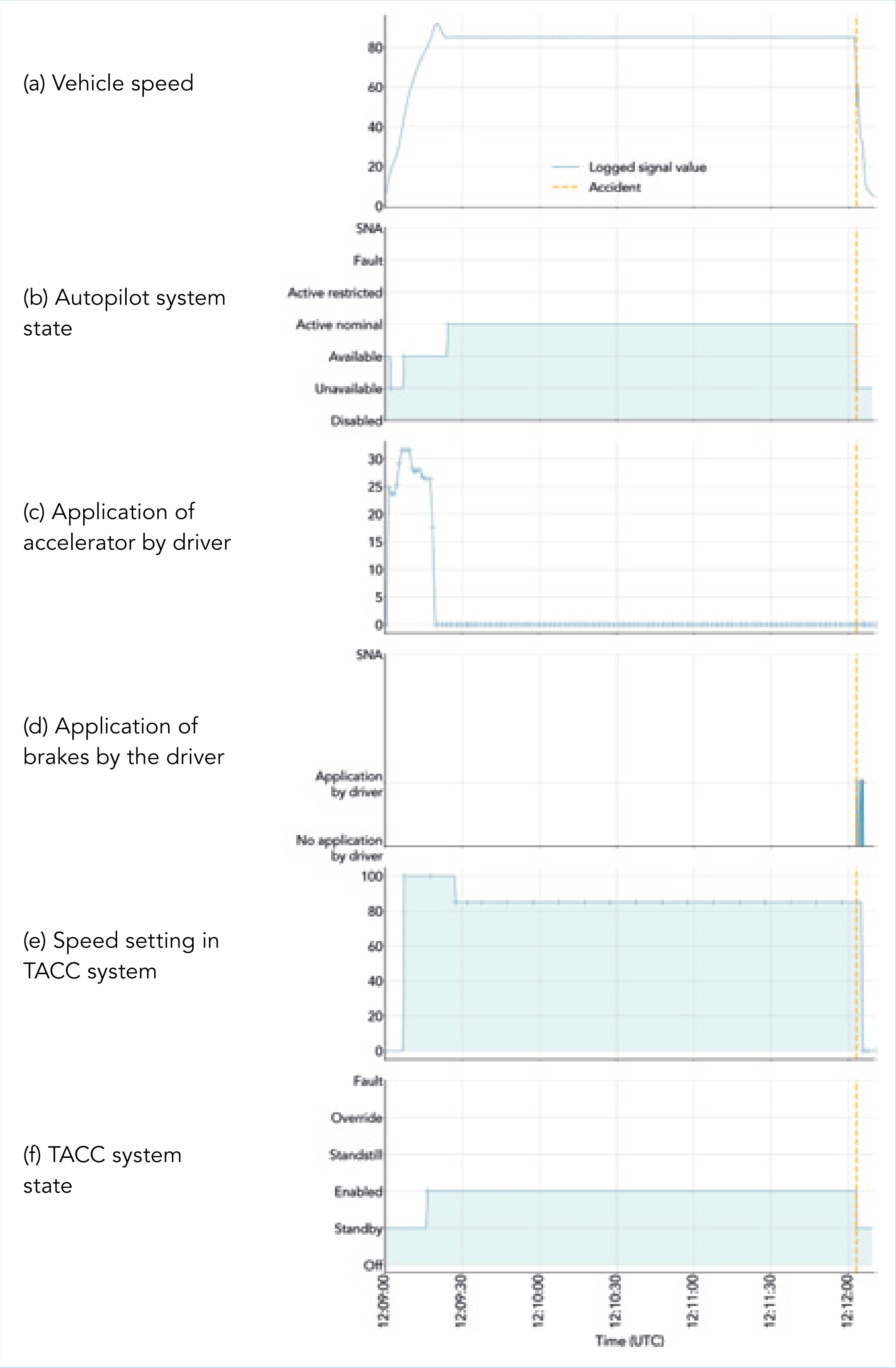


*Figure 26: Time lapse recording of a number of parameters from the vehicle log files (Tesla Model S, Ouddorp).*

Content

Appendix A. Explanation of the investigation

Appendix B. Responses to the draft report

Appendix C. Accidents

Appendix D. ADAS

Appendix E. Legislation and regulations

### C.2.6 Head-on collision between two cars

On 30 January 2019, a Tesla Model S was driving on the N277, a provincial road near Zeeland (Noord-Brabant). The vehicle was equipped with Autopilot and an emergency braking system.

To engage the Autopilot, the driver must successively engage Traffic Awareness Cruise Control (TACC) and Autosteer. This is done by means of a shift lever on the left rear of the steering wheel. Autosteer only functions on roads with clear road marking that can be detected by the system. If Autosteer is available, a grey icon is displayed on the dashboard. After activation by means of the shift lever, a blue icon is displayed next to the vehicle speed (see Figure 27).

**Activating Tesla's Autopilot**

The Tesla's Autopilot is engaged by means of a shift lever on the left rear of the steering wheel. Autopilot comprises a combination of TACC and Autosteer. TACC can be engaged in two ways. The current speed can be set and maintained by moving the cruise control lever up or down. By pulling the lever towards the driver, the speed limit or current speed of the vehicle is maintained. TACC can only be switched on when the system is available, as shown by the grey speedometer icon on the instrument panel.

If Autosteer is available, a grey Autosteer icon will appear on the display, and it can be engaged by pulling the lever towards the driver again. This must be done shortly after activating TACC. After activating Autosteer, the driver receives an audio signal and the Autosteer icon will turn blue. Moving the lever up or down adjusts the pre-set TACC speed incrementally but will not disengage Autosteer.

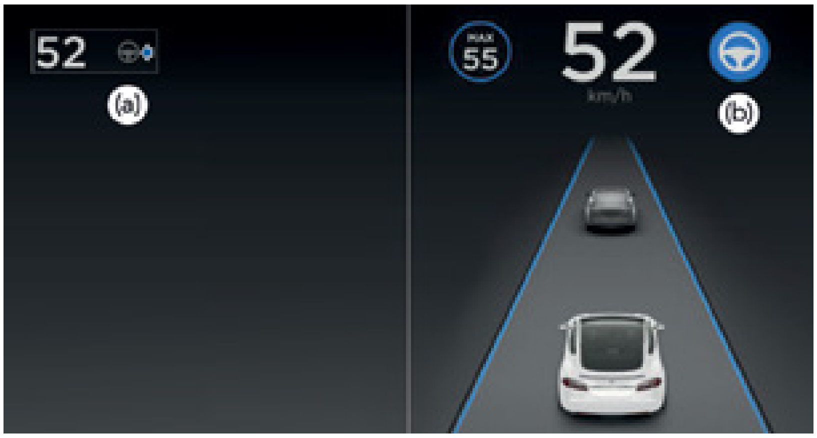


*Figure 27: (a) If Autopilot is available, a grey Autosteer icon is displayed on the instrument panel. (b) The icon turns blue when Autosteer is engaged. (Source: Tesla Model S user manual[167])*

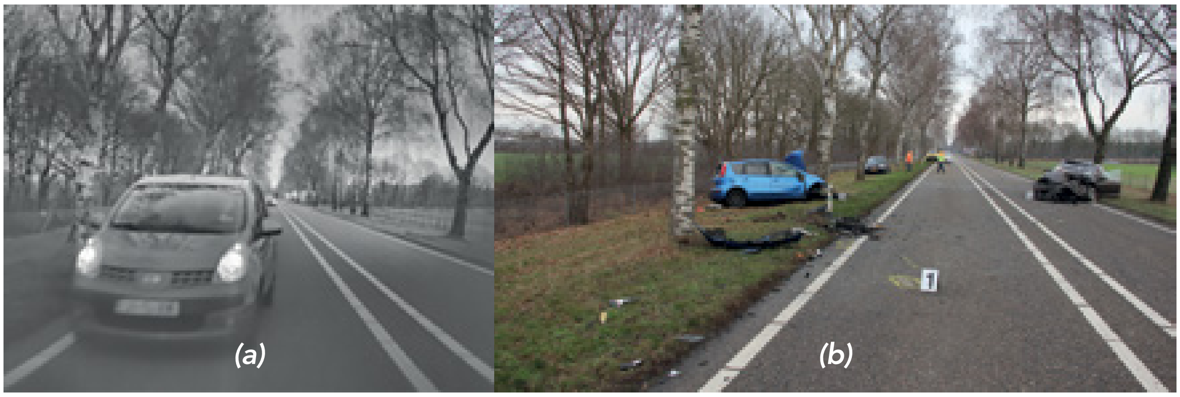


*Figure 28: (a) Photograph taken by the camera in the Tesla just before the collision. (b) The remains of both vehicles after the collision (Source: police).*

Data from the vehicle (see Figure 29 a to f) revealed that the vehicle was travelling at a speed of approximately 83 km/h with TACC engaged. Autosteer was not engaged. Approximately 23 seconds before the impact, the driver pressed the shift lever of the Autopilot system up twice in quick succession. The first time the shift lever was pressed up it adjusted the TACC pre-set speed to the current speed. The second time, the pre-set speed was increased to 85 km/h. Autosteer was not engaged. The driver stated that he thought that he had engaged the Autopilot, and hence also TACC and Autosteer. Engaging TACC and increasing the speed (pressing the shift lever up twice) is a very similar procedure to engaging TACC and Autosteer (pulling the shift lever towards the driver twice). The driver may have thought that he had engaged Autosteer.

[167] Tesla, *Tesla Model S user manual*, 2018.

When the driver briefly turned his attention to the screen in the centre console, he noticed that the vehicle had moved to the adjacent lane and was approaching an oncoming vehicle. The Tesla collided into the oncoming Nissan. The data reveals that the driver did not have his hands on the wheel for a period of about 9 seconds, and the system did not provide a warning because Autosteer was not engaged[168]. The driver of the Nissan was killed in the collision; the driver of the Tesla was uninjured. The AEBS was never engaged, nor was an FCW warning provided. The current generation of these systems is not designed to detect impending collisions with oncoming vehicles.

[168] If Autopilot had been engaged, at a speed of 83 km/h, the system would have performed a hands-on detection every 40 seconds. Variables that trigger an immediate warning include: no valid lane marking detected, abnormal lane marking, possible imminent collision with an object in the direction of travel.

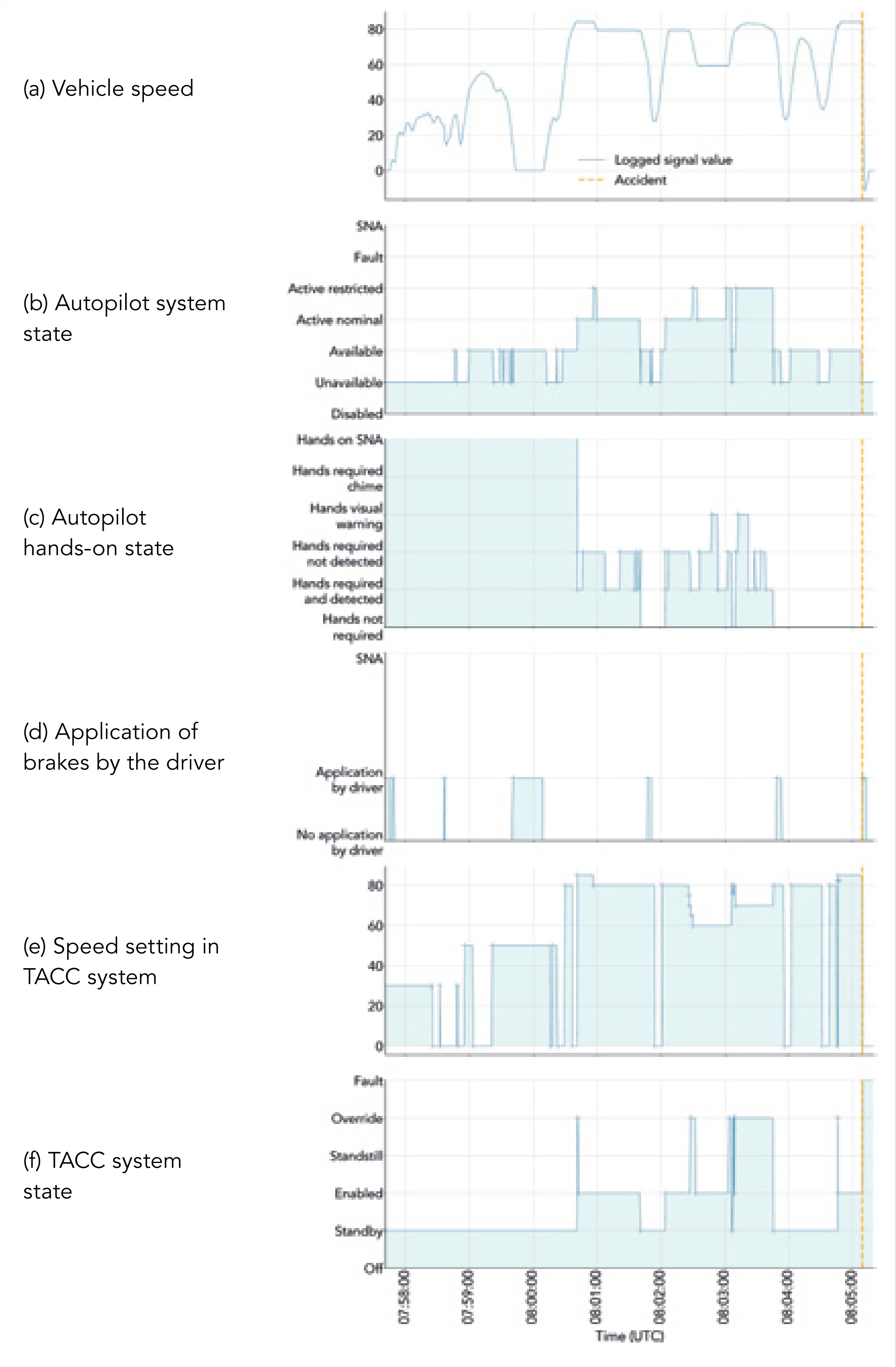


*Figure 29: Time lapse recording of a number of parameters from the vehicle log files (Tesla Model S, Zeeland).*

Content

Appendix A. Explanation of the investigation

Appendix B. Responses to the draft report

Appendix C. Accidents

Appendix D. ADAS

Appendix E. Legislation and regulations

### C.2.7 Accidents involving a car that were not related to ADAS

The Dutch Safety Board investigated several accidents involving cars. However, ADAS did not play a role in a large number of these accidents because this system was not engaged. An overview of these accidents is provided below.

| | |
|---|---|
| 15 March 2015 | Residential area in Wormerveer<br>The driver was about to leave a parking space when the Tesla suddenly shot forward, collided into some poles and hit a cyclist. The driver had the impression that the Tesla was out of control. An investigation revealed that the driver had been applying the accelerator pedal the whole time, i.e. this accident concerned a driver error. It should be noted, however, that a Tesla has much more power than an average petrol or diesel car. |
| 7 September 2016 | Provincial road in Baarn<br>Tesla has frontal collision with tree at high speed. The driver is killed instantly. Part of the battery pack came loose and eventually spontaneously combusted. The driver could only be recovered from the vehicle by the fire brigade after several hours. According to Tesla, the collision speed was approx. 155 km/h and so the Autopilot could not have been engaged[169]. |
| 20 July 2017 | A35 near Hengelo<br>Tesla X collides into rear of queue. The vehicle collided into the rear-end of a Mercedes while travelling at about 130 km/h and without applying the brakes. The Mercedes was slammed into the rear of a Volvo, which was also pushed forward into the rear of a Volkswagen. Autopilot was not engaged. The possible role of human machine interaction in this accident (e.g. the driver thought that the systems were engaged and entrusted the vehicle to them) was not further investigated. |
| 27 February 2019 | Provincial road near Vogelenzang<br>A Jaguar I-Pace, equipped with adaptive cruise control, lane keeping assist and an emergency braking system, collided with a BMW that was heading south and wanted to turn off the road to enter a driveway. EDR data showed that the Jaguar was travelling at an average speed of 120 km/h, a serious violation of the current speed limit (50 km/h). Such speeds are outside of the operational domain of the emergency braking system. Vehicle detection works with this version of the emergency braking system up to 80 km/h. Moreover, it is not possible to detect oncoming traffic with this version. |

[169] The Autopilot speed limit was only increased to 145 km/h in a later software version.

## C.3 Accidents in the USA

### C.3.1 Tesla collides into turning truck, Florida, USA

On 7 May 2016, a Tesla S collided with the side of the semi-trailer of a tractor-semitrailer truck. This accident was extensively investigated by the NTSB[170].

The Tesla was driving on US Highway 27A at 120 km/h, while the truck coming from the opposite direction was turning left into an unpaved side street. The Tesla hit the right side of the semitrailer, slid under it, and then came off the road. The roof of the car was ripped off during the collision with the undercarriage of the semitrailer. The driver of the Tesla was killed.

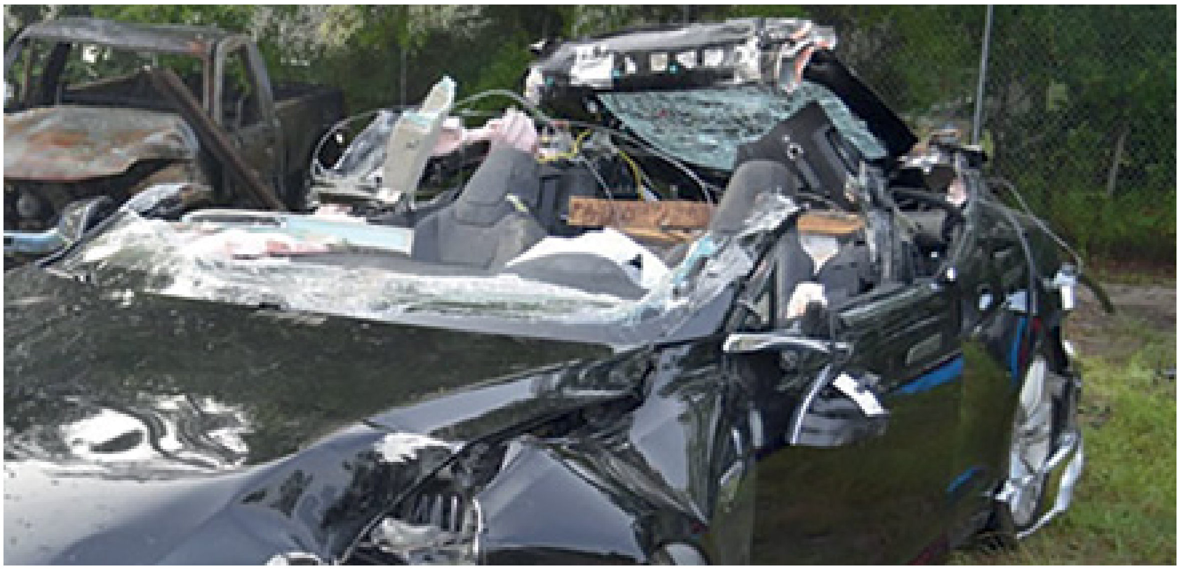


*Figure 30: Tesla Model S after the collision with the truck. (Source: Florida Highway Patrol)*

**Findings:**

- Both the truck driver and the driver of the Tesla had sufficient visibility to respond in time and prevent the accident. It is not clear why neither driver was sufficiently alert.
- The driver of the Tesla probably overestimated the reliability of the automated systems and did not understand their limitations.
- Limitations of the system: data from the Tesla revealed that the Autopilot was engaged 11 km before the collision. This level 2 automation technology cannot reliably identify and respond to intersecting traffic.
- Limitations of the system: the car was equipped with an advanced emergency braking system (AEBS), which is designed to automatically apply the brakes to reduce the severity of an impact or to help prevent frontal and rear-end collisions. The system is not designed to detect intersecting vehicles.

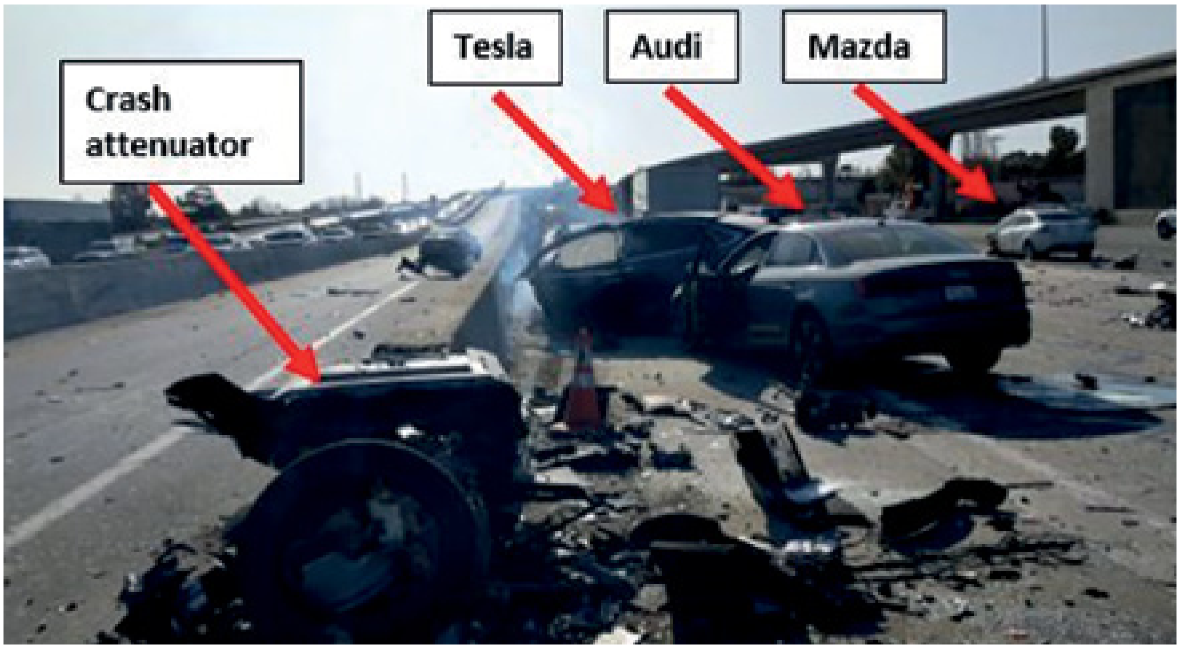
[170] NTSB, *Collision Between a Car Operating With Automated Vehicle Control Systems and a Tractor-Semitrailer Truck*, Highway Accident Report, 2017.

### C.3.2 Tesla collides with central crash barrier, California, USA

On 23 March 2018, a Tesla X collided with a crash barrier between the main road and an exit lane. This accident is currently being investigated by the NTSB[171].

The driver had engaged the Autopilot as he approached the exit to US Highway 85. This exit is on the left of the road. The Tesla started to steer left as the driver approached the chevron marking between the two lanes. The Tesla then collided with the central crash barrier, which was missing its impact absorber[172] due to an earlier collision. The Tesla did a complete flip and hit two other vehicles. The Tesla then burst into flame whereby the driver was fatally injured. The driver of one of the other two cars sustained minor injuries.

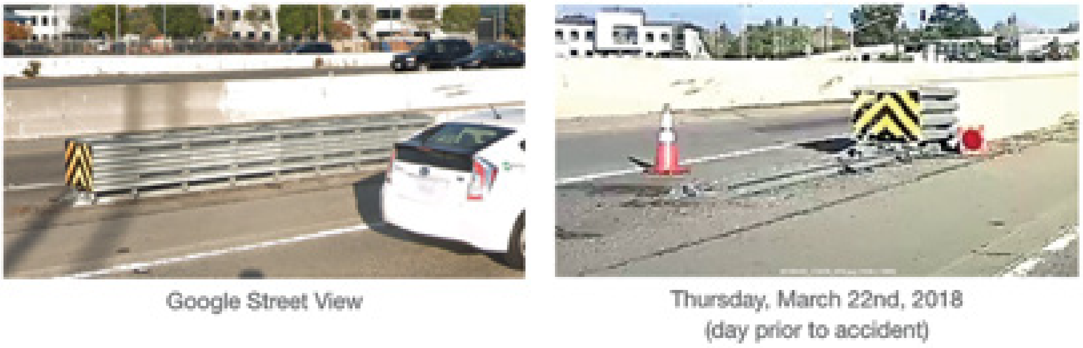
*(a) Accident location.*



*(b) Remains of various vehicles including the Tesla.*

[171] NTSB, *Preliminary Report: Highway HWY18FH011*, 2018.
[172] Also called a crash cushion, impact attenuator or crash attenuator.

Content
Appendix A. Explanation of the investigation
Appendix B. Responses to the draft report
Appendix C. Accidents
Appendix D. ADAS
Appendix E. Legislation and regulations



Google Street View

Thursday, March 22nd, 2018 (day prior to accident)

*(c) Impact absorber in normal situation and one day before the fatal collision.*

*Figure 31: Tesla Model X collides with central crash barrier on highway. (Source: NTSB report)*

**Findings:**

- The driver of the Tesla failed to apply the brakes or steer the vehicle away from the barrier.
- The driver last had his hands on the steering wheel 6 seconds before the collision.
- The Tesla accelerated from 100 km/h to 114 km/h 3 seconds before the collision. The car did not brake before the collision and did not steer away from the barrier.
- Limitations of the system: the Autopilot probably had trouble recognizing and following the lane marking on the road. The Autopilot system has less situational awareness than a human driver.
- The driver had previously complained to the dealer that the car veered to the left at this point on the motorway when on Autopilot, yet he still failed to be alert to the situation and did not intervene.[173]
- Another Tesla driver made a video shortly after this incident with the Autopilot function enabled in which it appears that his Tesla also veers to the left at the same point on the motorway.[174] There is another video of a Tesla driving straight at a central crash barrier with the Autopilot switched on.[175]

### C.3.3 Uber self-driving car collides into pedestrian, Arizona, USA

On 18 March 2018, an Uber test vehicle collided into a pedestrian crossing in the dark. The Uber vehicle, a modified Volvo V90 equipped with an integrated self-driving system (a test version close to SAE level 3) comprising a number of sensors and computer units, was travelling in self-driving mode on a main road with median strip at approximately 70 km/h. There was a driver behind the wheel of the Uber test vehicle whose task was to monitor the self-driving system and the traffic and to intervene if necessary. The pedestrian walked a bicycle out of the vegetation on the median strip and onto the road. The pedestrian was killed in this accident.

[173] Abc7news, I-TEAM EXCLUSIVE: *Victim who dies in Tesla crash had complained about Autopilot*, http://abc7news.com/automotive/i-team-exclusive-victim-who-died-in-tesla-crash-had-complained-about-autopilot/3275600/, accessed on 27 May 2018.

[174] Youtube, *Tesla Autopilot 2 Almost Crashes Into Barrier (ala Deadly Mountain View crash)*, https://www.youtube.com/watch?v=TIUU1xNqI8w, accessed on 20 May 2018.

[175] Youtube, *This is what may have happened in the recent Tesla Autopilot Crash*, https://www.youtube.com/watch?v=6QCF8tVqM3I, accessed on 20 May 2018.

Content
Appendix A. Explanation of the investigation
Appendix B. Responses to the draft report
Appendix C. Accidents
Appendix D. ADAS
Appendix E. Legislation and regulations

The NTSB has launched an investigation into this accident, the preliminary report of which has been published[176].

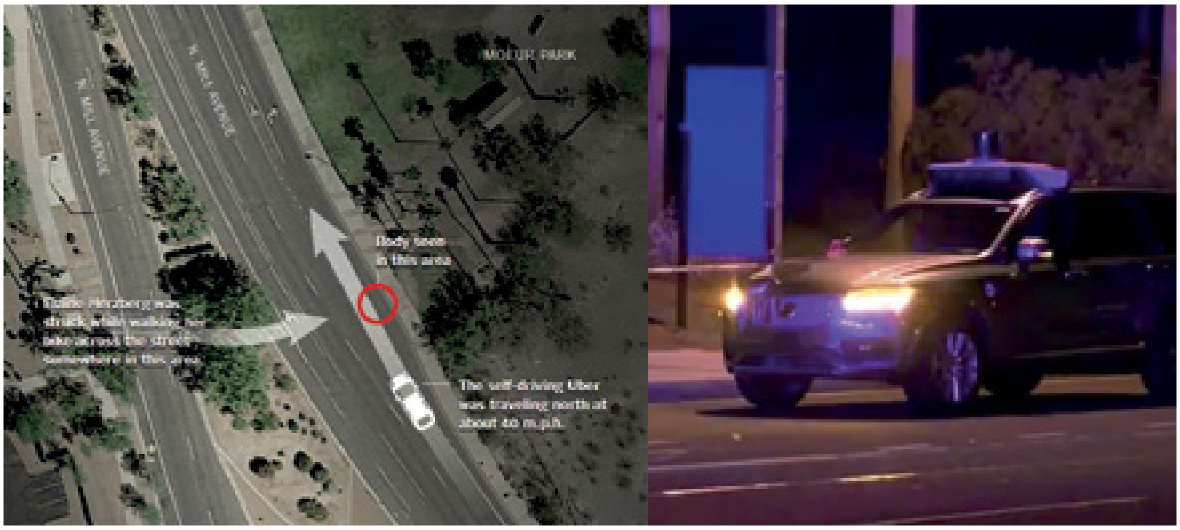

N. MILL AVENUE
N. MILL AVENUE
Body seen in this area
Elaine Herzberg was struck while walking her bike across the street somewhere in this area.
The self-driving Uber was traveling north at about 40 m.p.h.

*Figure 32: Accident involving a Volvo V90 owned by Uber and equipped with a self-driving system. Left: the accident location with the route of the Uber (in green) and the pedestrian (orange). Right: the Uber car after the accident with damage to the right front. (Source: ABC, Forbes)*

**Findings:**

- It was dark, the pedestrian was wearing dark clothes and the bike had no side reflectors.
- The driver had to do two things at the same time: watch the road and monitor the diagnostic screen under the dashboard.
- The driver was not watching the road at the time of the accident. It is not yet known what the driver was doing.
- The sensors detected the pedestrian 6 seconds before the collision, but the self-driving system did not take any action. This was possibly because the system had trouble classifying the situation: was the object a person, a vehicle, stationary, etc.?
- The Volvo collision avoidance system[177] (CAS) was disabled. In addition to the Volvo system, the vehicle was equipped with a custom-made self-driving system installed by Uber. The Uber system was also equipped with an FCW system; this system (which is unable to brake and only provides warnings) established that an emergency brake was required at 1.3 seconds before the collision. However, the brake was not applied because the Volvo's emergency brake software had been disabled.

[176] NTSB, *Preliminary Report - Highway - HWY18MH010*, 2018.

[177] CAS functions differently to FCW: FCW only provides warnings, while CAS can engage the brakes (and in some cases also the steering mechanism). CAS can hence be seen as FCW combined with AEBS.

Content
Appendix A. Explanation of the investigation
Appendix B. Responses to the draft report
Appendix C. Accidents
Appendix D. ADAS
Appendix E. Legislation and regulations

# ADAS

## D.1 History of digitization and automation in cars

The ongoing digitization of the automobile involves the introduction of more and more automated systems in vehicles.

*Digitization*

The digitization of cars has a long history. In the late 1960s, the first computers were installed in cars to make the ignition process more efficient. Small microprocessor-based computer systems called Electronic Control Units (ECUs) were used for this purpose.[178] ECUs for electronic petrol injection have been in use since 1968. Later, ECUs were also produced for other applications. Examples of ECUs are: Transmission Control, Seat Position Control, Electric Power Steering, Adaptive Front Lighting, Airbag Deployment, Telematic Control Unit (TCU) and Brake Control Module (BCM), ABS or ESC. These in-car microcomputers have enabled new functionalities that offer extra comfort for the driver or take over driving tasks. Modern cars have more than a hundred interconnected ECUs installed.[179]

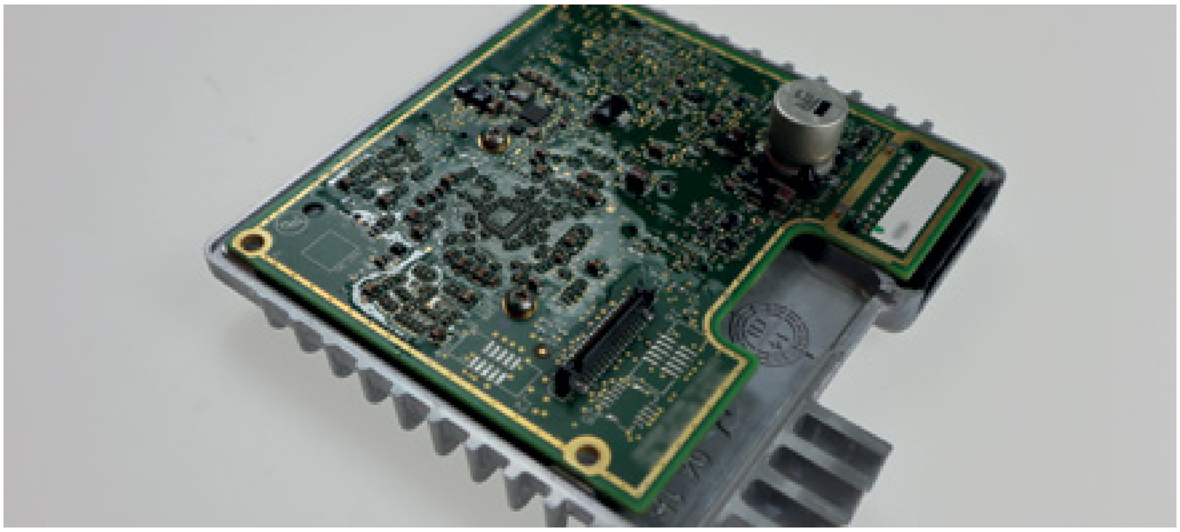


*Figure 33: An ECU.*

[178] Nick Davis, *Automotive Electronics: What are they, and how do they differ from "normal" electronics? - Power Electronics*, https://www.powerelectronicsnews.com/technology/automotive-electronics-what-are-they-and-how-do-they-differ-from-normal-electronics, accessed August 23, 2019.

[179] National Instruments, *Building Flexible, Cost-Effective ECU Test Systems*, 2019.

With the increase of the number of ECUs in cars, the amount of software has also increased significantly. By 2015, modern cars were thought to have as much as ten million lines of code in their systems.[180] The flexibility of software versus hardware offers many new opportunities to develop applications for cars, but also brings new challenges in the form of bugs, vulnerabilities and updates.

The automotive industry traditionally develops a new ECU for every new function, but there is currently a shift in the design of new cars towards the use of a central computer system with more computing power that receives information from many different sensors.[181] This is needed to process the huge amount of data and provide the computing power required for ADAS and self-driving technologies. In addition, combining several separate computer modules (the ECUs) makes it easier to manage the car as a whole and also facilitates the standardization of hardware and software. As such, the car is transforming from a mechanical vehicle with various computer systems on board into a data centre on wheels.

*Automation*

Automation supports the driver in performing the driving task. This can involve providing the driver with information and warning them of dangerous situations or by taking over certain tasks.

The automation of the driving task started with the introduction of cruise control (CC) in 1959. Although this application was initially mechanical, the number of cars with CC only really took off once the systems were controlled by ECUs (since the late 1980s). Since then, more and more ways for automated systems to assume the driver's primary driving task have been introduced. The digitization of the car has made this automation possible. Figure 34 provides a timeline of when the various automated functions were introduced.[182, 183] The more recent functions are often referred to as Advanced Driver Assistance Systems (ADAS).

[180] McCandless, Doughty-White, and Quick, *Million lines of code*, https://informationisbeautiful.net/visualizations/million-lines-of-code/, accessed July 10, 2019.

[181] McKinsey&Company, *Rethinking car software and electronics architecture*, 2018.

[182] BCG, *A Roadmap to safer diving through Advanced Driver Assistance Systems*, 2015.

[183] CAR, *Technology roadmaps: Intelligent Mobility Technology, Materials and Manufacturing Processes, and Light Duty Vehicle Propulsion*, 2017.

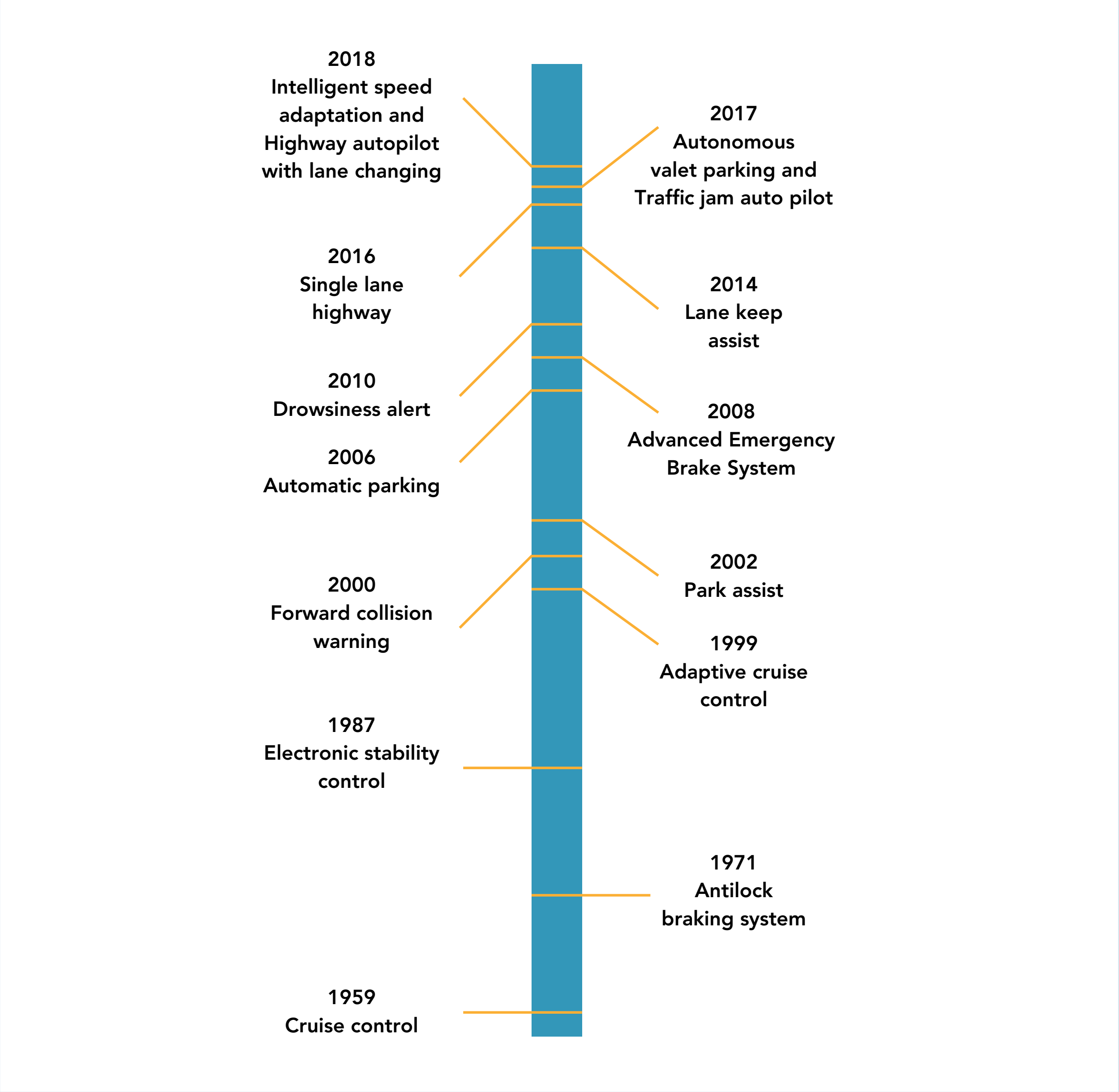

2018
Intelligent speed adaptation and Highway autopilot with lane changing
2017
Autonomous valet parking and Traffic jam auto pilot
2016
Single lane highway
2014
Lane keep assist
2010
Drowsiness alert
2008
Advanced Emergency Brake System
2006
Automatic parking
2002
Park assist
2000
Forward collision warning
1999
Adaptive cruise control
1987
Electronic stability control
1971
Antilock braking system
1959
Cruise control

*Figure 34: Vehicle automation timeline.*

## D.2 What are ADAS?

There is no single definition of Advanced Driver Assistance Systems (ADAS). In some cases, ADAS refers to all technologies used to support the driver while driving, including cruise control and ABS. In other cases, the emphasis is on ‘Advanced’, and only the more complex systems such as Lane Changing Assistance are covered by ADAS. The choice is often related to the reference framework:

- The focus is on the driver and the definition is based on the extent to which the system supports the driver.
- The focus is on the technology and the definition is based on the extent to which the system can control the vehicle autonomously.

The ADAS Alliance describes three characteristics of ADAS:[184]

- The driver has full responsibility, but shares control with the vehicle.
- The vehicle and the driver both detect and respond to objects and events, called Object and Event Detection and Response (OEDR).
- The driver may not perform any secondary tasks other than those permitted during normal driving.

The Dutch Safety Board uses the following definition:

**Definition ADAS**
Advanced Driver Assistance Systems (ADAS) support the driver in performing the primary driving task. These systems observe their surroundings using sensors and can take over control of the speed and/or direction of the vehicle under the responsibility of the driver. Such systems can also alert the driver to situations that the system estimates to be dangerous.

With this definition, the Dutch Safety Board places the emphasis on the driver. This is a broader definition than those used by the ACEA[185] and the SAE[186].

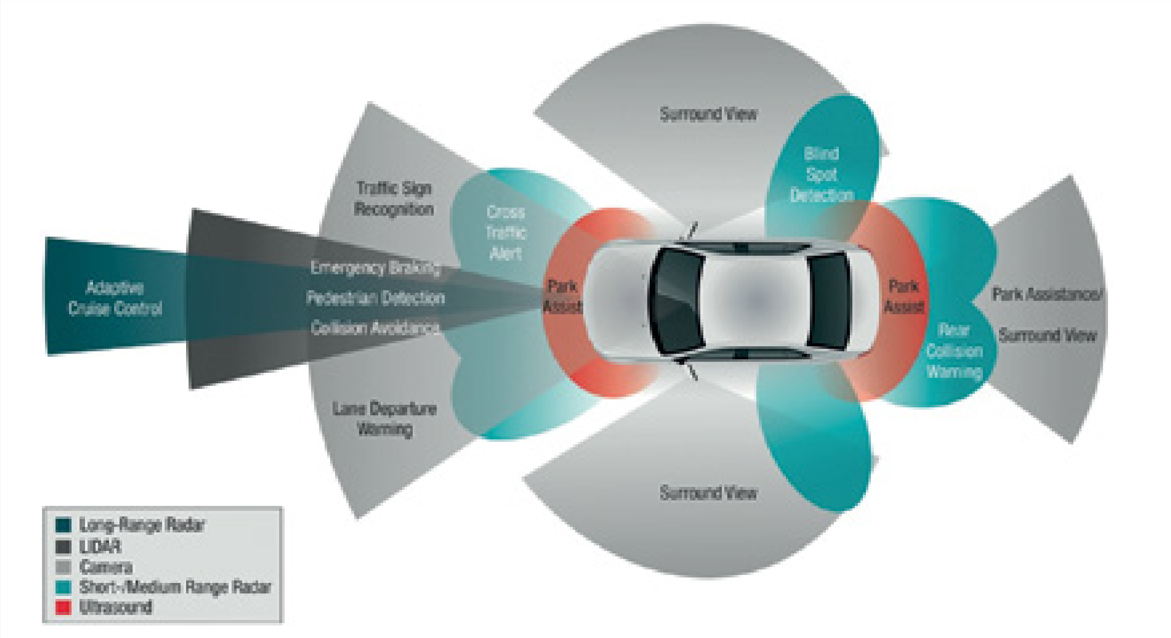


*Figure 35: Sensors in automated cars.*[187]

[184] ADAS Alliance, ADAS Convenant, 2019.
[185] Knapp e.a., *Code of practice for the design and evaluation of ADAS*, 2009.
[186] SAE International, *Taxonomy and definitions for terms related to Driving Automation Systems for on-road motor vehicles - Surface Vehicle Information Report*, 2014.
[187] Michigan Tech Research Institute, *Benchmarking sensors for vehicle computer vision systems*, https://mtri.org/automotivebenchmark.html, accessed August 28, 2019.

Content
Appendix A. Explanation of the investigation
Appendix B. Responses to the draft report
Appendix C. Accidents
Appendix D. ADAS
Appendix E. Legislation and regulations

An important feature of ADAS is that they use sensors to observe the vehicle's environment. The ADAS makes decisions based on the data from the sensors. There are various types of sensors, each with specific characteristics, such as radar, lidar and camera systems for different applications (see Figure 35). For example, radar works well for long distances but is less good at estimating direction. Radar is therefore used in adaptive cruise control when the vehicle in front has to be detected some way ahead. In some cases, information from multiple sensors is combined to produce a more accurate picture (this is called sensor fusion).

An overview of various types of ADAS with short descriptions can be found in Table 6.

| ADAS | Abbreviation | Description |
|---|---|---|
| Adaptive Cruise Control | ACC | System that adjusts the speed of the car to the speed of the vehicle in front. Also called Intelligent Adaptive Cruise Control. |
| Lane Keeping Assist | LKA | Helps the driver to keep the car in its lane. |
| Lane Departure Warning | LDW | Warns the driver if the car is about to move out of its lane. |
| Forward Collision Warning | FCW | Warns the driver of a possible forward collision. |
| Intelligent Speed Adaptation | ISA | Adjusts the car's speed based on information on the road infrastructure (based on a received signal or observations of road signs). |
| Automatic Parking | | Vehicle parks itself at low speed on the driver's command. |
| Drowsiness Alert | | Warns drivers if they are not paying sufficient attention to the performance of the driving task. |
| Single Lane Highway | LKA+ACC | Combination of LKA and ACC that enables the car to drive independently in its lane. |
| Advanced Emergency Brake System | AEBS | Emergency braking system that is activated in the event of an imminent collision. |

*Table 6: Various ADAS.*

The above table might suggest that ADAS has an unambiguous taxonomy, but this is not the case in practice. ADAS are often used by marketing departments to make cars more distinct. As a consequence, the same functionality may be called different names by different manufacturers, e.g. Nissan's ProPILOT, Tesla's Autopilot and Volvo's Pilot Assist all offer similar functionality.

## D.3 Artificial intelligence

Artificial intelligence (AI) is increasingly used in the development of ADAS and other automated functions[188, 189, 190, 191, 192], mainly for processing and interpreting sensor data. AI systems can perform complex tasks without human intervention or guidance. AI is mainly used to build systems that can operate, respond to their environment (based on sensor data), improve and adapt autonomously. These systems comprise various technologies that jointly ensure that a given level of intelligent behaviour is displayed in a given context.

AI systems can be divided into systems whereby humans have identified all possible situations in advance and drawn up corresponding decision rules (rule-based AI), and self-learning systems that are able to learn based on previous experiences or simulations (Machine Learning).

*Rule-based AI*
In the case of rule-based AI, a decision tree with instructions is created with which the system can more or less independently achieve a certain goal in specific situations. It is based on a predefined static model of the environment. A decision tree is used in many current ADAS, however this is not always called AI.

*Machine learning*
Machine Learning (ML) is a learning system based on algorithms that are able to learn from previous experiences. These are adaptive systems that can adjust their parameters depending on the external input. There are ML systems that are trained once with a specific dataset, and systems that learn continuously. Machine Learning is used for various ADAS applications, such as object detection (required for Single Lane Highway support).

*Improving rule-based systems*
ADAS have to respond to many different traffic situations based on complex algorithms that form the basis of the system's decisions. It requires a lot of effort to develop and improve these rule-based systems. One way to resolve this is to apply rule-based Machine Learning.[193] Using this method, the system 'observes' in the background to identify new useful rules that can be added to the decision tree. These new decision rules can then be extensively tested and verified before implementation. An improved learning system is created by using the aggregated data of all cars instead of only the data from a single vehicle.

[188] Russel and Norvig, *Artificial Intelligence – A Modern Approach,Artificial Intelligence – A Modern Approach*, 2010.
[189] Vetzo, Gerards, and Nehmelman, *Algoritmes En Grondrechten,Algoritmes En Grondrechten*, 2018.
[190] De Jong, Kool, and Van Est, *Zo Brengen We AI in de Praktijk Vanuit Europese Waarden*, 2019.
[191] Tricentis, *AI Approaches Compared: Rule-Based Testing vs. Learning*, https://www.tricentis.com/artificial-intelligence-software-testing/ai-approaches-rule-based-testing-vs-learning/, accessed August 23, 2019.
[192] Iriondo, *Differences Between AI and Machine Learning, and Why It Matters*, https://medium.com/datadriveninvestor/differences-between-ai-and-machine-learning-and-why-it-matters-1255b182fc6, accessed August 23, 2019.
[193] Weiss and Indurkhya, *Rule-based machine learning methods for functional prediction*, Journal of Artificial Intelligence Research 3 1995.

Content
Appendix A. Explanation of the investigation
Appendix B. Responses to the draft report
Appendix C. Accidents
Appendix D. ADAS
Appendix E. Legislation and regulations

*New developments*

Deep Learning (DL) is an advanced form of ML that uses artificial neural networks. Deep Learning is not yet present in modern cars. These are large, multi-layer models that operate in a similar way to the neuron function in the brain. Training a DL model correctly, with the right input data and extensive verification of the final performance, is an essential step to achieve the required model quality, and a lot of data is needed for the model to be effective. Deep learning technologies are essential for self-driving vehicles. Autonomously operating vehicles are closer to becoming reality thanks to the enormous amount of sensor data and the computing power that have become available.

## D.4 Classificatie automatisering

As described earlier, there are various definitions of ADAS and various approaches to automation. As a result, the systems are classified in various ways. The most common classification of automation in cars was developed by the Society of Automotive Engineers and laid down in document SAE-J3016[194]. Another system is the UNECE's formal legal classification. Euro NCAP's classification system is also important, because it distinguishes between safety systems and other systems.

[194] SAE International, *Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles - Surface Vehicle Information Report*, 2014.

| | Level 0 No automation of the driving task | Level 1 Driver support | Level 2 Semi automated | Level 3 Conditional automation | Level 4 High degree of automation | Level 5 Fully automated |
|---|---|---|---|---|---|---|
| **Who is driving the vehicle?** | A human driver controls the vehicle (determines the direction and speed). If automation is used, the human driver must be able to intervene. The human driver monitors the traffic situation and can use various instruments to do so. | | | The human driver must be on stand-by to take over control from the automated system if it so requests. | The automated system controls the vehicle; the human driver is no longer needed. | |
| **What do these systems do?** | Automated systems can provide warnings in the event of dangerous situations and temporarily intervene, for example in the event of an imminent collision with another road user or object. | The automated system can assume control of the direction or speed of the vehicle. The human driver monitors the traffic situation and can use various instruments to do so. | The automated system can assume control of the direction and speed of the vehicle simultaneously. The human driver monitors the traffic situation and can use various instruments to do so. | The automated system has full control over the vehicle under certain conditions (e.g. on motorways and/or while driving in queues). Level 3 automation will not work in all situations. | The automated system has full control over the vehicle under most conditions. Level 4 automation will not work in all situations (e.g. only in certain regions). | The automated system has full control over the vehicle under all conditions. |
| **Examples** | Automatic Emergency Braking System (AEBS)<br>Lane Departure Warning (LDW), Front Collision Warning (FCW)<br>ABS, ESC, traction control | Adaptive Cruise Control (ACC), Lane Keeping Assist (LKA), Park Assist (PA) | ACC combined with LKA, e.g. Tesla Autopilot, Nissan ProPILOT, Volvo Pilot Assist. | | | Fully automated vehicle |

*Table 7: SAE levels of road traffic automation. The orange-shaded boxes are the systems that were the main focus of this investigation.*

Content
Appendix A. Explanation of the investigation
Appendix B. Responses to the draft report
Appendix C. Accidents
Appendix D. ADAS
Appendix E. Legislation and regulations

*SAE levels*

The SAE has divided the automated systems in cars into five categories. An overview of the various levels can be found in Table 7. The five levels can be briefly described as follows:

- At levels 1 and 2, the driver makes the tactical choices, but the system gradually takes over the driving task and the driver assumes the role of operator, who must be ready to take over control and reassume the familiar role of active driver if the system fails or makes a mistake.
- At level 3, the driver has become a full operator.
- At levels 4 and 5, the driver no longer has a role in controlling the vehicle. At level 4 this applies to a limited environment and at level 5 this is unrestricted.

The scope of the ADAS discussed in this investigation report corresponds in any case to SAE levels 1 and 2. According to our ADAS definition, level 3 systems also fall within the scope of the investigation, but there are currently few, if any, examples of this system on the roads. Of the SAE level 0 systems, AEBS also fall within the scope of our investigation, but other emergency systems in level 0 do not.

*UNECE*

UN Regulation No. 79 defines the most important terms and categories concerning the automation of the driving task. The automated systems in cars are classified here based on much more technical criteria than in the SAE levels. Only systems that influence steering are classified, because there are as yet no specific requirements for ADAS that continuously influence the speed of the vehicle. This classification is included in Annex E.4.

*Euro NCAP*

Euro NCAP is an institute that assesses the safety of cars in critical situations, such as the protection of occupants in the event of a collision. Euro NCAP distinguishes between safety systems and other systems. Safety systems are included in the star rating system under the ‘safety assist’ systems, which include three different types of ADAS:

- AEB Interurban (also called AEBS at higher speeds)
- Lane Support (lane departure warning or intervention systems and blind spot monitoring systems)
- Speed Assist (systems that warn of speeding, systems that display the speed limit and systems that limit the speed)

Other safety systems that have nothing to do with automation, such as seatbelt reminders, are also taken into account. The Euro NCAP system does not consider the level of automation of the driving task, but only whether a particular type of system provides proven safety benefits.

**Star rating system**
The Euro NCAP star rating system provides an assessment of additional safety measures installed in a car above the requirements. This includes the protection of the adult driver, the child occupants, vulnerable road users such as pedestrians, and the safety assist systems mentioned above. The safety assist systems comprise ADAS that help the driver to drive safely.

# APPENDIX E

## LEGISLATION AND REGULATIONS

### E.1 Introduction

Vehicles driving on public roads in the Netherlands must meet certain requirements. These requirements vary according to the type of vehicle. For the purposes of this investigation, we have confined ourselves in the first place to requirements for motor vehicles, and in particular to requirements for mass-produced passenger cars. In the second place, we consider only requirements with a direct relationship to road safety. For example, we do not assess the regulations for noise and emissions, nor do we consider the differences between electric cars and cars with a combustion engine. The emphasis is on active safety (systems such as ABS and various ADAS) and not on passive safety (seatbelts, headrests, airbags, crumple zones, etc.).

### E.2 Establishing the regulations

Car manufacturers come from different countries and continents and produce and compete in an international market. Manufacturers have a strong interest in ensuring that the same rules and technical standards apply in as many countries as possible. This is already the case in the European Union's internal market. For example, cars approved in the Netherlands are also allowed to drive in other European Member States and vice versa. Dutch vehicle legislation is harmonized at the European level for most motor vehicles, including passenger cars and lorries. Proposals for EU legislation are prepared and submitted by the European Commission and adopted by the Member States, who are united in the European Council of Ministers and the European Parliament. EU legislation falls into two categories: regulations, which have direct and immediate force of law in all EU Member States, and directives, which must be implemented by the Member States in national legislation and regulations. The EU directives and regulations incorporate many international regulations, particularly in the field of technical requirements. These have been established by UNECE (United Nations Economic Commission for Europe) in Geneva. The main objective of UNECE is to promote pan-European economic integration. Because the decision-making process within UNECE is aimed at reaching consensus, extensive consultation takes place at various levels. UNECE has a wider mandate than only transport, but its other focus areas are not considered in the context of this investigation. Figure 36 provides an overview of UNECE's transport organization.

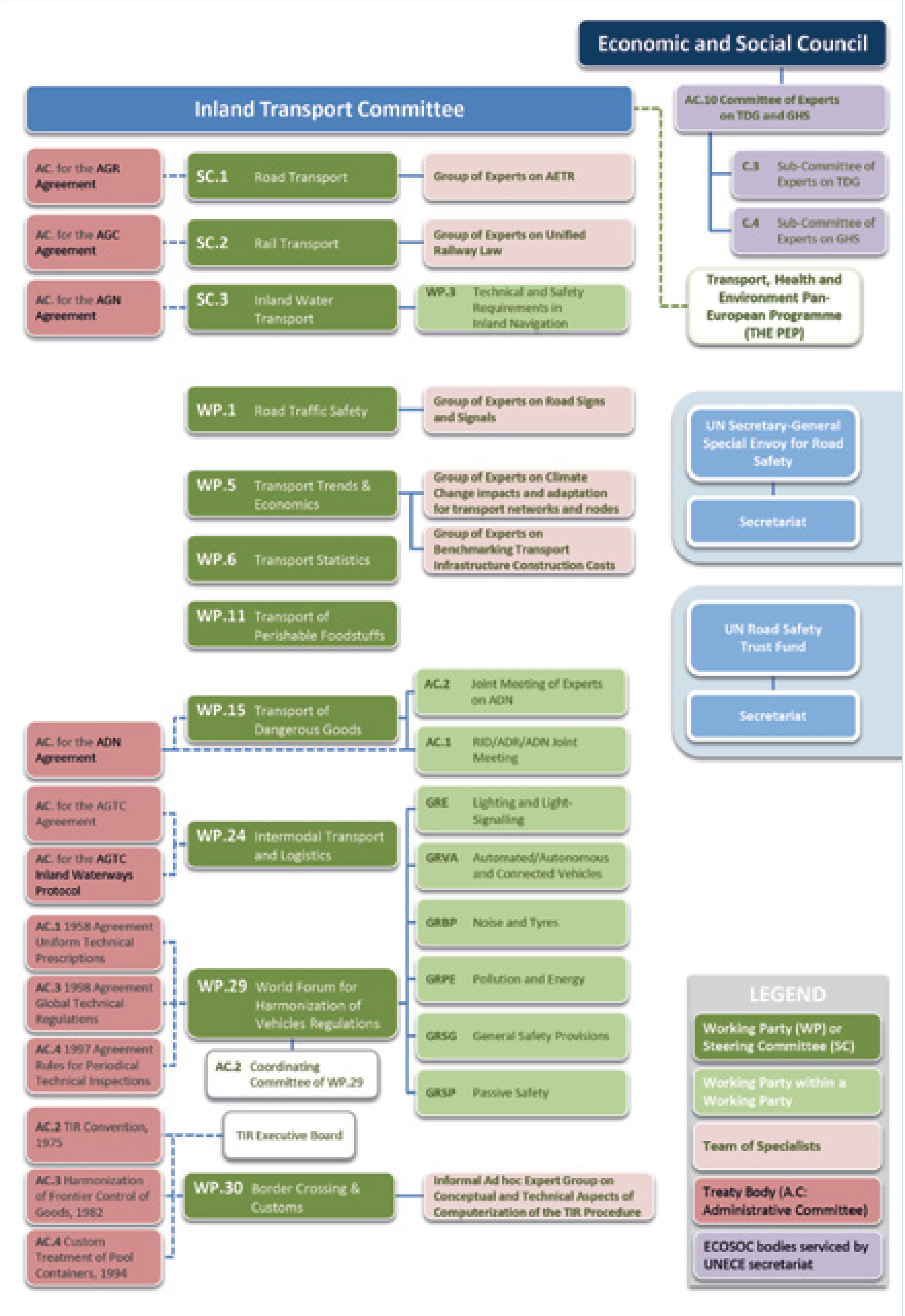

Economic and Social Council
Inland Transport Committee
AC.10 Committee of Experts on TDG and GHS
C.3 Sub-Committee of Experts on TDG
C.4 Sub-Committee of Experts on GHS
Transport, Health and Environment Pan-European Programme (THE PEP)
AC. for the AGR Agreement
SC.1 Road Transport
Group of Experts on AETR
AC. for the AGC Agreement
SC.2 Rail Transport
Group of Experts on Unified Railway Law
AC. for the AGN Agreement
SC.3 Inland Water Transport
WP.3 Technical and Safety Requirements in Inland Navigation
WP.1 Road Traffic Safety
Group of Experts on Road Signs and Signals
UN Secretary-General Special Envoy for Road Safety
Secretariat
WP.5 Transport Trends & Economics
Group of Experts on Climate Change impacts and adaptation for transport networks and nodes
Group of Experts on Benchmarking Transport Infrastructure Construction Costs
WP.6 Transport Statistics
WP.11 Transport of Perishable Foodstuffs
UN Road Safety Trust Fund
Secretariat
AC.2 Joint Meeting of Experts on ADN
WP.15 Transport of Dangerous Goods
AC. for the ADN Agreement
AC.1 RID/ADR/ADN Joint Meeting
AC. for the AGTC Agreement
GRE Lighting and Light-Signalling
WP.24 Intermodal Transport and Logistics
AC. for the AGTC Inland Waterways Protocol
GRVA Automated/Autonomous and Connected Vehicles
AC.1 1958 Agreement Uniform Technical Prescriptions
GRBP Noise and Tyres
AC.3 1998 Agreement Global Technical Regulations
WP.29 World Forum for Harmonization of Vehicles Regulations
GRPE Pollution and Energy
GRSG General Safety Provisions
AC.4 1997 Agreement Rules for Periodical Technical Inspections
AC.2 Coordinating Committee of WP.29
GRSP Passive Safety
AC.2 TIR Convention, 1975
TIR Executive Board
AC.3 Harmonization of Frontier Control of Goods, 1982
WP.30 Border Crossing & Customs
Informal Ad hoc Expert Group on Conceptual and Technical Aspects of Computerization of the TIR Procedure
AC.4 Custom Treatment of Pool Containers, 1994
LEGEND
Working Party (WP) or Steering Committee (SC)
Working Party within a Working Party
Team of Specialists
Treaty Body (A.C: Administrative Committee)
ECOSOC bodies serviced by UNECE secretariat

*Figure 36: UNECE transport organization (Source: UNECE).*

Content
Appendix A. Explanation of the investigation
Appendix B. Responses to the draft report
Appendix C. Accidents
Appendix D. ADAS
Appendix E. Legislation and regulations

Major automobile manufacturing countries outside the EU are also members of UNECE, including the United States, Japan and South Korea. UNECE is hence a global platform for technical vehicle regulation. The initiative for new regulations is sometimes taken in Brussels (European Commission) and sometimes in Geneva (UNECE). Proposals for EU legislation are prepared by the EC and adopted by the European Council and the European Parliament. The EU is a member of UNECE and the European Commission votes on behalf of the EU Member States on new UNECE regulations or amendments to existing regulations, whereby the EU position is coordinated with the EU Member States in Brussels in advance. This coordination takes place in various committees and working groups within both the European Commission and the European Council. The regulations adopted by the EU in Geneva are binding for all EU Member States.

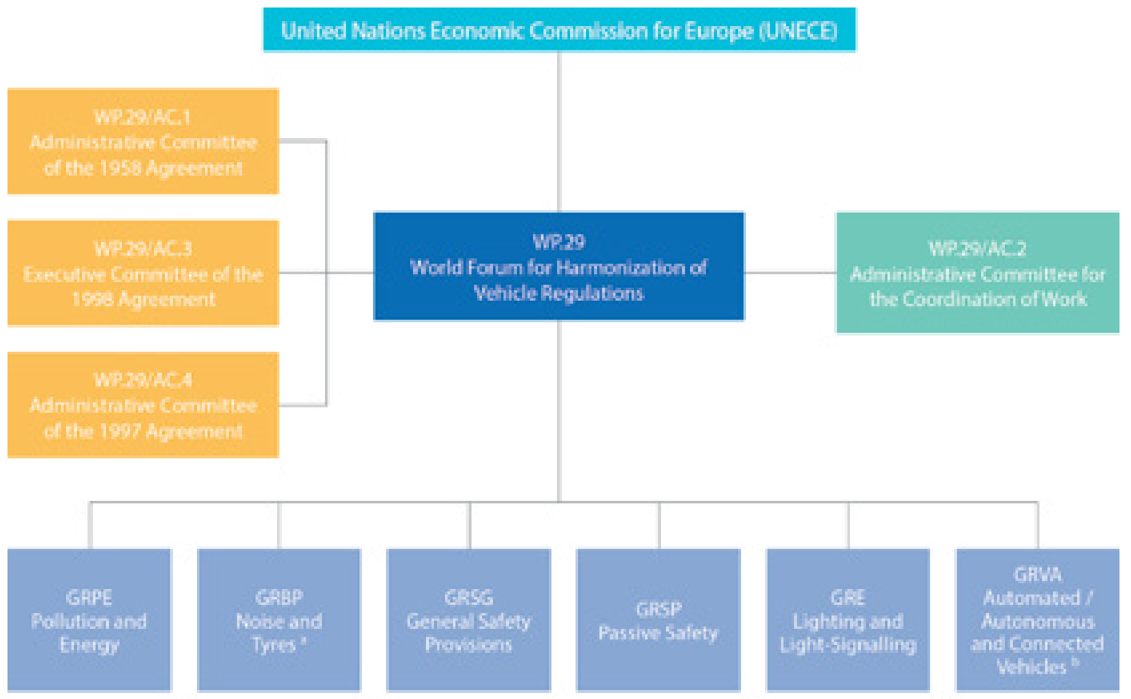
Two so-called Working Parties within the UNECE are important for the purposes of this investigation:

- WP.1 'Global Forum for Road Traffic Safety'. This Working Party focuses on improving road safety based on three decisive and interrelated aspects: the vehicle, the behaviour of road users and the infrastructure.
- WP.29 'World Forum for Harmonization of Vehicle Regulations'. The 'Blue Book'[195] provides an overview of this Working Party's working method, which is aimed at establishing broadly supported and widely applicable technical regulations for vehicles. This is based on three Agreements, which are not discussed here. Under WP.29, six working groups are active in various fields, the most important of which for this investigation is the GRVA, the working group on 'Automated/Autonomous and Connected Vehicles'. This working group prepares the ADAS regulations and submits them to WP.29, which decides whether to implement them. A number of informal working groups for specific types or components of ADAS also operate under the GRVA. Figure 37 displays a general organizational chart of WP.29.

Only representatives of the member countries sit on WP.1 and WP.29. An employee of the Ministry of Infrastructure and Water Management represents the Netherlands in WP.1. The Ministry has mandated an employee of RDW to represent the Netherlands in WP.29. RDW and the Ministry of Infrastructure and Water Management regularly coordinate their activities in regard to UNECE. The member countries vote and decide on the proposed regulations (UN Regulations, UN Global Technical Regulations and UN Rules; depending on the Agreement under which they are regulated), which are prepared by the working groups under these Working Parties and also include representatives of car manufacturers, suppliers, interest groups and approval authorities such as RDW. The aim of these consultations is to agree on technical requirements, in which wide-ranging political and economic interests also play an important role. The regulations lay down minimum requirements in the field of road safety. These regulations may not be made stricter by individual Member States, but car manufacturers are free to produce safer cars than required by law. This is where car manufacturers can distinguish themselves from, and compete with, each other. Euro NCAP (see Annex D) assesses a number of non-statutory safety measures in cars (based on tests) and classifies them according to a star rating system. As of recently,

[195] UNECE, *World Forum For Harmonization of Vehicle Regulations (WP.29); How It Works, How to Join It*, 2019.

a limited number of ADAS are also included in the tests and the classification. This star rating system encourages car manufacturers to take additional measures to improve the active and passive safety of their cars. When many car manufacturers have implemented a certain additional measure, it will often be incorporated in the regulations by UNECE and the EU.


United Nations Economic Commission for Europe (UNECE)
WP.29/AC.1 Administrative Committee of the 1958 Agreement
WP.29/AC.3 Executive Committee of the 1998 Agreement
WP.29/AC.4 Administrative Committee of the 1997 Agreement
WP.29 World Forum for Harmonization of Vehicle Regulations
WP.29/AC.2 Administrative Committee for the Coordination of Work
GRPE Pollution and Energy
GRBP Noise and Tyres [a]
GRSG General Safety Provisions
GRSP Passive Safety
GRE Lighting and Light-Signalling
GRVA Automated / Autonomous and Connected Vehicles [b]

a Decision by WP.29 at the November 2018 session.
b Former Working Party on Brakes and Running Gear (see ECE/TRANS/WP.29/1139, paras. 15 and 33).

*Figure 37: Organizational chart of UNECE's WP.29 (Source: UNECE).*

## E.3 Types of requirements for passenger cars

Mass-produced passenger cars that use public roads must comply with three types of requirements: approval requirements, permanent requirements and operating requirements.

The **approval requirements** are tested by means of a type approval test in one of the EU Member States. This is carried out by an authorized European testing laboratory. Such tests can be carried out both on vehicles and on the systems, components and separate technical units intended for use in vehicles. A type approval in an EU Member State automatically entails approval in the entire EU. Once an approval has been obtained, it remains in force even if the approval requirements are later changed or tightened. This means that approved vehicles do not have to be modified to comply with new rules, but newly produced cars of a certain make may have to meet the stricter requirements. The approval requirements and the testing methods are described in European Directive 2007/46/EC, which forms the basis of the Dutch Motor Vehicle Regulations (a new version of which came into force on 20 May 2018). The Motor Vehicle Regulations implement sections III and VI of the 1994 Road Traffic Act. For type approvals,

Content
Appendix A. Explanation of the investigation
Appendix B. Responses to the draft report
Appendix C. Accidents
Appendix D. ADAS
Appendix E. Legislation and regulations

the Motor Vehicle Regulations refer directly to Directive 2007/46/EC. This directive describes detailed requirements to ensure that type approvals conducted in different countries lead to the same result. Some of the requirements are included in the Directive, while others refer to UNECE regulations which are binding on the EU and its Member States by agreement.

Article 34 'UNECE regulations required for EC type-approval' in Directive 2007/46/EC explicitly provides for this. These regulations are descriptive and quantitative for conventional (largely mechanical) parts and systems in cars. The regulations for ADAS are qualitative and functional or non-existent. We will come back to this below.

European legislation and regulations in the field of vehicle approval requirements are renewed approximately once every ten years. For example, the successor to Directive 2007/46/EC has already been drafted in the form of Regulation (EU) 2018/858 and will enter into force on 1 September 2020. The current regulations will need to be supplemented during this ten-year period, for example to take account of new technical developments. We will come back to this below. In April 2019, the European Council and the European Parliament also adopted the General Safety Regulation (GSR), which includes additional requirements in the field of vehicle regulations from a road safety perspective. These requirements will be explained in more detail in a following section.

**Permanent requirements** are requirements that the vehicle must meet when used on the road. These requirements focus on road safety aspects, such as the proper functioning of lights, brakes, steering and tyres. These components are checked by the police and during MoT (Periodic Vehicle Inspection) tests. These checks must be able to be carried out quickly without disassembling the vehicle or conducting a driving test. The permanent requirements are therefore much less extensive than the approval requirements. The permanent requirements and the testing method are clearly and exhaustively described in the Motor Vehicle Regulations and are based on Directive 2014/45/EU. They contain very few provisions on ADAS; those that do refer only to the proper functioning of audible warnings and indicator lights to alert the driver.

**Practical requirements** relate to practical operations such as coupling trailers and carrying passengers and are not relevant in the context of this investigation.

## E.4 Existing European approval requirements for ADAS

The Dutch Motor Vehicle Regulations apply the approval requirements for mass-produced passenger cars and their parts in Directive 2007/46/EC in their entirety. This directive describes detailed approval requirements for motor vehicles as a whole, but also for the systems, components and separate technical units installed in these motor vehicles. EU type approvals apply to vehicles as these are delivered from the manufacturer. New passenger cars often contain systems, components and separate technical units that have been used previously, often in several makes and/or models. These systems, parts and components can be given separate type approvals, which in turn can be used as building blocks when applying for a type approval for a new car. However, Directive 2007/46/EC did not contain any approval requirements for ADAS when it was implemented.

*Anticipating innovations in the approval process*

Directive 2007/46/EC regulates (in general terms) how parts for which no approval requirements have been established should be assessed in order to qualify for a separate type approval. Two articles of this Directive apply in particular (see Figure 38).

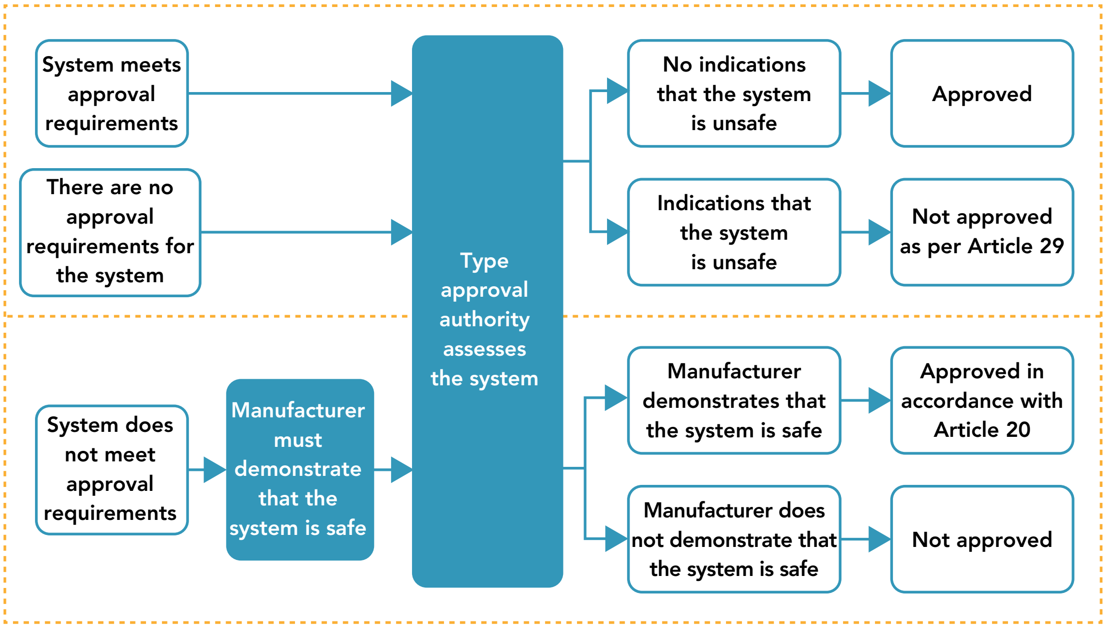

System meets approval requirements
There are no approval requirements for the system
System does not meet approval requirements
Manufacturer must demonstrate that the system is safe
Type approval authority assesses the system
No indications that the system is unsafe
Indications that the system is unsafe
Manufacturer demonstrates that the system is safe
Manufacturer does not demonstrate that the system is safe
Approved
Not approved as per Article 29
Approved in accordance with Article 20
Not approved

*Figure 38: Flowchart for processing an application for type approval.*

Article 20 'Exemptions for new technologies or new concepts' in Chapter VIII 'New technologies or concepts incompatible with separate directives' enables manufacturers to apply for an EC type approval for a system, component or separate technical unit that incorporates technologies or concepts which are incompatible with the existing regulations. The application may be submitted in any Member State. When granting the approval (initially only in the Member State concerned) for a type of vehicle covered by the requested exemption, the Member State must inform the EC and Member States of the following matters:

a. the reasons why the technologies or concepts in question make the system, component or separate technical unit incompatible with the requirements,
b. a description of the safety and environmental considerations concerned and the measures taken, and
c. a description of the tests, including their results, demonstrating that, by comparison with the requirements from which exemption is sought, at least an equivalent level of safety and environmental protection is ensured.

Article 20 further establishes how the provisional approval in one Member State can be extended to an EC type approval valid in all Member States. Article 21 regulates how to adapt the existing directives and regulations (for so-called non-essential parts), including in the case of UNECE regulations.

Article 29 'Vehicles, systems, components or separate technical units in compliance with this Directive' in Chapter XII 'Safeguard clauses' states that: 'If a Member State finds that new vehicles, systems, components or separate technical units, albeit in compliance with the applicable requirements or properly marked, present a serious risk to road safety, or seriously harm the environment or public health, that Member State may, for a maximum period of six months, refuse to register such vehicles or to permit the sale or entry into service in its territory of such vehicles, components or separate technical units. In such cases, the Member State concerned shall immediately notify the manufacturer, the other Member States and the Commission accordingly, stating the reasons on which its decision is based and, in particular, whether it is the result of any of:

- shortcomings in the relevant regulatory acts, or
- incorrect application of the relevant requirements.

Article 29 also regulates the subsequent measures to be taken by the EC.

*UNECE Regulations for ADAS*
Three UNECE documents are important for the regulation of ADAS in passenger cars.

1. UN Regulation No.79, Addendum 78, Revision 4 'Uniform provisions concerning the approval of vehicles with regard to steering equipment' became effective as of 18 October 2018 (hereinafter referred to as UN R.79). This regulation deals with ADAS that for a limited duration take over the steering function from the driver, called Advanced Driver Assistance Steering Systems (ADASS). The driver can always overrule an ADASS. This regulation also takes account of the future and the possibility of self-driving cars without a driver. The required systems are known as Autonomous Steering Systems (ASS). Although ASS are defined in UN R.79, it is currently not permitted to approve this autonomous variant for use on the road and so no further technical requirements have been described for this system. Within ADASS, UN R.79 distinguishes between Automatically Commanded Steering Functions (ACSF)[196] and Corrective Steering Functions (CSF)[197]. ACSF are comfort systems that support the driver in the primary driving task. The document divides the ACSF into six categories according to their function (see Table 8).

| Category | Description |
|---|---|
| A | A function operating at a speed no greater than 10 km/h to assist the driver, on demandt, in low speed or parking manoeuvring. |
| B1 | A function which assists the driver in keeping the vehicle within the chosen lane, by influencing the lateral movement of the vehicle. |
| B2 | A function initiated or activated by the driver which keeps the vehicle within its lane by influencing the lateral movement of the vehicle for extended periods without further driver command/confirmation. |
| C | A function which is initiated/activated by the driver and which can perform a single lateral manoeuvre (e.g. lane change) when commanded by the driver. |
| D | A function which can indicate the possibility of a single lateral manoeuvre (e.g. lane change) but performs that function only following a confirmation by the driver. |
| E | A function which is initiated/activated by the driver and which can continuously determine the possibility of a manoeuvre (e.g. lane change) and complete these manoeuvres for extended periods without further driver command/confirmation. |

*Table 8: ACSF categories according to UN R.79.*

Technical requirements have already been established for the ACSF categories A, B1 and C, but not yet for B2, D and E. The use of ACSF is optional and the driver can engage or disengage it while driving.

[196] Examples of ACSF are Lane Change Assist (Category C) , High way pilot (Category E) of ParkAssist (Category A).
[197] An example of CSF is LDA (Lane Departure Avoidance).

CSF are emergency systems which intervene in case of incidental unexpected changes in the lateral movement of the car. These systems are always active in the background and intervene only occasionally and briefly (as with ABS and ESC). A warning light must illuminate to indicate that a CSF has intervened, and an audible warning must be provided if the intervention continues for more than ten seconds. This audible warning will only cease if the driver takes over the steering.

2. UN Regulation No. 130 'Uniform provisions concerning the approval of motor vehicles with regard to the Lane Departure Warning System (LDWS)' became effective as of 9 July 2013. In contrast to a CSF, an LDWS only provides a warning and does not intervene.
3. Annex 6 'Guideline on cybersecurity and data protection' of the Consolidated Resolution on the Construction of Vehicles (R.E.3)[198] provides a general guideline for measures to ensure cybersecurity and data protection in cars with ADAS. This guideline refers to standards developed and applied in other sectors in the field of information security (ISO 27000 series), cybersecurity (ISO/IEC 15408) and the security of electrical and electronic systems. WP.29 is working on new proposals[199] in the field of cybersecurity and Over-The-Air (OTA) communication between ADAS and other systems in cars and car manufacturers, for example for updating ADAS.

Informal UNECE working groups under the GRVA are preparing regulations in the area of EDR/DSSAD (Event Data Recorder and Data Storage System for Automated Driving) and AEBS for passenger cars, among other things. The emphasis here is on systems of SAE level 3 and higher. The roadmap of WP.29 also contains subjects that will have to be taken up later, such as the training of drivers and the way in which vehicles with ADAS will have to be maintained and inspected during their lifecycle.

[198] UNECE, *ECE/TRANS/WP.29/78/Rev.6, Consolidated Resolution on the Construction of Vehicles (R.E.3)*, Revision 6, 2017.
[199] UNECE, *ECE/TRANS/WP.29/GRVA/2019/2, Proposal for a Recommendation on Cyber Security*, 2019.

DUTCH
SAFETY BOARD

**Visiting address**
Lange Voorhout 9
2514 EA  The Hague
T 070 333 70 00
F 070 333 70 77

**Postal address**
PO Box 95404
2509 CK  The Hague

www.safetyboard.nl