Chapter 21
From Controllability to Safety in Use: Safety Assessment of Driver Assistance Systems

Alexander Huesmann, Mehdi Farid, and Elke Muhrer

21.1 Introduction

Controllability of driver assistance systems is the topic addressed by the “Code of Practice for the Design and Evaluation of ADAS”, and controllability in general is already mentioned in the Vienna Convention on Road Traffic of 1968 [1]. Nevertheless, in the automotive development context, the statement that drivers must at all times be able to control their vehicles can be interpreted very differently. Very often the thought of controlling the vehicle in a critical road scenario is present. However, controllability associated with assistance systems and automation has an entirely different facet. The aim here is, that the driver controls the vehicle in its nominal function, at the system limits and in case of system failures, meaning the driver is able to cope with traffic situations without harming himself or others.

In the context of automation, aspects of, the to-be-avoided, systems-over-confidence and mode awareness increase in importance and must be considered in the system composition.

The basis for the development of higher automation functions in the vehicle is the established methods and procedures for the controllability of driver assistance systems. Such approaches largely consider single scenarios isolated.

Due to the increasing complexity and networking of future systems, such singular considerations of single scenarios are not likely to be sufficient. Thus, a holistic consideration of the traffic situation is required.

This chapter is based on: Klaus Kompaß et al.: Fahrerassistenz und Aktive Sicherheit. Wirksamkeit—Beherrschbarkeit—Absicherung. expert verlag, Renningen 2015.

A. Huesmann • M. Farid • E. Muhrer
BMW AG, 80788 Munich, Germany
e-mail: Alexander.Huesmann@bmw.de; Mehdi.Farid@bmw.de; Elke.Muhrer@bmw.de

© Springer International Publishing Switzerland 2017

D. Watzenig, M. Horn (eds.), Automated Driving,
DOI 10.1007/978-3-319-31895-0_21
Initially, the controllability of driver assistance systems and the corresponding references will be addressed. Following this, the method of analysis of safety in use will be introduced and explained. This includes the definition of terms and their delimitations.

### 21.2 Controllability of Driver Assistance Systems

Nowadays, if controllability is mentioned in the context of driver assistance systems (DAS), it immediately is associated with two documents. The older one is the Vienna Convention on Road Traffic of 1968 [1]. Herein, the international rules of road traffic were agreed upon. The other is the code of practice (CoP) for the design and evaluation of advanced driver assistance systems (ADAS) [2]. The CoP emerged from the work of a series of European projects, in particular as a report in the RESPONSE 3 [2] project which was part of the integrated project of PReVENT [3].

The launch of the RESPONSE projects started out just before the new millennium, when the first driver assistance systems such as active cruise control (ACC) became available on the market and others in the automotive industry were under way. The central question was how to generate and verify the product safety of such assistance systems.

First, for formulating development standards, the field of application has to be determined. One of the questions in the project RESPONSE was what was meant by ADAS. For this purpose the three levels into which driving tasks can be divided were used: navigating, maneuvering, and stabilizing the vehicle [4].

It was agreed to observe rule-based systems under normal driving conditions, which are acting on the maneuver level, such as a lane change assistant. Furthermore, systems have been taken into account that are in transition between maneuvering and stabilizing, namely, assistance systems in emergency situations, such as an automatic emergency brake system.

A systematic assessment of emerging risks ultimately distinguished two categories: the technical safety and the safety of the human–machine interaction.

The technical safety of systems and how to develop appropriate safety concepts were excluded, because around the same time, the ISO 26262 standard for functional safety in the vehicle [5] was under development; hence, an appropriate set of procedural rules to ensure safety in E/E errors emerged.

The main focus within the research project RESPONSE 3 is the safety of the human–machine interaction, which is made possible by the controllability of the driver. Controllability is divided into three steps:

- The ability of the driver to perceive the criticality of a situation
- The ability of the driver to decide on an appropriate countermeasure
- The ability of the driver to also perform this countermeasure

Controllability is the focal point in the project RESPONSE 3.
Controllability has already been mentioned as a criterion in the Vienna Convention on Road Traffic of 1968 [1].

Thus, Article 8.5 states that:

- Every driver shall at all times be able to control his vehicle or to guide his animals.

And in Art. 13.1, it is written that:

- Every driver of a vehicle shall in all circumstances have his vehicle under control.

Herein it is implied that in the context of driver assistance, the driver also has to be able to manage traffic situations when using driver assistance systems. This includes handling the various traffic situations while driving with the support of the system, at the system boundaries, and in case of system errors.

A system error is considered as mentioned above in the standard for functional safety. Development guidelines for the nominal function and its system boundaries, in particular the human–machine interaction of assistance systems, are considered in the code of practice (CoP) for the design and development of ADAS which was published on the website of the ACEA and thus made publicly available in 2009 [2].

In the CoP the procedure for safety-oriented development and evaluation of safety aspects of driver assistance systems are described with a clear focus on the human–machine interaction. This is based on the identification of risks and the preparation of hazard and risk analysis as well as risk assessments. During the development process, measures aimed at ensuring the controllability of the assistance systems are derived from these actions.

When looking at the relationship of driver performance and automation [6], it is clear that with increasing automation, the controllability of situations, in which the driver has to take over the driving task or correct the trajectory, is not necessarily given. A common classification of automation levels in terms of requirements for the driver can be found in [7].

Here, the transition between partly automated driving and highly automated driving is essential. While partly automated driving, the driver needs to monitor the system permanently and has to be able to take over the driving task at any given moment. At the next higher level of automation, the highly automated driving, the driver no longer has to permanently monitor the system, and in case of a takeover request, the driver is given sufficient time to react. However, when the driver no longer needs to monitor the system, perceiving the criticality of a situation can no longer be fulfilled continuously, hence impairing already the first point of the abovementioned criteria of controllability. In addition, such functions would stand in contradiction to the Vienna Convention, where control of the vehicle is required. This triggered a proposal for amendment to the Vienna Convention [8] and was officially put to vote in 2014. This proposal also included an amendment to Art. 8, which states, that “a vehicle meets the requirements of Art. 8 paragraph 5 and Art. 13 paragraph 1, if it meets the requirements of the international certification regulations” (e.g., UN ECE rules). In addition, the requirements referred to in Article 8 and 13 are met if the driver is given the opportunity to turn off or override
the assistance system. This amendment of the wording is intended to ensure the conformity of highly automated driving functions with the Vienna Convention.

It is becoming obvious that the criterion of controllability for a holistic safety assessment of functions with increasing levels of automation will not suffice any longer. Thus a holistic consideration of the traffic with all influencing components is required.

### 21.3 Safety in Use: A Holistic Consideration of the Driver, Vehicle, and Environment

In Sect. 21.2 we addressed the factor controllability. When evaluating the controllability, the overall situation of the driver, his vehicle, and its environment is of special importance (Fig. 21.1).

By that, controllability arises not only through the skill level and the performance of the driver but is heavily influenced by components of the traffic situation. On the one hand, every drivers’ profile differs by the extent of long-term experiences and long-term knowledge, short-term intentions and states, and different perceptions of the environment; thus, every driver most likely reacts in a different way. The environmental conditions vary in weather, visibility, road conditions, and traffic density. Vehicles have different engines and different assistance systems on board. Depending on the chassis, vehicles also react differently in certain dynamic driving situations. This is not an exhaustive list of possible influences but is intended to show that all of the influencing components may take various forms. The driver steers the vehicle, reacts to the feedback of the vehicle, and moves it within its environment. A holistic approach of the traffic situations to be managed by the driver has to include these three interacting components. In other words: depending on the ratio of the components, the driver has to perform different maneuvers to safely navigate his vehicle through traffic.

For example, the driving task of paying attention and maintaining the speed level when driving on a route with low traffic density changes rapidly in a high-density environment (i.e., a traffic jam ahead of the driver), where stopping and starting

![Fig. 21.1](image-url)  
**Fig. 21.1** A holistic traffic situation integrates the interaction of the driver, the vehicle and the environment
the vehicle is the main task. For these situations, different “levels” that have to be included in the risk assessment arise. Therefore, all factors in the assessment of risks in road traffic must be complied with. However, the complexity of traffic situations requires that the situations are systematically assessed. Without such, an exhaustive assessment of risks is not possible.

In this article, the methodology of safety in use is introduced. For this purpose the system behavior of an “error-free” function in regular use cases and at the system limits is systematically analyzed. Here, both the intended use and the likely misuse are mostly relevant. The term “error-free” case requires a more precise specification. This will take place in the following chapter. The aim of the analysis of safety in use is to know the total risk, which is evident from the use of a function in the different situations that may occur. Based on this assessment, the decision for specific actions in the system development can be made.

21.3.1 Systematic Analysis of Safety in Use

The initial focus of the safety assessment needs to be clarified first, in order to carry out a systematic analysis of whether a function is safe to use.

Safety must always be seen in the context of risks, where risks are described as the product of the likelihood of a negative event to occur and its damage severity.

The likelihood of occurrence of adverse events relating to road transport in the context of driver assistance is determined by the likelihood of occurrence of the respective traffic situation, the ability of an assistance system to suitably handle these situation, and, if necessary, the ability of the driver to master the situation. A holistic consideration does not limit the focus of technology and driver merely to the ego vehicle but may also take participating road users’ skills into account.

The damage in traffic ranges from property damage to personal injury. The following analysis of safety in use is, according to the ISO 26262, oriented toward the avoidance of personal injury.

The well-known procedures of risk analysis and risk assessments form the basis for the analysis of safety in use. During this, the nominal function is considered as well as the anticipated misuse of it. What is not considered is the case of a technical error (E/E error according to ISO 26262). However, the limits of the sensors’ performance are very well considered. In the drivers’ perception, both cases show the same effect and are called “errors”, for example, when the vehicle does not detect a risky situation in due time. The cause, however, can be different (e.g., the technical error resulted from an error in the control unit). By technical measures the likelihood of errors occurring can be downsized to the required extent. Any object not detected by the sensors because of its systematic blur is understood as a system boundary and thus part of the function in its nominal state, which includes the system limits.
A team of experts further combines their knowledge about the system development, the sensor development, the driver behavior, and the traffic situation, and as part of the risk analysis, the collective presents a list of likely events.

These events are evaluated in terms of their likelihood of occurrence in the traffic situation, their manageability by the technical solution, and the drivers’ ability to control the system. If necessary, measures are derived from the evaluation to reduce the likelihood of occurrence, on the one hand, as a technical measure (e.g., as requirements for the sensory detection of the environment), and on the other hand, as a constitutive measure to increase the drivers’ controllability of the system. Figure 21.2 shows an example of the structure of such an analysis of safety in use.

In some cases, a more detailed consideration of the events may be required. This is the case if there is ambiguity about the overall likelihood of occurrence and where the impact in terms of the damage is important for a holistic consideration of the safety in use. An example could be the event of personal injury when using the autopilot on the highway. In such cases it makes sense to disassemble the event into the parts that must occur collectively in order for the entire event to occur. Its methodological approach is the event tree.

The event tree is comparable to the error tree simply that the interesting situation was not an error but an event, as part of the regular use of the system.

In the disassembly the causes are identified and linked logically. For one thing, this approach can be used qualitatively to illustrate the cause mechanisms and to make them plausible. On the other hand, the individual events may also be quantified, thus creating greater transparency for the overall evaluation. A detailed sensitivity analysis is also possible on this basis.

Figure 21.3 shows an example of an event tree in the event of personal injury when using the autopilot system on the highway.

The event of the collision with a person on the highway is located at the top of the event tree. The level below describes the traffic situation (traffic jam) in which the event occurred. At the same level, the proportion of traffic jams within the overall operating time of the vehicle is taken into account. The next level describes how the event takes place. Here, the preceding vehicle performs a lane change maneuver very close to the obstacle to avoid a collision but does this too late for the driver to react in time and the on-board safety systems do not respond sufficiently.

The aspects that relate to the driver are displayed at the next level. At the bottom layer of the event tree, the likelihood to encounter a person on the highway can be specified for different causes for this particular traffic situation (i.e., traffic jam). By no means this example is complete but it is merely intended to illustrate the approach.

By this simplistic and incomplete example, it is obvious that a great deal of information, for the controllability of a specific traffic situation, is needed. This is information about the traffic situation, the technical performance of the system and its event chain, as well as the performance of the driver. Some approaches and examples, to obtain information in terms of the traffic situation and the drivers, are described in Sect. 21.4.
| Evaluated Scenario: Functional characteristics in specific operating situations | Classification of the Situation | Accident Scenario | Assessments of the accident consequences | Averting of dangers | Assessment of the controllability | Justification for 'No' or proposal for action |
|---|---|---|---|---|---|---|
| Customer uses the function A in situation B... | i.e. exceptional Situation, misuse of system, ... | Scenario may lead to accident XY... | consequences of the accident may be averted by XY | | | Proposed action n (1) Proposal A (2) Proposal B |
| Customer drives with active highway traffic jam assistant in the use case. Vehicle leaves the lane and people are on the side track. | Vehicle leaves the lane and people are on the side track -> likelihood of occurrence very rare. | Vehicle leaves the lane and collides with people. | Collision with people: very high risk of injury. | The driver brakes or pedestrians leave the danger zone. | Situation for observant driver at low speed easily controllable. | Yes |
| Based on a high automation trust prolonged response time can be expected: 1) avoid high automation trust 2) detection of pedestrian at highway traffic jam assistant. |
| Customer drives with active highway traffic jam assistant in the use case. Preceding vehicle changes lanes, since the current lane is blocked due to a broken down vehicle / accident vehicle | Preceding vehicle changes lanes because of an accident vehicle accident in its' immediate vicinity -> likelihood of occurrence is very rare. | Vehicle continues unrestrained, collides with person outside the broken down vehicle. | Collision with people: very high risk of injury. | Driver brakes or people leave danger zone | Situation for observant driver at low speed easily controllable. | Yes |
| Based on a high automation trust prolonged response time can be expected: 1) avoid high automation trust 2) detection of pedestrian at highway traffic jam assistant. |

Fig. 21.2 Exemplary presentation of an extract from a possible analysis of safety in use
21.3.2 Reference Values for Safety in Use

The previous section explained how to systematically arrive at a holistic risk assessment to determine the likelihood of personal injury when using driver assistance systems. In addition it was described how to employ the results as a basis for deriving safety-oriented measures.

So far, there is no reference for the regular use of an automobile. However, there are risk assessments in the area of mobility and consumer protection that could be used as a starting point. Two exemplary approaches that are considering the safety risk of accidental errors and of high-risk product characteristics shall be introduced here: first, the DIN EN 50126, which is used for the safety of the European railways and, secondly, the RAPEX procedure which develops guidelines for the rapid exchange of information on risks of general product safety in Europe.

The DIN EN 50126 was given the headline “The specification and demonstration of the Reliability, Availability, Maintainability and Safety (RAMS)” with the footnote “railroad application” [9].

Within the document, methods for managing the issues referred to in the title are given. Of particular interest here is the paragraph on risk and the assessment and acceptance of risks. Literally, it is written: “The acceptance of risks should be based upon commonly accepted principles”, and in addition, as the criterion used in Germany, the minimum endogenous mortality (MEM) is specified.

In the Annex of the standard, the MEM is described in more detail by examples of risk acceptance principles. The MEM is based on the classification of death causes
including a group named “technological facts”. This includes categories such as entertainment and sports, home improvement, engines and machines, and traffic. Not included therein are death events due to illness and congenital malformation. The term “endogenous mortality” refers to the proportion of a group to the whole extent of fatalities, which in turn can be broken down depending on age. In economically developed countries, the age-related minimum is the group of 5–15-year-olds (Fig. 21.4).

A normalized simultaneity of influencing systems is determined by the approach that new technical systems should not have a higher risk than already existing ones and that humans are always exposed to multiple systems simultaneously. This simultaneity factor is 20 and thus the reference value of the minimal endogenous mortality is again divided by 20 [10].

A second approach for a possible reference value provides the RAPEX procedure, which is described in the Directive 2001/95/EC on general product safety [11]—a community system for the rapid exchange of information among the European countries for product safety risks. This Official Journal of the European Commission also addresses risk assessment. The details of the RAPEX are laid out in the Commission’s decision “on establishing guidelines for the management of the System for a Rapid Exchange of Information ‘RAPEX’ established under the Article 12 and the notification procedure under the Article 11 of the Directive 2001/95/EC on general product safety” [12].

Different degrees of risks are defined and can be determined from the sum of the degree of injury and the likelihood of occurrence. Cases which pose a serious health and safety risk to the consumer, i.e., the highest risks, are to be reported.

In the Annex of the document, injury scenarios, from bruises to death, are subdivided into four categories of injury. The likelihood of occurrence is expressed as a percentage value of the damage during the life span of a product and is further
subdivided into eight levels between 50% and $1 \times 10^{-6}$. Finally, for the evaluation and classification of the risk determined, a reference table is given, as shown in Fig. 21.5.

Rather than using existing procedures of dealing with safety risks occurring from errors or risky product features, the approach of a risk–benefit analysis seems also reasonable. Here, the security risk is assessed in relation to the gain of safety by using the systems. An effectiveness analysis could provide such a methodological approach [13]. The performance of the driver increases considerably in importance, and the issue of which performance would be recognized as a benchmark would be raised: here, the reference depends on whether the driver is averagely experienced or has more than average driving skills. In addition, results from the accident statistics could give orientation, when the question of “how often a driver error is responsible for an event” is considered. Also a legitimate approach in analogy to the abovementioned MEM, to not cause any adverse effect on the relevant risk group, would be the issue of the share of accidents related to the overall traffic situation.

It is obvious that there is still a need for the development of appropriate references and criteria.
21.4 Informative Sources for the Creation of an Analysis of Safety in Use

In Sect. 21.3.1, the systematic approach to the creation of an analysis of safety in use was described. On the one hand, all possible scenarios are collected; on the other hand, a quantification of the risk is tried to be achieved. Thereof, measures are derived in order to suitably contain the risk of damage.

Basically, there are three approaches to reduce risk:

The first category includes increasing the systems’ controllability by the user and other road users. This, for example, can be achieved by enabling drivers to easily override the system or by other measures of the human–machine interaction, like takeover requests to improve the so-called mode awareness.

The expansion of technologies for situational awareness and control by the vehicle constitutes the second category. For example, the use of additional and redundant sensors for reliable and accurate object detection or the optimization of the detection algorithm in the classification of the relevant objects could be possible measures.

The third category includes functional adjustments, which limit or preclude the use of the system in potential risk scenarios. By that, the use of the systems in scenarios with a high risk of safety in use will be restricted. Examples of functional limitations are limiting of the speed reduction in automatic emergency brake systems to a level that is manageable for the following traffic or to limit the steering assistance of lane-keeping systems to scenarios where track lines are available and detected.

To ensure that the measures derived from an analysis of safety in use are necessary and can fulfill the desired outcome, the consideration must be very detailed and carried out with great care. This requires experts who have sufficient in-depth knowledge of the field.

At this point, it shall be briefly mentioned that studies from different scientific disciplines show that expert judgments that are not based on a sufficiently large and valid data base but are associated with significant inaccuracies concerning specific forecast predictions [14]. The inaccuracy of the forecasts increases with the increasing complexity of relationships within the observation unit. Driver assistance systems show an especially high complexity, since many interacting factors are involved (driver, vehicle, environment), each, which in turn show a high complexity of their own. Accordingly, for a reliable and sufficiently detailed analysis of safety in use, experts need data sources of which statistical data and facts can be derived as input variables for the event tree, and questions of the following type can be answered.

“What transport scenarios with a potential safety hazard may occur during the system use?” or “How often do relevant traffic scenarios and relevant scenario parameters occur?” or “How well do different drivers and other road users handle the relevant traffic scenarios?” For a realistic assessment of the controllability, both
the performance of the driver in the first encounter of the system and the medium- and long-term handling of the assistance system are of significance. A further question to be addressed is “How does the system perform in the scenarios under consideration?”

Thus, a key challenge in the conduct of an analysis of safety in use is to provide the data required in sufficient quality.

In principle two categories of data sources can be distinguished: the scenario-based and driver performance-related data sources. Some methods provide answers for both categories, while others only provide data for one. Figure 21.6 gives an overview of different methods for data generation. It is evident that the validity of the data increases depending on the complexity of each method.

Complexity here refers to the sum of the organizational, financial, and technical requirements for the preparation, implementation, and analysis of the data obtained from each method. For example, a literature review, based on a targeted analysis of “relevant” literature, is associated with much less effort in terms of the technical and organizational requirements than a driving simulator study with subjects.

On the other hand, a driving simulator study is, in turn, associated with far less effort than the so-called naturalistic driving study (NDS) or a field operational test (FOT). Both, the NDS and the FOT, involve several months to years of organizational and technical preparations before results can be obtained. However, the knowledge gained by a well-prepared and broadly based NDS/FOT study is tangible, reliable, and informative, because these methods are based on the observation of the driver behavior in dealing with one or more systems in a natural field environment and in a real vehicle.

Often, several of the methods described above must be used in the context of an analysis of safety in use in order to increase the reliability of the data to a sufficient level. In general, it is unlikely that a single method provides all the necessary data and facts. Different methods must therefore be used in parallel and complementary to close the knowledge gaps in the conduct of consumer safety
analyzes. Below, the mentioned methods are briefly described and examples in the context of semiautomated driving functions are provided. It is important to note that a further method is the method of simulation, while these method is not addressed in this paper.

21.4.1 Data Collection: Literature Review

Literature reviews can be used for answering questions of relevant traffic scenarios and their frequencies, as well as questions related to the performance and controllability of systems by the driver. Particularly, in the field of driver performance and controllability, relevant literature sources are available. In the context of driver assistance systems, scientific contributions in the fields of general cognitive psychology, traffic psychology, ergonomics, human–computer interaction, and norms and standards of such may provide a first basis for evaluating the controllability and driver performance.

Starting with a limited number of relevant sources, the advantages of this method, if standard sources are used, lie in the limited effort and the general acceptance of the facts.

A disadvantage of the method is that the standard literature often provides only first generic advice and information for the use of safe design systems.

A disadvantage of the method is that the standard literature often provides only first generic advice and information of the safety in use of systems. Also, the reported facts of the assessed driver performance and controllability are often quite system specific. In addition, due to the increasing complexity of innovative driver assistance systems, they have not yet been studied in a high level of detail.

Consequently, the results of a literature review need to be interpreted carefully due to the lack of the informative value and reliability for a specific question for the system-specific safety in use. In regard to scenario-specific data, similar advantages and disadvantages, when conducting a literature review, apply. Factors for the evaluation of relevant traffic scenarios, such as the characteristics of the road and traffic, congestion time, average travel time and travel distance, weather conditions, velocity, and much more, have been studied and described in various sources. However, their codependency is often not considered (e.g., the likelihood of congestion depending on the weather conditions).

21.4.2 Data Collection: Questionnaires

Interviewing specially selected driver groups is another way to obtain basic data for an analysis of safety in use. Different groups can often give relatively good indication of the occurrence of relevant and potentially critical traffic situations. Especially where only few publications exist, a questionnaire study may provide
first qualitative and quantitative indications. An advantage of surveys is they can be used to gain insight into specific experiences of a relatively large number of people. Additionally, a survey can be carried out in different places and in different countries, thus facilitating a quick data collection of different regions’ traffic situations. To the advantage that the necessary infrastructure for the preparation, implementation, and evaluation of such studies compared to other methods is relatively low. Due to possible different interpretations of questions, linguistic and cultural peculiarities, and the objectivity of the respondents, a survey study is often associated with uncertainties regarding the reliability of the results. Surveys in the field of assessing the controllability of critical situations are less advisable, as several studies have shown that respondents without experience of the situation in question often overestimate their own performance.

As an example of a questionnaire study, a study of the likelihood of certain traffic situations in China will be introduced (internal study of BMW). The background of the study was the need to acquire knowledge about the traffic situation in China for the safety in use of partially automated assistance functions. Due to the relatively short history of motorized road traffic and the ever-changing structures in the country, hardly any publication sources exist, which provide the latest and quantifiable picture of the traffic situation in China. The aim was to compare the frequency of safety-relevant traffic situations on Chinese motorways with those in Germany and to use them as an initial estimate for assessing the safety in use of assistance systems in China.

In preparation of the study, several interviews with German employees, working in China, and Chinese employees were conducted to identify the main differences of road traffic between China and Germany. It quickly became apparent that the opinion of respondents remained vague in interviews and did not allow for a quantification of the so-called exceptional situations. With exceptional situations such traffic situations were meant which pose a potential accident risk due to road users’ unlawful conduct of their vehicle in traffic. Examples of exceptional situations are, among others, reverse driving on the motorway, wrong-way drivers, and cyclists and pedestrians on the motorway.

The development of the questionnaire and the implementation and evaluation of the study included several steps. First the definition of the questionnaires’ main focus took place on the basis of interviews with Chinese experts. Subsequently, the questionnaire was developed, the rating scale selected, and the questionnaire was translated into English and Chinese language. A test phase in China was carried out, to optimize the questionnaire until it was finally distributed to selected participants in China and Germany. The analysis and interpretation of results marked the end of the study.

Three different samples of participants took part in the study: German employees working in Munich \( (n = 25) \), Chinese employees working in Beijing \( (n = 34) \), and German employees sent to work in Beijing \( (n = 26) \). In addition to the demographic items, the questionnaire included further questions about driver behavior and driving experience as well as the perception of the frequency of some exceptional situations.
The results of the survey revealed that Chinese respondents, on average, drive 260 hours per year on a highway in a traffic jam. Thus, Chinese participants experienced on average 23 times more often congestions on highways than the German participants. According to the results of the study, the German participants, on average, experience approximately 12 hours of traffic jam driving on German motorways, in 1 year.

The analysis of the questions regarding the exceptional situations has shown that all exceptional situations included in the survey were ten times more frequently experienced on Chinese motorways than on German highways, some even more often. Striking was that the results of the assessment of Chinese respondents in China partially differed from the assessment of the German respondents: German respondents who worked in China partially differed from the assessment of the German respondents: German respondents who worked in China rated the likelihood of occurrence of the exceptional situations higher than the Chinese respondents.

Different perceptions of the criticality of traffic situations, due to cultural differences, driver training, or habituation effects of the local population, are just some of the possible explanations for this discrepancy. The different assessment of the frequency of traffic situations generally raises the question of how objective the results of survey studies are and highlights the need to validate the results. Nevertheless, such results provide an initial orientation or tendency of the differences in the two countries.

The example described shows how data about traffic situations and exceptional situations can be obtained with relatively little effort and in a short time through the use of questionnaires. However, the results also show that such questionnaire study must be validated or supplemented by more sophisticated methods.

### 21.4.3 Data Collection: Studies in the Driving Simulator or in Real Vehicles

Alongside with volunteer studies in the real vehicle, different types of driving simulator studies, assessing driver performance, controllability of driver assistance systems, and developing human–machine interfaces are increasingly being applied.

Both methods, with their advantages and disadvantages, can be applied in the course of the development and validation of the assistance system. Real studies hold the advantage of participants experiencing real driving dynamics in the examined scenarios, which is important for observing realistic driver reactions. However, the design of a real driving study is limited by safety issues and obvious limitations of the surrounding infrastructure.

Basically, to conduct a study with real vehicles, safety-oriented modifications have to be taken in order to reduce the risk of participants getting harmed. These include limiting the scenarios studied to low or medium vehicle dynamics, carrying out studies on safe and enclosed test routes and areas, excluding particularly critical traffic scenarios, and some other. Further, the influence of secondary and tertiary
driving tasks on the driving performance can only be observed to a very limited extent, due to safety issues.

Another infrastructural limitation of real driving studies that, if at all, can be managed with great effort is the presentation of complex traffic scenarios that require several vehicles and other road users. Further, ensuring the reproducibility of the study traffic scenarios is often impeded because of external factors such as the changes in weather conditions. The conduct of real driving studies outside of the public traffic space may result in the examined traffic scenarios as being too artificial, leaving the issue as to whether the collected data of the driver’s performance corresponds to the actual performance of the subjects.

An example of a study in the real vehicle, which provides basic data for an analysis of safety in use, can be found, for example, in [15]. The study examined two error categories to assess potential steering system disorders. Here, the controllability of the leap in the steering angle by switching off the active steering system and the controllability of the manipulated errors in different amplitudes was observed at various levels of velocity. Based on the analysis of the driver behavior, two different reaction phases can be distinguished: on the one hand, the initial response, i.e., the time interval until the end of the first driver engagement, and, on the other hand, the error compensation phase in which the occurring driving dynamics and lane tracking errors are compensated. Both the subjective assessment and the characteristics of the vehicle operation and the vehicle reactions show that a resulting leap from the system shutdown in the steering ratio is easy to control, even with demanding steering maneuvers. For the positioning error, there is apparent that up to a positioning error amplitude of $0.3^\circ$ of the front wheel angle, no safety-relevant implications apply.

In [16], the drivers’ performance was studied in approaching a stationary obstacle in the low speed range with an active ACC stop & go system. The study showed that all drivers were able to stop the ego vehicle in case of loss of the target object during the approach in time. In addition, strong learning effects were found in the study during the repetition of the test scenario.

In driving simulator studies, most safety-related and infrastructure-related constraints of a real vehicle study can be overcome, depending on the type of the simulator. The lack of driving dynamics in the static simulator or the limited dynamics in the dynamic simulators remains a significant weakness of the simulator methods. In recent years, a new method of volunteer studies has been deployed. It is called the vehicle-in-the-loop method. Here, the strengths of the simulator technology (e.g., the virtual driving environment) and the real vehicle (e.g., real dynamics) are combined. However, resulting from the combination, new challenges arise that need to be addressed [17, 18].

Simulator studies have been increasingly used in recent years for studies on driver performance and controllability of partial and highly automated assistance systems and provide valuable information that can be used in an analysis of safety in use.

In [19] a simulator study is described where the drivers’ performance was studied in three different takeover request scenarios. The ability of the driver to take over is one main topic in automated systems. Depending on the scenario, subjects had
to handle different driving maneuvers after the takeover request was given (e.g., stabilizing, maneuvering, and navigating). In the study, each scenario was run with takeover times of 4, 6, and 8 s. The driving speed during the highly automated driving was set to 100 km/h and test subjects had to simultaneously perform a tertiary driving task.

It has been found that a drop in the takeover period from 6 to 4 s leads to a particular high loss of comfort in subjective evaluations of the subjects. In contrast, no subjectively perceived comfort profit could be established when the takeover time was increased from 6 to 8 s.

In [20], a simulator study demonstrated the quality of the takeover by the influence of certain environmental parameters and different non-related driving tasks.

It was shown that visual–acoustic takeover request lead to significantly faster takeover times and improved lane-keeping performance in contrast to a strictly visual takeover request.

Depending on the request stimulus, the time the drivers needed to put the hands back onto the steering wheel, respectively, to take over the driving task while driving highly automated and given different complex takeover requests, was investigated in [21].

The examples described illustrate the advantages of simulator studies in the investigation of a variety of complex and reproducible traffic scenarios, non-related driving tasks, and risky takeover scenarios without endangering the driver or other road users.

### 21.4.4 Data Collection: Observation of Traffic

The observation of traffic can be performed either from a static or a dynamic observation point. In the case of static traffic observations, observation platforms are built at the relevant transport nodes, to capture the flow of traffic and the behavior of road users. In this case, road users refer to vehicles but also pedestrians and other, so-called, vulnerable road users. By analyzing the data of the observed traffic nodes, insight into the behavior of road users can be gained. A disadvantage of this method is that seldom other sensors than cameras are being used. Thus important parameters such as intervals between vehicles, velocity, and acceleration, among others cannot be determined sufficiently.

Alternatively to the static monitoring station, the detection of mundane road traffic situations can be realized from a first-person view by establishing one or more vehicles with sensors and environmental monitoring equipment. By this approach, the technical, financial, and organizational effort to carry out the measurements can vary greatly, depending on the amount of the used monitoring equipment, the number of vehicles, and the overall required length of the route. Often, this approach is used to selectively look for traffic events and their likelihood of occurrence. Since the effort of extracting the relevant events from the raw data can be extremely time
Fig. 21.7 The graphical user interface used in the above described study

As an example, a recent traffic observatory study was conducted in China and will be presented here. The study used test vehicles to gain insight into the traffic situation in China. As part of a pilot study, two test vehicles have been set up in order to acquire first data on the traffic situation in congested traffic in China. Each vehicle has traveled about 8 hours a day for 4 months, with much of the travel time consisting of congested traffic. Due to the built-in measurement technology, consisting of four cameras and four radars, the traffic situation in the front, rear, and side regions of the vehicle were recorded.

The vehicles were driven in two selected cities by two Chinese drivers. During the journeys, the codriver coded the relevant scenarios and objects that have been defined prior to the study.

For this purpose, the codriver was given a control panel with a graphical user interface (Fig. 21.7) to mark predefined road characteristics, such as the type of the road (urban, expressway, and interstate), speed limit, number of lanes, physical separation to opposing traffic, and observed objects, such as pedestrians, cyclists, and lorries. For a better understanding of the scenario, the codriver also recorded additional details, such as light conditions and of special sections of the road (tunnel, junction, roundabout, etc.).

During the analysis of the data, the search for the relevant situations was considerably facilitated by the trigger signals and captured characteristics of the situation set by the codriver. In addition, all site features tagged by the codriver were reviewed and, if felt necessary, corrected. 90% of the codrivers’ captured site features were identified and validated in the video analysis.
During the study an overall travel distance of 8400 km was recorded, with about two-thirds of the travels corresponding to congested traffic. A total of 4610 situations were marked by the codrivers. 1345 cases refer to pedestrian situations and 430 cases to cyclists’ situations. If the number of captured pedestrian situations is set in relation to the distance and time traveled, a pedestrian situation occurs every 47 minutes on a Chinese motorway (interstate). The likelihood of occurrence of pedestrians on the expressways (city ring roads) is about ten times higher. Cyclists occur once, every 8.5 hours on interstate roads and on approximately every 15 minutes on the expressways.

By conducting a traffic observation with vehicles, the likelihood of occurrence of traffic situations, which have to be considered in an analysis of safety in use, can relatively well be objectified. The main disadvantage of this approach is that by the use of professional drivers in the test vehicles, in respect to the driver’s driving style, a low variability arises. Also possible influences due to the drivers’ behavior in emerging traffic situations cannot be excluded.

21.4.5  Field Operational Test

The following section is intended to present a specific method which is particularly useful for collecting in-depth knowledge of the driver, the vehicle, and the environment within their specific constellations. The field operational test (FOT) is a method where participants drive specially equipped vehicles under normal traffic conditions, in order to gain insight and to detect a drivers’ natural driving behavior. When conducting a FOT, a large number of aspects must be considered. These aspects will shortly be described based on a study conducted by BMW. In contrast to the FOT, in the naturalistic driving study, subjects use their own vehicles. However, with both methods, the vehicles are equipped with the appropriate instrumentations to measure drivers’ inherent behavior in the field.

Recently, a FOT was performed in Germany in order to collect information from daily traffic situations. This information can be used for the safety in use assessment and therefore for the safe development of assistance systems. Additionally, a lot can be learned about how drivers handle and interact with the assistance systems and how to incorporate this knowledge into a customer value in the development of future systems. The focus is on the questions of how often certain events (e.g., emergency lanes, congestions, etc.) occur in traffic, how critical they are (e.g., minimum distances to the front vehicle), and how drivers handle them. Here, the method is different to the aforementioned traffic monitoring: the ego driver is the essential factor of this measurement method.

In the current study, seven vehicles were equipped with appropriate measurement technology. They were used by selected drivers for a period of 3 months during the daily driving process. Before making such a time- and cost-intensive study, different factors must be considered and planned accurately. These factors are divided into the following working packages: the general experimental planning and design
phase, vehicles and measurement technology, driving phase, documentation, and evaluation.

In the following paragraphs, these steps are explained in detail and the first results are displayed.

First, the aspect of the “general experimental planning and design” phase will be considered. This includes factors like question selection, sampling, and questionnaire development. A wide range of issues is the basis for all further decisions of the experimental design, e.g., the sample selection. Because vehicles are usually available only for a limited time period, you have to decide whether you want to investigate a lot of different drivers who drive only a short time or a few drivers who can collect long-time experience with the vehicle and the assistance systems. In this study, for example, it was of interest how drivers behave with the assistance systems for an extended period. Questions such as “Adapt drivers their behavior?” and “Can they deal with assistance system limits?” can be addressed.

For the selection of the drivers, certain criteria were applied. Thus, drivers should often take longer routes with a high traffic density, should not work in the development of driver assistance systems, and should not be a novice or a professional test driver. Seven drivers were selected (mean age 32 years; 2 women, 5 men). In addition to the sampling, the development of questionnaires is equally of importance. Therefore, understanding which questions cannot be detected by objective data and need to be covered with other methods are included in this phase. The occurrence of critical events, for example, is particularly important: “Which traffic situation led to the critical event?” and “How was the situation assessed by the driver?” are questions that can be covered with the method of questionnaires.

Next, we take a closer look to the aspect of “vehicles and measurement technology.” This aspect includes factors such as “What kind of assistance systems the vehicles have on board?” and “Which measurement technology and/or additional sensors must be implemented?” Answering these questions and the decision for a specific measurement technology is mainly depending on the issues to be answered. For example, if additional sensors are required, the measurement technology has to ensure that this data will be integrated, and a synchronized recording of the vehicle data and the advanced sensor data is possible. For the questions of the current FOT, the traffic environment was particularly relevant. That is why in addition to the existing sensor technology of the vehicles, four side radars and four cameras were installed in the vehicles. The cameras were each directed to one side, forward, and to the driver.

If the technical modification completed, the sample selected, the test materials and questionnaires finalized, and the participants instructed, starting the driving phase of the field study is feasible. During the conduction the measurement technology should be checked regularly. In complex technical structures in which multiple components must be synchronized, it is advisable to consider not only the functionality of these components but also the quality of data to detect any failures and to correct errors. Another aspect is the support of the participants during they have the vehicle. In addition, the participants had to complete weekly and monthly
given questionnaires, which were related to certain aspects of driving events or the evaluation of the experienced assistance systems.

In parallel to the execution of the driving, the analysis of the data available can be started. In the following some results will be shown.

A system often used by the drivers was the traffic jam assistant. This system helps the driver in longitudinal and lateral control and keeps the vehicle in traffic jams to 60 km/h within certain system limits in the lane. Especially of interest was in which cases the driver overrides this function? What are the causes for the drivers’ wishes to drive differently than the system? To answer this question, a number of parameters can be used. On the one hand, the driving data shows us how many times the function has been overridden by the driver (Fig. 21.8).

This frequency of overrides seems high at the first glance. However, during the study, the traffic jam assistance function was 1812 times active, thus qualifies the absolute number of overriding. On the other hand, you can use the results from the questionnaires to assess how often the driver has experienced a function override. In Fig. 21.9, we can see how drivers evaluate these override moments throughout the study.

This result can be supported with the question of what was the reason for the override. Figure 21.10 shows that vehicles cutting in the drivers’ lane are most often cited as responsible for overriding the function. With some distance, vehicles veering out and after those too little distances to the lane marks are stated reasons for an override.

These results can now be synchronized with the video data and the data of the car. So the information that is available is, for example, whether it was really necessary that the driver reacts or whether the situation could actually have been handled by the system. Using the example “function overdrive”, one can see that it makes sense to refer to various parameters to answer questions. Over time, the drivers are able to detect system deficiencies and system behavior and to decide whether an override is necessary. Therefore, the observation of this parameter throughout the course of the experiment is particularly relevant.
In principle we can summarize that from such extensive studies, a variety of information can be obtained. These are—regarding the driver reactions and driver behavior—especially valid because they were obtained in the natural traffic environment.

### 21.5 Conclusion

With the method of analysis of safety in use, a systematic approach for a holistic assessment of possible risks has been presented, which can be applied with respect to automated systems in road traffic. An essential point is the difference of the concept of system errors in accordance to the ISO 26262 of functional safety. In the ISO 26262, the E/E failure of systems is considered, but not, for example, the
limits of sensor performance. This often perceived by customers as a failure of the functions properties is in the system development per definition a known limit of the function or sensors and no error. Therefore, the system limit is also included in the analysis of safety in use.

For a detailed assessment of the likelihood of personal-hazardous events, extensive knowledge on driver behavior and driving situations is required. The more accurately the quantification of probabilities, the more basic knowledge must be known. For that reason, well-known methods of driver performance studies in the driving simulator to studies in regular traffic or field operational tests, respectively, naturalistic driving studies, are carried out. Aspects like country-specific factors and cultural differences increase the complexity of the analysis, hence, can increase the cost of data collection significantly.

The questions for accepted comparative values in the framework of the quantification of risks are still not answered in the context of automated driving today. In this paper, two approaches, the minimum endogenous mortality and the RAPEX procedure, were explained, which supply as a result of comparable values. Another approach could be to derive indications from a risk–benefit assessment. The development of such reference values and the scientific and social establishment is one of the most important tasks on the way to highly automated driving.

**References**

1. Convention on Road Traffic done at Vienna on 8 November 1968 (1968), http://www.unece.org/fileadmin/DAM/trans/conventn/crt1968e.pdf. Accessed 28 Sept 2015
2. Code of Practice for the Design and Evaluation of ADAS (2009), http://www.acea.be/uploads/publications/20090831_Code_of_Practice_ADAS.pdf. Accessed 28 Sept 2015
3. http://www.transport-research.info/web/projects/project_details.cfm?id=20297. Accessed 28 Sept 2015
4. E. Donges, Aspekte der Aktiven Sicherheit bei der Führung von Personenkraftwagen. Automobil - Industrie 27, 183–190 (1982)
5. ISO 26262, Road Vehicles – Functional Safety.
6. Bengler K, Grundlegende Zusammenhänge von Automatisierung und Fahrerleistung, Beitrag in Fahrerassistenz und Aktive Sicherheit, 16./17.4.2015 (Haus der Technik, Essen, 2014)
7. Rechtsfolgen zunehmender Fahrzeugautomatisierung, Bericht der Bundesanstalt für Straßenwesen, Fahrzeugtechnik Heft F83, 2012
8. Report of the sixty-eighth session of the Working Party on Road Traffic Safety, ECE/TRANS/WP.1/145 (2014). http://www.unece.org/fileadmin/DAM/trans/doc/2014/wp1/ECE-TRANS-WP1-145e.pdf
9. EN DIN 50126, Spezifikation und Nachweis der Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit und Sicherheit (RAMS)
10. Human Mortality Database (University of California, Berkeley and Max-Planck-Institut für Demographische Forschung, Rostock, 2015). www.mortality.org or www.humanmortality.de. Accessed 18 Feb 2015
11. Richtlinie 2001/95/EG des Europäischen Parlaments und des Rates vom 3. Dezember 2001 über die allgemeine Produktsicherheit (2001). http://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32001L0095&from=DE
12. Entscheidung der Kommission, zur Festlegung von Leitlinien für die Verwaltung des gemeinschaftlichen Systems zum raschen Informationsaustausch “RAPEX” gemäß Artikel 12 und des Meldeverfahrens gemäß Artikel 11 der Richtlinie 2001/95/EG über die allgemeine Produktsicherheit (2009).

13. Kompaß K, Helmer T, Wang L, Kates R, Gesamthafte Bewertung der Sicherheitsveränderung durch FAS/HAF im Verkehrssystem: Der Beitrag von Simulation, Beitrag in Fahrerassistenz und Aktive Sicherheit, 16./17.4.2015 (Haus der Technik, Essen, 2014)

14. P. Tetlock, Expert Political Judgment (Princeton University Press, Princeton, NJ, 2005)

15. Neukum A, Krüger H-P, Fahrerreaktionen bei Lenksystemstörungen - Untersuchungsmethodik und Bewertungskriterien, in VDI-Gesellschaft Fahrzeug- und Verkehrstechnik (Hrsg.), Reifen-Fahrwerk-Fahrbahn (VDI-Berichte, Nr. 1791) (VDI-Verlag, Düsseldorf, 2003)

16. Neukum A, Lübbeke T, Krüger H-P, Maysr C, Steinle J, ACC-Stop&Go: Fahrerverhalten an funktionalen Systemgrenzen, in 5. Workshop Fahrerassistenzsysteme - FAS 2008, ed. by M. Maurer, C. Stiller (FAS, Karlsruhe, 2008), S. 141–150

17. T. Bock, Vehicle in the Loop – Test- und Simulationsumgebung für Fahrerassistenzsysteme. Audi Dissertationsreihe, Bd 10, 1st edn. (Cuvillier Verlag, Göttingen, 2008)

18. G. Berg, Das Vehicle in the Loop – Ein Werkzeug für die Entwicklung und Evaluation von sicherheitskritischen Fahrerassistenzsystemen, Dissertation, Universität der Bundeswehr München, 2014

19. D. Damböck, M. Farid, L. Tönert, K. Bengler, Übernahmeverzeiten beim hochautomatisierten Fahren. Paper presented at the 5. Tagung Fahrerassistenz, München, 2012

20. Radlmayer J, Gold C, Lorenz L, Bengler K, How Traffic Situations and Non-Driving-Related-Tasks Affect the Take Over Quality in Highly Automated Driving (HFECS, Chicago, 2014)

21. Naujoks F, Mai Ch, Neukum A, The effect of urgency of take-over requests during highly automated driving under distraction conditions. Proceedings of the 5th International Conference on Applied Human Factors and Ergonomics AHFE 2014, Kraków, Poland 19–23 July 2014