Development and Approval of Automated Vehicles: Considerations of Technical, Legal, and Economic Risks

28

Thomas Winkle

28.1 Introduction

Sensor technology and data processing are constantly improving in their performance. This enables both: continuous further development of driver assistance systems and increasing automation of the driving task, right up to self-driving vehicles [1].

In the following chapter the author traces the technical improvements in vehicle safety over recent decades, factoring in growing consumer expectations. Considering Federal Court of Justice rulings on product liability and economic risks, he depicts requirements that car manufacturers must meet. For proceedings from the first idea until development to sign, he recommends interdisciplinary, harmonized safety and testing procedures. He argues for further development of current internationally agreed-upon standards including tools, methodological descriptions, simulations, and guiding principles with checklists. These will represent and document the practiced state of science and technology, which has to be implemented in a technically viable and economically reasonable way.

28.1.1 Motivation

In the course of this development, technical, especially electrical/electronic systems and software are becoming far more complex in the future. Therefore, safety will be one of the key issues in future automobile development and this results in a number of major new challenges, especially for car manufacturers and their developers. In particular, changing vehicle guidance from being completely human-driven, as it has so far been, to being

T. Winkle (✉)
Department of Mechanical Engineering, Institute of Ergonomics,
Technische Universität München – TUM, 85747 Garching, Germany
e-mail: winkle@carforensic.com

M. Maurer et al. (eds.), *Autonomous Driving*,
DOI 10.1007/978-3-662-48847-8_28

highly or fully automated, raises fundamental questions regarding responsibility and liability. This calls for new approaches—first and foremost new safety and testing concepts [2]. From the legal point of view, automated vehicles require protective safety measures in the development process [3]. The remaining risk must be accepted by users. According to a judgment by the German Federal Court of Justice (Bundesgerichtshof, or BGH), such vehicles must be possible to construct—within the limits of what is technically possible and economically reasonable—according to the respective current state-of-the-art, state-of-science, and must enter the market in a suitably sufficient form to prevent damage [4].

28.1.2 Questions of Increased Automation's Product Safety

Media reports on car manufacturers, suppliers and IT companies' automated research vehicles have predicted for years the preparation for the development of self-driving vehicles, produced in series. Several things still need to be in place however, before these vehicles can be launched on the market. Increasing automation of vehicle guidance calls for cutting-edge, highly complex technology. Particularly with the use of electric/electronic hard- and software, unforeseeable reactions have to be expected, which in the worst cases may even be danger to life and limb. Due to the growing complexity, fully automating all driving tasks in driverless vehicles (see [3])—without a human driver as a backup—currently involves risks, which are difficult to assess. In addition, there are new liability questions and limited tolerance for technical failure. While over 3000 deaths in road traffic currently seem to be acceptable to society in Germany, there is likely to be zero tolerance for any fatal accident involving presumable technical failure. Although automation in driving promises considerable potential safety benefits, the comprehensive commercialization of driverless vehicles can only take place when questions surrounding who is liable and responsible for damage caused by technological systems have been clarified. Acceptance by society may only occur when amongst other things, the benefits perceived by the individual clearly exceed the experienced risks.

An in-depth analysis of automated vehicles' risks to be considered, based on many years' experience in research and product liability, will provide basics for preparing their future series development and commercialization. From this, recommendations for safety assessment will be concluded. To date, amongst others, the following questions remain unsolved:

- How safe is safe enough?
- How is the duty of care assured during development?
- What requirements need consideration when developing and marketing safe automated vehicles?
- Under what conditions is an automated vehicle considered defective?

28.1.3 Technical Continued Development of Assistance Systems—New Opportunities and Risks

From a technical point of view, automated vehicles are presently already able to autonomously take-over all driving tasks in moving traffic. Current series-production vehicles with an optimized sensor, computer, and chassis technologies enable assistance systems with increasing greater performance. Some of the driver-assistance systems on the market today give warning when they recognize dangers in parallel or cross traffic (Lane Departure Warning, Collision-, Lane Change-, Night Vision- and Intersection-Assistance). Others intervene in the longitudinal and lateral dynamics (e.g. anti-lock braking—ABS, Electronic Stability Control—ESC, Adaptive Cruise Control—ACC). Active parking/steering assistance systems provide increased convenience by interventions of steering and braking at low speeds. These partially automated vehicle systems, with temporary longitudinal and lateral assistance, are currently offered for series-production vehicles, but exclusively on the basis of an attentive driver being able to control the vehicle. Supervision by a human driver is required. During normal operation at and beyond the system limits, the system limits or failures of these Advanced Driver Assistance Systems, or ADAS, are thus compensated by the proof of controllability due to the driver (see [5, 6]).

For fully automated driving on the other hand, the driver is no longer available as a backup for the technical limits and failures. This replacing of humans, acting by their own responsibility, with programmed machines goes along with technical and legal risks, as well as challenges for product safety. However, future expectations regarding driverless vehicles—even in a situation of possible radical change—can only be described as using previous experience. Analogies based on past and present expectations concerning vehicle safety will therefore be examined in the following section.

28.2 Expectations Regarding Safety of Complex Vehicle Technology

28.2.1 Rising Consumer Expectations for Vehicle Safety

Fully automated vehicles must be measured against today's globally high level of consumer awareness in vehicles' failures. Since 1965, critical awareness regarding the car industry has evolved more and more, strengthened by the book *Unsafe at Any Speed—The Designed-In Dangers of the American Automobile* [7, 8]. In this publication, the author Ralph Nader blamed car makers for cost savings and duty-of-care breaches at the expense of safe construction and production. With its presentation of safety and construction deficiencies at General Motors and other manufacturers, the book's content scared the public. Nader went on to found the Center for Study of Responsive Law, which launched campaigns against the "Big Three" automobile manufacturers in North America, Volkswagen and other car

companies. Technical concepts were subsequently reworked and optimized. At the center of Nader's criticism was the Chevrolet Corvair. Amongst other things, Nader criticized the unsafe vehicle dynamics resulting from the rear-mounted engine and swing axle. Under compression or extension, it changed the camber (inclination from the vertical axis). By a design modification into an elastokinematic twist-beam or a multilink rear suspension, the inclination remains largely unchanged, which results in more stable driveability and handling. Later, the VW Beetle also came under fire for similar reasons due to its sensitivity to crosswinds. It was also designed with a rear-mounted engine and a swing axle. As a technical improvement VW therefore replaced the Beetle with the Golf, with a front engine, front-wheel drive and more stable handling (market introduction 1974).

Besides the development of new vehicles that were of better design and drove more safely, a further consequence of this criticism was the establishment of the US National Highway Traffic Safety Administration (NHTSA), located within the Department of Transportation. Based on the Highway Safety Act of 1970, it improves road traffic safety. It sees its task as protecting human life, preventing injury, and reducing accidents. Furthermore, it provides consumers with vehicle-specific safety information that had previously been inaccessible to the public. Moreover, the NHTSA accompanies numerous investigations of automobile safety systems to this day. Amongst other things, it has actively promoted the compulsory introduction of Electronic Stability Control (ESC). Parallel to NHTSA activities, statistics from the German Federal Motor Transport Authority (Kraftfahrt-Bundesamt, or KBA) also show increasingly sensitive ways in handling safety-related defects, by supporting and enforcing product recalls [9]. Furthermore, there are now extremely high expectations for vehicle safety. This also can be seen in the extensive safety equipment expected today in almost every series production vehicle across the globe. It includes anti-lock braking (ABS), airbags, and Electronic Stability Control (ESC). The frequency of product recalls has increased, despite passenger vehicles' general reliability and functional safety noticeably rising at the same time. Endurance tests in trade magazines such as *Auto Motor und Sport* show that a distance of 100,000 km can be obtained more often without any breakdowns, unscheduled time in the garage, or defective parts, and without any defect.

28.2.2 Risks and Benefits of Automated Vehicles

Automated vehicles will arguably only gain acceptance within society when the perceived *benefit* (depending on the *degree of efficiency*: "*driver*" versus "*robot*") outweighs the expected *risks* (depending on the *degree of automation*: "*area of action*" versus "*area of effectiveness*"). In order to minimize the risks, manufacturers carry out *accident-data analysis* and corresponding *risk management* (see Fig. 28.1).

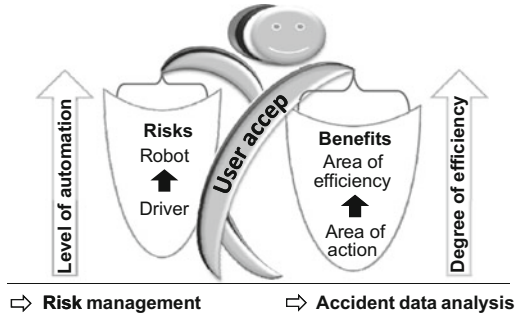

Fig. 28.1 Societal and individual user acceptance may occur contextually, while consumers weigh up the perceived beneficial options and fear for risks in the relevant contexts (see Chaps. 29, 30). Risks depend on the level of automation, benefits of the degree in efficiency. Risk management and accident data analysis (see Chap. 17) allow for objectivities (see Chap. 30) and optimization. Image rights: Autor

For car manufacturers and their suppliers, automated vehicles are an interesting product innovation with new marketing possibilities. Investment decisions and market launches however involve risks that are difficult to assess:

- What risks exist for product liability claims when autonomous vehicles do not meet the requirements of a safe product?
- Which failures may lead to product recalls?
- Will the brand image be sustainably damaged if the automated vehicle does not comply with consumer expectations?

28.3 Legal Requirements and Effects

Society's and individual expectations of technical perfection in vehicles are rising. Higher demands in vehicle quality and functions also call for corresponding safety measures when rolling out automated vehicles. This for example can be seen in the increase of recall campaigns despite increasing technical vehicle-reliability or additional requirements and standards. Applicable comprehensive safety campaigns, such as the Motor Vehicle Safety Defects and Recalls or new obligations for documentation by public authorities also indicate increasing requirements. One example of the latter is the Transportation Recall Enhancement, Accountability and Documentation (TREAD) Act in the USA [10], which introduced a series of new and extensive obligations for documentation and report-keeping for the National Highway Traffic Safety Administration (NHTSA). At the same time, human errors in road traffic are sanctioned individually, without bringing the whole road transport system itself into question.

Highly complex technologies and varying definitions slow down any launch of autonomous vehicles. In addition, the interdisciplinary context contains various technical guidelines. Developers used to be able to get their specifications with standards or guidelines

such as “generally accepted good engineering practice”, “generally recognized and legally binding codes of practice”, “industry standards”, or the “state of the art.” With its decision of 06/16/2009, the German Federal Supreme Court of Justice (BGH) wanted to ramp up requirements for the automotive industry and surprisingly shaped the term “latest state of the art and science”. This creates additional challenges for developers. Functions that are currently feasible in research vehicles for scientific purposes are under laboratory conditions far from fulfilling expectations for series production vehicles, e.g. protection from cold, heat, vibrations, water, or dirt.

From a developer’s point of view, these legal requirements for a careful development of new complex systems can only be fulfilled after validation tests. These should ideally be internationally harmonized and standardized. The German BGH judgment from 2009 explained these development requirements—excluding economic and technical suitability for production—with “… all possible design precautions for safety …” based on “state-of-the-art and science” [4] on the basis of an expert opinion for the preservation of evidence. This opinion, however, requires ultrasound sensors as redundancy for recognition of critical objects to trigger airbags. It should be possible, “… to attach ultrasound sensors around the vehicle which sense contact with an object and are in addition verified by existing sensors before airbag deployment …” [4].

This expert opinion for the preservation of evidence however from an engineering point of view is more than questionable, as current sensor designs only permit a range of a few meters in series production vehicles. Subject to the current state of the art, the application of ultrasonic sensor systems is limited to detecting static surroundings at slow speeds in the scope of parking assistance. The sensors’ high-frequency sound waves can be disturbed by other high frequency acoustic sources such as jackhammers or trucks and buses’ pneumatic brakes, which can lead to false detections. Also poorly reflecting surfaces will not lead to a reflection of sound waves. Object recognition is then entirely excluded [11]. Furthermore, the lawsuit finally concluded that the sensor system concerned worked error-free according to the technical specification.

In addition, the previous fundamental BGH judgment requires that risks and benefits be assessed before market launch:

> Safety measures are required which are feasible to design according to the state of the art and science at the time of placing the product on the market … and in a suitable and sufficient form to prevent damage. If certain risks associated with the use of the product cannot be avoided according to state of the art and science, then it must be verified - by weighing up the risks, the probability of realization, along with the product benefits connected – whether the dangerous product can be placed on the market at all. [4]

28.3.1 Generally Accepted Rules of Technology

An interpretation of the term “generally accepted rules of technology” (allgemein anerkannte Regeln der Technik, or aaRdT) as a basic rule was shaped in a German

Imperial Court of Justice (Reichsgericht) judgment from 1910 based on a decision from 1891 during criminal proceedings concerning Section 330 of the German Penal Code (§ 330 StGB) in the context of building law:

> Generally accepted rules of technology are addressed as those, resulting from the sum of all experience in the technical field, which have been proven in use, and wherever correctness experts in the field are convinced.

In various legal areas, they have different meanings. In terms of product liability, generally accepted rules of technology concern minimum requirements. Noncompliance to the rules would indicate the required safety has not been reached. They are described in DIN-VDE regulations, DIN standards, accident prevention regulations, and VDI guidelines, amongst others [12].

28.3.2 The Product Safety Law (ProdSG)

The German Product Safety Law (Produktsicherheitsgesetz, or ProdSG), in its revised version of 11/08/2011 establishes rules on safety requirements and consumer products. Its predecessor was the Equipment and Product Safety Law (Geräte- und Produktsicherheitsgesetz, or GPSG) of 01.05.2004, which in turn had replaced the Product Safety Law (Produktsicherheitsgesetz, or ProdSG) of 22.04.1997 and the Equipment Safety Law (Gerätesicherheitsgesetz, GSG) of 24.06.1968. Section 3 GSG it describes the general requirements for providing products on the market:

> A product may … only be placed on the market if its intended or foreseeable use does not endanger the health and safety of persons. [13]

28.3.3 The Product Liability Law (ProdHaftG)

Independent of its legal basis for a claim, the term "product liability" commonly refers to a manufacturer's legal liability for damages arising from a defective product. A manufacturer is whoever has produced a final product, a component product, a raw material, or has attached its name or brand name to a product. For product liability in Germany, there are two separate foundations for claims. The first basis is fault based liability, as found in Section 823 of the German Civil Code (BGB) [13]; the second is strict liability regardless of negligence or fault related to the tortfeasor, as contained in the Product Liability Law. Section 1 of the Product Liability Law (ProdHaftG—Law Concerning Liability for Defective Products) of 12/15/1989 describes the consequences of fault as:

> If a person is killed or his or her body or health injured, or if property is damaged, due to a defect of a product, the manufacturer of the product is thus obliged to compensate the injured parties for any losses. [14]

Independently of whether the product defect is caused intentionally or through negligence, a defect is defined in Section 3 of ProdHaftG as follows:

> A product is defective when it is lacking safety which the public at large is entitled to expect, taking into account the presentation of the product, the reasonably expected use of the product and the time when the product was put into circulation. [14]

Should damage arise from a defective product, the Product Liability Law regulates the liability of the manufacturer. Firstly, this entails potential claims of civil liability for property damage, financial losses, personal injury, or compensation for pain and suffering. Liability rests primarily with the manufacturer. In justified cases suppliers, importers, distributors, and vendors may also be made liable without limitation. Furthermore, in cases of legally founded criminal liability, there may also be particular consequences for top management or individual employees, if it is proven that risks were not minimized to an acceptable level (see Fig. 28.3). In cases of serious fault or depending on the offense as negligence, this may involve criminal personal proceedings against a developer.

Besides the potential legal consequences, manufacturers must also expect considerable negative economic effects. Negative headlines in the media can lead to substantial loss in profits or revenue, damage to image, loss in trust and consequently loss of market share. Therefore, when developing new systems, both consequences of potentially legal and economic risks must be considered. Figure 28.2 gives an overview of the potential effects of failures in automated vehicles.

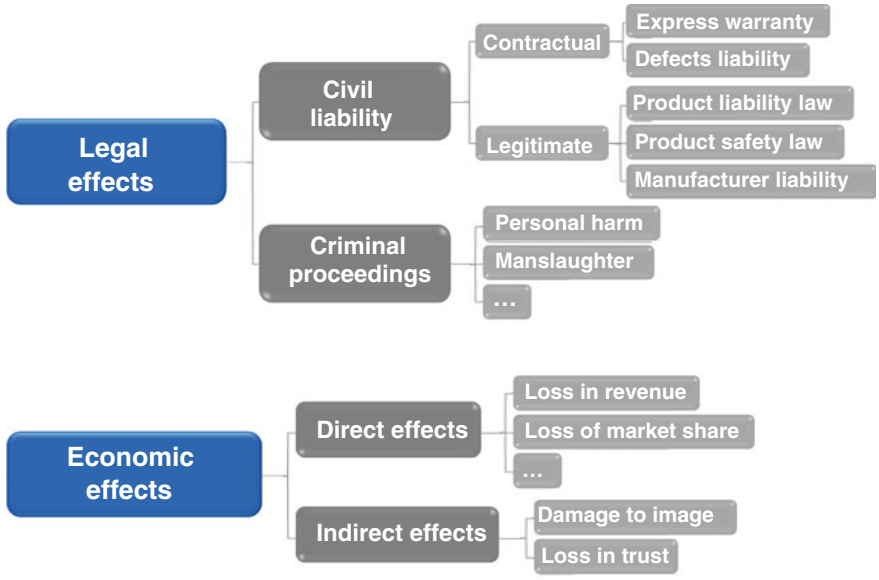

Fig. 28.2 Potential effects of failures in automated vehicles. Image rights: Author

28.4 Product Safety Enhancement in Automated Vehicles Based on Expert Knowledge from Liability and Warranty Claims

28.4.1 Experience from Product Crises

In the future, safe automated vehicles will further depend on integrated quality management systems [15, 16] and safe interactions [17]. In the past, advanced and successful vehicles were frequently affected by product crises.

28.4.1.1 Defective Supplier Parts and -Systems

The following examples document how supplier parts and -systems triggered extensive product crises.

The Ford Explorer was the worldwide best-selling sports utility vehicle. In the USA in May 2000, the NHTSA contacted both the Ford and Firestone companies due to a conspicuously high rate of tires failing with tread separation. Ford Explorers, Mercury Mountaineers, and Mazda Navajos were affected. All were factory-fitted with Firestone tires. At high speeds, tire failures led to vehicles skidding out of control and rollover crashes with fatal consequences. Firestone tires on Ford Explorers were linked to over 200 fatalities in the USA and more than 60 in Venezuela. Ford and Firestone paid 7.85 million dollars in court settlements. Overall compensation and penalties in total amounted to 369 million dollars. In addition to recalling several million tires at great expense, communication errors were made during the crisis: the managers responsible publicly blamed each other. This shattered friendly business relations between the two companies that dated back over 100 years. Harvey Firestone had sold Henry Ford tires for the production of his first car as long ago as 1895. As the crisis progressed it led to serious damage to the companies' images, with sales collapsing for both parties [18].

General Motors (GM) announced a further example of defective supplier parts in February 2014. As a consequence of the financial crisis, the car company had been on the brink of bankruptcy in 2009. It returned to profit for the first time, and won awards for its new models, after a government bailout. But the ignition switches on some models had seemingly been too weakly constructed since 2001, which meant the ignition key sometimes jumped back to the "Off" position while driving. When this happened, not only did the motor switch off, but the brake booster, power steering, and airbags also became deactivated. GM engineers were accused of having ignored the safety defect in spite of early warnings for more than ten years. The company has therefore already been fined 35 million dollars for a delayed recall and now faces billions of dollars of damages claims from accident victims and vehicle owners after mass product recalls [19].

Another huge airbag recall campaign by NHTSA involved 11 different vehicle manufacturers and more than 30 million vehicles only in the United States. Airbag Inflators supplied by Takata ignited with explosive force. The inflator housing in some cases under persistent high humidity as well as high temperature conditions could rupture with metal

shards spraying throughout the passenger cabin and injured or killed car occupants. Several fatalities and more than 100 injuries have been linked to this case which imposed a record civil penalty of 200 million dollar. The airbags were installed worldwide in vehicles from model year 2002 through 2015. Despite these injury risks the Department of Transportation estimated that between 1987 and 2012 frontal airbags have saved 37,000 lives [20].

28.4.1.2 Alleged Sudden Unintended Accelerating or Decelerating Vehicles

Vehicles that automatically intervene in longitudinal and lateral guidance hold considerable risks and provide a target for those who assert that vehicles steer, accelerate and decelerate in unintended, unexpected or uncontrolled ways. The accusation of unintended acceleration due to alleged technical defects has already found some car manufacturers in the media's crossfire. Mainly in the USA, vehicles with automatic transmission are said to have accelerated in an unintended manner by themselves, causing fatal accidents. Affected drivers have initiated waves of lawsuits lasting for decades.

One example of this were the accusations against Toyota, a globally successful company known for quality. Toyota came off very well in customer-satisfaction studies by the American market research firm J. D. Power and Associates in 2002, 2004, and 2005. In 2009, however, it faced accusations of alleged, unintended and sudden accelerating vehicles. These were initially triggered by single incidents of sliding floor mats, which had supposedly been responsible for gas pedals getting jammed. It was then argued that vehicles would have accelerated unintentionally while driving due to the mechanically jammed gas pedals. As Toyota had not responded to the allegations quickly enough in the eyes of the NHTSA, the company was accused of covering up safety problems linked with more than 50 deaths. As well as compensation payments, Toyota had to pay the authority penalties of 66.15 million dollars. This was followed by extensive product recalls, claims for damages and a record 1.2 billion dollar criminal penalty [21].

A further instance of a proven technical defect that led to unwanted accelerations can be seen in an NHTSA recall action in June 2014. The software problem occurred in some Chrysler Sport Utility Vehicles (SUV). When optional adaptive cruise control was activated and the driver temporarily pressed the accelerator pedal to increase (override) vehicle's set speed more than the cruise control system would on its own, the vehicle could continue to accelerate briefly after the accelerator pedal was released again. In this case and according to technical requirements the vehicle has to decelerate to the requested set speed. There were no accident victims to lament. The short-notice initiated recall was restricted to a mere 6042 vehicles [22].

Other great challenges already occurred because autonomous braking systems decelerated in some individual cases without a visible reason for the driver and put vehicles at risk of a rear-end collisions. However, automatic braking and collision warning systems have great potential in reducing road accidents and saving lives. After recognizing a relevant crash object they can automatically apply the brakes faster than humans, slowing the vehicle to reduce damage and injuries. Therefore these systems are recommended to

be made standard equipment on all new cars and commercial trucks. Since November 2013 EU legislation has mandated Autonomous Emergency Braking Systems (AEBS) in different stages with respect to type-approval requirement levels for certain categories of motor vehicles to cover almost all new vehicles in the future [23].

According to NHTSA, the Japanese car manufacturer Honda Motor Company had to recall certain model year 2014–2015 Acura vehicles with Emergency Braking. The reason was that the Collision Mitigation Braking System (CMBS) may inappropriately interpret certain roadside infrastructure such as iron fences or metal guardrails as obstacles and unexpectedly apply the brakes [24]. Furthermore NHTSA investigated complaints alleging unexpected braking incidents of the autonomous braking system in Jeep Grand Cherokee vehicles with no visible objects on the road [25].

Another recall of Chrysler vehicles from 2015 July 24 was, in accordance with NHTSA the first, caused by a software hack. US researchers brought a moving Chrysler Jeep under their control from afar, which forced the company to recall and ensure cyber-security of their onboard software. The affected vehicles were equipped with Uconnect radio entertainment systems from Harman International Industries. Software vulnerabilities could allow third-party access to certain networked vehicle control systems via internet. Exploitation of the software vulnerability could result in unauthorized manipulation and remote control of certain safety related vehicle functions—such as engine, transmission, brakes and steering—resulting in the risk of a crash [26].

In addition to the increase of recall actions the costs for penalties have increased significantly. In 2014 alone, NHTSA issued more than 126 million dollars in civil penalties, exceeding the total amount collected by the agency during its forty-three year history.

Many new technological risks for automated functions in future may not be visible during development and testing. These issues arise in real-life traffic situations and developers have to make necessary changes to the technology ensuring real world traffic safety (see Sect. 28.4.7).

28.4.2 Essential Questions from Previous Product Liability Cases

The author's own experience of previous product liability cases has shown that interdisciplinary structured development is a minimum requirement, especially for safe automated vehicles (see Sect. 28.4.6). In case of damage, the following questions are the key for avoiding civil and criminal claims:

– Before developing a new product, has it already been checked for potential faults—under consideration of the risks, the likelihood of their occurrence, and the benefits—whether the vehicle can be type-approved to be licensed for road traffic use in the intended technological specification?

Essentially, besides general type approval requirements, no globally agreed upon and harmonized methods for fully automated vehicles exist today. These can be generated using international legally binding development guidelines with checklists—similar to the RESPONSE 3—ADAS Code of Practice for the Design and Evaluation of Advanced Driver Assistance Systems ("ADAS with active support for lateral and/or longitudinal control") [5] linked to ISO 26262 [27] (Section 3, Concept phase, Page 24, Controllability):

– What measures beyond purely legal framework were taken to minimize risk, damage, and hazards?

Future guidelines will either be orientated towards today's requirements or to a large extend adopt them. The methods for evaluating risk during development (see Sect. 28.4.4) ensure that no unacceptable personal dangers are to be expected when using the vehicle. Therefore the general legally valid requirements, guidelines, standards and procedures during the development process must at the very least, take into consideration as a minimum requirement:

– Were generally accepted rules, standards, and technical regulations fulfilled?

Only complying with current guidelines is usually insufficient. Furthermore it raises the following questions:

– Was the system developed, produced, and sold with the required necessary care?
– Could the damage that occurred have been avoided or reduced in its effect with a different design?
– How do competitors' vehicles behave, or how would they have behaved?
– Would warnings have been able to prevent the damage?
– Were warnings in the user manuals sufficient or additional measures required?

Whether an automated vehicle has achieved the required level of safety or not can be seen at the end of the development process:

– Was a reasonable level of safety achieved with appropriate and sufficient measures in line with state of the art and science at the time it was placed on the market?

Even after a successful market introduction, monitoring of operation is absolutely necessary. This is still the case when all legal requirements, guidelines, and quality processes for potential malfunctions and safe use of the developed automated vehicle functions have been complied with. The duty to monitor is the result of the legal duty to maintain safety as found in Section 823 Paragraph 1 of the German Civil Code (BGB) [13], where breach of duty triggers liability for any defect that should have been recognized as such. This raises the concluding question for product liability cases:

– Was or is the automated vehicle being monitored during customer use?

28.4.3 Potential Hazard Situations at the Beginning of Development

The day-to-day experience of our technologically advanced society shows: risks and risky behavior are an unavoidable part of life. Uncertainty and imponderables are no longer seen as fateful acceptable events but rather as more or less calculable uncertainties [28]. The result of this are higher demands referring to risk management for the producers of new technologies.

A structured analysis of the hazards in consideration of all possible circumstances can help to give an initial overview of potential dangers. Therefore, in the early development stages it makes sense to provide a complete specification of the automated vehicle, to ensure a logical hazard analysis and subsequent risk classification (see Sect. 28.4.4).

On this basis, it is possible for an interdisciplinary expert team (see Fig. 28.6) to draw up a list of well-known potentially dangerous situations at the start of a project. This usually leads to a large number of relevant situations. Due to practical considerations, scenarios for expert assessment and testing should later be restricted to the most relevant (e.g. worldwide relevant test scenarios based on comprehensively linked up geographically defined accident-, traffic-flow- and weather data collections, see Chap. 17).

According to the system definition, it is recommended to initially gather situations in a list or table. This should take the following into consideration:

- When should the automated function be reliably assured (normal function)?
- In what situations could automation be used in ways for which it is not designed for (misinterpretation and potential misuse)?
- When are the performance limits for the required redundancy reached?
- Are dangerous situations caused by malfunctioning automation (failure, breakdown)?

Jointly drawing up a maximum number of dangerous situations relevant to the system makes it likely that no potential major hazard is omitted or forgotten. Summarizing the hazards with direct impact on safety is recommended as a next step. After cutting the situations down to those that are actually safety-relevant, will technical solutions then be developed.

28.4.4 Methods for Assessing Risks During Development

In discussing phasing out nuclear energy, a German Federal Government publication states that German society—as a “community with a common destiny” and as part of the “global community of risk”—wishes for progress and prosperity, but only accompanied by controllable risks [29]. This is surely only partially transferable to road traffic, where risks of automated vehicles are limited—in contrast to nuclear energy - to a manageable group of people. However, the specific requirements for the methods used in analyzing and assessing risks are similar. Five common methods are outlined below.

28.4.4.1 Hazard Analysis and Risk Assessment

The hazard-analysis and risk-assessment procedure (H&R) is described and annotated in ISO 26262 Part 3 for functional safety of complex electrical/electronic vehicle systems as well as in the related ADAS Code of Practice for the development of active longitudinal and lateral functions (referenced in ISO 26262-3, Concept phase) [5, 6]. Parts of the methods given as examples in the following section (HAZOP, FMEA, FTA, HIL) also point to the H&R. Aim of H&R is to identify the potential hazards of a considered unit, to classify them, and set targets. This will enable dangers to be avoided, thus achieving a generally acceptable level of risk. In addition, an "item" is judged on its impact on safety and categorized to an Automotive Safety Integrity Level (ASIL). An "item" is defined in ISO 26262 as a complex electrical/electronic system or a function that may contain mechanical components of various technologies. The ASIL is ascertained through a systematic analysis of possible hazardous situations and operating conditions. It also involves an assessment of accident severity levels via Abbreviated Injury Scale (AIS) [30] in connection with the probability of occurrence. A reduction to an assumed hardware mean safety failure rate, e.g. ASIL D: $< 10^{-8}$ h^{-1}, for a social and individual accepted risk (see Fig. 28.3) is achieved with external measures [27].

Basically, risk R can be expressed for an analytical approach as function F of the frequency f with which a hazardous event occurs, and the potential severity of harm S of the resulting damage:

$$R = F(f, S) \tag{28.1}$$

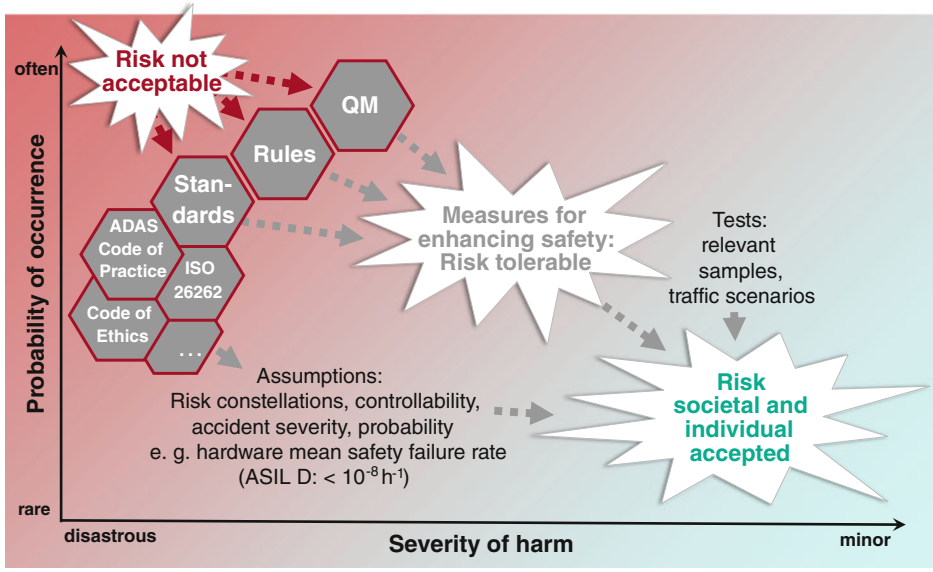

Fig. 28.3 Measures to increase safety for social and individual accepted risks. Image rights: Author

The frequency f with which a hazardous event occurs is in turn influenced by various parameters. One essential factor to consider is how often or how long a person is in a situation where a hazard can occur (E = exposure). Another influence on whether a hazardous event occurs, is if individuals and road users involved in the accident can react with timely response, preventing potentially damaging effects (C = controllability). Controllability via the driver, however, is not present in case of driverless and fully automated vehicles participating in an accident. The product $E \times C$ is a measure of the probability that a defect has the potential in a certain situation to have a corresponding impact on the damage described.

A further factor (λ = failure rate) can be traced back to undetected random hardware failures of system components and dangerous systematic errors remaining in the system. It gives the frequency of occurrence with regard to E with which the automated vehicle can trigger a hazardous event itself. The product f thus describes the number of events to be expected during period E, e.g. kilometers driven or the number of times a vehicle is started.

$$f = E \times \lambda \tag{28.2}$$

Furthermore, ISO 26262 stipulates that the Failure in Time (FIT) of technical and electronic components must also be considered. The unit FIT gives the number of components that fail within 10^9 h.

$$1\,\text{FIT} = \frac{1\,\text{failure}}{10^9\,\text{hours of device operation}} \tag{28.3}$$

Probability of occurrence f and—where possible—controllability C give the Automotive Safety Integrity Levels: either ASIL rating into B, C (a recommended probability of occurrence lower than 10^{-7} h^{-1}, corresponding to a rate of 100 FIT) or D (required probability of occurrence smaller than 10^{-8} h^{-1} corresponding to a rate of 10 FIT). The highest requirements are thus for ASIL D. Besides normal vehicle operation, ISO 26262 also considers service requirements, up to decommissioning of the vehicle. In this regard, developers should take the consequences of aging into account when selecting components. Control units or sensors must be sufficiently protected by robust design in case they were fitted with age-sensitive electrolytic capacitors for energy reserves. A failure must not suspend any important functions [27].

28.4.4.2 Hazard and Operability Study—HAZOP

A Hazard and Operability Study (HAZOP) is an early risk assessment, developed in the process industry. A HAZOP looks for every imaginable deviation from a process in normal operation and then analyzes the possible causes and consequences. Typically, a HAZOP search is carried out systematically by a specialist team from the involved development units. This is to reduce the likelihood of overlooking any important factors [5].

28.4.4.3 Failure Mode and Effects Analysis—FMEA

Failure Mode and Effects Analysis (FMEA) and the integrated Failure Mode, Effects and Criticality Analysis (FMECA) are methods of analyzing reliability that identify failures with significant consequences for system performance in the application in question. FMEA is based on a defined system, module or component for which fundamental failure criteria (primary failure modes) are available. It is a technique for validating safety and estimating possible failure states in the specified design-review stage. It can be used from the first stage of an automation system design up to the completed vehicle. FMEA can be used in the design of all system levels [31, 32].

28.4.4.4 Fault Tree Analysis (FTA)

Fault Tree Analysis (FTA) involves identifying and analyzing conditions and factors that promote the occurrence of a defined state of failure that noticeably impacts system performance, economic efficiency, safety, or other required properties. Fault trees are especially suitable for analyzing complex systems encompassing several functionally interdependent or independent subsystems with varying performance targets. This particularly applies to system designs needing cooperation between several specialized technical design groups. Examples of systems where Fault Tree Analysis is extensively used include nuclear power stations, aircraft, communication systems, chemical and other industrial processes.

The fault tree itself is an organized graphic representation of the conditions or other factors causing or contributing to a defined undesired incident, also known as the top event [5]. One possible approach is to demonstrate the probability of road accidents by the use of a fault tree which presumes both: inappropriate behavior and the existence of a conflicting object [33].

Figure 28.4 shows an example for a Fault Tree Analysis. A single failure does not necessarily have dangerous impact. This Fault Tree Analysis demonstrates that traffic accidents result by the coincidence of several causes. Series of unfortunate circumstances and inappropriate behavior of traffic participants can worsen the risk situation to be uncontrollable. Human traffic participants are the crucial link in the chain to prevent a car crash (see Chap. 17). Especially automated vehicles will require appropriate safety measures. Figure 28.4 demonstrates an excerpt of safety measures for a safe active steering as used in automated vehicles.

28.4.4.5 Hardware-in-the-Loop (HIL) Tests

Increasing vehicle interconnection places particular demands on validating the safety of the entire Electronic Control Unit (ECU) network, e.g. onboard wiring systems safety, bus communication, vehicle-state management, diagnosis, and flash application's behavior. Hardware-in-the-Loop (HIL) tests can be used as soon as a hardware prototype of the system or part of it,—e.g. an electronic control unit in a vehicle—is available. As the Device under Test (DUT), the prototype is placed in a "loop," a software-simulated virtual

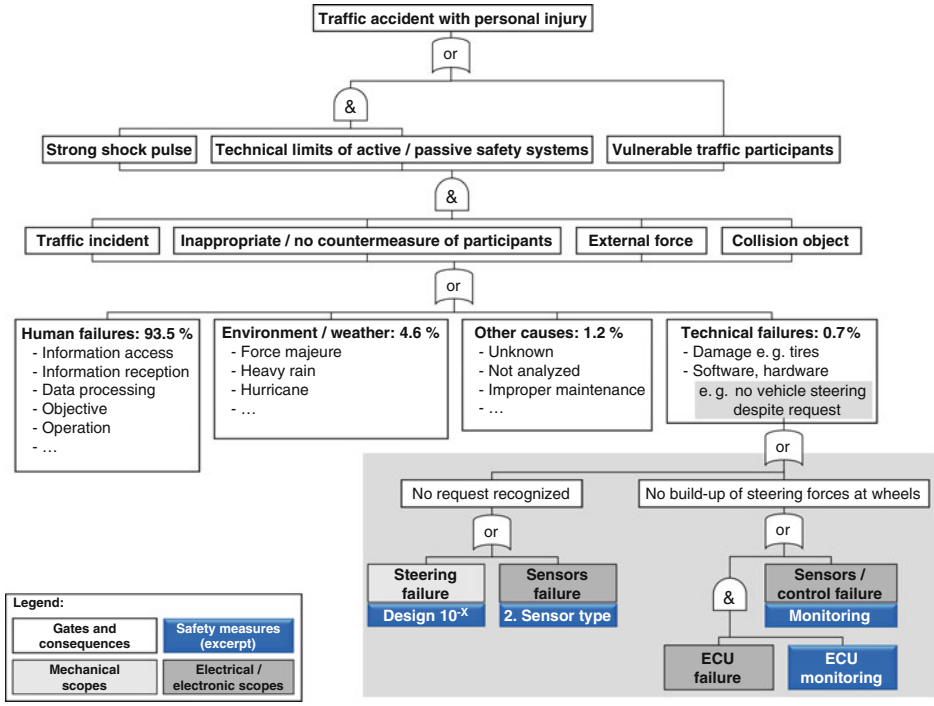

Fig. 28.4 Fault Tree Analysis (*FTA*): functional safety measures prevent traffic accidents caused by technical active steering failures with the risk of personal injury. Image rights: Author

environment. This is designed to resemble the real environment as closely as possible. The DUT is operated under real-time conditions [34].

28.4.4.6 Software-in-the-Loop (SIL) Tests

The method Software-in-the-Loop (SIL) in contrast to HIL, does not use special hardware. The created model of the software is only converted to the code understandable for the target hardware. This code is performed on the development computer with the simulated model, instead of running as Hardware-in-the-Loop on the target hardware. SIL tests must be applied before the HIL.

28.4.4.7 Virtual Assessment

Virtual assessment verifies prospective, quantitative traffic safety benefits and risks (see Sect. 28.1.2). They can be quantified using virtual simulation-based experimental techniques. For this purpose traffic scenarios can be modeled taking into account key safety-relevant processes and stochastic simulation using large representative virtual samples. Virtual representations of traffic scenarios are based on detailed, stochastic models of drivers, vehicles, traffic flow, and road environment, along with their interactions. The models include information from global accident data (see Chap. 17), Field

Operation Tests (FOT), Natural Driving Studies (NDS), laboratory tests, driving simulator tests, and other sources. Wide ranging, extensive simulations help identifying and evaluating safety relevant situations of automated vehicles.

28.4.4.8 Driving Simulator Tests

Driving simulator tests use models of vehicle dynamics and virtual driving scenarios. They allow artificial driving situations and repeatable tests with various subjects. Potentially hazardous traffic scenarios can also be tested because in contrast to real driving the virtual scenario is harmless. Different types of simulators, such as mock-up, fixed based simulator, or moving base simulator exist. Subjective and objective methods can be used to measure the performance of test subjects in the driving task. Depending on the kind of potentially hazardous situations, controllability can be tested by some of these methods. Typical situations for driving simulator tests are high risk situations, driver take-over reactions or interaction between automated driving system environment monitoring and manual human driver mode.

28.4.4.9 Driving Tests and Car Clinics

Driving tests with different drivers provide useful feedback based on empirical data. Dynamic car clinics allow testing of driver behaviour and performance while driving the automated vehicle in defined situations within a realistic environment. In a first step the objective is to identify relevant scenarios and environments (see Chap. 17). This makes it possible to specify and implement virtual tests followed by confirmation via driving tests and car clinics on proving grounds. Finally, before sign-off and start of production (SOP), field tests confirm identified scenarios and environments if necessary.

28.4.5 Approval Criteria from Expert Knowledge

During the approval process, test procedures must be provided. Approval criteria in terms of "passed" and "not passed" are thus recommended for the final safety verification of automated vehicles. Regardless of which methods were chosen for final sign-off confirmation, the experts should all agree on which test criteria suffice for the vehicle to cope successfully with specified situations during a system failure or malfunction. Generally accepted values for achieving the desired vehicle reactions should be used for such criteria. An evaluation can result by using established methods.

Taking the list of potentially hazardous situations as a basis (see Sect. 28.4.3), test criteria for safe vehicle behavior, and if possible also globally relevant test scenarios, are developed by internal and external experts. Of particular importance is a team of system engineers and accident researchers. The former group offers knowledge of the precise system functions, time factors, and experience of potential failures, while accident researchers bring with them practical knowledge of high-risk traffic situations (see Chap. 17). Every known risky situation that a vehicle can get into must be considered. At

least one corrective action with regard to safety requirements should be specified by the developers for the risks identified. In terms of final sign-off confirmation, a test scenario has thus been "passed" when the automated vehicle reacts as expected or otherwise deals with the situation in a satisfactory accepted manner.

28.4.6 Steps to Increase Product Safety of Automated Vehicles in the General Development Process

To guarantee the product safety of automated vehicles, a thorough development concept is needed that is at least in line with state of the art and science. To this end, a general development process is proposed below, as is principally in use amongst car manufacturers for the development of series production vehicles, partially with small adjustments. For highly automated vehicles the development refers to measures regarding the safety process, activities to ensure controllability and appropriate human machine interaction (see Fig. 28.5).

The generic development process for fully automated vehicle functions even more focuses on interdisciplinary networking expert knowledge, the safety process and is represented graphically as a V-Model (see Fig. 28.6). As well as the development stages for the

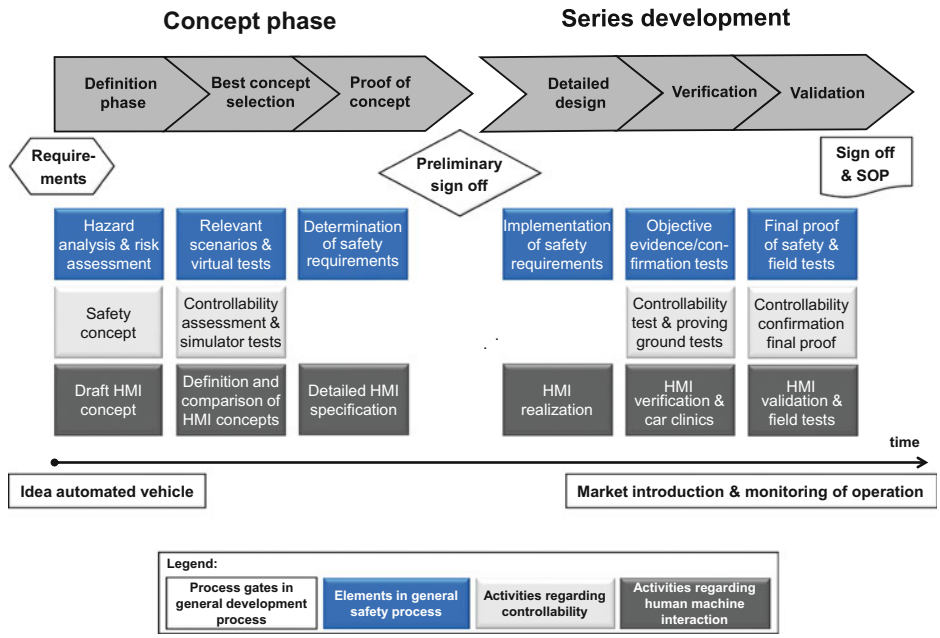

Fig. 28.5 Development process for automated vehicles from the idea until market introduction—involving the safety process, activities regarding controllability and human machine interaction. Image rights: Author

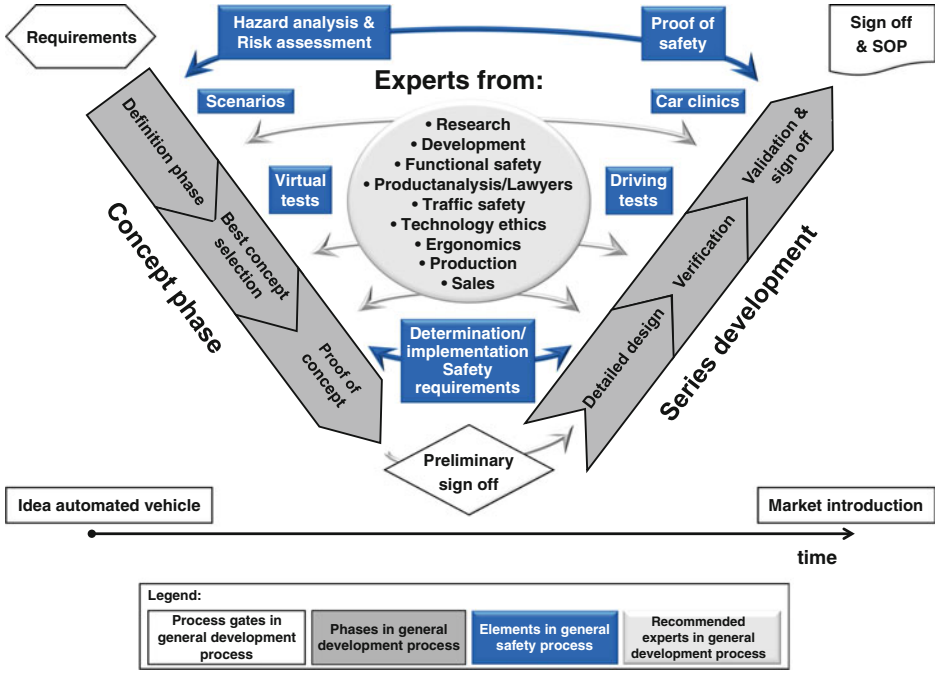

Fig. 28.6 Development process for highly automated vehicles as a V-Model from the idea until market introduction involving recommended interdisciplinary networking experts and the elements of functional safety. Image rights: Author

high automation it depicts logical sequences of product development phases and selected milestones but not necessarily how long each stage lasts or the time between phases [5, 35].

The process thus forms a simplified representation in the form of a V-Model. This allows for iteration loops within the individual development phases involving all parties. Within this V-shaped process structure (see Fig. 28.6) elements of the safety process are taken into consideration. In addition, early and regular involvement of interdisciplinary expert groups is recommended. From the definition phase until validation, sign-off, and start of production—interdisciplinary networking experts from research, (pre-)development, functional safety, product analysis, legal services, traffic safety, technology ethics, ergonomics, production, and sales should participate in the development process.

In the development steps for advanced automated vehicles' product safety functional safety, stands out as a key requirement. It relates to the whole interaction between the vehicle and its environment. Safe driver interaction and take-over procedures [1, 36] should thus be considered when there is an interface necessary to the use case and functionality. Concerning product safety, fully automated vehicles essentially include the following five usage situations: Of prime importance is the functional safety of fully automated vehicles within, at and also beyond the performance limits. Furthermore,

functional safety should be examined during and after system failures. Careful development with regard to a safe usage of driverless vehicles must ensure that they are able to recognize the criticality of a situation, decide on suitable measures for averting danger (e.g. degradation, driving maneuver) that lead back to a safe state, and then carry out these measures.

Figure 28.7 gives an overview of a possible workflow regarding final sign-off, up to decommissioning of a vehicle. In the final stages of developing an automated vehicle, the development team decides whether a final safety test for validation is required. This serves to confirm that a sufficient level of safety for production has been reached. For this, the development team verifies that a vehicle reacts as previously predicted or in other ways appropriate to the situation. The data used here may come from risk-assessment methods used during development, such as hazard and risk analysis. There are three equally valid paths for signing off vehicles. A direct sign-off will be carried out through an experience-based recommendation of the development team. In addition, final evidence of safety can be passed after corresponding reconfirmation via an interdisciplinary forum of internal and external experts or an objective proof. Evidence of functional safety is possible via means of a confirmation test with relevant traffic scenarios based on accident-,

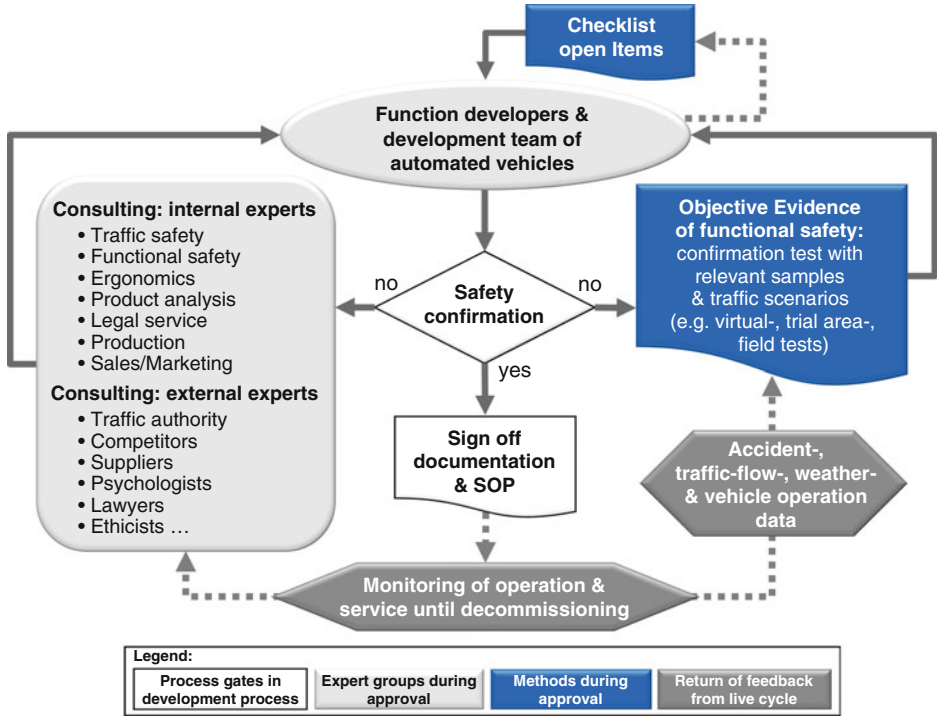

Fig. 28.7 Recommended sign-off process for automated vehicles. Image rights: Author

traffic-flow-, weather- and vehicle operation data (see Chap. 17), or other verifiable samples (see Fig. 28.7).

The development team chooses an appropriate path for each individual scenario. A mixed approach is also possible. When the safety team has conclusively confirmed the safety of the system design functionality, the final sign-off can be given (see [5]).

28.4.7 Product Monitoring After Market Launch

Subsequent to the careful development, a manufacturer is obliged to monitor automated vehicles after placing them on the market, in order to recognize previously unknown hazards and take necessary additional safety measures. If necessary, car manufacturers are urged to analyze potential dangers (that can also arise in unintended use or misuse) and react with appropriate measures, such as product recalls, redesign, or user information (see Fig. 28.7).

A judgment of the German Federal Court of Justice (BGH) is often quoted amongst product safety experts as a particular example of the product-monitoring duty for combination risks with third-party accessories. Model-specific motorbike handlebar cladding, from accessories that had first been passed by officially recognized experts from a testing organization in June 1977, were supposed to have been responsible for three spectacular accidents including one fatality. On the day before the fatal accident, the motorcycle manufacturer in question wrote personal letters to warn all the riders of the affected model it had on record. The victim, however, never received the letter. Although the motorbike manufacturer expressly warned of using the cladding, the company was ordered to pay damages. The BGH's judgment in the matter established a pioneering principle:

> In future, companies will not only be required to monitor the reliability of their products in practice but, above all, to refer their customers to any hazards in daily operation – including those that arise from the application or installation of accessories of other manufacturers. [37]

28.4.8 Steps for Internationally Agreed Best Practices

Due to their networking and complexity, it will be difficult to get a clear overview about all the risks of automated vehicles in series operation. Therefore the objective is establishing worldwide agreed best practices for legislation, liability, standards, risk assessment, ethics and tests.

The ADAS Code of Practice as a result of the Response 3 project was a fundamental step towards European agreed and legally binding guidelines for Advanced Driver Assistance Systems (ADAS). ADAS were characterized by all of the following properties: They support the driver in the primary driving task, provide active support for lateral and/or longitudinal control with or without warning, detect and evaluate the vehicle environment, use complex signal processing and interact direct between the driver and the system [5]. Primarily ADAS operate rule based at the maneuvering level (between about one and ten

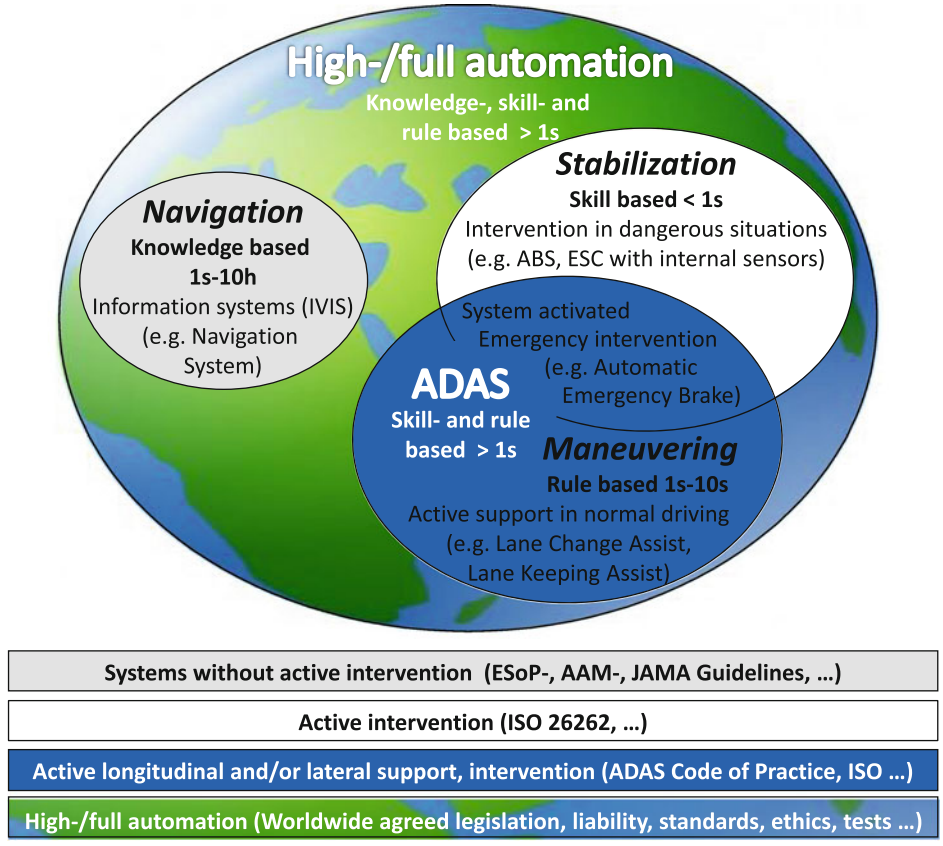

Fig. 28.8 Worldwide agreed legislation, liability, standards, ethics and tests for high-/fully automated vehicles with integration of knowledge based navigation, skill based stabilization and rule based maneuvering levels (globe = outer circle). Further development of the Response 3 ADAS Code of Practice for active longitudinal and lateral support or intervention in dangerous situations (ADAS = *blue* circle). Image rights: Author

seconds) and furthermore within parts of the skill based stabilization level (time spans less than one second). High and fully automated vehicles will intervene in a knowledge-, skill- and rule based manner for more than one second at all driving levels (see Fig. 28.8).

In general increasing sensitivity for defects is visible through a significant growth in product recalls worldwide. If unknown failures appear after vehicles have gone into production, appropriate measures have to be taken where necessary according to a risk assessment.

For analyzing and evaluating risks stemming from product defects after market launch—in view of the necessity and urgency of product recalls—the EU and the German Federal Motor Transport Authority (Kraftfahrtbundesamt) uses tables from the rapid alert system RAPEX (Rapid Exchange of Information System) [38]. To classify risks, first *accident*

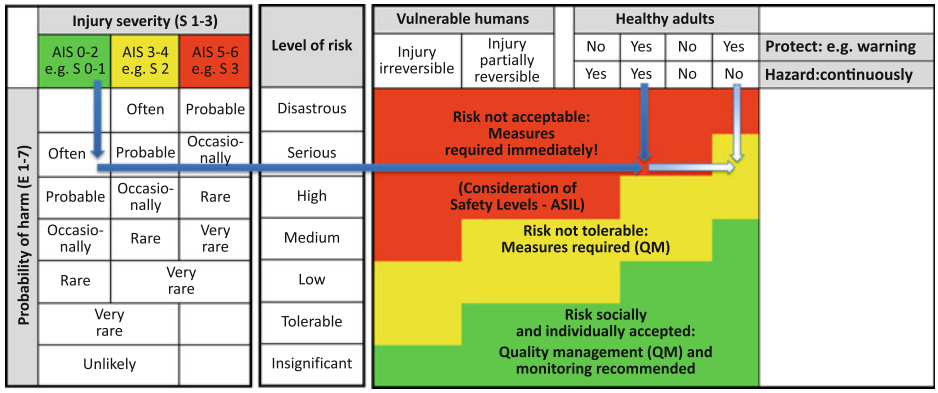

Fig. 28.9 Risk assessment and derivation of essential measures in accordance with RAPEX, ALARP and ISO 26262. *Sources* RAPEX, ADAS Code of Practice, ISO 26262, ALARP. Image rights: Author

severity (extend of damage S according to AIS, for example) and *probability* of harm are assessed—similarly to the ALARP principle (As Low As Reasonably Possible) [39], the ISO 26262 standard [27], and ADAS Code of Practice for active longitudinal and lateral support. The *degree of risk* is derived from this. Final assessment concerning the urgency of required measures looks at the risk of injury for those at particular risk of being injured (as influenced by age, state of health, etc.) and hazard for a mentally healthy adult, and the use of protective measures as appropriate warnings (see Fig. 28.9).

28.5 Conclusion and Outlook

On the one hand, society's expectations are understandable as they increasingly require the highest, state-of-the-art levels of safety for new technologies. On the other hand, unrealistic demands for technical perfection and the striving for 100 % fault-free operation may hinder automated vehicles being launched on the market, and thus the chance of revolutionary potential benefits.

Many groundbreaking technologies would not be available to us today had caution and reservation gained the upper hand during their introduction. One example of courageous innovation is provided by the German engineer and car pioneer Carl Friedrich Benz. As early as 1885, he completed the first test drives with his prototype, the properly functioning Benz Patent-Motorwagen. In his book *Lebensfahrt eines Erfinders*, Benz remembers about his first trip:

> Until that point, it had been at great preference to undertake my test drives far away from the city – on factory grounds or outside on the old, lonely ramparts (ring road), which at that time still went around the city of Mannheim and was hardly walked on –, I no longer shied away from people and their criticism from spring 1886 on. [40]

As the motorcar lay motionless with a breakdown, however, Benz attracted pity, scorn, and derision:

> How can one sit in such an unreliable, squalid, ear-splitting mechanical box. (…) If I had such a stinking box, I would stay home. [40]

Despite all the denial and rejection with which his unceasing work through countless nights for his mission of life was received, Benz, with the support of his wife, held firm to his belief in the future of his Patent-Wagen. Thus he became a trailblazer for one of the most significant innovations of modern mobility.

The preparation of vehicles with advanced degrees of automation likewise requires a determined approach in the mold of Benz. The market launch of highly and fully automated vehicles has also had barriers placed in its path. The first vendors on the market—the pioneers—therefore take on increased risks at the outset, so that the potential total benefit of these new technologies to society can only be achieved together with all interdisciplinary networking parties. Homann describes these decision conflicts during market launch by the decision-theory concept of the so-called "Prisoner's Dilemma". To overcome this dilemma as it pertains to highly and fully automated vehicles, the incalculable risks for manufacturers must be made assessable and determinable through new institutional arrangements [41]. Unconditional information and transparent policy encourage and accelerate public discourse across all disciplines.

Due to previous licensing requirements for series production vehicles, drivers almost always have to keep their hands on the steering wheel and permanently stay in control of the vehicle. Automated research vehicles and vehicle development from IT companies, car manufacturers, and component suppliers will also be required to have a human driver as a responsible backup level in complex traffic situations for the nearby future.

Driverless vehicles, on the other hand, signify the beginning of an utterly new dimension. New approaches and activities are essential [42]. It is required to orientate ourselves to the future potential of automated driving functions, to learn from previous patterns and within the bounds of what is technically and economically reasonable and adjust old methods to validly state of the art or state of science [43].

Besides generally clarifying who is responsible for accident and product risks, new accompanying measures depending on different automation and development levels (see Fig. 28.6) will also be of use for a successful market launch and safe operation. This includes identifying relevant scenarios, environments, system configurations and driver characteristics. Relevant maneuvers of driving robots have to be defined and assessed for example using accident data (see Chap. 17) and virtual methods. Further investigation of real driving situations in comparison with system specifications and additional tests on proving grounds, car clinics, field tests, human driver training or special vehicle studies are recommended. For the required exchange of information, storage of vehicle data (e.g. Event Data Recorder) and possible criminal attacks protective technical measures are necessary (see Chaps. 25, 30). Beside challenging and agreed data protection guidelines [44], experts in technology ethics will ensure compliance with ethical values (see Figs. 28.3, 28.6, 28.7).

Within this, safety requirements have to be answered in terms of "How safe is safe enough?" Expert experience can also decisively contribute in increasing safety and meeting customer expectations for acceptable risks. In light of increasing consumer demands, such experience —particularly of previous product liability actions—makes a valuable contribution to improving product safety during development and approval stages.

Before highly complex automated vehicle technologies—which will additionally be applied in a multi-layered overall system—can go into mass commercialization, interdisciplinary concerted development and sign-off processes are required. A reliable evaluation for sustainable solutions ready for production demands new harmonized methods for comparable safety verification, e.g. by simulating relevant scenarios [45, 46] including the planning of field tests [47] from worldwide available and combined accident-, traffic-flow-, weather- and vehicle operation data (see Chap. 17). This also applies to fulfilling legal and licensing regulations, identifying new options for risk distribution (see [42]), and creating new compensation schemes. To verify the duty of care in existing quality management systems, it is recommended to further develop experience-based, internationally valid guidelines with checklists built on the previous ADAS Code of Practice [5, 48]. These standards will further embody and document state of the art and science within the bounds of technical suitability and economic feasibility. The former ADAS Code of Practice was developed to provide safe Advanced Driver Assistance Systems, with active support of the main driving task (lateral and/or longitudinal control, including automated emergency brake interventions—AEB), on the market and published 2009 by the European Automobile Manufacturers Association (ACEA). It corresponds with the ISO 26262 for requirements of electrical, electronic and software components. As a development guideline it contains recommendations for analysis and assessment of ADAS-Human-Machine-Interactions with occurrence during normal use and in case of failure [5, 6]. With increasing level of automation, upgrades of functional safety, controllability (ISO 26262, ADAS Code of Practice) and other standardized methods will be necessary such as virtual simulation [45, 46]. Today the standards do not cover functional disabilities for instance misinterpretation of objects, traffic situations and resulting false positive system interventions. An integral, scenario based approach is recommended because automated systems will be able to control scenarios. In the event of serious malfunctions that threaten severe damage, product experts from the development process should be involved in the study of the causes and be listened to. With regard to future court decisions, motor vehicle experts who are not directly involved in the development should acquire the expertise to be prepared for a specialist appraisal of new technologies.

In the development of automated driving, networked thinking covering all disciplines is required with a flexible, yet structured area for action. So far, the development has opened up an unknown world with many uncertainties that may cause reservation and resistance. For a successful launch of automated vehicles ready for production, insights collected in vivo from both the past as well as the present are essential prerequisites. Despite the technical, legal, and economic risks, production readiness will be of benefit to society in this way.

References

1. Bengler K, Flemisch F (2011) Von H-Mode zur kooperativen Fahrzeugführung – Grundlegende Ergonomische Fragestellungen, 5. Darmstädter Kolloquium: kooperativ oder autonom? Darmstadt
2. Bengler K, Dietmayer K, Färber B, Maurer M, Stiller C, Winner H (2014) Three Decades of Driver Assistance Systems: Review and Future Perspectives, IEEE Intelligent Transportation System Magazine, ISSN 1939-1390, Volume 6, Issue 4, pp. 6-22
3. Gasser T, Arzt C, Ayoubi M, Bartels A, Bürkle L, Eier J, Flemisch F, Häcker D, Hesse T, Huber W, Lotz C, Maurer M, Ruth-Schumacher S, Schwarz J, Vogt W (2012) Rechtsfolgen zunehmender Fahrzeugautomatisierung, Wirtschaftsverlag NW (Berichte der Bundesanstalt für Straßenwesen F83) Bergisch Gladbach
4. Bundesgerichtshof (2009) Zur Haftung eines Fahrzeugherstellers, BGH Urteil vom 16.06.2009 - VI ZR 107/08, Karlsruhe
5. Knapp A, Neumann M, Brockmann M, Walz R, Winkle T (2009) Code of Practice for the Design and Evaluation of ADAS, Preventive and Active Safety Applications, eSafety for road and air transport, European Commission Integrated Project, Response 3, European Automobile Manufacturers Association—ACEA, www.acea.be, Brussels
6. Donner E, Winkle T, Walz R und Schwarz J (2007) RESPONSE 3—Code of Practice für die Entwicklung, Validierung und Markteinführung von Fahrerassistenzsystemen (ADAS). In Technischer Kongress 2007, Verband der Automobilindustrie (VDA), Sindelfingen, pp. 231-241
7. Nader R (1965) Unsafe at any speed—the designed-in dangers of the american automobile, Grossman Publishers, Inc., New York
8. Nader R (1972) Unsafe at any speed – the designed-in dangers of the american automobile, Expanded edition, Grossman Publishers, Inc., New York
9. Kraftfahrtbundesamt Jahresberichte (2014) http://www.kba.de, Flensburg
10. United States of America (2000) Transportation Recall Enhancement, Accountability, and Documentation TREAD Act—H.R. 5164, and Public Law No. 106-414
11. Noll M, Rapps P (2012) Ultraschallsensorik. In: Handbuch Fahrerassistenzsysteme, 2. Auflage, pp. 110-122, Vieweg+Teubner, Wiesbaden
12. Krey V, Kapoor A (2012) Praxisleitfaden Produktsicherheitsrecht, Hanser, 2. Auflage, Munich
13. Köhler H (2012) BGB Bürgerliches Gesetzbuch, Deutscher Taschenbuch Verlag, 69. Auflage, Munich
14. European Commission (1985) Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products, Brussels

15. International Organization for Standardization (ISO), ISO 9001 (2015) Quality management systems - Requirements, Geneva
16. International Organization for Standardization (ISO), ISO/TS 16949 (2009) Particular requirements for the application of ISO 9001 for automotive production and relevant service part organizations—Functional safety, Geneva
17. Akamatsu M, Green P, Bengler K (2013) Automotive Technology and Human Factors Research: Past, Present and Future, In: International Journal of Vehicular Technology, Hindawi Publishing Corporation, Cairo, New York
18. Hartley R F (2011) Management Mistakes and Successes, 25th Anniversary Edition, 1. Auflage, USA 2011, pp. 342
19. National Highway Traffic Safety Administration (2014) Recall: Electrical System: Ignition Switch, NHTSA Campaign Number: 14V-047, Report Receipt Date: February 7, 2014, http://www.nhtsa.gov
20. National Highway Traffic Safety Administration (2014, 2015) Recall: Defective Front / Side Passenger Air Bag Inflators, Component Manufacturer: Takata Corporation, NHTSA Recall Numbers: 15V-285, 15V-286, 15V-312, 15V-313, 15V-318, 15V-319, 15V-320, 15V-321, 15V-322, 15V-323, 15V-324, 15V-345, 15V-346, 15V-354, 15V-361, 15V-370, 15V-444, 15V-382, http://www.nhtsa.gov
21. National Highway Traffic Safety Administration (2014) Additional Information on Toyota Recalls and Investigations, http://www.nhtsa.gov
22. National Highway Traffic Safety Administration (2014) Recall: Forward Collision Avoidance, Adaptive Cruise Control, Vehicle Speed Control, Accelerator Pedal, Manufacturer: Fiat Chrysler Limited Liability Company LLC, NHTSA Campaign Number: 14V293000, Report Receipt Date: June 4, 2014, http://www.nhtsa.gov
23. Juncker J-C (2015) Commission Regulation (EU) 2015/562 of 8 April 2015 amending Regulation (EU) No 347/2012 implementing Regulation (EC) No 661/2009 of the European Parliament and of the Council with respect to type-approval requirements for certain categories of motor vehicles with regard to advanced emergency braking systems, Official Journal of the European Union, Brussels
24. National Highway Traffic Safety Administration (2015) Recall: Forward Collision Avoidance, Activation of Collision Mitigation Braking System, Manufacturer: Honda Motor Company, NHTSA Campaign Number: 15V301000, Report Receipt Date: May 20, 2015, http://www.nhtsa.gov
25. National Highway Traffic Safety Administration (2015) Date Investigation: Forward Collision Avoidance, Activation of Collision Mitigation Braking System, Manufacturer: Fiat Chrysler Limited Liability Company LLC, NHTSA Action Number: PE15021, Date: June 01, 2015, http://www.nhtsa.gov
26. National Highway Traffic Safety Administration (2015) Recall: Radio Software Security Vulnerabilities, Third Party Access to Vehicle Control Systems, Manufacturer: Fiat Chrysler Limited Liability Company LLC, NHTSA Campaign Number: 15V461000, Date: July 23, 2015, http://www.nhtsa.gov
27. International Organization for Standardization (ISO), ISO 26262 (2011) Road Vehicles—Functional safety, Geneva
28. Grunwald A (2013) Handbuch Technikethik, J.B. Metzler, Stuttgart
29. Merkel A, Töpfer K, Kleiner M, Beck U, Dohnany K, Fischer U, Glück A, Hacker J, Hambrecht J, Hauff V, Hirche W, Hüttl R, Lübbe W, Marx R, Reisch L, Renn O, Schreurs M, Vasssilidis M, Bachmann G, Sauer I, Teuwsen R, Thiel G (2011) Ethik-Kommission Sichere Energieversorgung Deutschlands, Energiewende—Ein Gemeinschaftswerk für die Zukunft, Presse- und Informationsamt der Bundesregierung, pp. 24 ff, Berlin

30. Association for the Advancement of Automotive Medicine (2005) The Abbreviated Injury Scale (AIS) Update 2008, Barrington IL
31. Werdich M (2012) FMEA—Einführung und Moderation—durch systematische Entwicklung zur übersichtlichen Risikominimierung, 2. Auflage, Springer Vieweg, Wiesbaden
32. Verband Deutscher Automobilhersteller (2006) VDA-Band 4, Qualitätsmanagement in der Automobilindustrie, Sicherung der Qualität vor Serieneinsatz—Produkt- und Prozess-FMEA, 2. Auflage, Frankfurt/Main
33. Reichart G (2000) Menschliche Zuverlässigkeit beim Führen von Kraftfahrzeugen, TU München, Maschinenwesen, Lehrstuhl für Ergonomie, Dissertation, Munich
34. Heising B, Ersoy M, Gies S (2013) Hardware-in-the-loop Simulation, In Fahrwerkhandbuch: Grundlagen, Fahrdynamik, Komponenten, Systeme, Mechatronik, Perspektiven, 4. Auflage, pp. 574-575, Springer Vieweg, Wiesbaden
35. Maurer M (2012) Entwurf und Test von Fahrerassistenzsystemen, In: Handbuch Fahrerassistenzsysteme, 2. Auflage, pp. 43-53, Vieweg Teubner, Wiesbaden
36. Bengler K, Zimmermann M, Bortot D, Kienle M, Damböck D (2012) Interaction Principles for Cooperative Human-Machine Systems In: Information Technology, Wissenschaftsverlag Oldenburg
37. Bundesgerichtshof (1987) BGH-Urteil 9.12.1986 = BGHZ 99, 167; BGH NJW 1987, Karlsruhe
38. Europäische Union (2010) Amtsblatt L 22—Entscheidung der Kommission zur Festlegung von Leitlinien für die Verwendung 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, Luxembourg
39. Becker S, Brockmann M, Jung C, Mihm J, Schollinski H-L, Schwarz J, Winkle T (2004) ADAS—from Market Introduction Scenarios towards a Code of Practice for the Development and Evaluation, RESPONSE 2, European Commission, Final Public Report, Brussels
40. Benz C (1925) Lebensfahrt eines deutschen Erfinders, Die Erfindung des Automobils, Erinnerungen eines Achtzigjährigen, Neuausgabe zur 50jährigen Erinnerung, Koehler & Amelang, März 1936, Leipzig
41. Homann K (2005) Wirtschaft und gesellschaftliche Akzeptanz: Fahrerassistenzsysteme auf dem Prüfstand. In Maurer M, Stiller C (eds) Fahrerassistenzsysteme mit maschineller Wahrnehmung, pp. 239-244, Springer, Berlin Heidelberg
42. Matthaei R, Reschka A, Rieken J, Dierkes F, Ulbrich S, Winkle T, Maurer M (2015) Autonomous Driving, In: Winner H, Hakuli S, Lotz F, Singer C (eds) Handbook of Driver Assistance Systems, pp. 1519–1556, Springer International Publishing, Switzerland
43. Scharmer O, Kaufer K (2013) Leading from the emerging future—from Ego-System to Eco-System economies—applying theory U to transforming business, society and self, Berrett-Koehler Publishers, San Francisco CA
44. Hilgendorf E (2015) Teilautonome Fahrzeuge: Verfassungsrechtliche Vorgaben und rechtspolitische Herausforderungen, In Hilgendorf E, Hötitzsch S, Lutz L, Rechtliche Aspekte automatisierter Fahrzeuge, Nomos, Baden-Baden
45. Kompass K, Helmer T, Wang L, Kates R (2015) Gesamthafte Bewertung der Sicherheitsveränderung durch FAS/HAF im Verkehrssystem: Der Beitrag von Simulation In: Klaffke W (eds) Kompass K, et.al. Fahrerassistenz und Aktive Sicherheit: Wirksamkeit—Beherrschbarkeit—Absicherung, Haus der Technik Fachbuch Band 137, Expert Verlag, Renningen
46. Helmer T (2015) Development of a Methodology for the Evaluation of Active Safety using the Example of Preventive Pedestrian Protection, Springer Theses, Springer International Publishing Switzerland

47. Wisselmann D (2015) Technische Fahrzeugentwicklung—Hochautomatisiertes Fahren ab 2020?, In Hilgendorf E, Hötitzsch S, Lutz L, Rechtliche Aspekte automatisierter Fahrzeuge, Nomos, Baden-Baden
48. Becker S, Schollinski H-L, Schwarz J, Winkle T (2003) Introduction of RESPONSE 2, EU Projekt. In: M. Maurer, C. Stiller, Herausgeber, Workshop Fahrerassistenzsysteme—FAS, Leinsweiler