Chapter 11
System Architecture and Safety Requirements for Automated Driving

Jan Becker, Michael Helmle, and Oliver Pink

11.1 Toward Automated Driving

Assisted driving functions already support the driver today by taking over either the longitudinal or the lateral driving task in specific situations. Examples are Adaptive Cruise Control or Lane Keeping Support. While these functions support the driver with regard to the longitudinal or lateral vehicle guidance within defined situations, handover of control back to the driver is required in case functional system boundaries are reached or a critical fault is detected. Therefore, the driver has to remain available all the time and provide fallback and recovery by means of human intervention.

Automated driving introduces the first driving functions that will carry out both longitudinal and lateral control tasks simultaneously and allow the driver to be absent from the active driving task for a limited amount of time. The driver will be responsible for permanently supervising partially automated functions, which is not required for highly and fully automated functions.

Different approaches exist on how to reach fully automated driving. One strategy is to incrementally increase the amount of automation for the respective function. For example, adaptive cruise control on highways is followed by combined longitudinal and lateral control with the driver constantly supervising the function. This is followed by highly automated driving where the driver may perform side tasks while driving, followed ultimately by fully automated driving on highways. Another approach is to jump directly to fully automated driving while significantly limiting

\[ J. \text{ Becker} \]
Robert Bosch LLC, Palo Alto, CA, USA
\text{e-mail: Jan.Becker@us.bosch.com}

\[ M. \text{ Helmle} \text{ • O. Pink} \]
Robert Bosch GmbH, Gerlingen-Schillerhöhe, Germany

© Springer International Publishing Switzerland 2017
D. Watzenig, M. Horn (eds.), Automated Driving,
DOI 10.1007/978-3-319-31895-0_11
velocity, e.g., to 25 km/h. For a detailed discussion on the different strategies and their implications the reader is referred to [1].

Below, we will adopt the incremental view and introduce a set of driving functions with increasing degree of automation to set the stage for the technical discussion. The functions referred to serve as a set of example specifications which are currently not standardized and represent a subset of possible future automated functions. We expect wide-scale introduction of automated driving in well-defined situations and restricted environments first. For example, a freeway provides an environment with unidirectional traffic flow, whereas urban driving scenarios include cross-traffic situations, pedestrians, and bicyclists. Consequently, the requirements on perception, situation recognition, and decision making are considerably higher in a more complex environment.

Figure 11.1 shows our expectation of the evolution of automated driving. For a detailed taxonomy of automated driving functions, we refer to [2]. Our vision for automated driving can be seen in [3] and, more specifically, how a user may experience a highway pilot system is shown in [4].

Therefore, we are expecting a function such as the traffic jam pilot to be the first highly automated driving function deployed to the market, followed by the highway pilot. Both functions will be restricted to highway-like environments. Below, we present a brief functional description of these two exemplary driving functions. The function definitions given here are tentative and serve as examples to derive requirements regarding the onboard network but are far from being standardized and, therefore, are subject to changes in definition.

Fig. 11.1 Examples for automated highway driving functions according to the level of automation: Adaptive Cruise Control and Lane Keeping Support function are examples for assisted functions (level 1); Integrated Cruise Assist and Highway Assist are examples for partial automation (level 2). The highway pilot and autopilot resemble high and full automation, respectively (level 3 and 4)
11.1.1 Traffic Jam Pilot

The traffic jam pilot is designed to provide automated guidance of the vehicle in situations with traffic congestions on highway-like road environments. This requires combined lateral and longitudinal guidance of the vehicle at velocities typically less than 60 km/h on roads with more than one lane per driving direction, wide lanes, and low curvature. Lateral guidance aims at keeping the vehicle in the current lane; automated lane changes are not supported. Longitudinal guidance aims at keeping a safe distance to the preceding vehicle. In case a system boundary is reached, the driver is requested to take over control of the vehicle. If the driver is not responding accordingly within a defined time limit, the system will start switching to the safe state.

11.1.2 Highway Pilot

The highway pilot will extend the traffic jam pilot to higher velocities of up to 130 km/h and to situations without surrounding vehicles. In addition, automated lane change maneuvers and finer lateral guidance within the ego lane are provided, resulting in a more comfortable distance to adjacent vehicles. Another evolution of the highway pilot is represented by the exit to exit function. It implements functional features such as transitions from one highway to another highway, including on-ramps and off-ramps. This allows the driver to enter a city area as target destination in the vehicle navigation system, and the pilot function automatically selects relevant combinations of highways to reach that destination. We refer to [4] for a potential implementation of such a highway pilot system.

11.2 System Architecture

The use cases in the previous section enable us to define requirements for individual components of an automated driving system. While an automated driving function does not necessarily have to cover all situations, it is desirable to cover as many as possible in order to obtain higher availability of the function and less frequent takeover requests to the driver. Furthermore, in case of the occurrence of any unforeseen situation, the function must be able to handle the situation until the driver has taken back control.

Similarly, in case of hardware failures, the system needs to stay operational, at least with reduced functionality, until the driver has taken back control. This imposes additional requirements on the sensor set, electronic control units (ECUs), communication network, power supply, and actuators [5].
The use cases to be covered by a respective function typically have an impact on all components. For example, snowfall can lead to limited sight of the sensors, will affect a surround-sensor-based localization system due to different appearance of the surroundings, may require decision making to drive more slowly, and causes a low friction road surface which requires appropriate motion control capabilities [6].

Technical solutions for automated driving have been developed during the 2007 DARPA Urban Challenge [7] and have been improved since [8–10]. These systems need to be further extended in order to be capable of handling all situations that occur in real traffic. In the following sections, the impact of handling the aforementioned use cases will be detailed for some of the key components of an automated driving system.

Figure 11.2 shows a simplified functional architecture for highly automated driving. Functional redundancy is employed on the sensor and actuator level.

### 11.2.1 Surround Sensors

The surround sensor set for automated highway driving must be capable of reliably detecting all relevant obstacles in any situation the vehicle may encounter. In addition to physical redundancy for handling, e.g., hardware failures, this requires a diverse sensor set with different sensing technologies. Even under adverse circumstances, relevant obstacles have to be detected by at least one sensor. Sensors have to fulfill different requirements in different areas around the vehicle. The detection range and reliability in each area are defined by the respective most challenging use case.

For the front sensor set, this could be a comfortable stop behind a standing vehicle, given that there is no oncoming traffic on highways, for example, the rear
end of a traffic jam. The object detection reliability is dependent on the distance from a vehicle ahead. Late detection of a slow vehicle ahead will lead to a harder and potentially uncomfortable braking maneuver. However, any potentially harmful object has to be detected early enough so that an emergency maneuver can be triggered. Consequently, the area guaranteed to be free of potentially harmful obstacles needs to be determined, and the vehicle must be able to perform a potential emergency maneuver within this area.

For the rearwards facing sensors, the most challenging use case encountered on highways is typically a fast approaching vehicle from behind with an approaching speed of up to 250 km/h.

For the side sensor set, the detection range is defined by the lane change use case and has to cover an area around the vehicle large enough to ensure that the neighboring lane is free. Consequently, the detection range has to cover at least two adjacent lanes to the left and two adjacent lanes to the right of the vehicle.

Figure 11.3 shows an exemplary sensor set for highly automated driving.

### 11.2.2 Perception

The main goal of the perception system is to combine all sensor measurements into a consistent representation of the surrounding world. There are many fusion algorithms proposed to this end. They can be categorized into object-level fusion, where each individual sensor delivers object hypotheses which are combined in a subsequent fusion step, e.g., [11], and feature-level fusion, where lower-level sensor data is directly used to update a world model, e.g., a grid or particle representation [12]. In general, the output of any fusion system is an obstacle representation, for example, an occupancy grid or an object list or a combination of both.
In addition to a representation of all known obstacles, perception also needs to provide a notion of the unknown for many use cases. For example, if the field of view is limited due to fog or obstructions, the system needs to adapt its speed accordingly, because there may be undetected obstacles outside the field of view. Instead of explicitly modeling the “knownness,” our perception system computes and outputs a “free space,” known to be free of obstacles. An area that is neither part of the free space nor part of an obstacle is considered unknown. The perception system uses measurements from the road surface and other clues, such as positions of detected obstacles, to determine the free space.

### 11.2.3 Localization

Localization is the process of estimating the vehicle position and orientation with respect to a given map. We distinguish three levels of localization precision:

- Road precision: On which road am I?
- Lane precision: On which lane am I?
- Sub-lane precision: Where within the lane am I?

The different levels are used at different steps during the decision making process. Localization on road level is required for function activation, e.g., if the function is limited to a certain set of roads, e.g., highways, and in order to determine the route from the current position to the desired destination. Lane-level localization is mainly required for lane change use cases, e.g., whether a lane change is possible or whether we have to change lanes in order to reach our navigation goal. Sub-lane level localization is required for maintaining the proper position within the lane. Unavailability of any of these localization levels may lead to degradation of the functional performance or even to a driver takeover request. For example, if the activation relies on road-level localization, it has to be available to offer the function to the driver. If lane localization is unavailable, lane changes may not be possible during this time. Special situations, such as driving in a tunnel or under a bridge, may lead to temporary unavailability of any of the aforementioned levels, even when using state-of-the-art satellite-based localization systems. To recover in these situations, we use surround-sensor information in addition to Global Navigation Satellite System (GNSS)-based information for localization. Such surround-sensor-based localization systems have been proposed for several sensor technologies (e.g., camera [13] or Lidar based [14]). Similar to the perception system, combining multiple sensing technologies increases the overall availability of the localization system. In order to guarantee a high availability, we are using a combination of all available sensing technologies for localization.
11.2.4 Decision Making

It is essential to adapt the behavior of an automated vehicle to the current driving situation, especially in challenging situations. This includes determining a safe maximum vehicle speed and safety distances for the current situation, for example, based on the current sensor viewing ranges, road surface condition, or the speed of other vehicles. Using the free space representation from the previous section, the maximum vehicle speed could be selected so that we can perform an emergency maneuver within the current free space.

Before executing any given maneuver, decision making also has to determine whether this maneuver can be performed safely in the respective situation. For example, lane changes will not be performed when fast vehicles are approaching from behind or if the vehicle is driving in a narrow curve where the field of view is limited.

Decision making is also responsible for following traffic rules. Essentially, the entire subset of local traffic rules [15, 16] that applies to highway driving needs to be implemented in the planning system. This differs significantly from country to country, which is illustrated by some of the rules that are implemented in our planning system for lane changes in the USA and Germany, respectively:

**USA:**

- Perform a lane change to another lane (left lane preferred but not mandatory) if the vehicle ahead is driving significantly slower than our desired speed.
- If approaching a highway split or exit, change onto a lane that continues toward our navigation goal.

**Germany:**

- Rightmost lane: Perform a lane change to the left if the vehicle ahead is driving significantly slower than our desired speed. Since passing other vehicles on the right-hand side is illegal, the same rule applies to any other vehicles ahead on our left-hand side.
- Middle lane(s): Perform a lane change to the left if the vehicle ahead in our lane (or in any lane left to us) is driving significantly slower than our desired speed. Change to the right if there is no vehicle in sight (the law states that continuous driving in the middle lane(s) is allowed if there is a vehicle in the rightmost lane “occasionally” present).
- Leftmost lane: Immediately change lanes back to the right if we can continue there with our desired speed for at least several seconds.
- If we approach a highway split or exit, the above rules apply to all lanes that continue toward our navigation goal. That is, if no other traffic is present, change onto the rightmost lane that continues toward our navigation goal.
- At speeds below 80 km/h, passing on the right-hand side with moderately higher speed is permitted.
In traffic jams, only change lanes if required (e.g., due to a lane ending), the rule of driving in the rightmost lane does not apply.

There are several additional rules related to lane changes that are not listed, for example, based on the distances and speeds of vehicles in the target lane. Our implementation makes use of a hierarchical state machine, which is a common approach for automated driving systems [17, 18]. Different driving behaviors, such as lane following or lane changing, are modeled as states. Maneuver decisions, including the aforementioned traffic rules, safety considerations, and interactions with other vehicles, are modeled as state transitions.

### 11.3 Functional Safety Concept

As one of the first activities in the safety lifecycle according to ISO 26262 [19], the hazard analysis and risk assessment (H&R) shall be conducted. As a result, the safety goals and the related ASIL ratings shall be defined.

For the traffic jam pilot, the hazard analysis and risk assessment yields among others the following safety goal: “Avoid insufficient vehicle deceleration when traffic jam pilot is active.” Evaluation of the severity of the possible harm (S3), exposure (E3), and controllability by the driver and other involved traffic participants (C3) leads to assignment of ASIL C for this safety goal. The definition of the safe states is based on this safety analysis. According to ISO 26262-1, the safe state is defined as “operating mode of an item without an unreasonable level of risk” (cf. [19]). In the context of automated driving, there are usually two types of safe states including different criteria (see Table 11.1).

In general, zero collision risk would imply to have a prediction horizon to infinite future times. We refer to the discussion in [20], where the authors conclude that all of the classic planning methods are arguably unsafe. However, in the context of a certain world model, it can be argued according to [20] that an automated vehicle does not actively harm and that it can be designed to be as safe as humanly possible. In simple terms, the safe state translates to bringing and keeping the vehicle in a

| Safe state | Criteria for the safe state |
|------------|-----------------------------|
| The driver takes over control of the vehicle | • Maximum period of time allowed for driver takeover  
• Functionality to be maintained while waiting for driver takeover |
| The automated driving functionality switched to a degraded operation mode and finally into the safe state | • Maximum estimated time to reach the safe state  
• Minimum functionality to be maintained while transitioning to the safe state |
standstill condition in a safe location while sending out warning signals to other traffic participants, e.g., via hazard messages or activated warning lights.

For the traffic jam pilot, a possible strategy is to moderately decelerate the vehicle within the current lane and keep it in standstill there, i.e., parking the vehicle. At first, a request for driver takeover is issued; however, if the driver does not respond or a critical failure is detected, the vehicle slows down automatically. The deceleration is accompanied by warning signals for the surrounding traffic participants and possibly by an emergency call, depending on the driver’s state.

For vehicle velocities lower than 60 km/h and an assumed deceleration of at least $-3 \, \text{m/s}^2$, the time required to reach standstill is approximately 6 s. The vehicle travels a maximum distance of approximately 50 m during this time within the current lane. This emergency trajectory has to be planned ahead and stored securely, since the traffic jam pilot will rely on it as the fall back reaction in case of a relevant system failure. Consequently, a valid emergency trajectory has to be available before the automated driving function can be activated.

This definition is insufficient for the highway pilot due to the higher relative velocity range and potentially more complex traffic situations compared to a traffic jam situation. The safe state has to be determined situation dependent and could be one of the following states:

- Driver takes over control of the vehicle.
- Stopping the vehicle in the current lane.
- Decelerate and pull over to the rightmost lane (for right-hand traffic).
- Decelerate and pull over to the emergency lane.
- Continue driving at reduced speed to a safe location.

These examples show that safe states for automated functionalities are very complex and can take quite some time to reach. The time to reach the safe state is defined as emergency operation interval in ISO 26262-1 (cf. [19]).

The maximum transition time to the safe state can be split in the following two contributions:

- The maximum time span to wait for driver takeover.
- The time span required to take the vehicle to the safe state without support by the driver.

Both add up to the fault reaction time, which is defined in Fig. 11.4. During both time durations, the system completely controls the vehicle. Therefore, the corresponding system function has to be provided with high reliability. For most cases, this corresponds to a safety goal rated ASIL D according to ISO 26262.

Table 11.2 summarizes preliminary concepts regarding maximum allowance for driver takeover and corresponding safe state for the traffic jam pilot and highway pilot. We want to emphasize that these numbers are given as an indication only. The exact values depend on many parameters such as

- Type of automated functions
- Definition of the safe state(s)
Fig. 11.4 Definition of fault reaction time and fault-tolerant time interval adapted from ISO 26262-1, 1.44 (cf. [19])

Table 11.2 Estimation of maximum tolerable times

| Automated driving function | Estimated time for driver takeover (s) | Possible safe state                      | Criteria for the safe state |
|----------------------------|----------------------------------------|------------------------------------------|-----------------------------|
| Traffic jam pilot          | 10–15                                  | Standstill in current lane               | Up to 5 s                   |
| Highway pilot              | 10–15                                  | Standstill on rightmost lane             | Approximately 30 s          |
| Highway pilot              | 10–15                                  | Standstill on emergency lane             | Approximately 60 s          |
| Highway pilot              | 10–15                                  | Standstill in breakdown bay or parking lot | Up to 30 min                |

– Driving conditions
– Vehicle type

Final assessment of these parameters will require in-depth HMI and user experience studies. From the safety perspective, critical procedures are activation and deactivation of the automated function. At these particular events, the responsibility for controlling the vehicle is transferred from the human driver to the system and vice versa. The HMI is responsible for providing transparent state information to the driver, i.e., whether the automated function can be activated and subsequently control the vehicle so that the driver can release control. The same argument applies for deactivation where handover of control to the driver is required. In addition, warning signals and indications of the planned driving maneuver in fallback mode need to be issued reliably to other traffic participants.

In the fallback mode of a highly automated vehicle, the system cannot rely on driver actions any more. The mechanical fallback solution that is offered by many brake systems in use today has no benefit in automated mode. Instead, the safety concept requires a redundant “drive-by-wire” functionality in the automated mode.
Legal aspects have to be considered as well, for instance, the Official Journal of the European Union, ECE_R13-H for the braking system [21] and ECE_R79 for the steering system [22], specifies explicit design and test criteria. At least two independent channels are required for the operating braking system as well as an additional fail-operational parking brake system. For the steering system, there is currently a test catalog defined in [22] which demands a degraded steering operation for an extended time interval of 40 min. We refer to [23] for a detailed discussion of the legal situation in the context of tele-operated and automated vehicles with respect to braking and steering systems.

Contemporary surround sensors have a limited ability to reliably detect and classify objects. Therefore, functional redundancy is required in a way that at least in critical regions around the vehicle surround sensors using different technologies can provide an overlapping field of view. This is in the functional safety concept addressed as functional redundancy (see Fig. 11.2). For the traffic jam pilot, a minimal set of surround and localization sensors is required to safely navigate to the safe state. For the highway pilot system, the sensor cluster becomes even more important since feed-forward control on a pre-computed fallback trajectory is not sufficient for the longer operation times in fallback mode, instead the fallback trajectory needs to be updated permanently.

11.4 Technical Safety Concept

In the following, we discuss exemplary architectural issues regarding the technical safety concept. Due to space restriction of our presentation, we will not be able to discuss software- and hardware-related safety measures but rather restrict ourselves to some aspects of the onboard communication and power network.

The technical safety concept referenced in the ISO 26262 has to specify technical safety requirements covering system external interfaces, environmental and functional constraints, and safety mechanisms related to detection and control of faults.

For highly safety relevant systems, it is recommended to carry out the safety analysis both in a deductive and an inductive way. However, a detailed safety analysis is beyond the scope of this article. We will restrict the discussion here to the most prominent components from the perspective of the safety concept. Firstly, these are the braking and steering systems and the control units. Depending on the definition of the safe state, also the power train can be of concern (not considered here).

Maintaining a fail-operational or fail-degraded system operation, while transitioning into the safe state, requires high availability of the actor control and in particular the actors. From the safety perspective, this can be achieved by a corresponding design or by employing redundancy concepts. As far as braking systems are concerned, redundancy concepts can be established based on technology already available today, for an example configuration see Sect. 11.4. As a prerequisite for
the braking system redundancy, the power supply system must reach a maximal availability (see Table 11.2). This results in requirements for the power supply system, which are beyond today’s implementations.

11.5 Requirements Imposed on the Onboard Network by Automated Driving Functions

In Sect. 11.3, we discussed the different automated driving functions together with the corresponding safe states and transition times to the safe state. In this section, we derive resulting requirements for the onboard electrical systems, i.e., the electric power network and the communication network.

11.5.1 Requirements for the Electric Power Supply

The electrical power net has to provide two independent energy storage capabilities that are able to supply the components required for transitioning to safe state. The electrical storage has to provide the energy capacity under all environmental and climatic conditions for which automated driving has been released. Monitoring of the energy content has to be implemented, and the energy content has to be checked reliably before the automated driving mode is offered to the driver. Moreover, the diagnostic system has to guarantee that automated driving mode can only be activated if the energy storage will be capable of supplying the critical components for at least a defined time that is needed to reach a safe state. This is a more delicate task than just monitoring voltage levels.

The power supply topology has to be designed in a way that defined minimum functionality can be provided in single-point failure situations. Resulting critical failures are rated ASIL D, and, therefore, the related failure rate must be sufficiently low. Wiring of components has to be organized in a way that a minimal set of required components in the fallback scenario will stay operational.

11.5.2 Requirements for the Communication Network

Our presentation of the communication network in Fig. 11.5 is kept very abstract, for instance, we have drawn all communication channels as point-to-point connections. Bus topologies can be used as well; however, the single-point failure tolerance has to be carefully evaluated.

A challenging requirement is the maximum tolerable latency time, which is imposed on the communication network. Maximum latency times can be derived
from the specification of the fault reaction time defined for each safety goal by subtracting the time required by the control units, sensors, and actors to process the request. Thereby, existing gateways and switches have to be considered as well. A guaranteed latency time with respect to the communication channel is easily achieved using time-triggered protocols but more difficult to assure for event-triggered communication.

Regarding the detection of errors that lead to missing or falsified data content, standard measures like end-to-end safeguarding have to be applied; the concepts for this are, for instance, described in [24].

### 11.6 Requirement Implications

Considering the requirements derived above, we present a coarse architecture solution, which addresses part of the constraints. In Fig. 11.5, we sketch the coarse E/E architecture of a hypothetical traffic jam pilot system. We have chosen to
display a distributed architecture variant with two separate control units. Using different control units supports the argumentation for freedom of interference of the redundant units. An alternative architectural variant could be based on a central ECU hosting both units sufficiently decoupled, i.e., with independent electrical supply, independent communication channels, and sufficiently low thermal coupling. The latter variant will save construction space and supports high data bandwidth between both units but requires a careful design for the assertion of freedom of interference.

Control unit 1 is responsible to compute the vehicle’s future collision-free trajectory. Therefore, control unit 1 receives input data from the environment sensors and the location sensors (sensing cluster 1) in order to judge the relative positions and velocities of objects in relation to the vehicle. The sensing clusters in Fig. 11.5 can be realized in different ways: as physically redundant sensors, as sensor units with redundant electrical and communication interfaces, or as sensors with different diverse data processing interfaces, provided that common cause faults are sufficiently controlled. We will not elaborate this issue further but rather focus on the onboard network. Since the correctness of this computation is rated safety critical, there has to exist a redundant path composed from sensing cluster 2 and control unit 2. The redundancy has to be static or dynamic in hot standby mode (see definition in [25], Fig. 11.6) in order to meet the timing requirements.

**Fig. 11.6** Redundancy concept for fail-degraded brake system. Each brake system has to be independently electrically supplied and connected to one of the two sets of wheel impulse counters (four for each set)
Depending on the interpretation of the situation, the redundancy can be asymmetric, i.e., the function executed on control unit 2 is not necessarily required to understand the situation in the same level of detail as the function hosted on control unit 1. This offers a good opportunity to implement diversity in the development of the function running on control unit 2. The same argument is applicable to the sensing clusters, where the use of sensors with diverse principles of physical measurement is usually required to cope with their weaknesses. The emergency trajectory has to be stored in both braking systems in order to be available with high reliability, even in degraded mode.

For the traffic jam pilot, we assumed in Sect. 11.1 that the safe state is defined as decelerating the vehicle to standstill in its current lane and keep it parked. Transition to the safe state is primarily a task for the braking system, which in case of a nonfunctional steering system can even provide small lateral corrections by asymmetric brake interventions required to keep the vehicle in the current lane. In fact, this is a steering control redundancy with limited performance.

Therefore, the capability to provide controlled braking of the vehicle is crucial and has to be maintained with high reliability. Taking into account legal requirements, which mandate two independent channels for a braking system (cf. [21]), this requirement translates into a fail-operational braking system where each unit has to be independently electrically supplied. In addition, a fail-degraded HMI is required to reliably communicate the system status to the driver in the context of activation and takeover.

For the highway pilot, this system architecture has to be complemented with a fail-operational steering system. The steering system thus needs a second electrical feed. This requirement is imposed by the possibly higher vehicle velocity leading to a longer distance to reach the safe state and the less constrained motion of other vehicles. Therefore, lateral control is necessary in the fallback mode for a certain period of time and a minimum of perception capabilities in order to avoid collisions with other traffic participants. Depending on the definition of velocity range and safe state, a reliable limp home functionality has to be supported. This would require a fail-degraded power train architecture and would represent an extension to the architecture given in Fig. 11.5.

11.7 Safety Architecture Solutions

In the previous section, the exemplary safety goal “avoid insufficient vehicle deceleration when traffic jam pilot is active” was derived. Below, the consequences with respect to the system architecture of the braking system will be elaborated.
In order to reach the traffic jam pilot safe state (vehicle is decelerated and parked within the driving lane), the following functionalities of the braking system have to be fail degraded:

- Active pressure buildup
- Avoidance of locked wheels at the rear axle in order to maintain stability of the vehicle

Control of the front-wheel slip in low μ situations to provide the lateral forces required for small corrective steering maneuvers in order to follow the pre-calculated emergency trajectory.

A possible concept for a fail-degraded brake system realizing this safe state is shown in Fig. 11.6. This figure focuses on specific parts of the redundancy concept and does not show all components in detail.

This exemplary setup contains two independent systems, each of them capable to fulfill the requirements regarding emergency operation to reach the safe state. During normal operation (both systems are free from errors), the ESP takes the tasks of vehicle stability control incl. the processing of vehicle deceleration requests (issued by the automated driving functionality). In case of a fault forcing the ESP into degraded mode (or even fail safe mode), the automated driving functionality is switched into degraded mode. In this scenario, the iBooster performs the task of bringing the vehicle into the safe state. This concept is called dynamic hot standby redundancy (cf. [25]).

The mechanical push-through that is available in today’s braking systems has no benefit in the automated driving mode. This is due to the fact that the driver is out of the loop in these automated driving situations. The same argument applies to the steering system; therefore, a fail-operational electrical steering is required. Redundant steering systems are likely to be designed as one-box solutions, embedding inherent redundancy rather than using two redundant systems. Such steering systems then require dual electrical feed from independent power sources as sketched in Fig. 11.5.

Our overall concept for redundant actuation is shown in Fig. 11.7. The redundant braking is realized by combining ESP and iBooster, while a redundant steering system is realized by combining electronic power steering with ESP, which can issue a yaw momentum through braking of individual wheels.

This paper has not yet discussed a detailed architecture of the environment sensor set. It will be a formidable future task to design an electrical and communication topology for the sensor clusters which will support all functional use cases, all safety goals, and at the same time manage to achieve target costs.

Finally, we would like to point out that the coexistence of other driving functionalities with an automated driving system, for instance, the functional behavior at defined system boundaries, shall also be considered for the design of the onboard network.
11.8 Conclusion

In this paper, we provided a high-level overview of our development of highly automated driving systems. We illustrated challenging situations and use cases and outlined their impact on system design, key technologies, and their technical realization. The paper also exemplifies how certain aspects of the system design as well as the implementation are country and use case specific. We are convinced that automated driving is becoming a reality, offering benefits for safe, relaxed, and economical driving, and we expect a stepwise introduction of automated driving starting with increased levels of automation on the highway. The first highly automated driving function will be a traffic jam pilot. The trend toward automated driving is generating new technical challenges for the sensors, algorithms, actuators, as well as for the E/E architecture of future vehicles. We discussed the implications of the new functionalities on the onboard supply and communication network in this paper. Derived from safety aspects and legal constraints, we argued that redundant electric onboard network and redundant communication network is required even for closer-to-market highly automated driving functions such as the traffic jam pilot. For the highway pilot, the standard concept of one safe state per safety goal has to be revisited in favor of a cascade of safe reactions. The corresponding transition times are likely to be on the order of minutes. The onboard net has to provide the required energy capacity during this time safely.
References

1. International Organization for Standardization, Road Vehicles—Functional Safety. ISO 26262-10, 2012 (2012)
2. L. Lutz, T. Tang, M. Lienkamp, Analyse der rechtlichen Situation von teleoperierten (und autonomen) Fahrzeugen (2012), http://www.ftm.mw.tum.de/uploads/media/07_Lutz.pdf. Accessed 28 Mar 2014
3. Robert Bosch GmbH, Bosch Automated Driving (2013), http://youtu.be/0D0ZN2tPihQ. Accessed 10 Jul 2015
4. Robert Bosch GmbH, Bosch User Experience for Automated Driving (2015), https://youtu.be/2i-t0C7RQWM. Accessed 10 Jul 2015
5. M. Helmle et al., Transient System Safety and Architectural Requirement for Partly and Highly Automated Driving Functions, in Electric & Electronic Systems in Hybrid and Electric Vehicles and Electrical Energy Management (2014)
6. J. Becker, M. Helmle, Architecture and System Safety Requirements for Automated Driving, in Road Vehicle Automation 2, ed. by G. Meyer, S. Beiker. Lecture Notes in Mobility, vol. 2 (Springer, Cham, 2015), pp. 37–48
7. M. Buehler, K. Iagnemma, S. Singh (eds.), The DARPA Urban Challenge. Autonomous Vehicles in City Traffic. Springer Tracts in Advanced Robotics, vol. 56 (Springer, Berlin, 2009)
8. Google Inc, Google Self-Driving Car Project, Monthly Report, May 2015, http://static.googleusercontent.com/media/www.google.com/us//selfdrivingcar/files/reports/report-0515.pdf. Accessed 8 Jun 2015
9. H. Lategahn, C. Stiller, Vision-only localization. IEEE Trans. Intell. Transp. Syst. 15(3), 1246–1257 (2014)
10. C. Stiller, J. Ziegler, Situation Assessment and Trajectory Planning for AnnieWAY, in IEEE/RSJ International Conference on Intelligent Robots and Systems. IROS Workshop on Perception and Navigation for Autonomous Vehicles in Human Environment, San Francisco, 30 Sep 2011
11. M. Aeberhard et al., Object Existence Probability Fusion Using Dempster-Shafer Theory in a High-Level Sensor Data Fusion Architecture, in Intelligent Vehicles Symposium (IV), 2011 IEEE, Baden-Baden, 5–9 Jun 2011
12. T. Gindele, S. Brechtel, J. Schroeder et al., Bayesian Occupancy Grid Filter for Dynamic Environments Using Prior Map Knowledge, in 2009 IEEE Intelligent Vehicles Symposium (IV), Xi’an, 3–5 Jun 2009
13. T. Jiang, S. Petrovic, U. Ayyer et al., Self-driving cars: Disruptive or incremental? in Applied Innovation Review, vol. 1 (Sutardja Center for Entrepreneurship & Technology, University of California, Berkeley, 2015), pp. 3–22
14. J. Levinson, S. Thrun, Robust Vehicle Localization in Urban Environments Using Probabilistic Maps, in 2010 IEEE International Conference on Robotics and Automation (ICRA), Anchorage, 3–8 May 2010
15. California DMV, California Driver Handbook (2015), https://apps.dmv.ca.gov/pubs/dl600.pdf. Accessed 10 Jul 2015
16. D. Sales, D. Correa, L. Fernandes et al., Adaptive finite state machine based visual autonomous navigation system, Eng. Appl. Artif. Intell. 29, 152–162 (2014)
17. SAE International, On-Road Automated Vehicle Standards Committee, Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems (2014), http://standards.sae.org/j3016_201401/. Accessed 30 Oct 2014
18. Federal Ministry of Justice and Consumer Protection, Straßenverkehrs-Ordnung StVO. Teil I (2013), http://www.gesetze-im-internet.de/stvo_2013/index.html. Accessed 1 Mar 2013
19. International Organization for Standardization, Road Vehicles—Functional Safety. ISO 26262-1, 2011 (2011)
20. R. Benenson, T. Fraichard, M. Parent, Achievable Safety of Driverless Ground Vehicles, in *10th International Conference on Control, Automation, Robotics and Vision*, 2008, Hanoi, 17–20 Dec 2008

21. United Nations Economic Commission for Europe, Regulation No 13-H of the Economic Commission for Europe of the United Nations (UN/ECE). Uniform provisions concerning the approval of passenger cars with regard to braking. Off. J. Eur. Union L 230, 1–80 (2010)

22. United Nations Economic Commission for Europe, Regulation No 79, Addendum 78, Revision 2, of the Economic Commission for Europe of the United Nations (UN/ECE). Uniform provisions concerning the approval of vehicles with regard to steering equipment. Off. J. Eur. Union L 137, 25–51 (2008)

23. J. Levinson et al., Towards Fully Autonomous Driving: Systems and Algorithms, in *Intelligent Vehicles Symposium (IV)*, 2011 IEEE, Baden-Baden, 5–9 Jun 2011

24. AUTOSAR R4.0, Rev 2, Technical Safety Concept report Status V1.1.0

25. R. Isermann, R. Schwarz, S. Stölzl, Fault-tolerant drive-by-wire systems. IEEE Control Syst. Mag. 22(5), 64–81 (2002)