The development of autonomous vehicles currently focuses on the functionality of vehicle guidance systems.\textsuperscript{1} Numerous demonstrations of experimental vehicles have shown their impressive capabilities—listed here with the most recent named first. For example, the drive on the Bertha-Benz route undertaken by the Karlsruhe Institute for Technology and Daimler AG [69], the Stadtpilot project of the Technische Universität Braunschweig [41, 60], activities of Google Inc. [13, 59], the BRAiVE Research Institute and the VIAC Project of the VisLab Institute of the University of Parma [4, 8], the research activities of the Collaborative Research Centre 28 of the German Research Foundation (DFG) [31, 55, 57] and the results of the DARPA Urban Challenge [51–53]. If the experimental vehicles were driving in traffic on public roads, a safety driver\textsuperscript{2} was always in the vehicle to monitor the technical system. This person had to intervene if a technical defect occurred meaning that the current situation was beyond the capabilities of the vehicle or if another

\textsuperscript{1}A vehicle guidance system is a technical system that steers the vehicle without human intervention. Unlike driver assistance systems, no monitoring by a human driver is necessary. The system, consisting of the vehicle and vehicle guidance system, forms an “autonomous vehicle”. The meaning of the term “driving robot” is very similar to that of the vehicle guidance system. However it is frequently understood as a mechatronic system, which operates a vehicle like a human (see \url{http://www.uni-ulm.de/in/mrm/forschung/mechatronik/kognitiver-fahrroboter.html}). To avoid confusing the two, the term “driving robot” will not be used in this article.

\textsuperscript{2}The article will use the terms “driver” and “safety driver” to indicate human drivers and safety drivers.

A. Reschka (✉)
Technische Universität Braunschweig, Institute of Control Engineering,
38106 Braunschweig, Germany
e-mail: reschka@ifr.ing.tu-bs.de
event necessitated this. This necessary monitoring of the technical system means that the indicated test drives on public roads are classified as semi-automated according to [20]. However, the aim of future vehicle guidance systems with higher levels of automation is to operate the systems independently in all situations without human monitoring.

Therefore, in the development of vehicle guidance systems, a safety concept is required that covers the various steps of the development process, such as the specification, design, development and the functional tests. In addition safety functions that can attain or attempt to sustain a so-called safe state are required in the system.

23.1 Safe State

The use of the term safe state is often ambiguous. Safety is a relative concept and depends on the individual perception of the observer. According to the ISO 26262 standard, an operating mode of a system or an arrangement of systems can be regarded as safe when there is no unreasonable risk (see “safe state”, ISO 26262, Part I, 1.102 [30]). This means that a safe state is only present when the current and future risk is below a threshold accepted in society (see “unreasonable risk”, ISO 26262, Part I, 1.136 [30]). This threshold is to be regarded as a value of what is not acceptable in a specific context according to social, moral or ethical considerations (see ISO 26262, Part I, 1.136 [30]). Risk is to be understood as a combination of the probability of occurrence and the severity of the personal injury (see “risk” and “harm”, ISO 26262, Part I, 1.99 and 1.56).

This definition allows us to understand a safe state as a state where risk from the system is reasonable. The frequently used term risk-minimized condition (e.g. in [20]) can be misunderstood as this does not place the risk in relation to an accepted risk and does not specify whether the system that is being operated with minimum risk is also safe.

The essential challenge when using the term safe state, in the sense of a condition with an acceptable level of risk for passengers and other road users, is the identification of a threshold under which the risk level is acceptable. When operating an automated vehicle, the level of acceptable risk depends on the current situation of the vehicle. The situation includes the following, according to [21] and [43]:

- All stationary and dynamic objects relevant to a driving decision
- The intention of the dynamic objects including the autonomous vehicle
- The pertinent legal conditions
- The mission of the autonomous vehicle
- The current power capability of the autonomous vehicle.

Therefore, for an autonomous vehicle, the current risk must be continuously determined on the basis of the current situation and a comparison of the risk with the threshold value that is regarded as still just about acceptable. In the sense of the ISO 26262 standard,
this means that the likelihood of personal injury and the severity of the injuries must be determined for every situation and all ways in which the situation can develop and the courses of action that present a reasonable and acceptable level of risk must be identified. The author is currently not aware of a technical solution for this problem.

23.1.1 Safe State in Driver’s Assistance Systems Used in Series-Production Vehicles

In the case of driver’s assistance systems, the driver monitors the technical system and has to pay close attention to the traffic situation. The driver is supported when driving. The current Mercedes-Benz p Class models are available with a system called “DISTRONIC PLUS with Steering Assist and Stop&Go Pilot”. This system supports the driver in guiding the vehicle both laterally as well as longitudinally [49]. The driver still needs to follow events on the road, and the steering assist system deactivates after a specified time if the driver takes his hands off the steering wheel:

If the Steering Assist with Stop&Go Pilot detects that the driver has taken his hands off the steering wheel during the journey, depending on the driving situation, the steering wheel inertia sensor, the environment detected and the speed, the driver is warned in the instrument cluster. If the driver does not respond, a warning tone is sounded and the steering assist is deactivated. (Translated [49])

For this reason, the system is to be regarded as semi-automated according to the standards laid out in [20] or as partial automation according to [48]. The longitudinal guidance can also switch off and cede control to the driver with a corresponding signal as soon as technical faults develop or—depending on the way the system is set—if specific threshold values such as a minimum speed are no longer met [62].

Hörwick and Siedersberger [25] presents a safety concept for semi-automated and highly automated driver assistance systems. However, the terms are again used differently here. In [25], fully automated DAS (FA-DAS) actually means semi-automated according to [20], as the driver has to monitor lateral and longitudinal motion. Autonomous DAS (A-DAS) in [25] has the same meaning as fully automated according to [20], as the driver does not need to constantly monitor the system and the system can attain a safe state on its own. According to [24], a safe state is attained by stopping at a nonhazardous location. As the focus is on a system for automated driving in traffic jams on the freeway up to 60 km/h (approx. 37 mph), stopping on a lane until a human takes over control appears as a safe state. The relative speeds are assumed to be low due to the traffic jam [24, 25].

A study on the potential of automated driving on freeways comes to the same conclusion [45]. This was drawn up as part of the development of an accident assistance system that can stop a vehicle (safe state) in the event of the driver losing consciousness or not being able to guide the vehicle for other reasons [32, 45]. Such a system is also presented in [37]. The safety requirements here are higher than those for a traffic jam assistance system, as the vehicle is not supposed to simply stop but leave flowing traffic
and come to a standstill on the shoulder. In addition the system was designed for normal freeway traffic and not for traffic jams, meaning the very high relative speeds can come into play. This means that the requirements of the system are very high in terms of reliability and environment/situation recognition, as other drivers/vehicles must be observed when changing lanes onto the shoulder [45]. Redundant sensors that cover at least the areas in front, to the rear and in countries that drive on the right, to the right side of the vehicle are required here. The benefits of such emergency assistance systems are still present even if the system is not fully available due to technical defects. A vehicle that is out of control on the freeway is more dangerous than a vehicle moving slowly or at a standstill that is indicating in a suitable manner—even if switching lanes to the shoulder is not possible [32, 37].

In summary, it is possible to say that, if a driver is present in the vehicle, driver assistance systems can attain a safe state by handing control to the driver or by braking to a standstill. The emergency assistance systems mentioned here can attempt to reach the shoulder, however the requirements for this are relatively high. Even with systems with higher levels of automation, handing over control to a driver who may be in the vehicle and braking to a standstill comprise possible ways in which a safe state can be attained.

### 23.1.2 Safe State in Experimental Autonomous Vehicles

The following projects focus on autonomous vehicles on all types of roads and in all environments. The developed systems should be able to take on the task of driving completely and no longer require humans for monitoring purposes. There are only a few publications on safety functions and safety concepts of the various projects. This could be because it is relatively simple to deploy a human to monitor the vehicle and therefore not to make use of comprehensive safety systems and also because the functional safety of the systems for autonomous operation has not yet received the attention this field deserves. The projects taken into consideration are listed chronologically and the levels of automation according to [20] and the safety mechanisms used are highlighted.

The projects from the 1950s to the 1990s focused solely on the functional aspects of automatic vehicle guidance, such as the first attempts to link infrastructure and the vehicle in the General Motors Research Labs. This project involved implanting magnets in the road surface that the vehicle could detect. The driver was required to maintain a constant vigilance over the road traffic and the system [17]. In the 1970s and ’80s in Japan research was conducted in the field of vehicle automation with the recognition of driving lanes with imaging cameras. Again, the system was constantly monitored by the driver [58]. The same applies for the research conducted in the 90s, for example the experiment No hands across America 1995 of the Carnegie Mellon University [50, 56]. In this case only the lateral guidance of the vehicle was automated. In terms of research in Europe, a test drive conducted by the University of the Federal Armed Forces from Munich to Odense with the VaMoRs-P experimental vehicle (again in 1995) must be mentioned. During this trip,
the lateral and longitudinal guidance was conducted automatically and supervised by the driver. In addition, the automatic lane changes were initiated by the driver \cite{36}. The ARGO experimental vehicle of the VisLab Institute of the University of Parma achieved a long-distance record in 1998. The level of automation covered not only lateral and longitudinal guidance but also lane changes initiated by the monitoring driver \cite{7}. All of the named projects are to be classified as semi-automated according to \cite{20}. The safe state was achieved by handing vehicle control to a monitoring driver or restored by interventions by the monitoring driver. A comprehensive overview of the developments of the 1990s can be found in Dickmanns’s work \cite{14}. The focus here is on camera-based image processing.

The Autonomes Fahren (Autonomous Driving) project in Lower Saxony in 1998 also examined the development of autonomous vehicles. Binfe-Kull et al. \cite{6} describes a safety concept that involves various methods that are feasible and logical parts of today’s systems. Table 23.1 lists error codes, the meaning of which and resulting actions could be executed by the vehicle in order to attain a safe state. The selected categorization is also possible in terms of the definitions of \cite{20}. A detailed discussion of the actions will be given in the context of the respective safe states for the use cases in Chap. 2.

In the DARPA Urban Challenge, all participating autonomous vehicles without drivers were operated on an enclosed military base. The safety concept was prescribed by DARPA and included an option for immediately stopping a vehicle via remote control and by means of an emergency switch on the outside of the vehicle \cite{2}. The safety concept of the CarOLO team of the Technische Universität Braunschweig used the time after the emergency stop to conduct self-rectification actions \cite{19,22,44}. This allowed the autonomous vehicle to restart faulty components of the vehicle guidance system \cite{2}. The other teams also followed a similar approach in the final of the Urban Challenge \cite{51–53}.

Table 23.1 Error codes from \cite{6}

| Error code | Meaning | Action |
|------------|---------|--------|
| F0         | “OK!”   | No action |
| F1         | “Maintenance required” | Take account of necessary maintenance |
| F2         | “Return home” | Return to maintenance/service station with reduced speed |
| F3         | “Safe parking” | Stop at the next available parking space |
| F4         | “Immediate stop” | Stop the vehicle immediately at the side of the road without endangering other road users |
| F5         | “Emergency stop” | Immediate, controlled braking to a standstill with steering function, if possible |
| F6         | “Emergency braking” | Immediate stopping of the vehicle by activating the brakes |
Emergency stopping via remote control as a last resort to attain a safe state was only possible because the vehicles were driving in a secured area, followed by observation vehicles. The other road users were either vehicles driven by professional drivers or other autonomous vehicles. A test involving vehicles with the capabilities of the experimental vehicles involved on public roads would have been too dangerous.

The Stadtpilot project of the Technische Universität Braunschweig has demonstrated semi-autonomous vehicles on public roads since 2010 [41, 60]. The research of this project focuses on fully-automated operation of the experimental vehicle—Leonie. However, when driving on public roads a safety driver has to monitor traffic and intervene before dangerous situations can arise.

The vehicle guidance system transfers control of the vehicle to the safety driver if it reaches the limits of the system’s abilities or if system faults occur. As no other safety actions may be performed on public roads, the safe state is to transfer control to the driver. As the system is partially capable of determining its own performance, for example the quality of localization, other actions are then also possible. For example stopping at the side of the road or even on the current driving lane is feasible, continuing travel with greater distances to the vehicles ahead and with reduced speed is also possible, however, this has only been tested on test tracks [46, 47].

Stanford University and the Volkswagen Electronic Research Lab 2010 demonstrated automated driving with the Junior 3 experimental vehicle [35, 54]. The design of the experimental vehicle is similar to that of Leonie from the Stadtpilot project. Automated driving functions are controlled by silver switches. These facilitate a connection between the vehicle guidance system and the actuators of the vehicle. In the fail-safe state, these switches are open and there is no connection between the vehicle guidance system and the vehicle. This means that control is in the hands of the necessary safety drivers. One special feature is the valet parking function of the vehicle that can be used without a safety driver in a closed-off area. For safety purposes the vehicle has a so-called e-stop function that was used in a similar way to the one in the DARPA Urban Challenge. The vehicle guidance system is monitored by a health monitor that detects malfunctions of software modules and triggers self-rectification functions. In addition the vehicle is capable of operating the brakes and stopping independently. The stationary vehicle thereby attains the safe state via the e-stop and the safety system.

In 2012, the VisLab Institute of the University of Parma demonstrated semi-automated driving on public roads in a partially closed-off area with the BRAiVE experimental vehicle. On parts of the circuit there were no drivers in the driver’s seat and only the front passenger could intervene with an emergency stop button. An e-stop function was also integrated [8, 23].

After the DARPA Urban Challenge, work continued at Carnegie Mellon University on the BOSS experimental vehicle and an approach for monitoring and reconfiguration in real-time was developed and published [33]. This approach, called SAFER, uses redundant software components that are usually switched to stand-by in normal operation and they can be activated as required. This makes it possible to switch a defective component to a
redundant solution within a very short time. As no hardware monitoring takes place, no sensors and actuators are monitored, which means the approach can be used to supplement hardware redundancy methods.

The last example of current autonomous vehicles development projects is the *Self Driving Car* project of Google Inc. As a first step of this project, vehicles approaching a stage in which they are ready for series production were equipped with sensors and operated on public roads in Nevada and California [13, 59]. Even though there is only sparse information on the technology used in vehicles, use without safety drivers does not seem possible at present. As described in [13], there are numerous situations that make too many demands on the performance of the system. The safe state of these vehicles also means the driver taking control. In 2014 a prototype was presented without operating elements for the driver and therefore can certainly be classified according to [20] as fully automated, as there are no possibilities for overriding the controls. However, this vehicle has not been used on public roads to date.

### 23.1.3 Summary

As the projects described show, there is currently no comprehensive safety concept that covers all requirements of vehicles without safety drivers on public roads. However, some of the projects have demonstrated powerful safety functions that cover the different situations and events on the streets. If one assumes that in future the safe state is to attain the specifications of the “ADOPTED REGULATION OF THE DEPARTMENT OF MOTOR VEHICLES” section 16.2 (d) from Nevada, an autonomous vehicle must be capable of leaving the traffic flow at any time during the journey and stopping at the side of the road or on the shoulder [39]. This would require a lane change which in turn would depend on reliably functioning environment perception, decision-making and their implementation. Simply to stop as performed in some of the projects along with handing control of the vehicle to the safety driver, is not sufficient. The use of a combination of the preset vehicle safety function approaches seems therefore to be necessary—probably other safety measures need to be taken in order to attain a higher level of reliability [39].

### 23.2 Safety Concepts in Use in Series-Production in Other Disciplines

In addition to autonomous vehicles and driver assistance systems, functional safety also plays an important role in other technological areas. The following section details safety concepts from other disciplines and examines their suitability for autonomous vehicles.
23.2.1 Track Vehicles

Track vehicles have been operated automatically for several years already. On public transport vehicles, a train driver is present in most cases to monitor the function of the systems [66]. Unlike the autonomous vehicles under consideration here, safety functions are frequently integrated in the infrastructure, for example track usage is coordinated in centralized control centers and the monitoring components are integrated in the tracks. The control systems have the task of avoiding collisions by ensuring the track sections are only ever occupied by one train. This is implemented by sensors and systems (wayside centric), such as axle counters at the entrance and exit of a section of track [42]. If a section is occupied, the signals are switched accordingly to prevent another train entering. The avoidance of collisions is therefore primarily a logistical problem particular to traffic operation technology. The mechanical lateral guidance without any degree of freedom on rail vehicles reduces the complexity of the situations and the number of options for action. Put simply, it all comes down to trains driving along free sections of track at a suitable speed to avoid derailing. Monitoring the track in front of the train is not possible with surround sensors due to the long stopping distances. However trains and carriages have emergency stop functions that can be triggered by passengers and train drivers and even externally on driverless trains.

On driverless trains, the speed of the journey is regulated automatically and in addition to monitoring track occupancy by the infrastructure, the systems also have on-board mechanisms (vehicle-centric). Communication between the control center and the vehicle is performed via wireless technology in exactly the same way as communication between platforms and driverless underground trains. Here, a redundant door monitoring system on the platform and in the train can be used to prevent hazards arising from closing doors. The communication-based train control (CBTC) has become a standard that is used in numerous railway systems all over the world [42].

Such an automatic train driving system is used in the RUBIN underground system in Nuremberg. Traffic on the track is a mix of driverless trains and trains with drivers. An essential component of the safety concept is the monitoring of the doors [38]. Components of the automatic train protection systems (ATP) and automatic train operation (ATO) are used; these are divided between stationary and on-board components. With ATP the speed is kept below existing limits and safety stops and emergency stops are triggered. The system must therefore fulfill the requirements of safety integrity level 4 (highest safety level) according to the European standard IEC50128:2011 [29]. The necessary hardware and software is inexpensive in relation to the comparatively high costs of track vehicles compared with road vehicles.

---

3 Information on the RUBIN project of Siemens AG: http://www.siemens.com/innovation/en/publikationen/publications_pof/pof_spring_2008/tailored_solutions/fahrerlose_ubahn.htm.
23.2.2 Purely Electrical Control of Actuators (X-by-Wire)

On autonomous vehicles the actuators are triggered and controlled by means of electrical signals. Gas, brakes, steering and special functions are controlled by controllers. The X-by-Wire technology is not yet completely available in series-production vehicles. The electronic gas pedal, the electromechanical steering and the electrohydraulic brake system have been around for several years. However the steering and brakes still have a mechanical/hydraulic linkage that is mostly permanent and only available as a fallback in seldom cases if the electrical system fails. The driver can thereby control the vehicle even without the electronic systems.

For autonomous vehicles, the actuators must therefore have several redundant control circuits, as is the case in airplanes, for example. Both communications systems between operating elements, control devices and actuators as well as operating elements, control devices and actuators (including the energy supply) are installed multiple times so that in the event of a fault, the redundant systems can be used [3]. In [67], a threefold redundant control system for a Boeing 777 passenger airplane is presented. Each safety-relevant component of the airplane control system is implemented in three different ways to implement a high level of availability of the controls to the pilots or the autopilot. Due to the criticality of vehicle piloting, in addition to the autopilots on passenger planes, it is mandatory to have two human pilots [15].

The architecture used in airplanes and also the hardware and software used for implementing this would appear to also be suitable for use in vehicles. In airplanes, the high costs of such redundant systems are not so significant when looked at in relation to the high overall costs of the vehicle. For road vehicles, an analogous use of three-fold redundant systems would entail three times the investment in development and three times the amount of hardware compared to today’s systems in vehicles. It remains to be seen whether threefold redundancy of the systems is really necessary in vehicles.

In air traffic, the flight paths are assigned by a central air traffic control center and the autopilots keep to these prescribed routes. Therefore an autopilot in an airplane can be compared with a semi-automated driver’s assistance system, as the pilots have the duty of monitoring the system. On unmanned airplanes, the monitoring by the pilot is omitted and the requirements of the airplane guidance systems are greater. Risks are reduced by using flight paths that only fly over sparsely populated areas. As there are no persons on board, crashing into an empty field is a possibility as nobody will be injured [34].

---

4 In 2012, the vehicle manufacturer Nissan presented a steering system that created a mechanical connection via a coupling in the event of a fault: http://www.newsroom.nissan-europe.com/de/de-de/Media/Media.aspx?mediaid=97910.
23.2.3 Robotics

Mobile robots can pose a danger to themselves and their surroundings due to collisions with objects, persons and other living creatures and by overlooking ledges, ditches, steps, etc. [1, 10, 18]. Automated manipulators that are either used on stationary or mobile platforms can endanger people by moving their joints and colliding with the humans or by injuring them with the tools they are using. Therefore, for both the mobile robot and the manipulators, the safe state is the stopping of all manipulators in their current position or a standstill [5]. In most cases the following applies: the faster this happens, the lesser the danger that arises for the robot and its environment. Exceptions to this are tools and manipulators such as hands and grabbers that can apply pressure. Stopping the actuators could result in a pressure that can lead to injuries and damage. If a robot is used for complex activities, injuries and damage could occur that are not directly caused by the motion of the robot, but by the consequences of its actions. For example fires may be started if an ironing robot suddenly stopped moving or if hazardous goods were being transported by a mobile robot [64].

In [64, 65], a safety-orientated architecture for robot control systems is presented that contains a safety layer. This is intended to always transfer the robot to a safe state. The safe states depend on the functions the robots are to fulfill. These can vary greatly and therefore in [64, 65] safety policies are suggested that contain a hierarchical rule structure that enables the safe operation of a robot. It is conceivable that a robot can find an unexpected solution—depending on its degree of autonomy and its inherent capabilities—and this can result in dangerous situations. As described in [9], this can occur with the frequently used subsumption architecture. In relation to autonomous vehicles, this means that driving decisions can be taken according to different criteria such as traffic law, efficient driving style and comfort, but a collision avoidance system that can take action as the higher level authority would have to be active at all times.

23.2.4 Power Station Technology

Atomic power stations are largely regarded as a particular risk, as faults can lead to significant environmental damage. The control and regulation systems used there must therefore fulfill the highest safety requirements in order to enable operation even after natural catastrophes, terror attacks or internal technical faults. As immediate shut-down is not possible with atomic power stations, and the combustion elements remain active and require cooling even after their deployment in the reactor, many redundant systems are required, particularly for cooling.

The safety of an atomic power station largely depends on the complete and fault-free specification and development of the control and monitoring systems. Integrating the entirety of the possible situations and events plays an important role, as it is especially chain reactions and multiple faults that can lead to hazards. For example, the Fukushima
Daiichi atomic power station in Fukushima, Japan was in a fail-safe condition after the earthquake and all safety systems were correctly automatically activated. However, after the tsunami wave hit, parts of the redundant safety systems were damaged, in particular the emergency power units. With hindsight, we can say that the error was not in the failure of the safety functions, but instead lay in the incorrect specifications [63].

Therefore, for autonomous vehicles it can be said that the numerous events and combinations of events and error sources must be taken into account in the specifications stage. Possibly this will require a standardization of the requirements, comparable with that for atomic power stations. When they are developed, safety plays an essential role in the design phase and is the focus of the development process (safety by design, [26]).

23.3 Safe States in the Use Cases

One important criterion in the operation of an autonomous vehicle is whether there are passengers on board or not. For example, when choosing a parking space, it is not necessary to take the safe exit of passengers from the vehicle into account, however the safety of other road users cannot be forgotten. In addition comfort plays no role, meaning that a different driving style is possible in which comfort can be neglected. However, if passengers are on board, the vehicle guidance system must take over the tasks of a human driver. This also includes monitoring the passengers, for example if they are wearing their safety belts and are sitting on the passengers’ seats or if they are acting in a dangerous manner. Collisions with other road users can occur at any time and therefore passive safety mechanisms such as safety belts and airbags are also necessary in autonomous vehicles. The same applies to the securing of loads, especially hazardous goods.

The following section will investigate the four use cases defined for the project and examine the respective properties of the safe states.

23.3.1 Use Case 1: Interstate Pilot Using Driver for Extended Availability

By restricting use to freeways, the number of possible and probable situations is lower than compared to use in urban traffic. The safety driver is basically present as a fallback and is able to take control at any time and whenever he or she regards this as necessary. The vehicle is in a safe state in the following situations:

1. The vehicle is standing still. A stationary vehicle poses no active or immediate danger (see [6, 27]). However, the safety of passengers and other road users depends on the location of the vehicle:
   - Lane on a freeway: Due to the presence of a safety driver, continuing the journey with manual control is very probably possible. If continuing the journey with manual control is no longer possible, a stationary vehicle on a lane on a freeway
can become a dangerous situation as defined in error codes F5 and F6 in [6] (see Table 23.1). On the one hand the vehicle could be overlooked or seen too late, on the other hand because the passengers may have to leave the vehicle. Another danger can arise if the automated vehicle blocks a path for emergency vehicles in a traffic jam. If driving under manual control is no longer possible, the safety driver is obliged to secure the vehicle in accordance with the pertinent legal requirements, e.g. according to §15 StVO (German highway code) [11].

- Shoulders on a freeway or the curbside of a freeway where there is no shoulder, parking lot emergency stop bay or other similar location: If an automated vehicle is stranded on the shoulder of a freeway, at the curbside or another similar location, it may be possible that the safety driver can continue driving under manual control or he needs to secure the vehicle in accordance with the pertinent legal requirements (see error codes F2, F3 and F4 in [6]).

2. The vehicle drives on a lane at either prescribed distance or at a greater distance due to the vehicle’s performance to other road users and at least at the minimum prescribed speed, respectively the highest permitted speed or the highest possible speed the performance of the vehicle permits. The vehicle is aware of its own performance and can therefore detect the limits of the system independently.

3. The vehicle guidance system reacts with an action (see Sect. 23.5) to an event (see Sect. 23.4) to reduce the current risk. In this way a safe state should be attained or maintained—for example, by handing over control to the safety driver.

### 23.3.2 Use Case 2: Autonomous Valet Parking

In this use case the maximum speed of the vehicle is only low [approx. 30 km/h (approx. 19 mph)]. This means that the resulting energy that would be required to brake in the event of an emergency is considerably lower than the 50 km/h (approx. 31 mph) that is permitted in urban areas in Germany. Transferring control to a safety driver is not possible in this use case as the vehicle can be operated without a driver. The safety of passengers plays no role as no passengers are on board when the vehicle is driving. The intended route must be planned so that the vehicle does not drive on any roads that the vehicle does not have command of, for example streets with level crossings.

The vehicle is in a safe operational state in the following situations:

1. The vehicle is at a standstill: The location of the stopped vehicle is relevant as the vehicle could be a dangerous obstacle for other vehicles and block emergency vehicles and emergency escape paths. Securing the stopped vehicle is more difficult because no human is on board to take over this task. It would appear that only the lighting on the vehicle can be used to secure it. In many countries there are special regulations on securing broken-down vehicles, for example a warning triangle that has to be set up
several meters behind the vehicle. It is hard to imagine that this could be performed by an autonomous vehicle. Therefore, one or more persons must be responsible for this. The vehicle must either be constantly monitored or request help independently in the event that it is forced to stop.

2. The vehicle is driving on a lane on the road as described in use case 1. However it is not possible to transfer control to a safety driver as there is none on board. There is a possibility of stopping the vehicle and attaining a safe state in this way. It is also conceivable that in the event of a fault, control of the vehicle is transferred to a remote operator who then drives the vehicle to a safe location by means of remote control.

3. The vehicle drives through a crossing or roundabout or turns off. If the vehicle has command of the situation and the traffic priority rules applicable to the situation, these maneuvers are safe. If the vehicle reaches the limits of the system, it can continue driving at a reduced speed while signaling to the other road users.

4. The vehicle is on a parking lot. The low relative speeds and the comparatively low levels of traffic mean that the requirements are lower here and the operating risk is also lower.

The greatest challenge is the lack of a safety driver. In the case of events that increase the risk, it is not possible to transfer control to a safety driver and a standstill can have hidden risks in many situations as the vehicle cannot be moved immediately under manual control. One solution could be the remote operator. This requires a communications channel to the vehicle for reporting problems and for the remote control of the vehicle. If stopping is required, this must be signaled accordingly to the other road users. Securing the vehicle by the safety driver is not possible in this case.

Blocking emergency vehicle access and emergency escape paths on single-lane roads and access points for emergency vehicles in front of buildings and other facilities is a special case. Blockages can mean the emergency rescue actions are delayed or complicated. On the one hand this is illegal, on the other it is a major ethical consideration. The author is not aware of any investigations that show the frequency that such situations occur. Therefore it is not possible to state whether this case needs to be explicitly taken into consideration or not. Non-automated vehicles can also break down, however it is simpler for the driver of the vehicle to drive or push the vehicle out of the way in a quick and uncomplicated manner.

23.3.3 Use Case 3: Full Automation Using Driver for Extended Availability

The safety and risks of this use case are very similar to a combination of use cases 1 and 2. The presence of a safety driver means it is possible to hand over control. The driver can also secure the vehicle should it break down.
The necessary driving maneuvers and situations are the same as this in use cases 1 and 2. In addition, the vehicle is also used on interstate connections. The maximum speed in this use case is restricted to 240 km/h (approx. 149 mph). This means that practically every speed is feasible, however the maximum speed must always be selected so that it is within the performance capability of the vehicle guidance system and the risk is correspondingly reduced.

In terms of the safe state, the same conditions apply as in use cases 1 and 2.

### 23.3.4 Use Case 4: Vehicle on Demand

In terms of (safety) technology, this use case is the most challenging. The vehicle must be capable of handling every situation that a human might have to handle. The risk has to lie below a threshold of risk that is reasonable for the passengers and other road users. Both driving maneuvers and the conditions for the safe state can be taken from use cases 1, 2 and 3, taking into account that there is no safety driver.

The vehicle is in a safe state in the following conditions:

1. The vehicle is standing still as in use cases 1, 2 and 3. In each situation the vehicle requires external help. In addition to potential passengers, other persons are involved who have to be informed of the state of the vehicle and respond to vehicle problems.
2. The vehicle is driving on a traffic lane as in use cases 1, 2 and 3. While driving, the vehicle must be independently capable of maintaining or attaining a safe state.

Due to availability on demand and the universal usability, the vehicle on demand must be capable of handling all traffic situations. The safety-relevant events that require a reaction from the vehicle are examined in greater detail in the next section.

### 23.3.5 Summary

Examining the four use cases has shown that the greatest challenges for the safe state are posed by high relative speeds, the lack of a safety driver and blocking of emergency vehicle access routes and emergency escape paths. Examining these aspects allows the safety requirements for the vehicle to be derived:

- An autonomous vehicle must be aware of its current performance capabilities.
- An autonomous vehicle must be aware of its current functional limits in relation to the current situation.
- An autonomous vehicle must always be operated in a condition in which the level of risk is reasonable for the passengers and other road users.
- A vehicle that is standing on the shoulder or by the curbside and is not blocking traffic is in a safe state.
A vehicle that is standing on a traffic lane is only in a safe state if all of the following conditions are met:

- The relative speed to other road users is below a maximum still to be defined.
- The stationary vehicle is not blocking emergency vehicle access routes or emergency escape paths.
- A safety driver or remote operator can remove the vehicle from this location within a short time.
- A safety driver can secure the vehicle.

A vehicle moving with a high level of risk or one that has come to a standstill at a dangerous location must be capable of sending an emergency signal and requesting help.

### 23.4 Safety-Relevant Events

Various events can occur in road traffic that affect the risk in the current situation and in the future development of the situation. On the one hand, technical defects and faults in the vehicle guidance system reduce its performance capacity and on the other hand changes to environmental conditions, situations that overtax the vehicle guidance system, incorrect behavior of other road users and acts of force majeure all increase the requirements of the vehicle guidance system. In particular a combination of reduced capabilities and the increased demands can lead to higher levels of risk.

Defects and technical faults on the vehicle and in the vehicle guidance system can occur suddenly and are therefore very difficult to foresee. In addition to mechanical defects on the vehicle, defects and development errors in the vehicle guidance system can result in a reduced performance capacity (see [16]). Adverse light and weather conditions increase the requirements of the durability of the sensors used to detect the surroundings. In addition, adverse weather conditions lead to worse road conditions. These directly affect driving dynamics. Due to the complexity of road traffic and the endless quantity of possible situations, it is probable that not all situations will be taken into account when developing a vehicle guidance system. If the vehicle encounters a situation that cannot be resolved with the existing software, this has a direct influence on the risk level.

Recognizing the ability of the vehicle and the limits of the system is a great challenge in such situations. The behavior of other road users does not always conform to the rules and it may occur that they behave in a dangerous manner. In some situations, operation of an automated vehicle can never be safe because other road users act in a dangerous manner. It is conceivable that this may even occur deliberately if an automated vehicle is recognized as such. Force majeure can also pose a higher risk to operation, for example due to earthquakes or flash flooding or solar bursts that result in interference to the systems used such as a global satellite navigation system or vehicle-to-vehicle
Such events are not taken into consideration when developing driving assistance systems in accordance with ISO 26262 [30]. How they will be handled in autonomous vehicles remains open [61].

23.5 Measures for Reducing Risk Levels

Assuming that an autonomous vehicle is always to be operated with an acceptable level of risk and at the same time should have as wide a functional scope as possible, actions are to be performed as a reaction to safety-relevant events that reduce the risk to an acceptable level or retain this level and simultaneously enable a higher scope of functionality. A reduction of driving speed, an increase in distance to the vehicles in the vicinity, safety-optimized planning of driving maneuvers, prohibition of certain driving maneuvers, and the execution of safety maneuvers are all possible. The underlying principle of graceful degradation comes from the field of biology and was presented in [40]. In [68], among other things, there is an overview of the applications of graceful degradation in aerospace technology, power station technology and other research areas. If errors occur in one system or if resources are limited, the vital processes are maintained and other less important processes are scaled back or ended. For example, if the field of vision is restricted, the speed of the vehicle can be reduced. However, in certain conditions, even the execution of these actions cannot reduce the risk to an acceptable level, meaning that stopping the vehicle becomes necessary [25, 46], or if this is too risky, leaving the traffic flow.

With graceful degradation, it is not only necessary to attain or maintain a safe state but also to improve performance by using mechanisms for self-repair and reconfiguration. In technical systems restarting components is a widely-used measure for restoring performance [22, 44]. Restarting needs time and, depending on the system structure, it can occur that restarting a component also means restarting or at least re-initialization of other components. Therefore safety-critical components often have (diverse) redundant designs (see [3, 28]).

In addition to redundancy there is also the possibility of restoring functionality for individual components. Sensors and actuators can be re-calibrated to improve their measured values or set-points can be implemented depending on the current situation. Reconfiguration mechanisms can be used for the overall system that enable safe operation even after risk-increasing events [33].

Recognizing risky situations is a challenge. External events must be detected and correctly interpreted by the environmental monitoring system. Technical faults on the vehicle and in the vehicle guidance system must also be detected. A driver uses his or her senses to observe warning and monitoring lamps and notices changes in the vehicle, for example due to technical defects. An autonomous vehicle must therefore integrate sensors and functions that detect faults and errors and determine the future performance level and possible scope of function on the basis of the severity of these faults and errors. The
complexity to be expected of a vehicle with a vehicle guidance system will lead to a large number of measured values. As a result, a self-representation of the vehicle will be created that will be used to create an evaluation of the current risk that depends on the situation and the performance capability. The so-called safety actions are performed on the basis of this evaluation [46].

### 23.6 Anticipation of Degradation Situations

Due to the highly dynamic nature of road traffic and the properties of electric and electronic systems, safety-relevant events can occur in a fraction of a second and therefore require a fast response from the system. However, it is better if situations in which high levels of risk are present can be foreseen or at least taken into consideration when planning driving maneuvers. **Anticipatory driving** by humans can be implemented in an even more wide-ranging manner in a vehicle guidance system as the monitoring and application of numerous measured values is performed directly from the vehicle.

All of the collected measured value data must be monitored and stored to predict how situations will develop. The broad scope of the data analysis could allow incipient errors to be detected. Even detecting difficulties a few tenths of a second before the event can lead to a safer reaction. A necessary braking maneuver that has been detected and triggered 0.3 s earlier can shorten the stopping distance by 4.2 m at a speed of 50 km/h (approx. 31 mph).

Communications with the infrastructure and other vehicles yields further potential for increasing safety. The sooner information on hazards is available, for example road surface damage, dirt and ice, traffic jams ahead or emergency brake maneuvers of vehicles ahead on the road, the sooner a response to these can be initiated.

### 23.7 Dilemmas

In some cases, a chain of events can lead to a situation that cannot be resolved without personal injuries. When faced with a dilemma, an automated vehicle must select a possible course of action, which even though it will result in personal injuries, will cause the minimum amount of damage. Material damage and road traffic law infringements are also possible, however these have lower priority. The number of passengers on board and the type and dynamics of other road users must be taken into account in the evaluation of possible uncertainties. Communication with other road users is particularly important here and can help to resolve such situations with the minimum amount of personal injuries.5

---

5 The DFG priority program “Kooperativ interagierende Fahrzeuge” [Cooperatively Interactive Vehicles] will research this field in the coming years: http://www.dfg.de/foerderung/info_wissenschaft/info_wissenschaft_14_34/.
A detailed ethical discussion of dilemmas can be found in Chap. 4 of this book. Therefore, the following section will solely focus on the technical aspects of dilemma situations.

Figure 23.1 shows two situations. The first can be resolved without a collision. The second can lead to a dilemma. At the start of the first situation, the vehicle is driving on a road lane and other vehicles are parked by the side of the road. Unexpectedly a person, who is barely discernible, steps between the parked cars and onto the road. The vehicle can respond in several different ways to avoid a collision with the pedestrian. Option 1: The vehicle can brake and stop before hitting the pedestrian. Option 2: The vehicle can switch to the neighboring road lane and thus avoid a collision. However, this requires crossing a continuous line between the road lanes. This would infringe road traffic law.

---

**Fig. 23.1** Example of two situations that could cause a dilemma. Image rights: Copyright off the Author
In the second situation a vehicle is driving in the oncoming direction on the second road lane. If one assumes that a braking maneuver will no longer prevent a collision with the pedestrian, the autonomous vehicle is facing a dilemma:

Colliding with the pedestrian could result in serious injuries to the pedestrian (option 2). Switching to the neighboring lane will result in a collision with the oncoming vehicle and possibly also result in injuries to the pedestrian (option 3). A collision with the parked vehicles to reduce the vehicle’s own speed is also feasible (option 4), however it would remain highly uncertain as to whether the pedestrian would emerge uninjured from the situation. In such situations the decision-taking software within the vehicle guidance system will have to be programmed with ethical principles.

Vehicle-to-vehicle communication between the autonomous and oncoming vehicle could solve at least this problem. The two vehicles could find a solution together. The oncoming vehicle could switch to the edge of the lane so that the autonomous vehicle can pass between the oncoming vehicle and the pedestrian without a collision occurring (option 5). Both vehicles would infringe road traffic law in this situation as both must cross a continuous line.

However, operation without communications with other road users and the infrastructure must also be possible as it is unlikely that these communication options will be available everywhere and for all road users.

Vehicle guidance must therefore be possible with the on-board sensors. This on-board autonomous operation (see [36]) makes the highest requirements of the vehicle guidance system on the one hand and on the other hand is also currently the only possible option for use in road traffic. This restricts options, especially in situations involving danger and dilemmas and increases the uncertainty in perceiving situations. Signalization to other road users is only possible in an optical and acoustic manner.

### 23.8 Summary

In the current state of development of driving assistance systems and related research and development areas, there are a wide variety of methods that could and possibly must be used in the development of autonomous vehicles. The wide range of technology means that these systems affect different areas of the development process and the system to be developed and also that they can contribute to the safety of autonomous vehicles.

First a metric must be found with which the operating risk of autonomous vehicles can be evaluated and then a generally acceptable risk threshold must be defined. The procedure used in power station development for determining the safety requirements and integrating functional safety in the overall system could be useful in this area.

In terms of the functional safety of the regulation of actuators, examples form aeronautics and aerospace and partially rail travel can be used in the current research and development of vehicle technology. Multiple, diverse redundancy is one of the most promising means. The same applies for software components for situation analysis,
decision-making and motion planning. Until now only the field of robotics has been faced with similarly complex situations. However, the level of risk there is mostly lower.

One of the biggest challenges is the reliability and dependability of environment perception systems that also include self-perception and situation perception. Due to the infinite quantity of possible situations, as far as the author is aware, it has not yet been possible to implement complex applications—as described in the use cases—in a safe manner. This will also require hardware, software and functional redundancies, for example in the composition of the sensors for perceiving the immediate environment.

A safety driver is still required in research projects for autonomous vehicles. This person monitors the system and can either take action directly or use remote emergency stop functions or an emergency stop switch. The research projects considered currently focus heavily on functions and less on their functional safety.

The safety of autonomous vehicles is one of the basic challenges of future research. The development of the technology not only requires the resolution of technical problems, but also legal and social problems. A large proportion of these will be discussed and examined in the later chapters of this book.

Open Access This chapter is distributed under the terms of the Creative Commons Attribution 4.0 International License (http://creativecommons.org/licenses/by/4.0/), which permits use, duplication, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, a link is provided to the Creative Commons license and any changes made are indicated.

The images or other third party material in this chapter are included in the work’s Creative Commons license, unless indicated otherwise in the credit line; if such material is not included in the work’s Creative Commons license and the respective action is not permitted by statutory regulation, users will need to obtain permission from the license holder to duplicate, adapt or reproduce the material.

References

1. Albers, A., Brudniok, S., Ottnad, J., Sauter, C., Sedchaicharn, K. (2006). Upper Body of a new Humanoid Robot - the Design of ARMAR III. 6th IEEE-RAS International Conference on Humanoid Robots, pp. 308-313. Genoa, Italy.
2. Basarke, C., Berger, C., Rumpe, B. (2007). Software & Systems Engineering Process and Tools for the Development of Autonomous Driving Intelligence. Journal of Aerospace Computing, Information, and Communication (JACIC), 4(12), pp. 1158-1174.
3. Bergmiller, P., Maurer, M., Lichte, B. (2011). Probabilistic fault detection and handling algorithm for testing stability control systems with a drive-by-wire vehicle. 2011 IEEE International Symposium on Intelligent Control (ISIC), pp. 601-606. Denver, CO, USA.
4. Bertozzi, M., Broggi, A., Coati, A., Fedriga, R. I. (2013). A 13,000 km Intercontinental Trip with Driverless Vehicles: The VIAC Experiment. Intelligent Transportation Systems Magazine, 5(1), pp. 28-41.
5. Bicchi, A., Peshkin, M. A., Colgate, J. E. (2008). Safety for Physical Human-Robot Interaction. In B. Siciliano, O. Khatib (Hrsg), Springer Handbook of Robotics, pp. 1335-1346. Springer-Verlag Berlin Heidelberg.
6. Binzet-Kull, M., Heitmann, P., Ameling, C. (1998). System safety for an autonomous vehicle. 1998 IEEE Intelligent Vehicles Symposium (IV), Stuttgart, Germany.
7. Broggi, A., Bertozzi, M., Fascioli, A. (1999). ARGO and the MilleMiglia in Automatico Tour. Intelligent Systems and their Applications, 14(1), pp. 55-64.
8. Broggi, A., Buzzoni, M., Debattisti, S., Grisleri, P., Laghi, M. C., Medici, P., Versari, P. (2013). Extensive Tests of Autonomous Driving Technologies. IEEE Transactions on Intelligent Transportation Systems, 14(3), pp. 1403-1415.
9. Brooks, R. A. (1986). A robust layered control system for a mobile robot. IEEE Journal of Robotics and Automation, 2(1), pp. 14-23.
10. Bubeck, A., Weisshardt, F., Sing, T., Reiser, U., Hägele, M., Verl, A. (2012). Implementing best practices for systems integration and distributed software development in service robotics - the Care-O-bot® robot family. IEEE/SICE International Symposium on System Integration (SII), pp. 609-614. Fukuoka, Japan.
11. Bundesministerium der Justiz, für Verbraucherschutz. (2013). Straßenverkehrs-Ordnung. Bonn, Germany.
12. Carrano, C. S., Bridgwood, C. T., Groves, K. M. (2009). Impacts of the December 2006 solar radio bursts on the performance of GPS. Radio Science, 44 (RS0A25).
13. Chatham, A. (2013). Google’s Self Driving Cars: The Technology, Capabilities, Challenges. Embedded Linux Conference. San Francisco, CA, USA.
14. Dickmanns, E. D. (2002). The development of machine vision for road vehicles in the last decade. 2002 IEEE Intelligent Vehicles Symposium (IV). Versailles, France.
15. EASA. (2013). EASA LIST OF CLASS OR TYPE RATINGS AEROPLANES. Cologne, Germany.
16. Echtle, K. (1990). Fehlerfortpflanzungverfahren. Springer-Verlag Berlin Heidelberg.
17. Fenton, R. (1970). Automatic vehicle guidance and control - A state of the art survey. Transactions on Vehicular Technology, 19(1), pp. 153-161.
18. Fischer, H., Voges, U. (2011). Medizinische Robotersysteme. In R. Kramme (Hrsg), Medizintechnik, pp. 915-926. Springer-Verlag Berlin Heidelberg.
19. Ganek, A., Corbi, T. (2003). The Dawning of the Autonomic Computing Era. IBM Syst. J., 42 (1), pp. 5-18.
20. Gasser, T. M., Arzt, C., Ayoubi, M., Bartels, A., Bürkle, L., Eier, J., Flemisch, F., Häcker, D., Hesse, T., Huber, W., Lotz, C., Maurer, M., Ruth-Schumacher, S., Schwarz, J., Vogt, W. (2012). Rechtsfolgen zunehmender Fahrzeugautomatisierung : gemeinsamer Schlussbericht der Projektgruppe. Wirtschaftsverlag NW, Verlag für neue Wissenschaft.
21. Geyer, S. (2013). Entwicklung, Evaluierung eines kooperativen Interaktionskonzepts an Entscheidungspunkten für die teilautomatisierte, manöverbasierte Fahrzeugführung. Phd thesis, Technische Universität Darmstadt, VDI Reihe 12 Band 770
22. Ghosh, D., Sharman, R., Raghav Rao, H., Upadhyaya, S. (2007). Self-healing systems - survey and synthesis. Decision Support Systems in Emerging Economies, 42(4), pp. 2164-2185.
23. Grisleri, P., Fedriga, I. (2010). The Braive Autonomous Ground Vehicle Platform. IFAC Symposium on intelligent autonomous vehicles, 7. Lecce, Italy.
24. Hörlück, M. (2011). Sicherheitskonzept für hochautomatisierte Fahrerassistenzsysteme. Phd thesis, Technische Universität München.
25. Hörlück, M., Siedersberger, K.-H. (2010). Strategy and architecture of a safety concept for fully automatic and autonomous driving assistance systems. 2010 IEEE Intelligent Vehicles Symposium (IV), pp. 955-960. San Diego, CA, USA.
26. IAEA. (2012). Safety of Nuclear Power Plants: Design - Specific Safety Requirements No. SSR-2/1. Safety of Nuclear Power Plants: Design - Specific Safety Requirements No. SSR-2/1, Wien, Austria.
27. Isermann, R. (2006). Fault-Diagnosis Systems: An Introduction from Fault Detection to Fault Tolerance. Springer-Verlag Berlin Heidelberg.

28. Isermann, R., Schwarz, R., Stözl, S. (2002). Fault-tolerant drive-by-wire systems. IEEE Control Systems, 22(5), pp. 64-81.

29. ISO. (2011). EN 50128:2011 Railway applications - Communication, signalling and processing systems - Software for railway control and protection systems. EN 50128:2011 Railway applications - Communication, signalling and processing systems - Software for railway control and protection systems (EN 50128). Geneve, Switzerland.

30. ISO. (2011). ISO 26262:2011 Road vehicles – Functional safety. ISO 26262:2011 Road vehicles – Functional safety (ISO 26262). Geneve, Switzerland.

31. Kammel, S., Ziegler, J., Pitzer, B., Werling, M., Gindele, T., Jagzent, D., Schröder, J., Thuy, M., Goebi, M., von Hadelnhausen, F., Pink, O., Frese, C., Stiller, C. (2008). Team AnnieWAY’s autonomous system for the 2007 DARPA Urban Challenge. Journal of Field Robotics, 25(9), pp. 615-639.

32. Kämpchen, N., Walldmann, P., Homm, F., Ardelt, M. (2010). Umfelderfassung für den Notfallassistenten – ein System zum automatischen Anhalten bei plötzlich reduzierter Fahrfähigkeit des Fahrers. AAET 2010, Braunschweig, Germany.

33. Kim, J., Rajkumar, R., Jochim, M. (2013). Towards Dependable Autonomous Driving Vehicles: A System-level Approach. SIGBED, 10(1), pp. 29-32.

34. Korn, B., Tittel, S., Edinger, C. (2012). Stepwise integration of UAS in non-segregated airspace-The potential of tailored uas atm procedures. Integrated Communications, Navigation and Surveillance Conference (ICNS), p 1-8. Herndon, VA, USA.

35. Levinson, J., Askland, J., Becker, J., Dolson, J., Held, D., Kammel, Kolter, J. Z., Langer, D., Pink, O., Pratt, V., Sokolsky, M., Stanek, G., Stavens, D., Teichman, A., Werling, M., Thrun, S. (2011). Towards fully autonomous driving: Systems and algorithms. 2011 IEEE Intelligent Vehicles Symposium (IV), pp. 163-168. Baden-Baden, Germany.

36. Maurer, M. (2000). Flexible Automatisierung von Straßenfahrzeugen mit Rechnersehen. VDI-Verlag.

37. Mirwaldt, P., Bartels, A., Lemmer, K. (2012). Gestaltung eines Notfallassistenzsystems bei medizinisch bedingter Fahrunfähigkeit. 5. Tagung Fahrerassistenz. Munich, Germany.

38. Müller, R. (2003). Das Projekt RUBIN - Automatische U-Bahnen ab 2006 in Nürnberg: Mehr Service, niedrigere Kosten im Nahverkehr. 19th Dresden Conference on Traffic and Transportation Science. Dresden, Germany.

39. NDMV. (2012). Adopted Regulation of the Department of Motor Vehicles LCB File No. R084-11. Carson City, NV, USA.

40. Norman, D. A., Bobrow, D. G. (1975). On data-limited and resource-limited processes. Cognitive Psychology, 7(1), pp. 44-64.

41. Nothdurft, T., Hecker, P., Ohl, S., Saust, F., Maurer, M., Reschka, A., Böhmer, J. R. (2011). StadtPilot: First fully autonomous test drives in urban traffic. 2011 IEEE International Annual Conference on Intelligent Transportation Systems (ITSC), pp. 919-924. Washington DC, USA.

42. Pascoe, R. D., Eichorn, T. N. (2009). What is communication-based train control? IEEE Vehicular Technology Magazine, 4(4), pp. 16-21.

43. Pellkofer, M. (2003). Verhaltensentscheidung für autonome Fahrzeuge mit Blickrichtungssteuerung. Phd thesis, Universität der Bundeswehr München.

44. Psaijer, H., Sustead, S. (2011). A survey on self-healing systems: approaches and systems. Computing, 91(1), pp. 43-73.

45. Rauch, S., Aeberhard, M., Ardelt, M., Kämpchen, N. (2012). Autonomes Fahren auf der Autobahn – eine Potentialstudie für zukünftige Fahrerassistenzsysteme. 5. Tagung Fahrerassistenz. Munich, Germany.
46. Reschka, A., Böhmer, J. R., Nothdurft, T., Hecker, P., Lichte, B., Maurer, M. (2012). A Surveillance and Safety System based on Performance Criteria and Functional Degradation for an Autonomous Vehicle. 2012 IEEE International Conference on Intelligent Transportation Systems (ITSC), pp. 237-242. Anchorage, AK, USA.
47. Reschka, A., Böhmer, J. R., Saust, F., Lichte, B., Maurer, M. (2012). Safe, Dynamic and Comfortable Longitudinal Control for an Autonomous Vehicle. 2012 IEEE Intelligent Vehicles Symposium (IV), pp. 346-351. Alcalá de Henares, Spain.
48. SAE International. (2014). Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems (J3016). SAE International.
49. Schopper, M., Henle, L., Wohland, T. (2013). Intelligent Drive - Vernetzte Intelligenz für mehr Sicherheit. ATZextra, 18(5), pp. 106-114.
50. Shladover, S. (2007). PATH at 20 - History and Major Milestones. Transactions on Intelligent Transportation Systems, 8(4), pp. 584-592.
51. Singh, S. (2008). Special Issue on the 2007 DARPA Urban Challenge Part I (Vol. 25). Wiley Subscription Services, Inc.
52. Singh, S. (2008). Special Issue on the 2007 DARPA Urban Challenge Part II (Bd. 25). Wiley Subscription Services, Inc.
53. Singh, S. (2008). Special Issue on the 2007 DARPA Urban Challenge Part III (Bd. 25). Wiley Subscription Services, Inc.
54. Stanek, G., Langer, D., Müller-Bessler, B., Huhnke, B. (2010). Junior 3: A test platform for Advanced Driver Assistance Systems. 2010 IEEE Intelligent Vehicles Symposium (IV), pp. 143-149. San Diego, CA, USA.
55. Stiller, C., Färber, G., Kammel, S. (2007). Cooperative Cognitive Automobiles. 2007 IEEE Intelligent Vehicles Symposium (IV). Istanbul, Turkey.
56. Thorpe, C., Jochem, T., Pomerleau, D. (1997). The 1997 automated highway free agent demonstration. 1997 IEEE Conference on Intelligent Transportation Systems (ITSC). Boston, MA, USA.
57. Thuy, M., Goebl, M., Rattei, F., Althoff, M., Obermeier, F., Hawe, S., Nagel, R., Kraus, S., Wang, C., Hecker, F., Russ, M., Schweitzer, M., Leon, F.P., Färber, G., Buss, M., Diepold, K., Eberspächer, J., Heißing, B., Wünsche, H.-J. (2008). Kognitive Automobile - Neue Konzepte und Ideen des Sonderforschungsbereichs/TR28. 3. Tagung Aktive Sicherheit durch Fahrerassistenz. Garching b. München, Germany.
58. Tsugawa, S. (1994). Vision-based vehicles in Japan: machine vision systems and driving control systems. Transactions on Industrial Electronics, 41(32), pp. 398-405.
59. Urmson, C. (2012). Realizing Self-Driving Vehicles. 2012 IEEE Intelligent Vehicles Symposium (IV). Alcalá des Henares. Spanien.
60. Wille, J. M., Saust, F., Maurer, M. (2010). Stadtpilot: Driving autonomously on Braunschweig’s inner ring road. 2010 IEEE Intelligent Vehicles Symposium (IV), pp. 506-511. San Diego, CA, USA.
61. Winkle, T., Gasser, T. M. (2014). E-Mail Communication.
62. Winner, H., Danner, B., Steinle, J. (2009). Adaptive Cruise Control. In Handbuch Fahrerassistenzsysteme, p 478-521. Wiesbaden: Vieweg&Teubner | GWV Fachverlage GmbH.
63. WNA. (2014). Fukushima Accident. Tech. rep., World Nuclear Association.
64. Woodman, R., Winfield, A. F., Harper, C., Fraser, M. (2010). Safety control architecture for personal robots: Behavioural suppression with deliberative control. The Seventh IARP Workshop on Technical Challenges for Dependable Robots in Human Environments. Toulouse, France.
65. Woodman, R., Winfield, A. F., Harper, C., Fraser, M. (2012). Building safer robots: Safety driven control. The International Journal of Robotics Research, 31(13), pp. 1603-1626.
66. Yasunobu, S., Miyamoto, S. (1985). Automatic Train Operation System by Predictive Fuzzy Control. In M. Sugeno (Hrsg), Industrial Applications of Fuzzy Control, pp. 12-29. Elsevier Science Publishers B.V. (North-Holland).

67. Yeh, Y. (1996). Triple-triple redundant 777 primary flight computer. 1996 IEEE Aerospace Applications Conference, pp. 293-307. Aspen, CO, USA.

68. Zhang, Y., Jiang, J. (2008). Bibliographical review on reconfigurable fault-tolerant control systems. Annual Reviews in Control, 32(2), pp. 229-252.

69. Ziegler, J., Bender, P., Lategahn, H., Schreiber, M., Strauß, T., Stiller, C. (2014). Kartengestütztes automatisiertes Fahren auf der Bertha-Benz-Route von Mannheim nach Pforzheim. Workshop Fahrerassistenzsysteme. Walting, Germany.