How Stochastic can Help to Introduce Automated Driving

Am Fachbereich Maschinenbau an der
Technischen Universität Darmstadt
zur Erlangung des Grades eines
Doktor-Ingenieurs (Dr.-Ing.)
genehmigte

Dissertation

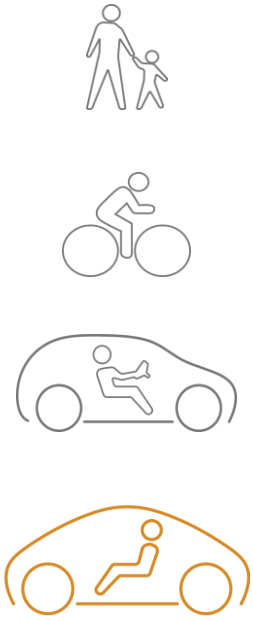
vorgelegt von

Dipl.-Ing. Walther Hans Karl Wachenfeld
aus Schwalmstadt

Berichterstatter:	Prof. Dr. rer. nat. Hermann Winner
Mitberichterstatter:	Prof. Dr. Armin Grunwald

Tag der Einreichung:	19.10.2016
Tag der mündlichen Prüfung:	20.12.2016

Darmstadt 2017
D 17



Erklärung

Hiermit erkläre ich, dass ich die vorliegende Arbeit, abgesehen von den in ihr ausdrücklich genannten Hilfen, selbständig verfasst habe.

Walther Wachenfeld, Darmstadt, 18.10.2016

List of Contents

List of Abbreviations

Abbreviation	Description
ABS	Emergency Brake Assist
ACC	Adaptive Cruise Control
ADAC	Allgemeine Deutsche Automobil-Club e. V.
ADAS	Advanced Driver Assistance System
AD2-	Automated Driving with level of automation 2 (SAE) and lower
AD3+	Automated Driving with level of automation 3 (SAE) and higher
AIS	Abbreviation Injury Scale
ASRS	Aviation Safety Reporting System
BASt	Bundesanstalt für Straßenwesen/General Federal Highway Research Institute
BFU	German Federal Bureau of Aircraft Accident Investigation
CDF	Cumulative distribution function
CIRS	Critical Incident Reporting System
CWA	Cross Wind Assist
DMV	Department of motor vehicles
EBA	Emergency Brake Assist
ECE	Economic Commission for Europe
EU	European Union
ENABLE-S3	European initiative to ENABLE validation for highly automated Safe and Secure Systems
ESC	ESC
ETSC	European Transport Safety Council
FCD	Floating Car Data
GPS	Global Positioning System
HIC	Head Injury Criterion
HiL	Hardware in the Loop
IRTAD	International Traffic Safety Data and Analysis Group
kR	Event Rate
LKA	Lane Keeping Assist
Lkw	Lastkraftwagen
MEM	Minimum Endogenous Mortality
NDS	Naturalistic Driving Studies
OEM	Original Equipment Manufacturer
OuT	Object under Test

PDF	Probability distribution function
PEGASUS	Project for Establishing Generally Accepted quality criteria, tools and methods as well as Scenarios And (German: Und) Situations for approval of highly automated driving functions.
Pkw	Personenkraftwagen
PoS	Proof of safety
RfU	Release for usage
ROC	Receiver Operating Characteristic
RSCS	Road Safety Control System
RSRS	Road Safety Report System
SAE	Society of Automotive Engineers
SHRP 2	Second Strategic Highway Research Program
SOP	Start of Production
SiL	Software in the Loop
StVG	Straßenverkehrsgesetz
StVUnfstatG	Straßenverkehrsunfallstatistikgesetz
SuVi	Super vision
TRL	Technology readiness level
USA	United States of America
VAAFO	Virtual Assessment of Automation in Field Operation
ViL	Vehicle in the Loop
VTTI	Virginia Tech Transportation Institute
V2X	Vehicle to X Communication
XiL	Something (X) in the Loop

List of Symbols and Indices

Symbol	Units	Description
A	-	Number of accidents
Apd	1/km	Accidents per distance driven
a	-	Factor
a	h	8766 h representing the average duration of one year in hours
AR	Depends on application	Number of accidents per amount of exposure
B	-	Binomial distribution function
bpd	€/km	Benefit per distance
C	€	Costs due to events
CP	km/€	Cost performance
cpd	€/km	Cost per distance
d	-	Differential operator
d	km	Distance
e	%	Probability of error
e	-	Euler's number is the base for the exponential function $\approx 2.718 \ldots$
$E(\,)$	Depends on application	Expected value operator
ER	-	Equipment ratio
F	-	Cumulative distribution function
f	-	Function relates numbers of accidents to years.
I	-	Injury
IpA	-	Injury per accident
Ipd	1/km	Injury per distance
$IpUt$	1/h	Injury per usage time
IR	1/h	Injury rate
j	-	Place holder natural number
k	-	Number of events
LoB	-	Level of blank
LoD	-	Level of detection
M	-	Mortality
m	-	Real number
ml	-	Mobility limitation as a share of existing mobility demands
n	-	Number of Bernoulli experiments

Symbol	Units	Description
N	-	Natural number
p	-	Probability for an event of the Bernoulli experiment
$P(\,)$	-	Probability measure
r	-	Ratio
R	Depends on application	Risk
SP	km	Safety performance
t	h	Point in time
Δt	h	Time span
UR	-	Usage ratio
$\bar{v}$	m/s	Average velocity during usage time
x	-	Outcome of a Bernoulli experiment
X	-	Count variable for the outcome of the Bernoulli experiment
y	-	Year
$V(\,)$	Depends on application	Variance operator
Δd	km	Small distance element in the sense of the Bernoulli experiment
μ	-	Expected value
ρ	-	Ratio between two values of same quantity
σ	-	Standard deviation
λ	event	Expected number of events of the Poisson distribution
ψ	km/h	Average yearly velocity

Index	Description
0	Ahead of the release for usage, thus during the testing time span
1	First
1Veh	One vehicle
a	During one year – annually
AB	Autobahn
AD3+	Automated driving level three and higher level
AD2-	Automated driving level two and lower level
all	All vehicles
allG	All vehicles in Germany
allow	Allowed
aRfU	After release for usage in general
aRfUi	After release for usage and real index i
AwI	Accident with injuries
AwF	Accident with fatalities

acc	accepted
acnt	Account
add	added
avo	avoided
avrg	average
bal	Balance in cost and benefit
bench	benchmark
best	Best-case estimation
C	Cost
count	Counted or experienced
cum	Cumulative
d	Distance
detL	Detectors limit
driven	Driven yearly velocity
end	End
endT	End of Δt
ER	Equipment ratio
ex	Exogenous
F	Fatal
fit	fitted
fItem	First item existent
FulDep	Full deployment
i	Real index
intro	Introduction phase
LvD	Mobility limited versus driven
ml	Mobility limitation
newReg	Newly registered
OuT	Object under Test
PbB	Proof being better than benchmark
Pop	Population
proof	Statistical proof of safety or less safety for the whole safety lifecycle
PwB	Proof being worst than benchmark
rel	Relative
replace	Replace
RfU	Release for usage
RvD	Newly registered versus driven
S	Severity
SP	Safety performance
startT	Start of Δt
test	Test

tol	Tolerated
u	Usage
UC	Use case
ud	Usage demand
veh	Vehicle
wF	With fatalities
wI	With injuries
worst	Worst-case estimation
$+$	Higher number of expected value, thus worse system
$-$	Lower number of expected values, thus better system
$\sum$	Total

Deutsche Zusammenfassung

Wie jede Technologie, die vom Forschungsgegenstand zum Massenprodukt weiterentwickelt wird, birgt auch automatisiertes Fahren verschiedenste Vor- und Nachteile. Besonders die Frage der Sicherheit (Safety) der unterschiedlichen Stakeholder in der Gesellschafft ist zu beantworten. Obwohl aktuell eine Vielzahl von Forschern und Entwicklern an der Thematik des automatisierten Fahrens arbeiten, fehlt dennoch ein Konzept zur Bewertung der Sicherheit des öffentlichen Straßenverkehrs mit automatisiert fahrenden Fahrzeugen.

Diese Arbeit schlägt ein solches Konzept zur Bewertung der Sicherheit vor. Das Konzept nimmt eine makroskopische Perspektive für die Sicherheitsbewertung ein, indem die Sicherheit des automatisierten Fahrens durch eine gefahrene Distanz und dabei aufgetretene Ereignisse (z.B. Unfälle) beschrieben wird. Dabei wird angenommen, dass die Verteilung der Ereignisse einer Wahrscheinlichkeitsverteilung für seltene diskrete Ereignisse folgt (Poisson-Verteilung). Der statistische Sicherheitsnachweis kann für aktuell bekannte Use-Cases des automatisierten Fahrens nicht wirtschaftlich erbracht werden. Besser zu sein als der heutige Straßenverkehr entspricht einer Sicherheitsanforderung, die mit dem heutigen Stand der Technik nicht bewiesen werden kann. Allerdings ist auch nicht nachzuweisen, dass der heutige Straßenverkehr an Sicherheit einbüßen würde, wenn das automatisierte Fahrzeug sich ähnlich sicher wie Fahranfänger verhalten würde.

Da beides nicht nachgewiesen werden kann, ist die Sicherheitsanforderung zu verfeinern. Aus einer werden damit zwei Anforderungen: 1. Der Nutzer des automatisierten Fahrens fordert eine objektive Abschätzung der geringsten Sicherheit, der er bei Nutzung ausgesetzt wird. 2. Die Gesellschaft fordert, dass maximal eine zuvor definierte akzeptable Anzahl an Ereignissen in Verbindung mit automatisiertem Fahren entsteht.

Das formalisierte, simulierte und ausgewertete Konzept nutzt Daten des heutigen Straßenverkehrs, sowie fiktive Testdaten um die Erfüllung beider Anforderungen sicherzustellen. Eine konkrete Einführungsstrategie ist das Ergebnis, die gezielt die Nutzung des automatisierten Fahrens limitiert und neu anfallende Informationen aus der Nutzung für eine iterative Anpassung der Limitierung einsetzt. Ein bestärkender Lernzyklus entsteht.

Herausforderungen für die Anwendung und Weiterentwicklung des Konzepts werden diskutiert. Damit das beschriebene Konzept die Einführung automatisierten Fahrens unterstützt, sind vor allem zwei Themen in Zukunft zu bearbeiten: 1. Die Sammlung von detaillierten Daten für die Anwendung des Konzepts auf konkrete Use-Cases. 2. Die Beantwortung einer unausweichlichen Frage: Wie viel Schaden, hervorgerufen durch automatisiertes Fahren, ist akzeptabel für Menschen, die der Technologie ausgesetzt sind?

Summary

Status Quo: Automated systems will replace the human operator at different tasks in everyday life. From today's perspective, these new technologies offer predicted but also unknown benefits. However, as every other new technology, also automated systems will have drawbacks for some stakeholders in our society. As long as new technologies are within readiness levels of research, their impact is mostly negligible. The technology readiness level of automated driving in road traffic is pushed forward strongly by many researchers and developers all over the world. Consequently, the demand for safety assurance gets urgent. From today's perspective, a concept that evaluates the safety of automated driving in an affordable and meaningful way is missing. However, this concept is necessary to enable the introduction of automated driving to public road traffic.

Objectives: The objective of this thesis is to improve the understanding of the challenge for safety assurance on automated vehicles. Therefore a concept is aimed for, that estimates the safety impact for the stakeholders of automated driving. Estimations are always based on assumptions and suffer from uncertainty. For that reason the concept needs to consider and express the underlying assumptions and uncertainties.

Methodology: The methodology for reaching the objectives is formed around the core assumption of the concept: The safety of an Object under Test (OuT) can be described by the parameter of a probability distribution. This parameter connects the number of events $\boldsymbol{k}$ that result from driving a distance d with the safety performance of the OuT $\boldsymbol{SP}_{\mathrm{OuT}}$.

Based on this core assumption a model for safety evaluation is developed iteratively (see Figure 1). First of all the relevant stakeholders that are influenced by the technology are identified and analyzed. The second step identifies measurable requirements for the safety of automated vehicles from the stakeholder's perspectives. Based on this preliminary work on the one hand a usage strategy is defined that controls the introduction of automated vehicles. On the other hand an examination strategy is developed to evaluate whether this strategy enables the automation to meet the requirements. In step four the usage strategy is examined for the Autobahn automation being one representative use case. The results, meaning testing effort and introduction possibilities, are compared and discussed. A refinement of stakeholders as well as requirements is performed. Such a refinement is necessary as only a more precise and subtle analysis will lead to a share between efforts and benefits of the introduction of automated vehicles that forms a basis for the discussion on the safety assurance challenge.

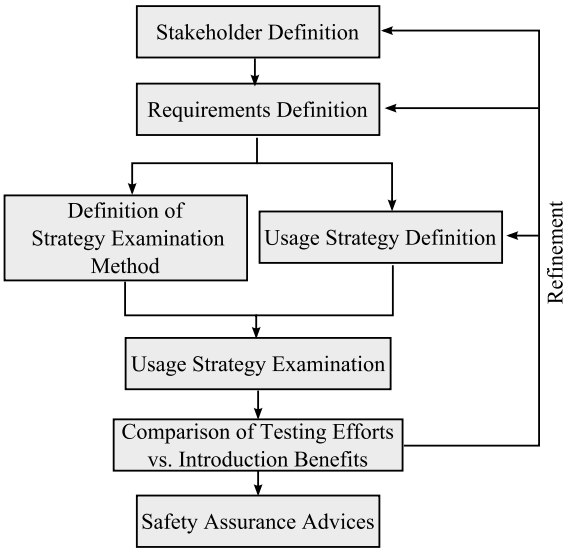


Figure 1 Modeling methodology

Results: The results of the thesis can be grouped into four mayor insights.

Firstly, the number of rare events like accidents can be handled as being a product of a random experiment that depends on a safety performance of a traffic participant and the number of driven kilometers. From today's perspective a falsification of this approach was not found and thus builds a simple first approach. Secondly, the statistical proof of safety based on real-world driving is not economically feasible before mass application of the automated vehicle. Thirdly, refinement of the requirements is necessary and justifiable to reduce the safety requirements. Splitting up the requirements of society and vehicle users leads to reduced testing efforts and an uncertainty-based usage strategy. This uncertainty most likely will reduce during usage, thus also enabling a statistical statement on safety at one point in future. Lastly, a method consisting of evaluation criteria as well as an introduction simulation is developed to examine proposed usage strategies. Thereby the possible safety impacts of the usage are studied.

Conclusion: As the safety of automated driving cannot be proven statistically before introduction, the introduction needs to be performed despite and under consideration of an estimated uncertainty. This does not mean that the introduced vehicles are less safe compared to their benchmark; however during introduction it will be uncertain.

As long as the uncertainty stays above a threshold a usage strategy that is included into the safety assurance concept is necessary. Such a usage strategy would be cautious and based on regular observation of the events encountered by introduced vehicles.

Several challenges have been identified for the developed introduction concept of automated vehicles. Based on these challenges further work should mainly address two topics: 1. The identification and collection of data that is necessary for concept application. 2. The answer of an unavoidable question: How much harm, caused by a human-built machine (AD3+), is acceptable for the exposed humans?

1 Introduction: The Assessment of Automated Systems

Q1 Should automated driving be used on public streets?

In 1886, the first motor vehicle called "Benz Patent-Motorwagen Nummer 1" drove[1] on public streets. A controversial discussion was held whether this new technology should be introduced or not. The supporters of the technology enforced the benefits of usage. Thereupon the automobile was introduced as a commercial (mass[2]) product and got available for many people. Today the automobile affects people worldwide and changed the individual mobility persistently. In the 21st century many new technologies are reaching a technology readiness level[3] that again requires the discussion whether these technologies should be introduced as commercial mass products or not.

Automated driving (find the definition in section 1.1) is one of these technologies. Approximately 80 years went by from the first concrete idea[4] on self-driving cars until experts[5] predict the technology reaching a technology readiness level (TRL) beyond research (TRL 4). Interviews with representatives of vehicle manufacturers present their confidence that "we will have complete autonomy in approximately two years"[6]. Today the stakeholders that will then be affected by automated driving could still discuss whether they want this effect or not. Actually they should discuss that, because automated driving, like most other technologies[7], will not as a matter of course come only with benefits. Gasser et al.[8] graphically explain this uncertain outcome of a new technology for the example of safety.

---

[1] Fersen, O. v.: Ein Jahrhundert Automobiltechnik (1986), p. 16f. https://www.2025ad.com/mission/-welcome-to-2025ad/mission-statement/ accessed 24.09.2016

[2] Volti, R.: Cars and culture: The life story of a technology (2006), p. 23.

[3] European Commission: Technology readiness levels (2014).

[4] Kröger, F.: AD im gesellschaftsgeschichtlichen Kontext (2015), p. 64.

[5] ERTRAC: Automated Driving Roadmap (2015), p. 35–37.

[6] Kirsten Korosec: Interview Elon Musk (2015).. Other vehicle manufacturers or suppliers aren't that optimistic. But from the stand point of safety assessment this is taken as the worst because nearest in future case.

[7] Grunwald, A.: Technikfolgenabschätzung - eine Einführung (2010), p. 23.

[8] Gasser, T. M. et al.: Rechtsfolgen zunehmender Fahrzeugautomatisierung (2012), p. 11.

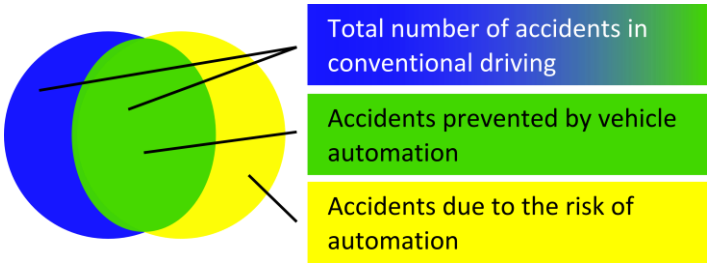


Figure 2: Theoretical potential for avoiding accidents with vehicle automation[8]

Figure 2 illustrates that on the one hand accidents will be prevented by the introduction of automated driving. On the other hand other probably different accidents will be produced by the risk of automation. Consequently, there might be benefits but also drawbacks following the introduction of automated vehicles. How does the ratio between benefits and drawbacks look like?

The goal of this thesis is to support the discussion on the introduction of higher automated vehicles by delivering concrete inputs for the weighting process of some of the most important pros and cons. The train of thoughts that is described in the following thesis explains basic principles to deliver these concrete inputs.

Train of Thoughts - Structure of this Thesis

In six chapters the challenge of weighting pros and cons of automated driving will be narrowed down to safety. This safety challenge will be described by statistical considerations. Its results are going to be interpreted and discussed critically.

The current chapter ("Introduction: The Assessment of Automated Systems") starts to define automated driving and thereby separates it from levels of automation that are already in use. Additionally, the chapter clarifies, which part of the assessment of automated vehicles is in focus and which perspectives are therefore considered.

Chapter 2 "State of the Art: Challenges of Today's Approach to Assess Automated Driving's Safety" explains why automated driving challenges today's approaches to assess safety. This chapter asks for new methods and tools for safety assessment of automated driving.

Chapter 3 "Theory: Stochastic Model for Safety Assessment" describes the main new contribution to research. A new concept for the safety assessment of automated vehicles despite given uncertainties is explained and discussed in detail. Conclusions for different concept parameter combinations are drawn from the simulation of introduction.

Chapter 4 "Application: Data to Apply the Usage Strategy" analyses the suitability of existing databases for the application of the model. Requirements are defined on data that is supposed to be used for application of the usage strategy.

Chapter 5 “Consequences: The Safety Lifecycle of AD3+” reflects how the presented stochastic concept for safety assessment affects the safety lifecycle of automated vehicles. Not only the phase before the start of production but also the other phases during usage are discussed.

Chapter 6 “Conclusion: Critical Concept Reflection” discusses the introduction challenges based on the presented concept. What needs to be done to apply the concept and what might be the result? An outlook will then conclude this thesis.

To simplify the understanding and highlight the necessity of each section a question driven approach is used. Each chapter and first level section answers one question that is of relevance for the train of thoughts. This question is explicitly stated at the beginning of each chapter. At the end of chapter 6 a conclusion is drawn on the meaning of this thesis to answer: “Q 1 Should automated driving be used on public streets?”

1.1 Automated Systems

Q2 What technology is the topic of discussion? What is automated driving?

In principle any field of safety-related automation could be addressed. Whenever automation replaces the human as a machine operator the questions discussed in this thesis get relevant. The questions discussed in this thesis are of special interest when the task is safety critical and an unsupervised/non-correctable automation[9] is installed. Nevertheless due to the motivation given above and the personal interest, this work focuses on on-road motor vehicles and the automation of their driving task.

Automated vehicles, automated driving, driverless driving, automated driving tasks are mainly not defined properly. Whenever these words are used in this thesis, they are used in place for the automated driving systems defined by the Society of Automotive Engineers (SAE). By definition[10] several levels of driving automation exist. These levels[11] are distinguished as depicted in Figure 3. At level zero the human driver executes steering and acceleration of the vehicle, monitors the environment and is the fallback solution for all driving modes. By further increasing the level of automation, the system performs more tasks of the human. The word “system” describes an entity of mechani-

[9] Wachenfeld, W.; Winner, H.: Do Autonomous Vehicles Learn? (2016), p. 457–458.; cf. Nusser, S.: Diss., (2009), p. 21–22.

[10] SAE: International Standard J3016 (2014).; Gasser, T. M. et al.: Rechtsfolgen zunehmender Fahrzeugautomatisierung (2012).; NTHSA: Preliminary Statement of Policy Concerning Automated Vehicles (2013).; VDA: Automatisierung (2015).

[11] The SAE: International Standard J3016 (2014). level are used as the reference.

cal, electrical and electronic hard- and software elements, which senses, thinks and acts like an artificial driver.

SAE level	Name	Narrative Definition	Execution of Steering and Acceleration/ Deceleration	*Monitoring* of Driving Environment	Fallback Performance of *Dynamic Driving Task*	System Capability *(Driving Modes)*
***Human driver* monitors the driving environment**						
0	No Automation	the full-time performance by the *human driver* of all aspects of the *dynamic driving task*, even when enhanced by warning or intervention systems	Human driver	Human driver	Human driver	n/a
1	Driver Assistance	the *driving mode*-specific execution by a driver assistance system of either steering or acceleration/deceleration using information about the driving environment and with the expectation that the *human driver* perform all remaining aspects of the *dynamic driving task*	Human driver and system	Human driver	Human driver	Some driving modes
2	Partial Automation	the *driving mode*-specific execution by one or more driver assistance systems of both steering and acceleration/ deceleration using information about the driving environment and with the expectation that the *human driver* perform all remaining aspects of the *dynamic driving task*	**System**	Human driver	Human driver	Some driving modes
***Automated driving system* ("system") monitors the driving environment**						
3	Conditional Automation	the *driving mode*-specific performance by an *automated driving system* of all aspects of the dynamic driving task with the expectation that the *human driver* will respond appropriately to a *request to intervene*	System	**System**	Human driver	Some driving modes
4	High Automation	the *driving mode*-specific performance by an automated driving system of all aspects of the *dynamic driving task*, even if a *human driver* does not respond appropriately to a *request to intervene*	System	System	**System**	Some driving modes
5	Full Automation	the full-time performance by an *automated driving system* of all aspects of the *dynamic driving task* under all roadway and environmental conditions that can be managed by a *human driver*	System	System	System	**All driving modes**

Figure 3: SAE-level for On-Road Motor Vehicle Automated Driving Systems[11]

Systems up to level 2 are already in traffic[12]. The definition[11] requires that these systems are supervised by the human driver. The human has to monitor the driving environment and he also is obliged to intervene if necessary. At least until today, these systems, that are made to support and do not replace the driver, were successfully tested and sold to customers.

Vehicle systems that monitor the driving environment itself, without the human as a supervisor, do not exist on public streets today. Exactly these systems, beginning from level 3-Conditional Automation, are in focus of the theory that is explained in the next chapters. For this thesis the relevant levels of automated driving systems are called AD3+.

These levels of automation describe only some characteristics of the new technology. But for discussing whether an introduction should be prevented or aimed for, the detailed application of technology is relevant. The so-called use cases[13] of the technology

[12] Bernhart, W. et al.: Index "Automatisierte Fahrzeuge" (2016), p. 5–6.; Winner, H. et al.: Handbook of Driver Assistance Systems (2016), p. 917 - 1396 of part VIII-IX.

[13] Wachenfeld, W. et al.: Use Cases for Autonomous Driving (2016).

can vary in a wide range and so can the benefits and drawbacks of the technology. If, for example, automated driving is applied to a slowly driving vehicle that serves as a campus shuttle, benefits and drawbacks are different ones than those of a privately owned car equipped with automated highway driving.

Literature describes many different use cases that could sooner or later become reality. Winner[14] structures the different use cases along three dominant introduction paths. One path starts at simple scenarios and reaches vehicle automation with the use case "Autobahn Pilot". The second path starts with low speed and develops to the first use case being the "automated valet-parking". The third orthogonal path addresses critical situations and will come to the first automated system by the so-called "emergency automation". To challenge the theory developed during the following chapters, one representative use case along each of the three paths will be discussed and therefore be introduced in the following.

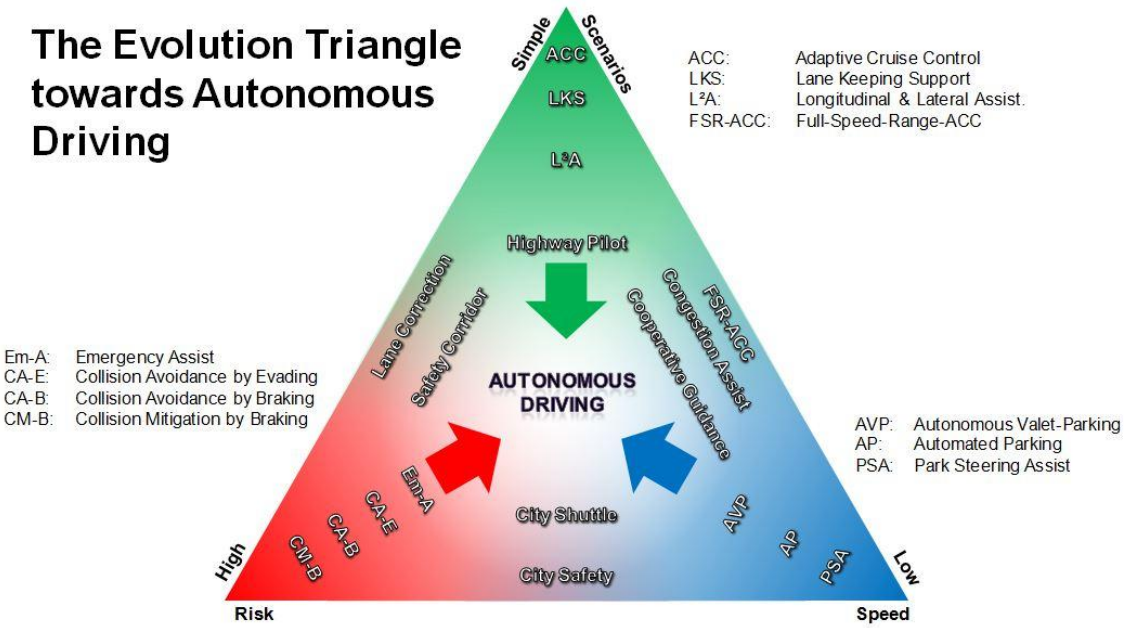


Figure 4: Evolution to automated driving, beginning with three starting points in the corners of the figure[14]

Besides the evolutionary approach following the triangle, there exist additional possibilities to increase the availability of automated driving successively within each path. Representative projects which follow this approach can be found at Google Inc.[15] or Volvo Car Corporation[16]. The availability of automated driving will firstly be limited to

[14] Winner, H.: ADAS, Quo Vadis? (2016), p. 1577ff.

[15] https://www.google.com/selfdrivingcar/ accessed 24.09.2016

[16] http://www.volvocars.com/intl/about/our-innovation-brands/intellisafe/intellisafe-autopilot/drive-me accessed 24.09.2016

a narrow area or circumstances. This could be a certain section of highways or infrastructure in general, like the roads from San Francisco to Palo Alto in sunny California or around the inner city of Gothenburg. A fourth use case, the "Seed Automation", is introduced to study the applicability of the developed theory for this kind of use cases as well (see section 1.1.4).

1.1.1 Use Case - Autobahn Pilot[17]

The driving robot takes over the driving task of the driver exclusively on interstates or interstate-like expressways (Autobahn). The driver is just a passenger during the automated journey, can take his/her hands off of the steering wheel, feet off the pedals, and can pursue other activities.

As soon as the driver has entered the Autobahn, he/she can, if desired, activate the driving robot. This takes place most logically in conjunction with indicating the desired destination. The driving robot takes over navigation, guidance, and control[18] until the exit from or end of the Autobahn is reached. The driving robot safely coordinates the handover to the driver. If the driver does not meet the requirements for safe handover, e.g. because he/she fell asleep or appears to have no situation awareness, the driving robot transfers the vehicle to the risk-minimal state on the emergency lane or shortly after exiting the Autobahn. During the automated journey, no situation awareness is required from the occupant; the definition for high automation according to SAE[19] applies. Because of simple scenery and limited dynamic objects, this use case is considered as an introductory scenario, even if the comparatively high vehicle velocity exacerbates accomplishing the risk-minimal state considerably.

1.1.2 Use Case - Automated Valet-Parking[17]

The driving robot parks the vehicle at a remote location after the passengers have exited and cargo has been unloaded. The driving robot drives the vehicle from the parking location to a desired destination. The driving robot re-parks the vehicle.

The driver saves the time of finding a parking spot as well as of walking to/from a remote parking spot. In addition, access to the vehicle is eased (spatially and temporally). Additional parking space and search for parking is arranged more efficiently.

If a driver has reached his/her destination (for example place of work, gym, or home), he/she stops the vehicle, exits, and orders the driving robot to park the vehicle. The

[17] Wachenfeld, W. et al.: Use Cases for Autonomous Driving (2016).

[18] Cf. Donges, E.: Fahrerverhaltensmodelle (2011).

[19] SAE: International Standard J3016 (2014).

vehicle can be privately owned, but might also be owned by a car-sharing provider or in general possession might change due to other business models. Therefore, the driving robot may now drive the vehicle to a private, public, or service-provider-owned parking lot. It is important to assign a parking lot to the driving robot. The search for the respective parking lot by the driving robot is not taken into consideration for this use case. Therefore a defined destination for the driving robot is always given. Because of the low velocity and the light traffic situation, the deployment of automated Valet-Parking is limited to the immediate vicinity of the location where the driver left the vehicle. This limitation reduces the requirements regarding the (driving-) capabilities of the driving robot significantly, because lower kinetic energy as well as shorter stopping distances result from lower velocity.

An authorized user in the vicinity of the vehicle can indicate a pick-up location to the driving robot. The driving robot drives the vehicle to the target destination and stops, so that the driver can enter and take over the driving task. If desired by the parking lot administration, the driving robot can re-park the vehicle.

1.1.3 Use Case - Emergency Automation

A human is driving the vehicle in regular situations. The emergency automation only intervenes in that moment when 9X % of human drivers would get into an emergency situation. Steering, braking, and accelerating the vehicle are the intervention options of the driving robot. The emergency automation is not limited to any area of application but to situations of high risk. Although the driving robot can handle situations of high risk, it is not made to drive the vehicle from A to B.

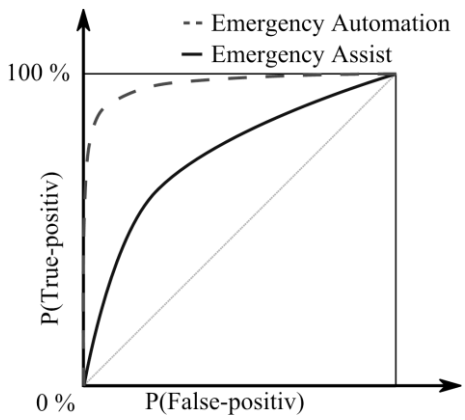


Figure 5: A best guess of an ROC for Emergency Assist vs. Emergency Automation

The difference between existing emergency assistants and the described emergency automation is the share of true-positive actions in respect to all actions. Today's systems, as they assist humans, can have a low number of true-positive actions. Figure 5 explains this by depicting a characteristic receiver operating characteristic (ROC). The

human compensates or just doesn't benefit as much as possible from the assistant system. The emergency automation however aims to reach a true-positive level that can compete with the upper percentile of human drivers without excessively showing false-positive reactions.

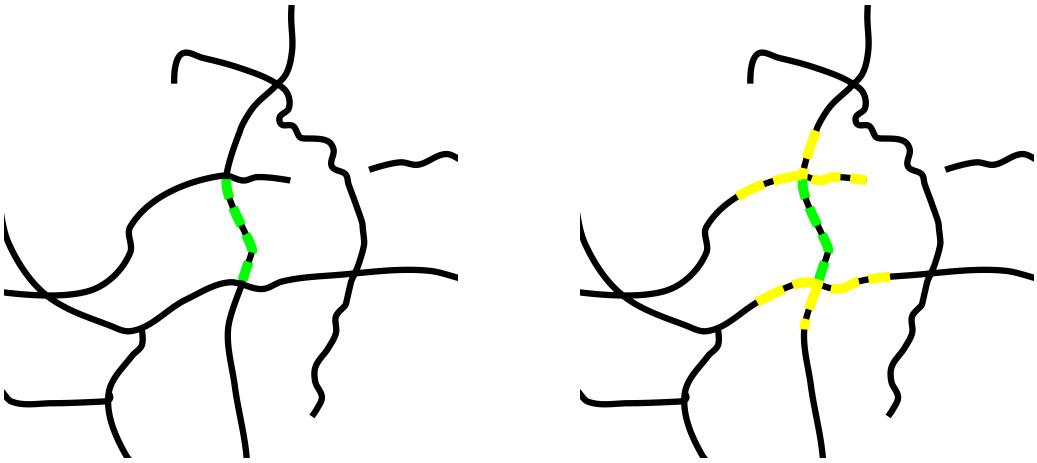
This automation aims to be active in every scenario and area in regular traffic.

1.1.4 Use Case - Seed Automation

The word "Seed Automation" is defined for the first time in this thesis. The automation is applied like a seed/a first starting point, which needs to grow along different dimensions to reach the full benefits of the described use cases. The dimension might be the area of application, the tolerated weather conditions for application etc.

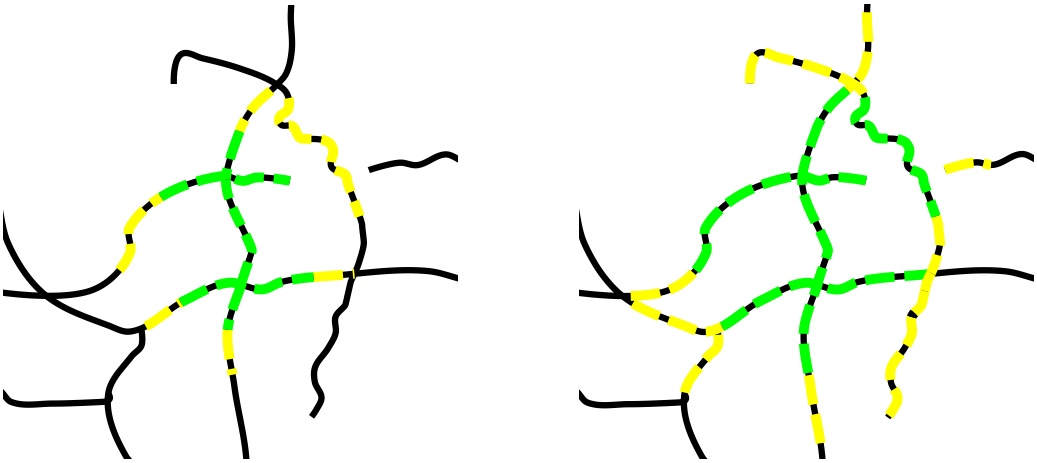
For example, the seed automation drives the vehicle in a narrow operation area of one of the above defined use cases. For example the Drive Me Project[20] aims to apply an Autobahn Pilot to a predefined road segment (approx. 80 km) that limits speed (average speeds of 70 km/h) and other dynamic objects (no pedestrians). Additionally for the beginning, the functions will be limited to certain, eventually good, weather conditions. The selected road segment is a closed loop from Hisingen, Frölunda to Mölndal.

The Drive Me Project has not reported whether the segment for application will be enlarged. However, the Seed Automation use case assumes this. The spatial evolution of the Autobahn Pilot is simplified and depicted in Figure 6. The use case starts between two Autobahn junctions. From time step to time step this area is extended.



a) Time Step 1 b) Time Step 2

[20] http://www.volvocars.com/intl/about/our-innovation-brands/intellisafe/intellisafe-autopilot/drive-me accessed 24.09.2016



c) Time Step 3 d) Time Step 4

Figure 6 Evolutionary growth of the seed automation at a road-net of highways at four time steps a) to d). Green areas are open for automated driving, yellow areas are under examination.

1.2 Benefits & Drawbacks of AD3+

Q3 What benefits and drawbacks result and thus support or prevent the introduction of AD3+?

The manifold the use cases of automated driving are, the manifold are their benefits and drawbacks. This section will not list benefits and drawbacks for automated driving. There exist many publications[21] and public discussions[22] that to greater or lesser extent systematically derive possible pros and cons. Of importance is the fact that many benefits and drawbacks could result from the introduction and these benefits and drawbacks are strongly interconnected. Thus, simply deriving requirements from one type of drawback without checking and evaluating other types of benefits is not valid. The decision on introduction can thus not be made based on one specific benefit. Examples for weighting different benefits and drawbacks exist in the mobility sector of today's public traffic. To go from one place to another different alternatives are accessible: walk, ride a bike or a motorbike, drive a car or truck, use an autobus, and go by train, boat or plane. Each modality has its own pros and cons and consequently is accepted for mobility demands. If just one criterion would be used for decision some forms of mobility would just not exist. The balance of different criteria leads to the decision of introduction.

The critical point of making a decision about the introduction is to clearly identify the benefits and drawbacks. Benefits and drawbacks can easily be speculated about. But most of them are not as easy to predict as it is often done. Especially when a technology or product does not exist, the exact definition of what will happen after the introduction is just not possible. The goal of this thesis is to participate on the research question on how to predict one of the crucial effects of automated driving. A new approach for predicting the safety impact resulting from the introduction and use of automated driving is the core of this thesis.

---

[21] Fraedrich, E. et al.: Transition pathways to fully automated driving (2015)., Thomopoulos, N.; Givoni, M.: The autonomous car—a blessing or a curse (2015)., Gurney, J. K.: Sue my car not me (2013)., Beiker, S. A.: Legal Aspects of Autonomous Driving (2012)., Litman, T.: Autonomous Vehicle Implementation Predictions (2014).; EU Transport Ministers: Declaration of Amsterdam (2016).

[22] http://www.statetechmagazine.com/article/2014/09/pros-and-cons-driverless-cars-infographic; http://www.autoinsurancecenter.com/top-20-pros-and-cons-associated-with-self-driving-cars.htm; https://sites.google.com/site/unibathautonomouscars/services ; http://www.gizmag.com/pros-and-cons-driverless-cars-traffic-future/35841/; http://www.itsinternational.com/categories/location-based-systems/features/autonomous-vehicles-the-pros-and-cons/;https://www.washingtonpost.com/news/the-switch/wp/2016/02/05/why-you-should-consider-getting-a-driverless-car-in-1-chart/; Hearing focus of SF 2569 Autonomous vehicles task force establishment and demonstration project for people with disabilities http://mnsenate.granicus.com/MediaPlayer.php?view_id=1&clip_id=235 all last accessed 22.09.2016

As safety in its general meaning is still a topic with many facets[23]:

> *Safety is the state of being "safe" (from French sauf), the condition of being protected against physical, social, spiritual, financial, political, emotional, occupational, psychological, educational, or other types or consequences of failure, damage, error, accidents, harm, or any other event that could be considered non-desirable.*

In the technical domain of road traffic it is already narrowed down to[24]

> *absence of unreasonable risk*

with risk beeing[24] the

> *combination of the probability of occurrence of harm and the severity of that harm*

and harm is explained as[24]

> *physical injury or damage to the health of people.*

This thesis explicitly concentrates on the safety that is described by the number and severity of road accidents where the word road accident describes the physical energy exchange of one vehicle with another vehicle, pedestrian, animal, road debris, infrastructure, or nature in general. Such an accident results property damage, injuries, or fatalities. This chosen focus excludes security[25] from the discussion, although security issues can also result in safety issues.

Nearly every motivation for automated driving argues that the human being is the cause for $9X$ % of today's accidents[26] in road traffic. It is concluded when we remove this human driver we will reduce the number of accidents. Of course it is true that the numbers caused by human errors will vanish. But there is missing one major step in the logic to compare the numbers. Someone, or rather something, has to conduct the vehicle thus take over this challenging job. As Figure 2 motivates, this can result in new and other cases of accidents. Consequently, if one will use safety as an argument for introduction, pros but also cons have to be identified, estimated and balanced carefully[27].

Figure 7 illustrates the theoretical risk avoidance potential in a qualitative way, depending on the severity of the accident. Figure 7 adheres to the findings of Heinrich[28] and

---

[23] Wikipedia: Safety (2015).

[24] ISO: DIS 26262: Road vehicles - Functional safety (2008), p. 1ff in part 1.

[25] http://www.oxforddictionaries.com/ defines security:"The safety of a state or organization against criminal activity such as terrorism, theft, or espionage" whereas safety:"The condition of being protected from or unlikely to cause danger, risk, or injury" accessed 24.09.2016

[26] U.S. DOT: Federal Automated Vehicles Policy (2016), p. 5. Singh, S.: Critical Reasons for Crashes (2015), p. 1.

[27] Grunwald, A.: Societal Risk Constellations for Autonomous Driving. (2016).

[28] Ward, R. B.: Revisiting Heinrich's law (2012).

Hydén[29] that accidents of decreasing severity occur in larger numbers. The scale of the related severity of the accident is ordinal, meaning that there is clearly an order between the different degrees of severity: For example, a fatality is weighted as graver than a serious injury. However, academics are divided[30] on the way how to derive and apply the relative weighting of these different degrees. While degrees of severity are compared in terms of costs, this scale gets continuous.

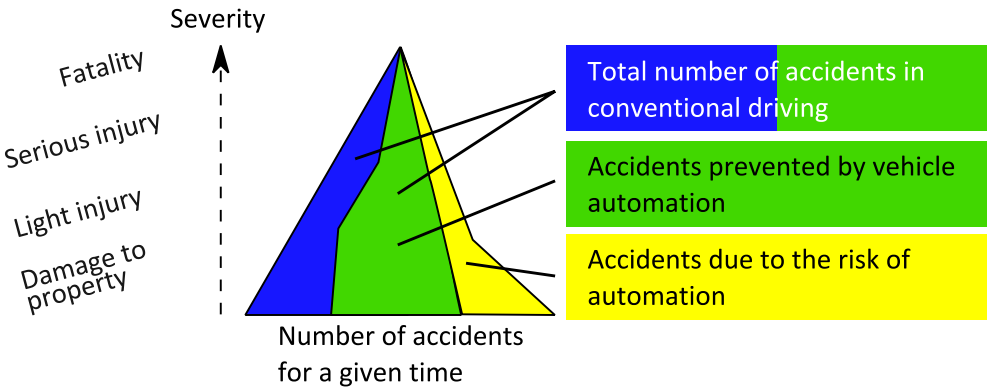


Figure 7 Theoretical potential for avoiding accidents with vehicle automation with consideration of severity of accident (similar to Gasser et al. see Figure 2)

Considering the severity and the number of accidents, it shows that while accidents are removed (Figure 7 green area), there are remaining ones (Figure 7 blue area) which are not addressed by vehicle automation. In addition, new accidents are created by the substitution of humans and the automated execution of the driving. The human is no longer available as a backup in the case of a failure or a defect. The yellow area in Figure 7 illustrates these additional numbers. It is uncertain whether the removal of accidents and the creation of additional ones are uniform across the degrees of severity. It is possible that there is a greater reduction in serious accidents but an increase in less serious accidents. Figure 7 illustrates this idea via the deformation of the assumed triangle.

For the safety assessment of fully-automated driving, this means that not only a reduction in the number of accidents must be proven, but rather an accepted ratio ρ_{acc} between avoided risk R_{avo} and additionally caused risk R_{add}.

$$\rho_{\mathrm{acc}} = \frac{R_{\mathrm{add}}}{R_{\mathrm{avo}}} \tag{1-1}$$

The value for this accepted ratio is the result of a complex discussion among those who would be affected by automated driving. This value varies depending on various factors such as societal, political and economic differences. A vivid example of this is the ac-

[29] Hydén, C.: The development of a method for traffic safety evaluation (1987).

[30] Baum, H. et al.: BASt: Volkswirtschaftliche Kosten Herleitung (2011), p. 7–10.

ceptance of the use of nuclear energy in Germany, the USA, or Japan in the last years: On the one hand, the accepted ratio varies considerably between the countries, and on the other, this changes over time, so that for example in Germany in 2012, a nuclear phase-out was decided on. For that reason later in this document one possible approach to derive a value for what could be acceptable is derived. However, this thesis is not able to state the final value. Something *accepted* is nothing that can be defined by some stakeholders. A discussion on what it means when people accept a new technology can be found in Fraedrich et al.[31]. It is the discussion of something acceptable that is in focus.

Risk as the opposite of safety[32] contains three central semantic elements following Grunwald[33]:

> *The moment of uncertainty, because the occurrence of possible damage is not certain; the moment of the undesired, because damage is never welcome; and the social moment, because both opportunities and risks are always distributed and are always opportunities and risks for particular individuals or groups.*

Before it can be answered what quantitative benefits and drawbacks by means of safety will result when introducing automated driving, the taken perspectives need to be identified.

1.3 Societal Risk Constellation[33]

Q4 Whose health or property is affected by the introduction of automated driving?

Every human is affected[33] individually by technology. To discuss the introduction of a new technology certain groupings need to be identified that hold similar characteristics. There exists a certain social risk constellation, for instance different groupings like decision-makers, regulators, stakeholders, affected parties, advisors, politicians and beneficiaries are affected and profit in a different way from automated driving[34]. As discussed above, this thesis will focus on the safety aspect that is connected with the occurrence of accidents. Thus, a certain physical proximity to a vehicle is necessary to be affected of automated driving. The ones that are in this proximity are called the

[31] Fraedrich, E.; Lenz, B.: Societal and Individual Acceptance of Autonomous Driving (2016).

[32] Safety is defined by the absence of unreasonable risks. ISO 26262 But cf. Smith, B. W.: Regulation and the Risk of Inaction (2015). p.595f

[33] To get a more detailed discussion on this topic the chapter of Grunwald, A.: Societal Risk Constellations for Autonomous Driving. (2016). should be read.

[34] Grunwald, A.: Societal Risk Constellations for Autonomous Driving. (2016). discusses different risks: accident, transportation system, investment, labor market , accessibility, privacy and dependency risk

affected parties and are in focus of this discussion. One vehicle driven in one street doesn't directly influence the safety of someone being in the neighboring street. This is different for a technology like nuclear plants or the like. One major nuclear plant accident does affect everyone in its greater vicinity. Consequently, no systemic risk results from one vehicle being driven automated.

When introducing more than one vehicle, this does not change. To be affected of the technology, one needs to be in the direct vicinity of a vehicle. But when connecting vehicles via network (V2X) the potential exists that cybercriminals could conquer control of all connected vehicles. Thereby they could create an effect similar to a systemic risk by initiating a crash of all vehicles at once. This is, in first place, a security issue, which is excluded from the discussion within this thesis. This exclusion is mainly based on the assumption that all safety-related functions are independent from communication and are designed to be diverse, thus not attackable at once. Additionally, a controlled shutdown of automated functions is expected in case any systemic risk gets obvious.

Consequently the risk constellation in means of accidents is similar to the risk constellation of other modalities of individual mobility today. In general there exist different risk categories and Grunwald defines[34]:

Risks that the individual can decide to take or not,

imposed risks that the individual can reasonably easily avoid,

imposed risks that can only be avoided with considerable effort and

imposed risks that cannot be avoided.

These different risk categories divide the affected parties into two different groupings. On the one hand there are active **users** or passengers. They are individuals that can decide whether or not to take the risk that arises from automated driving vehicles. On the other hand there are other traffic participants or bystanders that are imposed with risks that they cannot avoid or could avoid only with significant limitations[34]. This second group will be called the exposed **society**, as nearly everybody in developed countries participates in traffic. For Germany[35] 2013, the participation in traffic is above 92 %.

During the introduction of a new technology these two groups are also distinguishable due to the risk level they are confronted with. Risk is defined[36] by the product of the probability of the accident occurring and the expected loss in case of the accident. For the individual of the group user and the individual of the group society the factor probability of occurrence differs significantly. During the whole operating time the user is in

[35] Streit, T. et al.: Deutsches Mobilitätspanel Bericht 2013/2014 (2015), p. 33.

[36] ISO: DIS 26262: Road vehicles - Functional safety (2008).

direct vicinity to the automated vehicle (as long as it is not driving without a passenger), thus the user has the highest exposure. If something happens he is involved. On the other side an individual of the society is nearly never exposed to an automated vehicle as long as their number is little. Even a person who is commuting between the same buildings like a user of an automated vehicle will have a little exposure. Presupposed both persons do not strictly follow each other 1/100 of their commutes. In this case an exposure smaller than 1 % of the average operating time of the automated vehicle results for the individual of the society. The active **user** is highly exposed and the individual of the **society** is little exposed to the technology of automated driving during the first phase of introduction, hence the level of risk of both groups is significantly different. This will be formalized further in the next subsections.

It is assumed that the share of benefits of automated driving is divided in a similar manner as the risks. The **user** will be the one that benefits most[37] from the functionality of automated driving. Whereas the **society** will probably gain not as much as the individual from the technology applied to some vehicles during the first phase of introduction. The formulation used here is vague as it is difficult to predict the real benefit that comes with automated driving. The share that is described above is intentionally used as a worst-case scenario. The benefits meet the group that can decide to take the risks whereas the group that is exposed to risks without the possibility to avoid them is nearly without benefits.

The groups identified above could easily be subdivided. Users could for example be regular drivers, excluded ones from individual mobility, like elderly, inebriated or sick people. The acceptance of each of these groups is of relevance if they should use the vehicle. Though, their acceptance depends on all their benefits and drawbacks as well as on individual values of each individual. The individual acceptance cannot be constructed externally. However, for developers, decision-makers and regulators the requirements on safety need to be derived from normatively expected acceptance i.e. the *acceptability* of the risks. Therefore these two groups, users and society, are defined as the equivalence groups for safety characteristics and are further discussed in the next chapters.

[37] It is not a given thing that the user is the one benefiting most. Think about an automated transportation service that replaces regular taxis. If saved costs would not be passed on to the user, he or she might not benefit at all compared to regular taxi usage. The beneficiary would be the organization running the service.

1.4 Possible Safety Impact of AD3+

Q5 What safety impact may result from the introduction of automated driving?

There exists an interview with Matt Schwall from 2016, speaking for Tesla Motors. He says (translated into English):

> *We reached a point, where we can prove that autonomous vehicles are safer than human.*[38]

How Schwall measures this safety and what he means by "autonomous vehicles" is unclear. In a publication from 1998 Binfet-Kull et al.[39] define a guideline:

> *A vehicle, which is able to drive without human intervention (autonomous) by use of electronic equipment, shall not entail a hazard to human beings and/or property which is greater than the hazard represented by the conventional (human) driver!*
>
> *Furthermore, the requirement is defined, that the machine has to be 10^{-2} times safer than the human being.*

In this paper it is not directly mentioned on which scale this "10^{-2} times safer" should be reached. Does 10^{-2} safer mean 100 times less safe? Reschka[40] concludes from the context in Binfet-Kull et al. that the frequency of failures per hour of operation is meant.

To answer the safety question a comparable quantity needs to be defined and derived for the different levels of automation in road traffic.

1.4.1 Quantities Representing Safety

Road Traffic Victims

Following for example Papadimitriou et al.[41], the safety outcome of a whole road system is the number of fatalities. The source of risk in road traffic is[42]

> *physical injury or damage to the health of people.*

---

[38] http://www.golem.de/news/autonomes-fahren-google-und-tesla-draengen-auf-das-lenkradlose-auto-1601-118826.html Matt Schwall from Tesla Motors: "Wir sind an einem Punkt angelangt, an dem erwiesen ist, dass autonome Autos sicherer als Menschen sind." Author of the Articel: Friedhelm Greis, Accessed March 18th 2016

[39] Binfet-Kull, M. et al.: System safety for an autonomous vehicle (1998), p. 470.

[40] Reschka, A.: Diss., Fertigkeiten- und Fähigkeitengraphen (2016), p. 82.

[41] Papadimitriou, E. et al.: Safety performance assessment in Europe (2013). referring on Hauer, E.: On exposure and accident rate (1995).

[42] ISO: DIS 26262: Road vehicles - Functional safety (2008).

This has already been cited for concretizing the drawbacks and benefits of AD3+. Thus the pure number of personal injuries $I(t) \in \mathbb{N}_0$ at the time t since the beginning of counting t_0 would be the simplest quantity for comparison. As these injuries have different severities also statistics separate these numbers into different severities. Mostly[43] the number of light injuries I_L, severe injuries I_S and fatalities I_F are distinguished. Additionally, more detailed ordinal scales as the Abbreviated Injury Scale (AIS), the Head Injury Criterion (HIC) and others are used[44] for in-depth studies. However the pure number $I(t)$ counted from the first occurred injury until a certain time t in total is without meaning when comparing a new with an existing technology. Consequently, an observation interval needs to be defined.

Social Risk

Fritzsche[45] defines the social risk for a defined population as the number of victims counted during a certain time frame Δt. For example the number of injuries I_a during one year $\mathrm{a} = 365.25\ \mathrm{days} = 8766\ \mathrm{h}$

$$I_\mathrm{a}(y) = I(y\text{-}12\text{-}31) - I((y-1)\text{-}12\text{-}31). \tag{1-2}$$

In this equation y is the number of years ($[y] = \mathrm{a}$), following the Gregorian calendar[46]. In the minuend $y\text{-}12\text{-}31$ is the last day of year y, whereas in the subtrahend $(y-1)\text{-}12\text{-}31$ is the last day of the preceding year $(y-1)$.

The weakness of the yearly number of victims with different severities as an indicator for safety gets obvious when comparing for example different countries. Austria counts less fatalities ($I_\mathrm{F,a} = 455$)[47] in 2013 then Germany ($I_\mathrm{F,a} = 3339$)[47] does. Does this mean that being part of Austrian road traffic is more safe then being part of German road traffic? Thus either this number needs to be compared always for the same population or the number of victims needs to be put into relation to a value of exposure to make these numbers comparable.

---

[43] BMVI et al.: Verkehr in Zahlen 2015/16 (2016). Schnieder, E.; Schnieder, L.: Verkehrssicherheit (2013), p. 124,150ff.

[44] Schnieder, E.; Schnieder, L.: Verkehrssicherheit (2013), p. 152ff.

[45] Fritzsche, A. F.: Wie sicher leben wir? (1986), p. 19–20.

[46] ISO 8601: Representation of dates and times (2004).

[47] Destatis: Verkehrsunfälle - Zeitreihen 2014 (2015).

Injury Rate

Exposure can be defined by a time. Thus, counting the number of victims for the different severity levels per time Δt, new as well as old technologies get comparable as long as their usage is the same. Given this assumption, the injury rate $IR \in \mathbb{R}^+$ is calculated on a statistic for one year $\Delta t = \mathrm{a}$ and the corresponding number of fatalities $I_{\mathrm{F,a}}$

$$IR_{\mathrm{F,a}} = \frac{I_{\mathrm{F,a}}}{\Delta t}. \tag{1-3}$$

For the above derived numbers the fatality rate in Austria would be $455/\mathrm{a} \approx 5.19 \cdot 10^{-2}/\mathrm{h}$ whereas in Germany the rate would be $3339/\mathrm{a} \approx 3.81 \cdot 10^{-1}/\mathrm{h}$. For Germany and Austria the usage during the same time interval differs, thus it is not sufficient to just refer to an observation time. An exposure value that measures usage is necessary for comparison of new and old technologies that might be used to a different extent.

Road Traffic Victims per Exposure Time - Exogenous Mortality

One possible exposure value is the exposure time t_{u} instead of the general observation time Δt. The number of injuries per exposure time $IpUt \in \mathbb{R}^+$ is defined by

$$IpUt = \frac{I_{\mathrm{a}}}{t_{\mathrm{u}}}. \tag{1-4}$$

Krebs et al.[48] explain and define the exogenous mortality $M_{\mathrm{ex}} \in \mathbb{R}^+$ based on prior work of Kuhlmann. It is the number of fatalities compared to the average number of users N_{Pop} and the average exposure time $t_{\bar{\mathrm{u}}}$ of a user for a specific unit of time (e.g. per year)

$$M_{\mathrm{ex,a}} = \frac{I_{\mathrm{F,a}}}{N_{\mathrm{Pop}} \cdot t_{\bar{\mathrm{u}}}} = \frac{I_{\mathrm{F,a}}}{t_{\mathrm{u}}}. \tag{1-5}$$

Krebs et al.[48] also define that the number of fatalities $I_{\mathrm{F,a}}$ should be corrected by the number of invalids (factor 0.1) and injured (factor 0.01). This weighting of different levels of severity will be discussed later and be neglected for further calculations of the mortality.

As a reference value the Minimum Endogenous Mortality (MEM) is defined by Kuhlmann[49] as the natural death rate (without deformity and immaturity) $M_{\mathrm{en,a}} = 2 \cdot 10^{-4}/\mathrm{a}$ for a 5-15 year old German based on numbers from 1973 from the German

[48] Krebs, H. et al.: MEM:ein universelles Sicherheitskriterium (2000), p. 821. Kuhlmann, A.: Alptraum Technik? (1977)., Kuhlmann, A.: Einführung in die Sicherheitswissenschaft Albert Kuhlmann (1981)., Schnieder, E.; Schnieder, L.: Verkehrssicherheit (2013), p. 177f.

[49] Kuhlmann, A.: Alptraum Technik? (1977), p. 37&50f.

statistical office. Coincidentally, this is similar to the non-natural death rate for this year. As Seeger[50] indicates this second rate, the non-natural death rate, is used for argumentation in EN 50126[51]. Kuhlmann as well as the EN 50126 suggest that the entire risk from all technical systems must not exceed this value. The MEM approach assumes that maximally 20 systems act simultaneously on the individual, thus an individual risk limit of $10^{-5}/\mathrm{a}$ is defined. This risk limit additionally is a function of severity as depicted by Figure 8 as defined by Kuhlmann[49]. However, also this is negligible for AD3+ as it is assumed (see negligence of security discussion) that events with more than 100 fatalities will not be caused by AD3+.

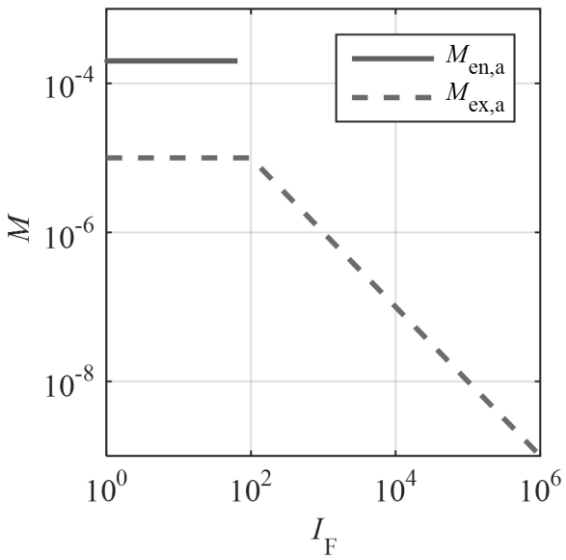


Figure 8 Individual risk limit for exogenous reasons as a function of fatalities per event[49]

As Seeger explains, these reference numbers have changed. The probability to die has reduced during the last 40 years. Compare the numbers from 1973 stated above with the overall mortality in Germany[52] 2013 (see Figure 9).

[50] Seeger, C.: MEM - eine Konstante? (2013), p. 14&15.

[51] DIN 50126 Bahnanwendungen (2000).

[52] statista.de: Sterbetafel: Deutschland, Jahre, Geschlecht,Vollendetes Alter (2013).

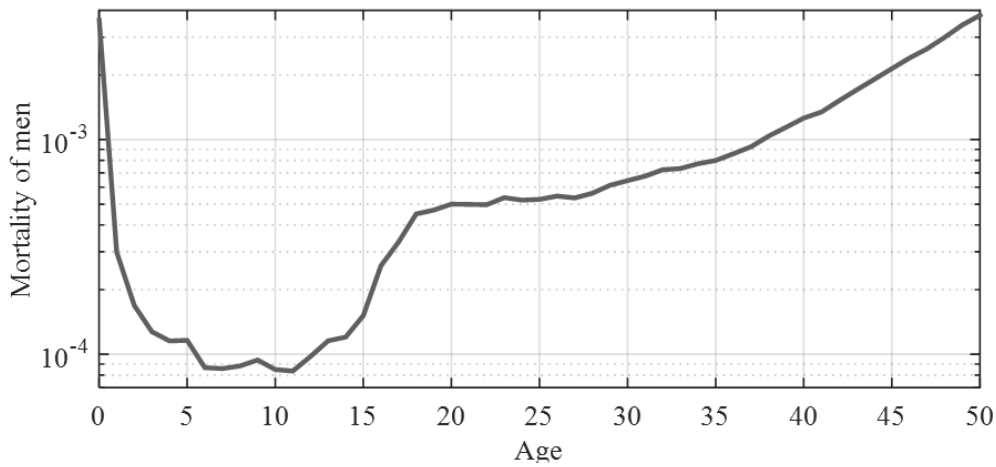


Figure 9 Mortality over age for German men in 2013

Calculating the MEM for 2013 and following the approach reported in Seeger two different values for MEM result. In 2013, the German population of 5-15 years olds was[53a] $N_{\mathrm{Pop}} \approx 7.254 \cdot 10^6$. Of these $I_{\mathrm{F,all}} = 609$ died[53b] and out of these $I_{\mathrm{F,ex}} = 148$ died[53c] from exogenous reasons (International Statistical Classification of Diseases and Related Health Problems (ICD-10)[54]). Thus, following either the Kuhlmann definition $M_{\mathrm{en,a}} = \frac{I_{\mathrm{F,all}} - I_{\mathrm{F,ex}}}{N_{\mathrm{Pop}}} \approx 6.36 \cdot 10^{-5}\ 1/\mathrm{a}$ results, or the EN 50126 definition $M_{\mathrm{en,a}} = \frac{I_{\mathrm{F,ex}}}{N_{\mathrm{Pop}}} \approx 2.04 \cdot 10^{-5}\ 1/\mathrm{a}$ results. Both numbers are meaningful to study.

Besides the minimum endogenous mortality also the current exogenous mortality caused by road traffic could be taken for comparison. As has been described the exogenous mortality depends on the kind of scenario one is exposed to. The exogenous mortality caused by road traffic is defined by the fatalities in road traffic $I_{\mathrm{F,a}}$, that has already been used. But what is the exposure time of road traffic? In general, this is not directly reported by any statistic. To identify the average exposure of the individual to road traffic $t_{\overline{\mathrm{u}}}$ the results of questionings give approximate values. For Germany in 2013, the time spent for mobility daily is reported[55] to be 84 min (German: Mobilitätszeit). Unfortunately it is not reported how much of this time is spent in road traffic. A modality split is given, but without distinguishing different forms of public transport. Based on these numbers approximately 80 % of these 84 min is the rough

[53] Destatis: Gesundheit, Todesursachen in Deutschland (2014), p. a:46, b:6, c:8.

[54] http://apps.who.int/classifications/icd10/browse/2016/en Class V01-Y98 Chapter XX accessed 24.09.2016

[55] Streit, T. et al.: Deutsches Mobilitätspanel Bericht 2013/2014 (2015), p. 37–39.

estimation[56] for this thesis, thus $t_{\bar{\mathrm{u}}} \approx 365.25 \cdot 67.2\ \mathrm{min} \approx 365.25 \cdot 1.12\ \mathrm{h}$ are assumed to be the average time spend in road traffic for the German population in 2013. The average population of Germany in 2013 was[57] $N_{\mathrm{Pop}} \approx 80.65 \cdot 10^6$. The exogenous mortality results to be $M_{\mathrm{ex,a}} \approx 8.87 \cdot 10^{-4}/\mathrm{a}$ caused by road traffic. For Austria the last questioning was held in 2008, thus no numbers exist for comparison of 2013. For the question on whether to use the road traffic victims per exposure time for quantifying the safety outcome of AD3+ two main results can be drawn: First, today's statistics do not directly offer the average exposure time to road traffic. Second, the roughly estimated exogenous mortality for road traffic exceeds the defined MEM limit.

Besides the challenge of identifying the usage time, this time not necessarily stands for a successful fulfillment of mobility needs. Mobility means the transport of someone or something from one place to another. Consequently, in the following subsection the distance d, another value for exposure, is studied.

Road Traffic Victims per Distance

Besides expressing the usage by exposure time t_{u}, also the distance d can be used as exposure. The values of victims per distance $Ipd \in \mathbb{R}^+$ and victims per exposure time $IpUt$ are connected by the average velocity $\bar{v}$

$$IpUt = \frac{Ipd}{\bar{v}}. \tag{1-6}$$

Caution: In Germany[58] 2013, private motorized transport covered 66.3 % of the distance in traffic whereas it only covered 46.5 % of the usage time spend in traffic. For walking the ratio is even more extreme: 19.9 % of the time and 2.7 % of the distance. Thus, it must be clearly defined what is referred to as the exposure.

Some approaches exist in literature that try to define first qualitative requirements for automated driving based on fatalities $I_{\mathrm{F,a}}$ per vehicle distance driven d_{a} during a time frame, for example one year a,

$$Ipd_{\mathrm{F,a}} = \frac{I_{\mathrm{F,a}}}{d_{\mathrm{a}}}. \tag{1-7}$$

Sivak and Schoettle[59] discuss different cases of automated driving fatalities per distance Ipd_{F} in comparison to conventional driving shown in Figure 10. Case 1, representing

[56] Additional effects like not represented foreigners in these questionings could be considered.

[57] Destatis: Verkehrsunfälle - Zeitreihen 2014 (2015), p. 6.

[58] Streit, T. et al.: Deutsches Mobilitätspanel Bericht 2013/2014 (2015), p. 36&38.

[59] Sivak, M.; Schoettle, B.: Road safety with self-driving vehicles (2015).

the line for a fleet containing only self-driving (Level 4) vehicles, is discussed to be unrealistic as it goes through zero on the vertical axis. Sivak and Schoettle leave it open which of the other cases will become reality.

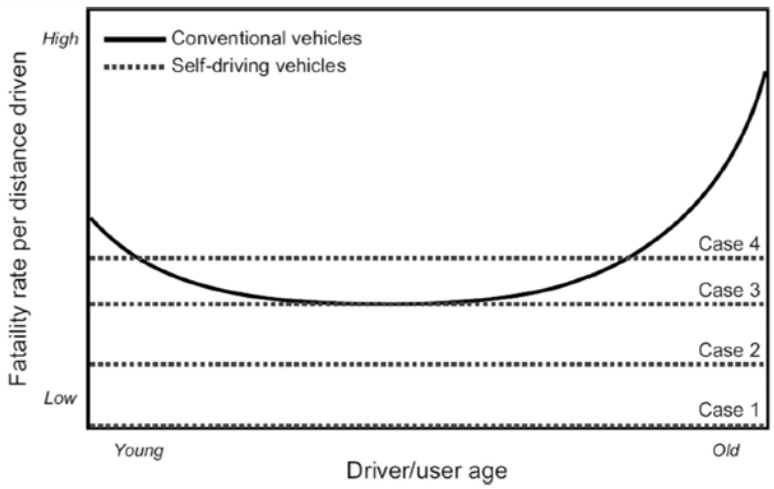


Figure 10 Fatalities per distance driven, using conventional vehicles and self-driving vehicles as a function of driver/user age[59]

The drawback of the discussion of personal injuries I and vehicle distance d is the fact that there exist events with more than one victim. Thus the value that is discussed with IpA would most likely not be seen in reality.

Accidents per Distance

The ratio IpA between victims of accidents[60] $I_{\mathrm{a}} \approx 377.5 \cdot 10^3$ and accidents with personal injuries[60] $A_{\mathrm{wI,a}} \approx 291.1 \cdot 10^3$ for the total Germany road traffic in 2013, is

$$IpA_{\mathrm{wI,a}} = \frac{I_{\mathrm{a}}}{A_{\mathrm{wI,a}}} \approx 1.3. \tag{1-8}$$

Consequently other approaches exist that discuss accidents per distance ApD to express the risk of road traffic. To *"[...] illumine a facet of the safety of some entity [...] where the entity may be a road section, a set of intersections of the same type, a group of vehicles having some common features, an age cohort of drivers and the like"* [61] Hauer more generically discusses the accident rate AR

$$AR = \frac{\text{Average number of accident in a specified time}}{\text{Amount of exposure in a specified time}} \tag{1-9}$$

[60] Destatis: Verkehrsunfälle - Zeitreihen 2014 (2015), p. 20.

[61] Hauer, E.: On exposure and accident rate (1995).

If from a motorist point of view the accident rate gets lower with exposure being vehicle distance traveled d_{a}, thus the accidents per distance Apd, the entity clearly gets safer[62]

$$Apd_{\mathrm{a}} = \frac{A_{\mathrm{a}}}{d_{\mathrm{a}}}. \tag{1-10}$$

Coming back to the previous example, as the distance driven[63] in Germany ($d_{\mathrm{a}} \approx 725.7 \cdot 10^9$ km) and the number of accidents with fatalitis[64] ($A_{\mathrm{wF,a}} = 3131$) are bigger than in Austria[65] ($d_{\mathrm{a}} = 78.11 \cdot 10^9$ km and $A_{\mathrm{wF,a}} = 435$) the two numbers on accidents with fatalities per billion kilometer $Apd_{\mathrm{wF,a}} \approx 4.31$ for Germany and $Apd_{\mathrm{wF,a}} \approx 5.57$ accidents with fatalities per billion kilometers for Austria result. Thus for people driving the same distance, the German road traffic system is safer. Changing the exposure and using time in traffic, number of trips, or others, also Austria could be safer. This simple example shows how difficult it is to fairly compare two entities in road traffic in means of safety. It is not just the kind of accident that needs to be specified, it is also the kind of exposure that is used for comparison. And even the numbers for distance driven are not unambiguous, because these numbers have to be estimated based on different measurements[66].

Although the distance between two events of the same kind is described by statistics, the drawback using the accident per distance quantity is the uncertain severity of an accident registered in the databases. The German Federal Statistical Office reports[64] three major classes of accidents for 2013: with "property damages" $A_{\mathrm{wD,a}} \approx 2.123 \cdot 10^6$, with "personal injuries" $A_{\mathrm{wI,a}} \approx 288 \cdot 10^3$ as well as with "fatalities" $A_{\mathrm{wF,a}} = 3131$. Besides these classes further accident classes are reported[67], which not necessarily are relevant for safety. Consequently these additional differentiations (e.g. accidents with victims influenced by intoxicating substances) are neglected for the further discussion.

---

[62] Just dividing by exposure does not always make accident rates comparable, as for example the number of accidents and the exposure could correlate. For further discussion on this topic especially in the context of road safety work and civil engineering see Hauer, E.: On exposure and accident rate (1995).

[63] Destatis: Verkehrsunfälle - Zeitreihen 2014 (2015).

[64] Destatis: Verkehrsunfälle - Zeitreihen 2014 (2015), p. 20.

[65] OECD IRTAD: Road Safety Annual Report 2016 (2016), p. 70. Statistik Austria: Straßenverkehrsunfälle Österreich (2016), p. 17.

[66] Hakkert, A. S. et al.: The uses of exposure and risk in road safety studies (2002), p. 8.

[67] BMJV: StVUnfStatG (1990).

Given these classes of accident severities the idea of the triangle from Figure 7 can be translated to accidents per distance and a discrete ordinal scale as depicted in Figure 11.

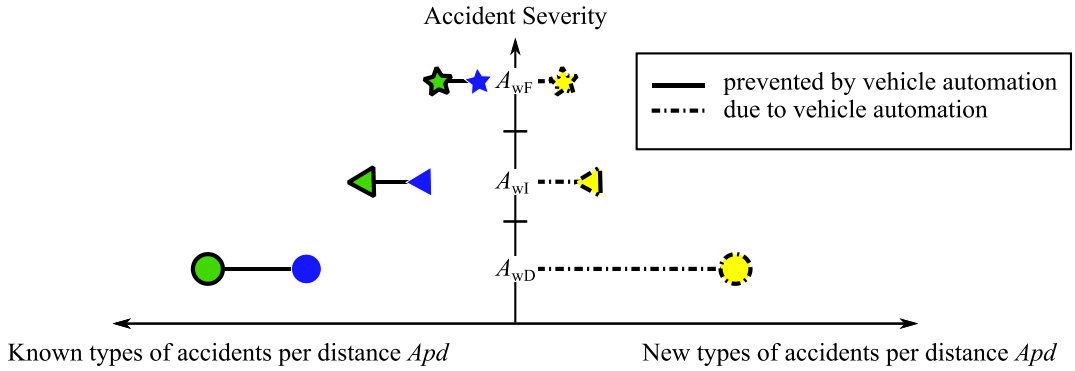


Figure 11 Theoretical potential to reduce accidents per distance with vehicle automation and consideration of accident severity

Exposure, Accidents, and Severity

The thoughts discussed above lead to the three dimensions of the so-called road safety problem from a public health point of view[68] that is depicted in Figure 12 (left).

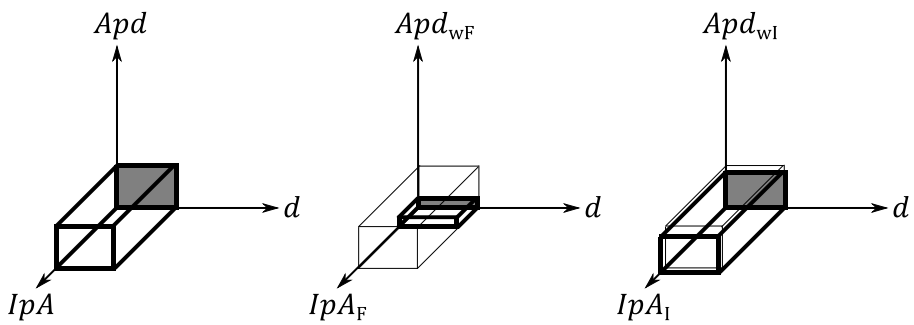


Figure 12 The size of the safety problem (number of human injuries and fatalities) illustrated as a function of the product of the three variables exposure d, crash risk Apd and injury consequence IpA (cf. Rumar[68]) (left: all accidents, middle: with fatalities, right: with injuries)

Depending on the level of severity that is studied the volume's shape changes. However, the severity selective gray areas must sum up to the overall number of accidents. The volumes representing the number of victims must sum up as well to the overall number of victims.

Al-Haji concludes that there are three ways of reducing the safety problem[69]:

[68] Rumar, K.: Transport safety visions, targets and strategies: beyond 2000 (1999), p. 17.

[69] Al-Haji, G.: Diss., Road Safety Development Index (2007), p. 43.

Reducing exposure factors (d): by reducing the amount of travel per person or vehicle and the total reduction in traffic volume.

Reducing accident risk factors (Apd): by for instance improving driver skills, road user education, vehicle performance, road standards, legislation and enforcement.

Reducing accident severity factors (IpA): by protecting people better in vehicles from injury severity. Protecting pedestrians and other vulnerable road users by vehicle design, and protecting two wheelers by using appropriate helmets.

In principle to study the overall safety outcome when introducing AD3+, all three dimensions need to be addressed. It should be mentioned that for studying the whole traffic system's safety different safety performance indicators exists[70], however the following has been defined to be focused in this thesis.

Safety Performance

To study a quantity that expresses the safety of a driving function of AD3+ without considering the usage and passive safety features, the inverse of the accidents per distance measure is defined as the safety performance SP:

$$SP = \frac{1}{Apd} = \frac{d}{A}. \tag{1-11}$$

It represents the distance between two accidents, or more generally the distance between two events of the same category. The bigger the safety performance SP, thus the distance, the safer the vehicle which is observed. As the thoughts on the severity classes of accidents expressed by Figure 11 still need to be taken into account, the safety performance is defined as a vector $\boldsymbol{SP}$. To study the effect of competing classes of events in this thesis two classes, accident with fatalities $\mathrm{A_{wF}}$ as well as with personal injuries $\mathrm{A_{wI}}$,

$$\boldsymbol{SP} = \begin{bmatrix} SP_{\mathrm{AwI}} \\ SP_{\mathrm{AwF}} \end{bmatrix} = \begin{bmatrix} \frac{1}{Apd_{\mathrm{wI}}} \\ \frac{1}{Apd_{\mathrm{wF}}} \end{bmatrix} \tag{1-12}$$

are considered.

The $\boldsymbol{SP}$ for the whole German traffic in 2013 follows, with the numbers given above, to be

[70] Al-Haji, G.: Diss., Road Safety Development Index (2007).; Chen, F. et al.: Benchmarking road safety performance (2016).

$$\boldsymbol{SP} = \begin{bmatrix} SP_{\mathrm{AwI}} \\ SP_{\mathrm{AwF}} \end{bmatrix} \approx \begin{bmatrix} 2.52 \cdot 10^6 \text{ km} \\ 2.32 \cdot 10^8 \text{ km} \end{bmatrix}. \tag{1-13}$$

In general also additional classes of events can be studied for assessing safety. For this reason the safety performance refers to events k in the following of the thesis.

Monetary Weighting

To come to one scalar value expressing the safety performance it seems obvious to weight by a monetary factor. Weighting a person's live against X severe injured people is ethically challenging and provokes criticism and rejection. Nevertheless, as the possibility exists to do so, my understanding is to discuss it and to objectively prepare information on this topic for broader discussion.

The German Federal Highway Research Institute (BASt) similar like other national institutes of other countries publishes approximated numbers on accident costs for different severities in Germany[71] (see Table 1).

Table 1 Economic costs of road accidents and victims in Germany[71]

	Severity		Value for 2013
Accident costs 10^9€ total	Person injuries total		13.42
	Fatalities $C_{\mathrm{AwF,a}}$		**3.95**
	Severe injuries	$C_{\mathrm{AwI,a}}$	**7.83**
	Light injuries		**1.65**
	Property damage		19.08
	Total		32.51
Person injuries costs of accident victims in 10^3€	Average fatality $\bar{C}_{I_{\mathrm{F}}}$		1182
	Average severe injury $\bar{C}_{I_{\mathrm{S}}}$		121.8
	Average light injuries $\bar{C}_{I_{\mathrm{L}}}$		4.982
Accident costs for property damage each accident in 10^3€	Average accident with fatalities		47.16
	Average accident with severe injuries		22.65
	Average accident with light injuries		14.52
	Average severe accident with only property damage		21.48
	Other property damage		6.095

From Table 1 the costs for victims of accidents in 2013 are used to come to an average cost for accidents with injuries $\bar{C}_{\mathrm{AwI}}$ and with fatalities $\bar{C}_{\mathrm{AwF}}$

[71] BASt: Volkswirtschaftliche Kosten von Straßenverkehrsunfällen (2015). Information on the methodology find here: Baum, H. et al.: BASt: Volkswirtschaftliche Kosten Herleitung (2011). Values for the USA and a critical reflection on that can be found in Blincoe, L. et al.: The economic and societal impact of vehicle crashes (2015). and Viscusi, W. K.; Aldy, J. E.: The value of a statistical life (2003).

$$\bar{C}_{\mathrm{AwI}} = \frac{C_{\mathrm{AwI,a}}}{A_{\mathrm{wI,a}}} \approx 32.9 \cdot 10^3 \text{ €}, \tag{1-14}$$

$$\bar{C}_{\mathrm{AwF}} = \frac{C_{\mathrm{AwF,a}}}{A_{\mathrm{wF,a}}} \approx 1.26 \cdot 10^6 \text{ €} \tag{1-15}$$

A mistake is made by assuming the numbers of severe and light injuries are zero ($I_{\mathrm{S}} + I_{\mathrm{L}} = 0$) for accidents with fatalities A_{wF}. It is neglected due to two reasons: the number of accidents with injuries is orders of magnitude higher than the number of accidents with fatalities ($A_{\mathrm{wI}} \gg A_{\mathrm{wF}}$) and the average cost of a fatality is magnitudes higher than that of severe or light injuries ($\bar{C}_{I_{\mathrm{F}}} \gg \bar{C}_{I_{\mathrm{S}}} \gg \bar{C}_{I_{\mathrm{L}}}$) (see Table 1).

Using the average accident cost the cost performance scalar CP is calculated by

$$CP = \left(\frac{\bar{C}_{\mathrm{AwI}}}{SP_{\mathrm{AwI}}} + \frac{\bar{C}_{\mathrm{AwF}}}{SP_{\mathrm{AwF}}} \right)^{-1}. \tag{1-16}$$

This theoretical value would express which distance could be driven with one cost unit, when accident costs should be balanced out. The values from equation (1-13) of the German road traffic in 2013 lead to a cost performance of

$$CP \approx 54 \ \frac{\mathrm{km}}{\text{€}}. \tag{1-17}$$

However, this cost performance is without meaning when discussing test distances. There are no events in real driving that “cost” one Euro. For that reason the CP is not used for safety evaluations. Other ways of using the monetary values for weighting are possible. For example, accidents with injuries could be converted into virtual accidents with fatalities by the factor $\frac{\bar{C}_{\mathrm{AwI}}}{\bar{C}_{\mathrm{AwF}}}$. This virtual number of fatalities could be used to define a virtual safety performance on the class of fatalities.

Nevertheless, this virtual safety performance would never be seen when testing in real traffic. For that reason the safety performance vector $\boldsymbol{SP}$ is used as the quantity representing the safety of vehicle driving and AD3+ driving functions in specific.

1.4.2 Prospective vs. Retrospective Assessment

The quantities explained above, that express the safety of an entity or a whole traffic system, are calculated either retrospective or prospective.

Retrospective

The retrospective evaluation counts the number of events that have happened, registers the costs that result and estimates the exposure values like the total vehicle distance

traveled d_{a}. Besides the numbers for the severity level fatalities, the accident numbers do not perfectly reflect the reality, as there exist especially bagatelles that are not reported or recorded. But also the numbers of light injuries differs from the real accident happenings. Blanco et al. state in this context[72]:

> *Two factors complicate the national crash data. First, states have different requirements concerning what incidents are reported as crashes. Second, many crashes go unreported. Estimates of unreported rates of crashes have ranged from as little as 15.4 percent to as much as 59.7 percent. The result is that the current national crash rate is essentially a low estimate of the actual crash rate.*

This needs to be taken into account when comparing the numbers for human driven vehicles with the automated driven ones. It is already a worst-case estimation, as the accident numbers of automated vehicles will be made transparent[73] whereas human accident numbers are inaccurate.

It is not just the number of accidents that contains errors. Also the level of severity or the costs that are recorded can differ significantly from what is the real result of that accident. The same counts for distance d_{a} as this is estimated based on other observations like gasoline consumption, traffic counting or odometer readouts[74]. Nevertheless, the retrospective evaluation based on records, countings and estimations seems to be the best that can be done to validate the safety assurance approach. After the concept of this thesis has been introduced, the challenges of existing data and corresponding requirements are derived in chapter 4 “Application: Data to Apply the Usage Strategy”.

To derive reference values and illustrate certain calculations with examples this thesis refers, whenever possible, to the numbers of the year 2013. Although, for many of the used parameters more up to date values are available, others like the cost factors or counting of the origin of vehicles on German Autobahn are not reported for 2014 or later.

Prospective

In contrast, the prospective evaluation estimates the number of events that will happen in the future. It estimates the costs that will result and assumes usage and exposure values like the distance d_{a} for AD3+. Due to the nature of each estimation and assump-

[72] Blanco, M. et al.: Automated Vehicle Crash Rate Comparison Using Naturalistic Data (2016), p. i. Cf. Blincoe, L. et al.: The economic and societal impact of vehicle crashes (2015).

[73] Own assumption based on the DMV approach: https://www.dmv.ca.gov/portal/dmv/forms/forms/ol/ol316.pdf accessed 24.09.2016

[74] Papadimitriou, E. et al.: Safety performance assessment in Europe (2013), p. 374 ff.

tion, it suffers uncertainty. But the goal of each safety assurance is to do a prospective safety evaluation based on all information that is available ahead of introduction.

The goal is not to speculate prospectively about the time in future when "Vision Zero" gets achievable. The goal of the thesis is to make a realistic prospective assessment of the safety question. To my understanding the argumentation doesn't need to just focus on zero accidents, as Grunwald[75] describes our society is used to road accidents. Traffic participants are aware that driving in a vehicle can end up with damage to property or health. A system has formed around this damage that tries to cover it by emergency services, trauma medicine, liability law, and insurance. As most of the people worldwide take part in road traffic, they do accept this system and the fact that accidents occur. Generalized this means that every human prospectively does a "small" safety assessment ahead of participating in today's road traffic. The chance exists to be part of a road traffic accident.

To get the type approval for the technology and handle liability argumentations it would be worth aspiring to show prospectively that automated driving reaches a safety expressed by the safety performance $\boldsymbol{SP}$. The following chapters will focus on that. Different approaches will be explained, its challenges will be indicated and a new concept that results in a specific usage strategy will be derived.

[75] Grunwald, A.: Societal Risk Constellations for Autonomous Driving. (2016).

2 State of the Art: Challenges of Today's Approach to Assess Automated Driving's Safety[76]

Q6 How to predict the safety impact of automated driving?

The goal is clear. Assess a new technology by prospectively deriving quantities representing safety. But why is *Q* 6 raised especially for automated driving? Why not for systems which were released for production in the past? Becker[77] concludes on this question in one of his talks:

> *The expenditure for validation of systems suffering higher complexity will increase by a factor of 10^6 to 10^7, thus: traditional statistical validation is not suitable for higher degrees of automation, highly automated systems require completely new release strategies.*

He underlines his thoughts with Figure 14 and formulates the goal:

> *Combination of statistical validation with new qualitative design and release strategies*

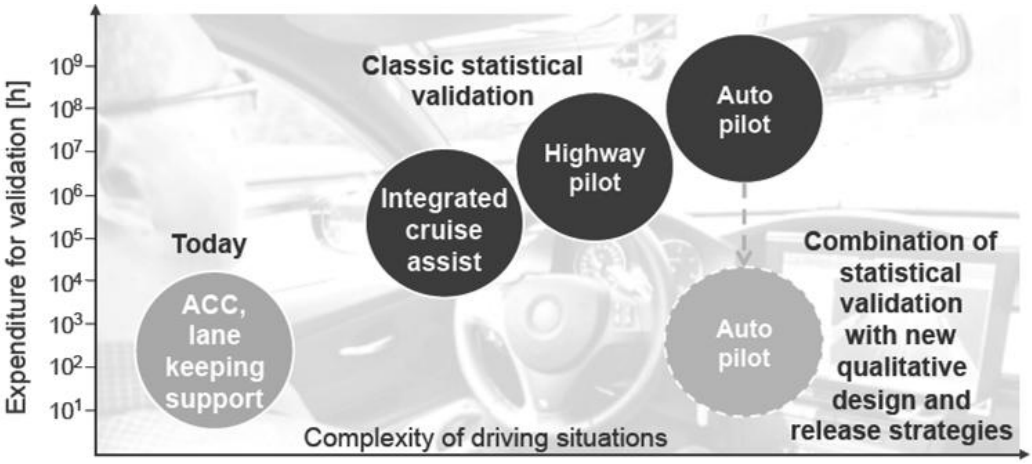


Figure 13 Validation and release process - challenges[77]

The following sections will firstly explain current test concepts, secondly define generic requirements for test concepts, and thirdly discuss the special features of automated driving compared to today's vehicles on the road, rail, and in avionics. Then subsection

[76] The main content and wording of this chapter is taken from Wachenfeld, W.; Winner, H.: The Release of Autonomous Vehicles (2016).

[77] Becker, J.: Toward Fully Automated Driving (2014).

2.4 will derive the challenges of releasing fully-automated vehicles. Based on this knowledge, the so-called “Approval-Trap” will be highlighted. Subsection 2.5 will conclude this state of the art with a review of existing approaches to overcome the “Approval-Trap”.

One of these approaches will be the “Theory: Stochastic Model for Safety Assessment” that is introduced in chapter 3. This concept of chapter 3 makes up the main contribution to research within this thesis.

2.1 Current Test Concepts in the Automobile Industry

Q7 How are today’s automobiles tested?

The safety validation concepts currently used in the automobile industry are obtaining approval for four distinct automation levels. To illustrate the difference for the test of these systems compared to AD3+, these four systems will be explained briefly:

The first system in series is the driver-only vehicle without the automation of the driving task. For these systems, it can be seen that, on the one hand, the components used do not exceed maximum failure rates, and on the other, that the driver is able to maneuver the vehicle reliably in road traffic (controllability). The abilities of the driver are relied on, as the results of the conducted tests with test drivers are transferred to future users in the subsequent area of use. Over the last decades, this has shown itself to be successful in serving as proof of safety. Despite the increasing number of kilometers driven in road traffic, the number of accidents remains[78] constant, and the number of fatalities has even decreased.

The second level of automation in series is the assisting system: For systems such as Adaptive Cruise Control[79] (ACC) or Lane Keeping Assist[80] (LKA), their functions have to be covered by the test in addition to the existing scope of testing. The option of a take-over by the driver and controllability must be provided in systems that actively support the driving task, increase comfort, and reduce the driver’s stress. The Code of Practice[81] thus assumes that, in this ADAS (Advanced Driver Assistance System), responsibility for vehicle behavior remains with the human driver. For these systems it

[78] Destatis: Verkehrsunfälle - Zeitreihen 2014 (2015).

[79] Winner, H.; Schopper, M.: Adaptive Cruise Control (2016).

[80] Bartels, A. et al.: Lateral Guidance Assistance (2016).

[81] Donner, E. et al.: RESPONSE 3 (2007), p. 237f.

also applies that the abilities of the driver are relied on, so that the results of the conducted tests with test drivers are transferred to future users in the subsequent area of use.

The first partly-automated systems[82] (AD-level 2) have also been approved for use in series cars: Depending on the speed, ACC in combination with LKA takes over the lateral and longitudinal control for the driver. According to the definition, in the third category of systems, the driver is also responsible for the vehicle behavior. Therefore, this test also focuses on the possibility of a take-over and the controllability by the driver; and so the same principle applies as with the assisting system, which relies on the abilities of the vehicle driver to correct undesired automation behavior. This level of automation presents the special challenge for the safety validation resulting from the conflict between relieving the driver and the necessary situation awareness of the supervisor of the lateral and longitudinal control. The basics of this conflict have already been described by Bainbridge[83] in 1983. However, again the driver is ultimately responsible.

Of particular interest for the test are emergency intervening systems, which automatically intervene in the vehicle control and thus in the vehicle dynamics. The goal of this fourth category of systems is to counter the driver's loss of control over the situation. For example, Electronic Stability Control[84] (ESC) and Emergency Brake Assist[85] (EBA) are components of mechatronic brake systems that apply additional or reduced braking force without any action on the part of the driver, thus actively intervening in the vehicle dynamics. This is performed during the driver's loss of control when the vehicle, in combination with the driver, is at a higher level of risk. ESC is designed in such a way that an intervention is carried out when the driver clearly no longer has control over the vehicle in the current situation (e.g. in the case of extreme over- or understeering). In contrast, the EBA becomes active when the reaction time and the braking distance before a rear-end collision are no longer sufficient for a human to prevent this accident. The goal of validating the system regarding safety requirements is to show that emergency intervening systems should only become active (true-positive) when the loss of control becomes obvious and thus there is a severely increased risk. For this, it must be shown that the false-positive rate becomes as small as possible[86] and/or the effects can be controlled by the driver; the false-positive and false-negative rates of the EBA mainly depend on the object perception. Figure 5 shows a Receiver Operating Characteristic curve (ROC curve) which describes this relationship for a fictitious object detection.

---

[82] Lüke, S. et al.: Traffic Jam Assistance and Automation (2016).

[83] Bainbridge, L.: Ironies of automation (1983).

[84] van Zanten, A.; Kost, F.: Brake-Based Assistance Functions (2016).

[85] Winner, H.: Fundamentals of Collision Protection Systems (2016).

[86] Rieken, J. et al.: Development Process of Forward Collision Prevention Systems (2016), p. 1182.

As these emergency intervening systems are systems with no guaranteed operation, an increase in safety can be achieved by reduced usage combined with a smaller false-positive rate. Additionally, these systems enable overriding[87]. ESC and EBA employ the selective braking of wheels to intervene mainly in the braking system, and various strategies can be used to override them, by steering and/or accelerating.

As has been shown, the main focus in the development of the four system levels is controllability by the driver. The goal is either to enable controllability for the driver or to restore it for him/her (design for controllability). Therefore, the driver as a backup is the basis for validating current vehicles regarding safety and hence also for the production release.

The development and verification of this controllability for the driver is generally carried out in accordance with the procedure model in Figure 14. This procedure based on the V-Model[88] differentiates between the downward branch on the left - development and design - and the upward branch on the right - verification and validation - as a mean of quality assurance. A test concept is followed for the quality assurance.

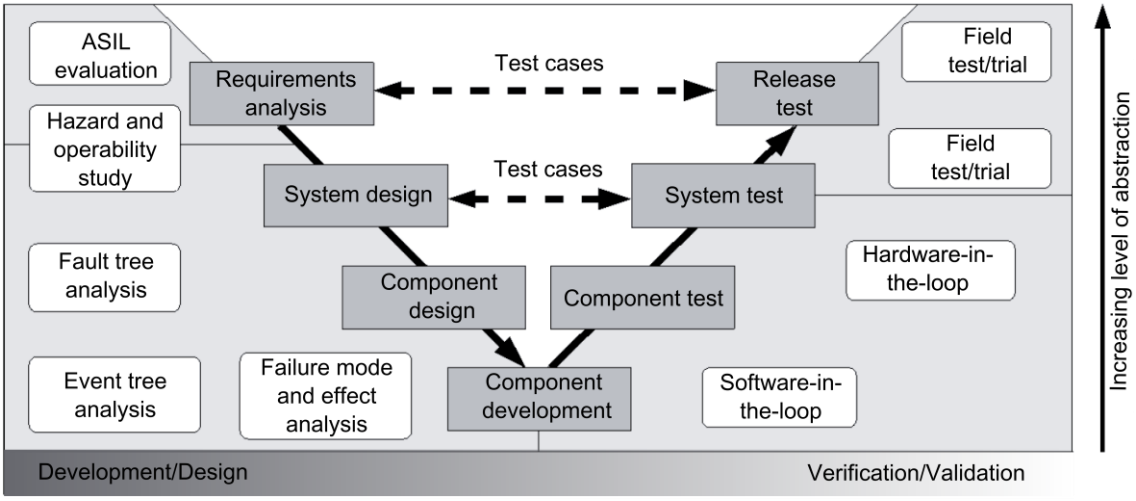


Figure 14 Safety evaluation methods in the development process (according to Weitzel et al.[89])

As shown by Schuldt et al.[90] in Figure 15, a test concept comprises the analysis of the test object (object under test – OuT), the test case generation, the test execution, and the test evaluation.

---

[87] Winner, H.: Fundamentals of Collision Protection Systems (2016), p. 1169.

[88] http://www.cio.bund.de/Web/DE/Architekturen-und-Standards/V-Modell-XT/vmodell_xt_node.html accessed 24.09.2016, ISO: DIS 26262: Road vehicles - Functional safety (2008).

[89] Weitzel, A. et al.: Absicherungsstrategien für Fahrerassistenzsysteme (2014).

[90] Schuldt, F. et al.: Effiziente systematische Testgenerierung (2013).

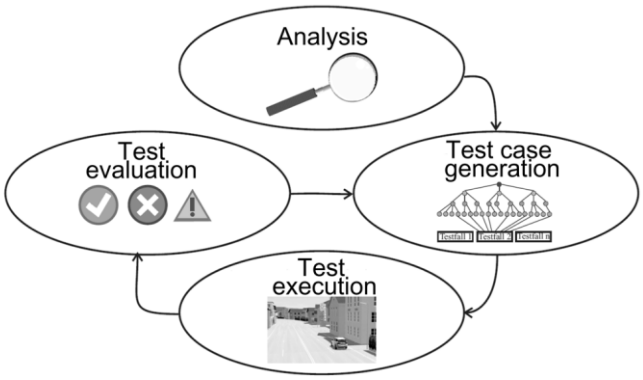


Figure 15 Procedure for test concept (according to Schuldt et al.[90])

The analysis of the test object and the test case generation should be performed during the development/design phase, so that the test cases to be carried out are already defined for the verification and validation (see Figure 14, procedure model). According to Horstmann[91] and Weitzel et al.[92], at present a distinction is made between three methods for the determination of test cases: One method is the test specification based on the specification sheet, whereby test cases are defined based on system specifications which have been set down in specification sheets. The second method is the risk-based test specification, whereby risk considerations are used to determine the test cases. The third method is the interface-based test specification, whereby the test cases are selected in order to cover the value ranges of the interfaces. For all these methods, the driver – vehicle system is the basis of the test case determination.

To start with the quality assurance as early as possible, tests are already carried out in virtual test environments[93] before the first test vehicles are ready for testing. The test execution by means of model- and software-in-the-loop tests is based on simulation models of the vehicle, the human, and the environment. The previously identified test cases are used here. The further the development progresses, the greater the number of real components available for testing. Test benches, driving simulators or testing grounds are used for these tests. The tests performed using hardware-in-the-loop, driver-in-the-loop, or vehicle-in-the-loop provide information about the quality of the components and functions being tested. To check the actions and reactions of the driver – vehicle – environment system (to close the loop), simulation models are also needed in performing these tests. Therefore, simulation models will be required continuously for the test execution up to this development point in order to test the entire vehicle. Simu-

[91] Horstmann, M.: Diss., Verflechtung von Test und Entwurf (2005).

[92] Weitzel, A. et al.: Absicherungsstrategien für Fahrerassistenzsysteme (2014).

[93] Hakuli, S.; Krug, M.: Virtual Integration in the Development Process (2016).

lation models are mappings of reality in software and per se have the property of simplifying the real world[94].

As a result of this fact, no safety-relevant function currently exists in a series vehicle that has not also been tested with real test vehicles. Thus, for testing current systems, the automotive industry always falls back on real vehicles, real humans, and a real environment.

An exemplary result of the necessary use of real driving is the production release of the Mercedes Benz E-Class (W212). A total of 36 million test kilometers were completed[95]. According to Fach et al.[96], the safety validation of a current driver assistance system alone requires up to 2 million test kilometers. This high number of test kilometers becomes understandable when realizing that 50,000 to 100,000 km test drives were necessary in between two interventions of the first level of the EBA (positive rate). This does not even consider the fact that the more critical second level of the EBA was not triggered during these test distance (compare assertion in Figure 5). This eight-figure total of test kilometers is accompanied by considerable costs for the vehicle prototypes, test drivers, test execution, and the evaluation of the same. While the time requirement can be reduced by means of parallel testing with multiple vehicles, additional costs are incurred for the vehicle prototypes.

This example shows that even for current driver assistance systems, validating safety based on real driving in road traffic represents an economic challenge for the OEM (Original Equipment Manufacturer). This challenge further grows against the background of the increasing number of functions and widening ranges of variants and versions for each vehicle model. For example, Burgdorf[97] deduces a number of $160 \cdot 2^{70}$ variants for the BMW 318i (E90) with components such as body form, engine, transmission, drive, color, A/C, infotainment.

Therefore, there are already endeavors to use other test execution tools alongside real driving for final safety validation. The only example of applying SiL known to me is the homologation of ESC systems. According to ECE Regulation 13H for the EU[98], there is the option to perform some of these tests in simulation:

---

[94] Hakuli, S.; Krug, M.: Virtual Integration in the Development Process (2016), p. 173f.

[95] Daimler AG Press: Press report E-Class (2009). "(…) The [E-Class] arrived by way of comprehensive virtual tests with digital prototypes and a total of 36 million test kilometers (…)." (Retrieved 28/07/2014)

[96] Fach, M. et al.: Bewertung der Beherrschbarkeit von Fahrerassistenzsystemen (2010).

[97] Burgdorf, F.: Diss., Eine kunden- und lebenszyklusorientierte Produktfamilienabsicherung (2010).

[98] UN/ECE: Regulation Nr. 13-H (2010).

> *When a vehicle has been tested physically in accordance with [(real world testing of a master car)], the compliance of other versions or variants of the same vehicle type can be proven by means of computer simulations that adhere to the test conditions […] and the test procedures […].*

Note that this only applies to the ESC system. As an example, Baake et al.[99] describe the homologation of ESC systems for vans from Daimler AG in collaboration with Robert Bosch GmbH and IPG CarMaker™: Using what are known as master cars, a vehicle model was created in CarMaker, and these master cars were used to collect reference data on the basis of which the simulation model was validated. This enabled a simulation-based recommendation for the approval of further vehicle variants with different settings. Baake et al. also report on the transfer of this procedure to the Cross Wind Assist (CWA) function, although this has not been done at the time of their publication.

2.2 Requirements for a Test Concept[100]

Q8 What does a test concept have to fulfill?

In order to discuss why AD3+ poses a particular challenge for safety validation, the requirements for test concepts to assess safety are recapitulated[100]. These are divided into effectiveness and efficiency criteria.

2.2.1 Effectiveness criteria

Representative – valid

The requirement for representativeness has two aspects: On the one hand, the test case generation has to ensure that the required test coverage is achieved. For example, a vehicle should not only be tested at 20°C and sunshine if it will be exposed to snow, rain, and temperatures under 0°C in real situations. Additionally, vehicle limit samples (tolerances during production) should be considered in the test case generation. On the other hand, the test execution (HiL, SiL, test tracks, etc.) must encompass the minimum degree of reality required. This means that the simplification in the representation of reality must neither influence the behavior of the OuT nor the behavior and properties of the environment with respect to real behavior.

[99] Baake, U. et al.: Testing and simulation-based validation of ESP systems for vans (2014), p. 30ff.

[100] Wachenfeld, W.; Winner, H.: The Release of Autonomous Vehicles (2016), p. 432ff.

Variable

The test execution must provide the option to implement all the test cases defined by the test case generation.

Observable

For the test evaluation in particular, it is necessary to observe parameters of the test execution. Only when the situation can be described, it is possible to make the statement test “passed” or “not passed”.

2.2.2 Efficiency criteria

Economical

There are two parts to the requirement for the economical test concept: On the one hand, the test execution should be prepared and carried out as quickly as possible in order to be able to provide feedback on the test object to the persons involved in the development immediately. On the other hand, it must be ensured that the test execution is prepared and carried out at the lowest cost possible.

Reproducible

Reproducibility greatly reduces the work required for regression tests. For example, if an error has been detected and the OuT modified accordingly, the goal is to subject the OuT to a test in the same scenario as before.

In good time

The earlier in the development process a product can be tested informatively, the fewer the development steps that need to be repeated in the case of an error.

Safe

The test execution should not exceed the accepted risk for all participants. This must be considered in particular for real driving, whereby road users are participating in the test without their knowledge.

The requirements described are fulfilled sufficiently by the current test concepts and therefore the four different automation levels presented are approved. However, the

recalls[101] or software updates[102] of all the OEMs, which affect millions of vehicles, indicate that these test concepts certainly do not address everything. Are these concepts also suitable for validating the safety of new systems such as higher automated driving in public road traffic? The presented requirements do not change for the assessment of AD3+. However, as will be described in the following section, the OuT changes greatly.

2.3 Special Features of AD3+

Q9 What is different comparing AD3+ and today's series vehicles?

In the following section, the difference between AD3+ and current driving in road traffic is explained. After this, the differences between the traffic systems for air travel, rail travel, and road traffic are presented in compact form to argue why only limited findings from these areas can be transferred to the assessment of AD3+.

2.3.1 Comparison between AD2- and AD3+ road vehicles

For the previously described safety validation of the levels of automation available in series (AD2-), the focus is on the vehicle. In particular the focus is on its controllability by the driver. In the combined representation of the three-level model for human target-oriented behavior based on Rasmussen[103] and the three-level hierarchy of the driving task based on Donges[104] in Figure 16, this validation corresponds to the elements with the green background. The vehicle and its behavior in the longitudinal and lateral directions are tested; in this process, the behavior and abilities of the future driver are not tested. Only the possibilities for the test driver to control the vehicle in the test cases by means of steering and acceleration control are addressed. Therefore, the green box only overlaps slightly with the area that represents the driver and the environment. Perhaps, from the point of view of a current test manager this seems unusual, because already today this little portion corresponds to a high expenditure (compare again 10^6 h from Figure 13). Nevertheless, this is just a small slice of the possible combinations the real environment[105] offers, especially when combining road surface conditions, lighting conditions, other objects, ego motion states, etc..

[101] Harald Altinger et al.: Testing methods used in the automotive industry (2014), p. 2.

[102] Tesla Motors Inc.: Upgrading Autopilot Release Notes v8 (2016).

[103] Rasmussen, J.: Human Performance Models (1983).

[104] Donges, E.: Fahrerverhaltensmodelle (2011).

[105] (The coloring of Figure 16 should be seen as a qualitative not quantitative comparison.)

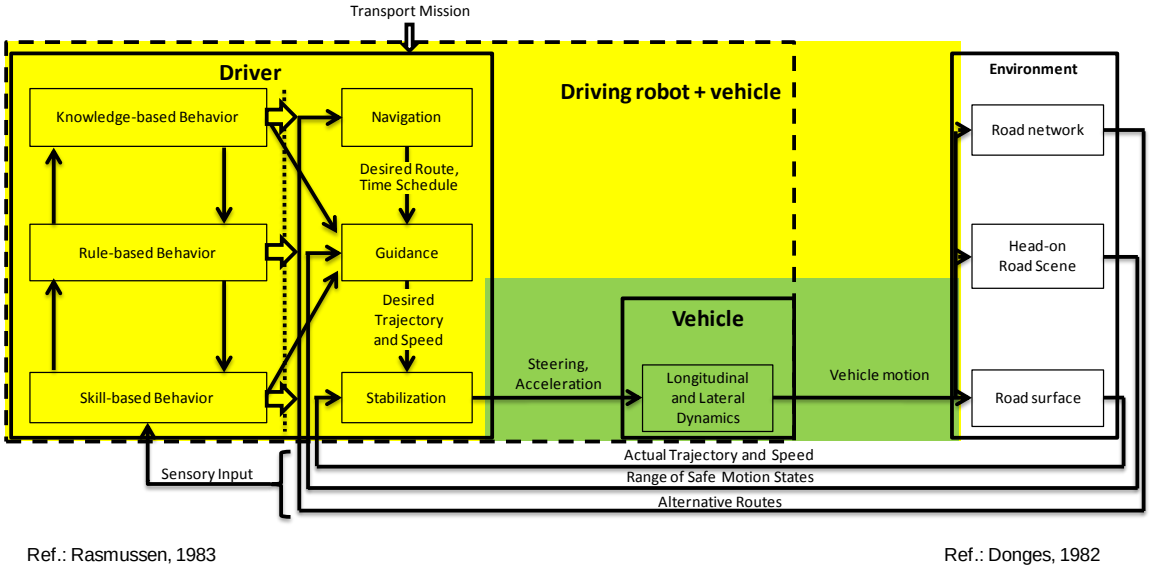


Figure 16 Three-level model for human target-oriented behavior based on Rasmussen[106] and the three-level hierarchy of the driving task based on Donges[106]

For AD3+, the abilities of the driver are now omitted and he/she no longer functions as a backup. The driving task, i.e. navigation, guidance, and stabilization/control, is taken over by the driving robot. This means that for AD3+, there is no test of the controllability, but only a test of the operation of a technical system. On the one hand, this makes the test easier because the uncertainties due to the human and its individual differences no longer need to be covered by the test. On the other hand, there is no longer the option to use test cases and test drivers to draw conclusions about other use cases. The human is omitted, who generally acts based on skills, rules, and knowledge.

For the safety validation of current systems, safety resulting from the driver and the vehicle in combination must be proven; however, for the production release of the vehicle, today's focus is solely on the vehicle. Additionally assumed, but not tested, is the "reliability" of the driver. In assessing the automated system in terms of safety, the safety which must be proven now results exclusively from the technical system of the driving robot and the vehicle (yellow field of Figure 16).

Figure 16 shows on the one hand that in case of AD3+ the quantity of tasks that must be tested increases: The driving robot is required for a wide variety of application areas (see the different use cases) such as navigation, guidance, and stabilization/control. This task quantity presents a particular challenge in public spaces without access limitations. On the other hand, the quality of tasks for the technical system changes. Current technical systems are merely tools following instructions, or are continuously monitored by

[106] Wachenfeld, W.; Winner, H.: The Release of Autonomous Vehicles (2016), p. 434. Additionally compare the primary source Donges, E.: Fahrerverhaltensmodelle (2011), p. 15. As well as Rasmussen, J.: Human Performance Models (1983), p. 258.

a human. While for AD3+ the unsupervised execution of a task must fulfill the requirements of safety discussed at the beginning of this document.

2.3.2 Comparison of the stipulations in air traffic, road traffic, and rail traffic

Along with road traffic, there are other traffic systems in which automation has established itself. The following section will discuss the extent to which the challenges and solutions from these areas are transferable to road vehicle automation.

The automation in (civilian) air travel does not currently provide any examples of full automation. Even if pilots only very rarely actually perform flying tasks, they are still present in a supervising and operating capacity. Table 2 provides an overview of the differences in the traffic systems, which is taken from Weitzel et al.[107] and Ständer[108]. For the safety validation, the safety concept for the traffic flow is of particular interest, as this shows the main differences between air travel and road traffic. Air travel operates in a legally self-contained traffic space, a collision warning system is mandatory, and external monitoring of operations is provided by air traffic control.

The railway traffic system provides examples of full automation: For example, an automated underground railway is in operation in Nuremberg[109]. However, according to Table 2, even in this traffic system the safety concept for the traffic flow in particular differentiates between road traffic and the railway. There is a legally self-contained traffic space for rail travel; in addition, logic-based systems and external monitoring are used to avoid a collision between two trains.

[107] Weitzel, A. et al.: Absicherungsstrategien für Fahrerassistenzsysteme (2014).

[108] Ständer, T.: Diss., Modellbasierte Methode zur Objektivierung der Risikoanalyse (2011).

[109] Reschka, A.: Safety Concept for Autonomous Vehicles (2016), p. 480.

Table 2 Comparison of the conditions in the traffic systems, taken from Weitzel et al. [107] and based on Ständer[108]

	Air travel	**Road traffic**	**Rail travel**
Movement options	3-D (space)	2-D (area)	1-D (line)
Operator			
Responsible vehicle operator	Usually redundant	Not redundant	Not redundant
Professionalism of the vehicle operator	Almost completely full-time occupation	Small proportion full-time occupation	Almost completely full-time occupation
Training			
Theory	> 750 hours	> 21 hours	~ 800 hours
Practice	> 1500 hours	> 9 hours	~ 400 hours
Training for vehicle type	Yes	No	Yes
Further training	Required	Not required	Required
Safety concepts of the traffic flow			
Traffic space self-contained	Legally defined boundaries	In special cases	Legally defined boundaries
Driving by sight	No, only in special cases	Yes	No, only in special cases
Technical equipment (examples)	Collision warning systems mandatory	Road markings, traffic lights, traffic signs	Automatic vigilance device, intermittent train control, automatic driving and braking controls
External monitoring	Yes, air traffic control	No	Yes, centralized traffic control, operation center
Technical framework			
Documentation of tours / operating hours	Yes	No	Monitoring of operating performance, autom. tachograph
Servicing, repairs	Only by certified companies	Workshops, Do it yourself	Only by certified companies, and then also small workshops
Accident analysis	Every accident / serious malfunction, by independent state-run body	In individual cases, by certified assessor	Every accident / serious malfunction, by independent state-run body
Number of vehicles (in Europe)	10^3 (decreasing)	10^6 (increasing)	10^3 (decreasing, with increasing kilometric performance of each traction unit)
Change of model	Approx. 20 years	Approx. 5-7 years	Approx. 20 years for traction units

As a mixed operation, road traffic does not fulfill the condition of a self-contained traffic space and external monitoring. The differences show why solutions for the production release cannot be transferred directly to the transport modality of automated driving.

Besides the differences of the traffic systems in general, there also exist differences in the statistics that challenges the comparison of safety of different means of transport. The definition of the severity of injuries for rail and road are harmonized in Germany since 2004. However, this is not the case for aviation as Vorndran[110] explains: Aviation counts an injury as severe if the victim had to stay in a hospital at least two days during one week after the accident, whereas road and rail define a severe injured victim if he/she had to stay in a hospital for at least 24 hours. Here it should be mentioned that for comparing traffic systems it is not reasonable to compare accident numbers, like for comparing different types of driving. The injury per accident numbers differ significantly. Also, the way an accident and thus a victim is registered in the statistics differs. In road traffic, the accidents are recorded by the police, whereas in rail traffic accidents are reported from the operating company and in avionics it is the German Federal Bureau of Aircraft Accident Investigation (BFU) that is responsible for the investigation of civil aircraft accidents and serious incidents within Germany. The accidents that are recorded for the different traffic systems also differ as road and rail only count accidents directly connected to traffic acts. However, avionics for example also register cases where people were injured due to objects falling down inside the cabin.

Not only the recorded accidents and the severity of injuries within the statistics differ. Also the safety reference numbers should be selected carefully. For example, the stock of vehicles or aircrafts as a reference figure is excluded by Vorndran[110], because the ones are means of individual mobility with an average[111] of 1.5 people using one vehicle, whereas others are means of mass transportation. Also, the usage time is excluded as figures for this do not exist separated for the different means of transportation. The same counts for the frequency of usage. These numbers aren't reported for rail and road. Also, the published numbers of people transported for the different means of transportation is imperfect – especially the private aviation sector is unreported. Nevertheless, following Vorndran[110] the numbers of people transported together with the distances traveled with the different means of transportation are used for comparison. Thus, the difference between mass and individual transport is supposed to be compensated by the exposure value passenger-distance. It should be mentioned that also the distance traveled is imperfect mainly due to the differences of inland vs. domestic traffic (German: Inlands- vs. Inländerkonzept). Inland traffic refers to traffic within a country whereas

[110] Vorndran, I.: Unfallstatistik-Verkehrsmittel im Risikovergleich (2010), p. 1084.

[111] Follmer, R. et al.: Mobilität in Deutschland 2008 (2010), p. 3.

domestic traffic refers to traffic generated by vehicles registered in the respective country. Due to traffic of non-domestic vehicles or aircrafts, these numbers differ for each mean of transportation.

In Vorndran[110] the following numbers are compared:

Table 3 The average numbers for 2005 to 2009 in Germany for victims per one billion passenger-kilometers for different means of transportation[112]

Mean of transportation (Verkehrsmittel)	Passenger vehicle (Pkw)	Bus (Kraftomnibus)	Train (Eisenbahn incl. S-Bahn)	Tram (Straßenbahn incl. Stadt,-Hoch,-Schwebe, U-Bahnen)	Aircraft weight at start > 5.7 t (Flugzeug)
Injured per one billion passenger-kilometers	275.8	73.9	2.7	42.3	0.3
Fatalities per one billion passenger-kilometers	2.93	0.17	0.04	0.16	0

The challenge increases for comparing safety when also looking at other countries. Find a discussion on safety comparison of different means of transportation for the USA in Savage[113]. As an example, similar numbers like above are given for the USA in Table 4.

Table 4 The average numbers for 2000 to 2009 in the USA for victims per one billion passenger-kilometers (1 km ≈ 0.6214 miles) for different means of transportation[114]

Mean of transportation	Car or light truck	Bus (> 10 passengers)	Commuter rail and Amtrak	Urban mass transit rail	Commercial aviation
Fatalities per one billion passenger-kilometers	4.52	0.0684	0.267	0.149	0.0435

The statistics of the different traffic systems show differences in quantity but also, as has been described, in the definition and methodology for recording and reporting events. Consequently, care needs to be taken if different means of transportation are used for comparison with AD3+ and road traffic in general.

The comparisons given above should not exclude the possibility that solutions from air travel and rail travel are of interest for road traffic. Certainly, similar problems such as

[112] Vorndran, I.: Unfallstatistik-Verkehrsmittel im Risikovergleich (2010), p. 1087.

[113] Savage, I.: Comparing the fatality risks in United States transportation across modes and over time (2013).

[114] Vorndran, I.: Unfallstatistik-Verkehrsmittel im Risikovergleich (2010), p. 1087.

the reliability of safety-relevant components exist. Nevertheless, due to structural and organization differences, existing solutions should be examined again for road traffic. These differences result in safety values that are orders of magnitude above those of road traffic. Thus, for the further development of a safety assessment concept, other means of transportation are neglected as a safety benchmark.

2.4 The Challenge of Releasing AD3+ for Production – "Approval-Trap"[115]

Q10 Why can today's concepts not be used to release automated driving?

As has been shown, the functions of automated driving as an OuT differ fundamentally from current road vehicles, but also from means of transportation in air and rail travel. Therefore, the meaningfulness of presented current test concepts when transferred onto AD3+ is examined. Additionally, in the following subsections, the effect of continuing with the current test concept is discussed.

2.4.1 Validity of current test concepts for automated driving

It has already been discussed that a test concept consists of test case generation and test execution. In the following it is discussed how and whether both are transferable to automated driving.

Test case generation

The three procedures for test case generation have already been explained briefly ahead; these procedures are based on the assumption of the driver's driving capability. The question of whether a random driver can control the test object is tied to the legally stipulated driver's license. According to the German Road Traffic Act[116] (§ 2 Abs. 2), this driver's license is only issued if, among other things:

- the applicant has attained a minimum age,
- he/she is suitable for driving a motor vehicle,
- he/she has received training,

[115] The basic idea of the "Approval-Trap" goes back to Winner, H.; Wolf, G.: Quo vadis, FAS? (2009).Winner, H.; Weitzel, A.: Die Freigabefalle des autonomen Fahrens (2011). As well as Winner, H.; Wachenfeld, W.: Absicherung automatischen Fahrens (2013).) and is elaborated in more detail in Winner, H.: Quo vadis, FAS? (2015).

[116] BMJV: StVG (2016).

- and has passed theoretical and practical tests.

And according to § 2 Abs. 4 StVG, suitable is taken to mean:

> *A person is suitable for driving motor vehicles if he/she fulfills the necessary physical and mental requirements and has not substantially or repeatedly contravened traffic regulations or criminal laws.*

On the basis of this required driving capability on the part of the driver, the test case generation is limited to example situations: It is assumed that when the test driver has mastered these example situations, he/she and every other driver with a driver's license will also master the other relevant non-tested situations when driving. These include situations in which the driver is actively driving, but also those situations in which the driver is supervising the system and takes over control if necessary. Therefore, in combination with the driver's license test, these test cases provide a metric that allows a conclusion to be drawn about the safety of the driver – vehicle system. The way in which it would be possible to further optimize the practical driver's license test, as an evaluation basis for assessing the driving capability, is discussed by Bahr[117].

In the absence of the driver, the currently accepted metric no longer applies, and therefore the reduction of the test cases is no longer admissible. The test case generation for AD3+ must cover the driving capabilities in particular – a new quality of functions – which the human previously brought to the driver – vehicle system. The theoretical and practical tests of the driver's license test do not represent the difficulty. However, the following paragraphs – § 10 Minimum Age, § 11 Suitability, and § 12 Visual Faculty of the Driver's License Regulation – present the challenge. Therefore, these paragraphs stand implicitly for comprehensive requirements for the properties of the humans who perform driving tasks. The human who fulfills these requirements has

- experienced tens of thousands of kilometers as a road user,
- experienced social behavior as a member of society,
- learned cognitive abilities,
- trained sensomotoric abilities.

I am not aware of any method for validly testing these functions for a technical system. Therefore, the accepted metric and the reduction of the test cases no longer apply if the human is removed from the responsibility of performing the driving task. The *current* test cases are not meaningful for releasing automated vehicles for production, and therefore the test case generation must be adapted to the new system.

[117] Bahr, M.; Sturzbecher, D.: Bewertungsgrundlagen bei der praktischen Fahrerlaubnisprüfung (2013).

Test execution

Different methods ranging from HiL to SiL to real test-driving are used for the test execution[118]. Although there is still a need for real test-driving as an important method for the approval[119]; the reason for this, in particular, is the validity combined with the justifiable economic effort. However, along with the economic effort, higher automated driving also presents a systematic challenge for the known methods. At present, real driving stands for driving in public road traffic with test drivers. The task of the test driver is to drive or supervise the vehicle in every situation in accordance with the task of the vehicle user. Transferred to AD3+, the use of a test driver in the driver's seat would not represent the behavior of a real user, as the user does not have to supervise the vehicle and the environment anymore, ready to intervene if the automation makes a mistake. Additionally, the vehicle could also participate in the road traffic without passengers (depending on the use case), and therefore a test driver would represent a non-real component in the vehicle. As a result, there is a risk that the use of a test driver could influence the other road users and alter their behavior. Further reflections on this topic can be found at Färber[120].

Therefore, along with the test case generation, the current test execution is not directly transferable to AD3+. Research and development has to be executed that adapts the test execution tools for assessing AD3+.

2.4.2 Millions of kilometers on public roads until the production release of fully-automated vehicles[121]

The following theoretical consideration will show what it means to retain the current test concept despite the differences shown. Let us assume that a reduction in the test cases was not possible for AD3+, because no method like the driver's license test for humans would exist. The objective still is to draw a conclusion as to whether the risk is increased or not by the use of the higher automated vehicle:

$$\rho_{\mathrm{acc}} = \frac{R_{\mathrm{add}}}{R_{\mathrm{avo}}} < 1$$

[118] Schittenhelm, H.: Real World effectiveness (2013).

[119] Schöner, H.-P. et al.: Testing with coordinated automated driving (2009), p. 1. Glauner, P. et al.: Effiziente Felderprobung von Fahrerassistenzsystemen (2012), p. 5.

[120] Färber, B.: Communication Problems Between Autonomous Vehicles and Human Drivers (2016).

[121] Winner, H.; Wachenfeld, W.: Absicherung automatischen Fahrens (2013).

Here it should be noted that this condition is in no way imperative. However, for the theoretical consideration, a condition of less than 1 is assumed to be the level to cope with.

As has been discussed in section 1.4.1, a metric that can be used to determine such a relationship are the figures from the subsequent evaluation of traffic accidents. For Germany, these are the figures from the Federal Statistical Office. In 2013 for example, the Federal Statistical Office[122] cites $A_{\mathrm{wF,a}} = 3131$ accidents with fatalities recorded by the police. The figure for fatalities is used because this represents the worst-case scenario for the verification required. With a total of $d_{\mathrm{a}} \approx 725.7 \cdot 10^9$ km driven in Germany[123], the safety performance SP_{wF} is represented by an average of $231.8 \cdot 10^6$ km between two accidents with fatalities. As these figures only represent an expected value, shorter or longer distances also exist between two accident events of this class. To represent this distribution of the accident for AD3+ events k, the Poisson distribution[124] is used:

$$P_\lambda(k) = \frac{\lambda^k}{k!} \mathrm{e}^{-\lambda} \tag{2-1}$$

It is assumed that the occurrence of an accident is an independent and non-exhaustive random process $P_\lambda(k)$. In the equation, k corresponds to the number of accident events of one class and λ to the expected value with which this event occurs. The expected value λ is defined by the quotient

$$\lambda = \frac{d_{\mathrm{test}}}{SP}, \tag{2-2}$$

whereby d_{test} stands for the observed test kilometers and SP for the safety performance of the system. The performance, as explained before, denotes the expected number of travel distance between the events. The probability distributions for $k = \{1\ 2\ 3\ 4\ 5\}$ and $\lambda = \{1\ 2\}$ are shown in Figure 17 as an example for the next gedankenexperiment.

The figure illustrates the problem of providing verification of a certain level of risk: It is assumed that the dark distribution stands for an AD3+ vehicle and the light distribution for a driver-only vehicle. Both vehicles are driven the same test distance $d_{\mathrm{test}} = a_d \cdot \bar{d}$, with the distance factor $a_d = 2$ and the average interval $\bar{d}$ between two fatal accidents in today's traffic. The safety performance of the AD3+ vehicle $SP_{\mathrm{OuT}} = a_{SP} \cdot SP_{\mathrm{bench}}$ is greater than that of the driver-only vehicle (SP_{bench}) by the safety performance factor $a_{SP} = 2$. The index of the AD3+ safety performance is called "OuT" as this is the object

[122] Destatis: Verkehr - Verkehrsunfälle - 2012 (2013).

[123] This number will be discussed in more detail in subsection 4.1 "Challenge of the Qualitative and Quantitative Data Demand".

[124] Further arguments for choosing the Poisson distribution are given in subchapter 3.2.

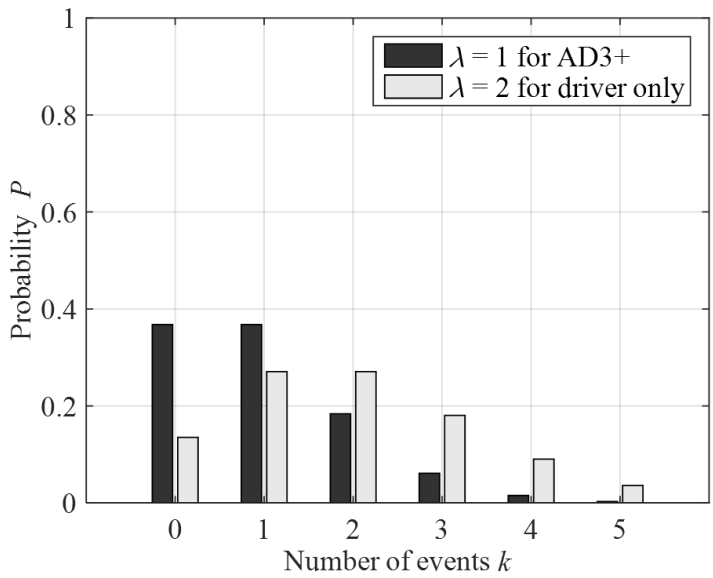


Figure 17 Poisson probability distribution for the number of accidents with two different expected values

under test, whereas the driver-only index is called "bench", indicating that the safety performance of the human driven vehicle builds the benchmark ($SP_{\text{bench}} = \bar{d}$). Consequently, the expected value for the automated vehicle is $\lambda = 1$, and for the driver-only vehicle $\lambda = 2$.

Even though the AD3+ vehicle is characterized by double the safety performance of the driver-only vehicle according to the previous assumption, during the test the AD3+ vehicle was unfortunately involved in a fatal accident (probability $P_1(1) = 1 \cdot \mathrm{e}^{-1} \approx 0.37$). In contrast, in this gedankenexperiment the driver-only vehicle was not involved in a fatal accident (probability $P_2(0) = 1 \cdot \mathrm{e}^{-2} \approx 0.14$). That is just one of many possible outcomes. However, for understanding the challenge this outcome is assumed. Therefore, a conclusion that the AD3+ vehicle is less safe than the driver-only vehicle must be called into question. In any case, this example shows that a distance factor a_d greater than 2 is necessary to be able to draw a conclusion with a sufficiently high significance about the safety performance of AD3+.

From a scientific point of view[125], an error probability must be assumed. For example the error probability $e = 5\ \%$ can be used. A correspondingly large distance factor a_d must be selected, depending on the number of events k_{count}, in order to have a probability of less than 5 % for a vehicle with a lower performance to achieve this small number of events. These thoughts are expressed by the inequality

$$P_{\lambda_+}(k \leq k_{\text{count}}) \leq e. \tag{2-3}$$

[125] Cowles, M.; Davis, C.: On the origins of the 5% level (1982).

The left side of the inequality represents the cumulative probability of the counted number of events k_{count}. A function $\lambda_+(k_{\text{count}}, e)$ is defined as the minimal solution of the numerical search for

$$P_{\lambda_+}(k \leq k_{\text{count}}) = \sum_{0}^{k_{\text{count}}} \frac{\lambda_+^{\text{k}}}{k!} \mathrm{e}^{-\lambda_+} = e \tag{2-4}$$

Exemplary results for the determining expected value λ_+ are found in tables in appendix A. The necessary distance factor a_d results from knowing λ_+ by solving equation (2-2)

$$\lambda_+ = \frac{d_{\text{test}}}{SP_{\text{bench}}} <=> \lambda_+ = \frac{a_d \cdot \bar{d}}{\bar{d}} <=> a_d = \lambda_+ \tag{2-5}$$

Figure 18 shows the result of this consideration and the numeric values.

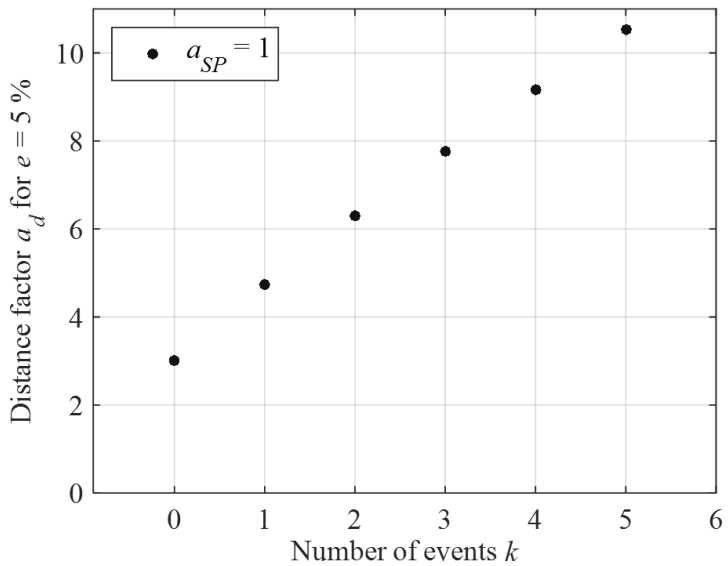


Figure 18 Distance factor at error probability 5 %

The data point at zero events means that, with a distance factor $a_d \approx 3$, the probability is less than 5 % that a vehicle performing worse than the comparison group is not involved in an event.

Unfortunately, the probability of success for this test is just as small. Because if the test vehicle is just as good as the comparison group, i.e. safety performance factor $a_{SP} = 1$ applies, it follows that the probability of success for this verification is also only 5 %. For the test to be successful, a greater probability of success is desirable, thus a greater safety performance of the OuT $a_{SP} > 1$. As an example, a probability of success of 50 % for the proof is now demanded; by which a test shows that the test vehicle is not worse than the comparison group. For this, the test vehicle must perform better than the test group.

This is formalized by

$$P_{\lambda_{SP}}(k \leq k_{\text{count}}) \leq 50\ \%. \tag{2-6}$$

The determining $\lambda_{SP} = \lambda_{+}(k_{\text{count}}, 50\%)$ is again found in tables or by numerical search. The necessary safety performance factor a_{SP} results from knowing λ_{SP} and solving equation (2-2)

$$\lambda_{SP} = \frac{d_{\text{test}}}{a_{SP} \cdot SP_{\text{bench}}} \Leftrightarrow \lambda_{SP} = \frac{a_d \cdot \bar{d}}{a_{SP} \cdot \bar{d}} \Leftrightarrow a_{SP} = \frac{a_d}{\lambda_{SP}} \tag{2-7}$$

Replacing the distance factor by equation (2-5), the safety performance factor is

$$a_{SP} = \frac{\lambda_{+}}{\lambda_{SP}} \tag{2-8}$$

Figure 19 shows the result of this consideration and the numeric values.

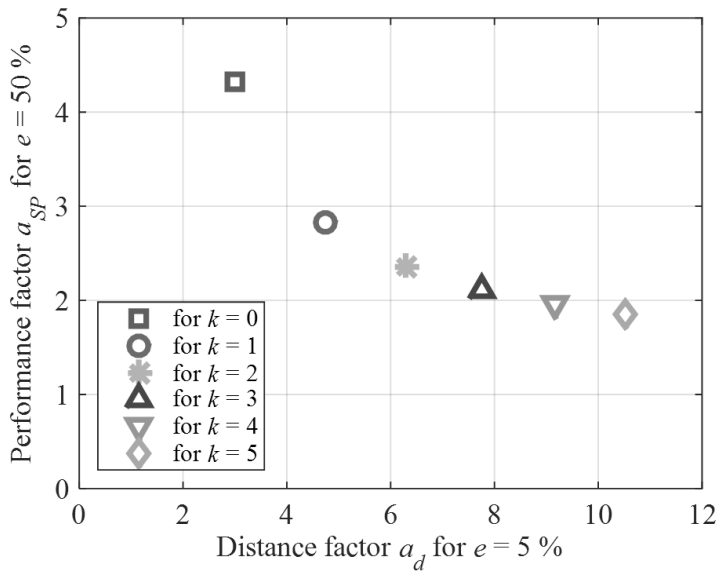


Figure 19 Performance factor over distance factor at an error probability of 5 % and a probability of success for the test of 50 %

The first point expresses the following: If the test vehicle is approximately 4.3 times better (a_{SP}) than the comparison group (SP_{bench}), the test has successfully proven with a probability of 50 % that the test vehicle is better than the comparison group with an error probability of 5 %.

The consequence for the test drive with the AD3+ vehicle is demonstrated by the safety performance benchmark $SP_{\text{wF}} \approx 231.8 \cdot 10^6$ km between two accidents with fatalities. The last point (blue diamond) in Figure 19 expresses the following: If the AD3+ vehicle is twice as good ($a_{SP} = 2$) as the comparison system (current vehicles), approximately a tenfold the test distance being at least $d_{\text{test}} = 2.3 \cdot 10^9$ km must be driven ($d_{\text{test}} =$

$a_d \cdot SP_{\mathrm{wF}}$). In this case, the verification would have been achieved with 50 % probability, but five events would also occur with the same probability.

Ironically, it follows from this consideration that the safer the vehicle driving benchmark is, the greater the testing distance has to be, as the comparison value is correspondingly higher.

What hasn't been discussed yet is the share between being responsible for an accident or being the person that is only affected by the accident without responsibility. If this would be taken into account for the calculation[126], the benchmark value would further increase. As an example[127], in Germany 2013, the average driver was responsible for 55.9 % of his accidents. In addition, age differences are reported. Drivers from 18 to 21 years are made responsible for 71.1 % of their accidents, whereas drivers from 45 to 55 years are only responsible for 49.1 %. This example shows that the selection of a benchmark is not trivial. Although this question might be of interest when it comes to the question of guilt or to liability cases, for the safety outcome in this thesis it is unimportant. Especially because no numbers or reasonable estimations on these exist for AD3+, it would result in an offset on the safety scale.

This theoretical excursion into statistics shows that production release can become a challenge, if not an actual trap, for AD3+ driving due to the high distances calculated. Hereby, a number of factors for determining the test distance have not been addressed yet; for example, a variation of the system would mean that the test distance would have to be driven again, or the test with and without passengers could use a factor of two in the calculation. The effect on the determined necessary kilometers of different parameters such as area of use, accident severity, accident cause, and comparison vehicle is not considered here but is derived in detail in Winner[128]. The publication from Kalra and Paddock[129] takes a similar approach and leads to corresponding results. Both publications in Europe and the US come to similar conclusions and propose similar actions.

These considerations are theoretical observations with freely made assumptions. However, this approach is still suitable for illustrating the problems and challenges, and for motivating the approaches that follow next.

---

[126] Winner, H.: ADAS, Quo Vadis? (2016), p. 1566.

[127] Destatis: Verkehrsunfälle - Zeitreihen 2014 (2015), p. 104.

[128] Winner, H.: ADAS, Quo Vadis? (2016), p. 1557ff.

[129] Kalra, N.; Paddock, S. M.: Driving to Safety: How Many Miles? (2016).

2.4.3 Conclusion on the Challenge of Releasing AD3+

The changing OuT reveals a lack of knowledge for the release of AD3+. New and special features, as discussed in section 2.3, have to be covered by testing. The pure test driving and statistical evaluation is economically not feasible, as explained in section 2.4. When shifting testing from real-world driving to HiL and SiL, knowledge is lacking on what to test. Additionally, the validity of these other test execution tools is uncertain for the new testing task.

Thus, the challenge is that knowledge is missing on what to test, as well as on how to adapt existing tools. This challenge is special compared to other new technologies developed in the past, because AD3+ covers special features by replacing the human driver and his or her high level of safety. Solutions are needed that close the lack of knowledge in a reasonable manner.

2.5 Possible Approaches for Solving the Challenge of Testing

Q11 Is there no approach other than real-world driving to solve the challenges of testing?

As has been shown, AD3+ represents a new OuT which, due to its properties, calls the classic test concepts into question. Adapted approaches are required to overcome the testing challenge described: Accordingly, the next section will discuss why reusing approved functions, and thus an evolutionary approach, seems necessary from the perspective of safety validation. After this, existing approaches that could speed up testing will be discussed. These approaches formulate today's approaches and therefore explain the best possible way to overcome the "Approval-Trap". (Of course completeness cannot be claimed here.) However, as will be discussed in the last Section 2.5.3, uncertainty will still exist when proving safety with these approaches. This motivates chapter 3 the "Theory: Stochastic Model for Safety Assessment".

2.5.1 Reusing Approved Functions

The first and simplest possibility of obtaining the production release for a new system is in reusing functions already released. If a system is used in the same way as before, a release already issued can be transferred to future products[130]. However, if the scope of

[130] ISO: DIS 26262: Road vehicles - Functional safety (2008), p. 33 - part 8.

functions is expanded, this new function must be treated again; the smaller the new involved area is, the less work is required.

Based on this argument, an evolution across all dimensions would seem to be a possible approach for overcoming the testing challenge. Dimensions in this case refer, for example, to the speed, the area of use, but also the level of automation. A distinction can be made between two perspectives in selecting the evolution steps: From the perspective of a function developer, due to the reduced speed and the limited access to the scene, the Autobahn during a traffic jam is a suitable starting scenario. From the perspective of the previously presented statistical considerations, a meaningful starting scenario would be one in which the human as a comparison group performs as badly as possible, that is making as many errors as possible. As many errors as possible corresponds to short distances between accidents, thus easing the validation of safety[131].

The revolutionary step – a fully-automated vehicle without evolutionary intermediate steps – contradicts this approach and seems unlikely. Smith[132] uses the phrases "something everywhere" and "everything somewhere" that explain the alternatives for evolutionary approaches in a simplified manner.

2.5.2 Speeding up Testing

Despite the evolutionary approach, the safety of new functions, although they are small, still has to be validated. To speed this up, there are basically two adjustments that can be made: Firstly, the *What* can be changed, and secondly the *How*. What test cases need to be inspected, and how will these tests be performed? Schuldt et al.[133] call this the test case generation and the test execution.

Test Case Generation

The test case generation defines the tests to be carried out. According to Schuldt et al.[133], the large number of influencing factors with a wide range of values results in a conspicuous number of test cases. As already described, the systems currently in use are based on the capability of humans and their options for controlling the vehicle. This results in a stark reduction of test cases that are theoretically required. Therefore, a metric exists that enables a conclusion about the safety without testing all the situations. This reduction does not apply for higher automated vehicles, and therefore new ways must be found for reducing the number of test cases for these vehicles. During the test

[131] Winner, H.: ADAS, Quo Vadis? (2016).

[132] Smith, B. W.: How Governments Can Promote Automated Driving (2016).

[133] Schuldt, F. et al.: Effiziente systematische Testgenerierung (2013).

case generation, the requirements for a test concept detailed above must be considered. In particular, the representativeness is at risk when test cases are omitted.

The approaches from Glauner [134] and Eckstein [135] describe the identification of relevant or critical situations in public road traffic. Based on previously defined event classes, potential critical situations are identified during the test drives or large-scale field studies. These critical situations are incorporated into the test case generation, and less critical situations can be omitted as a result. This reduction is based on the assumption that situations that are less critical are covered by critical situations. A task that remains unsolved at present is the search for a valid measure of criticality that enables an evaluation in the first step, and the selection of critical situations in the second step.

Another procedure for reducing test cases is provided by Schuldt et al.[136]: A generic test case generation is proposed to cover factors influencing the safety ensured by the system in a sufficient way. This should use black-box testing procedures and combinatory, and be low-redundancy and efficient. This approach is based on statistical considerations without knowledge and experience of the test object, but it still has the potential to reduce the test cases required. The remaining question for research is the definition of influencing factors.

The approach described by Tatar and Mauss[137] is also suitable for black-box testing: an optimization is used for the generation of test cases. Here, the input variables of a XiL simulation are varied in such a way that the evaluation function to be defined for the test is optimized. Despite the challenge of the valid XiL simulation and the required evaluation function, this approach provides the option to focus the test cases on those evaluated as relevant.

A fourth theoretical approach is to use and test a safety concept using formal methods[138]. Similar to the human assumed to be a monitor and a part of the safety concept of current vehicles, a verified reliable safety concept could make testing the overall functionality of the vehicle in its complete representativeness superfluous. This would make a reduction of the test cases possible. These approaches stand or fall by the validity of the formalized world as will be described below. Formalized verification actually combines the test case generation with the test execution.

---

[134] Glauner, P. et al.: Effiziente Felderprobung von Fahrerassistenzsystemen (2012).

[135] Eckstein, L.; Zlocki, A.: Combined Methods for an Effective Evaluation (2013).

[136] Schuldt, F. et al.: Effiziente systematische Testgenerierung (2013).

[137] Tatar, M.; Mauss, J.: Systematic Test and Validation of Complex Embedded Systems (2014).

[138] Mitsch, S. et al.: Provably Safe Obstacle Avoidance (2013).

Test Execution / Test Tool

Along with the possibility of reducing the test cases during the test case generation, the test execution also has potential for speeding up the process. However, if we deviate from real driving and select another testing tool for the test execution, there is always an attendant simplification. This is described by means of Table 5. This table divides the testing tools into nine classes which are differentiated based on the representation of vehicle and environment. The passenger is assigned to the vehicle in this representation, as he/she is situated in the vehicle and does not actively intervene in the automated driving.

Table 5 Classification of testing tools for testing automated vehicles[139]

		Environment		
		virtual	**artificial**	**real**
Vehicle	**virtual**	SiL		-
	artificial			
	real	-		real driving

valid

economical

Real driving represents both the environment and the vehicle in reality. Accordingly, during these tests there is the risk of real accidents and their consequences. The environment is not controlled, and this results in test situations based on the randomness of reality; accordingly, the reproducibility for complex situations with other road users is not a given. This testing tool can be used, at the earliest, with the first roadworthy prototypes, and therefore occurs at the end of the development process.

An alternative is to test real vehicles in an artificial environment: This corresponds to driving on a test ground[140], as situations are created artificially on the one hand, and on the other the “road users” are conscious of being involved in a test. Reality is simplified for the benefit of safety, variability, observability, and reproducibility. From economic perspectives, while the test cases are tested specifically and do not have to be experienced randomly as in real driving, setting up the test field requires additional time and financial resources.

Additionally, an artificial vehicle could move within a real environment; in this case, artificial refers to equipping the automated vehicle with a supervisor, for example, that has the option to intervene in the driving task. This could be a test driver with a steering

[139] Wachenfeld, W.; Winner, H.: The Release of Autonomous Vehicles (2016).

[140] Schöner, H.-P.; Hurich, W.: Testing with Coordinated Automated Vehicles (2016).

wheel and pedals, or alternatively a technical system that is superior to the series system due to its more powerful (additional) sensors. If components are represented artificially, the closeness to reality suffers, but gains are created in terms of safety, reproducibility, and observability.

Along with the option of creating the environment and the vehicle artificially, there are tools that use a virtual representation in the form of computer simulations. However, strictly speaking, the two fields (gray) that combine real and virtual do not exist. This is due to the fact that the task of sensors and actuators is to "translate" between virtual and real signals. A real radar sensor cannot sense a virtual environment and a virtual converter cannot create real voltage.

In contrast, combinations of artificial and virtual environments and vehicles are possible and do exist. Examples of these are provided by different concepts of vehicle-in-the-loop (ViL)[141]. To close the loop made up of actions and reactions of the environment and the vehicle, real components are mapped in the simulation in the form of models. Here, either the sensors or actuators mentioned are stimulated. This means that they are either artificially instigated (examples of this are simulation-based videos as stimulation for camera systems or dynamometers as stimulation for drive actuators) or that the testing tools directly simulate the power signals, such as the electromagnetic wave, and try to represent real effects of sensors and actuators in the simulation with the aid of models. For more information on this, see Hendriks[142]. The use of described models calls the meaningfulness of these testing tools into question. To get valid results using such models, it must be verified that these models do not contain any impermissible simplification; here, impermissible is to be seen in the context of the function. It means that deviations from reality are only permissible below the tolerances of the function. However, if this validity has been verified, the testing tool enables greater safety during the test execution. Objects of the environment and the vehicle only encounter each other in the virtual world. Due to the virtual components, these testing tools are distinguished by greater variability, observability, and reproducibility. From an economic perspective, this testing tool has the advantage of easily varying the virtual environment or representing the vehicle in a wide range of variants. An economic disadvantage could be the validation of the models (see below). An advantage of this testing tool is the option of performing tests early in the development phase using the simulated vehicle.

The last level of abstraction represents the combination of a virtual vehicle and the virtual environment: The software-in-the-loop testing tool represents the closed control loop by modeling relevant components in the simulation[143]. In contrast to the previous

[141] Berg, G. et al.: Vehicle in the Loop (2016)., Bock, T.: Vehicle in the Loop-Simulation (2012).

[142] Hendriks, F. et al.: Prescan and VeHIL (2010).

[143] Hakuli, S.; Krug, M.: Virtual Integration in the Development Process (2016).

testing tools, the entire testing world is virtual. The tests are safe, variable, observable, and reproducible; there is also the option of using this tool early on during the development. The economic advantage is provided by the hardware independence, as there is no connection to real time any more. The execution of the tests is only limited by the computer power; simulations can be run day and night, and also parallel on a large scale. On the other hand, there is the necessary closeness to reality of the virtual test world, and therefore of every individual model: Only when the validity of the used models can be verified, virtual tests are sufficiently conclusive for a production release. Accordingly, for the economic consideration of simulation-based procedures, the validation of the models must be considered above all.

The same challenge exists for the use of formal methods. Mitsch[144] writes in this context: "We do (…) prove that collisions can never occur (as long as the robot system fits to the model)." This means that even for formal methods, the degree of reality of the models used determines the conclusiveness of the results. For example, a particular challenge that is therefore a focus of the research is the formalization of the uncertainties of machine perception or the behavior of other road users.

The discussion of test execution and testing tools shows the potential to speed up the testing. With the aid of the artificially created environment and vehicle, test cases can be set up and executed specifically. Additionally, the virtual approach enables the tests to be sped up and run in parallel, depending on the computer power used.

However, the discussion also shows that the validity of the tests, and therefore their conclusiveness, presents a challenge when artificial and virtual components are introduced.

2.5.3 Conclusion on Possible Approaches to Overcome the Approval-Trap[145]

All approaches introduced above are based on simplifications and assumptions to either replace real parts of a test with artificial/virtual ones or neglect irrelevant situations/parameter combinations. These simplifications and assumptions *can* be invalid when applied on Object under Test (OuT) assessment.

To avoid simplifications and assumptions that are not proper for OuT assessment, real driving such as road testing is necessary. This time test-driving is used for safety validation of test tools and for safety validation of assumptions. The validation of tools for a

[144] Mitsch, S. et al.: Provably Safe Obstacle Avoidance (2013).

[145] The main content and wording of this subchapter is taken from Wachenfeld, W.; Winner, H.: The new role of road testing. (2016), p. 419–435.

defined number of test cases seems possible. But again, who can tell whether the selection met the necessary situations? Therefore, we come back to the challenge raised by the statistical train of thoughts. How can we show that the tools and assumptions are valid for OuT safety assessment?

An advantage for tool and assumption validation is that the full target testing distance doesn't need to be driven with the OuT. This simplifies the accumulation of testing distance. Another factor that would reduce the huge number of possible situations that need to be covered for tool or assumption validation could be the independence of different parameters of a situation. For example, properties of traffic models are independent of properties of radar sensor models and therefore do not need to be modeled and validated in combination. This independence does not exist for the validation of the OuT as errors in real sensors lead to different behavior depending on the surrounding traffic. A disadvantage is that even more things need to be validated. For example, the behavior of other road participants needs to be reflected by the tool, at least to a certain extent.

Until now, we have not seen any proof that the advantages outweigh the disadvantages resulting in lower testing distance necessary to be driven (no matter who collects the stated amount). On the one side, the more components are replaced and the more cases are neglected, the more validation effort for tools and assumptions has to be made. On the other side, the more cases are left for road testing, the more validation of the OuT has to be performed on the road. This seems to be a trade-off between OuT validation on the one hand and tool validation for OuT validation on the other hand. Additionally, the long term perspective has to be considered as well. It may be that the first validation of tools needs a higher effort as the road testing itself, but when validating another version, vehicle type or new generation, the overall effort could be reduced by orders of magnitude. An example for that effort reduction is described in Baake et al.[146] for ESC testing.

At this point a conclusion can be drawn: When pursuing approaches to replace or reduce road testing, road tests will still be of interest as these approaches need to be validated. At least until now, it is unclear whether other approaches reduce the validation effort for the *first* AD3+ generation.

Of course, if a tool or an assumption is validated, its advantages and potential to increase efficiency can be utilized. But up to that point, validation activities based on real driving are and will be necessary.

The proof of safety of the OuT by simply road testing before SOP is economically infeasible with statistical significance. For alternative approaches, it is at least uncertain

[146] Baake, U. et al.: Testing and simulation-based validation of ESP systems for vans (2014).

if the required validation effort is reduced. Tool and assumption validation could equal out the reduction of OuT validation. This leads to the conclusion that, from a statistical perspective, the first vehicles that will be introduced will not satisfy a scientific proof of comparable safety. This conclusion is based on the assumption that the safety benchmark leads to testing distances that are economically not tolerable.

This conclusion seems to be an obstacle on the way to everyday automated driving. The state of the art does not deliver an approach to assess the safety of AD3+ in an economical way ahead of introduction. Consequently, the automotive research community should extend their research on safety assessment of higher automated driving functions!

To address the challenge of bringing automated vehicles safely into market, it is necessary to concentrate on two approaches. One is the **microscopic** and deterministic test case approach. The alternatives to real test driving described beforehand mainly address this microscopic approach. But as this first approach will leave uncertainties on safety when introducing the first AD3+, the second approach should exactly focus on these uncertainties. Thus, the second approach is called the **macroscopic** and stochastic real-world driving approach. It is important to work on both approaches and *not* to see the microscopic and deterministic test case approach as contradictory to the macroscopic and statistic real-world driving approach. Both together are of great relevance and should be seen as complementary approaches to come to a solution for the raised challenge.

For current research regarding the first, the microscopic deterministic test case approach, it is referred to two representative public funded projects:

- PEGASUS[147]: Project for Establishing Generally Accepted quality criteria, tools and methods as well as Scenarios And (German: Und) Situations for approval of highly automated driving functions. It focuses on the test cases and their generation. It is funded by the German Federal Ministry for Economic Affairs and Energy.
- ENABLE-S3[148]: European initiative to ENABLE validation for highly automated Safe and Secure Systems. It focuses on the test execution and test tools. It is funded as an ECSEL Joint Undertaking.

The second approach, the macroscopic and stochastic real-world driving approach, is addressed in this thesis. In the following two chapters, the “Theory: Stochastic Model for Safety Assessment” and the “Application: Data to Apply the Usage Strategy” focus on “How Stochastic can Help to Introduce Automated Driving”. In chapter 5, the “Consequences: The Safety Lifecycle of AD3+” are discussed and a way to connect

[147] http://pegasus-projekt.info/de/ accessed 01.02.2017

[148] http://www.enable-s3.eu/ accessed 01.02.2017

both approaches is proposed. This proposal bases on the assumption that the test cases used for assessment by the microscopic deterministic approach represent a certain number of test distance in the stochastic macroscopic approach.

3 Theory: Stochastic Model for Safety Assessment

Q 12 How to use stochastic to achieve a safe usage of automated driving?

Holló et al. describe contributing factors to road safety[149]:

> *The pyramid model can be understood as a conceptual framework describing the causal relationships between different factors present in the road safety system, but it does have certain limits.*

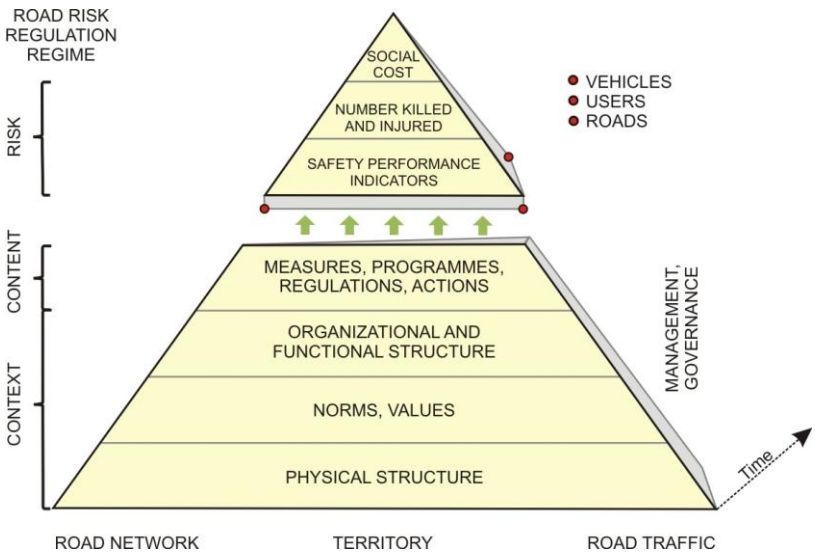


Figure 20 Road safety pyramid representation of road safety system[149]

One limitation for explaining the occurrence of accidents is the underlying stochastic process. Although I would put the pyramid shape in question, the general idea of Holló et al.'s Figure 20 is of importance to understand the difference between a purely random event and an event that underlies a stochastic process. Different factors contribute in improving or reducing road safety. Clear correlations have been shown between governance actions or road network changes and the safety outcome of road traffic. Nevertheless, numbers of killed or injured cannot be predicted in a deterministic way by these contributing factors. One, 10, 100, or even 1000 accidents (depending on the road system under observation and the severity) more or less cannot be explained by a determin-

[149] Holló, P. et al.: Road safety performance indicators (2010), p. 1142–1143.

istic model. Therefore, stochastic processes need to be discussed when arguing about road safety.

This chapter will first of all start to discuss the relationship between accidents and stochastic. Therefore, an engineer's perspective on the names "accident" and "stochastic" is discussed. Secondly, section 3.2 "The Occurrence of Accidents follows a Poisson Process" takes a step back and derives the Poisson distribution used above by a theoretical contemplation. The assumptions for using Poisson as well as the literature about different usage examples are discussed.

Up to this point, the thesis discusses whether or not to assume a stochastic process and which probability distribution should be used. From section 3.2 on, the stochastic approach using the Poisson process is defined as the core assumption that represents the basis for all further argumentations. In the state of the art, this core assumption has been used for challenging the safety of automated driving. To further develop the state of the art, the next scientific step is made. Section 3.3 tries to falsify the hypothesis of a safe AD3+. The result will be that neither more nor less safety is economically provable ahead of introduction. Section 3.4 draws the consequences and takes the next step to refine the requirements. On top of these refined requirements, the following two sections 3.5 and 3.6 define and examine an uncertainty-based usage strategy that might pave the way for the introduction of AD3+.

The applicability of the strategy to further defined use cases from subsection 1.1 is presented in the next chapter 4 that looks into existing "Application: Data to Apply the Usage Strategy".

3.1 The Meaning of "Accident" and "Stochastic"

Q13 Why should we think about stochastic when we think about accidents?

As my mother tongue is German, the following concentrates on both languages German and English.

Accidents

The origin of the word "accident" is reported in the Online Etymology Dictionary[150]:

> *late 14c., "an occurrence, incident, event," from Old French accident (12c.), from Latin accidentem (nominative accidens), present participle of accidere "happen, fall out, fall upon," from ad- "to" (see ad-) + cadere "fall" (see case(n.1)). Meaning grew*

[150] Harper, D.: "accident". Online Etymology Dictionary.

from "something that happens, an event," to "something that happens by chance," then "mishap." Philosophical sense "non-essential characteristic of a thing" is late 14c. Meaning "unplanned child" is attested by 1932.

Different definitions for today’s use of the word “accident” exist. For the use today, the Cambridge dictionary online[151] says:

something bad that happens that is not expected or intended and that often damages something or injures someone

In German accident/Unfall is defined by Duden online[152]:

„den normalen Ablauf von etwas plötzlich unterbrechender Vorfall, ungewolltes Ereignis, bei dem Menschen verletzt oder getötet werden oder Sachschaden entsteht”

Both definitions define that an event where someone or something is damaged or injured could be an accident. Additionally, the event needs to be not expected or not intended. This indicates a small chance that the event happens.

Stochastic

The origin of the word “stochastic” is also reported in the Online Etymology Dictionary[153]:

*1660s, "pertaining to conjecture," from Greek stokhastikos "able to guess, conjecturing," from stokhazesthai "to guess, aim at, conjecture," from stokhos "a guess, aim, target, mark," literally "pointed stick set up for archers to shoot at," from PIE *stogh-, variant of root *stegh- "to stick, prick; pointed" (see sting (v.)). The sense of "randomly determined" is from 1934, from German stochastik (1917).*

Stochastic in its use today is defined by the Cambridge dictionary online[154] as:

A stochastic process or system is connected with random probability

Duden online[155] explains the word stochastic/stochastisch with:

vom Zufall abhängig.

The definitions explain that a stochastic process is not deterministic and that the events that happen depend on some kind of randomness. There is the chance that an event happens or not.

---

[151] https://dictionary.cambridge.org/dictionary/english/accident accessed 24.09.2016

[152] http://www.duden.de/suchen/dudenonline/unfall accessed 24.09.2016

[153] Harper, D.: "stochastic". Online Etymology Dictionary.

[154] https://dictionary.cambridge.org/dictionary/english/stochastic accessed 24.09.2016

[155] http://www.duden.de/rechtschreibung/stochastisch accessed 24.09.2016

The Occurrence of Accidents as a Stochastic Process

The Cambridge online dictionary[156] offers the word "accident", amongst others, as a synonym or related word for "stochastic". This shows that the word "accident" by its original meaning and its use in the English language is somehow connected to a stochastic process.

Interestingly, the German language offers the word "per accidens" which means "durch Zufall"[157]. Thus, the connection between "accident" and "stochastic" as a fortuitous event also exists in German. Consequently, the word accident already naturally leads to stochastic processes.

Looking back into the history of the usage of both words "road accident" and "stochastic" by applying the Google Books Ngram Viewer[158], it seems like the occurrence of the report and discussion of road accidents might have also stimulated the thoughts on stochastic. Figure 21 depicts that during the thirties and forties of the 20th century the frequency of both strings increased.

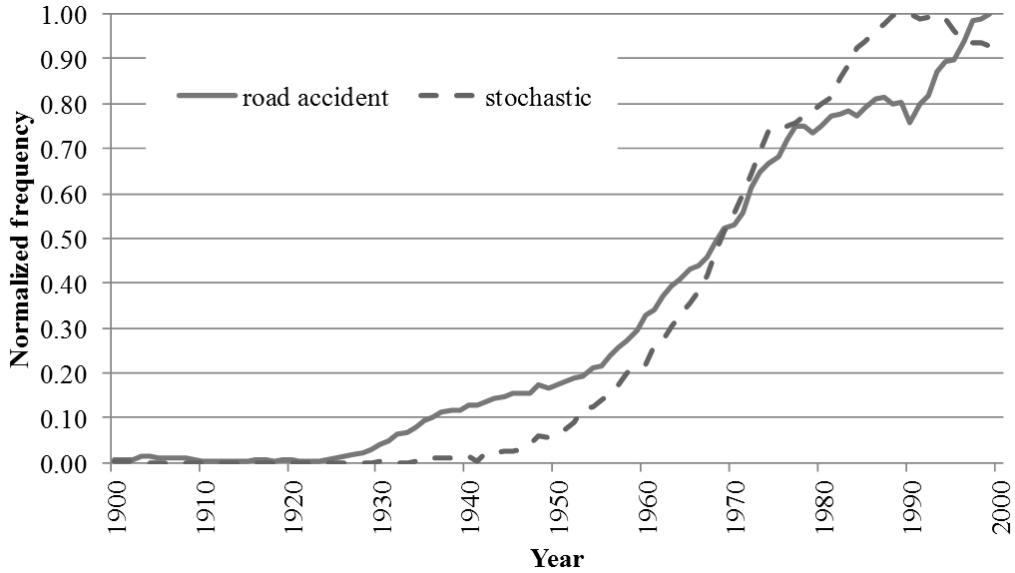


Figure 21 Normalized Google Books Ngram Viewer results that charts frequency for the two strings found in Google's text corpora "English" for the years 1900 to 1999. [158]

A possible conclusion: An accident can be seen as a special stochastic process with low probability and an unwanted outcome. The following section formalizes this conclusion.

---

[156] https://dictionary.cambridge.org/dictionary/english/stochastic?a=british accessed 24.09.2016

[157] http://www.duden.de/rechtschreibung/per_accidens accessed 24.09.2016

[158] https://books.google.com/ngrams/ accessed 24.09.2016

3.2 The Occurrence of Accidents follows a Poisson Process

Q14 Why should accident numbers follow the Poisson process?

In section 2.4 "The Challenge of Releasing AD3+ for Production – "Approval-Trap"", the Poisson distribution has shortly been motivated and used. As this is not a given approach and subject to discussion, one step back will be taken for explanation. Firstly, the usage is derived by a theoretical contemplation. Secondly, a glance will be given on the usage of this distribution in other disciplines.

Haight[159], the author of the handbook of the Poisson distribution, begins his chapter on accidents with the sentence:

> *The Poisson process as binomial limit, […], seems to fit exactly the sense of the word "accident", as a completely fortuitous event.*

The Poisson process as a basic but important example for a stochastic process takes an important role in accident analysis[160], as we will see in the following. The idea of the following section is to understand why.

3.2.1 From a Bernoulli Experiment to the Poisson Process

In accordance to an introduction into stochastic by Mittag[161], the occurrence of road accidents will now be described by a probability distribution that is derived step by step. Starting with a Bernoulli experiment:

Bernoulli experiment

First of all, the limited observation or test of a traffic participant has two safety outcomes x: Either an accident x_1 or no accident x_0, or more general an event x_1 or no event x_0. Therefore, it is assumed that the observation or test i of the road participants is a small part of real participation in traffic like for example $\Delta d = 1$ m. Δd is a part of a driven distance, not a piece of the street system. The word small in this case means that within this traveled distance not more than one event will take place. From a theoretical point of view, the small part could converge to 0 ($\Delta d \to 0$), thus the event could be seen

[159] Haight, F. A.: Handbook of the Poisson Distribution (1967), p. 103.

[160] Reichart, G.: Diss., Zuverlässigkeit beim Führen von Kraftfahrzeugen (2001), p. 20. Herz, R. et al.: Angewandte Statistik (1992), p. 75ff.

[161] Mittag, H.-J.: Statistik: Eine Einführung mit interaktiven Elementen (2014), p. 161 ff.

as a Dirac impulse $\delta(d)$. However, this is described as a Bernoulli experiment by equation (3-1) with the indicator variable X_i

$$X_i = \begin{cases} 1 & \text{if } x_1 \quad = \quad \text{event} \\ 0 & \text{if } x_0 \quad = \quad \text{no event.} \end{cases} \tag{3-1}$$

If the Bernoulli experiment is repeated n times for either the same or another traffic participant $i = [1,2, \dots, n]$, a count variable X can be written as

$$X = \sum_{i=1}^{n} X_i. \tag{3-2}$$

In equation (3-2) X_i are n independent indicator variables with the expected value

$$E(X_i) = p \tag{3-3}$$

and the variance

$$V(X_i) = p \cdot (1 - p). \tag{3-4}$$

This expected value equation (3-3) describes the probability that an event occurs during one observation. The variance for a Bernoulli experiment is just defined by equation (3-4).

Binomial distribution

The distribution of X is called Binomial distribution. The expected value $E(X)$ and the variance $V(X)$ of the Binomial distribution are

$$E(X) = \mu = n \cdot p \tag{3-5}$$

$$V(X) = \sigma^2 = n \cdot p \cdot (1 - p). \tag{3-6}$$

Up to this point, basics of statistic were described. The variables n and p will now be used to again connect the statistical theory of Binomial distributions to road events. When testing a vehicle for a distance of d_{test}, defined in km, this would lead to

$$n = \frac{d_{\text{test}}}{\Delta d} \tag{3-7}$$

observations. To get the characteristic values describing the above defined distributions, the probability p for one of the outcomes $[x_0, x_1]$ needs to be defined. The probability $p(x_1)$ for an event within this small part of real driving is estimated by the numbers of existing event statistics. When k_{a} is the number of events that are recorded during one year a and n_{a} is the number of parts that have been observed during the same year or time span in general, the probability is calculated by

$$p(x_1) = \frac{k_\mathrm{a}}{n_\mathrm{a}}. \tag{3-8}$$

The number of parts that have been observed can be calculated by the distance traveled by all relevant road participants during this year and the defined Δd by

$$n_\mathrm{a} = \frac{d_\mathrm{a}}{\Delta d}. \tag{3-9}$$

Based on equations (3-8) and (3-9), we define the reference safety performance of the object under observation or test SP by:

$$SP = \frac{1 \cdot \Delta d}{p(x_1)}. \tag{3-10}$$

This performance describes the average distance that can be traveled based on the probability $p(x_1)$ until one event ($k = 1$) happens. The performance is synonymous with the average distance between two events for the related observation time span. With the two equations (3-7) and (3-10) describing the Bernoulli experiment, the expected value (3-5) and the variance (3-6) of the Binomial distribution can be calculated:

$$E(X) = n \cdot p = \frac{d_\mathrm{test}}{SP} \tag{3-11}$$

$$V(X) = \frac{d_\mathrm{test}}{SP}\left(1 - \frac{\Delta d}{SP}\right). \tag{3-12}$$

As a discrete random variable is not just defined by its $E(X)$ and $V(X)$, the probability distribution function of X is necessary to be defined. This function can be derived by looking back to the Bernoulli experiment. The probability to experience k times x_0 before experiencing $(n-k)$ times x_1 is a special Bernoulli series $[x_0, \dots, x_0, x_1, \dots, x_1]$. Due to the independence of the experiments, the probability results in $p^k(1-p)^{n-k}$ (see Mittag[161]). But as the order of the series is unimportant for the result of the sum (3-2), there exist $\binom{n}{k}$ other series that lead to the same result. Therefore, the probability function $P(X = k)$ for the Binomial distribution is defined by

$$P(k) = \begin{cases} \binom{n}{k} p^k (1-p)^{n-k} & \text{for } k = 0,1,\dots,n \\ 0 & \text{for all other } k \end{cases}. \tag{3-13}$$

The cumulative distribution function $F(k)$ is defined by the sum

$$F(k) = \sum_{m=0}^{k} \binom{n}{m} p^m (1-p)^{n-m}. \tag{3-14}$$

Poisson distribution

As accidents are extremely rare events, rare[162] in the sense of the Binomial distribution with the probability $p \ll 0.05$ and the number of observations $n \gg 30$, the Binomial distribution can be approximated by the Poisson distribution

$$B_{n,p} \approx P_\lambda \tag{3-15}$$

$$P_\lambda(X = k) = \begin{cases} \frac{\lambda^k}{k!} \mathrm{e}^{-\lambda} & k \in \{0,1,\dots\}. \\ 0 & \text{for all other} \end{cases} \tag{3-16}$$

For the approximation[163] based on $p \to 0, n \to \infty, n \cdot p = \text{const.}$, equations (3-5) and (3-6) lead to

$$E(X) = V(X) = n \cdot p = \lambda = \frac{d_{\text{test}}}{SP}. \tag{3-17}$$

Figure 22 illustrates an example of the approximation. In the four subplots, $n \cdot p$ is kept constant whereas the number of trials n is increased and the probability p is reduced. It can be seen that the PDF's (Probability Distribution Function) are merging while n increases.

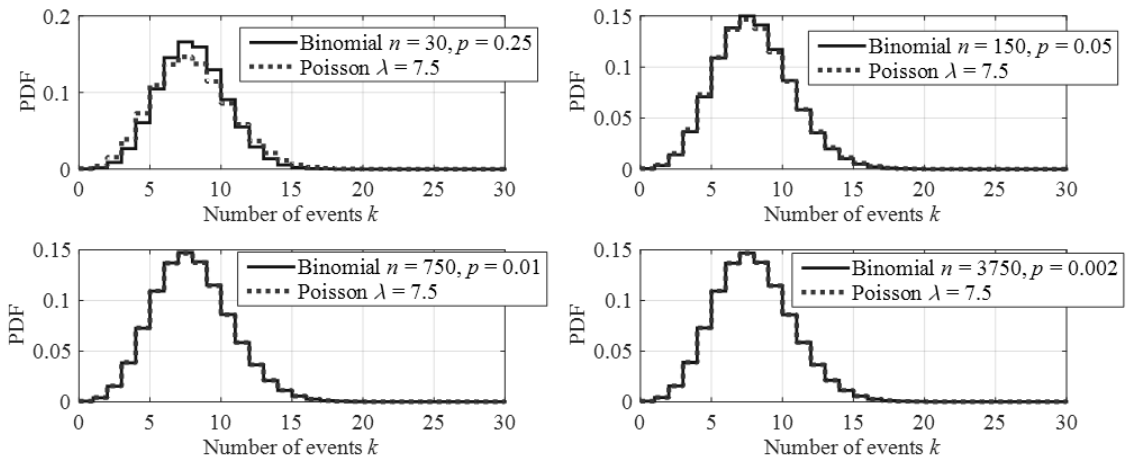


Figure 22 Comparison of Binomial- and Poisson-Probability Distribution Functions for highlighting the approximation

Although the Poisson distribution was derived as an approximation of the Binomial distribution, the necessary assumptions for using the Poisson distribution are discussed in the following. For example, Fahrmeir et al.[164] state:

[162] Accord. to Fahrmeir, L. et al.: Statistik (2007), p. 574.

[163] Fahrmeir, L. et al.: Statistik (2007), p. 262.

Two events cannot occur simultaneously.

The probability that an event takes place during the small time interval Δt is approximately $\lambda \Delta t$. If Δt is small enough the probability is small as well.

The probability for occurrence of a certain number of events during a time interval depends only on the length l but not on its absolute place on the time scale.

The numbers of events of two disjunctive time intervals are independent.

Let's discuss what that means for the assumption that numbers of accidents follow a Poisson process. Fahrmeir's requirements are based on the time domain. The requirements are transformed to the spatial domain assuming an average speed $\frac{\Delta d}{\Delta t}$. This average speed depends on the use case that is examined and thus will vary. Nevertheless, both approaches (time and spatial domain) can be used to discuss the occurrence of accidents. For illustration reasons, this thesis examines the spatial domain, meaning accident rates referring to distance as exposure:

- Can two accidents occur simultaneously? Examining one vehicle, only one accident can happen at one place. This results as it is unimportant if a collision with one or two or more obstacles is the cause for a damage/injury. The worst outcome "counts". When examining more than one vehicle, these other vehicles also had to travel a certain distance to "reach" the accident. When "drawing" the driven distances of all examined vehicles on a virtual line (see Figure 23) and marking the accidents on that line, these accidents will not happen at the same observation interval, thus not simultaneously.

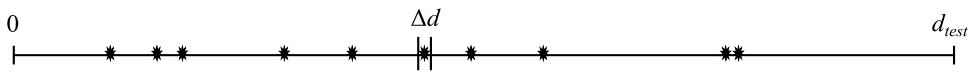


Figure 23 Driven distances lined up and accidents marked

- When the examined distance decreases, does the probability for an accident become small? Before answering this question, the word small needs to be defined. Like stated above[162], "small" in the sense of Poisson means smaller than 0.05. As automated driving will be compared in some way with human driven vehicles, the probability of occurrence of an event should be orders of magnitude smaller than 5 % per meter. Consequently, the probability for an accident can be assumed as small.
- Does the probability for occurrence of a certain number of accidents only depend on the examined distance and not on the absolute position? This cannot be stated without limitations. In road traffic, there exist temporal and spatial accident hot spots. On one hand, it does not change the general validity of Poisson statistics be-

[164] (translated from German) Fahrmeir, L. et al.: Statistik (2007), p. 262.

cause the total number of events can be seen as a sum of sub Poisson processes with different properties. On the other hand, the travel distance that is taken under consideration needs to be representative covering these spatial and temporal specialties. That means that exactly this question raises the requirements for tests and latter introduction. The test distance should not only be representative to the usage kilometer. To fulfill Poisson process requirements, elements of the total distance should be representative to each other.

- Are the numbers of accidents independent from each other when looking at two different intervals? This question cannot be answered globally for AD. What is assumed for the thesis is that every road participant drives as "good" as he or she or it is able to. When this is the case, the individual numbers may change but do not depend on each other and equal out the changes. Especially for AD, this question connects with the question whether an AD learns, thus is adaptable or not. Because then one accident might reduce the chance for the next one and so on. For the first introduction, it is assumed that AD3+ does not change over time[165]. Additionally, it is assumed that there is a process that generates rare events that will never "run empty".

Whether the four requirements to apply the Poisson distribution on accident numbers are completely fulfilled is object of discussion. Nevertheless, the Poisson distribution enables the easiest and thus first approach to describe the uncertainty of accident counts. Other stochastic processes for discrete events base on at least one parameter or more. The problem with applying these other stochastic processes before observing AD3+ in real traffic is not knowing their parameters. The next section sums up how the Poisson process is used in literature.

3.2.2 Literature on the use of the Poisson distribution for accident counts

History

The Poisson assumption has a long history in accident research[166]. As Hauer[166] assumes, the first use of the Poisson distribution to model accident numbers was done by von Bortkiewitcz in 1898. Hauer[166] writes:

[165] Wachenfeld, W.; Winner, H.: Do Autonomous Vehicles Learn? (2016).

[166] Haight, F. A.: Handbook of the Poisson Distribution (1967)., Gerlough, D. L.; Schuhl, A.: Use of Poisson Distribution in Highway Traffic (1955)., Lee, J.; Mannering, F.: Impact of roadside features on accidents (2002)., Chin, H. C.; Quddus, M. A.: Random effect negative binomial model to examine traffic accident (2003)., Hauer, E.: Regression Modeling in Road Safety (2015), p. 205.

[von Bortkiewitcz[167]] had data about the number of deaths by horse-kick in ten Prussian army corps over 20 *years. When comparing the number of years with* $0, 1, \cdots, 5$ *deaths to the number predicted by the Poisson distribution the fit was remarkably good.*

The Poisson Theorem for Accident Counts[168]

A good starting point for a discussion on the basic concepts of road accident statistics is the work by Poisson (Elvik[169]; Feller[170]), who investigated the properties of binomial (Bernoulli) trials, i.e. trials with two possible outcomes: success or failure.

Modern versions of this standard theorem (in many textbooks f.i. Feller[170]; Shorack[171]) do not require the probability of each trial to be the same, and state that under reasonable conditions the probability distribution of the sum S_n *of all successful trials would tend to a Poisson probability distribution. Feller[172] concludes 'We conclude that for large n and moderate values of* $\lambda = p_1 + p_2 + \cdots + p_n$ *the distribution of* S_n *can be approximated by a Poisson distribution.' The following remarks in the context of road safety research should also be taken into account:*

The trials should be considered as situations that may result in one accident.

The results indicated above mean that the number of accidents will be approximately Poisson distributed given the number of trails n and their nature reflected in the values $p_1, \ldots, p_n$*. This is detailed information on exposure.*

This result is relevant to the distribution of the number of accidents, not the number of victims or other outcomes of accidents (except being an accident).

It is assumed that the outcomes of the events are independent. It may be a good idea to further research this aspect.

Only registered accidents exceeding a certain level of severity are usually considered. This would yield that the relevant p-value would be: 'a small probability of resulting in an accident with a certain severity and being registered'.

---

[167] Bortkiewicz, L. von: Das Gesetz der kleinen Zahlen (1898).

[168] This whole subchapter (one page) is taken from Papadimitriou, E. et al.: Safety performance assessment in Europe (2013), p. 372.

[169] Elvik, R.: Traffic safety (2004).

[170] Feller, W.: An introduction to probability theory (1968).

[171] Shorack, G. R.: Probability for statisticians (2000).

[172] Feller, W.: An introduction to probability theory (1968), p. 282.

The registration system cannot be saturated by the accident process (e.g. limited police resource allocation to less severe accidents would have an effect on the applicability of the theorem above).

Note that although these results suggests that the number of accidents should be distributed according to a Poisson distribution, in practice, the distribution of accident counts will never be exactly according to a Poisson distribution, if only due to the limited number of trials on which it is based. If a count is based on a high number of trials (e.g. annual national counts), it is likely that for all practical purposes the count follows a Poisson distribution. However, care must be taken when the actual number of trials is rather low (Lord et al.[173]).

In practice, variants of the Poisson distribution are commonly used in the analysis of road safety count data, see for instance Lord et al.[173] and the references therein.

Other Disciplines using the Poisson distribution

The Poisson distribution in general was introduced[174] by Simone Denis Poisson in 1837. Since then it is used in different disciplines for explaining, prediction, and studying the occurrence of different events. To get an idea of the different application disciplines, a list of applications from Haights[175] and Letkowski[176] is given:

The number of mutations on a given strand of DNA per time unit

The number of bankruptcies that are filed in a month

The number of arrivals at a car wash in one hour

The number of network failures per day

For reliability analysis in general the instants of breakdown

The distribution of plants and animals in space or time

The sampling of bacteria per square

The number of defected teeth per individual

The number of victims of specific diseases

The number of cars passing a point in a fixed time interval

The physical aspects of particle counting

---

[173] Lord, D. et al.: Regression models of motor vehicle crashes (2005), p. 36 ff.

[174] Haight, F. A.: Handbook of the Poisson Distribution (1967), p. 113.

[175] Haight, F. A.: Handbook of the Poisson Distribution (1967), p. 100–107.

[176] Letkowski, J.: Developing Poisson probability distribution applications (2014), p. 3.

Of special interest for discussing the usage of AD3+ is the identification of individual humans that are more or less safe compared to other human drivers. An idea would be to replace those by automated vehicles that reduce the safety in road traffic most. However, based on the Poisson distribution, Drösler[177] and Gründl[178] argue that a selection of individuals being bad drivers is not possible. The reason for that is the same that leads to the "Approval-Trap". There will not be enough distance one person could drive in his lifetime to prove he or she is a bad driver (given the fact, that the person is allowed to keep its driver license). This is different when looking for groups of people that might result in lower road safety values. In average, different SP level can be defined given a certain age, experience, or other characteristics[179]. Thus, the question might arise: "Why should these not be driven by an automated vehicle?" A quick answer would have been: "Because the automated vehicle is less safe than this group of people." Can lower safety of AD3+ be shown? At this point, the next scientific question needs to be answered by applying the Poisson distribution: "Is the automated vehicle less safe than the worse group of people?"

3.3 Falsifying the Safety Hypothesis

Q15 If we cannot prove safety, is automated driving unsafe then?

As presented in chapter 2, today's literature[180] concludes that the scientific statistical proof of safety of automated vehicles is economically not feasible before the mass introduction of automated vehicles. These conclusions are made on the Poisson distribution explained before. If an economic benefit is aimed for, hundreds of millions or even billions of miles spent on testing in real traffic do not seem appropriate. Additionally, it was shown that alternative testing approaches also lack knowledge for application. Does it then mean we should stop developing and never introduce automated driving?

No, because the nature of the statistical proof of safety is the attempt to reduce the uncertainty. When we want to prove safety, we raise the requirements to a level of significance. By raising the requirements, we also increase the chance to reject a safe system. When counting for example two events ($k = 2$) during an observed test (d_{test}), the statement on proven safety depends on the required level of significance. Using an

[177] Drösler, J.: Zur Methodik der Verkehrspsychologie (1965), p. 258 ff.

[178] Gründl, M.: Diss., Fehlverhalten als Ursache von Verkehrsunfällen (2005), p. 15–19.

[179] Maycock, G.; Lockwood, C. R.: The accident liability of British car drivers (1993).

[180] Winner, H.: Quo vadis, FAS? (2015)., Wachenfeld, W.; Winner, H.: The Release of Autonomous Vehicles (2016), p. 446–447., Becker, J.: Toward Fully Automated Driving (2014), p. 16., Kalra, N.; Paddock, S. M.: Driving to Safety: How Many Miles? (2016).

error probability $e = 1\ \%$, a distance factor of $a_d \gtrsim 8.4$ is necessary for proving safety ($k = 2$). Whereas using $e = 50\ \%$, a distance factor of only $a_d \gtrsim 2.67$ results as being necessary to prove safety[181]. Both are statistically right, although the second has the same meaningfulness as guessing whether the vehicle is as safe as the reference or not. However, using the first level of significance, there is a good chance to reject the safe automated vehicle by mistake. Figure 24 illustrates how the necessary distance factor for the proof of being safer depends on the probability of error e.

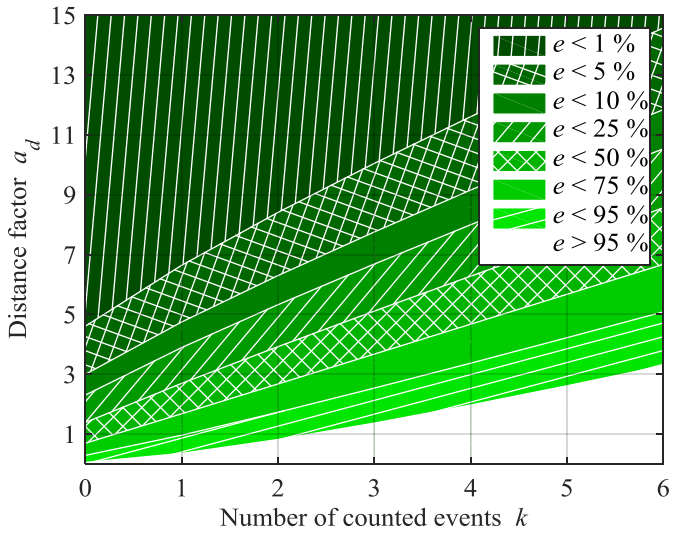


Figure 24 Distance factor a_d as a function of the probability of error e and the number of counted events k for the proof of being better than SP_{bench}

Consequently, the research question needs to be extended to study the falsification. We should not only ask "When have we proven safety?" but we should also ask "When have we proven the automated vehicle to be *unsafe*?". As the proof of being less safe can be answered based on the same theory as the question on the proof of more safety has been answered, this theory will shortly be recapitulated[182]. To represent the distribution of accident events, we apply the Poisson distribution[183] from equation (2-1):

$$P_\lambda(k) = \frac{\lambda^k}{k!} \mathrm{e}^{-\lambda}$$

This distribution assumes that the occurrence of an event is an independent and non-exhaustive random process $P_\lambda(k)$. In the equation, k corresponds to the number of

[181] Usually an error probability of $e < 10\%$ is used.

[182] This short explanation is mainly taken from Wachenfeld, W.; Winner, H.: The new role of road testing. (2016)..

[183] Nicholson, A.; Wong, Y.-D.: Are accidents poisson distributed? (1993).; Gründl, M.: Diss., Fehlverhalten als Ursache von Verkehrsunfällen (2005).

events and λ to the expected value with which events occur. The expected value λ is defined by the quotient like equation (2-2) formalizes

$$\lambda = \frac{d_{\text{test}}}{SP}$$

whereby d_{test} stands for the observed test distance and SP for the safety performance of the system. The performance represents the expected number of kilometers between two events of the same kind. It is assumed that a certain number of kilometers d_{test} were driven and a number of events k_{count} occurred. Can we now define a worse and a better performance level SP from this test? Equations (2-1) and (2-2) connect this with the search of an expected value λ. Based on a probability of error value[184] e_{proof} that is the same for both proofs $e_+ = e_- = e_{\text{proof}}$, the questions can be mathematically formulated with two equations. Section 2.4.2 already discusses equation (2-3)

$$P_{\lambda_+}(k \leq k_{\text{count}}) \leq e_+.$$

This equation asks for which λ_+ the probability that k_{count} or less events happened is at most e_+. In this case, a numerical search[185] for equation (2-4) provides the value λ_+. This says that when k_{count} events occur after a distance of d_{test} it is statistically proven with a probability of e_+ that the vehicle is *better* in terms of safety compared to a performance level of $SP = \frac{d_{\text{test}}}{\lambda_+}$. To prove that the OuT is better than the benchmark (SP_{bench}), the test d_{test} has to cover a multiple (a_d) of the distance that lies between two events $d_{\text{test}} = a_{\text{d}} \cdot SP_{\text{bench}}$ for the benchmark. Thus $a_d = \lambda_+$.

What has not yet been discussed is the proof of being unsafe expressed by equation (3-18)

$$P_{\lambda_-}(k \geq k_{\text{count}}) \leq e_- \,. \tag{3-18}$$

For which expected number λ_- is the probability to have at least k_{count} events counted less than or equal to e_-? A function $\lambda_-(k_{\text{count}}, e)$ is defined as the maximum solution of the numerical search for

$$P_{\lambda_-}(k \geq k_{\text{count}}) = 1 - \sum_{0}^{k_{\text{count}}-1} \frac{\lambda_-^{\text{k}}}{k!} \mathrm{e}^{-\lambda_-} = 1 - P_{\lambda_-}(k \leq k_{\text{count}} - 1) = e \tag{3-19}$$

Exemplary results for the determining expected value λ_- are found in tables in appendix A. This says that when k_{count} events occur after a distance d_{test}, it is statistically prov-

[184] The value (5 %, 1 %, 0.1 % etc.) that is taken needs further considerations but is just one variable in that theory.

[185] Tabular values or approximations exist but aren't necessary as the numerical search is easely performed in any calculation tool like Excel™ or Matlab™ for example.

en with error probability e_- that the vehicle is *worse* in terms of safety compared to a performance level of $SP = \frac{d_{\text{test}}}{\lambda_-}$.

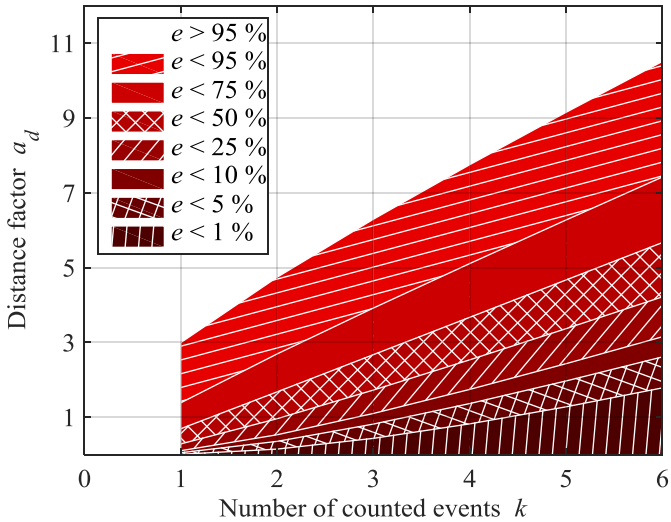


Figure 25 Distance factor a_d as a function of the probability of error e_{proof} and number of counted events k for the proof of being worse than SP_{bench}.

Figure 25 depicts this connection between error probability, number of counted events, and the distance factor. When for example two events occurred ($k_{\text{count}} = 2$), one can conclude that the vehicle is less safe than SP_{bench} if the distance tested is smaller than $a_d \lesssim 0.15$ times the reference on an error probability $e_{\text{proof}} = 1\ \%$. If $a_d \lesssim 1.68$ times the reference, the proof is given for an error probability $e_{\text{proof}} = 50\ \%$. It makes sense that the areas flipped around from Figure 24 to Figure 25 as for proving higher safety we need less distance when reducing the level of significance and for proving less safety the other way around. Notice that at least one accident needs to be counted before one can state that the system is worse than anything else. That is the reason why the plot in Figure 25 starts at $k = 1$. Figure 24 can be converted into Figure 25 by shifting the values for one event and calculating $e_- = 1 - e_+$.

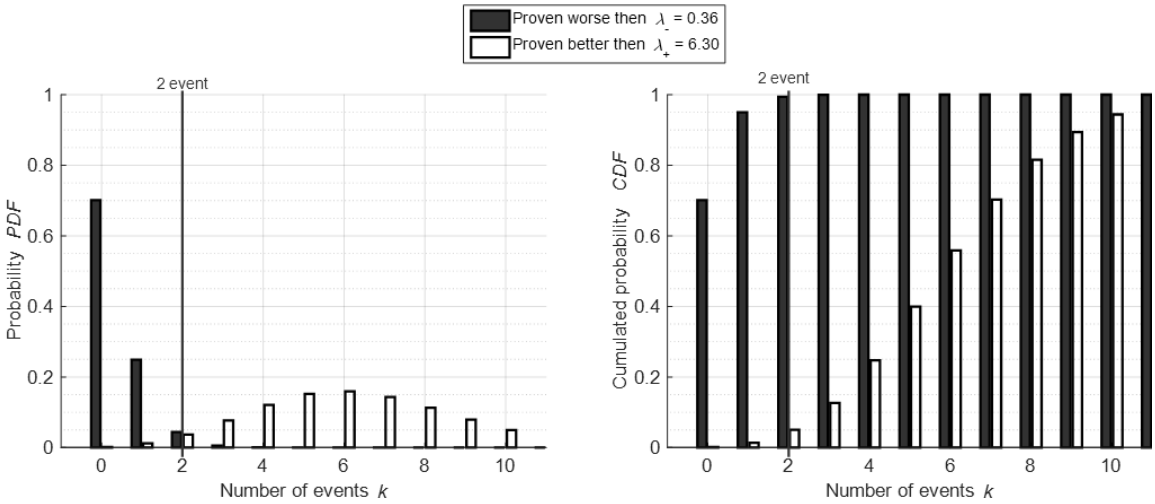


Figure 26 PDF and CDF for an example of $k_{\text{count}} = 2$ and $e_{\text{proof}} = 5\%$

For better understanding of the difference between equations (2-3) and (3-18), Figure 26 illustrates an example. For $k_{\text{count}} = 2$ and $e = 5\ \%$, the resulting PDF and CDF plots are presented, the light-open bars for the proven being better λ_+ and the dark-closed bars for the proven being worse λ_-.

Consequently, there exists an interval of uncertainty in-between proving safety and proving less safety. Let's assume that the performance level for the benchmark is $SP = SP_{\text{bench}}$. So after a distance of SP_{bench}, one of the relevant events should happen in statistical average. Now we want to introduce the OuT after it was tested for distance

$$d_{\text{test}} = a_d \cdot SP_{\text{bench}} \tag{3-20}$$

and k_{count} events occurred. The necessary distance factor a_d describes the ratio between the test distance and the benchmark. From equation (3-18), it is known that the performance level of the OuT SP_{OuT} is equal or worse

$$SP_{\text{OuT}} \leq \frac{d_{\text{test}}}{\lambda_-}. \tag{3-21}$$

Combining both equation (3-20) and (3-21), the performance level of the OuT is

$$SP_{\text{OuT}} \leq \frac{a_d \cdot SP_{\text{bench}}}{\lambda_-}. \tag{3-22}$$

Equation (3-22) tells us that the OuT is worse than $\frac{a_d}{\lambda_-}$ times the benchmark. On the other hand, it only says that the vehicle is better than

$$SP_{\text{OuT}} \geq \frac{a_d \cdot SP_{\text{bench}}}{\lambda_+}. \tag{3-23}$$

With this test it cannot be proven that the OuT is less safe than $\frac{a_d}{\lambda_-}$ times the benchmark, and on the other hand it is only proven that the OuT is safer than a $\frac{a_d}{\lambda_+}$ times worse system

$$\frac{a_d \cdot SP_{\text{bench}}}{\lambda_+} \leq SP_{\text{OuT}} \leq \frac{a_d \cdot SP_{\text{bench}}}{\lambda_-}. \tag{3-24}$$

To illustrate how either the number of events or the testing distance needs to change to come to a statement, both Figure 24 and Figure 25 can be combined in Figure 27.

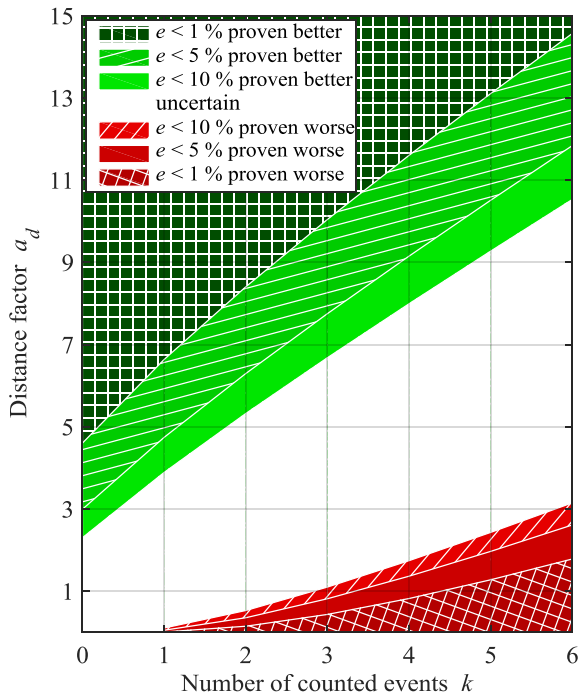


Figure 27 Distance factor a_d as a function of the probability of error e and number of counted events k for comparison of proving better or worse.

For the proof of being safer, the "Approval-Trap" explains why for economic reasons we will stay ahead of introduction in the white area of Figure 27. The same will result for the proof of less safety assuming an SP_{OuT} being comparable with today's benchmark. If we can't prove it is less safe than the benchmark: Why should this system not be introduced into traffic? If we just know that it is safer than a $\frac{a_d}{\lambda_+}$-times worse system: Why should we take the risk to introduce the system?

These questions will only be answered when the different positions of the affected parties, as described in section 1.3 "Societal Risk Constellation", are discussed. The party that is affected negatively would argue: "Safety has not been proven, thus do not expose us to that risk and prevent the introduction of the vehicle!" The party that profits

from the technology would argue: “No one has proven less safety, thus do not withhold us from the benefits and introduce the vehicle!”

On the one hand, the user is the one that will profit in first place. Thus, the question is: Will users tolerate a technology that is not safety proven and use it as long as no one has proven less safety? On the other hand, the bystanders would be the first that are mostly negatively affected. Is there a way these bystanders, called society, could be convinced to accept the uncertainty of the not yet been given proof of safety?

It has been shown that the proof of safety is economically not possible up to the point of mass introduction but the proof of *less* safety is also pending. Obviously, it is necessary to refine the requirement. The next section will elaborate on the idea to split and refine the requirements depending on the affected parties.

3.4 Requirements Refinement

Q16 Which safety level do humans require before using automated vehicles?

Q17 Which safety level does society require to tolerate the use of automated vehicles?

Two sources of requirements have been identified on the safety assessment of AD3+. On the one hand, the individual of society, as the disadvantaged person, could ask for the proof of higher safety compared to today’s vehicles. On the other hand, the users, as the beneficiaries of automated driving, could ask for the proof of less safety if someone wants to prohibit the introduction of automated driving.

Unfortunately, none of both attempts, taking a statistical proof under consideration, will succeed. The economics constraints together with an assumed level of safety will avoid the verification of any of both requirements before the mass introduction.

Consequently, when both requirements can’t be fulfilled, the requirements need to be refined to make them verifiable. Therefore, this chapter will propose the so-called “safety detector”, firstly for the users’ perspective and secondly for the society’s perspective. Be aware that neither this thesis nor respective research activities can define requirements which society and users would accept offhandedly[186]. Nevertheless, my understanding is to concretize, formalize, and propose refined requirements as this seems necessary for a successive constructive follow up discussion.

[186] A more detailed discussion on the subjective versus objective persception of risks can be found in Fritzsche, A. F.: Wie sicher leben wir? (1986).

3.4.1 Users' "Safety Detector"

Freewill is the gateway to discuss the users' requirement on safety. Fritzsche[187] discusses the difference of acceptable and inacceptable individual fatality risks reported in literature, illustrated in Figure 28. Among other topics, Fritzsche highlights that those humans taking risks voluntarily may accept risk levels they would never accept for work or, in general, involuntarily.

Users of automated vehicles can be seen as taking these risks resulting from usage on free will. Consequently, the requirement from users on the safety of automated vehicles depends on her or his individual weighting. The requirement on safety assessment from a user's perspective is concluded to be the need for transparency that he or she is able to weight responsibly. Objective numbers are necessary for the user to come up with a subjective conclusion.

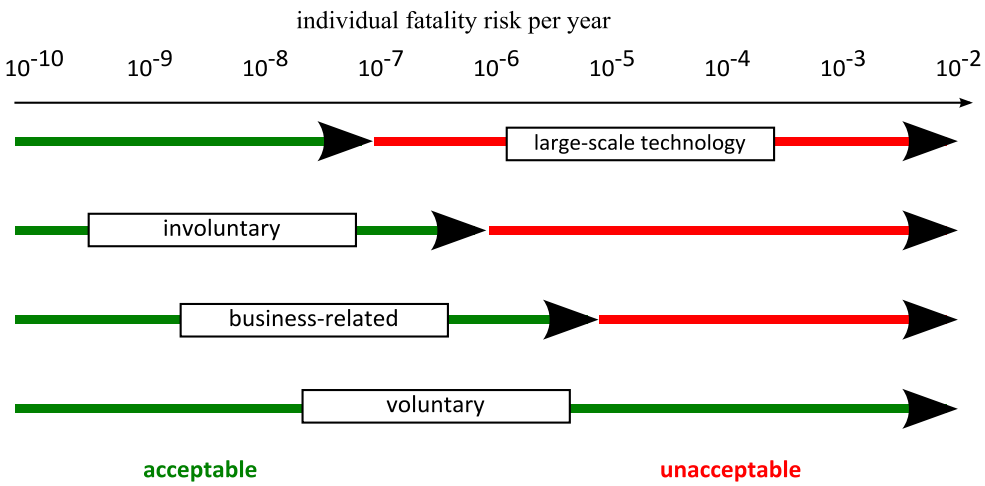


Figure 28 Properties affecting the acceptable individual fatality risk (translated) [187]

Two exemplary objective numbers are stated:

- The safety performance level estimation in best- and worst-case. This follows from equation (3-24). After testing the vehicle, the values for $\lambda_-, \lambda_+, a_d$ are known and SP_{bench} is derived from given statistics, thus the best- and worst-case can be calculated

$$SP_{\text{OuT,worst}} \leq SP_{\text{OuT}} \leq SP_{\text{OuT,best}}. \tag{3-25}$$

  As already discussed, this number has an additional "degree of freedom": the probability of error e_{proof}.

[187] Steininger, U.; Wech, L.: Wie sicher ist sicher genug? (2013). Condensed information from Fritzsche, A. F.: Wie sicher leben wir? (1986).

To avoid this number as a degree of freedom, another error probability can be used as the objective number itself (see next).

- A less intuitive but also expressive number is the error probability estimation e_{PbB} for the proof of being safer as a benchmark. This follows equation (2-3). After testing the vehicle, the values for k_{count} are known and λ_{bench} is derived from given statistics and the distance driven expressed by the distance factor a_d

$$P_{\lambda_{\mathrm{bench}}}(k \leq k_{\mathrm{count}}) = e_{\mathrm{PbB}}. \tag{3-26}$$

  Additionally, the error probability estimation e_{PwB} for the proof of being less safe as a reference can be given by adapting equation (3-18)

$$P_{\lambda_{\mathrm{bench}}}(k \geq k_{\mathrm{count}}) = e_{\mathrm{PwB}}. \tag{3-27}$$

  The only degree of freedom with equations (3-26) and (3-27) is the benchmark that is used for deriving λ_{bench}. Different benchmarks can be used as long as their risk can be expressed on the same scale as the OuT risk. Take for example the safety performance SP using a motorbike.

Obviously, by changing the requirements from proving safety to producing transparency, the users' role in safety assessment of automated vehicles has changed. The users are not anymore treated as one homogeneous group, but rather as many individuals. Each of the individuals has to weight, based on objective information, whether it wants to use the automated vehicle or not.

The stricter requirement on the safety assessment of automated vehicles sensibly results from the disadvantaged persons (the society) and will be explained in the next section.

3.4.2 Society's "Safety Detector"

It is assumed that society will not be satisfied with transparency for the assessment process if the safety outcome of automated driving could lower safety. This is related to the benefit and drawback share for society. Road traffic participants are only hardly able to avoid automated vehicles in total. That is one of the big differences compared to the user of the vehicles. It is an involuntary change in their risk constellation. Thus, it seems necessary to prove that by the introduction of automated vehicles the safety outcome of road traffic for society or the individual of the society will not change or only change in an acceptable manner. Therefore, we will first lay out some theoretical thoughts on the safety detector for the society and secondly derive one exemplary detector.

Theoretical Thoughts

Hauer states on the problem of road safety[188]:

> *Thus, in the context of heavy-truck safety, the question does not seem to be whether some kind of truck is over-represented, nor whether the accident rate of one type is larger than that of another type. Any interest which we might have in characteristic accident rates will derive from questions such as: 'what will be the change in the number and severity of accidents if the use of a certain kind or size of vehicle is allowed?'*

As explained in section 1.4.1, the social as well as the individual safety for society depend on the absolute number of injuries I_{a}. If it is not possible to prove safety using the safety performance SP-dimension of the three-dimensional road safety problem (see again Figure 12), another dimension has to be addressed to come to a proof of safety for society. This could either be the exposure expressed by the distance driven d or the ratio of injuries per accident IpA.

On the one hand, without reducing the velocity (kinetic energy) of the OuT in comparison to the benchmark use case, it seems impossible to reduce the injury per accident rate significantly. And even then the IpA_{F} can only reduce to 1, thus only offers a minimal improvement potential compared to the value derived for 2013 ($IpA_{\mathrm{F}} \approx 1.3$). If the velocity is reduced stronger, it would mostly change the use case and thus the reference. On the other hand, by limiting the distance d_{driven} that is driven with the new technology, thus limiting the exposure of the society, the risk for society can be controlled significantly. Generally spoken this follows the idea of the finding of Paracelsus[189] in chemistry:

> *Alle Dinge sind Gift, und nichts ist ohne Gift; allein die dosis machts, daß ein Ding kein Gift sei.*

Translated[190]:

> *All things are poisonous and nothing is without poison; only the dose makes a thing not poisonous.*

The question to answer for road traffic safety is: What is the acceptable dose of AD3+ vehicles within today's road traffic? If $d_{\mathrm{AD2-,a}}$ is the distance driven of vehicles with lower levels of automation and $d_{\mathrm{AD3+,a}}$ the distance of AD3+ vehicles in automated

[188] Hauer, E.: On exposure and accident rate (1995).

[189] Paracelsus, T.: Septem Defensiones (1538), p. 73.

[190] Ottoboni, M. A.: The dose makes the poison (1991).

mode, the question is expressed by the right size of the value for $d_{\mathrm{AD3+,a}}$. If assuming an unchanged injury per accident ratio

$$IpA = \text{const.} \tag{3-28}$$

as well as an unchanged total number of distance driven by all vehicles together

$$d_{\mathrm{AD2-,a}} + d_{\mathrm{AD3+,a}} = d_{\mathrm{all,a}} = \text{const.} \tag{3-29}$$

the question on road traffic safety narrows down to the change in numbers of accidents due to $d_{\mathrm{AD3+,a}}$. The discussion is obvious for the Vision Zero example. If no accidents occur, the highest safety for society has been reached in road traffic. But if the number of accidents with fatalities or other severity classes isn't zero, the question is what number expresses no or positive change in road safety for society. An obvious conclusion is that the lower the accident number with respect to severity is, the higher the safety for society[191]. When checking the time series of accident numbers for a traffic system with defined boundaries, you will not find monotonic figures. Accordingly, also higher numbers within a limited range are tolerated by society as long as a trend leads higher or equal safety. Some kind of noise that is influenced by surrounding factors and not only by the skills of the single driven vehicle changes the accident numbers. Consequently, higher accident numbers cannot directly be linked with less safe single vehicles. For this reason, the society's safety detector has a detector limit. This detector limit represents the lowest change in numbers which can be interpreted as higher, lower, or no change in safety.

Thus, society's requirement is defined: "as long as safety has not been proven by the safety performance SP, a proof has to be given that the expected accident numbers will stay below a tolerated limit for society's safety".

One exemplary Detector

A detector limit is deduced based on the example in Figure 29. Each year, a discrete number of events was recorded. Over the years, the number decreased following a certain monotonic trend. This trend is not given but can be fitted by, for example, a least square approximation of a suitable mathematical function like a linear function[192] f_{fit}.

[191] For these conclusions and theory, the system boarders of evaluation do not change. Germany is an example where this has to be taken into account as accident numbers cover after the reunification also the numbers of the former German Democratic Republic (GDR/DDR).

[192] $k = -30.1 \cdot i + 996$

Other ways of time-series analysis may be applied like discussed in Bergel-Hayat and Zukowska[193].

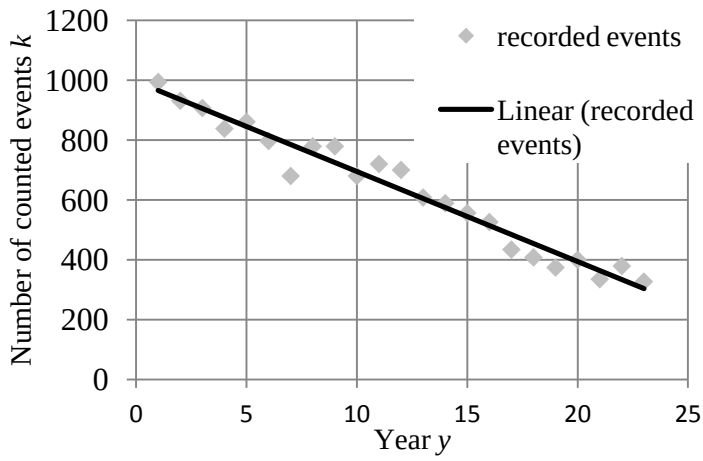


Figure 29: Number of events recorded for 23 years and fitted by a linear equation

As a simplification, the fitting is done for this example by the (red/solid) line (see Figure 29). All points differ from the trend line. These deviations are still independent from the technology we want to introduce. This fact leads to the question: How does the next number of recorded events has to differ from the values in the past, fitted by the trend line, to be sure that it was affected negatively?

To propose one answer, the standard deviation of these events compared to the trend line is derived

$$\sigma = \sqrt{\frac{1}{N_y}\sum_{y=y_1}^{y_{\text{end}}}(k_y - f_{fit}(y))^2}. \tag{3-30}$$

In this equation, N_y is the number of years and k_y is the number of events recorded in year y. y_1 is the first year of evaluation and y_{end} the last year. We now define that

$$k_{\text{end}+1} \leq f_{fit}(y_{\text{end}} + 1) + k_{\text{detL}} \tag{3-31}$$

is indistinguishable from the trend line for society. $k_{\text{detL}} = \frac{\sigma}{\beta}$ expresses the indistinguishable limit of numbers of events for the safety detector. This change in numbers is β times smaller than the standard deviation and therefore disappears in the noise of numbers each year. There is actually no way to prove or detect that the trend is affected negatively as the number is too small and lies below the limit of detection.

Other approaches exist to define these limits for example for clinical laboratory measurements. The Clinical and Laboratory Standards Institute (CLSI) has published a

[193] Bergel-Hayat, R.; Zukowska, J.: Review of time-series analysis (2015), p. 651–654.

guideline EP17[194] where the Limit of Blank (LoB), Limit of Detection (LoD), and Limit of Quantitation (LoQ) is derived from the Normal distribution. Based on this, Armbruster and Pry specify[195a]:

> *LoB is the highest apparent analyte concentration expected to be found when replicates of a blank sample containing no analyte are tested.*
>
> $$LoB = mean_{blank} + 1.645(\sigma_{blank})$$
>
> *LoD is the lowest analyte concentration likely to be reliably distinguished from the LoB and at which detection is feasible. LoD is determined by utilising both the measured LoB and test replicates of a sample known to contain a low concentration of analyte.*
>
> $$LoD = LoB + 1.645(\sigma_{low\ concentration\ sample})$$
>
> *LoQ is the lowest concentration at which the analyte can not only be reliably detected but at which some predefined goals for bias and imprecision are met. The LoQ may be equivalent to the LoD or it could be at a much higher concentration.*

The number of 1.645 corresponds to 95 % cumulative probability of the Normal distribution[195b]. It should be highlighted that for LoB and LoD also a repetition rate is recommended[195b]:

> *A recommended practical number of LoB and LoD samples to be used by a manufacturer to establish these parameters is 60, while a laboratory verifying a manufacturer's LoD (and possibly the LoB) is 20.*

Accident numbers may change in future, probably due to the introduction and use of automated driving. Consequently, the standard deviation might also be derived as a time variant parameter. Nevertheless, the limit proposed above is seen as a simplified first version that is used in the following.

Coming from two requirements that can economically not be met ahead of introduction, this section 3.4 derived two refined requirements. These proposed requirements reflect the different societal risk constellations of users and society. This analysis led to less ambitious requirements that still could reflect the safety needs of the different affected parties. The next section 3.5 will lay out a strategy that aims to fulfill both requirements derived above. The society's requirement suggests to widen the scope of safety assessment, extending the testing phase, and planning the introduction. That is because the society's safety detector works on numbers for the next year of real-world application. Thus, the following strategy describes the test, introduction, and supervision of automated vehicles based on estimated uncertainties.

---

[194] Pierson-Perry, J. F. et al.: Detection capability for clinical laboratory measurement (2012).

3.5 Uncertainty-Based Usage Strategy

Q18 How can users' and society's safety requirements be fulfilled?

The main goal of this concept is to describe a way how to introduce automated driving *and* fulfill the users' and society's safety requirements.

On top of that it seems reasonable that during usage there will come the point in time at which a statistical proof of safety or less safety is achievable (t_{PoS}). How should then be continued with the introduction of new vehicles, either human or automated driven? It should be noticed that the requirements derived above do not vanish when automated vehicles have been introduced. Consequently, as long as AD3+ are in usage, the requirements should be fulfilled at least from today's perspective.

The three following sections propose an uncertainty-based usage strategy for three phases of the automated vehicle usage. The testing phase Δt_{test}, the introduction phase $\Delta t_{\mathrm{intro}}$, and the supervision phase Δt_{suvi} (see Figure 30). The timeline in Figure 30 depicts different time spans Δt as well as certain points in time t that are important for the understanding of the following explanation. The timeline will thus be used for explanation.

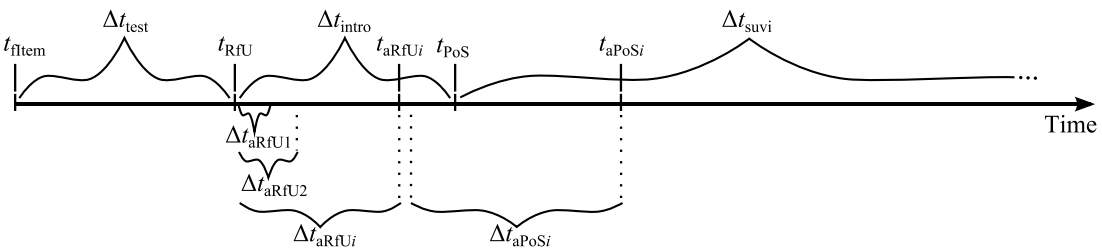


Figure 30 Timeline with crucial points in time t and time spans Δt for the usage theory

After this subsection, in 3.6 "Usage Strategy Examination" certain parameter variations of the usage strategy are examined for the Autobahn Pilot and its safety outcomes.

3.5.1 Testing Phase

For the classical safety lifecycle of the automobile described in the ISO 26262[196], testing is defined as the

> *process of planning, preparing and executing or exercising a system or system component to verify that it satisfies specified requirements, to detect errors, and to create confidence in the system behaviour.*

[195] Armbruster, D. A.; Pry, T.: LoB, LoD, LoQ (2008), p. a:49, b:50.

[196] ISO: DIS 26262: Road vehicles - Functional safety (2008), p. 16 part I.

Testing is part of verification and validation, thus the overall system development. It ends with the release for production. However, from today's perspective the start of production does not need to be the end of development. Examples from Tesla Motors Inc.[197] and others exist that report the activation of software-based functions after the vehicle is already in use by the customer. Due to that reason, the testing phase is defined as the phase starting with the first testable item of the automated vehicle t_{fItem} and ending with the release for usage (RfU→t_{RfU}) instead of the release for production. How this could actually change the safety lifecycle in automotive industry will be discussed in chapter 5. To evaluate the testing phase at t_{RfU}, the concept needs input data.

Concept input during testing phase:

To apply the concept, three steps need to be carried out:

1. Identification of safety benchmark:

The safety benchmark $\boldsymbol{SP}_{\mathrm{bench}}$, describing the distance between two relevant events, needs to be defined. This benchmark is a vector of different severities. Exemplary severities that will also be used in the next sections are accidents with injuries and accidents with fatalities. Conceivable are also near misses, describing a proximity to a real accident. As described in section 1.4 by the accident triangle, different severities need to be studied to come to a statement on safety

$$\boldsymbol{SP}_{\mathrm{bench}} = \begin{bmatrix} SP_{\mathrm{bench,AwI}} \\ \vdots \\ SP_{\mathrm{bench,AwF}} \end{bmatrix}. \tag{3-32}$$

The source for concrete values might be road traffic statistics as described for the Autobahn Pilot in section 3.6 and in general in chapter 4.

2. Collection of test distance:

The object under test (OuT) needs to be tested[198] in a representative way. Representatively covers all behavior effecting elements in a scenario. The vehicle itself should have reached a version that is as close to the series product as possible. The test driver and other passengers should behave representatively. This means that the test driver should be able to supervise and overwrite the vehicle without being recognizable as a driver. Concepts like the "Wizard-of-Oz" vehicle[199] or driving instructor vehicle preparations could be a way to reach this illusion for the surrounding. Besides the passengers and the vehicle itself, a scenario is affected by the surrounding of the vehicle due to its

[197] Tesla Motors Inc.: SOFTWARE RELEASE NOTES v7.1, p. 1.

[198] Schoettle, B.; Sivak, M.: Real-World Crashes Involving Self-Driving Vehicles (2015), p. 18.

[199] Mok, B. K.-J. et al.: Wizard of Oz Design (2015).

sensors and force exchange with the environment. Depending on the use case, the surrounding needs to be met in a representative way by testing the vehicle. This can either be done by defined test cases where representativeness needs to be shown, or by real-world driving. The representativeness of real-world driving can be derived from the use case itself and knowledge about the users' behavior for this use case. The same distance driven can lead to different levels of representativeness, so that the right selection of the travelled routes and environmental conditions plays a key role for this theory. This will be addressed in chapter 4 in more detail.

The amount of representative distance needs to be collected during the testing time span Δt_{test} and is called

$$d_{\text{test},0} = d_{\text{test}}(\Delta t_{\text{test}}). \tag{3-33}$$

The function $d_{\text{test}}(\Delta t)$ leads the distance driven during the time span Δt for which the start t_{startT} and t_{endT} end time can be found in Figure 30

$$d_{\text{test}}(\Delta t) = d(t_{\text{endT}}) - d(t_{\text{startT}}). \tag{3-34}$$

More distance will be driven also after t_{RfU} in the following phases. One of the main questions today is: How many kilometers should be tested before introduction? On that topic exists literature, but that mainly predicts[200] numbers roughly.

Besides these predicted literature values, two other methods are derived theoretically in the following. One method is called the "prevention of less safety" and the other the "monetary balance". How the different test distances affect the usage strategy will be evaluated in section 3.6.

The "prevention of less safety" proposes to drive that many test kilometers that although one new event $(k+1)$ would occur the proof of less safety compared to the benchmark would fail. This is formalized by demanding

$$P_{\lambda\_}(k \geq k_{\text{count}} + 1) \leq e_{\text{proof}} \tag{3-35}$$

and $\lambda(k_{\text{count}} + 1, e_{\text{proof}})$ leads to the values in Table 6. These values are the same as listed in appendix A, Table 15, but shifted by one event.

Table 6 Necessary distance as a factor of $\boldsymbol{SP}_{\text{bench}}$ that is necessary to prevent the proof of less safety by one more event counted ($e_{\text{allow}} = 5\ \%$).

Number of events k_{count}:	0	1	2	3	4	5
Distance factor a_d:	0.051	0.355	0.818	1.37	1.97	2.61

[200] Becker, J.: Toward Fully Automated Driving (2014), p. 16.

Thus, one way to define the test distance before RfU could be

$$d_{\text{test},0} : \geq 0.051 \cdot SP_{\text{bench,AwF}}. \tag{3-36}$$

Table 6 lists further values for $k_{\text{count}} = \{1 \ldots\}$. These values could be used in the case that one event was recorded before the distance factor in column one was reached. If this happened, the proof of less safety would have been given during testing. For a comparable good system, this would be unlikely as has been described above (falsification). Consequently, for further calculations the value from the first column is assumed to apply.

The second method, the "monetary balance", proposes to formalize the benefits of using the technology and set this in ratio with the costs of testing and using the technology. The principle is motivated by the ALARP approach (as low as reasonable practical). A simple relation is proposed for that

$$d_{\text{test}}(\Delta t_{\text{aRfU}i}) bpd_{\text{aRfU}} \geq d_{\text{test},0} cpd_{\text{test}} + d_{\text{test}}(\Delta t_{\text{aRfU}i}) cpd_{\text{aRfU}}. \tag{3-37}$$

In this equation, $d_{\text{test}}(\Delta t_{\text{aRfU}i})$ represents the driven distance after the RfU. The time span $\Delta t_{\text{aRfU}i}$ begins at the release for usage t_{RfU} and covers the time until the i's evaluation after the release for usage $t_{\text{aRfU}i}$. This distance is multiplied once by a benefit factor bpd_{aRfU} and by a cost factor cpd_{aRfU}. The value of driven distance during testing $d_{\text{test},0}$ is added to the inequality and multiplied by a cost factor cpd_{test}. Equation (3-37) summarizes the monetary benefits on the left of the inequality and the costs on the right. No matter when the test distance is driven, in average a certain distance d_{proof} is necessary to reach the statistical proof of safety, thus

$$d_{\text{proof}} = d_{\text{test},0} + d_{\text{test}}(\Delta t_{\text{aRfU}i}). \tag{3-38}$$

Applying equation (3-38) to equation (3-37), we can derive another definition of the distance that should be driven during testing phase

$$d_{\text{test},0} \begin{cases} \geq d_{\text{proof}} \left(\frac{cpd_{\text{aRfU}} - bpd_{\text{aRfU}}}{cpd_{\text{aRfU}} - bpd_{\text{aRfU}} - cpd_{\text{test}}} \right) & \text{if } cpd_{\text{aRfU}} - cpd_{\text{test}} \geq bpd_{\text{aRfU}} \\ < d_{\text{proof}} \left(\frac{cpd_{\text{aRfU}} - bpd_{\text{aRfU}}}{cpd_{\text{aRfU}} - bpd_{\text{aRfU}} - cpd_{\text{test}}} \right) & \text{if } cpd_{\text{aRfU}} - cpd_{\text{test}} < bpd_{\text{aRfU}} \end{cases}. \tag{3-39}$$

Two cases need to be studied (equation (3-39)). As long as $cpd_{\text{aRfU}} - bpd_{\text{aRfU}} - cpd_{\text{test}} \geq 0$, it would be better to test more distance before introduction, thus increase $d_{\text{test},0}$. In the other case $cpd_{\text{aRfU}} - bpd_{\text{aRfU}} - cpd_{\text{test}} < 0$, it would be better to stop testing and start the usage.

From these three values ($cpd_{\text{aRfU}}, bpd_{\text{aRfU}}, cpd_{\text{test}}$), the benefits during usage (bpd_{aRfU}) as well as the costs during testing (cpd_{test}) are independent from the safety performance of the OuT. The determining factor to calculate cpd_{aRfU} is the number of

events that will occur. Assuming the performance vector of the OuT ($\boldsymbol{SP}_{\mathrm{OuT}}$) and combining this with the weighting factors explained in section 1.4.1, the cost factor can be defined as

$$cpd_{\mathrm{aRfU}} := \bar{C}_{\mathrm{AwI}} \cdot \frac{1}{SP_{\mathrm{OuT,AwI}}} + \bar{C}_{\mathrm{AwF}} \cdot \frac{1}{SP_{\mathrm{OuT,AwF}}}. \tag{3-40}$$

Applying this to the lower case of equation (3-39), a relation defines for which worst-case estimation the test *during* usage should be started

$$\bar{C}_{\mathrm{AwI}} \cdot \frac{1}{SP_{\mathrm{OuT,AwI,worst}}} + \bar{C}_{\mathrm{AwF}} \cdot \frac{1}{SP_{\mathrm{OuT,AwF,worst}}} - cpd_{\mathrm{test}} < bpd_{\mathrm{aRfU}}. \tag{3-41}$$

For further discussions, ahead of testing without knowledge about the SP_{OuT}, a ratio between the safety performance level of different severities $a_{\mathrm{S},SP}$ is assumed

$$a_{\mathrm{S},SP} = \frac{SP_{\mathrm{OuT,AwI,worst}}}{SP_{\mathrm{OuT,AwF,worst}}}. \tag{3-42}$$

Equations (3-41) and (3-42) result in an inequality that defines a lower boundary for the worst-case estimation of the safety performance of the OuT

$$SP_{\mathrm{OuT,AwF,worst}} > \frac{\bar{C}_{\mathrm{AwI}} + a_{\mathrm{S},SP}\bar{C}_{\mathrm{AwF}}}{a_{\mathrm{S},SP}(bpd_{\mathrm{aRfU}} + cpd_{\mathrm{test}})}. \tag{3-43}$$

As soon as it can be proven that the OuT's performance is above that level, the "monetary balance" approach suggests to give the RfU. The necessary distance for this proof can be calculated based on equation (3-23). The distance factor (based on $e_{\mathrm{allow}} = 5\ \%$) as the result of this calculation is given in Table 7 and has already been discussed in Figure 18.

Table 7 Necessary distance as a factor of $\boldsymbol{SP}_{\mathrm{OUT,worst}}$ that is necessary for monetary balance (based on $e_{\mathrm{allow}} = 5\ \%$).

Number of events k_{bal}:	0	1	2	3	4	5
Distance factor $a_{d,\mathrm{bal}}$:	3	4.74	6.3	7.75	9.15	10.5

Thus, another way to determine $d_{\mathrm{test},0}$ is formalized by

$$d_{\mathrm{test},0} := a_{d,\mathrm{bal}} \cdot \frac{\bar{C}_{\mathrm{AwI}} + a_{\mathrm{S},SP}\bar{C}_{\mathrm{AwF}}}{a_{\mathrm{S},SP}(bpd_{\mathrm{aRfU}} + cpd_{\mathrm{test}})}. \tag{3-44}$$

However, the table highlights that there is not just a single value that can be defined as the necessary distance. This distance depends on the safety performance of the OuT.

Thus, a logical loop is defined: The necessary distance for identifying the safety performance of the OuT depends on the safety performance of the OuT. This loop only exists when trying to estimate the necessary distance before introduction, not when applying the theory during real testing. This logical loop can be solved when asking for

the most probable case that is described by the expected number of events $\lambda_{\text{bal}} = \frac{d_{\text{test,0}}}{SP_{\text{OuT,AwF}}}$. Given this, together with equation (3-44), the column from Table 7 can be selected when

$$P_{\lambda_{\text{bal}}}(k > k_{\text{bal}}) < e_{\text{allow}}. \tag{3-45}$$

A possible way to determine the cost and benefit factors ($cpd_{\text{aRfU}}, bpd_{\text{aRfU}}, cpd_{\text{test}}$) as well as the right column of Table 7 is presented in the next section 3.6, when the usage strategy is parameterized.

3. Record of events:

Different events will occur during testing. These are separated into:

a) Accidents due to automation control
b) Accidents due to human control
c) Near misses due to automation control
d) Near misses due to human control
e) Interventions due to danger
f) Interventions due to instruction
g) Others

Events that are of relevance are accidents and near misses due to automation control and interventions due to danger as the test driver anticipates an arising accident. Thinking back to the Bernoulli experiment, k_{count} in general would be

$$k_{\text{count}} = \sum_{i=1}^{n_{\text{test}}} X_i \tag{3-46}$$

with n_{test} trials until the end of the testing phase t_{RfU}. Or similar to the test distance, the number of events within the testing distance is defined by

$$k_{\text{count}}(\Delta t) = k(t_{\text{endT}}) - k(t_{\text{startT}}). \tag{3-47}$$

These events sensitive to severity need to be counted

$$\boldsymbol{k}_{\text{count}} = \begin{bmatrix} k_{\text{count,AwI}} \\ \vdots \\ k_{\text{count,AwF}} \end{bmatrix}. \tag{3-48}$$

Interventions due to danger (case e)) need to be post-processed, as the hypothetical severity is unknown. Without a corresponding severity, no benchmark for comparison with human driven vehicles would exist, and these numbers could only serve to compare automated vehicles. Due to the reason that more events will be counted in the

following phases, a time step is introduced indicating testing Δt_{test}, so that the number of events can be assigned to testing by $\boldsymbol{k}_{\text{count}}(\Delta t_{\text{test}})$.

Fulfillment of users' requirement evaluated during testing phase:

Per definition, during testing phase, the test drivers take care of the automated vehicle's safety. Nevertheless, based on the kilometers and events that are counted during testing, a prediction on the automated vehicle's safety after RfU is necessary. The question that should be answered is whether the OuT fulfills users' requirements during usage. As is described in section 3.4.1, two main approaches exist to transparently report the predicted safety of automated vehicles for future users based on the testing results and thereby to fulfill the requirement. These approaches are briefly repeated to explain the strategy.

- Calculate the best- and worst-case estimation

To apply a best- and worst-case estimation, a concrete value for the level of significance e_{proof} needs to be defined. Of importance is that this value is communicated and explained for interpretation. Applying equation (3-21) on e_{proof}, $\boldsymbol{k}_{\text{count}}$, and d_{test}, the best- and worst-case estimation of the OuT's safety performance vector $\boldsymbol{SP}_{\text{OuT,worst}}(t_{\text{RfU}}, e_{\text{proof}})$ and $\boldsymbol{SP}_{\text{OuT,best}}(t_{\text{RfU}}, e_{\text{proof}})$ can be calculated. Both have two components for the different severity levels. The t_{RfU} indicates that the estimation is calculated at t_{RfU} and uses the data collected before. To better understand the different time indices, please see Figure 30.

- Calculate the proof's uncertainty

Following equations (3-26) and (3-27) the uncertainty vector for the proof of being better $\boldsymbol{e}_{\text{PbB}}(t_{\text{RfU}})$ and the uncertainty vector for the proof of being worst $\boldsymbol{e}_{\text{PwB}}(t_{\text{RfU}})$ is calculated using $\boldsymbol{SP}_{\text{bench}}$. The smaller the proof-of-being-better uncertainty the better for introduction.

Fulfillment of society's requirement evaluated during testing phase:

The test driver serves as the safety fallback solution and thereby fulfills the society's safety requirements during the testing phase. The goal is to predict whether the OuT will also fulfill the safety requirement stated by society when the test driver is not present. Therefore, the society's tolerated number of events $k_{\text{tol},\Delta t_{tol}}(t_{\text{RfU}})$ needs to be derived. Δt_{tol} represents the time span for which the numbers k_{tol} are tolerated. The observation time for the explained society's "Safety Detector" (see section 3.4.2) was one year, thus this time span is also used for deriving the tolerated numbers

$$\Delta t_{\text{tol}} = \text{a} = 8766\ \text{h}. \tag{3-49}$$

This tolerated number $k_{\mathrm{tol,a}}$ can be derived using different approaches. Three possible approaches that are objectively arguable are explained in the following. Others and more complex ones are possible. In principle, the approaches explained in the following base on the detector limit $\boldsymbol{k}_{\mathrm{detL}}$ and formalize additional possible events.

- *The Detector's Limit:* Understanding automated driving as a new mode of mobility, it is difficult to argue that events due to existing mobility concepts are "replaced". Accordingly, it is consequent to require that existing safety in road traffic is not being influenced by the introduction of automated vehicles. The consequence would be to equate the tolerated number of events with the detector's limit, derived for example from equation (3-31) on a yearly base

$$\boldsymbol{k}_{\mathrm{tol,a}}(t) = \boldsymbol{k}_{\mathrm{detL}}(t). \tag{3-50}$$

- *The Mobility Replacement:* One could argue differently when understanding automated driving as a replacement for human driving. On top of the detector's limit, the society could additionally allow the vehicle to "replace" the number of events $\boldsymbol{k}_{\mathrm{replace}}(t_{\mathrm{RfU}})$ that arise if human driven vehicles would be used

$$\begin{aligned}\boldsymbol{k}_{\mathrm{tol,a}}(t) &= \boldsymbol{k}_{\mathrm{detL}}(t) + \boldsymbol{k}_{\mathrm{replace}}(t) \\ &= \left\lfloor \boldsymbol{k}_{\mathrm{detL}}(t) \odot \left(1 + \begin{bmatrix} \frac{SP_{\mathrm{OuT,AwI,worst}}(t)}{SP_{\mathrm{bench,AwI}}} \\ \frac{SP_{\mathrm{OuT,AwF,worst}(t)}}{SP_{\mathrm{bench,AwF}}} \end{bmatrix}\right)\right\rfloor.\end{aligned} \tag{3-51}$$

  The "$\odot$" symbol indicates[201] the Hadamard- or Schur-product that is defined for two matrices of the same dimension as the element-wise multiplication. To calculate the expected number of events that would result from conventional human driving ($\boldsymbol{k}_{\mathrm{replace}}(t_{\mathrm{RfU}})$), equation (2-2) is applied. Necessary for application is the average performance of human drivers $\boldsymbol{SP}_{\mathrm{bench}}$ and the worst-case estimation of the safety performance of the OuT $\boldsymbol{SP}_{\mathrm{OuT,worst}}$ to calculate the event ratio. The safety performance of the human as the benchmark has already been defined by equation (3-32).

- *The Special Needs Safety Account:* The before explained approach predicts safety into future application. A more conservative approach would look back in time and ask for the experience on the safety impact. A concept would be to have a safety event account. The tolerated number of events depends on the sum of the detector limit and on this account $\boldsymbol{k}_{\mathrm{acnt}}(t_{\mathrm{RfU}})$

$$\boldsymbol{k}_{\mathrm{tol,a}}(t) = \boldsymbol{k}_{\mathrm{detL}}(t) + \boldsymbol{k}_{\mathrm{acnt}}(t). \tag{3-52}$$

[201] Voigt, C.; Adamy, J.: Formelsammlung der Matrizenrechnung (2012), p. 13.

The account numbers can be derived in different ways based on the information known at t. As at the point in time t_{RfU} there is no history of usage, the value for the account can be derived for the first time after the release for usage.

$$\boldsymbol{k}_{\mathrm{acnt,avrg}}(t) = \left\lfloor \frac{d_{\mathrm{test}}(\Delta t)}{\boldsymbol{SP}_{\mathrm{bench}}} \right\rfloor - \boldsymbol{k}_{\mathrm{count}}(\Delta t). \tag{3-53}$$

Either the difference of the number of events an average human driver generates compared to the number of events counted during testing ($\boldsymbol{k}_{\mathrm{count}}(\Delta t)$) will be added to the detector's limit (equation (3-53). Or like initiatives try to motivate, a more differentiated consideration of additional benefits might be tolerable. Considering the usage demand of mobility-limited people, a share of the distance ($d_{\mathrm{ud,ml}}$) could be seen as of higher benefit for these mobility-limited people. Consequently, a lower safety performance ($\boldsymbol{SP}_{\mathrm{bench,ml}}$) as the safety performance of the benchmark increases the number of tolerated events. The resulting special needs event account replaces the event account in equation (3-52) by

$$\boldsymbol{k}_{\mathrm{acnt,ml}}(t) = d_{\mathrm{ud,ml}}(\Delta t) \cdot \begin{bmatrix} \frac{1}{SP_{\mathrm{bench,ml,AwI}}} \\ \frac{1}{SP_{\mathrm{bench,ml,AwF}}} \end{bmatrix} - \boldsymbol{k}(\Delta t). \tag{3-54}$$

These three approaches have a significant impact on the usage strategy because they limit the usage as is described in the following. Additionally, approaches two and three have a self-reinforcing character. They reward a potentially safe system and penalize a potentially worse system.

The key question is: How to predict whether the consequences of deploying automated vehicles in means of event numbers will or will not exceed the tolerated numbers derived above? A careful approach is to assume a worst-case safety performance and limit the number of allowed distance driven. A possible way would be to use the $\boldsymbol{SP}_{\mathrm{OuT,worst}}(t_{\mathrm{RfU}}, e_{\mathrm{proof}})$ estimated above, but using e_{proof} would neglect the intervention by the limitation of distance. By limiting the distance, the consequences of a misjudgment are reduced. Type one and type two errors are caught by the introduction phase evaluation in every time step $t_{\mathrm{aRfU}i}$. Because of that impact reduction, the worst-case estimation is performed with less significance e_{allow}. In general, the inequality (3-55) states an order between the probability of error, but as has been described[202] the specific values are arbitrary

$$e_{\mathrm{proof}} < e_{\mathrm{allow}}. \tag{3-55}$$

[202] Cowles, M.; Davis, C.: On the origins of the 5% level (1982), p. 1.

The worst-case estimation of the OuT's performance vector $\boldsymbol{SP}_{\mathrm{OuT,worst}}(t, e_{\mathrm{allow}})$ thus follows equation (3-21) and this time applies e_{allow}.

Adapting equation (2-1), the requirement to not exceed the tolerated number of events can be formulated mathematically:

$$P_{\boldsymbol{\lambda}_{\mathrm{tol}}}\left(\boldsymbol{k} \geq \boldsymbol{k}_{\mathrm{tol,a}}\right) \leq e_{\mathrm{allow}} \tag{3-56}$$

Find the expected value $\boldsymbol{\lambda}_{\mathrm{tol,a}}(t_{\mathrm{RfU}})$ that leads to more then $\boldsymbol{k}_{\mathrm{tol,a}}$ events with an error probability e_{allow}. The expected value for tolerated events is found on each severity level by $\lambda_{\mathrm{tol,a}}(t_{\mathrm{RfU}}) = \lambda_{-}(k_{\mathrm{tol,a}}(t_{\mathrm{RfU}}), e_{\mathrm{allow}})$. With the expected value of the Poisson-distribution $\boldsymbol{\lambda}_{\mathrm{tol,a}}(t_{\mathrm{RfU}})$ and the worst-case safety performance $\boldsymbol{SP}_{\mathrm{OuT,worst}}(t_{\mathrm{RfU}}, e_{\mathrm{allow}})$, "tolerated" distances are calculated by

$$\boldsymbol{d}_{\mathrm{allow,a}}(t_{\mathrm{RfU}}) \leq \boldsymbol{\lambda}_{\mathrm{tol,a}}(t_{\mathrm{RfU}}) \odot \boldsymbol{SP}_{\mathrm{OuT,worst}}(t_{\mathrm{RfU}}, e_{\mathrm{allow}}). \tag{3-57}$$

The minimum is chosen from the vector of allowed distances $\boldsymbol{d}_{\mathrm{allow,a}}$, as only one limitation can be set. The allowed distances refer to a certain time window Δt_{tol} that is defined by the analysis time span of the tolerated number of events. The shorter the chosen time window the lower the tolerated number of events will be. When observing a year $\Delta t_{\mathrm{tol}} = \mathrm{a}$, the number of tolerated events is obviously higher compared to an observation of one day.

To decouple the examination from this observed time window, an expected event rate can be derived. As long as this rate is constant over time it can be derived by the following quotient

$$\dot{\boldsymbol{\lambda}}_{\mathrm{tol}}(t_{\mathrm{RfU}}) = \frac{\boldsymbol{\lambda}_{\mathrm{tol,a}}(t_{\mathrm{RfU}})}{\mathrm{a}}. \tag{3-58}$$

Alternatively, the expected event rate could also be calculated by the derivative of the event rate as a function of time

$$\dot{\boldsymbol{\lambda}}_{\mathrm{tol}}(t_{\mathrm{RfU}}) = \left.\frac{\mathrm{d}\boldsymbol{\lambda}_{\mathrm{tol}}(t)}{\mathrm{d}t}\right|_{t_{\mathrm{RfU}}}. \tag{3-59}$$

For reasons of simplicity, at a point in time yearly constant tolerated expected values $\boldsymbol{\lambda}_{\mathrm{tol,a}}$ are assumed. Similar like before, the calculated expected event rate $\dot{\boldsymbol{\lambda}}_{\mathrm{tol}}(t_{\mathrm{RfU}})$ can be used to restrict the usage of automated systems. This time the usage is limited by a defined maximum average yearly velocity the vehicles are allowed to drive in automated mode

$$\boldsymbol{\psi}_{\mathrm{allow}}(t_{\mathrm{RfU}}) \leq \dot{\boldsymbol{\lambda}}_{\mathrm{tol}}(t_{\mathrm{RfU}}) \odot \boldsymbol{SP}_{\mathrm{OuT,worst}}(t_{\mathrm{RfU}}, e_{\mathrm{allow}}). \tag{3-60}$$

From the vector of velocities $\boldsymbol{\psi}_{\mathrm{allow}}$, the minimal number is chosen for limitation.

Caution: The defined velocity is the allowed *average yearly* velocity for all automated vehicles *together*. This upper limit of velocity follows the idea: the higher the velocity, the more Bernoulli experiments n are carried out during a certain time. Thus, by limiting the velocity, the chance to encounter a relevant event within one trial stays the same, but the number of trials reduces and consequently the outcome of relevant events gets lower. How this velocity is influenced by different parameters like the test distance or the approach to derive the tolerated events is discussed in section 3.6 based on examples.

Based on this theory, the automated vehicles will be introduced during the introduction phase, explained in the next subsection.

3.5.2 Introduction Phase

The introduction or deployment of AD3+ vehicles to real traffic *without* a human driver as a supervisor begins with t_{RfU}. At this point, the statistical proof of higher safety of the OuT is still pending. Nevertheless, the users' and society's requirements are fulfilled. However, the fulfillment of the requirements could change as new test distance and events are collected by driving in real traffic. This new experience and knowledge is used to reduce uncertainty about the safety of automated vehicles. The introduction phase ends with the proof of more or less safety at t_{PoS}. The introduction phase is handled as follows:

Concept input during introduction phase:

Not more than the allowed velocity derived with equation (3-60) should be driven with automated vehicles within the planned use case. This should be ensured either by the users or better by the automated driving function itself[203]. The allowed velocity can be shared between all vehicles that enable automated driving within the defined use case. Knowing the average velocity of the vehicles $i_{\text{veh}} = [1, \dots, N_{\text{veh}}]$, their velocity driven automated is limited by

$$\psi_{\text{allow}} \geq \sum_{i_{\text{veh}}=1}^{N_{\text{veh}}} \psi_{i_{\text{veh}}}. \tag{3-61}$$

When the velocity of the individual vehicle is unknown, the velocity can be limited by the amount of active automated driving functions $N_{\text{AD3+}}$ that result either from the assumed average yearly velocity ψ_{UC}

[203] The jam assist of different OEMs today also is limited to highway scenarios. This should be adaptable also for the described use case. This limitation could be extended to a velocity limitation.

$$N_{\mathrm{AD3+}} \leq \left\lfloor \frac{\psi_{\mathrm{allow}}}{\psi_{\mathrm{UC}}} \right\rfloor \tag{3-62}$$

or from the maximum drivable velocity of the use case $v_{\mathrm{UC,max}}$ by

$$N_{\mathrm{AD3+}} \leq \left\lfloor \frac{\psi_{\mathrm{allow}}}{v_{\mathrm{UC,max}}} \right\rfloor. \tag{3-63}$$

No matter which way the velocity is limited, as long as it is above zero the result of application will be more driven distance within the use case. New driven distance means new information for assessment. At any point in time $t_{\mathrm{aRfU}i}$ $i = [1,2,\dots,N]$ after release of usage, the fulfillment of the requirements is evaluable. Assuming the knowledge about the driven velocity $\psi_{\mathrm{driven}}(t)$, the additional distance should be recorded and can be seen as the test distance $d_{\mathrm{test}}(t)$. As this distance has been collected during real-world usage, the representativeness is without question. Together with the test distance during testing phase, a total is defined by

$$\begin{aligned} d_{\mathrm{test},\Sigma} &= d_{\mathrm{test},0}(\Delta t_{\mathrm{test}}) + d_{\mathrm{test}}(\Delta t_{\mathrm{aRfU}i}) \\ &= d_{\mathrm{test},0}(\Delta t_{\mathrm{test}}) + \int_{t_{\mathrm{RfU}}}^{t_{\mathrm{aRfU}i}} \psi_{\mathrm{driven}} \mathrm{dt}. \end{aligned} \tag{3-64}$$

Due to new distance, additional relevant events will occur. The sum over time of the events follows equation (3-48)

$$\boldsymbol{k}_{\mathrm{count}}(\Delta t_{\mathrm{aRfU}i}) = \begin{bmatrix} k_{\mathrm{count,AwI}} \\ \vdots \\ k_{\mathrm{count,AwF}} \end{bmatrix}. \tag{3-65}$$

Together with the events during testing phase, a total of events is defined by

$$\boldsymbol{k}_{\mathrm{count},\Sigma} = \boldsymbol{k}_{\mathrm{count}}(\Delta t_{\mathrm{test}}) + \boldsymbol{k}_{\mathrm{count}}(\Delta t_{\mathrm{aRfU}i}). \tag{3-66}$$

For the introduction phase, all relevant events are connected with a severity level as no test driver exists to intervene before a near miss or accident[204] event (see automated driving definition in section 1.1).

Based on these new events and distance, the fulfillment of stated requirements needs to be checked:

[204] To the authors understanding the interaction concept between human and machine is still unknown for higher automated vehicles. Accordingly the chance exists that also during introduction phase the normal drivers might be able to overrule the automation. This should be kept in mind, when counting events.

Fulfillment of users' requirement during introduction phase:

The more distances driven, the better distinguishable two systems with different performance values are. See the example in Figure 31 where system one is twice as good as system two $\boldsymbol{SP}_1 = 2 \cdot \boldsymbol{SP}_2$. System one gets distinguishable from system two the more kilometers d_{test} are driven. To calculate the values of the Poisson distributions in Figure 31, the test kilometers have been increased from column one to three by the factors $\{1, 10, 20\}$.

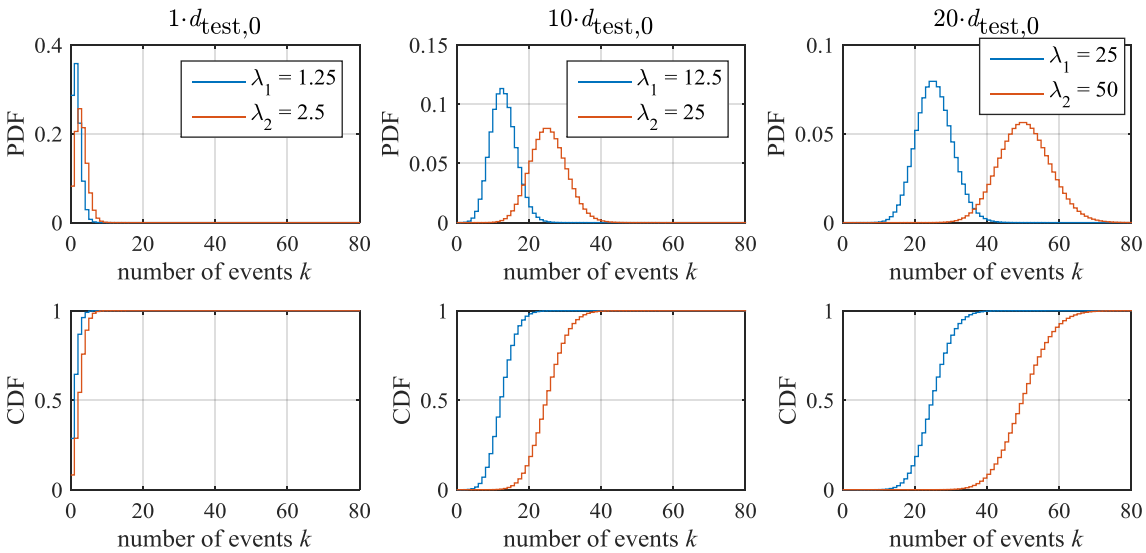


Figure 31 Poisson distribution PDF and CDF comparison of two safety performance level for different test kilometer as evaluation basis and one severity k.

This example illustrates that updating the performance estimations $\boldsymbol{SP}_{\text{OuT,worst}}(t_{\text{aRfU}i}, e_{\text{proof}})$ and $\boldsymbol{SP}_{\text{OuT,best}}(t_{\text{aRfU}i}, e_{\text{proof}})$ at $t_{\text{aRfU}i}$ by the gained data will be necessary to keep the information up to date for users of automated vehicles. The same is true for the uncertainty evaluation $\boldsymbol{e}_{\text{PbB}}(t_{\text{aRfU}i})$ and $\boldsymbol{e}_{\text{PwB}}(t_{\text{aRfU}i})$.

Fulfillment of society's requirement during introduction phase:

The allowed velocity for automated vehicles $\psi_{\text{allow}}(t_{\text{aRfU}i})$ will change due to new information about the estimated safety of automated vehicles $\boldsymbol{SP}_{\text{OuT,worst}}(t_{\text{aRfU}i}, e_{\text{allow}})$ and a change in tolerance of events $\boldsymbol{k}_{\text{tol,a}}$ due to automated driving. At certain points in time $t_{\text{aRfU}i}$, the allowed velocity can be updated by adapting the equations (3-56) to (3-60) to the new time span and point in time following Figure 30.

Additionally, the risk which has been taken can be evaluated during introduction, expressed as an error probability by deploying the automated driving technology. This is similar to the uncertainty evaluation for the users' perspective. Known is the worst-case

approximation of the OuT $\boldsymbol{SP}_{\mathrm{OuT,worst}}(t_{\mathrm{aRfU}i}, e_{\mathrm{allow}})$ and the driven distance $d_{\mathrm{test}}(\Delta t_{\mathrm{aRfU}i})$ as well as the tolerated number of events $\boldsymbol{k}_{\mathrm{tol,a}}(\Delta t_{\mathrm{aRfU}i-1})$ defined one point in time ahead of evaluation $(i-1)$. Using these information first

$$\boldsymbol{\lambda}_{\mathrm{intro}} = \begin{bmatrix} \dfrac{d_{\mathrm{test}}(\Delta t_{\mathrm{aRfU}i})}{SP_{\mathrm{OuT,AwI,worst}}(t_{\mathrm{aRfU}i}, e_{\mathrm{allow}})} \\ \dfrac{d_{\mathrm{test}}(\Delta t_{\mathrm{aRfU}i})}{SP_{\mathrm{OuT,AwF,worst}}(t_{\mathrm{aRfU}i}, e_{\mathrm{allow}})} \end{bmatrix} \tag{3-67}$$

and secondly the probability that the counted number of events would have occurred is calculable by

$$P_{\boldsymbol{\lambda}_{\mathrm{intro}}}\left(\boldsymbol{k} \geq \boldsymbol{k}_{\mathrm{tol}}(\Delta t_{\mathrm{aRfU}i-1})\right) = \boldsymbol{e}_{\mathrm{intro}}(\Delta t_{\mathrm{aRfU}i}). \tag{3-68}$$

These values are sensitive to the level of severity, thus $\boldsymbol{\lambda}_{\mathrm{intro}}$ is a vector and equation (3-68) has to be evaluated for each level of severity.

3.5.3 Supervision Phase

Above the requirement to generate objective information for users, the introduction phase has the potential to generate enough distance that is necessary for the final proof of safety. This was not achievable during testing phase (see section 2.4.2). The more distance is driven, the better the chance to distinguish a safe from an unsafe OuT. This is depicted for explanation in Figure 31. One theoretical exception exists for $\boldsymbol{SP}_{\mathrm{bench}} = \boldsymbol{SP}_{\mathrm{OuT}}$. In real application, the chance for exactly $\boldsymbol{SP}_{\mathrm{bench}} = \boldsymbol{SP}_{\mathrm{OuT}}$ is very little and thus this is more a theoretical problem. Over time $(t_{\mathrm{aRfU}i})$, the estimated performance $\boldsymbol{SP}_{\mathrm{OuT,worst}}\left(t_{\mathrm{aRfU}i}, e_{\mathrm{proof}}\right)$ will converge to the real performance $\boldsymbol{SP}_{\mathrm{OuT}}$.

At one point in time t_{PoS} (see Figure 30), the estimated performance will exceed the benchmark

$$\boldsymbol{SP}_{\mathrm{OuT,worst}}\left(t_{\mathrm{PoS}}, \mathrm{e}_{\mathrm{proof}}\right) \geq \boldsymbol{SP}_{\mathrm{bench}}, \tag{3-69}$$

or in contrast it could also occur that the best-case estimation drops below the benchmark

$$\boldsymbol{SP}_{\mathrm{OuT,best}}\left(t_{\mathrm{PoS}}, e_{\mathrm{proof}}\right) \leq \boldsymbol{SP}_{\mathrm{bench}}. \tag{3-70}$$

Equation (3-69) formalizes case 1: the proof of more safety and equation (3-70) formalizes case 2: the proof of less safety. It seems wise to keep in mind that one of these two cases can happen. Firstly, because it is unclear what happens if automated vehicles of different brands get directly comparable in means of safety? Would certain vehicles be withdrawn from traffic? Secondly, it is unclear what happens if the automated system is proven less safe? Would then all vehicles get banned from road traffic? Thirdly, it is

unclear what happens after safety has been proven? Would then the limitation of velocity be obsolete?

The first question is out of our scope. The second and third question can be addressed by reviewing both, the users' requirements and the society's requirements. The results might be applied to the supervision phase (Δt_{suvi}) after the proof of safety (t_{aPoS}).

Concept input during supervision phase:

To argue about a safety evolution, further driven distances as well as resulting events need to be counted and reported. Obviously, after a safety proof, the question may arise why a further supervision is of relevance. However, it should be kept in mind that the safety proof was given on data of the past. A proof can only be given retrospective or based on the guarantee that the system under observation, meaning road traffic in this case, is not changing over time. I assume that no one can give this guarantee for open road traffic. Consequently, the proof of safety, although it is the best guess for the future, is only valid for the past. As today's traffic changes over time, the different capabilities of human driver and automated driver will result in changing performance levels $\boldsymbol{SP}_{\mathrm{bench}}$ and $\boldsymbol{SP}_{\mathrm{OuT}}$ over time[205]. Accordingly, the check for fulfillment of both requirements should not end with t_{PoS} because the requirements will not vanish either. Thus, at several points in time $t_{\mathrm{aPoS}i}$ the data and information from $\Delta t_{\mathrm{aPoS}i}$ should be exermined.

Fulfillment of users' requirement during supervision phase:

The users' requirement asks at $t_{\mathrm{aPoS}i}$ for the update of the objective safety indicators being the performance estimations $\boldsymbol{SP}_{\mathrm{OuT,worst}}(t_{\mathrm{aPoS}i}, e_{\mathrm{proof}})$ and $\boldsymbol{SP}_{\mathrm{OuT,best}}(t_{\mathrm{aPoS}i}, e_{\mathrm{proof}})$. The same should be done for the uncertainty evaluation $\boldsymbol{e}_{\mathrm{PbB}}(\mathrm{t}_{\mathrm{aPoS}i})$ and $\boldsymbol{e}_{\mathrm{PwB}}(t_{\mathrm{aPoS}i})$.

The equations to calculate these values remain the same. A time window $\Delta t_{\mathrm{aPoS}i}$ for evaluation has to be chosen carefully. During the first evaluation at t_{PoS}, the whole amount of distance and corresponding events must be used for evaluation. This point in time is the first time when enough information is accessible to conduct the proof of safety. This whole time span is described by $\Delta t_{\mathrm{test}} + \Delta t_{\mathrm{intro}}$. All the information within this time span is necessary to reach the required level of significance. After t_{PoS} this might change. To keep the same significance, not all information before t_{PoS} is necessary for evaluating safety. In other words: when using all information, also the "oldest",

[205] Wachenfeld, W.; Winner, H.: Do Autonomous Vehicles Learn? (2016).

we do not evaluate the actual safety but implement some kind of filter that smoothes the safety information.

Therefore, a sliding window with an adaptive width defined by its evaluation point in time $t_{\mathrm{aPoS}i}$ and its time span $\Delta t_{\mathrm{aPoS}i}$ is defined. Its characteristic is that based on the information within this time window the required error probability e would be reached. Using this time window, up to date information about the safety of existing vehicles applied to today's road traffic is gathered. Important is that the distance traveled within this time window is representative. If this can't be stated, neglecting old data is not reasonable. For this thesis, the studied OuT as well as the area of usage is assumed to be time-invariant. Consequently, a sliding window is not necessary. Nevertheless, for real-world application this issue needs to be addressed.

If the proof of safety (case 1) occurs, the user's requirements are fulfilled given a pre-defined uncertainty. Thus, there is no reason from users' perspective to further limit the introduction of these vehicles.

If the proof of less safety (case 2) occurs, the users' requirements are still fulfilled as long as these results are transparently and instantaneously reported. To my understanding, expressed by equation (1-1), it is not absolute to ask for higher safety. Obviously, this is discussable depending on the benefits besides safety and needs a strong debate by affected parties. At this point in time, this debate can be conducted as knowledge from real usage exists. From the users' perspective, the proof of less safety doesn't change his/her task to interpret the knowledge about safety for him- or herself.

Fulfillment of society's requirement during supervision phase:

The output of the society's requirement is the allowed velocity for automated vehicles $\psi_{\mathrm{allow}}(t_{\mathrm{aRfU}i})$. This velocity is affected differently depending on the case that occurs.

Proof of higher safety - case 1: Should the allowed velocity be set unlimited and thereby should the usage of automated vehicles not be limited anymore after t_{PoS}? On the one hand, arguments exist to not limit the usage: Safety has been proven thus it can be treated as regular vehicles today. Today's distances traveled as the result of a velocity are not limited. Why should automated usage be limited? On the other hand, arguments exist to further limit the usage: When increasing the allowed velocity, the number of events could increase although the vehicles drive safer. This might happen especially when additional distance will be driven, due to the chance that vehicles drive without passengers. This would be of interest if the numbers of vehicles are reduced and car and/or ride sharing concepts are implemented. To give access to existing users and enable the same amount of mobility, the vehicles need to be distributed without passengers. The number and speed of AD2- vehicles today is limited by driver licenses. AD3+, if not

limited artificially for example by the allowed speed, would theoretically not be limited by anything than economic reasons.

Proof of lower safety - case 2: Should the allowed velocity be set to zero and thereby should the usage of automated vehicles be prevented after t_{PoS}? The answer depends on additional benefits that might outweigh the additional risks. Some kind of limited usage seems appropriate. The approaches explained to derive the allowed velocity already include a reaction on a bad best-case estimation. The usage strategies reduce the allowed velocity and thereby limit the impact on safety for society.

No matter which case occurs, this point in time t_{PoS} defined by the proof of lower or higher safety should be seen as the point in time when a profound decision can be made: What is the future of AD3+ mobility? A strict prohibition as well as a strict deregulation seems not appropriate from the safety point of view. It is more about the question on how to limit the risks for everybody.

3.6 Usage Strategy Examination

Q19 How will the usage strategy affect the deployment of automated driving and how will different parameters influence the safety outcome?

To answer Q 19, the usage strategy described above is now applied for a fictive Autobahn-Pilot in Germany. The performed calculation steps described above are arranged for better understanding in a simplified flowchart, depicted in Figure 32. This flowchart separates the usage strategy evaluation (gray background) from the reality simulation (light background). The reality simulation needs to be performed, as no real AD3+ vehicle has yet been tested and used.

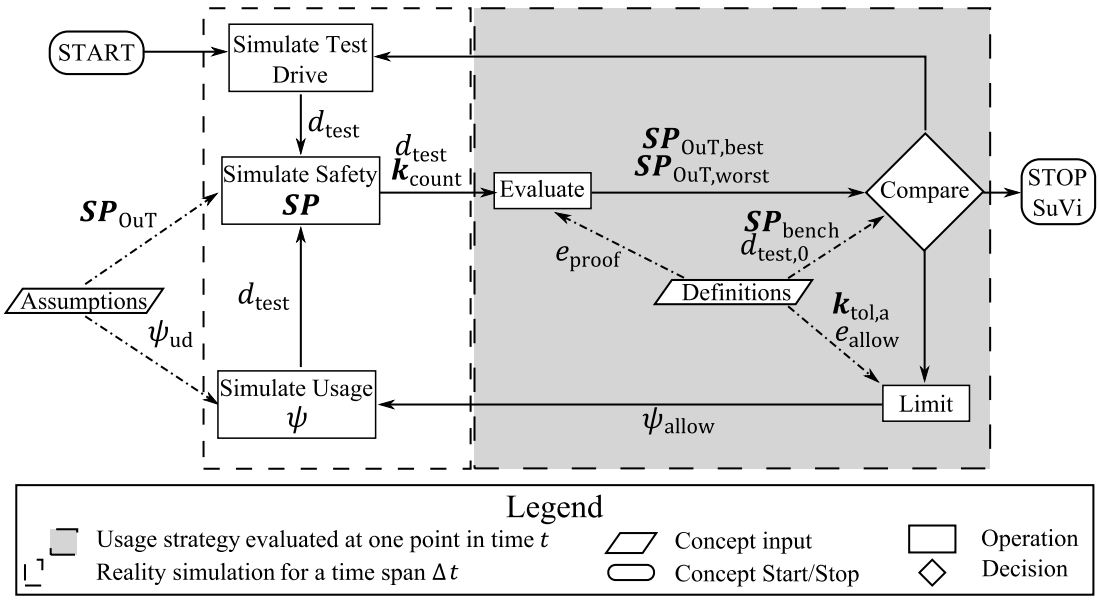


Figure 32 Simplified flowchart of usage strategy for automated systems

To study the application of the strategy, simplifications for reality simulation are assumed. One main simplification is that the surrounding world is not changing (time-invariant), i.e.:

- The SP of the benchmark and the OuT do not change over time.
- The costs of events do not change over time.
- The usage demand and behavior do not change over time
- The tolerance, general infrastructure, etc. do not change over time.

Given these simplifications, the following subsections first identify and define the parameters that influence the strategy by explaining the flowchart. Second, assign exemplary values to the parameters. Third, define criteria for evaluation. Fourth, analyze the result of the simulation. Last, subsection 3.6.5 will conclude on the usage strategy examination.

3.6.1 Usage Strategy Parameter Identification

Today, concrete values are unknown for the application of the usage strategy. These values are:

- ψ_{ud} – The usage demand formalized by four different average yearly velocities.
- $\boldsymbol{SP}_{OuT}$ – The safety performance vector of the OuT that describes average distance in between two events of the same severity level.

These parameters are defined as assumptions and serve as concept input in Figure 32. These assumptions are used to simulate the output of testing and real usage (light background). Obviously, these assumptions are not necessary if a real automated vehicle is

tested and introduced. The usage demand depends on the users that would request the vehicle. The safety performance vector is the safety characteristic of the automated vehicle itself. Thus, in section 3.6.2, values are assigned to these assumptions for studying the theory's outcome.

As Figure 32 indicates, another input is needed for the application of the usage strategy (gray background). The so-called definitions have to be derived also in real-world application of the theory:

- e_{proof} – The probability of error that is used to derive the best- and worst-case estimations of the OuT for the proof of lower or higher safety.
- $d_{\text{test,0}}$ – The total distance which the automated vehicles have been driven under testing conditions before the release for usage t_{RfU}.
- $\boldsymbol{SP}_{\text{bench}}$ – The safety performance vector is used as the benchmark for comparison.
- $e_{\text{allow}}, \boldsymbol{k}_{\text{tol,a}}$ – The probability of error, the tolerated number of events. Both are used to derive the allowed velocity.

Thus, in section 3.6.2, these definitions are assigned values to simulate the usage strategy.

Given these assumptions and definitions as model input, the theory can be applied. Application means to execute different numerical calculations either for the usage strategy evaluation (Figure 32 gray-background) or the reality simulation (Figure 32 light background). At a point in time t, the updated distance driven by automated vehicles, either during testing or usage, as well as the number of events is taken for evaluation. Based on the defined probability of error, the best- and worst-case performance vectors of the OuT are estimated. These estimations are compared with a defined performance benchmark vector to either stop the usage, go back to testing, or to limit the usage. The limitation is done by the defined error of probability and the tolerated number of events resulting in an allowed velocity.

This allowed velocity is the output of the usage strategy evaluation and the input of the usage simulation. The simulated usage closes the evaluation loop by calculating a distance traveled during the time span Δt as well as the numbers of events that might have happened during this time span. The simulated usage limits the velocity either by the allowed velocity or the velocity demanded by newly registered vehicles.

As Figure 32 indicates, the evaluation which is depicted as a loop is executed several times and its output (ψ_{allow}) influences its inputs ($\boldsymbol{k}_{\text{count}}$ and d_{test}). Consequently, two simulation parameters need to be assigned:

- Δt – The length of the time span between two evaluations.
- t_{end} – The end of simulation for this usage strategy examination.

3.6.2 Usage Strategy Parameter Assignment

To study the theory, values need to be assigned to the parameters identified above. Either specific values can be derived theoretically or, if this is not possible, the following sections will study the sensitivity of the usage strategy outcome for different parameter combinations.

Necessary Assumptions

ψ_{ud} – Several technologies exist that have found their way into every newly registered automobile. From Litman[206] there exists a publication that tries to predict the autonomous vehicle implementation based on these technology experiences and on different other contributing factors. In general, all predictions of future take rates suffer high uncertainty. Especially for a new technology, if few comparable products exist. However, there will still be some difference between the real introduction depending on the usage demand and the total introduction when every new vehicle is equipped with a technology (equipment ratio $ER(t) = 1$).

Accordingly to Sefati[207], the ESC (electronic stability control) equipment ratio from 1995 until 2015 is considered to get a simple predictor of the usage demand of automated driving functions. The ESC equipment ratio is chosen because it describes the ratio from 0 to 1 of newly registered vehicles in Germany, thus it stands for a successful introduction. Additionally, it is a safety relevant function that supports the driver. Although the real equipment demand will differ from this approximation, it is seen as a first best guess.

---

[206] Litman, T.: Autonomous Vehicle Implementation Predictions (2014).

[207] Sefati, M.: Benefit Analysis of Automated Safety Systems, Report Project Ko-KOMP (2013), p. 8–9.

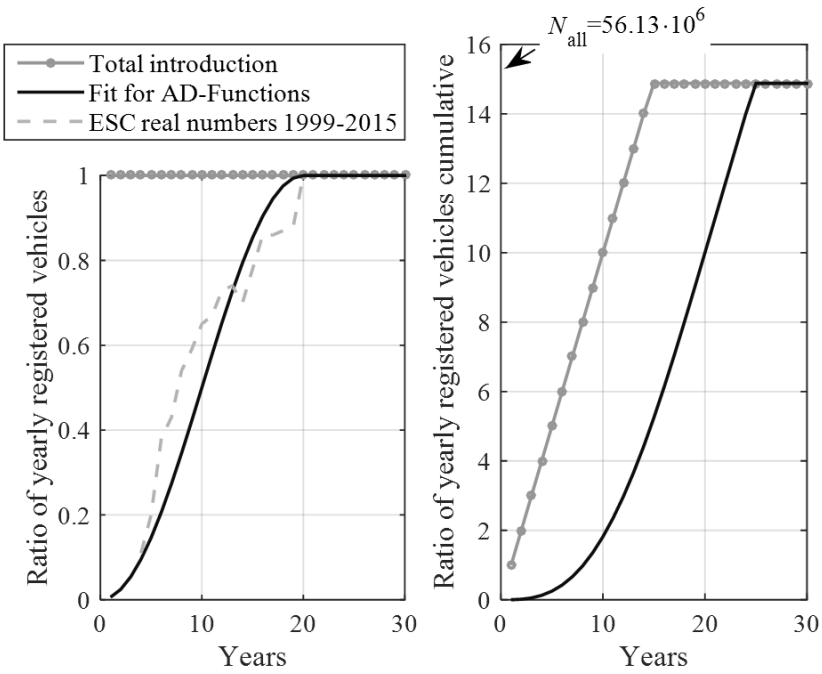


Figure 33 Automotive technology equipment rate for ESP and predicted for AD3+

Figure 33 depicts the equipment ratio for ESC where year 0 is the year of introduction 1995. To derive a possible equipment ratio for automated driving, the ESC numbers are fitted by a cosine function up to year 20

$$ER(t) := \begin{cases} \frac{1}{2}\left(1 - \cos\left(\frac{\pi}{20\,\mathrm{a}} \cdot t\right)\right) & t \leq 20\,\mathrm{a} \\ 1 & t > 20\,\mathrm{a} \end{cases}. \tag{3-71}$$

The usage demand for automated driving is expressed by the average yearly velocity ψ. This average yearly velocity ψ is defined by

$$\psi = \frac{d_\mathrm{a}}{\mathrm{a}} \tag{3-72}$$

where d_a is the annually driven distance and the number of hours of one year are $\mathrm{a} = 8766\,\mathrm{h}$. This velocity should not be confused with the average velocity $\bar{v}$ that is defined by the distance driven d and the time it takes to drive this distance t_u

$$\bar{v} = \frac{d_\mathrm{a}}{t_\mathrm{u}}. \tag{3-73}$$

The usage ratio UR is defined by the quotient of both velocities

$$UR = \frac{\bar{v}}{\psi} = \frac{t_\mathrm{u}}{\mathrm{a}}. \tag{3-74}$$

For one vehicle in today's Autobahn traffic, the average yearly velocity is

$$\psi_{1\mathrm{Veh,AB}} = \frac{d_{\mathrm{a,AB}}}{\mathrm{a} \cdot N_\mathrm{all}} \approx 0.456\ \frac{\mathrm{km}}{\mathrm{h}}. \tag{3-75}$$

That is calculated based on the distance driven[208a] by all vehicles (Kfz) on the Autobahn in Germany in 2013 $d_{\mathrm{a,AB}} \approx 224.2 \cdot 10^9$ km, the number of registered vehicles that might access the Autobahn (passenger cars/Pkw: $43.4 \cdot 10^6$, motorcycles/Krafträder: $3.98 \cdot 10^6$, busses/Kraftomnibusse: $0.076 \cdot 10^6$, trucks/Lkw: $2.58 \cdot 10^6$ articulated vehicles/Sattelzüge: $0.18 \cdot 10^6$ and others/übrige Kfz: $0.27 \cdot 10^6$) in Germany[208b] 2013 $N_{\mathrm{allG}} \approx 50.52 \cdot 10^6$ and the hours of one year $\mathrm{a} = 365.25 \cdot 24$ h. Additionally, a factor $a_{\mathrm{intV}} = \frac{N_{\mathrm{all}}}{N_{\mathrm{allG}}} \approx 1.11$ is necessary to correct the numbers of vehicles as also vehicles not registered in Germany lead to driven distances on German Autobahn. This factor is taken from a counting[209] of foreign vehicles on German Autobahn in 2008. Thus, the usage demand in general is calculated by multiplying a number of vehicles with this average yearly velocity $\psi_{\mathrm{1Veh,AB}}$. For all vehicles $N_{\mathrm{all}} \approx 56.13 \cdot 10^6$ that drove on German Autobahn in 2013, the usage demand is expressed by the velocity

$$\psi_{\mathrm{ud,all}} = \psi_{\mathrm{1Veh,AB}} \cdot N_{\mathrm{all}} \approx 25.58 \cdot 10^6 \ \frac{\mathrm{km}}{\mathrm{h}}. \tag{3-76}$$

The usage demand of newly registered vehicles is a function of time

$$\psi_{\mathrm{ud,newReg}}(t) = \psi_{\mathrm{1Veh,AB}} \cdot \int_0^t \dot{N}_{\mathrm{newReg}} \mathrm{dt} \tag{3-77}$$

with the rate of newly registered vehicles being

$$\dot{N}_{\mathrm{newReg}}(t) = \frac{N_{\mathrm{NewReg}}}{\mathrm{a}} \approx 430.4/\mathrm{h}. \tag{3-78}$$

The number of newly registered vehicles (Kfz) in Germany 2013 multiplied with the correction factor is $N_{\mathrm{NewReg}} \approx 3.77 \cdot 10^6$.

When assuming an equipment ratio being smaller than 1 described by equation (3-71), the usage demand follows to be

$$\psi_{\mathrm{ud,ER}}(t) = \psi_{\mathrm{1Veh,AB}} \cdot \int_0^t \dot{N}_{\mathrm{ER}} \mathrm{dt}. \tag{3-79}$$

The rate of registered vehicles following an equipment ratio is defined as

$$\dot{N}_{\mathrm{ER}}(t) = \frac{N_{\mathrm{NewReg}}}{\mathrm{a}} ER(t). \tag{3-80}$$

The usage demand increases from year to year and represents how many vehicles would be driven automated in real traffic if no limitations by a usage strategy are implemented. This is depicted in Figure 34. The life expectancy of vehicles is not modelled. Assuming the usage demand is not changing, there will be an upper limit given by $\psi_{\mathrm{ud,all}}$.

---

[208] BMVI et al.: Verkehr in Zahlen 2015/16 (2016), p. a:106, b:133.

[209] Lensing, N.: BASt-Zählung Ausländischer Kraftfahrzeugverkehr 2008 (2010), p. 18.

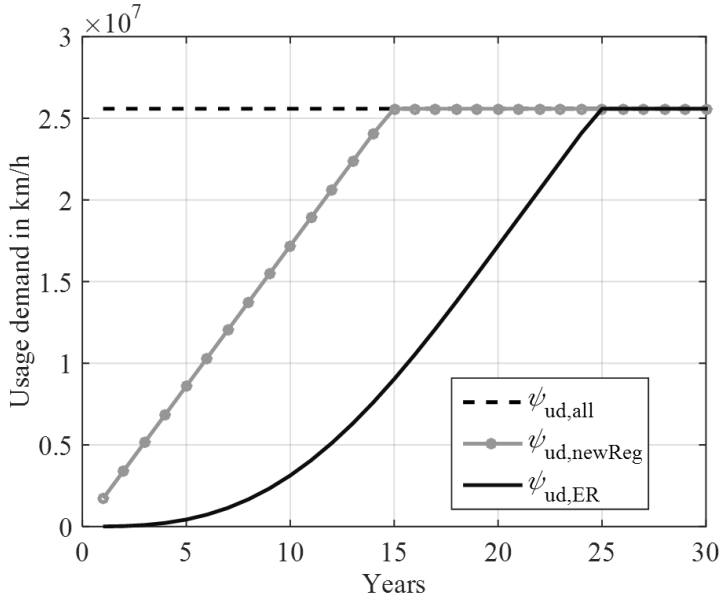


Figure 34 Usage demand for the Autobahn pilot

Predicting the equipment ratio ER for 30 years into the future suffers high uncertainty for different reasons. One is the comparison with a technical system of the past (e.g. ESC) that has different benefits and drawbacks. Others are the regulatory dependency or the self-reinforcing effect as the usage demand would be highly influenced by the safety impact. Additionally, financial and lifestyle factors in general affect the usage demand. Nevertheless, for the simulation the usage demand expressed by different velocities ψ_{ud} is necessary to analyze and compare the impact of different parameters. For the real-world application of the theory, ER should be measured or at least estimated continuously to reduce these uncertainties.

Besides the upper limit for a usage demand $\psi_{\mathrm{ud,all}}$, a lower limit can also be calculated. This lower limit can for example be motivated by the "Convention on the Rights of Persons with Disabilities" (CRPD) Article 4.1.g[210]:

> *To undertake or promote research and development of, and to promote the availability and use of new technologies, including information and communications technologies, mobility aids, devices and assistive technologies, suitable for persons with disabilities, giving priority to technologies at an affordable cost;*

The lower limit of demand would be for the benefit of people with mobility limitations due to disabilities. This lower limit may be calculated based on numbers from representative surveys. In 2002, a seventh of the respondents of the German mobility study[211]

[210] UN: Protection and Promotion of the Rights and Dignity of Persons with Disabilities (2006), p. 9.

[211] Follmer, R. et al.: Mobilität in Deutschland 2002 (2004), p. 141–144. The newer study from 2008 doesn't deliver the same information to calulate ml. See Follmer, R. et al.: Mobilität in Deutschland 2008 (2010), p. 85–86.

suffered disabilities. Of these respondents, 2/3 answered that this would result in mobility limitations. This limitation for individual mobility resulted for them in only 10.3 km of self-driving whereas people without disabilities ended up driving 26.3 km a day. The average distance for all respondents is reported with 25.1 km. From these figures, a mobility demand considering a mobility limitation factor $ml \approx 0.06$ is derived and is applied to the total number of newly registered vehicles

$$\psi_{\mathrm{ud,ml}}(t) \coloneqq ml \cdot \psi_{\mathrm{ud,newReg}}(t) \tag{3-81}$$

$$ml = \frac{1}{7} \cdot \frac{2}{3} \cdot \frac{(26.3-10.3)}{25.1} \approx 0.06. \tag{3-82}$$

This number of 6 % has to be used carefully, because it is a rough simplification of the actual challenge mobility limited people are confronted with. Automated driving might be one step to overcome their limitations, but other hindrances for mobility like difficult building access will still exist. In addition, the Autobahn-Pilot will not be the first use case for mobility limited people.

$\boldsymbol{SP}_{\mathrm{OuT}}$ – The second assumption that needs to be assigned is the safety performance vector of the automated vehicle. As the missing information about the performance is the origin point for the whole thesis, different values are assumed. The relation between the safety performance values and the safety outcome of the strategy is studied. The range of performance level that is reasonable to be discussed may be derived from today's performance level variation due to human vehicle control. Studies[212] have been conducted that deliver a factor of approximately 6 between an experienced driver and a young (17 years old) inexperienced driver. Their performance is measured in accidents per year. The principle of the model that is built based on the results of the study is depicted in Figure 35. The median number of accidents of this studied sample is[212a] $0.1286/\mathrm{a}$ for drivers with 6000-9999 annual mileage. The variation of the assumed performance factor $\boldsymbol{SP}_{\mathrm{OuT}}$ is defined by

$$\boldsymbol{SP}_{\mathrm{OuT}} \coloneqq a_{SP} \cdot \boldsymbol{SP}_{\mathrm{bench}} \tag{3-83}$$

$$a_{SP} = \{0.1, 0.2, 1.34, 10\} \tag{3-84}$$

where $1.34 \cdot \boldsymbol{SP}_{\mathrm{bench}}$ represents the upper end of human performance and $0.2 \cdot \boldsymbol{SP}_{\mathrm{bench}}$ the lower end. One order of safety performance better and worse OuT are chosen as representatives to see how the strategy deals with significantly worse or better systems.

[212] Maycock, G.; Lockwood, C. R.: The accident liability of British car drivers (1993), p. a:235 Table 1. Caution: these are numbers for British drivers reported 1993. This is a first best attempt to use meaningful ratios between median and extreme values. An update for this numbers should be done for concept application.

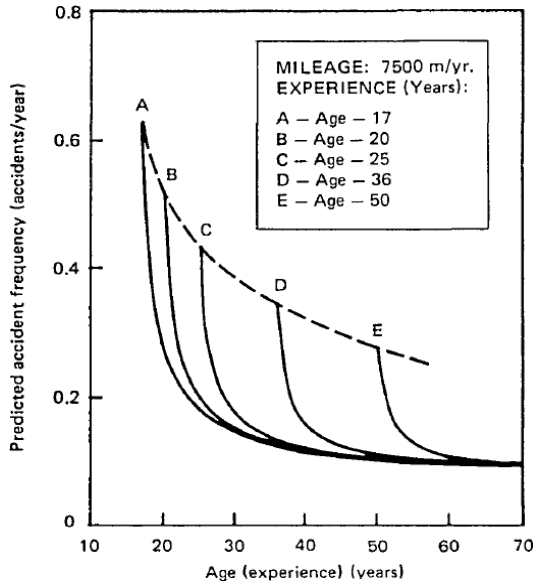


Figure 35 The predicted effect of age and driving experience on accident liability.[213]

This performance vector of the automated vehicle can be used in different ways to simulate the occurrence of an event. Either the Poisson process is simulated or a deterministic simulation using the expected value is performed. To study the effect of the different assumptions and definitions, a deterministic process is used as this is what is most likely to happen in reality.

Necessary Definitions

$\boldsymbol{SP}_{\text{bench}}$ - The Autobahn Pilot for Germany is studied, thus today's average values (2013)[214] are taken as the benchmark

$$\boldsymbol{SP}_{\text{bench}} := \begin{bmatrix} \dfrac{d_{\text{a,AB}}}{A_{\text{wI,AB}}} \\ \dfrac{d_{\text{a,AB}}}{A_{\text{wF,AB}}} \end{bmatrix} \approx \begin{bmatrix} \dfrac{224.2 \cdot 10^9}{18073}\,\text{km} \\ \dfrac{224.2 \cdot 10^9}{379}\,\text{km} \end{bmatrix} \approx \begin{bmatrix} 1.24 \cdot 10^7\ \text{km} \\ 5.92 \cdot 10^8\ \text{km} \end{bmatrix} \tag{3-85}$$

with the number of accidents with injuries $A_{\text{wI,AB}}$ and fatalities $A_{\text{wF,AB}}$. The higher the event's severity, the higher the performance of today's road traffic. For real application of the theory, additional severity level should be used. The lower the safety performance at another level of severity, the more probable is an indicator for safety. For understanding the theory, it is not important how many different level of severity are discussed as long as two competing ones are handled.

[213] Maycock, G.; Lockwood, C. R.: The accident liability of British car drivers (1993), p. 240.

[214] Destatis: Verkehrsunfälle - Zeitreihen 2014 (2015), p. 6 & 23.

$e_{\text{allow}}, e_{\text{proof}}$ - both error probabilities are difficult to derive theoretically. Obviously, type 1 and type 2 errors and the weighting of their outcome may lead to a decision for a specific level. The explanation for the error types is given in Table 8. Values for both error probability parameters need to be defined. From literature[215] and especially common in medical tests[216], these values are arbitrarily defined as

$$e_{\text{proof}} \coloneqq 1\ \%. \qquad e_{\text{allow}} \coloneqq 5\ \%. \tag{3-86}$$

Table 8 Systematic of error types[217]

		Null hypothesis (H0) is	
		Valid/True	Invalid/False
Judgment of Null Hypothesis (H0)	Reject	Type I error (False-Positive)	Correct inference (True-Positive)
	Fail to reject	Correct inference (True-Negative)	Type II error (False-Negative)

$\boldsymbol{k}_{\text{tol,a}}$ - As has been described (see section 3.5), different methods exist to define these tolerated numbers. To see how these methods influence the usage strategy, the three approaches are studied as representatives for others. All three methods depend on the detectors' limit $\boldsymbol{k}_{\text{detL}}$. As this detector limit is not necessarily derived as explained in section 3.4.2, its impact on the introduction will be studied as well. Therefore, besides the derived values that are calculated as the floored standard deviation ($\beta = 1$) to a fitted trend line at the yearly numbers from 1992-2014 for German Autobahn events[218], also a floored tenth ($\beta = 10$) as well as the often required vision zero ($\beta = 10^4$) is examined:

$$\boldsymbol{k}_{\text{detL}}(\beta) \coloneqq \begin{bmatrix} \frac{k_{\text{detL,AwI}}}{\beta} \\ \frac{k_{\text{detL,AwF}}}{\beta} \end{bmatrix}. \tag{3-87}$$

For the severity level of accidents with fatalities, $k_{\text{detL,AwF}} = \{0, 3, 39\}$ results.

[215] Cowles, M.; Davis, C.: On the origins of the 5% level (1982), p. 553–557.

[216] Altman, D. G. et al.: Statistics with confidence (2000 // 2011), p. 219.

[217] https://en.wikipedia.org/wiki/Type_I_and_type_II_errors accessed 24.09.2016

[218] Destatis: Verkehrsunfälle - Zeitreihen 2014 (2015), p. 23.

1. The Detector's Limit – This approach gives a tolerated number for each severity level following equations (3-31) and (3-50). This approach is chosen as a representative approach because a fixed number is derived that is not adapted during the years.

$$\boldsymbol{k}_{\mathrm{tol,a}} \coloneqq \boldsymbol{k}_{\mathrm{detL}}(\beta). \tag{3-88}$$

2. The Mobility Replacement – This approach uses the hypothesis that the allowed velocity ψ_{allow} calculated based on the detector limit will be driven by the automation. Thereby the automation replaces human driven distances, thus human driven events. This replacement strategy assumes that these replaced events would additionally be tolerable for the automation. Thus, the tolerated number of events results to be as defined in equation (3-51)

$$\begin{aligned}\boldsymbol{k}_{\mathrm{tol,a}}(t_{\mathrm{aRfU}i}) &= \boldsymbol{k}_{\mathrm{detL}}(\beta) + \boldsymbol{k}_{\mathrm{replace}} \\ &= \boldsymbol{k}_{\mathrm{detL}}(\beta) \odot \left(1 + \begin{bmatrix} \dfrac{SP_{\mathrm{OuT,AwI,worst}}}{SP_{\mathrm{bench,AwI}}} \\ \dfrac{SP_{\mathrm{OuT,AwF,worst}}}{SP_{\mathrm{bench,AwF}}} \end{bmatrix}\right).\end{aligned} \tag{3-89}$$

Assuming a tolerable replacement of events, the number of events increases depending on the ration of the safety performance values of the different level of severity.

3. The Special Needs Safety Account – The additional tolerated events are depending on the detectors' limit and the events of the past

$$\boldsymbol{k}_{\mathrm{tol,a}}(t_{\mathrm{aRfU}i}) = \boldsymbol{k}_{\mathrm{detL}}(\beta) + \boldsymbol{k}_{\mathrm{acnt}}(t_{\mathrm{aRfU}i}).$$

Equation (3-52) for $\boldsymbol{k}_{\mathrm{acnt}}$ is concretized by the mobility limitation factor $ml = 0.06$ that is used to define the demand for the test distance with special treatment $d_{\mathrm{ud,ml}}$.

$$d_{\mathrm{ud,ml}}(t_{\mathrm{aRfU}i}) = \int_{t_{\mathrm{RfU}}}^{t_{\mathrm{aRfU}i}} \psi_{\mathrm{ud,ml}}(t)\mathrm{d}t. \tag{3-90}$$

The performance level tolerated for special needs is defined as the safety performance of an inexperienced young driver. A concrete value for that is defined by $\boldsymbol{SP}_{\mathrm{bench,ml}} \coloneqq a_{SP,\mathrm{ml}} \cdot \boldsymbol{SP}_{\mathrm{bench}}$ with a factor of $a_{SP,\mathrm{ml}} = 0.2$ derived from Figure 35.

$$\boldsymbol{SP}_{\mathrm{bench,ml}} = \begin{bmatrix} SP_{\mathrm{bench,ml,AwI}} \\ SP_{\mathrm{bench,ml,AwF}} \end{bmatrix} \approx \begin{bmatrix} 2.48 \cdot 10^6\ \mathrm{km} \\ 1.18 \cdot 10^8\ \mathrm{km} \end{bmatrix}$$

For every new evaluation ($t_{\mathrm{aRfU}i}$), the safety account vector $\boldsymbol{k}_{\mathrm{acnt}}$ is updated leading to a reinforced strategy. The better the vehicle compared to the inexperienced young driver, the more events are tolerated.

$d_{\mathrm{test,0}}$ – Another parameter influencing the usage strategy is the amount of testing distance, which will be run before the release for usage. As has already been cited, there

exists a rough prediction of Becker[219] that the Autobahn Pilot will need up to 10^8 km of testing using today's approaches. Therefore, this would be defined as the upper limit.

$$d_{\text{test},0} \coloneqq \{\dots, 10^8 \text{ km}\} \,. \tag{3-91}$$

However, besides taking this value from literature, two other approaches have been described. By assuming concrete values for each of the approach's parameters, further test distances for examining the usage strategy are simulated. On the one hand, the "prevention of less safety" leads to test distances by applying the defined safety performance benchmark $SP_{\text{bench,AwF}} = 5.92 \cdot 10^8$ km to equation (3-36) (see page 89)

$$d_{\text{test},0} \coloneqq \{\dots, 2.96 \cdot 10^7, 10^8\} \text{ km} \,. \tag{3-92}$$

On the other hand, the "monetary balance" approach can be evaluated when assigning values to $cpd_{\text{aRfU}}, bpd_{\text{aRfU}}, cpd_{\text{test}}$. The weighting factors[220] have been derived (section 1.4.1) to $\bar{C}_{\text{AwI}} = 32.9 \cdot 10^3$ € and $\bar{C}_{\text{AwF}} = 1.26 \cdot 10^6$ €. The monetary benefit during usage $bpd_{\text{aRfU}} \approx 0.522 \frac{€}{\text{km}}$ is approximated based on two reports. Dungs et al.[221] identified the value of time to be $16 \frac{€}{\text{h}}$ on average. Additionally, Follmer[222] identified time and distance used for mobility demand. The study identified the time it took the questioned to travel one kilometer $0.0326 \frac{\text{h}}{\text{km}}$. The cost for test driving is approximated by $cpd_{\text{test}} \approx 2.65 \frac{€}{\text{km}}$. This approximation assumes costs for the vehicles and costs for the test drivers (see appendix B). Other costs as post-processing are neglected because of the assumption that these would be alike the costs for supervision during the introduction phase. As the severity safety performance factor, today's values are used for the first best guess $a_{\text{S},SP} = \frac{SP_{\text{bench,AwI}}}{SP_{\text{bench,AwF}}} \approx 0.0209$. Thus, equation (3-44) is

$$d_{\text{test},0} = a_{d,\text{bal}} \cdot \frac{\bar{C}_{\text{AwI}} + a_{\text{S},SP}\bar{C}_{\text{AwF}}}{a_{\text{S},SP}(bpd_{\text{aRfU}} + cpd_{\text{test}})}. \tag{3-93}$$

The unknown distance factor for "monetary balance" $a_{d,\text{bal}}$ depends on the safety performance of the object under test SP_{OuT} (see Table 7) and is selected when relation

[219] Becker, J.: Toward Fully Automated Driving (2014), p. 16. Calculated assuming 50 km/h average velocity for Autobahn/Highway.

[220] At this point mistake is made when excluding certain level of severity. Nevertheless for the sake of simplicity the theory stays with two level of severity for explanation.

[221] Dungs et al.: The Value of Time (2016), p. 16. Further approaches for the USA and additional countries can be found in: Trottenberg, P.; Belenky, P.: Valuation of travel time in economic analysis (2011).

[222] Follmer, R. et al.: Mobilität in Deutschland 2008 (2010), p. 21.

(3-45) on page 91 is fulfilled. As long as the OuT has not more than k_{bal} events after testing the distance $d_{\text{test,0}}$, the OuT might be introduced into usage.

Table 9 Check for fulfillment of inequality (3-45) for the worst studied OuT

$a_{d,\text{bal}}$	k_{bal}	SP_{OuT}	λ_{bal}	$P_{\lambda_{\text{bal}}}(k > k_{\text{bal}})$
3	0	$0.1 \cdot 5.92 \cdot 10^8$ km	0.0233	4.42 %

Although the safety performance of the OuT is varying by a magnitude of two, the probability for more than 0 events using $a_{d,\text{bal}} = 3$ stays below 5 % for all OuT. Table 9 summarizes the calculation to check whether relation (3-45) is fulfilled. Consequently, the test distance $2.67 \cdot 10^6$ km is added for all of the SP_{OuT} assumptions.

Overall, three different approximations of test distances have been put in concrete terms and will be used for the examination of the usage strategy

$$d_{\text{test,0}} \coloneqq \{2.67 \cdot 10^6, 2.96 \cdot 10^7, 10^8\} \text{ km}. \tag{3-94}$$

Necessary Simulation parameter

t_{end} - For the current discussions, it is of interest how automated driving vehicles will affect road traffic. Therefore, one could evaluate the mean length of an automobile's safety life cycle. This is estimated in Germany 2013[223] with 8.7 years and constantly lengthened over the last years. However, for the technology of automated driving it is of greater interest how a usage strategy would influence the market penetration and thereby the whole traffic system. Therefore, the simulation will study the time span that other technologies needed to be fully deployed in the market

$$t_{\text{end}} = t_{\text{FulDep}} \coloneqq 30 \cdot \text{a}. \tag{3-95}$$

This value is taken from Figure 33 and represents the time that is necessary until the technology is fully deployed.

Δt – Figure 32 shows that the usage strategy results influence the next usage step by a limitation of velocity. As long as no new event occurs, the $SP_{\text{OuT,worst}}$ estimation improves and the velocity consequently increases. Thus, the last evaluation step influences the next evaluation step. This can be described by an ordinary differential equation and an initial value, as long as the tolerated number of events does not change. Due to the introduction of different usage strategies ("Detectors Limit", "Mobility Replacement" etc.), these tolerated numbers ($k_{\text{tol,a}}$) may change. Consequently, a numerical solution

[223] statista.de: Durchschnittliches Alter von Pkw in Deutschland 1960 bis 2016 (2016).

of the differential equations is necessary and the Euler method is applied[224]. Due to that reason, the outcome of the usage strategy is sensitive to Δt. The smaller the time step Δt, the more accurate the simulation, especially the self-reinforcing effects, are calculated. In appendix C it is shown that the maximum relative error of the cumulative distance traveled at the end of the simulation time $d_{\mathrm{cum}}(t_{\mathrm{FulDep}})$ is smaller than 10 % that might result in the worst-case scenario if $\Delta t < 0.4$ h. The worst-case is designed by choosing the longest overall simulation time as well as the biggest gradient possible at this point in time. This worst-case might change when different usage strategies are defined. During real-world application of the theory, the value for Δt should be chosen much smaller than this value because the computation time is irrelevant. For simulation during this thesis, $\Delta t = 2.5$ h is chosen to reduce computation time.

3.6.3 Usage Strategy Simulation Evaluation Criteria

The parameter space is reduced to a four dimensional space by the parameter assignment above, see Figure 36. The assumption on the safety performance of the OuT is one parameter (SP_{OuT}). The other three parameters define the usage strategy: $d_{\mathrm{test,0}}$ defines the test distance ahead of introduction. Hidden behind the parameter $\boldsymbol{k}_{\mathrm{tol,a}}$ is the method that derives the tolerated number M-k_{tol} of events as well as the detector limit $\boldsymbol{k}_{\mathrm{detL}}$.

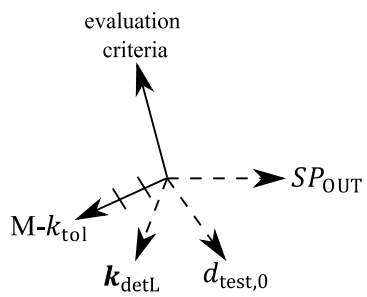


Figure 36 Parameter space for parameter study

When each of the assigned values of the four parameters is combined fully factorial, $3 \cdot 3 \cdot 3 \cdot 4 = 108$ simulations result. To identify the effect of these parameters, the results of the usage simulation need to be comparable. Therefore, the results of the simulation over several time spans are condensed to numeric values for discussion. What criteria make the usage strategy evaluable given different assumptions ($\boldsymbol{SP}_{\mathrm{OuT}}$) and definitions (M-$k_{\mathrm{tol}}$, $\boldsymbol{k}_{\mathrm{detL}}$, $d_{\mathrm{test,0}}$)?

The usage strategy itself takes care that the requirements of users and the society are fulfilled. Consequently, as long as the observed world follows the prerequisites, the

[224] Dahmen, W.; Reusken, A.: Numerik für Ingenieure (2006), p. 386.

requirements cannot be taken as evaluation criteria. Given the reality simulation explained in Figure 32, the prerequisites are fulfilled by definition.[225]

However, when having safety in focus, the results of different usage strategies are evaluated in comparison to different usage demands (ψ_{ud}). To study how a change of parameter values (M-$k_{\mathrm{tol}}, \boldsymbol{k}_{\mathrm{detL}}, d_{\mathrm{test,0}}$) changes the usage strategy outcomes, a worse and better outcome is identified and formalized by numeric values. These numeric values are defined for two time spans. First the introduction phase $\Delta t_{\mathrm{intro}}$ and second the supervision phase Δt_{suvi}.

Evaluation criteria for $\Delta t_{\mathrm{intro}}$

Firstly, to evaluate the strategy the usage time with high uncertainty is analyzed. This time begins with t_{RfU} and ends at t_{PoS}. Before t_{RfU}, the test drivers reduce the uncertainty on safety. After t_{PoS}, enough data is available that reduces uncertainty about the safety performance of the OuT SP_{OuT} in comparison to a benchmark. In between, the usage following the strategy is compared with different alternatives. To develop evaluation criteria, three extreme cases with different OuT's performance are discussed:

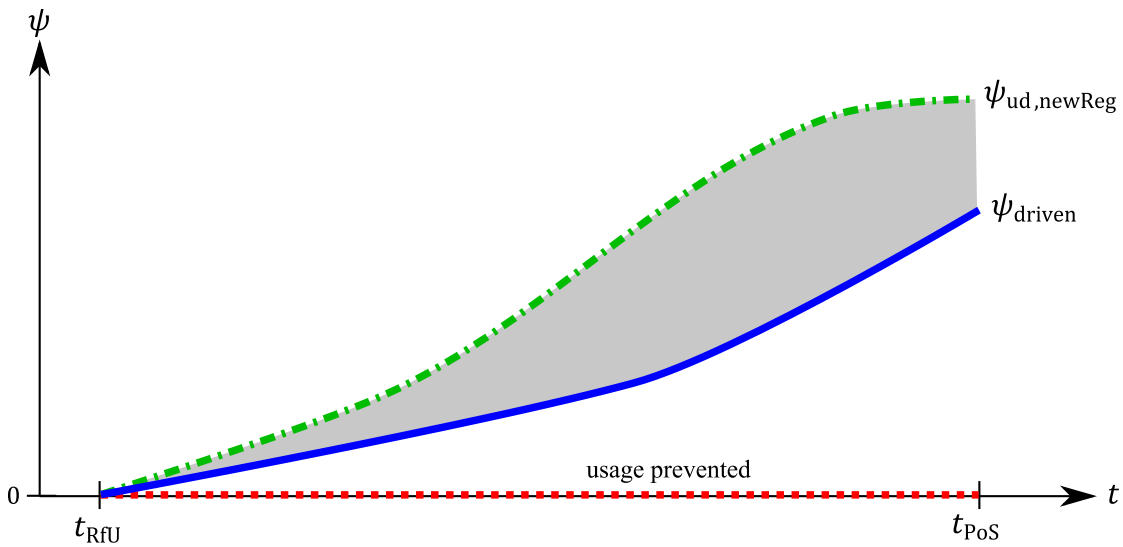


Figure 37 Qualitative example to derive the evaluation criteria for the case of a better OuT

- The OuT is as good as or better than the benchmark – A good usage strategy would hinder the usage of the OuT as *little* as possible compared to an unlimited registration of new vehicles.

[225] Attention: This changes when real vehicles that drive in reality are examined.

The first criterion is formalized by comparing the distance driven due to the usage demand of newly registered vehicles $d_{\mathrm{ud,newReg}}(t_{\mathrm{PoS}})$ with the distance driven due to the strategy's limitation $d_{\mathrm{driven}}(t_{\mathrm{PoS}})$ (see light gray area in Figure 37).

The gray area (called RvD: newly Registered vs. Driven) is describable with two values. On the one hand, this area represents a loss in automated driving kilometers Δd_{RvD} that users suffer when the strategy limits the usage below the demanded values.

$$\Delta d_{\mathrm{RvD}} = \sum_{t_i=t_{\mathrm{RfU}+1}}^{t_{\mathrm{PoS}-1}} \begin{cases} \left(\psi_{\mathrm{driven}}(t_i) - \psi_{\mathrm{ud,newReg}}(t_i)\right)\Delta t(t_i) & \text{if } \psi_{\mathrm{driven}} < \psi_{\mathrm{ud,newReg}} \\ 0 & \text{if } \psi_{\mathrm{driven}} \geq \psi_{\mathrm{ud,newReg}} \end{cases} \tag{3-96}$$

On the other hand, it depends also on the performance of the OuT whether it is good to have the blue solid line closer to the upper or lower line in Figure 37. For that reason, the performance vector of the OuT $\boldsymbol{SP}_{\mathrm{OuT}}$ and the performance of the benchmark $\boldsymbol{SP}_{\mathrm{bench}}$ are used for evaluation. These values and $\Delta d = \Delta d_{\mathrm{RvD}}$ are used to define an average delta in events as the evaluation criteria

$$\Delta \boldsymbol{k}(\Delta d) = \boldsymbol{k}_{\mathrm{bench}}(\Delta d) - \boldsymbol{k}_{\mathrm{OuT}}(\Delta d) = \begin{bmatrix} \dfrac{\Delta d}{SP_{\mathrm{bench,AwI}}} \\ \dfrac{\Delta d}{SP_{\mathrm{bench,AwF}}} \end{bmatrix} - \begin{bmatrix} \dfrac{\Delta d}{SP_{\mathrm{OuT,AwI}}} \\ \dfrac{\Delta d}{SP_{\mathrm{OuT,AwF}}} \end{bmatrix}. \tag{3-97}$$

The closer to zero $\Delta \boldsymbol{k}(\Delta d_{\mathrm{RvD}})$ the lower is the hindrance due to the strategy. If the OuT is better than its benchmark, the safety change gets negative as the strategy prevents the technology to reduce the number of accidents ("lost safety").

Actually, $\Delta \boldsymbol{k}(\Delta d_{\mathrm{RvD}})$ is a vector and consists of independent numbers. The different level of severity can be weighted (see section 1.4.1) to define one indicator value that expresses the average change in safety due to the usage strategy in a monetary way[226]

$$C_{\mathrm{RvD}} = [\bar{C}_{\mathrm{AwI}} \quad \bar{C}_{\mathrm{AwF}}] \cdot \Delta \boldsymbol{k}(\Delta d_{\mathrm{RvD}}). \tag{3-98}$$

$$C_{\mathrm{all}} = [\bar{C}_{\mathrm{AwI}} \quad \bar{C}_{\mathrm{AwF}}] \cdot \boldsymbol{k}_{\mathrm{all,a}} \cdot \frac{\Delta t_{\mathrm{intro}}}{\mathrm{a}}. \tag{3-99}$$

To judge whether this is a high number or not, it is related to the accident costs generated by all registered vehicles during this time span $\Delta t_{\mathrm{intro}}$

[226] Attention: As already discussed, the monetary assessment is simplified. Only costs due to accident events for two level of severity are under consideration. What misses are further level of severity as accidents without personal injury. Above that, also congestion, valuable lifetime etc. due to automated driving will change additional cost factors.

$$r_{\mathrm{C,RvD}} = \frac{C_{\mathrm{RvD}}(\Delta d_{\mathrm{RvD}})}{C_{\mathrm{all}}}. \tag{3-100}$$

The same approach is used for the formalization of sentence two.

- The OuT is as good as an inexperienced young driver – A good usage strategy would hinder better users but satisfy individual mobility demands for people with mobility limitations.

Equation (3-96) is adapted and now describes the distance that is missing to satisfy the demand of mobility limited groups (equation (3-101)).

$$\Delta d_{\mathrm{LvD}} = \sum_{t_i=t_{\mathrm{RfU}+1}}^{t_{\mathrm{PoS}-1}} \begin{cases} \left(\psi_{\mathrm{driven}}(t_i) - \psi_{\mathrm{ud,ml}}(t_i)\right)\Delta t(t_i) & if\ \psi_{\mathrm{driven}} < \psi_{\mathrm{ud,ml}} \\ 0 & if\ \psi_{\mathrm{driven}} \geq \psi_{\mathrm{ud,ml}} \end{cases} \tag{3-101}$$

For explanation this is depicted as the black area (called LvD: mobility Limited vs. Driven) in Figure 38.

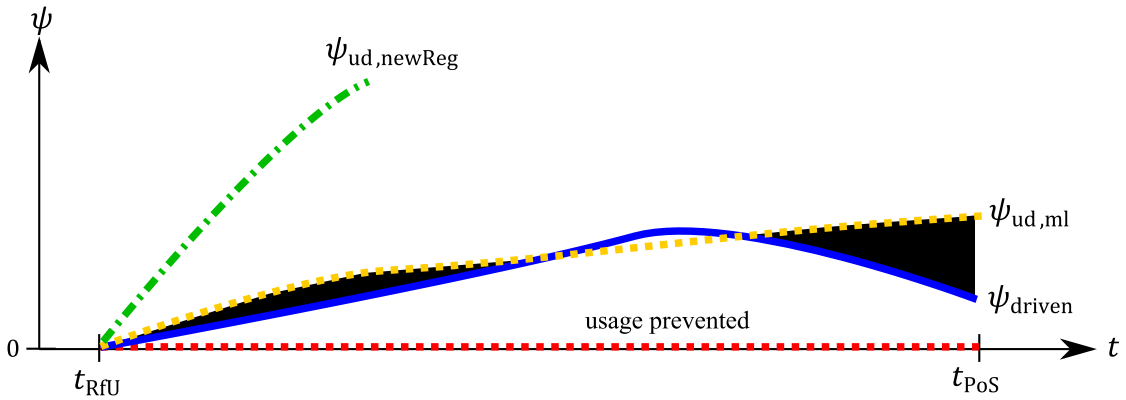


Figure 38 Qualitative example to derive the evaluation criteria for the case of a OuT being as good as a young inexperienced driver

To get an idea how much the usage strategy hinders AD3+ usage, this delta is related to the total demand of mobility limited people until the PoS.

$$r_{d,\mathrm{LvD}} = \frac{\Delta d_{\mathrm{LvD}}}{\sum_{t_i=t_{\mathrm{RfU}+1}}^{t_{\mathrm{PoS}-1}} \psi_{\mathrm{ud,ml}}(t_i)\Delta t(t_i)} \tag{3-102}$$

This value describes the theoretically available mobility, provided by automated driving in relation to the demanded of the mobility limited people. Whether these people use the automated driving vehicles or not is not discussed. This is left open for a political discussion whether a certain preferential treatment of limited people will be enforced.
For the formalization of sentence three, the figure is adapted again.

- The OuT is worse than an inexperienced young driver – A good strategy would protect the society by hindering the mass usage compared to the unlimited introduction.

Figure 39 illustrates: if the usage is unlimited ($ER = 1$), thus no strategy exists to limit the usage, the proof of less safety would have occurred earlier $t_{\mathrm{PoS,ud}} \leq t_{\mathrm{PoS}}$. The area, respectively the traveled distance below the green (dash-dotted) line until $t_{\mathrm{PoS,ud}}$, is equal to the area below the blue (solid) line. This is due to the fact that the same number of kilometers (d_{proof}) needs to be collected to come to the proof of safety no matter how fast it is collected.

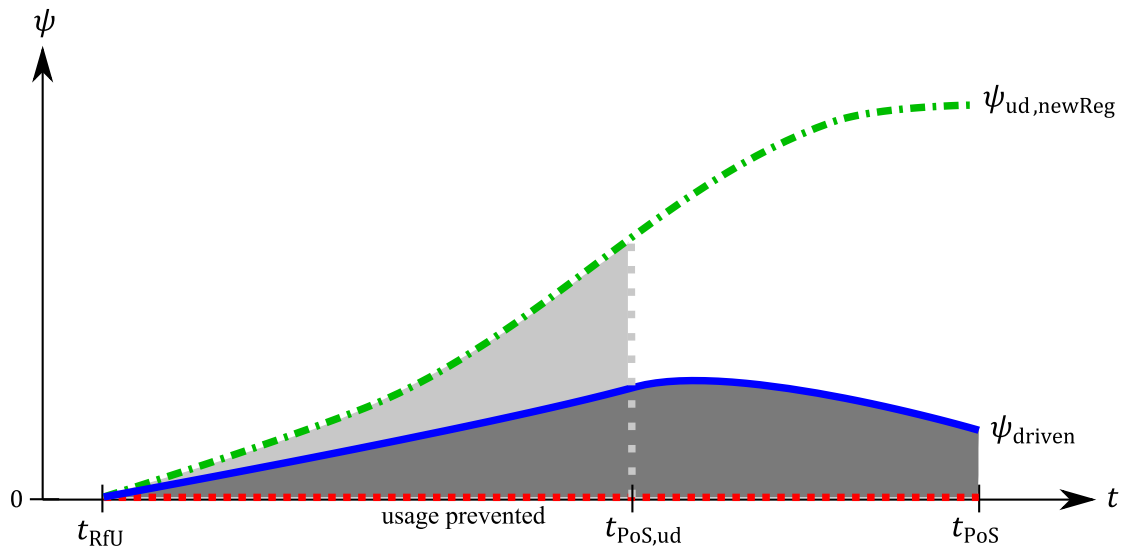


Figure 39 Qualitative example to derive the evaluation criteria for the case of a worse OuT

Consequently, the velocity of the unlimited introduction might be different compared to the one driven. If the unlimited introduction leads to higher velocities, the tolerated number of events by society needs to be higher as well. As this would contradict the requirement of the society, the ratio between the different limitations is derived as another indicator. Thus, the third sentence is formalized by describing the ratio between the maximum velocities

$$r_{\psi} = \frac{\max\limits_{t_i \in [t_{\mathrm{RfU}}, t_{\mathrm{PoS,ud}}]} \psi_{\mathrm{ud,total}}(t_i)}{\max\limits_{t_i \in [t_{\mathrm{RfU}}, t_{\mathrm{PoS}}]} \psi_{\mathrm{driven}}(t_i)}. \tag{3-103}$$

Be aware that the time span for the search of a maximum is different for denominator and numerator. The maximum of both time spans is chosen to evaluate the strategy because this ratio expresses how much the strategy hinders the usage and thereby protects the society. Thus: the bigger the r_{ψ} the better the usage strategy.

These criteria described by equations (3-98) to (3-103) are theoretically derived and condense the information gained by the simulation. From my point of view, a weighting

of these criteria to derive one single evaluation criteria value is not reasonable. The reason for that are the different units as well as the challenge to compare the monetary value of time and the monetary value of health. Additionally, further evaluation criteria should be considered depending on the point of view and the information about the real usage of the vehicles.

Evaluation criteria for Δt_{suvi}

Secondly, the usage time after the proof of higher or lower safety is analyzed. What are the characteristics of a usage strategy that would motivate a further limitation of the usage? The criteria that formalize this motivation are still derived from the goal to improve road traffic safety. The following three criteria are identified:

- The OuT is as good or better as the benchmark – The usage of automated vehicles doesn't need to be hindered compared to the known usage demand from today's registration numbers.

To evaluate the criteria, an evaluation time span has to be defined. Therefore, the time is studied where a usual technology would need to be fully deployed to the whole existing market t_{FulDep}.

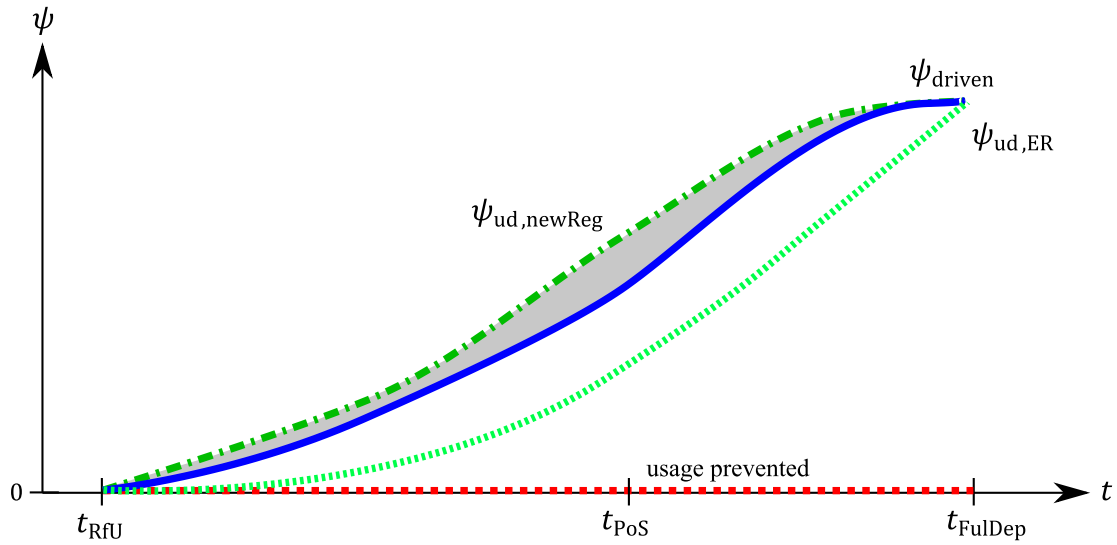


Figure 40 Area that expresses the first criteria for evaluation after PoS in the ψt-diagram

The first criterion is formalized by calculating the area marked light-gray in Figure 40

$$\Delta d_{\mathrm{RvD,total}} = \sum_{t_i=t_{\mathrm{RfU}+1}}^{t_{\mathrm{FulDep}}} \left(\psi_{\mathrm{driven}}(t_i) - \psi_{\mathrm{ud,newReg}}(t_i)\right) \Delta t(t_i) \tag{3-104}$$

This delta in distance $\Delta d = \Delta d_{\mathrm{RvD,total}}$ results in a delta of events $\Delta \boldsymbol{k}(\Delta d_{\mathrm{RvD,total}})$ that occurs given the safety performance values for the benchmark and the OuT and applying equation (3-97). This delta in events is translated to accompanied costs by the known weighting factors

$$\Delta C_{\mathrm{total}}(\Delta d_{\mathrm{RvD,total}}) = [\bar{C}_{\mathrm{AwI}} \quad \bar{C}_{\mathrm{AwF}}] \cdot \Delta \boldsymbol{k}(\Delta d_{\mathrm{RvD,total}}) \,. \tag{3-105}$$

The more negative this delta, the more costs have not been omitted due to the hindrance of the strategy.

- The OuT is as good as a young and inexperienced driver – The usage should be enabled for people suffering mobility limitations whereas more usage should be hindered.

To formalize the second criterion, the gray area in Figure 41 is determined by

$$\Delta d = \sum_{t_i=t_{\mathrm{RfU}+1}}^{t_{\mathrm{FulDep}}} \begin{cases} \left(\psi_{\mathrm{ud,ml}}(t_i) - \psi_{\mathrm{driven}}(t_i)\right) \Delta t(t_i) & \text{if } \psi_{\mathrm{driven}} < \psi_{\mathrm{ud,ml}} \\ 0 & \text{if } \psi_{\mathrm{driven}} > \psi_{\mathrm{ud,ml}} \end{cases} . \tag{3-106}$$

This area, representing the delta in distance, is put into ratio with the dotted area representing the total demand of the mobility limited people. This ratio is defined by

$$r_{\mathrm{d,ml}} = \frac{\Delta d}{\sum_{t_i=t_{\mathrm{RfU}+1}}^{t_{\mathrm{FulDep}}} \psi_{\mathrm{ud,ml}}(t_i) \Delta t(t_i)} . \tag{3-107}$$

The closer this ratio is to zero, the less usage demand of the mobility limited people has been omitted by the strategy.

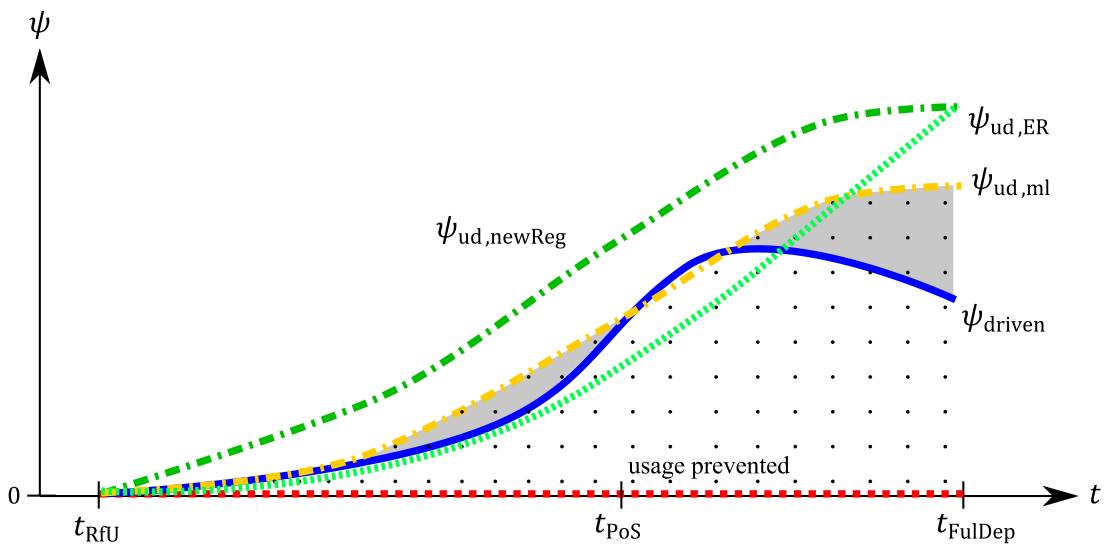


Figure 41 Areas that express the second criteria for evaluation after PoS in the ψt-diagram

- The OuT is worse compared to a young and inexperienced driver – The usage should be hindered as much as possible.

The last criterion represented by the light gray area in Figure 42 is formalized by

$$d = \sum_{t_i=t_{\mathrm{RfU}+1}}^{t_{\mathrm{FulDep}}} \psi_{\mathrm{driven}}(t_i)\Delta t(t_i). \tag{3-108}$$

This distance is translated in a delta of events

$$\Delta \boldsymbol{k}(d) = \frac{d}{\boldsymbol{SP}_{\mathrm{bench}}} - \frac{d}{\boldsymbol{SP}_{\mathrm{OuT}}} \tag{3-109}$$

and respectively to a difference in costs

$$C_{\mathrm{driven}} = [\bar{C}_{\mathrm{AwI}} \quad \bar{C}_{\mathrm{AwF}}] \cdot \Delta \boldsymbol{k}(d). \tag{3-110}$$

The closer this value is to zero, the less additional costs have been introduced by letting a less safe vehicle drive in real traffic.

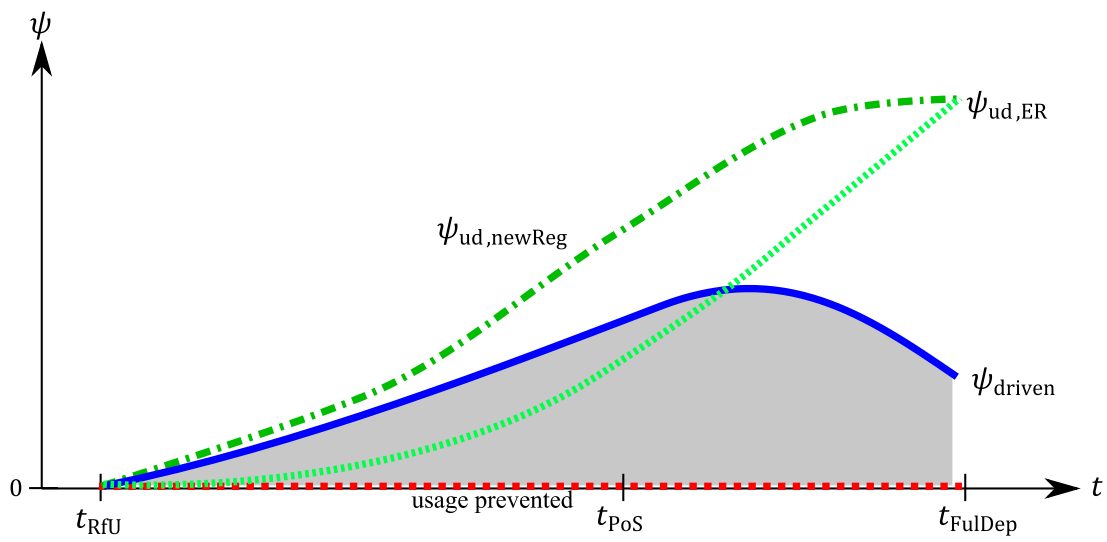


Figure 42 Area that expresses the third criteria for evaluation after PoS in the ψ-t-diagram

3.6.4 Usage Strategy Simulation Result Analysis

A stochastic process for the occurrence of accidents and vehicle safety performance has been defined. Based on this, the users' as well as the society's requirements have been discussed and a possible formalization has been given. To fulfill these requirements, different usage strategies have been proposed. To study these strategies, the necessary definitions and assumptions are concretized for the German Autobahn-Pilot of 2013. Based on these definitions and assumptions, the introduction is simulated 108-times,

thus fully factorial. To explain the effect of the changed parameters on the simulation, first a selection of simulations is studied in detail and second the evaluation criteria are compared for all 108 simulations.

Exemplary Explanation of Simulation Results

An each-once combinatory is exemplarily studied. Three out of four parameters are kept constant and one is changed from simulation to simulation. $3 + 3 + 3 + 4 = 13$ simulations of the 108 simulations are therefore discussed in detail. Given the evaluation criteria defined above, the driven velocity ($\psi_{\mathrm{driven}}(t)$[227]) and the safety performance estimation ($SP_{\mathrm{OuT,worse}}(t)$) are the two main results from simulation. These two main results are now discussed for the 13 simulations in four sets. First, $d_{\mathrm{test,0}}$ is varied (3 simulations – set 1), then M-k_{tol} is varied (3 simulations – set 2), then k_{detL} is varied (3 simulations – set 3), and lastly SP_{OuT} is varied (4 simulations – set 4).

$d_{test,0}$ is varied – the other parameters are kept constant:

The first result, the velocity in every simulation step, is depicted in Figure 43. The double logarithmic scale is chosen because of the broad velocity range (y-scale) that covers 30 years and the importance of the first years (x-scale) for the usage strategy.

[227] Velocity ψ in this context is still the average yearly velocity (incl. standstill while parking or the time outside a use case). It must not be confused with the average velocity during usage $\bar{v}$. For comparison, equation (3-75) calculated $\psi_{\mathrm{1Veh,AB}} \approx 0.456\ \frac{\mathrm{km}}{\mathrm{h}}$ for one vehicle in Germany 2013. Thus, the number of automated driving vehicles can be approximated by $N_{\mathrm{AD}} \approx 2 \cdot \psi$. The whole vehicle fleet $N_{\mathrm{all}} \approx 56.13 \cdot 10^6$ drove $\psi_{\mathrm{ud,all}} \approx 25.58 \cdot 10^6\ \frac{\mathrm{km}}{\mathrm{h}}$ (see equation (3-76) on page 106).

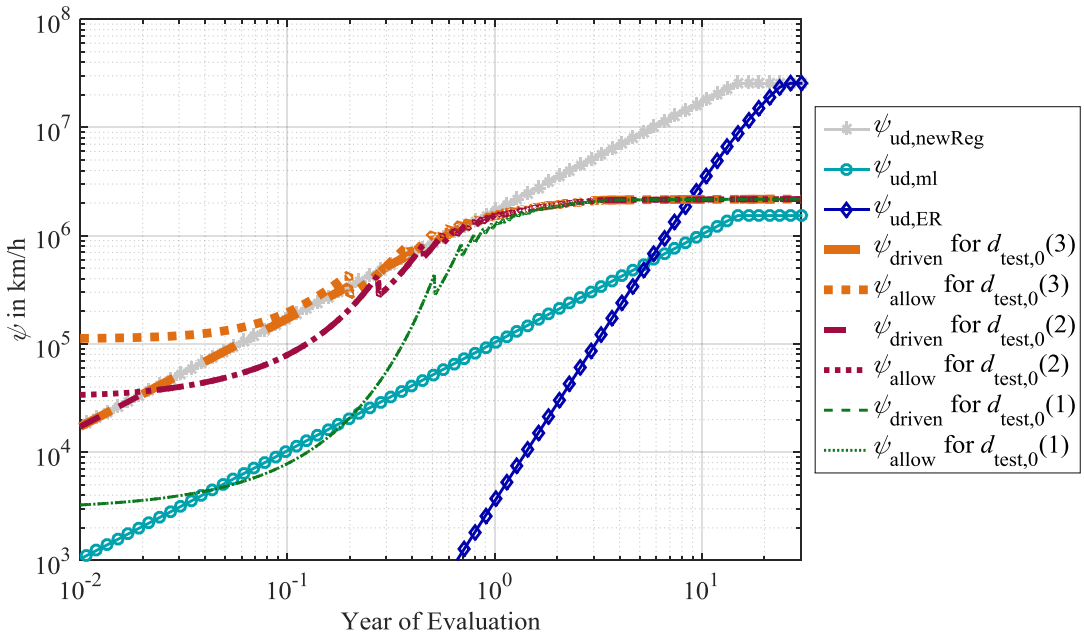


Figure 43 Simulation result ψ over t for $\boldsymbol{SP}_{\text{OuT}} = 1.34 \cdot \boldsymbol{SP}_{\text{bench}}$ and M-k_{tol} = "Detector's Limit", $\boldsymbol{k}_{\text{detL}} = [1216; 39]$ and $d_{\text{test,0}} := \{2.67 \cdot 10^6, 2.96 \cdot 10^7, 10^8\}$ km

The usage demands $\psi_{\text{ud,newReg}}, \psi_{\text{ud,ml}}, \psi_{\text{ud,ER}}$ are not sensitive to the parameter combinations that are simulated, thus these values are reference figures for all 13 simulations. To recapitulate, the velocity $\psi_{\text{ud,newReg}}$ expresses the usage demand of newly registered vehicles. The velocities $\psi_{\text{ud,ER}}$ result when assuming equipment ratios as explained in 3.6.2. $\psi_{\text{ud,ml}}$ represents the usage demand when assuming a certain mobility limitation.

ψ_{allow} and ψ_{driven} are the values that are sensitive to the parameter combinations. The allowed velocity ψ_{allow} is defined by equation (3-60) and updated every evaluation. For the simulation, the driven velocity is defined as follows

$$\psi_{\text{driven}}(t) = \min\left(\psi_{\text{ud,newReg}}, \psi_{\text{allow}}\right) \tag{3-111}$$

The three parameter combinations in Figure 43 differ in the test distance driven ahead of introduction $d_{\text{test,0}}$. Please have a closer look at ψ_{driven} and ψ_{allow}. At several points in Figure 43, the lines lie on top of each other. Due to the line style the lines are distinguishable. As an exemplary qualitative interpretation, the following conclusions can be drawn that are similar for the three parameter combinations:

- Before year 9, the strategy would not hinder the introduction compared to the deployment given an equipment ratio like assumed above. This conclusion is derived from Figure 43: the line (blue-diamond) for $\psi_{\text{ud,ER}}$ is below the lines (green, red and orange-dashed) for ψ_{driven}.

- The driven velocities ψ_{driven} approach similar values for all three parameter combinations.
- The upper limitation of ψ_{driven} reached approximately 1/10 of the total mobility demand of today registered vehicles. A maximum velocity is reached for which the tolerated event numbers will not be exceeded, given a certain worst-case estimation of the safety performance $SP_{\text{OuT,worst}}$.
- Comparing the allowed velocity (ψ_{allow}) with the demanded velocity by newly registered vehicles ($\psi_{\text{ud,newReg}}$), the further introduction is hindered after one year, no matter which strategy is used.

By changing the driven distance ahead of introduction ($d_{\text{test,0}}$), the following changes result and are derived from Figure 43:

- The mobility demand of mobility limited people would be fulfilled during the whole examination time frame, except a little portion for the smallest testing distance. The line (turquoise-circle) for $\psi_{\text{ud,ml}}$ is nearly always below the line for ψ_{driven}.
- The higher $d_{\text{test,0}}$, the higher $\psi_{\text{allow}}(0)$. Consequently, the longer the usage demand of newly registered vehicles ($\psi_{\text{ud,newReg}}$) can be fulfilled.
- Parameter combination one with $d_{\text{test,0}}(1) = 2.67 \cdot 10^6$ km is limiting the usage from $t \approx 1.7 \cdot 10^{-3}$ a ≈ 15 h on (out of scope). The two lines (green-dashed) ψ_{driven} and (green-dotted) ψ_{allow} are below $\psi_{\text{ud,newReg}}$.
- The same happens later at $t \approx 2 \cdot 10^{-2}$ a for parameter combination two with $d_{\text{test,0}}(2) = 2.96 \cdot 10^7$ km. For this combination the hindrance is smaller.

Figure 44 presents the second result, being the safety performance values SP over time. The depicted group of lines represents the evolution of the fatal accident level of severity. A similar group of lines exists for the discussion of accidents with injuries. Not sensitive to any parameter combination is the defined benchmark SP_{bench} (black-solide). This is the reference for all simulations studied.

In this set of simulations, also the assumed safety performance of the object under test is not changing SP_{OuT}. The black-dashed line is the value to which the best- and worst-case estimations converge to.

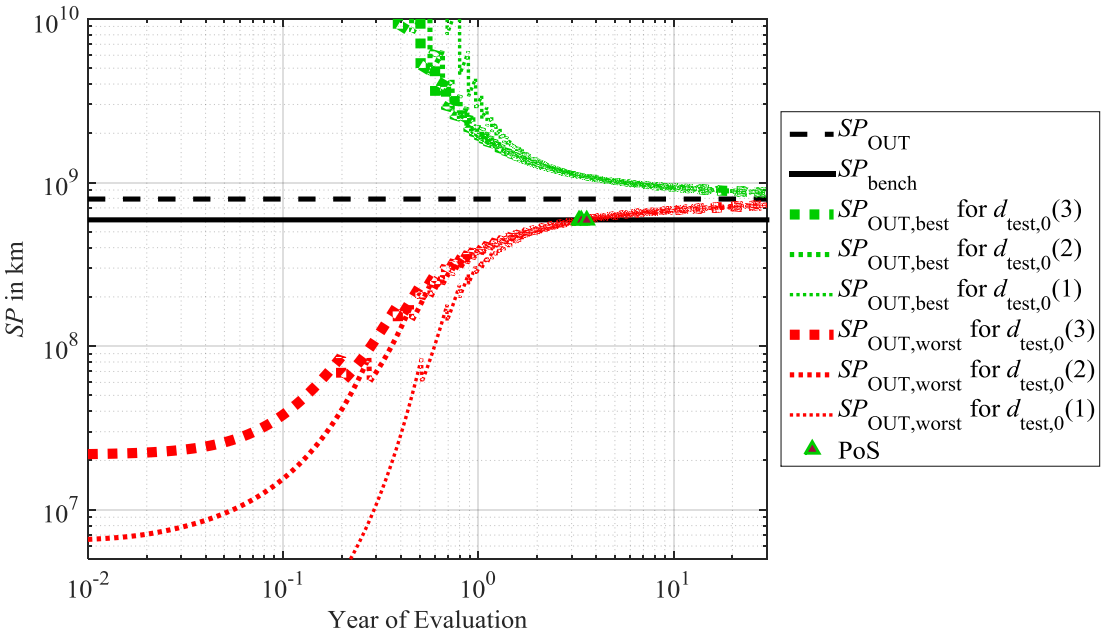


Figure 44 Simulation result SP_{AwF} over t for $\boldsymbol{SP}_{\mathrm{OuT}} = 1.34 \cdot \boldsymbol{SP}_{\mathrm{bench}}$ and M-k_{tol} = "Detector's Limit", $\boldsymbol{k}_{\mathrm{detL}} = [1216; 39]$ and $d_{\mathrm{test,0}} := \{2.67 \cdot 10^6, 2.96 \cdot 10^7, 10^8\}$ km

Conclusions that are the same for the three parameter combinations:

- The light-green best-case estimation $SP_{\mathrm{OuT,best}}$ converges from above against the assumed safety performance SP_{OuT}.
- The red worst-case estimation $SP_{\mathrm{OuT,worst}}$ converges from below against the assumed safety performance SP_{OuT}.
- The best- and worst-case estimations are not steadily increasing or decreasing. As long as no further event occurred, the worst-case estimation of the SP leads to higher safety performance values (e-function shape). Once a new event occurred, this estimation is corrected. The fact that events are discrete occurrences leads to the unsteady line for the SP estimations. The speed ψ_{allow} calculation of equation (3-60) depends on the worst-case estimation, thus also the allowed speed is unsteady (see Figure 43 above).
- The more distance has been driven, the smaller the safety performance uncertainty. The factor $\frac{SP_{\mathrm{OuT,worst}}}{SP_{\mathrm{bench}}}$ for accident with fatalities is approximately 0.0367 after testing $d_{\mathrm{test,0}} = 10^8$ km ($t = 0$). Whereas when testing $d_{\mathrm{test,0}} = 2.67 \cdot 10^6$ km the factor reduces to 0.00098. For comparison[228], the ratio for accident with *personal injury* per distance (Apd) when driving a car compared to driving a motorbike is

[228] Caution: Accidents with fatality per distance of motorbikes is not reported in standard statistics for comparison.

$0.191 \approx 1/5$ in Germany[229] 2013. When comparing fatalities per distance (Ipd), a factor of $0.0652 \approx 1/15$ results[229].

- The worst-case estimations cross the benchmark line, thus a proof of higher safety is given indicated by upwards directing triangles. Depending on the test distance, the PoS is reached earlier or later in the fourth year of usage.
- The more distance has been driven ahead of introduction, the earlier the proof of safety is given. But in this case the necessary distance for the proof of safety is orders of magnitude higher than the testing distance. Consequently, the difference at the time of the proof is small. In these three simulations, the main distance for the proof is collected during usage.

M-k_{tol} *is varied – the other parameters are kept constant:*

For the set of simulations studied now, the method how to derive the tolerated number of events is varied. The speed over time result is depicted in Figure 45. The usage demand velocities haven't changed and can be seen as the reference. What hasn't changed either is the simulation that uses the "Detector's Limit" approach (green-thinnest line). The comparison of this simulation to the other leads to:

- All simulations start with similar allowed speeds ψ_{allow}. This is reasonable as on the one hand the safety account realizes no delta in events, as no events have occurred. On the other hand, the mobility replacement leads to little more tolerated events as the worst-case estimation is orders of magnitude lower than the reference at the beginning of simulation.
- After approximately two months, the difference between the approaches gets visible in the logarithmic plot.
- The approach following the "Special Needs Safety Account" (broadest-orange) follows the usage demand of mobility limited people as soon as the events due to this usage demand get significant in comparison to the event numbers of the detector limit k_{detL}. The allowed speed has a positive offset to the usage demand of mobility limited people due to the higher safety performance of the object under test compared to the inexperienced young driver.

[229] Kühn, M.: Motorradunfälle in Deutschland (2016), p. 10.

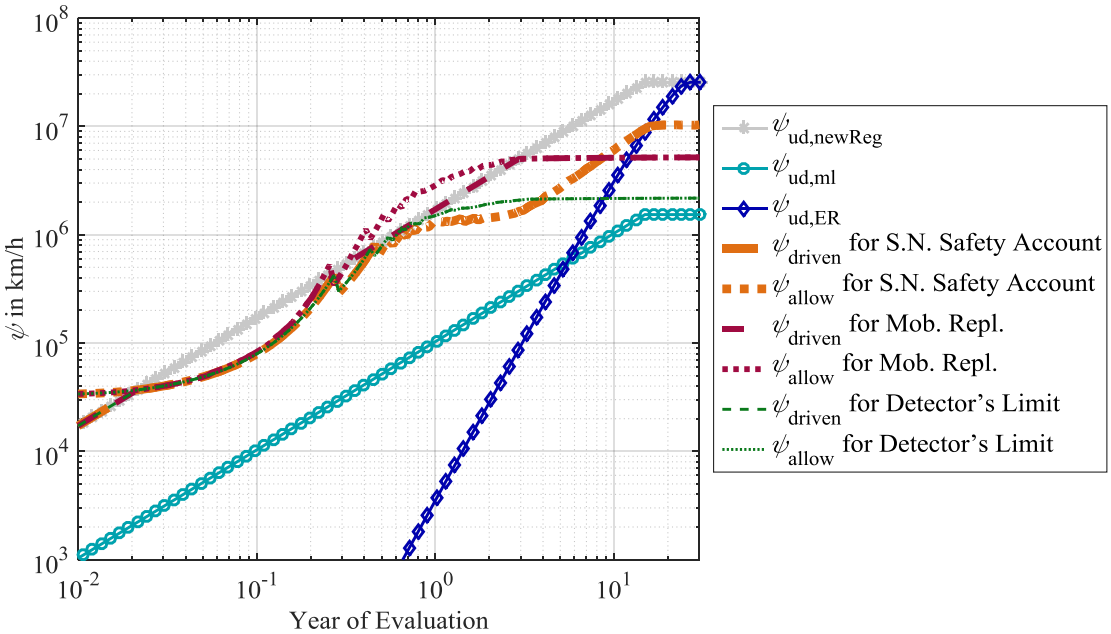


Figure 45 Simulation result ψ over t for $\boldsymbol{SP}_{\mathrm{OuT}} = 1.34 \cdot \boldsymbol{SP}_{\mathrm{bench}}$ and M-k_{tol} ={"S.N. Safety Account", "Mob. Repl.", "Detector's Limit"}, $\boldsymbol{k}_{\mathrm{detL}} = [1216; 39]$ and $d_{\mathrm{test},0} := 2.96 \cdot 10^7$ km

Especially during the first year of usage, the driven velocities are close together for all three simulations. This is reflected in the second result depicted in Figure 46. The safety performance worst-case estimation for the first year seems to be the same for all three simulations. The zoom on the right side of Figure 46 shows the worst-case safety performance estimation for the "Special Needs Safety Account" during the proof of higher safety.

- For these simulation parameters, the proof of safety is firstly reached by the "Mobility replacement", then by the others.
- The zoom shows the unsteady line that result from the discrete events.
- Due to this unsteady course, the proof of safety or less safety needs to be combined with a hysteresis or a smoothing filter to avoid alternating safety statements.

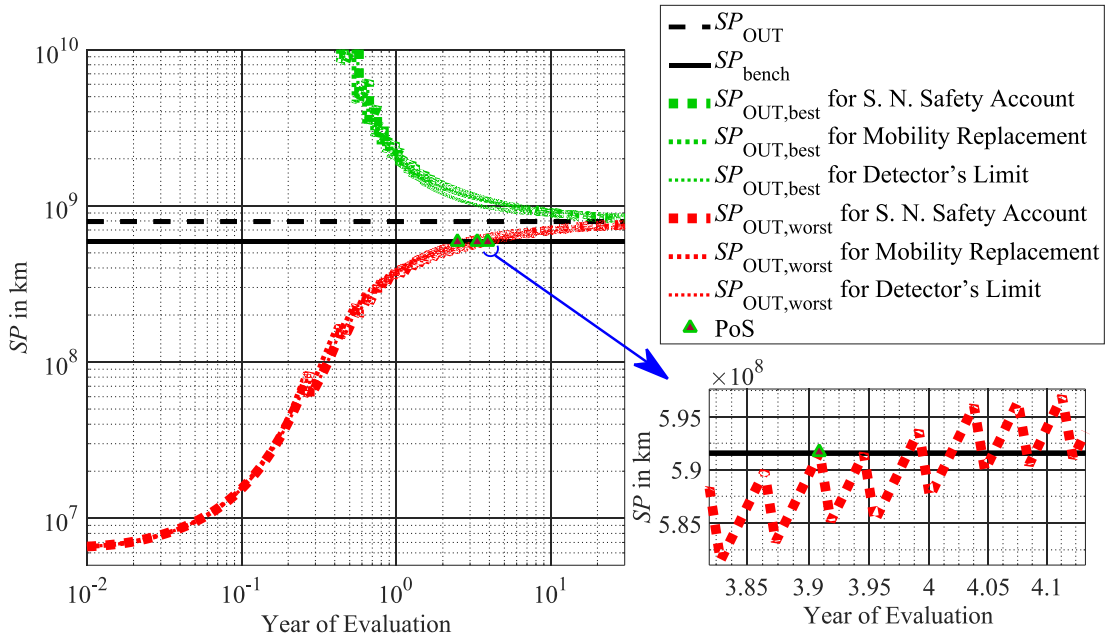


Figure 46 Simulation result SP_{AwF} over t for $\boldsymbol{SP}_{\mathrm{OuT}} = 1.34 \cdot \boldsymbol{SP}_{\mathrm{bench}}$ and M-k_{tol} ={"S.N. Safety Account", "Mob. Repl.", "Detector's Limit"}, $\boldsymbol{k}_{\mathrm{detL}} = [1216; 39]$ and $d_{\mathrm{test,0}} := 2.96 \cdot 10^{7}$ km.

k_{detL} is varied – the other parameters are kept constant:

A major parameter affecting the introduction is the number of events that are defined as the detector's limit k_{detL}. In subsection 3.4.2, the detector's limit is derived for the society's safety detector from the standard deviation of the trend of yearly counted accidents with fatalities on Autobahn. This limit as well as two alternatives were simulated $k_{\mathrm{detL,wF}} = \{0, 3, 39\}$. For these combinations, the method to derive the tolerated numbers is the "Detector's Limit". The simulation outcome is illustrated in Figure 47. The three different simulations vary significantly:

- If k_{detL} is zero, the introduction and usage is hindered the most. Figure 47 does not even show the line for these values as it does not increase above the level of 1000 km/h after 30 years. Therefore, less than 2000 vehicles are negligible within the fleet of over $50 \cdot 10^{6}$ vehicles in Germany after 30 years.
- For $k_{\mathrm{detL}} = 3$ the usage demand assumed based on a regular equipment ratio could be satisfied for approximately half a year. Later in time, the limitation still increases but strongly hinders the usage. Overall, the line (red-medium) would converge to a value below the usage demand of mobility limited people.
- The third line of $k_{\mathrm{detL}} = 39$ is known from the two simulation sets from above. With this number of tolerated events, the demand of mobility limited could be fulfilled. However, the registration or activation of further demanded AD3+ vehicles would be hindered.

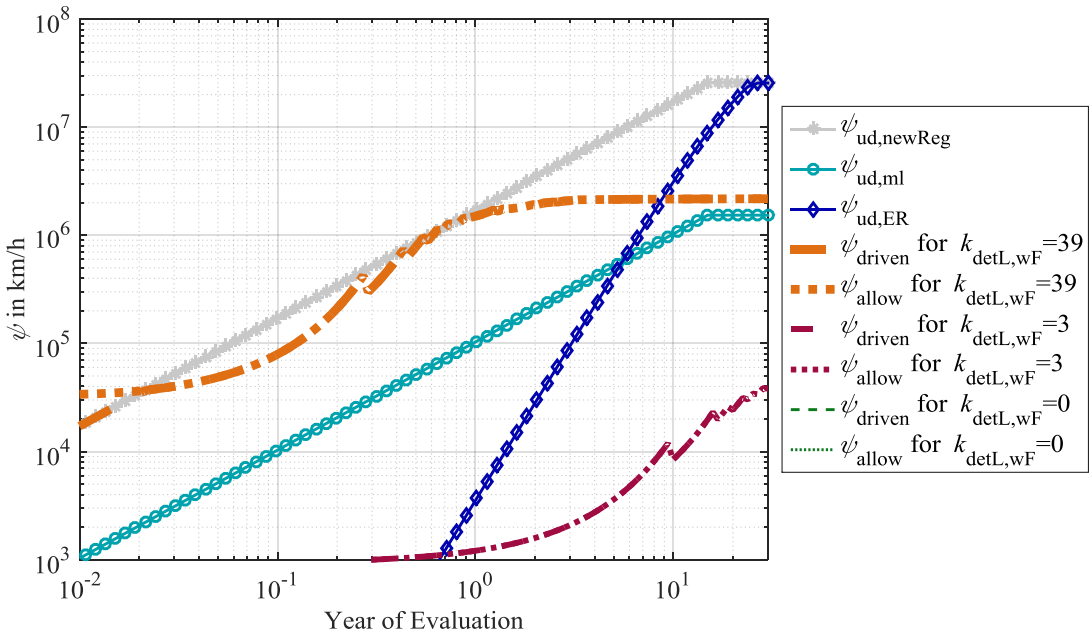


Figure 47 Simulation result ψ over t for $\boldsymbol{SP}_{\mathrm{OuT}} = 1.34 \cdot \boldsymbol{SP}_{\mathrm{bench}}$ and M-k_{tol} = "Detector's Limit", $k_{\mathrm{detL,wF}} = \{0, 3, 39\}$ and $d_{\mathrm{test,0}} := 2.96 \cdot 10^7$ km

The estimation of the worst-case safety performance only improves when additional information, thus additional distance and events are collected. Consequently, the safety performance estimation for the same object under test is sensitive to k_{detL}:

- If only minimal additional distance is driven, the estimation does not change. For $k_{\mathrm{detL,wF}} = 0$ the line (red-thinnest) depicts that. All estimations start at the same level as the test distance ahead of introduction $d_{\mathrm{test,0}}$ is the same.
- For three events, as the detector's limit, the estimation improves (red-medium). The proof of safety is not reached during the 30 years of simulation.
- The third line (red-broadest) is known from above. The proof of safety is reached during the fourth year of introduction.

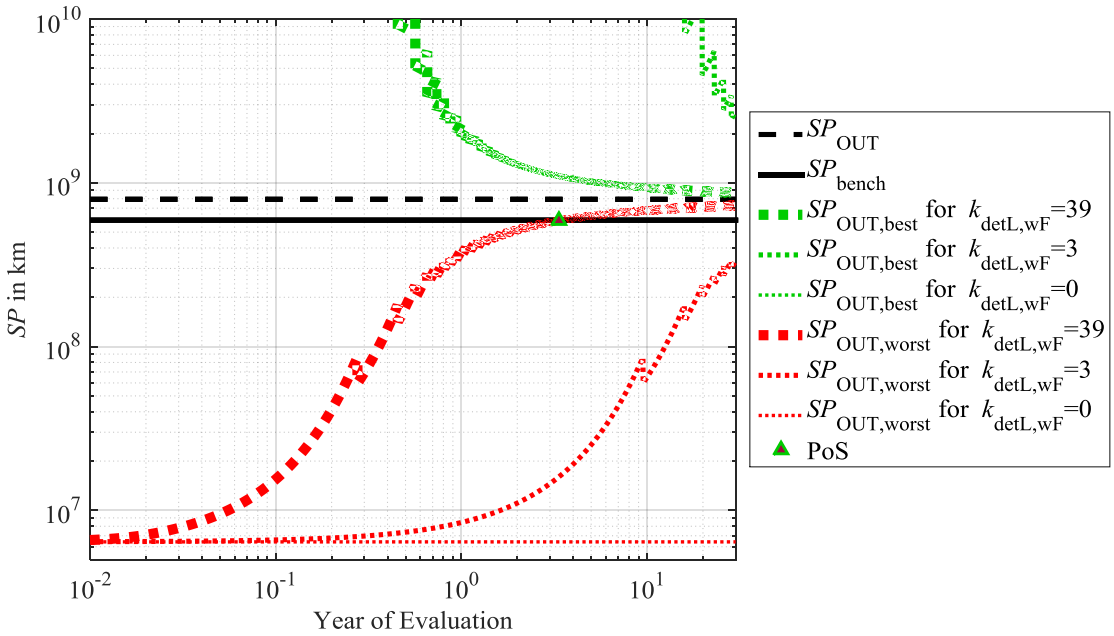


Figure 48 Simulation result SP_{AwF} over t for $\boldsymbol{SP}_{\mathrm{OuT}} = 1.34 \cdot \boldsymbol{SP}_{\mathrm{bench}}$ and M-k_{tol} = "Detector's Limit", $k_{\mathrm{detL,wF}} = \{0, 3, 39\}$ and $d_{\mathrm{test,0}} := 2.96 \cdot 10^{7}$ km

SP_{OuT} is varied – the other parameters are kept constant:

Above, parameters were varied that actually can be directly manipulated during real application. The safety performance SP_{OuT} can also be developed to a higher level, however it is unknown which level it has reached. Thus, the question studied now is how the usage strategy will change depending on the safety performance of the object under test. Figure 49 illustrates the effect on the allowed velocity:

- The better the object under test, the higher the value of the allowed velocity at the end of simulation.
- During the first month until $t = 0.07$ a, the allowed velocity of all objects under tests beside the worst one are the same. This results from the fact that none of these vehicles had an accident with fatalities.
- The longer the simulation takes, the broader the range of the different allowed velocities gets.

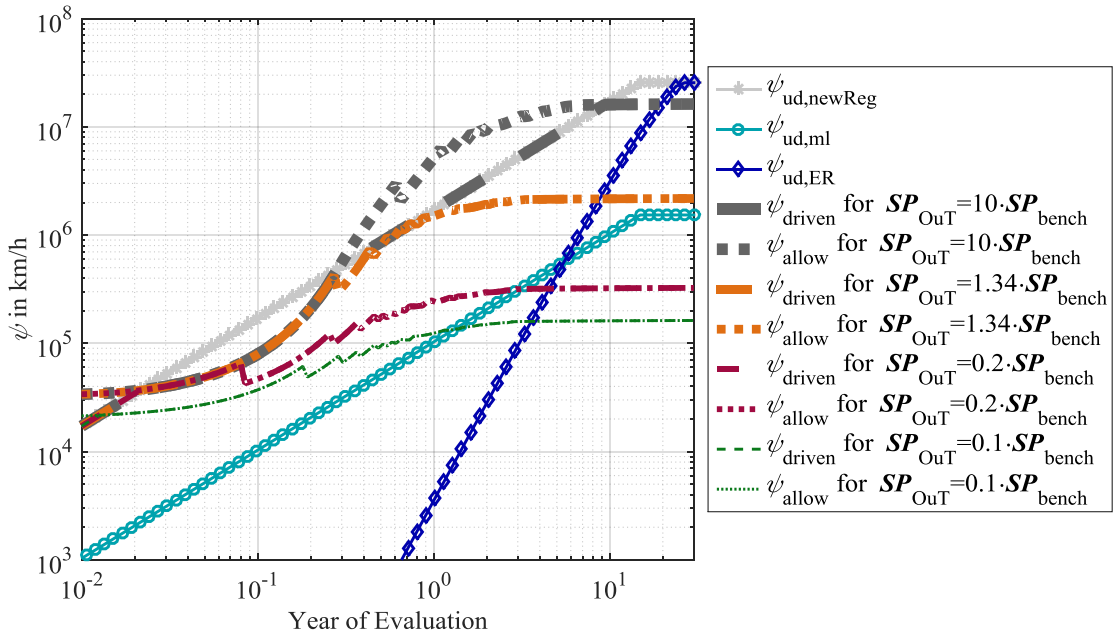


Figure 49 Simulation result ψ over t for $\boldsymbol{SP}_{\mathrm{OuT}} = \{0.1, 0.2, 1.34, 10\} \cdot \boldsymbol{SP}_{\mathrm{bench}}$ and M-k_{tol} = "Detector's Limit", $\boldsymbol{k}_{\mathrm{detL}} = [1216; 39]$ and $d_{\mathrm{test},0} := 2.96 \cdot 10^7$ km

The reason for these different allowed velocities gets understandable with Figure 50. Only the benchmark and the lines for $\boldsymbol{SP}_{\mathrm{OuT}} = 1.34 \cdot \boldsymbol{SP}_{\mathrm{bench}}$ are the same like in the figures above. All other lines have changed due to the simulation parameter. For this parameter combination also the proof of less safety is indicated by a downwards directing triangle (red). The following conclusions can be drawn from this figure:

- For all simulation parameter combinations, the best- and worst-case estimations converge against the object under test safety performance.
- The two less safe objects are found to be less safe at $t \approx 0.29$ a and $t \approx 0.46$ a.
- The two safer objects are found to be safer at $t \approx 0.62$ a and $t \approx 3.35$ a.
- Besides the worst systems, all worst-case estimations start at the same point. This again happens as there has not been an event for any of these systems during the testing phase.
- For $\boldsymbol{SP}_{\mathrm{OuT}} = 0.2 \cdot \boldsymbol{SP}_{\mathrm{bench}}$ the best-case estimation is calculated the first time at $t = 0.08$ a. Before, there is no best-case estimation because no accident with fatalities happened.

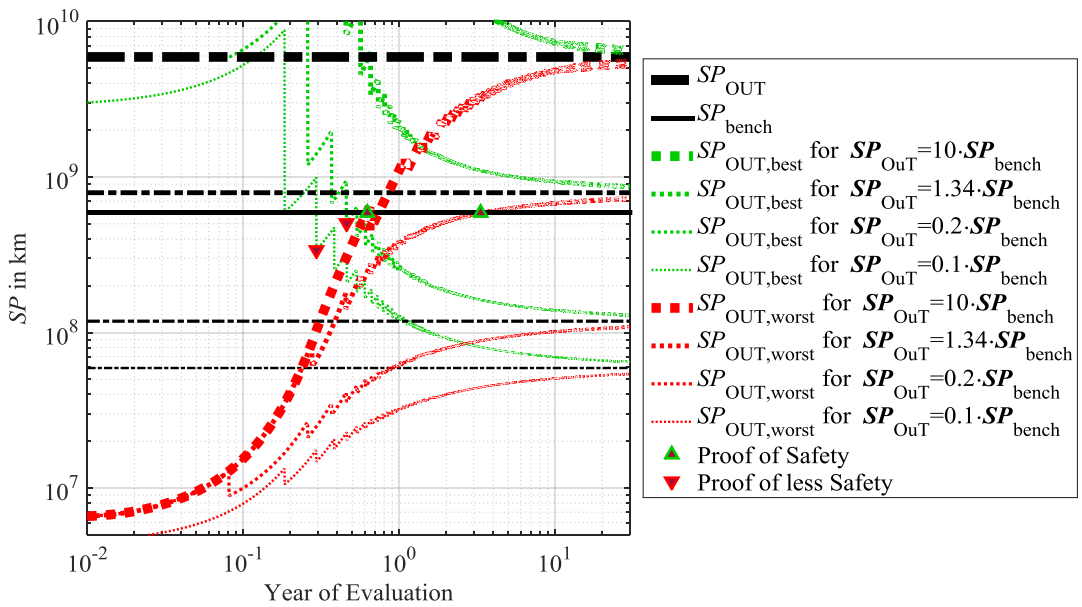


Figure 50 Simulation result SP_{AwF} over t for $\boldsymbol{SP}_{\mathrm{OuT}} = \{0.1, 0.2, 1.34, 10\} \cdot \boldsymbol{SP}_{\mathrm{bench}}$ and M-k_{tol} = "Detector's Limit", $\boldsymbol{k}_{\mathrm{detL}} = [1216; 39]$ and $d_{\mathrm{test,0}} := 2.96 \cdot 10^{7}$ km

To further analyze the impact of the usage strategy parameters, the evaluation criteria are presented for all 108 simulations in appendix D and discussed in the following.

Characteristic Value t_{PoS}

For the 108 defined parameter combinations, the time in years for which the proof of safety has been given is presented in Table 18 and Table 19 (see appendix D). The error probability and the safety performance benchmark for the proof are the same for all parameter combinations, as explained in section 3.6.2 "Usage Strategy Parameter Assignment" on page 105. As the PoS requires a severity sensitive examination, both proofs of safety are depicted, one for accidents with injuries the other for accidents with fatalities. The interpretation of this characteristic value leads to:

- The first proof of less safety for accidents with fatalities is reached at $t = 0.098$ a for the worst OuT ($a_{SP} = 0.1$), the usage strategy "Mobility Replacement", the highest detector limit, and $d_{\mathrm{test,0}} = 10^{8}$ km. The first proof of higher safety is reached at $t = 0.59$ a for the best OuT ($a_{\mathrm{sp}} = 10$), the highest detector limit, and with the longest testing distance $d_{\mathrm{test,0}} = 10^{8}$ km.
- During t_{FulDep}, the PoS is reached earlier, the more extreme the ratio in safety performance between OuT and benchmark (a_{SP}) is.
- The more has been tested before RfU, the earlier the PoS is reached.

- As long as no events are tolerated, the proof of higher or less safety cannot be reached.
- The more events are tolerated, the faster the PoS or PolS is reached.
- As the OuT and the benchmark for events with injuries are lower than that of events with fatalities, the proof of less safety is reached earlier. For the worse OuTs studied the PolS is given before the release for usage (RfU). Thus, the lower level of severity may serve as a good safety indicator. Caution: It might also happen as explained by Figure 11 (the severity sensitive pyramid), that at lower levels of severity safety can be proven although on higher level of severity it cannot. The other way around might reasonably also happen.

Evaluation Criteria for the Time Span $\Delta t_{\mathrm{intro}}$

For the 108 defined parameter combinations, Table 20 lists $r_{\mathrm{c,RvD}}$. This ratio compares the delta in costs with the total cost of traffic events until t_{PoS}. Either events are saved (positive values) or are created (negative values) by limiting the usage based on the usage strategy. For better OuT ($a_{SP} > 1$), this value should be close to zero, for worse OuT as big as possible.

- The longer test distances have been driven, the more costs (saved and created) have been shifted to the testing phase.
- As long as high numbers for the detector's limit are tolerated the ratio is small, thus the limitation is little.
- The further a_{SP} is from 1, the more a usage strategy affects the usage and its outcome.
- The "Special Needs Safety Account" method to derive the tolerated number of events reduces the limitation for worse OuT ($a_{SP} < 1$). Because of that, the proof of safety is reached for all parameter combinations. Consequently, also additionally costs aren't hindered for worse systems ($a_{\mathrm{SP}} = 0.1$) than the inexpirienced drivers. This result demands a method to derive tolerated events, that stronger punishes for worse safety performance compared to the young inexperienced driver ($a_{\mathrm{SP}} = 0.2$).

For the 108 defined parameter combinations, $r_{d,\mathrm{LvD}}$ in Table 21 illustrates how much of the mobility demand of mobility limited people is not satisfied due to the limitation of a usage strategy until a PoS can be given.

- The main contribution to this criteria has the detector's limit k_{detL}. For zero and three events this strongly limits the usage, thus the usage demands of mobility limited people is not met.

- Especially for an OuT that is at least as good as the young inexperienced driver, the "Special Needs Safety Account" method enables a partial fulfillment of mobility limited people's demand.

For the 108 defined parameter combinations, r_{ψ} in Table 22 presents the ratio of two maximum velocities. The numerator is the velocity demanded from newly registered vehicles up to the point the PoS would have occurred when following this demand. The denominator is the velocity during usage strategy limitation until t_{PoS}.

- The worse the OuT, the more the usage strategy "protects" the society by limiting the velocity.
- If the safety performance level of the OuT is below a certain limit, the proof of safety is either found ahead of usage or during the first month. In this case, the hindrance of the limitation is little because only little additional distance is necessary to reach the proof of less safety.
- For the OuTs that are better than the benchmark, also values smaller than 100 % occur. This happens when the vehicles are introduced first slowly and later abruptly. When the test distance was small and consequently the uncertainty big, additional distance driven leads to a fast improvement of the worst-case estimation and thus to an allowed velocity gradient that is bigger than the gradient of the usage demand of newly registered vehicles.

Evaluation Criteria for the Time Span Δt_{suvi}

For the 108 defined parameter combinations, $\Delta C_{\mathrm{total}}$ in Table 23 presents the delta in costs that is either saved (positive values) or is created (negative value) by limiting the usage to values below the usage demand of newly registered vehicles.

- As long as the OuT and benchmark have the same SP, no delta exists.
- As long as the OuT is worse than the benchmark, the usage strategy prevents events and safes costs.
- Even for a 10-times better OuT more than 3 events as a detector limit or a new usage strategy are necessary to not miss any safety benefits of AD3+ when applying the usage strategies.

For the 108 defined parameter combinations, $r_{\mathrm{d,ml}}$ in Table 24 presents the hindrance of the usage demand of people with mobility limitation during the whole simulation t_{FulDep}.

- "Vision Zero" does never fulfill the demand – not even for mobility limited people.
- All usage strategies hinder the OuT that is as good (or bad) as an inexperienced young driver when the detector limit is below 3, despite the "Special Needs Safety Account".

- The “Special Needs Safety Account” also enables the usage of a 10 times worse system. This might be seen as a drawback of this method for defining the tolerated number of events. More complex methods can be defined that hinder worse systems stronger and still enable the fulfillment of the usage demand of mobility limited people.
- To meet the usage demand of mobility limited people, even for a better system than the benchmark, either the “Special Needs Safety Account” method needs to be applied or a detector limit higher than the studied three events needs to be defined.

For the 108 defined parameter combinations, ΔC_{driven} in Table 25 presents the delta in costs that is either saved (positive values) or is created (negative value) by driving with AD3+ when following the usage strategy.

- If no events are tolerated, there is no effect on road traffic safety.
- The “Special Needs Safety Account“ tolerates more costs, because it respects the special needs of mobility limited people. Its nearly independent from the detector’s limit $k_{\text{detL,wF}}$
- The safety effect of the different usage strategies varies significantly. In case of a better OuT than the benchmark ($a_{SP} = 1.34$) the saved costs range from little testing and little detector’s limit $\Delta\text{C}_{\text{driven}} \approx 2.81 \cdot 10^6$ € to the opposite $\Delta\text{C}_{\text{driven}} \approx 2.38 \cdot 10^9$ €.

3.6.5 Conclusions on the Usage Strategy Examination

Direct Conclusions

The evaluation criteria indicate changing safety outcomes when varying the usage strategy and its definitions. Conclusions on the qualitative and quantitative discussion are drawn: Firstly, for the time until PoS. Secondly, for the time after PoS.

What conclusions can be derived until the PoS?

- To come to a PoS in a reasonable time, more than 0 events have to be tolerated. A risk tolerance is required.
- If the mobility demand of mobility limited people should be satisfied, more than 0 events have to be tolerated.
- The derived “Detector’s Limit” enables the fulfillment of mobility demands of mobility limited people. The minimum number of events that describe the detector’s limit might be derived for real-world application by an optimization.
- When assuming equipment ratios derived from other technologies that found their way into the automobile, the limitation by the usage strategy sometimes gets obsolete. The take rates are sometimes a stricter limitation as the usage strategy as long

as more than zero events are tolerated. Special care must be taken if take rates exceed known values. Due to the benefits that might come with AD3+, this must be kept in mind.

- The impacts of different methods to define the tolerated event numbers (M-k_{tol}) differ up to t_{PoS} mainly by the value for the detector's limit. The reason for that is the little number of events that could influence the "Safety Account" as well as the "Mobility Replacement" approach.
- As can be seen, it takes some time until the PoS is reached. During this time there should be a further system development to avoid identified challenges for the OuT. Unfortunately, by changing the OuT the meaning of the collected test distances gets questionable. Consequently, there should be a way to conserve the knowledge gained during this distance that can be used for testing OuT updates ahead of RfU.
- Challenging is that the proof of safety and less safety would be possible during less than one year. This would neglect special effects eventually only occurring during the winter months or vice versa the summer months. To take care of these effects, the supervision of the OuT seems reasonable, at least for one year suffering different natural seasons.

What conclusions can be derived for the usage during supervision?

- A pure tolerated number of the same size as the studied values ("Detector's Limit") that does not adapt over time hinders the usage even if the OuT is 10 times better than the benchmark.
- The approach to additionally tolerate the replaced number of events ("Mobility Replacement") saturates at a certain level as well. Thereby, it would also hinder a better OuT than the benchmark.
- When, in addition, trying to fulfill special needs, these have to be formalized and implemented into the usage strategy. Thereby, the hindrance can be reduced for these special needs.
- The price the society would have to pay for accounting these special needs would be in this example approximately $1.32 \cdot 10^9$ €, when allowing an OuT SP at the inexperienced young driver level. In general, the effect of defining different usage strategies is addressing thousands of fatalities and billions of € especially when covering 30 years. These hypothetical values neglect additional costs besides fatalities and light injuries and suffer the simplifications that the simulation and value determination is based on.

A problem is formalized, a solution is proposed, its sensitivity to parameters has been studied, and its outcome for an exemplary case was simulated. This represents a methodology for the challenge of a prospective assessment. Not necessarily the exemplary

results of the methodology, but the methodology itself should be seen as the main contribution of this thesis.

Abstracted Methodic Conclusions

At the beginning of this chapter, Q 12 asked: How to use stochastic to achieve a safe usage of automated driving? The chapter proposes a methodology for the prospective assessment. The methodology mainly consists of three steps:

1. Formalization

- Use the Poisson process as the first best guess for expressing the uncertainty on the occurrence of accidents with AD3+.
- Use the safety performance SP and distance traveled d as key values for evaluation.
- Take care of different levels of severity.
- Define criteria by analyzing the allowed velocity to compare the outcome of different usage strategies.
- Define a usage strategy by concretizing the method to calculate the tolerated number of events M-k_{tol}, k_{detL} and $d_{\mathrm{test,0}}$.

2. Simulation

- Study the defined criteria for a time span like t_{FulDep}.
- Execute a case study for different performance levels SP_{OuT} and usage demands to evaluate how a usage strategy would fulfill the criteria.

3. Consideration/Weighing up

- Visualize the outcome by plotting the safety performance SP and the velocity ψ, etc..
- Compare the numbers of the criteria.
- Criteria could be used for optimizing the usage strategy parameter. But as simplifications as well as non up to date data have been used in this thesis, this optimization should be done when the simplifications are adapted as well as the data has updated.

To apply the proposed concept (the usage strategy) to real cases, real-world data have to be used and today's safety lifecycle of the automobile has to be extended. Both topics are discussed in the following: First in chapter 4 the "Application: Data to Apply the Usage Strategy" and second in chapter 5 the "Consequences: The Safety Lifecycle of AD3+".

4 Application: Data to Apply the Usage Strategy

Q20 Do the data for all use cases exist, which is necessary for application of the usage strategy?

A concept has been described about how to handle the safety performance SP uncertainty. The concept compares and estimates safety performances. Based on these estimations, the concept defines a careful usage strategy that considers requirements of the user as well as the individual of the society.

For the example of the Autobahn-Pilot use case the concept has been applied above. Might these specific results be used for the real introduction of an Autobahn-Pilot? In principle, yes. But the data used for application must be accepted for application by the different stakeholders.

To study what is necessary for application, firstly the data demand is derived. Secondly, the availability of these data is discussed for the use cases derived in subsection 1.1. Thirdly, other existing use cases are studied to answer whether the data exists to apply the concept. For the third part, the focus is set on a selection of use cases where numbers are reported like the Google driverless project or the Autopilot™ from Tesla Motors Inc. This chapter ends with recommendations derived from the data demand.

4.1 Challenge of the Qualitative and Quantitative Data Demand

Q21 What data are necessary and what requirements have to be fulfilled for concept application?

Up to this point in thesis, it was assumed that the data for application exists. Before application, data should be examined for each use case. The usage strategy bases only on two kinds of data:

- distances d and
- events k.

However, different distance data d_{test}, d_{a} and event data $\boldsymbol{k}_{\text{count}}$, $\boldsymbol{k}_{\text{a}}$ are required. The requirements on that data result from their use. Their use is described in subsection 3.5 and is examined to come to the following individual requirements:

4.1.1 Data for Object under Test Assessment

d_{test} – based on the driven test distance, the safety performance best- and worst-case estimations for the object under test are performed, applying a statistical concept ($\boldsymbol{SP}_{\text{OuT,worst}}, \boldsymbol{SP}_{\text{OuT,best}}$). The object under test is under observation, thus the recording of the driven distance is assumed to be guaranteed by analyzing vehicle data recorder. As the safety performance will be estimated for the corresponding use case, d_{test} should be a sample of the possible distance driven within this use case. How should this sample be chosen for testing? This question is a classical question of the right sampling method. In general, non-probability sampling and probability sampling are distinguished[230a]. To apply the statistical concept, a probabilistic sampling is necessary. The challenge of designing a probabilistic sampling is to know the probability of appearance[230b] of certain properties in advance. Today, both the relevant properties as well as their probability of appearance are unknown. As mentioned above, the goal of running projects is to identify these properties by the microscopic approach. Consequently, this information is necessary to come to representative distances for application of the developed concept. Let's take a simple example for explanation: By comparing the maximum height of snow in Germany in 2012/2013 with 2013/2014 huge differences exist[231]. For Frankfurt am Main, as an example, in 2012/2013 it was 18 cm whereas in 2013/2014 no day with snow was reported. Thus, when testing in the winter 2013/2014 it would be likely to miss something in the Frankfurt area that might cause an event in the next years. The right selection of test distance is an essential pre-requisite to apply the derived concept. Unfortunately, the question on what the right selection might be is not answered within this thesis. This topic is noted for the thesis outlook.

$\boldsymbol{k}_{\text{count}}$ – based on the counted events, the object under test was involved in, the safety performance best- and worst-case is estimated ($\boldsymbol{SP}_{\text{OuT,worst}}, \boldsymbol{SP}_{\text{OuT,best}}$). Thus, all events must be recorded that are defined to be relevant in order to avoid overestimating the safety performance. Therefore, either the vehicle itself needs to be able to identify an event or the user must be obliged to report the events. To determine the severity of an accident (property damage, with injury or fatality) an examination of each case is necessary. Depending on the severity levels, the examination might be more or less detailed. During the testing phase, as has been described, also a re-simulation and estimation of the severity is necessary.

[230] Kauermann, G.; Küchenhoff, H.: Stichproben (2011), p. a:7, b:11.

[231] Andre Hegerath: Maximale Schneehöhe in Frankfurt.

4.1.2 Data for Benchmark Definition

d_{a} – based on the yearly driven use case distance, the safety performance benchmark $\boldsymbol{SP}_{\mathrm{bench}}$ is defined. Compared to the test distance, other requirements exist. By the use case description it must clearly be defined what distance corresponds to the yearly driven use case distance. Unfortunately, there is no direct report of driven distances today[232]. Thus, also the yearly driven distance for a use case needs to be estimated. In principle, several methods for direct measuring and estimation exist[233]: The most aggregated numbers that are recorded during regular vehicle inspections are vehicle odometer readings. These numbers, depending on the sample of the vehicle, are recorded in Germany every half a year[234]. Obviously, by this method distances traveled of vehicles registered in Germany are recorded, thus the domestic traffic (German: Inländerkonzept) is recorded. It is unknown where this distance was traveled exactly. Another method using fuel sales and estimated fuel consumption is not a direct recording of distances but estimates the distance traveled by a model based approach[235]. The distances calculated based on the fuel sales are a mixture of inland vs. domestic traffic recording, whereas by the model based approach different effects like fuel prices and border crossing traffic are tried to be compensated to come to an inland traffic recording[236]. Besides this aggregated numbers also more disaggregated distances are recorded. Therefore two, "in-situ" approaches can be distinguished[237]: Either intrusive (pneumatic road tubes, piezoelectric sensors, or magnetic loops) or non-intrusive approaches (manual counts, passive and active infrared, passive magnetic, microwave radar, ultrasonic, and passive acoustic or video image detection). Based on the traffic counting, the vehicle distance can be calculated as long as it is defined where the counted vehicles need to travel after being counted. This is simple on highways and needs less counting stations, whereas in urban areas it is more challenging to determine accurate numbers. Another approach to identify the use case distance traveled is survey data. In Germany, a mileage survey, household mobility survey as well as the German Mobility Panel is regularly

[232] BMVI et al.: Verkehr in Zahlen 2015/16 (2016).

[233] Leduc, G.: Road traffic data: Collection methods and applications (2008).; Madre, J.-L.; Kalinowska, D.: Vehicle-Based Surveys (2008).; Hautzinger, H. et al.: Laufende Hochrechnung der Kfz-Fahrleistungen (2010).; Hakkert, A. S. et al.: The uses of exposure and risk in road safety studies (2002).; BMVI et al.: Verkehr in Zahlen 2015/16 (2016).; Papadimitriou, E. et al.: Safety performance assessment in Europe (2013).

[234] KBA: Methodische Erläuterungen zu Statistiken über den Verkehr in Kilometern der deutschen Kraftfahrzeuge (2015).

[235] Bergk, F. et al.: Erweiterung der Software TREMOD um zukünftige Fahrzeugkonzepte, Antriebe und Kraftstoffe (2016).

[236] BMVI et al.: Verkehr in Zahlen 2015/16 (2016), p. 151.

[237] Leduc, G.: Road traffic data: Collection methods and applications (2008), p. 3–4.

conducted to obtain mobility behavior of passenger cars as well as the Survey of Road Freight Transport to record data from tractive vehicles with at least 3.5 tonnes load capacity[238]. The survey approach might provide deep insight depending on the survey design, but is costly thus not all of these are updated yearly. The most detailed insight into distances traveled is given by floating car data (FCD)[239]. This data might be collected via GPS and mobile phone combination over nearly the entire road network. FCD might enable an accurate determination of the yearly driven use case distance. Attention must be paid on privacy concerns. This is addressed via ISO 24100:2010 on "basic principles for personal data protection in probe vehicle information services". Another solution for gaining this data is conducting naturalistic driving studies (NDS). The study of Blanco et al.[240] used the SHRP 2 NDS Dataset[241]. Within this NDS, the distance ($34 \cdot 10^6$ miles) together with additional information (time, place, driver, etc,) was recorded by the equipped vehicles in the USA. For determining the driven use case distance, not only different approaches exist but also differences within countries in Europe[242] and worldwide (see for example the USA[243]) must be considered.

$\boldsymbol{k}_{\mathrm{a}}$ – based on the events counted yearly for the use case, the safety performance benchmark $\boldsymbol{SP}_{\mathrm{bench}}$ is defined. The benchmark is calculated as the expected value of a distance between two events for the studied population of drivers. The described concept assumes to know the explicit expected value and no distribution. In general[244], the standard deviation of an estimated expected value depends on the sample size k by $1/\sqrt{k}$ as well as on the variance of the population. To fulfill the requirement of a known expected value, a survey is required that covers a large number of samples. The question on what is large cannot be defined without knowing the variance of the population. A generic requirement is defined:

$$\sqrt{\mathrm{V}(\widehat{SP})} < 0.1 \cdot SP. \tag{4-1}$$

The standard deviation of the safety performance estimation $\widehat{SP}$ should be at least an order of magnitude smaller than the expected value. The value of 1/10 is defined randomly to indicate a well estimated safety performance. Further research on respective numbers should concretize the requirement on the necessary sample size. Thus, for the

[238] Madre, J.-L.; Kalinowska, D.: Vehicle-Based Surveys (2008), p. 5–6.

[239] Leduc, G.: Road traffic data: Collection methods and applications (2008).

[240] Blanco, M. et al.: Automated Vehicle Crash Rate Comparison Using Naturalistic Data (2016).

[241] Antin, J. et al.: SHRP 2 Naturalistic Driving Study (2015).

[242] Papadimitriou, E. et al.: Safety performance assessment in Europe (2013), p. 378.

[243] Campbell, K. L. et al.: Sources of exposure data for safety analysis. (1996).

[244] Kauermann, G.; Küchenhoff, H.: Stichproben (2011), p. 22.

defined requirement the arithmetic mean is close to the expected value. Different as for the object under test, no full supervision of the population exists. Road events in Europe are collected[245a] by the police and are reported to ministries and statistical services[246]. In Germany, this is regulated by the German law on statistics of road traffic accidents (Straßenverkehrsunfallstatistikgesetz-StVUnfStatG)[247]. Additional information on damage only accidents is collected and reported by insurances[245b]. For the reported accidents information are available to classify an event as relevant for the use case or not (StVUnfStatG §2). If more in-depth information is necessary, special studies exist. However, these do not cover all accidents within the reported statistics[248]. Besides the information depth the underreporting[249] especially for less severe, single vehicle and two wheeler accidents is a challenge for defining an objective benchmark. No study was found on the identification of unreported accidents for Germany, although in the ETSC[250] report 8 % underreporting of death in Germany is stated. Whereas in the IRTAD[251] report 5 % killed, 32 % severly injured, and 36 % slightly injured are mentioned to be unreported in Germany. Blanco et al.[252a] summarize similar findings for the USA. Different estimates provide a wide range of different numbers about unreported crashes. National estimates[253] vary for not reported injury crashes from 15.4 % up to 39.7 % and property damage from 35.6 % to 59.7 %. Besides the national estimates, also estimates based on the SHRP 2 study are made. 84 % of the 279 identified crashes were unreported. Thus when using these numbers for the safety performance benchmark, the benchmark is overestimated as long as no correction is applied.

4.1.3 Generic Data Requirements

Blanco et al.[252b] conclude on the comparison of crash data:

---

[245] ETSC: Road Accident Data (2006), p. a:12, b:13.

[246] http://ec.europa.eu/transport/road_safety/specialist/index_en.htm accessed 24.09.2016

[247] BMJV: StVUnfStatG (1990).

[248] Seeck, A. et al.: GIDAS project (2009).

[249] Schnieder, E.; Schnieder, L.: Verkehrssicherheit (2013), p. 158. ETSC: Road Accident Data (2006), p. 13.

[250] ETSC: Road Accident Data (2006), p. 14.

[251] Derriks, H. M.; Mak, P. M.: IRTAD: Underreporting of casualties (2007), p. 19.

[252] Blanco, M. et al.: Automated Vehicle Crash Rate Comparison Using Naturalistic Data (2016), p. a:16f b:i.

[253] Blincoe, L. et al.: The economic and societal impact of vehicle crashes (2015). and M. Davis & Co.: National Telephone Survey (2015). qtd. in Blanco, M. et al.: Automated Vehicle Crash Rate Comparison Using Naturalistic Data (2016), p. 16.

> *Thus, we have a situation in which we are attempting to analyze self-driving car data, which has a full record of all crashes, relative to the current vehicle fleet, which has an incomplete record of crashes. The comparison is, as the old saying goes, apples to oranges.*

Their study mainly concentrates on the accident numbers of the benchmark. It should be emphasized that all of the data, necessary as explained above, needs to be appropriate and fit to each other: distance as well as accidents. Whether the data is appropriate or not, strongly depends on the use case. Consequently, besides the requirements that result from the individual usage of the data, there exist also generic requirements the data needs to fulfill:

- The data must be associated with a detailed use case documentation.
- The data must be derived following a documented and reviewed method.
- The data must be up-to-date.
- The data must be accessible at least from RfU on, together with the documentations.
- The data must be archived for the life time of the vehicles together with the documentations.

4.2 Data to Examine the Use Cases

Q22 Is data available to apply the usage strategy on the described use cases?

The application of the usage strategy for the different use cases strongly depends on the data that exists. In subsection 1.1, four different use cases are introduced. For each use case, the existence of data is checked and systematic challenges for application of the usage strategy resulting from the use case are discussed. The application of the usage strategy is examined for Germany, as for other countries differences in data acquisition exist.

4.2.1 Autobahn Pilot Examination

Data for Object under Test Assessment

No data exist, because no such vehicle is in testing phase or to be precise no data are communicated about any vehicle being in the testing phase. That is the reason why the usage strategy examination explained above is based on theoretically derived values.

d_{test} – By the street type Autobahn in Germany it is fairly easy defined where (spatially) to collect the test distance. In 2013, the German Autobahn was[254] approximately 12,917 km long. Even if it would be necessary to drive each lane and approx. 3 lanes exist in average, this would add up to less than 80,000 km. But the question remains when and how often to drive these roads. There needs to be a test design that delivers a test routing that takes care to come to a probabilistic sampling. If due to weather conditions discussed above, representativeness cannot be guaranteed, also a limitation of usage might be necessary (see the concept of the Seed Automation). The methodology to derive the necessary data needs to be defined, documented, as well as published and archived. Data needs to be collected, updated, and communicated with RfU.

$\boldsymbol{k}_{\text{count}}$ – Since no distance has been driven, no events are reported. When starting test driving, a simulation environment should be in place. Re-simulation during the testing phase of test driver interventions needs a simulation environment, together with simulation models. If accuracy of the simulation environment is uncertain, a worst-case simulation should be executed. The methodology for re-simulation needs to be defined, documented, as well as published and archived. Data need to be collected, updated, and communicated with RfU.

Data for Benchmark Definition

d_{a} – The distance driven on Autobahn (inland) exists and is published. The documentation exists and is published as well. Although the data is updated regularly, the process might be improved in a similar manner as safety assessment data will be collected when AD3+ vehicles will be connected. Digital recording and direct reporting would help to achieve an up-to-date benchmark. The two alternatives of either floating car data or automated vehicle identification in combination with existing toll stations would make this possible[255]. Many new vehicles are already equipped with hardware to generate and send all necessary data. This should be used to improve reporting.

$\boldsymbol{k}_{\text{a}}$ – Accident numbers are recorded and reported for the Autobahn. Unknown is the number of unreported accidents. Especially the underreport of accidents with minor severity are challenging the object under test. At an early stage of testing, these minor cases are the first indicators of potential higher or lower safety. Care must be taken that the missing knowledge on minor cases of the benchmark does not hinder the introduction of automated vehicles. A correction factor should be identified and used to define the benchmark. Additionally, the aggregation of events today needs several administrative steps. The same as for the collection of distances should also apply for the number

[254] BMVI et al.: Verkehr in Zahlen 2015/16 (2016), p. 101.

[255] Martí, F. S.: Highway travel time estimation with data fusion (2016), p. 111.

of events. The police records should directly be digitalized and reported to the statistical office.

Today's constellation, however, leads to an overestimation of today's traffic's safety performance, thus the benchmark. This overestimation of the human and the underestimation of AD3+ is the ratio which guarantees safety for the society and it should be taken care that it will not be the other way around.

4.2.2 Automated Valet Parking Examination

Data for Object under Test Assessment

In general, the same situation exists for the use case of automated valet parking. This use case is still a vision of the future, thus no data for real object under test assessment exists.

d_{test} – The definition of the use case as it is given in subsection 1.1.2 is too fuzzy to really identify the area where the use case should be tested. Today, at least in most of Europe, normal driving and the attempt to find a parking lot as well as to park merge into each other. When limiting the use case to multi-story car parks (German: Parkhaus), the challenge of defining relevant properties as well as their probability of appearance might be reduced. Within car parks, weather as well as lighting might be controlled. Thus, this use case is an example that would need a more detailed description before any test design might be given.

$\boldsymbol{k}_{\text{count}}$ – When distance is driven, again, the counting and corresponding re-simulation can be performed. For the reason that parking use cases are performed at low speed, it is of interest if the chance of an accident with higher levels of severity might be negligible. Existing studies on car-pedestrian accidents[256] as well as car-car accidents[257] indicate a monotonic relationship between fatality risk and car impact speed converging to zero for lower speeds. Based on additional comprehensive studies for the object under test it might be arguable to neglect the chance of a fatality. This would ease the introduction of automated valet parking and be a motivation for this use case from this safety assessment concept.

Data for Benchmark Definition

d_{a} – As today there is no corresponding use case of automated valet parking the distance driven by the benchmark within this use case is unknown. There is no direct indi-

[256] Rosen, E. et al.: Literature review of pedestrian fatality risk vs. impact speed (2011), p. 28.

[257] Richards, D. C.: Relationship between speed and risk of fatal injury (2010), p. 42.

cator like a certain road network that clearly defines a distance driven to be the valet parking case. Thus, by the use case definition it needs to be defined which of the distance driven by the benchmark is seen as relevant for comparison. In difference to the Autobahn network, as this is a special type of road, there is no information on driven distances for special inner-city areas[258]. Thus, for defining the benchmark for a valet parking use case, data is lacking.

$\boldsymbol{k}_{\mathrm{a}}$ – When the use case is precisely defined the information on events within this use case exist due to police reports. However, today this information is not processed to a resolution that would be necessary for defining the benchmark. A direct digitalization of accidents and association with annotated road network data (OpenStreetMap for example) would ease the whole stochastic process.

Thus, from the use case described in this thesis, it is concluded that requirements result also for the use case description (or item definition) when the safety assessment concept should be applied.

4.2.3 Emergency Automation Examination

Data for Object Under Test Assessment

d_{test} – The use case is described to be active for the whole road network covering all environment conditions. By trying to come to a probabilistic sample, the same challenge for routing exists as has been described for Autobahn only, but for this use case the potential road network is[259] approximately 830,000 km in Germany.

$\boldsymbol{k}_{\mathrm{count}}$ – When routing has been defined, the events resulting from the driven distance are countable. The amount of events that have to be counted during the test and usage of the different use cases obviously depends on the safety performance of the object under test. However, when addressing all emergency situations by this use case, also areas with a high frequency of events as in urban scenarios or high severity of events as in rural road scenarios are covered. The concept explained above does not include the discussion whether safety performance estimation should also be sensitive to different areas of usage. Thinking about an object under test that only causes events close to playgrounds or schools and somewhere else never causes any event. Although the safety performance indicates no difference in safety as it calculates a weighted mean for all areas, the local safety perception could be different. An area selective safety performance could help to define a more detailed assessment.

[258] BMVI et al.: Verkehr in Zahlen 2015/16 (2016), p. 151.

[259] BMVI: Verkehr und Mobilität in Deutschland (2015), p. 4.

Data for Benchmark Definition

d_{a} – For Germany, the domestic distance[260a] (including German vehicles distance in foreign countries, excluding foreign vehicles distance in Germany) exists. $725.7 \cdot 10^9$ km were driven in 2013. The inland distance is not reported but should be used for the calculation of the benchmark. For the area selective approach, a survey of area selective distance driven would be necessary.

$\boldsymbol{k}_{\mathrm{a}}$ – The numbers[260b] for events in Germany 2013 are processed for accidents with property damage, with injuries, and with fatalities separated for inside and outside of town, for different street types (Autobahn, Bundesstraße, Landstraße, Kreisstraße, others) and federal states. As the data exist also for a finer area separation the data should be processed again for the area selective approach if necessary.

4.2.4 Seed Automation Examination

The area selective approach directly leads the seed automation. The idea of the fourth use case is not to start with the whole road network but with a small section (spatial, temporal, weather, etc.) of real traffic and constantly evolving this section.

Data for Object under Test Assessment

d_{test} – The area where to drive is exactly defined for the use case example explained in subsection 1.1.4. As it is limited to less than 100 km around Gothenburg, the probabilistic sample is simplified.

$\boldsymbol{k}_{\mathrm{count}}$ – The events that might occur during driving should be re-simulated and recorded. There seems to be no special challenge.

Data for Benchmark Definition

d_{a} – The distance driven within the narrow area can easily be derived by a sample counting or even by a direct measurement as exits and entrances to the closed loop are little.

$\boldsymbol{k}_{\mathrm{a}}$ – The challenge for defining a benchmark results from the small number of events within this narrow area. For the Gothenburg municipality (Swedish: varav Göteborgs kommun), a total of 5 accidents with fatalities and 70 with personal injuries were reported[261] 2015. Although it is not reported in the published statistics, there is a good

[260] Destatis: Verkehrsunfälle - Zeitreihen 2014 (2015), p. a:4, b:20–48. Cf. Deutsches Institut für Wirtschaftsforschung. 2012 based on estimations of Bundesanstalt für Straßenwesen.

[261] Trafikanalys: Road traffic statistics Sweden (2016), p. 63.

chance that there was not even one accident with fatalities on the defined road section. Following the equation (1-11) for the safety performance, a theoretical infinite safety performance for accidents with fatalities would result. Trying to prove the higher or equal safety of AD3+ is impossible. The reason for that is the definition of the benchmark. For the number of events the requirement has been defined, that the sample size together with the underlying distribution fulfills equation (4-1). To increase the sample size, it is either necessary to increase the use case area or to increase the observation time. The challenge for the increase of observation time results from the time variant safety performance. The benchmark may also have changed due to improvements in vehicle technology or other factors (see Figure 20). Thus, the definition of a benchmark could be done by studying road types of the same kind and to assume similar safety performances. An alternative way would be to also study the distribution of safety performance and therefore compare two safety performance distributions, the one of AD3+ and the one of the benchmark. This is noted for the outlook and is left open for further research.

4.3 Data to Examine Existing Use Cases

Q23 Are data available to apply the usage strategy on existing use cases?

Today AD2- exists[262] and is sold for use in real traffic. AD3+ is not in the testing phase (TRL 7) yet. As far as communicated, vehicles are driven worldwide to test functional behavior and use these results for further development and improving, meaning further changing the AD3+ functions. A test driver is in place to intervene. Thus, from the thesis concept point of view today no data exists or is communicated for the safety assessment goal.

Nevertheless, in the USA two prominent examples exist that argue about safety using an accident per distance ratio and looking for a benchmark in today's road traffic statistics.

4.3.1 Tesla Motors Inc. Model S Autopilot Tech Package

In the user's manual[263] of the Tesla Model S (Software Version 7.1) the Autopilot Tech Package including Traffic-Aware Cruise Control, Autosteer, Auto Lane Change, Autopark, as well as Auto High Beam is part of the Driver Assistance Features. The manual informs that:

[262] VDA: Automatisierung (2015), p. 15.

[263] Tesla Motors Inc.: Model S - Owners guide 7.1, p. 67.

> *Warning: Traffic-Aware Cruise Control is designed for your driving comfort and convenience and is not a collision warning or avoidance system. It is your responsibility to stay alert, drive safely, and be in control of the vehicle at all times. Never depend on Traffic-Aware Cruise Control to adequately slow down Model S. Always watch the road in front of you and be prepared to take corrective action at all times. Failure to do so can result in serious injury or death.*

Thus, despite the naming the vehicle should be used as an AD2- vehicle. Consequently, the necessity for application of the usage strategy is not given. Nevertheless, a statement of the Tesla Team[264] to the preliminary fatal accident evaluation[265] of the National Transportation Safety Board exists. In this statement, three values are given:

> *This is the first known fatality in just over 130 million miles where Autopilot was activated. Among all vehicles in the US, there is a fatality every 94 million miles. Worldwide, there is a fatality approximately every 60 million miles.*

Although, they do not argue on safety, why should these numbers be stated otherwise? As it has been derived above, if these numbers would be used for comparison of safety, the actual use case of Autopilot should be defined explicitly. Given this use case, it should be asked whether the distance driven by the object under test (Autopilot) is a good sample for this use case. Besides the object under test assessment, also the data to define the benchmark should be explicitly derived and explained. If this had been done, the numbers could be used to ask whether the OuT is safer or less safe as the benchmark by the approach explained in subsection 3.3. Figure 51 illustrates the result assuming that the data above fulfills these requirements and all relevant events got known:

---

[264] Tesla Motors Inc.: A Tragic Loss (2016).

[265] NTSB: Preliminary Report, Highway HWY16FH018 (2016).

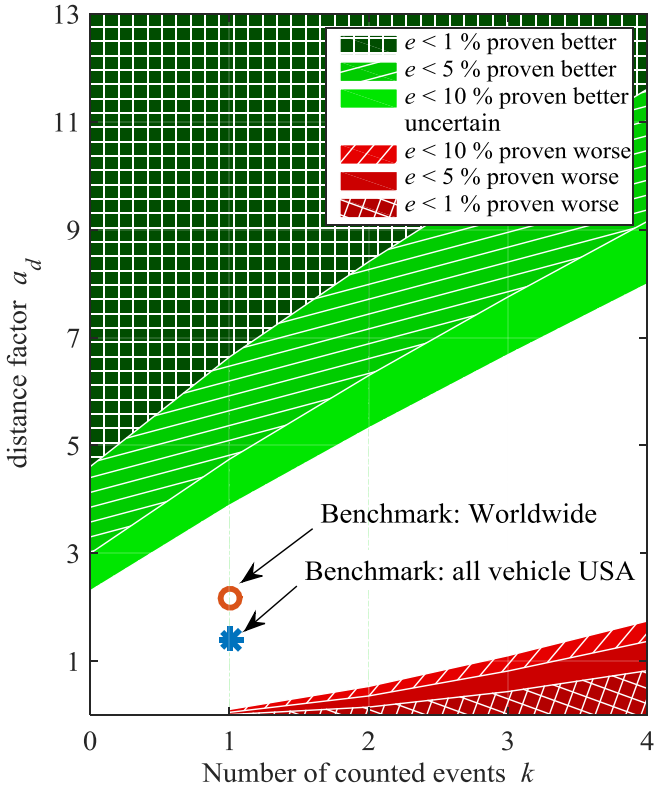


Figure 51 Distance factor a_d as a function of the probability of error e and number of counted events k for comparison of the Tesla numbers with two benchmarks.

The numbers do not serve to either prove or reject the safety hypothesis. This comparison is done for the severity of accidents with fatalities. It would be of interest how this hypothesis changes for other level of severity. Unfortunately, these numbers are not published. But again, this is an AD2- system. And it is improbable that the data used reflects the benchmark as well as the OuT. Events avoided due to human intervention are not reported. A conclusion from this numbers for an AD3+ usage must not be drawn.

4.3.2 Google Self-Driving Car Project

The departments of motor vehicles (DMV) in different states of the USA are working to adopt regulations governing both the testing and public use of autonomous vehicles[266]. In September 2016, the U.S. Department of Transportation has published a federal automated vehicles policy[267] to further harmonize the activities in different states. However, the DMV of California has been the first that adopted their regulations on testing in September 2014. The regulation requires a report of accidents as well as a report of

[266] Blanco, M. et al.: Automated Vehicle Crash Rate Comparison Using Naturalistic Data (2016), p. 8.

[267] U.S. DOT: Federal Automated Vehicles Policy (2016).

disengagement in certain conditions:[268] Accidents within 10 days (§ 227.44) and disengagements of autonomous mode yearly (§ 227.46). Thereby, a first framework for gathering the necessary data has been defined by the requirement of the DMV in California. Similar regulations exist for other states[269].

The results of these reports[270] are that the Google's Self-Driving Car Project encountered the most events, but has also driven the longest distance by factors. Can the vehicles operated by Google be proven to be safer or less safe? Due to the fact that the use case is not described clearly for the Self-Driving Car Project and it is unclear (from reporting) where the vehicle operated during the mileage that was collected, it could just be compared against the average vehicle and usage. Due to the challenges on gathering the necessary benchmark data, as indicated above, a study[271] has been driven from the Virginia Tech Transportation Institute (VTTI) to adjust or correct the data. This adjustment was done by using naturalistic driving study data (SHRP2) to mainly correct for unreported events. As this NDS data deliberately oversampled younger and older drivers, an age adjustment was performed. Also variations on speed zones, locality, and others are discussed in the study. The study concludes with the comparison of accident per distance values for three crash severity levels (see Table 10).

Table 10 SHRP 2 and Self-Driving Car Calculated Crash Rates per Million Miles Driven[271]

Crash Severity	SHRP 2 Age-Adjusted Estimated Rate per Million Miles	Self-Driving Car Estimated Rate per Million Miles
Level 1	2.5	1.6
Level 2	3.3	1.6
Level 3	14.4	5.6

The different severity levels are defined by Table 11.

Table 11 SHRP 2 NDS Crash Severity Classifications[272]

SHRP 2 NDS Crash Severity Level	SHRP 2 NDS Classifications
Level l	Crashes with airbag deployment, injury, rollover, a high Δv, or that require towing. Injury, if present, should be sufficient to require a doctor's visit, including those self-reported and those from apparent

[268] DMV California: Autonomous Vehicles Testing Regulations (2014), p. 11–12.

[269] http://www.dmvnv.com/autonomous.htm accessed 24.09.2016

[270] Soublet, B. G.: Autonomous Vehicles in California (2016), p. 5&9.

[271] Blanco, M. et al.: Automated Vehicle Crash Rate Comparison Using Naturalistic Data (2016), p. 41.

[272] Blanco, M. et al.: Automated Vehicle Crash Rate Comparison Using Naturalistic Data (2016), p. iii.

	video. A high Δv is defined as a change in speed of the subject vehicle in any direction during impact greater than 20 mph (excluding curb strikes) or acceleration on any axis greater than ±2 g (excluding curb strikes).
Level 2	Crashes that do not meet the requirements for a Level 1 crash. Includes sufficient property damage that one would anticipate is reported to authorities (minimum of $1,500 worth of damage, as estimated from video). Also includes crashes that reach an acceleration on any axis greater than ± 1.3 g (excluding curb strikes). Most large animal strikes and sign strikes are considered Level 2.
Level 3	Crashes involving physical conflict with another object (but with minimal damage) that do not meet the requirements for a Level 1 or Level 2 crash. Includes most road departures (unless criteria for a more severe crash are met), small animal strikes, all curb and tire strikes potentially in conflict with oncoming traffic, and other curb strikes with an increased risk element (e.g., would have resulted in a worse crash had the curb not been there, usually related to some kind of driver behavior or state, for example, hitting a guardrail at low speeds).

From these numbers for the different severity levels, the attempt to prove higher or less safety can be made when knowing the safety performance benchmark from Table 10, the event numbers[273] for the object under test (Level 1: 2 times, Level 2: 2 times and Level 3: 7 times) as well as the testing distance[273] of 1,266,611 miles in automated mode. The result is depicted in Figure 52.

For each level, one point is depicted. The meaning for proving higher safety or lower safety of the level one point, the most severe level, is nearly neutral. For level two, the statement on safety is still uncertain (error probability >10 %). This second point is above the point of level one because the benchmark for level two is less safe ($SP_{\text{bench,level1}} > SP_{\text{bench,level2}}$). The third point for level three is clearly within the upper green proven better ($e < 1$ %) area.

Thus, the data correction of the VTTI report as well as the reported numbers of the Google Self-Driving Car Project can neither prove higher safety nor lower safety. However, a first indicator is given by the lowest severity level. On this level, the proof of higher safety has been given. This might be used for a careful prediction based on the argumentation of the accident triangle from Heinrich[274] and Hydén[275]. But as indicated

[273] Blanco, M. et al.: Automated Vehicle Crash Rate Comparison Using Naturalistic Data (2016), p. 8&9.

[274] Ward, R. B.: Revisiting Heinrich's law (2012).

[275] Hydén, C.: The development of a method for traffic safety evaluation (1987).

by the distorted triangle in Figure 7 and Figure 11, this proof on lower levels must not be taken for the overall proof on safety only.

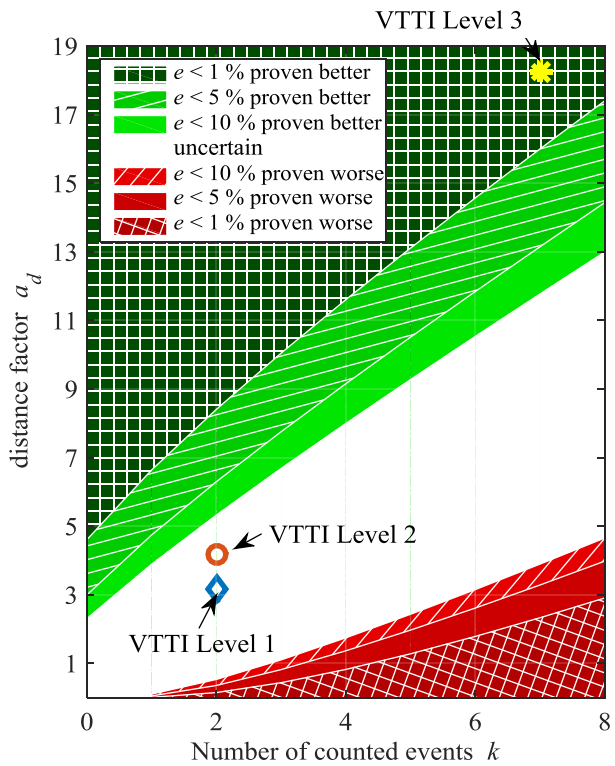


Figure 52 Distance factor a_d as a function of the probability of error e and number of counted events k for comparison of the VTTI numbers with three level of severity.

The conclusion of both examples is: “I know that I know nothing”. To be accurate: to know nothing is wrong. For the idea of the introduction strategy one necessary pre-requisite is given: Less safety has not been proven. The assessment leads to a value in the uncertain area for higher and thus more relevant levels of severity.

The conclusion of this application chapter is that there is no system where the usage strategy needs to be applied today. Nevertheless, the use cases exist and are about to become reality. Thus, data is necessary that needs to be collected and processed. This as well as the future usage strategy application itself asks for a study of the safety lifecycle of an automated vehicle.

5 Consequences: The Safety Lifecycle of AD3+

Q24 Does the usage strategy affect the safety lifecycle of AD3+?

The challenge to introduce AD3+ has been explained. A concept to overcome this challenge has been derived. As the concept should be seen as an extension to the existing development process, but by no means as a replacement, today's safety lifecycle is studied. The safety lifecycle is described[276] by the meaning of its two words. The lifecycle of an item is the entirely of phases from item definition to decommissioning (see Figure 53). The goal should be to reach the absence of unreasonable risks during all these phases. Is the approach described in the ISO 26262 able to cope with AD3+ and the macroscopic approach?

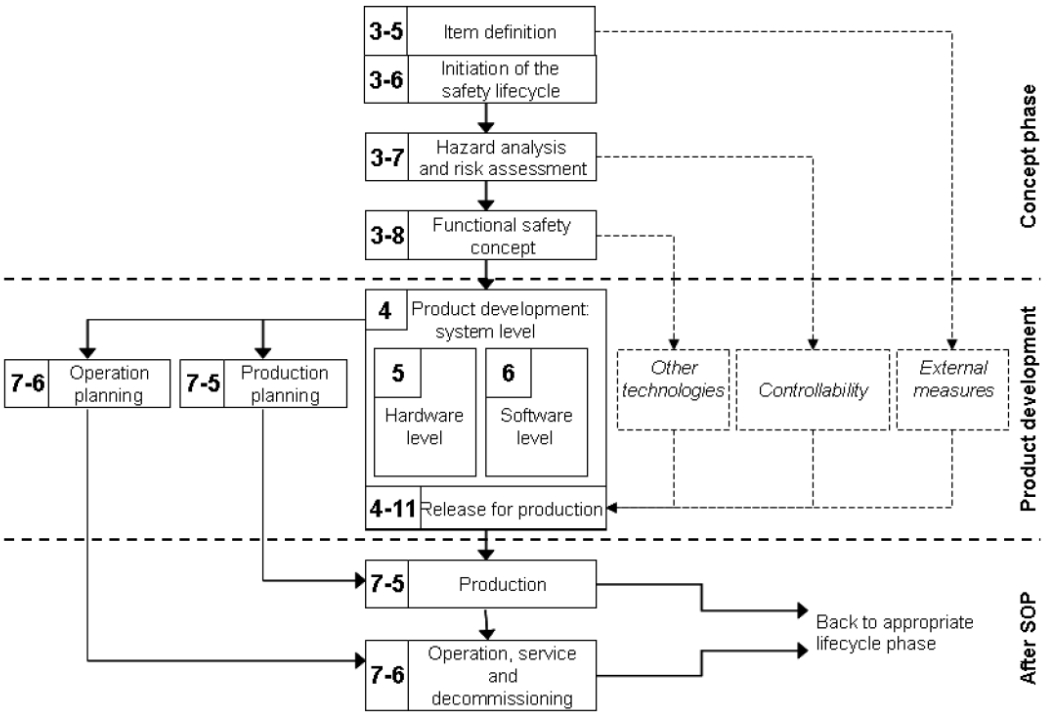


Figure 53 Automotive safety lifecycle as depicted in ISO 26262[276]

Firstly, the challenges for the safety lifecycle resulting from the safety assessment described in this thesis are highlighted. Secondly, a potential adaptation of the safety lifecycle to handle these challenges is proposed. The third subsection gives an outlook

[276] ISO: DIS 26262: Road vehicles - Functional safety (2008), p. 3f. - Part 2.

on potential tools that might address unmentioned major challenges, the collection of data and the limitation of usage.

5.1 Challenges for Applying Today's Safety Lifecycle

Q25 Why is today's safety lifecycle not sufficient for AD3+?

Today, the comprehensive statistical macroscopic proof of safety is not given for the release for production because it is not necessary as explained in subsection 2.1. The main challenge for applying the existing ISO 26262 results from the following two objectives. The objective of the release for production[277a] defines:

> *The release for production confirms that the item complies with the requirements for functional safety at vehicle level.*

Whereas the objective of the hazard analysis and risk assessment[277b] is:

> *to identify and categorise the hazards of the item and formulate the safety goals related to the prevention or mitigation of these hazards, in order to avoid unreasonable risk.*
>
> *A safety goal shall be determined for each hazardous event evaluated in the hazard analysis. Safety goals are top-level safety requirements for the item. They lead to the functional safety requirements needed to avoid an unreasonable risk for each hazard.*

Thus, the person signing the release for production confirms that the item complies with the requirements that should avoid an unreasonable risk. But what if these requirements are not sufficient? This question is addressed[278] by the initiative addressing the safety of the intended functionality (SoTIF). But what if safety still remains uncertain due to economic reasons as long as the usage of the item is not controlled?

Today's lifecycle is not addressing this handling of uncertainty on the safety performance that may exist for AD3+. Consequently, as a result of this thesis, a proactive handling of this uncertainty needs to be established. Due to the existing uncertainty, events may happen during usage. They might be caused by the item. This must be addressed proactively on management level. The one that signs the release for production must, even if a perfectly developed vehicle is brought to usage, discuss the acceptability

[277] ISO: DIS 26262: Road vehicles - Functional safety (2008), p. a:27 - Part 4, b:6ff -Part 3.

[278] Bergenhem, C. et al.: How to reach complete safety requirement refinement for autonomous vehicles (2015).

of accidents. There is no possibility to introduce automated driving without generating acceptability for accidents, as will be explained in the following:

In appendix C, the analytical equation (C-7) describing the simplified usage strategy by the exponential function has been derived to be

$$d_{\mathrm{cum}}\left(t_{\mathrm{FulDep}}\right) = d_{\mathrm{cum}}(0) \cdot \mathrm{e}^{\frac{\lambda_{\mathrm{allow}}}{\lambda_{+}\Delta t_{\mathrm{tol}}} t_{\mathrm{FulDep}}}.$$

The elements of the exponential function are the worst-case OuT estimation for the expected value λ_{+}, the allowed expected value rate $\dot{\lambda}_{\mathrm{allow}} = \frac{\lambda_{\mathrm{allow}}}{\Delta t_{\mathrm{tol}}}$ as well as the length of observation t_{FulDep}. The initialization distance is the test distance before release for usage $d_{\mathrm{cum}}(0) = d_{\mathrm{test,0}}$. The question to be answered is whether and how the proof of safety of AD3+ is possible without acceptance of accidents of these AD3+ vehicles. For the proof in general, the next inequality needs to be fulfilled

$$\lambda_{+} \cdot SP_{\mathrm{bench}} < d_{\mathrm{cum}}\left(t_{\mathrm{FulDep}}\right) \tag{5-1}$$

Up to a certain time t_{FulDep} enough distance d_{cum} must be driven to prove safety. This must be a multiple of the benchmark. When demanding not more than one accident during the time of full deployment $\dot{\lambda}_{\mathrm{allow}} t_{\mathrm{FulDep}} \leq 1$ equation (5-1) can be rewritten as

$$\lambda_{+} \cdot SP_{\mathrm{bench}} < d_{\mathrm{test,0}} \cdot \mathrm{e}^{\frac{1}{\lambda_{+}}}. \tag{5-2}$$

For the best-case, thus the vehicle is safe and no accident will occur, $\lambda_{+} = 3$ is necessary (see Table 15 for $k = 0$) to proof safety. Consequently, if more than $2.14 \cdot SP_{\mathrm{bench}} < d_{\mathrm{test,0}}$ has been tested, most likely less than one event will occur. The conclusion of this is that the careful introduction of a very good system may work without an accident, but caution: at least twice the safety performance distance needs to be tested and then only the distance $0.85 \cdot SP_{\mathrm{bench}}$ is allowed to be driven for usage during the time t_{FulDep}. As it is economically not feasible to test more than to use a system, an acceptability of events needs to be derived and proposed during the concept phase of AD3+.

Only little challenges from the derived concept result for the product development phase, as long as during concept phase the uncertainty has been addressed.

Major challenges exist for the phase after the release for production. The derived concept handles the uncertainty with an updated assessment and limitation of usage. Today, during the operation there are maintenance and service activities planned. Additionally a safety management after release for production[279] is required:

[279] ISO: DIS 26262: Road vehicles - Functional safety (2008), p. 16&17 -Part 2.

The organization shall institute, execute and maintain a field monitoring process with respect to functional safety.

The data is used for decisions and measures e.g. a recall concerning safety incidents. However, these measures as well as "proven in use arguments" foresee a reporting of events for another purpose then limiting the usage.

The awareness for need[280] of a more advanced field monitoring process exists. Schittenhelm[281] proposed a continuous evaluation process of real-world effectiveness. The process is separated into predicting real-world efficiency during development as well as proving real-world efficiency during real-world usage based on take rates of spare parts, insurance claim data, and road accident statistics. But this will only be the first step to apply the usage strategy.

Prerequisites for the usage strategy are the collection of testing distance, the reporting of corresponding events and a possibility to control usage. Consequently, the following subsection will state requirements that should be addressed by the management of the safety lifecycle for AD3+.

5.2 Potential Adaptations of the Safety Lifecycle of AD3+

Q26 How could the safety lifecycle be adapted for AD3+?

The results of this thesis lead the necessity to adapt or most likely extend the safety lifecycle in principle when addressing AD3+. Therefore two components are added to the safety lifecycle for AD3+ as depicted in Figure 54.

One is the macroscopic safety concept. The other is the safety concept application.

The macroscopic safety concept requires a precisely defined use case of AD3+. Based on this use case definition, a concept needs to be defined and to be studied similar as has been explained within chapter 3. The concept must handle possible safety performance uncertainties of the object under test. This macroscopic safety concept shall be defined during the concept phase. The work product of this step is a documentation of this concept.

The safety concept application requires a precisely defined macroscopic safety concept from above. Additionally, it requires the data for application. Most likely it will be the

[280] U.S. DOT: Federal Automated Vehicles Policy (2016), p. 17ff.

[281] Schittenhelm, H.: Real World effectiveness (2013).

data discussed in chapter 4. The application must collect the data defined by the macroscopic safety concept. The application must put the decision on the handling of these uncertainties into practice, thus influence the possibility to activate AD3+. The results of the applied concept should also be considered for the release for production. Additionally, the application must cover the whole phase of operation as long as it has not been decided to be terminated. As described above and indicated by the circle in Figure 54, it should be seen as experiential learning from operation to adapt the usage limitation. Work products should be a documented database on relevant data as well as a concrete influence on AD3+ usage.

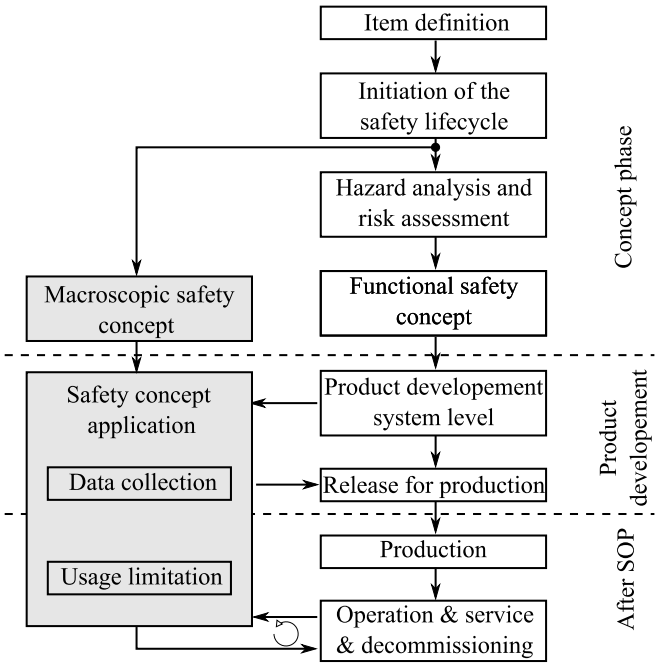


Figure 54 Extended safety lifecycle for AD3+.

This thesis has proposed a basic macroscopic safety concept to instantiate the first component of Figure 54. The thesis leaves open how to instantiate the second component of Figure 54: the collection of data as well as the control of the usage of AD3+. The next subsections lay out thoughts on how to address the collection as well as the control as a methodological outlook for future research.

5.3 Collecting Data for Safety Assessment

Q27 How can the collection of data be designed more efficiently?

5.3.1 Test Translation Factor

The explained concept of the uncertainty-based introduction strategy has the potential to significantly reduce the necessary testing distance ahead of the release for usage. The numbers for $d_{\text{test},0}$ discussed in subsection 3.6 may even be drivable in real traffic with test drivers. Important to mention, however, is the assumption that underlies the explained concept: The OuT, thus the AD3+ vehicle including hard- as well as software that effects safety, must not be changed during assessment. When a change on any of these elements occurred, the distance collected before is not relevant for safety assessment anymore.

Starting the safety assessment over again is especially costly when updates during usage and testing are necessary. As both seem unavoidable at least during the first versions of AD3+, collecting test data needs to be optimized. The approaches described in subsection 2.5 “Possible Approaches for Solving the Challenge of Testing” therefore need to be enabled to contribute to the collection of test data. The basic idea is to derive a translation factor for testing tools combined with test cases other than real-world driving. Is a driven kilometer, as a part of a certain test case on proving ground, as valuable or valid as a kilometer driven in real world, or even more meaningful? Can a variation of scenarios in simulation be translated into testing distance for the macroscopic assessment approach? The same questions can be asked for the events that have been counted during testing. Is it possible to derive event numbers from testing tools and test cases other than real-world driving? Can a safety benchmark be defined based on data from driving simulators or naturalistic driving studies?

In general, a translation of results from tests other than real-world driving to the safety outcome of AD3+ real-world driving is to my knowledge unknown today. These questions are subject of today’s research. However, a test translation factor would be necessary to include all results from the microscopic approach to the macroscopic safety assessment.

As this translation factor is missing today, the goal of the tool described in the following is to stay as close to real driving as possible but enabling economical coverage of reality and reducing additional risks to zero.

5.3.2 Virtual Assessment of Automation in Field Operation (VAAFO)

The basic idea of the VAAFO concept[282] is derived from the so-called Trojan Horse approach[283]. This Trojan Horse approach addressed the testing of emergency intervening

[282] Wachenfeld, W.; Winner, H.: VAAFO (2015), p. 161–170.

systems like emergency brake assist[284] (EBA), which try to mitigate accidents. For this EBA, the results of assessment by means of false-positive and false-negative rates are clear. When assessing systems that control vehicle dynamics constantly (AD3+), this unambiguity is not granted anymore. For this reason, the Trojan Horse has to be developed further, resulting in the VAAFO concept. Similar but less concrete ideas are written down in a patent from Hoye et al.[285] and at a press interview from an employee at Robert Bosch GmbH[286] as well as in the Autopilot Release Notes from Tesla Motors Inc.[287]. All of them mention ideas without giving further insight into their developments.

From a functional point of view, automated driving can be decomposed into three major levels: The automated driving function senses, thinks and acts. All possible sources of risks in terms of safety can be assigned to one of these three levels similarly as presented for the human driver in Graab et al.[288]. Level one (sense) describes causes that happen within the information perception phase. The absence of sensor information leads to an absence of data needed to be processed. For example, an object may be covered or contain undetectable characteristics. Level two (think) classifies all errors that lie within the information processing such as the application of nowadays algorithms. Level three (act) categorizes all causes of accidents that occur after the decision is made due to improper control of the vehicle movement.

On the one hand, the VAAFO tool uses the real sensors (level one/sense) as well as the real processing hardware (level two/think) to stay as close to the real automated driving function as possible. On the other hand it uses the decomposition of the vehicle automation to prevent additional risk by simulating the desired action (level three/act) of the automation.

The VAAFO tool requires the following hardware:

- The basis is a series vehicles that is driven by a human (SAE level 0) or assisted by advanced driver assistance systems (SAE level 1) or partially automated (SAE level 2).
- This series vehicle is equipped with sensors suitable for higher automated driving (SAE level 3+, called AD3+). These sense the real environment.

---

[283] Winner, H.: Einrichtung zum Bereitstellen von Signalen in einem Kraftfahrzeug (2002). Cf. Reschka, A. et al.: Entwicklungsprozess von Kollisionsschutzsystemen für Frontkollisionen (2015), p. 932.

[284] Winner, H.: Fundamentals of Collision Protection Systems (2016).

[285] Hoye, B. et al.: Autonomous Driving Comparison and Evaluation (2015).

[286] Sokolov, D. A.: heise.de - Danke dass Sie das Auto von morgen testen (2015).

[287] Tesla Motors Inc.: Upgrading Autopilot Release Notes v8 (2016).

[288] Graab, B. et al.: Analyse von Verkehrsunfällen (2008), p. 6.

- Additionally, the microprocessors and respective processing algorithms are installed. These algorithms process the data coming from real sensors similar like the ones later used for AD3+.

On the resulting perceived environment representation, the VAAFO tool is applied as depicted in Figure 55.

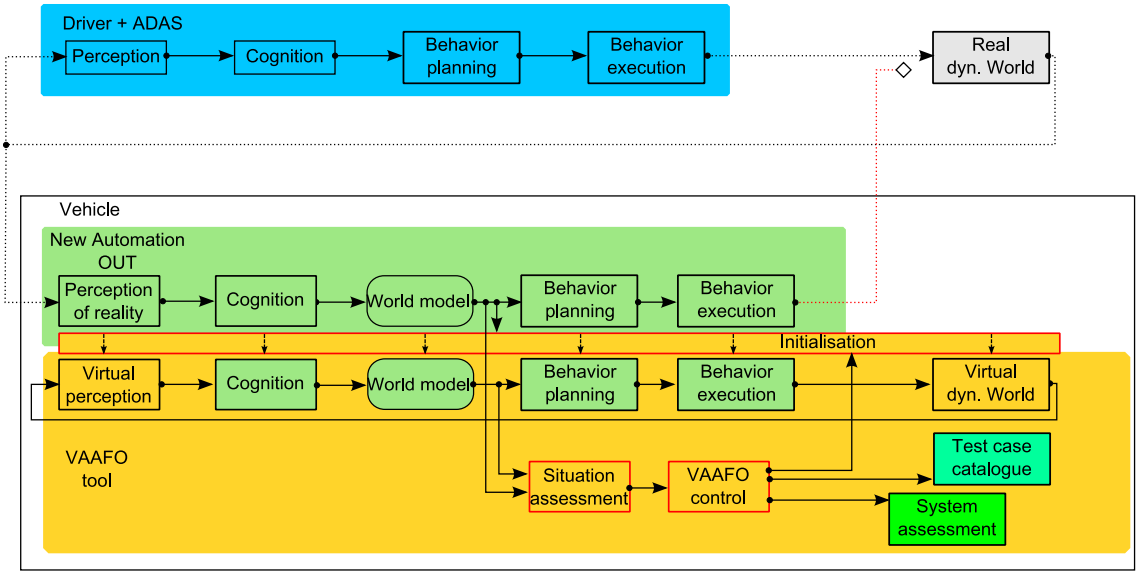


Figure 55 VAAFO concept architecture[289]

Further detailed explanation on this concept can be found in Wachenfeld and Winner[289] or Junietz et al.[290]. Figure 55 illustrates that with this concept both data sources are accessible: human driving behavior at real usage in state of the art vehicles as well as AD3+ simulated behavior for this real usage. It is an advanced naturalistic driving study with both systems in place that should be compared. Of course, this approach is not free from the necessity of a translation factor, but it is as close to real driving as possible.

When VAAFO is applied in a huge scale, all information about the distance driven as well as the events that occur during this driving is accessible. The equipment of vehicles with these functionalities may violate rights of data protection. To address the contradiction of data protection and data need, the information in the data should proactively be anonymized. The principle[291] of collecting safety relevant events by a centralized entity has already been implemented in different risky industrial sectors. The Aviation Safety Reporting System (ASRS)[292] of the Federal Aviation Administration in the USA handles

[289] Wachenfeld, W.; Winner, H.: VAAFO (2015), p. 164ff.

[290] Junietz, P. et al.: Gaining Knowledge on Automated Driving's Safety (unpublished yet approx. 2016).

[291] Thomeczek, C. et al.: Critical incident reporting system (CIRS) (2012), p. 37 & 51.

[292] http://asrs.arc.nasa.gov/ accessed 24.09.2016

reports on potentially dangerous scenarios confidentially and guarantees immunity for reporting persons when they report within ten days. Similar Critical-Incident-Reporting-Systems (CIRS) exist in the medical area to improve patients' safety in hospitals. Following these examples and their lessons learnt, a Road Safety Reporting System (RSRS) should be implemented to enable the collection of data and enable more efficient tools for this data collection.

5.4 Limitation of AD3+ Usage

Q28 How can the usage of AD3+ be limited?

As chapter 3 explains, the introduction of AD3+ should be careful to consider the safety performance uncertainty. Depending on updated numbers, the usage should be limited by the defined allowed average velocity ψ_{allow}.

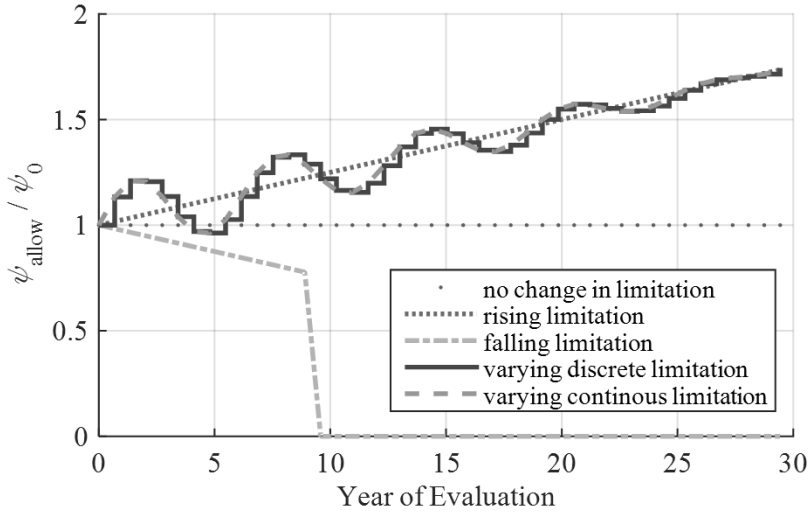


Figure 56 Possible limitation necessities

Figure 56 illustrates possible limitation scenarios. Due to changing numbers, it will be unlikely that the limitation $\psi_{\text{allow}}(t)$ will not change during the evaluation time. If the safety performance estimation will lead to higher values and/or the tolerated number of events increases, the limitation may relax, thus rise. The limitation would be tightened, thus $\psi_{\text{allow}}(t)$ would fall if the safety performance estimation indicates lower numbers and/or the tolerated numbers reduce. The limitation must also be able to hinder the total usage of AD3+ whenever the defined macroscopic theory leads to this result or a competent authority requires this step. On the other hand, also the cancellation of any limitation might result from the proof of safety.

No matter how these different possible limitations might be implemented, several generic requirements must be taken into account:

- The limitation must be use-case-embracing. Due to the tolerated number of events that is derived for a use case not an explicit product, but all vehicles within a use case must be addressed by the limitation.
- This use-case-embracing approach needs a neutral central control structure. Consequently, it seems reasonable to implement a road safety control system (RSCS) as the counterpart to the road safety report system (RSRS).
- The update of allowed average velocities would ideally happen in real-time. By implementing an update rate, it must be studied what additional risk might result from not real-time updating.
- As the possibility exists that the permission for driving AD3+ is rejected, an availability concept for the vehicles including a regular licensed driver must be in place at least during the introduction of AD3+.
- When rejecting the permission for AD3+, driving a safe handover must be guaranteed.

The requirements focus on the general managing of the control. The technical implementation might be studied as well, but due to existing concepts of OEMs there should be no technical challenge for realizing this limitation. Partially automated functions are spatially[293] or event-based[294] restricted and in combination with existing communication infrastructure[295] this limitation could also be made controllable from an external entity.

[293] Lüke, S. et al.: Traffic Jam Assistance and Automation (2016), p. 1290.

[294] Tesla Motors Inc.: Upgrading Autopilot Release Notes v8 (2016).

[295] Fuchs, H. et al.: Car-2-X (2015).; Klanner, F.; Ruhhammer, C.: Backendsysteme zur Erweiterung der Wahrnehmungsreichweite von Fahrerassistenzsystemen (2015).

6 Conclusion: Critical Concept Reflection

Q29 What are the conclusions of this thesis?

This thesis opens a new perspective on the safety assessment of AD3+. The main results will be summarized in the following four subsections. First, the concept's findings on the safety assessment are described. It is not a given thing to apply the developed concept. Consequently, the existing main challenges for concept application are described in subsection 6.2. These challenges indicate that the concept needs to be further developed before it is applied to a real-world use case. The concept consists of a usage prediction and an iterative introduction that, in principle, will improve the closer the real introduction gets. An outlook is given that describes the most important and promising next steps to improve the assessment from my point of view. The last subsection will close up the thesis. Given the knowledge gained by the taken stochastic perspective, the first question asked in this thesis is reflected: Q 1 Should automated driving be used on public streets?

6.1 Findings of the Concept on Safety Assessment of AD3+

Q30 What does the described concept tell us about the safety assessment of AD3+?

The findings are summarized chapter-wise in the following 5 subsections.

6.1.1 Findings from the Introduction Chapter

The SAE level of automation are a first step for defining the object under test, but a more detailed look on the real use cases is necessary to weight benefits and drawbacks. Benefits are versatile. Given different use cases, these can vary significantly. A good understanding of potential benefits and drawbacks is essential as other benefits besides safety are necessary to pave the way for the introduction.

Benefits and drawbacks are shared unequally in society. Taking a closer look and studying certain stakeholder groups affects and refines requirements. To come to a conclusion on the introduction, requirements on safety need to be concretized and formalized. Therefore, different quantities exist. From the society's perspective, accidents occur that lead to injuries which generate unwanted costs. These values need to be related to an exposure to the object under test. By a theoretical argumentation the safety performance

is selected to compare AD3+'s safety impact. The safety performance expresses safety by the expected distance between two events of the same kind. This safety performance was defined as two dimensional, comparing accidents with fatalities as well as accidents with injuries. Additional levels could and should be discussed.

Although safety requirements are formalized, a prospective assessment suffers uncertainty due to assumptions and simplifications. That as the result of a lack of knowledge is an unchangeable fact. Nevertheless, as the first introduction is pending it may be influenced when addressing these uncertainties proactively to enable a win-win situation for all stakeholders.

6.1.2 Findings from the State of the Art

Current test concepts are not prepared for the assessment of AD3+. Today, the human driver's controllability builds the backbone of the test concept. Comfort systems of SAE level 2 and less have been assessed and improve today's road traffic system.

The general requirements for test concept haven't changed. Test concepts must be valid, variable, observable, economical, reproducible, in good time, and safe.

However, the object under test has changed. It is unknown how the human's abilities to drive in everyday traffic can be assessed when a machine executes the driving task. As today's test concepts have not been enabled for assessing AD3+, one could attempt to prove safety by just driving enough test distance. The necessary test distance, however, leads to the "Approval-Trap": The statistical proof of safety assuming the Poisson distribution for accident events is economically not feasible ahead of introduction due to the high safety standard of today's road traffic and economical boundary conditions.

Different approaches exist to address this "Approval-Trap". These approaches are separated mainly into the microscopic approach and the macroscopic approach. The microscopic approach is part of today's research within the automotive industry and not discussed further. The macroscopic approach is the one that is described in this thesis.

6.1.3 Findings from the Concept Derivation

The macroscopic approach assumes that accidents underlie a stochastic process. Why the occurrence of accidents follows a Poisson process can be motivated by three ways. Firstly, it is a discrete process with low probability for an event so that it can be argued to follow from the Bernoulli experiment. Secondly, it has been used in the past and by different authors in research for similar studies. Thirdly, no data exists to falsify or confirm this assumption. Additionally, I assume that if enough data would exist to confirm and use another probability distribution function, the introduction challenge would have been solved.

The next scientific question, as long as a proof of safety based on the assumption of Poisson cannot be given, should be whether the proof of less safety is possible or not. When assuming an object under test approximately as good as the benchmark, this falsification of safety would again not be able ahead of introduction.

What to do next?

Refined requirements are proposed by splitting up the requirements for the user and the individual of society. The user must be enabled to come to an individual decision whether to use AD3+ or not. Therefore, it is proposed to estimate the best- and worst-case safety performance based on existing testing distance and occurred events. This should be compared with today's benchmarks of similar use cases or other means of transportation. The user can decide for himself weather to take the risk or not.

On the other hand, the individual of the society cannot choose whether to be exposed to AD3+ or not. As a part of society, the individual is just exposed because he/she participates in road traffic. But as long as the object under test is introduced only little, the safety impact for the individual of society is small. It is assumed that it is also negligible or tolerable, when the impact on safety disappears in existing noise of the society's safety detector.

Using these two refined requirements, an uncertainty-based usage strategy is defined that guarantees to a certain error probability that both requirements will be fulfilled. The specialty about the introduction theory is that it carefully and iteratively introduces and analyses safety.

How this will work, depends on several parameters of the usage strategy. These need to be defined explicitly. To understand their influence on the safety outcome, different parameter combinations (108) are studied. The main finding is that there might be an optimum for how much should be tested, how many events need to be tolerated, and how many vehicles enabling AD3+ can then be introduced. Different evaluation criteria that might be used for the real-world use case specific optimization have been identified.

This is what this thesis can offer: proposing a formalization, a prediction, and criteria for decision. To provide road traffic benefits, the concept must be applied to real use cases and must contribute to the safety lifecycle of AD3+.

6.1.4 Findings from the Discussion of Application

As the concept has been formalized, it requires data to be applied, data to define a benchmark, and data to assess the object under test. Which data should be taken for benchmark definition and object under test assessment can only be defined when a precise use case description exists. In general, it is 4 values that change over time that

need to be collected: The distance of the benchmark driven in the use case, the number of events that occur during this driving, the test distance driven of the object under test driven in the use case, as well as the number of events that occur during test driving. This sounds simple but the devil is in the detail. Additionally, generic data requirements to apply the strategy have been defined: Data must be associated with a detailed use case documentation, derived by a reviewed derivation, be up-to-date, publicly accessible, and archived.

From the four studied use cases, only the Autobahn Pilot is defined sufficiently to be assessed by this theory. For special cases, benchmarks do not exist. The right over- and under-estimation to solve this missing benchmark is necessary.

To start with a seed automation at a high safety area is not a good choice from the safety assessment point of view, as the benchmark reaches high level of safety. This might change when it is possible to neglect certain level of severity for assessment. If it is possible to convince that it is not possible to be killed by the object under test, the corresponding assessment on accident with fatality level could be obsolete.

The overall safety assessment could be a merging of area selective safety performance assessments depending on the acceptance of splitting up the usage area. The known installation of reduced speed areas like in the surrounding of schools and kindergartens is a motivator, whereas the German constitution[296] as a demotivating factor tells:

> *The dignity of man is inviolable. To respect and protect it shall be the duty of all public authority.*

Existing use cases that reported numbers for the distance driven and events that occurred (Tesla's Autopilot/Google Self-Driving) thus have no precise use case description and consequently an assessment cannot be done. The existing numbers that are used for argumentation just indicate that the "Approval-Trap" exists.

6.1.5 Findings for the Safety Lifecycle

Today's safety lifecycle that addresses all phases from item definition up to decommissioning constructs the necessary safety for AD2- vehicles. The concept described in ISO 26262 relies on the human driver's controllability. The uncertainty whether the new technology will improve safety is "hidden" behind the individual human abilities.

For AD3+ vehicle development, this uncertainty must be addressed proactively. Therefore, two safety lifecycle extensions are proposed:

[296] Grundgesetz für die Bundesrepublik Deutschland (1949), p. 1 1.Art1(1).

One is the macroscopic safety concept definition during concept phase. It is shown that the concept is necessary because more than zero events must be tolerated to start the introduction. Although no event will occur at the end, it is necessary to argue introducing. The findings from the concept theory above could build the basis for this macroscopic safety concept.

The second extension would be the application of the defined concept. This means the collection of data and control of AD3+ activation. This application of the concept must cover the development phase, as it influences the release for production. Additionally, it must cover the phase after release for production as it actively influences the operation of AD3+ vehicles.

Although the developed concept refines requirements and thereby reduces the amount of necessary testing distance ahead of introduction, the collection of data still is the challenge for usage. Real test driving will be the basis for data collection but should not be the only test tool. Especially for the testing of potential changes in software, a test translation factor is motivated. How can software-in-the-loop testing or test track testing be translated to the macroscopic safety assessment? To stay as close as possible to real-world test driving but still improve efficiency and safety, the Virtual Assessment of Automation in Field Operation (VAAFO) is proposed. It can be seen as an advanced naturalistic driving study that generates data for defining the benchmark as well as assessing the object under test.

When the concept has been defined, it has been accepted, the data has been collected, and the vehicles are in place, one thing is missing. A controlled release for usage has to be given. The technology for this centralized control already exists or is in development. But the management and how the control of AD3+ activation is realized are up for research.

6.2 Challenges for Concept Application

Q31 What might hinder the introduction of AD3+, despite the refined requirements?

6.2.1 Identification of Challenges for Concept Application

Three possible future scenarios wait for the concept application. Firstly, the concept or an offspring is accepted and AD3+ vehicles are introduced. Secondly, the concept or an offspring is accepted and AD3+ is not introduced. Thirdly, the concept and an offspring are not accepted.

The concept must be distinguished from the statistical proof of higher or less safety. The statistical proof is a part of stochastic and as an area of mathematics it is out of question. What could be challenged, however, are the numbers the concept takes to compare safety as well as to develop the introduction strategy. To study challenges beforehand that could lead the futures two and three, these challenges are identified. Let's start with the second possible future and ask: What may lead to the avoidance of introduction although the concept is applied?

- Although the introduction strategy was applied, the necessary testing distance is too large to come to an economically meaningful introduction. "Too large" has two reasons. It results from a combination of the benchmark which is too safe and the economic appropriateness that is missing.
- The safety performance level of the OuT is just not high enough. Either it is proven ahead of release for usage that the OuT is less safe compared to the defined benchmark, or the resulting allowed velocity is too small. The allowed velocity could be negligible that no significant outweighing benefits result.
- Due to an unlucky incident, an accumulation of events leads the proof of less safety although the OuT is safer. The probability of error will never be zero, thus it might happen.
- The users are not willing to accept the reached worst-case safety performance estimation. Thus, the usage demand is too little.
- The society does not tolerate any personal damage caused by an automated unsupervised system. The society or its representatives thereby would proactively decide against the introduction of the technology and require the proof of safety ahead of introduction. Thereby, society would take the risk to avoid the introduction at all. This would be a massive step and must clearly be communicated. However, examples for bans exist like the nuclear phase-out or the prohibition of fracking.

All of these reasons are reasonable and it is out of scope of this thesis to judge on that. This is different when thinking about reasons why the concept idea is not accepted to be applied. Because it should be taken care that the safety requirements identified ahead or further refined ones are met. It must not necessarily be the described concept, but there must be any concept in place to address the requirements. What may lead to the missing acceptance for application of the concept?

- Someone is just confident that the OuT is safe enough and takes the risks to introduce it. This might be possible as long as the introduction is not avoided by any type of type approval or if self-certification is sufficient without any further tests. It is questionable if this is compatible with the government's task to protect its society. This approach might end with AD3+ driving and improving safety but might al-

so end the other way around. Liability might be necessary in last instance to counterbalance unreasonable risks for affected stakeholders.

- Someone just invests the money to drive enough test distance to prove safety, although from today's point of view this seems uneconomical. Then the concept does not need to be applied as uncertainty on the safety performance has already been reduced sufficiently.
- Society just might accept low safety performance levels due to outstanding other benefits. Questionable will be if this acceptance is without opposition.
- No one can be found that finally defines the necessary definitions. The final numerical definition of tolerated fatalities for example will be one of these decision points.
- The theoretical concept is just not accepted from any of the stakeholder and another concept that for example solely bases on an established microscopic approach is applied.
- Or the reason for leaking acceptance is just a deep disagreement between the objectively derived method, discussing safety and the subjective perception of this safety. Thus, it might be that a subjective safety might only be a social construct rather than a real absence of unreasonable risks. Haverkamp and Arnold[297] explain this simplified with the safety quadrate in Table 12.

Table 12 The safety quadrat[297]

objective		
safe	unsafe	
safe	supposed safe	safe
supposed unsafe	unsafe	unsafe

subjective

The subjective perception of risks has not been in focus of this thesis but should not be forgotten when discussing the uncertainty risk based introduction of automated vehicles. The technical approach on risk analysis is not the only perspective that can be taken when thinking of public acceptance and acceptability. As Pavone et al.[298] discuss, also other approaches exist that tackle risk analysis and its acceptability. For example can causes for technology acceptability from the psychological approach be distinguished as shown in Table 13.

[297] Haverkamp, R.; Arnold, H.: Subjektive und objektive Sicherheiten (2014), p. 283.

[298] Pavone, V. et al.: Key factors affecting public acceptance and acceptability (2015), p. 51ff.

Table 13 Psychological aspects attenuating or amplifying risk perception[299]

Attenuate risk perception		Amplify risk perception
Familiarity	↔	Exoticism
Individual control	↔	Control by others
Natural	↔	Man-made
Statistical	↔	Catastrophic
Clear benefit	↔	Little or no benefit
Fair distribution	↔	Unfair distribution
Voluntary	↔	Imposed
Information from trusted sources	↔	Information from noncredible sources
In the media	↔	Not in the media

To address the challenges explained above and thereby to avoid a missing acceptability, the following outlook summarizes the necessary next steps.

6.2.2 Addressing the Challenges for Concept Application

Again, the three future scenarios from above are discussed step by step to give an outlook on how the identified challenges for concept application might be addressed:

Firstly, if the concept or an offspring is accepted and AD3+ vehicles are introduced nothing needs to be done. However, given the simplifications and outdated data this seems unlikely and it is not advised.

Secondly, if the concept or an offspring is accepted and AD3+ is not introduced it is not the concept that needs to be changed. On the contrary, it might be the purpose of the concept in this case to avoid the introduction and usage of AD3+ for the studied use case. However, this leads to another conclusion: The macroscopic safety concept may be used to find the right use case for AD3+ introduction. All the reasons that have been given are use case, user, and society sensitive. If the benchmark for a use case is too good, another use case should be chosen. If the proof of less safety has been given, it has been given for a certain use case. If the usage demand is too little due to the low safety performance estimation, other users might be addressed. If the society does not tolerate events, the exposed society should be chosen differently. Consequently, further work should not only improve the concept but also look for the right use case to apply the concept. The user as well as the society must be the ones that benefits most, because they also bear the risks.

Thirdly, if the concept and an offspring are not accepted the concept should be improved. The basic of the concept is explained in this thesis, thus it is a starting point for others to further improve the concept. As long as the required numbers exist, everybody

[299] Pavone, V. et al.: Key factors affecting public acceptance and acceptability (2015), p. 55.

can simulate their special use case. From my point of view, the main activities to improve the concept ahead of introduction should be:

- Transparently discuss the tolerated number of events k_{tol}. Additional methods to derive this value must be defined, prepared by science journalism, and actively communicated. Especially important is to identify and communicate who the responsible entity will be that defines the final value. These might be elected representatives or each individual.
- Law research should drive a case study: What would happen if a tolerated number was defined, somebody signed the fulfillment of AD3+ and different numbers of fatal events happened in reality? This would clarify the personal responsibility before these cases happen in reality. Needs for adaptation can be identified and improve the introduction.
- The right selection of test distance is an essential prerequisite to apply the derived concept. A more advanced calculation of an economic balance can be performed by companies having a more detailed insight, but also by the government. The economic balance is relative and depends on the benefits and costs that are defined as relevant.
- The simulation should be improved by introducing time variant values and improving assumptions: the safety performance benchmark SP_{bench} improves during several years of simulation, the same counts for the tolerated number of events as well as for the usage demand in general and the usage demand of mobility limited people as well as the equipment ration.

When information on real testing of AD3+ gets accessible and the introduction comes closer, the following activities are necessary:

- The motivated Road Safety Reporting System (RSRS) as well as the Road Safety Control System (RSCS) must be developed and established in good time. The RSRS should be in place as soon as the first test of AD3+ begins, but latest with the release for usage. The RSCS system must be in place with the release for usage as the communication of the release should be given by this system.

The recorded information by the RSRS could be used to:

- adapt the concept to the question: Who to blame for an accident? This ratio between being a victim or the responsible should be used do adapt the safety performance estimation.
- The same counts for the injury per accident rate IpA. If this number is known, it should be added to the concept.
- Once the time has come and the accident process underlying probability distribution gets checkable, this should be done. Especially when a super vision is planned, the new information must improve the safety assessment as well as prediction of its impact in the future.

Besides these concrete next steps, also general ideas to improve the acceptance from the psychological point of view should be studied. As a first proposal that directly follows from Table 13:

- When the usage strategy is applied, the users as well as the society should be made familiar with the concept. The promotion process should start today and report safety performance values instead of fatalities each year, or similar statistics.
- Users but also the individual should get a chance to contribute to key elements on the decision about usage.
- Catastrophic risks must be avoided. Actively developed security must hinder a systemic risk.
- The users but also the society must benefit and this should actively be influenced.
- The benefits must be distributed as the risks are. There should not be the one that is only exposed without the chance to benefit.
- AD3+ vehicles design should be in a way that the usage is voluntary. The exposure of the individual of society will not be voluntary but should follow the defined concept.
- An independent entity should inform about the concept.
- The information should proactively be communicated.

6.3 How Stochastic can Help to Introduce Automated Driving

Q32 Should automated driving be used on public streets?

This question cannot be answered using the change in safety of road traffic as the only argument, because the result of the safety assessment will most likely remain uncertain ahead of introduction. Consequently, other benefits must enable a decision to take a well-defined risk and introduce AD3+. If this prerequisite is given, the remaining uncertainty should proactively be addressed. Stochastic will help to handle this uncertainty on safety. This thesis, as one possible approach, could be used to introduce automated driving. I am not aware of other approaches addressing the safety performance uncertainty proactively.

To close up the dissertation, I want to come back to the first sentence on page 1. I assume that the first automobile has been introduced without the thoughts of this thesis. The main reason might be: 1. The mass market for automobiles did not exist, 2. The safety standards were lower, thus acceptance of events higher. Even if everybody wanted to drive an automobile in 1886, they could not. In 1903, 11235 automobiles were

sold[300] in the US. In 1923, it were[300] more than $3.62 \cdot 10^6$. Figure 57 illustrates[301] the introduction of the automobile to the world since 1900.

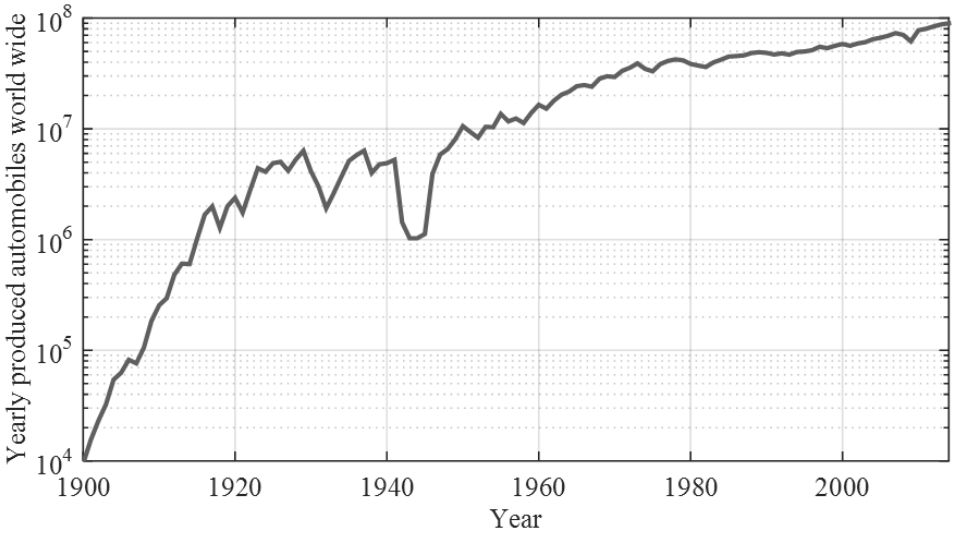


Figure 57 Yearly produced automobiles world wide (1900-2014)

Today, more than $80 \cdot 10^6$ vehicles are produced yearly. That is a huge difference compared to the introduction of the automobile that began around 1900. Thus, the usage strategy required for AD3+ was inevitably applied in 1886 for the first automobile. During these times there was no other choice to introduce the technology than do it slowly.

Today, we can shape road traffic and the use of technology. The informed individual should decide for himself whether to use AD3+ or not. Important is a risk management that controls how *much* it is used on public roads. Whether this management will then hinder the introduction or not depends on two things: The safer the AD3+ will be, the faster it will become a mass product for everyone. But more important is, the more the society tolerates that a human-built machine may also hurt a human, the faster this technology will be available.

I see this last point as the core question that must be answered or a methodology must be found to answer this question to reach the next step on the way to automated driving:

Q33 How much harm, caused by a human-built machine (AD3+), is acceptable for the exposed humans?

[300] Volti, R.: Cars and culture: The life story of a technology (2006), p. 23.

[301] Wikipedia.de: Wirtschaftszahlen zum Automobil. Cf. Ward's Automotive Group: Ward's world motor vehicle data (2007). And OICA: Automobile production statistics.

A. Tables with Values of the Poisson Distribution

Table 14 Expected values λ for fulfilling equations (2-3) and (3-18) for a probability of error of $e = 0.01$.

k	λ_-	λ_+
0	0.000	4.605
1	0.010	6.638
2	0.149	8.406
3	0.436	10.05
4	0.823	11.60
5	1.279	13.11
6	1.785	14.57
7	2.330	16.00
8	2.906	17.40
9	3.507	18.78
10	4.130	20.14
11	4.771	21.49
12	5.428	22.82
13	6.099	24.14
14	6.782	25.45
15	7.477	26.74
16	8.181	28.03
17	8.895	29.31
18	9.616	30.58
19	10.35	31.85
20	11.08	33.10
21	11.83	34.35
22	12.57	35.60
23	13.33	36.84
24	14.09	38.08

k	λ_-	λ_+
25	14.85	39.31
26	15.62	40.53
27	16.40	41.76
28	17.17	42.98
29	17.96	44.19
30	18.74	45.40
31	19.53	46.61
32	20.32	47.81
33	21.12	49.01
34	21.92	50.21
35	22.72	51.41
36	23.53	52.60
37	24.33	53.79
38	25.14	54.98
39	25.96	56.16
40	26.77	57.35
41	27.59	58.53
42	28.41	59.71
43	29.23	60.88
44	30.05	62.06
45	30.88	63.23
46	31.70	64.40
47	32.53	65.57
48	33.36	66.74
49	34.20	67.90

Table 15 Expected values λ for fulfilling equations (2-3) and (3-18) for a probability of error of $e = 0.05$.

k	λ_-	λ_+
0	0.000	2.996
1	0.051	4.744
2	0.355	6.296
3	0.818	7.754
4	1.366	9.154
5	1.970	10.51
6	2.613	11.84
7	3.285	13.15
8	3.981	14.43
9	4.695	15.71
10	5.425	16.96
11	6.169	18.21
12	6.924	19.44
13	7.690	20.67
14	8.464	21.89
15	9.246	23.10
16	10.04	24.30
17	10.83	25.50
18	11.63	26.69
19	12.44	27.88
20	13.25	29.06
21	14.07	30.24
22	14.89	31.41
23	15.72	32.59
24	16.55	33.75

k	λ_-	λ_+
25	17.38	34.92
26	18.22	36.08
27	19.06	37.23
28	19.90	38.39
29	20.75	39.54
30	21.59	40.69
31	22.44	41.84
32	23.30	42.98
33	24.15	44.13
34	25.01	45.27
35	25.87	46.40
36	26.73	47.54
37	27.59	48.68
38	28.46	49.81
39	29.33	50.94
40	30.20	52.07
41	31.07	53.20
42	31.94	54.32
43	32.81	55.45
44	33.69	56.57
45	34.56	57.69
46	35.44	58.82
47	36.32	59.94
48	37.20	61.05
49	38.08	62.17

B. Cost Calculation for Real-World Testing

Stated values for the costs for real-world testing have not been found. This, however, is necessary to define cpd_{test} for subsection 3.6.2. A value of $cpd_{\text{test}} = 2.65\ €/\text{km}$ has been estimated given the following numbers. The vehicle costs including operation have been defined based on numbers calculated from the German automobile association[302] and are listed for three examples in Table 16.

Table 16 Average vehicle costs for a user of a vehicle[302].

							Total cost (15000 km/month)	
Brand and model:	**Power kW**	**Catalog price**	**Fixed cost**	**Repair shop cost**	**Operating cost**	**Depreciation**	$\frac{€}{\text{month}}$	$\frac{€}{\text{km}}$
Audi A8 3.0 TDI quattro tiptronic	193	81000	199	83	107	1288	1677	1.342
BMW 730d Steptronic	195	82600	200	59	89	1140	1488	1.19
Mercedes S 350 d 9G-Tronic	190	82222	211	112	99	1185	1607	1.286

The costs per kilometer are weighted by the profit margin of the companies from 2012 (Mercedes Benz Cars: 7.1 %, BMW: 10.8 %, Audi: 11 %)[303] resulting in an average cost of 1.15 €/km. Besides the vehicle costs, also the costs for the test driver are necessary. These are estimated and derived based on the assumptions in Table 17.

Table 17 Assumptions to derive the average costs per kilometer of a test driver.

Average speed in km/h	50
Driving time per day in h	6
Distance per day in km	300
Working days per year	222
Distance per year in km	66600
Costs per year in €	100000
Average cost in €/km	1.50

Based on these assumptions, the average cost for test driving sums up to $cpd_{\text{test}} = 2.65\ €/\text{km}$.

[302] ADAC: ADAC Autokosten 2016.

[303] statista.de: Daimler AG - Statista-Dossier, p. 19. statista.de: BMW Group - Statista-Dossier, p. 19. statista.de: Audi AG - Statista-Dossier, p. 19.

C. Usage Strategy Δt Sensitivity

In section 3.6.2, a Δt value is assigned. This value results from the following system analysis based on the functional diagram depicted in Figure 58.

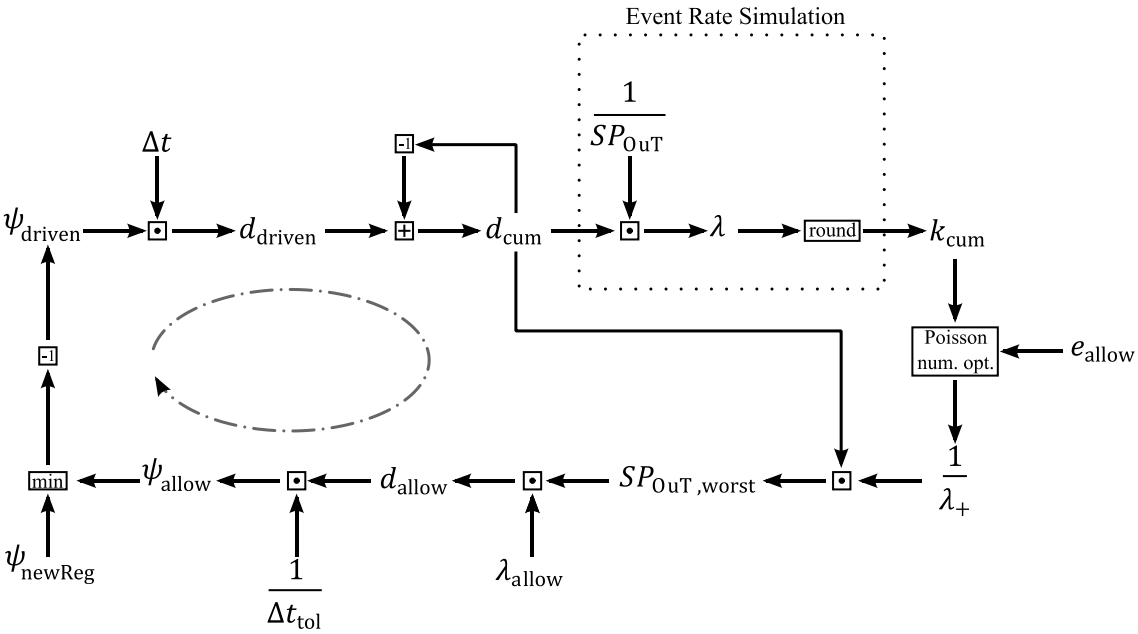


Figure 58 Functional diagram of the basic usage strategy simulation

To study the sensitivity of the usage simulation outcome, the algebraic equation to calculate d_{cum} for the end of simulation t_{FulDep} is derived. As can be seen, it depends on the size of the time steps Δt

$$\Delta t = \frac{t_{\mathrm{FulDep}}}{N} \tag{C-1}$$

and leads N simulation loops. For the first simulation loop, the equation can be written as

$$d_{\mathrm{cum}}(1 \cdot \Delta t) = \psi_{\mathrm{driven}}(1 \cdot \Delta t)\Delta t + d_{\mathrm{cum}}(0) \tag{C-2}$$

with the driven velocity being

$$\psi_{\mathrm{driven}}(1 \cdot \Delta t) = \frac{\lambda_{\mathrm{allow}}}{\lambda_+ \Delta t_{\mathrm{tol}}} d_{\mathrm{cum}}(0) \tag{C-3}$$

together results

$$d_{\mathrm{cum}}(1 \cdot \Delta t) = d_{\mathrm{cum}}(0)\left(\frac{\lambda_{\mathrm{allow}}}{\lambda_+ \Delta t_{\mathrm{tol}}}\Delta t + 1\right). \tag{C-4}$$

When calculating the Nth step thus until the end of simulation t_{FulDep} the cumulative distance gets

$$d_{\mathrm{cum}}\left(t_{\mathrm{FulDep}}\right) = d_{\mathrm{cum}}(0)\left(\frac{\lambda_{\mathrm{allow}}}{\lambda_{+}\Delta t_{\mathrm{tol}}}\Delta t + 1\right)^{N}. \tag{C-5}$$

Applying equation (C-1) to (C-5), the sensitivity of the outcome (represented by the overall distance) is described by

$$d_{\mathrm{cum}}\left(\, t_{\mathrm{FulDep}}\right) = d_{\mathrm{cum}}(\,0)\left(1 + \frac{\lambda_{\mathrm{allow}}}{\lambda_{+}\Delta t_{\mathrm{tol}}}\frac{t_{\mathrm{FulDep}}}{N}\right)^{N} \tag{C-6}$$

In this case, the behavior of the equation is studied under the limit of N to infinity. Formulary tells[304] that for $N \to \infty$ the limit is $\left(1 + \frac{i}{N}\right)^{N} \to \mathrm{e}^{i}$. Applying this to equation (C-6) results in the limit

$$\begin{aligned} d_{\mathrm{cum}}\left(t_{\mathrm{FulDep}}\right) &= \lim_{N\to\infty} d_{\mathrm{cum}}(0)\left(1 + \frac{\lambda_{\mathrm{allow}}}{\lambda_{+}\Delta t_{\mathrm{tol}}}\frac{t_{\mathrm{FulDep}}}{N}\right)^{N} \\ &= d_{\mathrm{cum}}(0)\cdot \mathrm{e}^{\frac{\lambda_{\mathrm{allow}}}{\lambda_{+}\Delta t_{\mathrm{tol}}}t_{\mathrm{FulDep}}}. \end{aligned} \tag{C-7}$$

Thus, when minimizing Δt the outcome convergs to one value. To choose Δt for simulation a worst-case estimation is executed. The relative error due to $\Delta t > 0$ can be calculated using equations (C-6) and (C-7)

$$\Delta_{\mathrm{rel},d_{\mathrm{cum}}}(N) = 1 - \frac{\left(1 + \frac{\lambda_{\mathrm{allow}}}{\lambda_{+}\Delta t_{\mathrm{tol}}}\frac{t_{\mathrm{FulDep}}}{N}\right)^{N}}{\mathrm{e}^{\frac{\lambda_{\mathrm{allow}}}{\lambda_{+}\Delta t_{\mathrm{tol}}}t_{\mathrm{FulDep}}}}. \tag{C-8}$$

It is assumed that if $\Delta_{\mathrm{rel},d_{\mathrm{cum}}}(N) < 0.1$, the error is small enough to be neglected. Thus for the worst-case estimation, the factor $\beta = \frac{\lambda_{\mathrm{allow}}}{\lambda_{+}\Delta t_{\mathrm{tol}}}$ as well as the time t_{FulDep} is concretized with reasonable values and the corresponding N is found numerically. The conclusion is, the larger β and t_{FulDep} the more simulation steps are needed and the smaller Δt gets (see Figure 59). The minimum value $\underline{\Delta \mathrm{t} > 0.4\ \mathrm{h}}$ is found for $\lambda_{\mathrm{allow}} = 39$, $\lambda_{+} = 3$, $\Delta t_{\mathrm{tol}} = 365 \cdot 24\mathrm{h}$ and $t_{\mathrm{FulDep}} = 30 \cdot 365.25 \cdot 24\mathrm{h}$ resulting in $6.5 \cdot 10^{5}$ simulation steps. This will be during the start of usage (t_{PoS}). λ_{+} will always increase whereas λ_{allow} might increase or decrease depending on the usage strategy.

[304] Merziger, G. et al.: Formeln+ Hilfen zur Höheren Mathematik. (2007), p. F3.

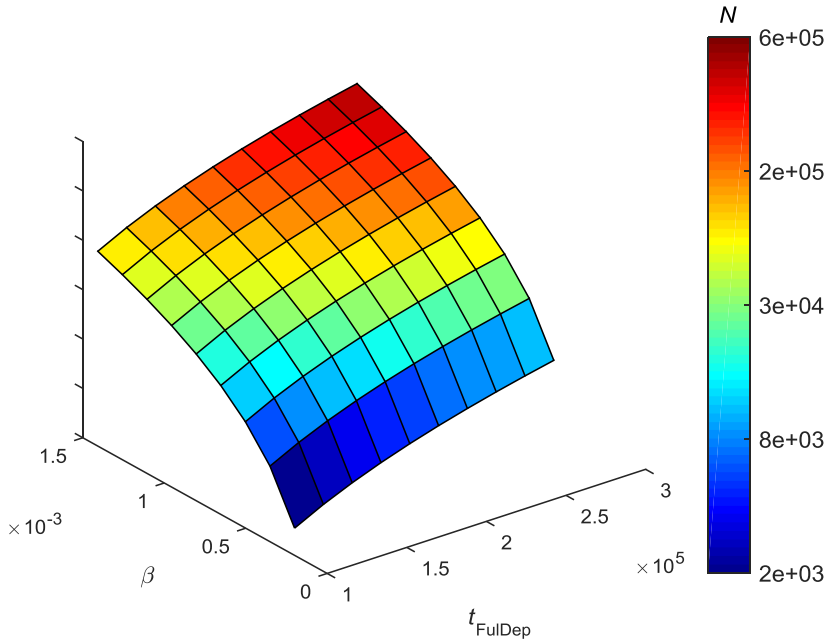


Figure 59 N fulfilling $\Delta_{rel,d,cum}(N) < 0.1$ as a function of β and t_{FulDep}

D. Tables to Examine the Usage Strategy Parameter Combinations

Characteristic Value – t_{PoS}

Table 18 lists the point in time t_{PoS} (in years) when the PoS for higher (dark) or lower (light) safety on events with *fatalities* is given depending on the assumption about the *SP* as well as the defined usage strategy. (nPoS/nPolS means no proof of safety or less safety during $\Delta t_{\mathrm{FulDep}}$)

Usage Strategy			$\frac{SP_{\mathrm{OuT}}}{SP_{\mathrm{bench}}}$			
M-k_{tol}	$k_{\mathrm{detL,wF}}$	$d_{\mathrm{test,0}}$ in 10^6km	0.1	0.2	1.34	10
Detector's Limit	0	2.67	nPolS	nPolS	nPoS	nPoS
		29.6	nPolS	nPolS	nPoS	nPoS
		100	nPolS	nPolS	nPoS	nPoS
	3	2.67	1.912E+01	2.485E+01	nPoS	2.538E+01
		29.6	1.031E+01	1.604E+01	nPoS	1.657E+01
		100	3.013E+00	1.045E+01	nPoS	1.211E+01
	39	2.67	5.342E-01	6.942E-01	3.579E+00	7.732E-01
		29.6	2.937E-01	4.574E-01	3.345E+00	6.206E-01
		100	1.001E-01	3.137E-01	3.296E+00	5.901E-01
Mobility Replacement	0	2.67	nPolS	nPolS	nPoS	nPoS
		29.6	nPolS	nPolS	nPoS	nPoS
		100	nPolS	nPolS	nPoS	nPoS
	3	2.67	1.912E+01	2.485E+01	nPoS	2.238E+01
		29.6	1.031E+01	1.604E+01	nPoS	1.357E+01
		100	3.013E+00	1.045E+01	nPoS	9.105E+00
	39	2.67	5.307E-01	6.762E-01	2.530E+00	7.481E-01
		29.6	2.900E-01	4.398E-01	2.484E+00	6.137E-01
		100	9.811E-02	2.989E-01	2.477E+00	5.901E-01
Special Needs Safety Account	0	2.67	2.797E+00	3.011E+00	5.445E+00	2.995E+00
		29.6	2.361E+00	2.708E+00	5.409E+00	2.663E+00
		100	1.724E+00	2.402E+00	5.392E+00	2.447E+00
	3	2.67	2.554E+00	2.785E+00	5.339E+00	2.764E+00
		29.6	2.069E+00	2.463E+00	5.304E+00	2.402E+00
		100	1.306E+00	2.121E+00	5.289E+00	2.163E+00
	39	2.67	5.456E-01	7.090E-01	3.936E+00	7.712E-01
		29.6	2.972E-01	4.786E-01	3.909E+00	6.206E-01
		100	1.001E-01	3.226E-01	3.902E+00	5.901E-01

Table 19 lists the point in time t_{PoS} (in years) when the PoS for higher (dark) or lower (light) safety on events with *injuries* is given depending on the assumption about the SP as well as the defined usage strategy. (nPoS/nPolS means no proof of safety or less safety during $\Delta t_{\mathrm{FulDep}}$)

Usage Strategy			$\frac{SP_{\mathrm{OuT}}}{SP_{\mathrm{bench}}}$			
M-k_{tol}	**$k_{\mathrm{detL,wI}}$**	**$d_{\mathrm{test,0}}$ in 10^6km**	0.1	0.2	1.34	10
Detector's Limit	0	2.67	nPolS	nPolS	nPoS	nPoS
		29.6	before RfU	before RfU	nPoS	nPoS
		100	before RfU	before RfU	nPoS	2.852E-04
	121	2.67	5.487E-01	4.321E+00	2.352E+01	1.122E+01
		29.6	before RfU	before RfU	1.471E+01	2.412E+00
		100	before RfU	before RfU	1.025E+01	2.852E-04
	1216	2.67	1.626E-02	1.215E-01	6.599E-01	3.143E-01
		29.6	before RfU	before RfU	4.207E-01	7.757E-02
		100	before RfU	before RfU	3.496E-01	2.852E-04
Mobility Replacement	0	2.67	nPolS	nPolS	nPoS	nPoS
		29.6	before RfU	before RfU	nPoS	nPoS
		100	before RfU	before RfU	nPoS	2.852E-04
	121	2.67	5.487E-01	4.321E+00	2.343E+01	1.122E+01
		29.6	before RfU	before RfU	1.462E+01	2.412E+00
		100	before RfU	before RfU	1.016E+01	2.852E-04
	1216	2.67	1.626E-02	1.215E-01	6.126E-01	3.134E-01
		29.6	before RfU	before RfU	3.890E-01	7.672E-02
		100	before RfU	before RfU	3.434E-01	2.852E-04
Special Needs Safety Account	0	2.67	1.196E+00	1.880E+00	2.939E+00	2.398E+00
		29.6	before RfU	before RfU	2.592E+00	1.637E+00
		100	before RfU	before RfU	2.365E+00	2.852E-04
	121	2.67	5.339E-01	1.502E+00	2.704E+00	2.108E+00
		29.6	before RfU	before RfU	2.326E+00	1.192E+00
		100	before RfU	before RfU	2.074E+00	2.852E-04
	1216	2.67	1.626E-02	1.215E-01	6.574E-01	3.143E-01
		29.6	before RfU	before RfU	4.275E-01	7.757E-02
		100	before RfU	before RfU	3.496E-01	2.852E-04

Evaluation Criteria for the Time Span $\Delta t_{\mathrm{intro}}$

Table 20 lists $r_{\mathrm{c,RvD}}$ depending on the assumption about the SP as well as the defined usage strategy. (nPoS means NN as no Proof of Safety during $\Delta t_{\mathrm{FulDep}}$)

Usage Strategy			$\frac{SP_{\mathrm{OuT}}}{SP_{\mathrm{bench}}}$			
M-k_{tol}	$k_{\mathrm{detL,wF}}$	$d_{\mathrm{test,0}}$ in 10^6km	0.1	0.2	1.34	10
Detector's Limit	0	2.67	nPolS	nPolS	nPoS	nPoS
		29.6	nPolS	nPolS	nPoS	nPoS
		100	nPolS	nPolS	nPoS	nPoS
	3	2.67	549.82%	280.23%	nPoS	-63.58%
		29.6	311.73%	214.43%	nPoS	-49.54%
		100	91.09%	140.47%	nPoS	-36.54%
	39	2.67	15.07%	8.28%	-1.59%	-0.93%
		29.6	7.28%	4.65%	-1.29%	-0.13%
		100	1.11%	2.43%	-1.22%	0.00%
Mobility Replacement	0	2.67	nPolS	nPolS	nPoS	nPoS
		29.6	nPolS	nPolS	nPoS	nPoS
		100	nPolS	nPolS	nPoS	nPoS
	3	2.67	549.82%	280.23%	nPoS	-60.04%
		29.6	311.73%	214.43%	nPoS	-40.96%
		100	91.09%	140.47%	nPoS	-27.43%
	39	2.67	14.96%	8.01%	-0.08%	-0.80%
		29.6	7.14%	4.35%	-0.01%	-0.09%
		100	1.02%	2.15%	0.00%	0.00%
Special Needs Safety Account	0	2.67	84.42%	40.24%	-3.68%	-8.69%
		29.6	71.24%	36.16%	-3.64%	-7.65%
		100	52.04%	32.06%	-3.63%	-6.97%
	3	2.67	77.02%	37.18%	-3.57%	-7.97%
		29.6	62.37%	32.84%	-3.54%	-6.82%
		100	39.35%	28.25%	-3.52%	-6.06%
	39	2.67	15.44%	8.50%	-2.02%	-0.92%
		29.6	7.40%	5.00%	-1.99%	-0.13%
		100	1.11%	2.60%	-1.99%	0.00%

Table 21 lists $r_{d,\mathrm{LvD}}$ depending on the assumption about the SP as well as the defined usage strategy. (nPoS means NN as no Proof of Safety during $\Delta t_{\mathrm{FulDep}}$)

Usage Strategy			$\frac{SP_{\mathrm{OuT}}}{SP_{\mathrm{bench}}}$			
M-k_{tol}	**$k_{\mathrm{detL,wF}}$**	**$d_{\mathrm{test,0}}$ in 10^6km**	0.1	0.2	1.34	10
Detector's Limit	0	2.67	nPolS	nPolS	nPoS	nPoS
		29.6	nPolS	nPolS	nPoS	nPoS
		100	nPolS	nPolS	nPoS	nPoS
	3	2.67	-99.91%	-99.82%	nPoS	-98.87%
		29.6	-99.75%	-99.67%	nPoS	-97.81%
		100	-98.84%	-99.36%	nPoS	-96.04%
	39	2.67	-3.42%	-1.18%	-0.04%	-0.95%
		29.6	0.00%	0.00%	0.00%	0.00%
		100	0.00%	0.00%	0.00%	0.00%
Mobility Replacement	0	2.67	nPolS	nPolS	nPoS	nPoS
		29.6	nPolS	nPolS	nPoS	nPoS
		100	nPolS	nPolS	nPoS	nPoS
	3	2.67	-99.91%	-99.82%	nPoS	-98.65%
		29.6	-99.75%	-99.67%	nPoS	-96.76%
		100	-98.84%	-99.36%	nPoS	-93.00%
	39	2.67	-3.46%	-1.25%	-0.09%	-1.02%
		29.6	0.00%	0.00%	0.00%	0.00%
		100	0.00%	0.00%	0.00%	0.00%
Special Needs Safety Account	0	2.67	-95.89%	-89.96%	-22.65%	-73.79%
		29.6	-95.30%	-88.40%	-16.19%	-63.10%
		100	-96.43%	-87.95%	-12.74%	-54.27%
	3	2.67	-95.07%	-88.27%	-18.92%	-69.35%
		29.6	-93.89%	-85.98%	-12.20%	-54.93%
		100	-93.80%	-84.56%	-8.65%	-41.91%
	39	2.67	-3.82%	-1.13%	-0.04%	-0.96%
		29.6	0.00%	0.00%	0.00%	0.00%
		100	0.00%	0.00%	0.00%	0.00%

Table 22 lists r_ψ depending on the assumption about the SP as well as the defined usage strategy. (nPoS means NN as no Proof of Safety during $\Delta t_{\mathrm{FulDep}}$)

Usage Strategy			$\frac{SP_{\mathrm{OuT}}}{SP_{\mathrm{bench}}}$			
M-k_{tol}	$k_{\mathrm{detL,wF}}$	$d_{\mathrm{test,0}}$ in 10^6km	0.1	0.2	1.34	10
Detector's Limit	0	2.67	nPolS	nPolS	nPoS	nPoS
		29.6	nPolS	nPolS	nPoS	nPoS
		100	nPolS	nPolS	nPoS	nPoS
	3	2.67	10898%	8061%	nPoS	1218%
		29.6	9824%	7795%	nPoS	1212%
		100	6266%	7047%	nPoS	1196%
	39	2.67	304.19%	224.96%	200.06%	77.76%
		29.6	274.70%	217.51%	200.00%	96.37%
		100	174.82%	196.50%	199.85%	100.00%
Mobility Replacement	0	2.67	nPolS	nPolS	nPoS	nPoS
		29.6	nPolS	nPolS	nPoS	nPoS
		100	nPolS	nPolS	nPoS	nPoS
	3	2.67	10898%	8061%	nPoS	303.18%
		29.6	9824%	7795%	nPoS	301.72%
		100	6266%	7047%	nPoS	297.69%
	39	2.67	295.18%	206.77%	98.03%	80.37%
		29.6	266.79%	199.83%	99.80%	97.49%
		100	169.87%	180.53%	100.00%	100.00%
Special Needs Safety Account	0	2.67	467.82%	294.09%	134.15%	39.91%
		29.6	607.41%	366.89%	139.85%	52.07%
		100	830.56%	434.81%	139.75%	65.74%
	3	2.67	512.71%	317.94%	139.89%	42.81%
		29.6	690.58%	405.60%	142.88%	57.08%
		100	1091%	495.40%	145.95%	73.86%
	39	2.67	313.18%	239.20%	194.33%	77.96%
		29.6	282.96%	238.47%	200.17%	96.37%
		100	174.82%	208.93%	201.22%	100.00%

Evaluation Criteria for the Time Span Δt_{suvi}

Table 23 lists C_{total} (in €) depending on the assumption about the SP as well as the defined usage strategy.

Usage Strategy			$\frac{SP_{OuT}}{SP_{bench}}$			
M-k_{tol}	$k_{detL,wF}$	$d_{test,0}$ in 10^6km	0.1	0.2	1.34	10
Detector's Limit	0	2.67	2.18E+11	9.69E+10	-6.14E+09	-2.18E+10
		29.6	2.18E+11	9.69E+10	-6.14E+09	-2.18E+10
		100	2.18E+11	9.69E+10	-6.14E+09	-2.18E+10
	3	2.67	2.18E+11	9.68E+10	-6.14E+09	-2.18E+10
		29.6	2.18E+11	9.68E+10	-6.14E+09	-2.17E+10
		100	2.18E+11	9.68E+10	-6.14E+09	-2.17E+10
	39	2.67	2.16E+11	9.53E+10	-5.48E+09	-6.34E+09
		29.6	2.16E+11	9.53E+10	-5.47E+09	-6.33E+09
		100	2.16E+11	9.53E+10	-5.47E+09	-6.33E+09
Mobility Replacement	0	2.67	2.18E+11	9.69E+10	-6.14E+09	-2.18E+10
		29.6	2.18E+11	9.69E+10	-6.14E+09	-2.18E+10
		100	2.18E+11	9.69E+10	-6.14E+09	-2.18E+10
	3	2.67	2.18E+11	9.68E+10	-6.14E+09	-2.02E+10
		29.6	2.18E+11	9.68E+10	-6.13E+09	-1.63E+10
		100	2.18E+11	9.68E+10	-6.13E+09	-1.41E+10
	39	2.67	2.16E+11	9.50E+10	-4.58E+09	-6.08E+06
		29.6	2.16E+11	9.49E+10	-4.58E+09	-3.29E+05
		100	2.16E+11	9.49E+10	-4.58E+09	-
Special Needs Safety Account	0	2.67	2.12E+11	9.14E+10	-3.81E+09	-2.97E+08
		29.6	2.12E+11	9.14E+10	-3.81E+09	-2.44E+08
		100	2.12E+11	9.14E+10	-3.81E+09	-2.15E+08
	3	2.67	2.12E+11	9.13E+10	-3.80E+09	-2.52E+08
		29.6	2.12E+11	9.14E+10	-3.80E+09	-2.01E+08
		100	2.12E+11	9.13E+10	-3.80E+09	-1.73E+08
	39	2.67	2.12E+11	9.13E+10	-3.77E+09	-8.00E+06
		29.6	2.12E+11	9.13E+10	-3.77E+09	-4.94E+05
		100	2.12E+11	9.13E+10	-3.77E+09	-

Table 24 lists $r_{\mathrm{d,ml}}$ depending on the assumption about the SP as well as the defined usage strategy.

Usage Strategy			$\frac{SP_{\mathrm{OuT}}}{SP_{\mathrm{bench}}}$			
M-k_{tol}	$k_{\mathrm{detL,wF}}$	$d_{\mathrm{test,0}}$ in 10^6km	0.1	0.2	1.34	10
Detector's Limit	0	2.67	100.00%	100.00%	100.00%	100.00%
		29.6	100.00%	100.00%	100.00%	100.00%
		100	100.00%	100.00%	100.00%	100.00%
	3	2.67	99.88%	99.79%	99.25%	97.95%
		29.6	99.81%	99.65%	98.41%	93.45%
		100	99.76%	99.57%	97.92%	90.34%
	39	2.67	86.42%	73.44%	-	-
		29.6	86.40%	73.43%	-	-
		100	86.39%	73.43%	-	-
Mobility Replacement	0	2.67	100.00%	100.00%	100.00%	100.00%
		29.6	100.00%	100.00%	100.00%	100.00%
		100	100.00%	100.00%	100.00%	100.00%
	3	2.67	99.88%	99.79%	98.86%	70.05%
		29.6	99.81%	99.65%	96.53%	31.00%
		100	99.76%	99.57%	95.04%	13.80%
	39	2.67	85.09%	68.38%	-	-
		29.6	85.06%	68.37%	-	-
		100	85.05%	68.37%	-	-
Special Needs Safety Account	0	2.67	52.67%	5.45%	1.00%	0.99%
		29.6	52.66%	5.46%	0.71%	0.67%
		100	52.66%	5.45%	0.55%	0.48%
	3	2.67	52.61%	5.34%	0.80%	0.79%
		29.6	52.60%	5.35%	0.51%	0.47%
		100	52.60%	5.33%	0.36%	0.29%
	39	2.67	51.92%	4.21%	-	-
		29.6	51.96%	4.29%	-	-
		100	52.00%	4.32%	-	-

Table 25 lists ΔC_{driven}(in €) depending on the assumption about the SP as well as the defined usage strategy.

Usage Strategy			$\frac{SP_{\text{OuT}}}{SP_{\text{bench}}}$			
M-k_{tol}	**$k_{\text{detL,wF}}$**	**$d_{\text{test,0}}$ in 10^6km**	0.1	0.2	1.34	10
Detector's Limit	0	2.67	-	-	-	-
		29.6	-	-	-	-
		100	-	-	-	-
	3	2.67	-1.66E+07	-1.18E+07	2.81E+06	2.62E+07
		29.6	-2.54E+07	-2.02E+07	5.78E+06	8.53E+07
		100	-3.15E+07	-2.53E+07	8.03E+06	1.27E+08
	39	2.67	-1.78E+09	-1.58E+09	6.66E+08	1.55E+10
		29.6	-1.79E+09	-1.59E+09	6.71E+08	1.55E+10
		100	-1.80E+09	-1.60E+09	6.72E+08	1.55E+10
Mobility Replacement	0	2.67	-	-	-	-
		29.6	-	-	-	-
		100	-	-	-	-
	3	2.67	-1.66E+07	-1.18E+07	3.60E+06	1.62E+09
		29.6	-2.54E+07	-2.02E+07	1.34E+07	5.54E+09
		100	-3.15E+07	-2.53E+07	1.77E+07	7.72E+09
	39	2.67	-1.96E+09	-1.89E+09	1.56E+09	2.18E+10
		29.6	-1.97E+09	-1.91E+09	1.56E+09	2.18E+10
		100	-1.98E+09	-1.92E+09	1.56E+09	2.18E+10
Special Needs Safety Account	0	2.67	-6.19E+09	-5.50E+09	2.34E+09	2.15E+10
		29.6	-6.19E+09	-5.50E+09	2.34E+09	2.15E+10
		100	-6.19E+09	-5.50E+09	2.34E+09	2.16E+10
	3	2.67	-6.20E+09	-5.51E+09	2.34E+09	2.15E+10
		29.6	-6.20E+09	-5.51E+09	2.34E+09	2.16E+10
		100	-6.20E+09	-5.51E+09	2.34E+09	2.16E+10
	39	2.67	-6.29E+09	-5.59E+09	2.38E+09	2.18E+10
		29.6	-6.29E+09	-5.59E+09	2.38E+09	2.18E+10
		100	-6.29E+09	-5.59E+09	2.38E+09	2.18E+10

List of References

ADAC: ADAC Autokosten 2016
Allgemeiner Deutscher Automobil-Club e.V.: ADAC Autokosten 2016

Al-Haji, G.: Diss., Road Safety Development Index (2007)
Al-Haji, Ghazwan: Road Safety Development Index: Theory, Philosophy and Practice, Dissertation Linköping University Electronic Press, 2007

Altman, D. G. et al.: Statistics with confidence (2000 // 2011)
Altman, Douglas G.; Machin, David; Bryant, Trevor N.; Gardner, Martin J.: Statistics with confidence, 2. Edition, BMJ Books, London, 2000 // 2011

Andre Hegerath: Maximale Schneehöhe in Frankfurt
Andre Hegerath: Winter-Chronik: Maximale Schneehöhe in Frankfurt basierend auf Daten des Deutschen Wetter Dienst; http://www.winterchronik.de/winter-chronik.jsf;jsessionid=51F4B139CA796A66B4D480BA3392A02C#, Access 03.09.2016

Antin, J. et al.: SHRP 2 Naturalistic Driving Study (2015)
Antin, Jon; Stulce, Kelly; Eichelberger, Lisa; Hankey, Jon: SHRP 2 REPORT S2-S31-RW-1. Naturalistic Driving Study: Descriptive Comparison of the Study Sample with National Data, Washington, D.C., 2015

Armbruster, D. A.; Pry, T.: LoB, LoD, LoQ (2008)
Armbruster, David A.; Pry, Terry: Limit of blank, limit of detection and limit of quantitation, in: Clin Biochem Rev Suppl 1, Issues 29, p. S49-52, 2008

Baake, U. et al.: Testing and simulation-based validation of ESP systems for vans (2014)
Baake, Uwe; Wüst, Klaus; Maurer, Markus; Lutz, Albert: Testing and simulation-based validation of ESP systems for vans, in: ATZ worldwide (2), Issues 116, p. 30–35, 2014

DIN 50126 Bahnanwendungen (2000), DIN 50126 Bahnanwendungen - Spezifikation und Nachweis der Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit, Sicherheit (RAMS); Deutsche Fassung EN 50126:1999, 2000

Bahr, M.; Sturzbecher, D.: Bewertungsgrundlagen bei der praktischen Fahrerlaubnisprüfung (2013)
Bahr, M.; Sturzbecher, D.: Bewertungsgrundlagen zur Beurteilung der Fahrbefähigung bei der praktischen Fahrerlaubnisprüfung, in: Winner, H.; Bruder, R. (Eds.): 6. Dar-

mstädter Kolloquium Mensch+Fahrzeug: Maßstäbe des sicheren Fahrens, Ergonomia, 2013

Bainbridge, L.: Ironies of automation (1983)
Bainbridge, Lisanne: Ironies of automation, in: Automatica (6), Issues 19, p. 775–779, 1983

Bartels, A. et al.: Lateral Guidance Assistance (2016)
Bartels, Arne; Rohlfs, Michael; Hamel, Sebastian; Saust, Falko; Klauske, Lars K.: Lateral Guidance Assistance, in: Winner, Hermann et al. (Eds.): Handbook of Driver Assistance Systems: Basic Information, Components and Systems for Active Safety and Comfort, Springer International Publishing, Cham, 2016

BASt: Volkswirtschaftliche Kosten von Straßenverkehrsunfällen (2015)
Bundesanstalt für Straßenwesen: Volkswirtschaftliche Kosten von Straßenverkehrsunfällen in Deutschland; http://www.bast.de/DE/Statistik/Unfaelle-Downloads/volkswirtschaftliche_kosten.html, 2015, Access 18.03.2016

Baum, H. et al.: BASt: Volkswirtschaftliche Kosten Herleitung (2011)
Baum, Herbert; Kranz, Thomas; Westerkamp, Ulrich: Volkswirtschaftliche Kosten durch Straßenverkehrsunfälle in Deutschland, Berichte der Bundesanstalt für Straßenwesen Reihe M, Heft 208, Bundesanstalt für Straßenwesen, Bergisch Gladbach, 2011

Becker, J.: Toward Fully Automated Driving (2014)
Becker, Jan: Toward Fully Automated Driving, Proceedings of the Automated Vehicles Symposium, San Francisco, 2014

Beiker, S. A.: Legal Aspects of Autonomous Driving (2012)
Beiker, Sven A.: Legal Aspects of Autonomous Driving, in: Santa Clara L. Rev. (1145), Issues 52, 2012

Berg, G. et al.: Vehicle in the Loop (2016)
Berg, Guy; Nitsch, Verena; Färber, Berthold: Vehicle in the Loop, in: Winner, Hermann et al. (Eds.): Handbook of Driver Assistance Systems: Basic Information, Components and Systems for Active Safety and Comfort, Springer International Publishing, Cham, 2016

Bergel-Hayat, R.; Zukowska, J.: Review of time-series analysis (2015)
Bergel-Hayat, Ruth; Zukowska, Joanna: Road safety trends at national level in Europe: a review of time-series analysis performed during the period 2000–12, in: Transport Reviews (5), Issues 35, p. 650–671, 2015

Bergenhem, C. et al.: How to reach complete safety requirement refinement for autonomous vehicles (2015)
Bergenhem, Carl; Johansson, Rolf; Söderberg, Andreas; Nilsson, Jonas; Tryggvesson, Jörgen; Törngren, Martin; Ursing, Stig: How to reach complete safety requirement

refinement for autonomous vehicles, in: CARS 2015-Critical Automotive applications: Robustness & Safety, 2015

Bergk, F. et al.: Erweiterung der Software TREMOD um zukünftige Fahrzeugkonzepte, Antriebe und Kraftstoffe (2016)
Bergk, Fabian; Heidt, Christoph; Knörr, Woflram; Keller, Mario: Erweiterung der Software TREMOD um zukünftige Fahrzeugkonzepte, Antriebe und Kraftstoffe, Berichte der Bundesanstalt für Strassenwesen - Fahrzeugtechnik (F), Issues 113, 1. Edition, Wirtschaftsverlag NW, Bremen, 2016

Bernhart, W. et al.: Index "Automatisierte Fahrzeuge" (2016)
Bernhart, Wolfgang; Olschewski, Ingo; Burkard, Christian; Galander, Sven: STUDIE 1. Quartal: Index "Automatisierte Fahrzeuge", Roland Berger GmbH & fka Forschungsgesellschaft Kraftfahrwesen mbH Aachen, 2016

Binfet-Kull, M. et al.: System safety for an autonomous vehicle (1998)
Binfet-Kull, Maria; Heitmann, Peter; Ameling, Christian: System safety for an autonomous vehicle, in: IEEE Intelligent Vehicles Symposium (IV), Stuttgart, Germany, 1998

Blanco, M. et al.: Automated Vehicle Crash Rate Comparison Using Naturalistic Data (2016)
Blanco, Myra; Atwood, Jon; Russell, Sheldon; Trimble, Tammy; McClafferty, Julie; Perez, Miguel: Automated Vehicle Crash Rate Comparison Using Naturalistic Data, Virginia Tech Transportation Institute, 2016

Blincoe, L. et al.: The economic and societal impact of vehicle crashes (2015)
Blincoe, Lawrence; Miller, Ted R.; Zaloshnja, Eduard; Lawrence, Bruce A.: The economic and societal impact of motor vehicle crashes, 2010 (Revised)(Report No. DOT HS 812 013), Washington, D.C., National Highway Traffic Safety Administration, 2015

BMJV: StVUnfStatG (1990)
Bundesministeriums der Justiz und für Verbraucherschutz Gesetz über die Statistik der Straßenverkehrsunfälle (Straßenverkehrsunfallstatistik- gesetz - StVUnfStatG); zuletzt durch Artikel 497 der Verordnung vom 31. August 2015 (BGBl. I S. 1474) geändert, 15. Juni 1990

BMJV: StVG (2016)
Bundesministeriums der Justiz und für Verbraucherschutz Straßenverkehrsgesetz (StVG); in der Fassung der Bekanntmachung vom 5. März 2003 (BGBl. I S. 310, 919), das zuletzt durch Artikel 15 des Gesetzes vom 24. Mai 2016 (BGBl. I S. 1217) geändert worden ist, 2016

BMVI: Verkehr und Mobilität in Deutschland (2015)
Bundesminister für Verkehr und digitale Infrastruktur: Verkehr und Mobilität in Deutschland, 2015

BMVI et al.: Verkehr in Zahlen 2015/16 (2016)
Bundesministerium für Verkehr und digitale Infrastruktur; Deutschland; Deutsches Institut für Wirtschaftsforschung: Verkehr in Zahlen 2015/16, 44. Edition, Dt. Verkehrs-Verl., Hamburg, 2016

Bock, T.: Vehicle in the Loop-Simulation (2012)
Bock, Thomas: Bewertung von Fahrerassistenzsystemen mittels der Vehicle in the Loop-Simulation, in: Winner, Hermann; Hakuli, Stephan; Wolf, Gabriele (Eds.): Handbuch Fahrerassistenzsysteme, Vieweg+Teubner Verlag, 2012

Bortkiewicz, L. von**: Das Gesetz der kleinen Zahlen (1898)**
Bortkiewicz, Ladislaus von: Das Gesetz der kleinen Zahlen, BG Teubner, 1898

Burgdorf, F.: Diss., Eine kunden- und lebenszyklusorientierte Produktfamilienabsicherung (2010)
Burgdorf, Florian: Eine kunden- und lebenszyklusorientierte Produktfamilienabsicherung für die Automobilindustrie, Dissertation KIT Scientific Publishing; Karlsruher Institut für Technologie, 2010

Campbell, K. L. et al.: Sources of exposure data for safety analysis. (1996)
Campbell, K. L.; Joksch, H. C.; Blower, D.; Kostyniuk, L. P.; Pendleton, O. J.; Griffin III, L. I.: Sources of exposure data for safety analysis. Publication No. FHWA-RD-97-025, U.S. Department of Transportation, 1996

Chen, F. et al.: Benchmarking road safety performance (2016)
Chen, Faan; Wu, Jiaorong; Chen, Xiaohong; Wang, Jianjun; Di Wang: Benchmarking road safety performance: Identifying a meaningful reference (best-in-class), in: Accident Analysis & Prevention, Issues 86, p. 76–89, 2016

Chin, H. C.; Quddus, M. A.: Random effect negative binomial model to examine traffic accident (2003)
Chin, Hoong C.; Quddus, Mohammed A.: Applying the random effect negative binomial model to examine traffic accident occurrence at signalized intersections, in: Accident Analysis & Prevention (2), Issues 35, p. 253–259, 2003

Cowles, M.; Davis, C.: On the origins of the 5% level (1982)
Cowles, Michael; Davis, Caroline: On the origins of the .05 level of statistical significance, in: American Psychologist (5), Issues 37, p. 553, 1982

Dahmen, W.; Reusken, A.: Numerik für Ingenieure (2006)
Dahmen, Wolfgang; Reusken, Arnold: Numerik für Ingenieure und Naturwissenschaftler, Springer-Lehrbuch, Springer-Verlag, Berlin, Heidelberg, 2006

Daimler AG Press: Press report E-Class (2009)
Daimler AG Press: Mercedes-Benz präsentiert in Genf Limousine und Coupé der neuen E-Klasse; http://www.presseportal.de/pm/68912/1362873, 2009, Access 23.09.2016

Derriks, H. M.; Mak, P. M.: IRTAD: Underreporting of casualties (2007)
Derriks, Harry M.; Mak, Peter M.: Underreporting of road traffic casualties, IRTAD Special Report, 2007

Destatis: Verkehr - Verkehrsunfälle - 2012 (2013)
Statistisches Bundesamt: Verkehr - Verkehrsunfälle - Fachserie 8 Reihe 7 2012, Wiesbaden, 2013

Destatis: Gesundheit, Todesursachen in Deutschland (2014)
Statistisches Bundesamt: Gesundheit - Todesursachen in Deutschland - Fachserie 12 Reihe 4 - 2013, Wiesbaden, 2014

Destatis: Verkehrsunfälle - Zeitreihen 2014 (2015)
Statistisches Bundesamt: Verkehrsunfälle - Zeitreihen 2014, Wiesbaden, 2015

DMV California: Autonomous Vehicles Testing Regulations (2014)
Department of Motor Vehilces California: Order to Adopt Title 13, Division 1, Chapter 1 Article 3.7 -Autonomous Vehicles;
https://www.dmv.ca.gov/portal/dmv/detail/vr/autonomous/testing, 2014

Donges, E.: Fahrerverhaltensmodelle (2011)
Donges, Edmund: Fahrerverhaltensmodelle, in: Winner; Hakuli; Wolf (Eds.): Handbuch Fahrerassistenzsysteme, 2011

Donner, E. et al.: RESPONSE 3 (2007)
Donner, Eckart; Winkle, Thomas; Walz, Rainer; Schwarz, Jürgen: RESPONSE 3 - Code of Practice für die Entwicklung, Validierung und Markteinführung von Fahrerassistenzsystemen, in: VDA Technischer Kongress, 2007

Drösler, J.: Zur Methodik der Verkehrspsychologie (1965)
Drösler, J.: Zur Methodik der Verkehrspsychologie, in: Psychologie des Straßenverkehrs. Bern: Huber, 1965

Dungs et al.: The Value of Time (2016)
Dungs; Duwe; Herrmann; Schmidt; Stegmüller; Gaydoul; Peters; Sohl: The Value of Time - Nutzerbezogene Service-Potenziale durch autonomes Fahren, Stuttgart, 2016

Eckstein, L.; Zlocki, A.: Combined Methods for an Effective Evaluation (2013)
Eckstein, Lutz; Zlocki, Adrian: Safety Potential of ADAS – Combined Methods for an Effective Evaluation, in: 23rd International Technical Conference on the Enhanced Safety of Vehicles (ESV), 2013

Elvik, R.: Traffic safety (2004)
Elvik, R.: Traffic safety, in: Handbook of Transportation Engineering, McGraw-Hill, New York, 2004

ERTRAC: Automated Driving Roadmap (2015)
ERTRAC: Automated Driving Roadmap;
http://www.ertrac.org/uploads/documentsearch/id38/ERTRAC_Automated-Driving-2015.pdf, 2015, Access 22.11.2015

ETSC: Road Accident Data (2006)
European Transport Safety Council: Road Accident Data in the Enlarged European Union, 2006

EU Transport Ministers: Declaration of Amsterdam (2016)
EU Transport Ministers: Declaration of Amsterdam - Cooperation in the field of connected and automated driving, 2016

European Commission: Technology readiness levels (2014)
European Commission: G. Technology readiness levels (TRL), Horizon 2020 - Work Programme 2014-2015 General Annexes. Extract from Part 19 - Commission Decision C(2014)4995.;
ec.europa.eu/research/participants/data/ref/h2020/wp/2014_2015/annexes/h2020-wp1415-annex-g-trl_en.pdf, 2014, Access 31.08.2016

Fach, M. et al.: Bewertung der Beherrschbarkeit von Fahrerassistenzsystemen (2010)
Fach, Markus; Baumann, Frank; Breuer, Jörg; May, Alexander: Bewertung der Beherrschbarkeit von Aktiven Sicherheits- und Fahrerassistenzsystemen an den Funktionsgrenzen, in: 26. VDI/VW-Gemeinschaftstagung Fahrerassistenz und Integrierte Sicherheit, 6./7. Oktober 2010 in Wolfsburg, 2010

Fahrmeir, L. et al.: Statistik (2007)
Fahrmeir, Ludwig; Künstler, Rita; Pigeot, Iris; Tutz, Gerhard: Statistik, Springer-Lehrbuch, Springer-Verlag, Berlin, Heidelberg, 2007

Färber, B.: Communication Problems Between Autonomous Vehicles and Human Drivers (2016)
Färber, Berthold: Communication and Communication Problems Between Autonomous Vehicles and Human Drivers, in: Maurer, Markus et al. (Eds.): Autonomous Driving, Springer-Verlag, Berlin, Heidelberg, 2016

Feller, W.: An introduction to probability theory (1968)
Feller, William: An introduction to probability theory and its applications, Wiley series in probability and mathematical statistics Probability and mathematical statistics, 3. Edition, Wiley, New York, 1968

Fersen, O. v.: Ein Jahrhundert Automobiltechnik (1986)
Fersen, Olaf v. (Ed.) Ein Jahrhundert Automobiltechnik, VDI-Verl., Düsseldorf, 1986

Follmer, R. et al.: Mobilität in Deutschland 2002 (2004)
Follmer, Robert; Kunert, Uwe; Kloas, Jutta; Kuhfeld, Hartmut: Mobilität in Deutschland, Ergebnisbericht Projekt-Nr.70.0736/2003, Deutschland, 2004

Follmer, R. et al.: Mobilität in Deutschland 2008 (2010)
Follmer, Robert; Gruschwitz, Dana; Jesske, Birgit; Quandt, Sylvia; Lenz, Barbara; Nobis, Claudia; Köhler, Katja; Mehlin, Markus: Mobilität in Deutschland 2008, Ergebnisbericht Struktur – Aufkommen – Emissionen – Trends, Bonn und Berlin, 2010

Fraedrich, E. et al.: Transition pathways to fully automated driving (2015)
Fraedrich, Eva; Beiker, Sven; Lenz, Barbara: Transition pathways to fully automated driving and its implications for the sociotechnical system of automobility, in: European Journal of Futures Research (1), Issues 3, p. 1–11, 2015

Fraedrich, E.; Lenz, B.: Societal and Individual Acceptance of Autonomous Driving (2016)
Fraedrich, Eva; Lenz, Barbara: Societal and Individual Acceptance of Autonomous Driving, in: Maurer, Markus et al. (Eds.): Autonomous Driving, Springer-Verlag, Berlin, Heidelberg, 2016

Fritzsche, A. F.: Wie sicher leben wir? (1986)
Fritzsche, Andreas F.: Wie sicher leben wir?, Verlag TUV Rheinland, 1986

Fuchs, H. et al.: Car-2-X (2015)
Fuchs, Hendrik; Hofmann, Frank; Löhr, Hans; Schaaf, Gunther: Car-2-X, in: Winner, Hermann et al. (Eds.): Handbuch Fahrerassistenzsysteme: Grundlagen, Komponenten und Systeme für aktive Sicherheit und Komfort, Springer Fachmedien Wiesbaden, Wiesbaden, 2015

Gasser, T. M. et al.: Rechtsfolgen zunehmender Fahrzeugautomatisierung (2012)
Gasser, Tom M.; Arzt, Clemens; Ayoubi, Mihiar; Bartels, Arne; Bürkle, Lutz; Eier, Jana; Flemisch, Frank; Häcker, Dirk; Hesse, Tobias; Huber, Werner; Lotz, Christine; Maurer, Markus; Ruth-Schumacher, Simone; Schwarz, Jürgen; Vogt, Wolfgang: Rechtsfolgen zunehmender Fahrzeugautomatisierung, Berichte der Bundesanstalt für Strassenwesen - Fahrzeugtechnik (F), Issues 83, Wirtschaftsverl. NW Verl. für neue Wissenschaft, Bremerhaven, 2012

Gerlough, D. L.; Schuhl, A.: Use of Poisson Distribution in Highway Traffic (1955)
Gerlough, Daniel L.; Schuhl, Andre: Use of Poisson Distribution in Highway Traffic, Eno Foundation for Highway Traffic Control, Saugatuck, Connecticut, 1955

Glauner, P. et al.: Effiziente Felderprobung von Fahrerassistenzsystemen (2012)
Glauner, P.; Blumenstock, A.; Haueis, M.: Effiziente Felderprobung von Fahrerassistenzsystemen, in: UNI DAS e.V (Ed.): 8. Workshop Fahrerassistenzsysteme, Walting, 2012

Graab, B. et al.: Analyse von Verkehrsunfällen (2008)
Graab, B.; Donner, E.; Chiellino, U.; Hoppe, M.: Analyse von Verkehrsunfällen hinsichtlich unterschiedlicher Fahrerpopulationen und daraus ableitbarer Ergebnisse für die Entwicklung adaptiver Fahrerassistenzsysteme, in: 3. Tagung Aktive Sicherheit durch Fahrerassistenz, 7.-8. April in Garching, 2008

Grundgesetz für die Bundesrepublik Deutschland (1949) Grundgesetz für die Bundesrepublik Deutschland in der im Bundesgesetzblatt Teil III, Gliederungsnummer 100-1, veröffentlichten bereinigten Fassung, das zuletzt durch Artikel 1 des Gesetzes vom 23. Dezember 2014 (BGBl.I S. 2438) geändert worden ist

Gründl, M.: Diss., Fehlverhalten als Ursache von Verkehrsunfällen (2005)
Gründl, Martin: Fehler und Fehlverhalten als Ursache von Verkehrsunfällen und Konsequenzen für das Unfallvermeidungspotenzial und die Gestaltung von Fahrerassistenzsystemen, Dissertation Universität Regensburg, 2005

Grunwald, A.: Technikfolgenabschätzung - eine Einführung (2010)
Grunwald, Armin: Technikfolgenabschätzung - eine Einführung, Gesellschaft - Technik - Umwelt, , N.F., 1, ed. Sigma, Berlin, 2010

Grunwald, A.: Societal Risk Constellations for Autonomous Driving. (2016)
Grunwald, Armin: Societal Risk Constellations for Autonomous Driving., in: Maurer, Markus et al. (Eds.): Autonomous Driving, Springer-Verlag, Berlin, Heidelberg, 2016

Gurney, J. K.: Sue my car not me (2013)
Gurney, Jeffrey K.: Sue my car not me: Products liability and accidents involving autonomous vehicles, in: U. Ill. JL Tech. & Pol'y, p. 247, 2013

Haight, F. A.: Handbook of the Poisson Distribution (1967)
Haight, Frank A.: Handbook of the Poisson Distribution, Wiley, New York, 1967

Hakkert, A. S. et al.: The uses of exposure and risk in road safety studies (2002)
Hakkert, A. S.; Braimaister, L.; van Schagen, I.: The uses of exposure and risk in road safety studies, SWOV Institute for Road Safety, 2002

Hakuli, S.; Krug, M.: Virtual Integration in the Development Process (2016)
Hakuli, Stephan; Krug, Markus: Virtual Integration in the Development Process of ADAS, in: Winner, Hermann et al. (Eds.): Handbook of Driver Assistance Systems: Basic Information, Components and Systems for Active Safety and Comfort, Springer International Publishing, Cham, 2016

Harald Altinger et al.: Testing methods used in the automotive industry (2014)
Harald Altinger; Franz Wotawa; Markus Schurius: Testing methods used in the automotive industry: results from a survey, in: Proceedings of the 2014 Workshop on Joining AcadeMiA and Industry Contributions to Test Automation and Model-Based Testing, ACM, San Jose, CA, USA, 2014

Harper, D.: "accident". Online Etymology Dictionary
Harper, Douglas: "accident". Online Etymology Dictionary; http://www.etymonline.com/index.php?allowed_in_frame=0&search=accident, Access 2016.08.19

Harper, D.: "stochastic". Online Etymology Dictionary.
Harper, Douglas: "stochastic". Online Etymology Dictionary.; http://www.etymonline.com/index.php?term=stochastic, Access 2016.08.19

Hauer, E.: On exposure and accident rate (1995)
Hauer, Ezra: On exposure and accident rate, in: Traffic engineering & control (3), Issues 36, p. 134–138, 1995

Hauer, E.: Regression Modeling in Road Safety (2015)
Hauer, Ezra: The Art of Regression Modeling in Road Safety, Springer; Springer International Publishing, Cham, 2015

Hautzinger, H. et al.: Laufende Hochrechnung der Kfz-Fahrleistungen (2010)
Hautzinger, Heinz; Fuchs, Mario; Schmidt, Jochen; Stock, Wilfried: Laufende Hochrechnung der Kfz-Fahrleistungen auf der Basis von Hauptuntersuchungsdaten - Schlussbericht Band 1 FE-Nr.: 70.0832/2008, Heilbronn/Mannheim, 2010

Haverkamp, R.; Arnold, H.: Subjektive und objektive Sicherheiten (2014)
Haverkamp, Rita; Arnold, Harald: Subjektive und objektive Sicherheiten - Barometer Sicherheit in Deutschland (BaSiD), in: Niggli, Marcel A.; Marty, Lukas (Eds.): Risiken der Sicherheitsgesellschaft, Neue kriminologische Schriftenreihe Nr. 115, 1. Edition, Forum Vlg Godesberg, Mönchengladbach, 2014

Hendriks, F. et al.: Prescan and VeHIL (2010)
Hendriks, F.; Tideman, M.; Pelders, R.; Bours, R.; Liu, X.: Development tools for active safety systems: Prescan and VeHIL, in: IEEE International Conference on Vehicular Electronics and Safety (ICVES), 2010

Herz, R. et al.: Angewandte Statistik (1992)
Herz, Raimund; Schlichter, Hans G.; Siegener, Wilfried: Angewandte Statistik für Verkehrs- und Regionalplaner, Werner-Ingenieur-Texte, 2. Edition, Werner, Düsseldorf, 1992

Holló, P. et al.: Road safety performance indicators (2010)
Holló, Péter; Eksler, Vojtech; Zukowska, Joanna: Road safety performance indicators and their explanatory value: A critical view based on the experience of Central European countries, in: Scientific Research on Road Safety Management (9), Issues 48, p. 1142–1150, 2010

Horstmann, M.: Diss., Verflechtung von Test und Entwurf (2005)
Horstmann, Marc: Verflechtung von Test und Entwurf für eine verlässliche Entwicklung

eingebetteter Systeme im Automobilbereich, Dissertation Technische Universität Carolo-Wilhelmina zu Braunschweig, 2005

Hoye, B. et al.: Autonomous Driving Comparison and Evaluation (2015)
Hoye, Brett; Lambert, Daniel; Sutton, Greg: Autonomous Driving Comparison and Evaluation, US Patent 20,150,175,168, 2015

Hydén, C.: The development of a method for traffic safety evaluation (1987)
Hydén, Christer: The development of a method for traffic safety evaluation: The Swedish traffic conflicts technique
Lund Institute of Technology. Department of Traffic Planning and Engineering, Lund, 1987

ISO: DIS 26262: Road vehicles - Functional safety (2008)
ISO: DIS 26262: Road vehicles - Functional safety, 2008

ISO 8601: Representation of dates and times (2004)
ISO 8601: Data elements and interchange formats — Information interchange — Representation of dates and times, 2004

Junietz, P. et al.: Gaining Knowledge on Automated Driving's Safety (unpublished yet approx. 2016)
Junietz, Philipp; Wachenfeld, Walther; Schönemann, Valerij; Domhardt, Kai; Tribelhorn, Wadim; Winner, Hermann: Gaining Knowledge on Automated Driving's Safety, Lecture Notes in Control Science, unpublished yet approx. 2016

Kalra, N.; Paddock, S. M.: Driving to Safety: How Many Miles? (2016)
Kalra, Nidhi; Paddock, Susan M.: Driving to Safety: How Many Miles of Driving Would It Take to Demonstrate Autonomous Vehicle Reliability?, 2016

Kauermann, G.; Küchenhoff, H.: Stichproben (2011)
Kauermann, Göran; Küchenhoff, Helmut: Stichproben, Springer-Lehrbuch, Imprint: Springer, Berlin, Heidelberg, 2011

KBA: Methodische Erläuterungen zu Statistiken über den Verkehr in Kilometern der deutschen Kraftfahrzeuge (2015)
Kraftfahrt Bundesamt: Methodische Erläuterungen zu Statistiken über den Verkehr in Kilometern der deutschen Kraftfahrzeuge, 2015

Kirsten Korosec: Interview Elon Musk (2015)
Kirsten Korosec: Fortune: Elon Musk Says Tesla Vehicles Will Drive Themselves in Two Years; http://fortune.com/2015/12/21/elon-musk-interview/?xid=yahoo_fortune, 2015, Access 23.09.2016

Klanner, F.; Ruhhammer, C.: Backendsysteme zur Erweiterung der Wahrnehmungsreichweite von Fahrerassistenzsystemen (2015)
Klanner, Felix; Ruhhammer, Christian: Backendsysteme zur Erweiterung der Wahrneh-

mungsreichweite von Fahrerassistenzsystemen, in: Winner, Hermann et al. (Eds.): Handbuch Fahrerassistenzsysteme: Grundlagen, Komponenten und Systeme für aktive Sicherheit und Komfort, Springer Fachmedien Wiesbaden, Wiesbaden, 2015

Krebs, H. et al.: MEM:ein universelles Sicherheitskriterium (2000)
Krebs, Heinrich; Le Trung, Bao.; El Koursi, El M.; Firpo, Pierluigi: Minimale Endogene Mortalität: ein universelles Sicherheitskriterium, in: ETR. Eisenbahntechnische Rundschau (12), Issues 49, p. 816–821, 2000

Kröger, F.: AD im gesellschaftsgeschichtlichen Kontext (2015)
Kröger, Fabian: Das automatisierte Fahren im gesellschaftsgeschichtlichen und kulturwissenschaftlichen Kontext, in: Maurer, Markus et al. (Eds.): Autonomes Fahren, Springer Berlin Heidelberg, 2015

Kuhlmann, A.: Alptraum Technik? (1977)
Kuhlmann, Albert: Alptraum Technik?, Hoppenstedt & TÜV Rheinland, Köln, 1977

Kuhlmann, A.: Einführung in die Sicherheitswissenschaft Albert Kuhlmann (1981)
Kuhlmann, Albert: Einführung in die Sicherheitswissenschaft Albert Kuhlmann, Vieweg, Wiesbaden, 1981

Kühn, M.: Motorradunfälle in Deutschland (2016)
Kühn, Matthias: Motorradunfälle in Deutschland, Zweiradsicherheit in Deutschland, Münster, 2016

Leduc, G.: Road traffic data: Collection methods and applications (2008)
Leduc, Guillaume: Road traffic data: Collection methods and applications, in: Working Papers on Energy, Transport and Climate Change (55), Issue1, 2008

Lee, J.; Mannering, F.: Impact of roadside features on accidents (2002)
Lee, Jinsun; Mannering, Fred: Impact of roadside features on the frequency and severity of run-off-roadway accidents: an empirical analysis, in: Accident Analysis & Prevention (2), Issues 34, p. 149–161, 2002

Lensing, N.: BASt-Zählung Ausländischer Kraftfahrzeugverkehr 2008 (2010)
Lensing, Norbert: Zählungen des ausländischen Kraftfahrzeugverkehrs auf den Bundesautobahnen und Europastraßen 2008, Berichte der Bundesanstalt für Straßenwesen : V, Verkehrstechnik, Issues 197, Wirtschaftsverl. NW, Bremerhaven, 2010

Letkowski, J.: Developing Poisson probability distribution applications (2014)
Letkowski, Jerzy: Developing Poisson probability distribution applications in a cloud, in: Journal of Case Research in Business and Economics, Issues 5, p. 1, 2014

Litman, T.: Autonomous Vehicle Implementation Predictions (2014)
Litman, Todd: Autonomous Vehicle Implementation Predictions, in: Victoria Transport Policy Institute, Issues 28, 2014

Lord, D. et al.: Regression models of motor vehicle crashes (2005)
Lord, Dominique; Washington, Simon P.; Ivan, John N.: Poisson, Poisson-gamma and zero-inflated regression models of motor vehicle crashes: balancing statistical fit and theory, in: Accident Analysis & Prevention (1), Issues 37, p. 35–46, 2005

Lüke, S. et al.: Traffic Jam Assistance and Automation (2016)
Lüke, Stefan; Fochler, Oliver; Schaller, Thomas; Regensburger, Uwe: Traffic Jam Assistance and Automation, in: Winner, Hermann et al. (Eds.): Handbook of Driver Assistance Systems: Basic Information, Components and Systems for Active Safety and Comfort, Springer International Publishing, Cham, 2016

M. Davis & Co.: National Telephone Survey (2015)
M. Davis & Co.: National Telephone Survey of Reported and Unreported Motor Vehicle Crashes, Findings Report. Report No. DOT HS 812 183, Washington, DC National Highway Traffic Safety Administration (NTHSA), 2015

Madre, J.-L.; Kalinowska, D.: Vehicle-Based Surveys (2008)
Madre, Jean-Loup; Kalinowska, Dominika: Vehicle-Based Surveys: Toward more accurate and reliable data collection methods, in: 8th International Conference On Survey Methods in Transportation, Annecy, 2008

Martí, F. S.: Highway travel time estimation with data fusion (2016)
Martí, Francesc S.: Highway travel time estimation with data fusion, Springer tracts on transportation and traffic, volume 11, Springer Science and Business Media, Heidelberg, 2016

Maurer, M. et al.: Autonomes Fahren (2015)
Maurer, Markus; Gerdes, J. C.; Lenz, Barbara; Winner, Hermann (Eds.) Autonomes Fahren, Springer Berlin Heidelberg, 2015

Maurer, M. et al.: Autonomous Driving (2016)
Maurer, Markus; Gerdes, J. C.; Lenz, Barbara; Winner, Hermann (Eds.) Autonomous Driving, Springer-Verlag, Berlin, Heidelberg, 2016

Maycock, G.; Lockwood, C. R.: The accident liability of British car drivers (1993)
Maycock, G.; Lockwood, C. R.: The accident liability of British car drivers, in: Transport Reviews (3), Issues 13, p. 231–245, 1993

Merziger, G. et al.: Formeln+ Hilfen zur Höheren Mathematik. (2007)
Merziger, Gerhard; Mühlbach, Günter; Wille, Detlef; Wirth, Thomas: Formeln+ Hilfen zur Höheren Mathematik., 5. Edition, Binomi Verlag, Springe, 2007

Mitsch, S. et al.: Provably Safe Obstacle Avoidance (2013)
Mitsch, Stefan; Ghorbal, Khalil; Platzer, André: On Provably Safe Obstacle Avoidance for Autonomous Robotic Ground Vehicles, in: Robotics Science and Systems (RSS), 2013

Mittag, H.-J.: Statistik: Eine Einführung mit interaktiven Elementen (2014)
Mittag, Hans-Joachim: Statistik: Eine Einführung mit interaktiven Elementen, Springer Spektrum, Berlin, Heidelberg, 2014

Mok, B. K.-J. et al.: Wizard of Oz Design (2015)
Mok, Brian K.-J.; Sirkin, David; Sibi, Srinath; Miller, David B.; Ju, Wendy: Understanding Driver-Automated Vehicle Interactions Through Wizard of Oz Design Improvisation, in: Proceddings of the 8th International Driving Symposium on Human Factors in Driver Assessment, Training and Vehicle Design, 2015

Nicholson, A.; Wong, Y.-D.: Are accidents poisson distributed? (1993)
Nicholson, Alan; Wong, Yiik-Diew: Are accidents poisson distributed? A statistical test, in: Accident Analysis & Prevention (1), Issues 25, p. 91–97, 1993

NTHSA: Preliminary Statement of Policy Concerning Automated Vehicles (2013)
National Highway Traffic Safety Administration: Preliminary Statement of Policy Concerning Automated Vehicles, 2013

NTSB: Preliminary Report, Highway HWY16FH018 (2016)
National Transportation Safety Board: Preliminary Report, Highway HWY16FH018, 2016

Nusser, S.: Diss., Robust Learning in Safety-Related Domains (2009)
Nusser, Sebastian: Robust Learning in Safety-Related Domains, Dissertation Otto-von-Guericke-Universität Magdeburg, 2009

OECD IRTAD: Road Safety Annual Report 2016 (2016)
OECD IRTAD: Road Safety Annual Report 2016, OECD Publishing, 2016

OICA: Automobile production statistics
Organisation Internationale des Constructeurs d'Automobiles: Automobile production statistics; http://www.oica.net/category/production-statistics/, Access 18.09.2016

Ottoboni, M. A.: The dose makes the poison (1991)
Ottoboni, M. A.: The dose makes the poison, 2. Edition, Van Nostrand Reinhold, New York, 1991

Papadimitriou, E. et al.: Safety performance assessment in Europe (2013)
Papadimitriou, Eleonora; Yannis, George; Bijleveld, Frits; Cardoso, João L.: Exposure data and risk indicators for safety performance assessment in Europe, in: Accident Analysis & Prevention, Issues 60, p. 371–383, 2013

Paracelsus, T.: Septem Defensiones (1538)
Paracelsus, Theophrast: Das Buch Paragranum / Septem Defensiones. Die dritte Defension wegen des Schreibens der neuen Rezepte. Textgrundlage sind die Ausgaben: Theophrast Paracelsus: Werke. Herausgegeben von Will-Erich Peukert. Bd. 1-5, Darm-

stadt: Wissenschaftliche Buchgesellschaft, 1965, CreateSpace Independent Publishing Platform 2013, 1538

Pavone, V. et al.: Key factors affecting public acceptance and acceptability (2015)
Pavone, Vincenzo; OU, Sara D.-E.; Santiago, Elvira: D 2.4–Key factors affecting public acceptance and acceptability of SOSTs, Surprise, 2015

Pierson-Perry, J. F. et al.: Detection capability for clinical laboratory measurement (2012)
Pierson-Perry, James F.; Vaks, Jeffrey E.; Durham, A. P.: Evaluation of detection capability for clinical laboratory measurement procedures; approved guideline - second edition, Accreditation preparedness essentials for verifying test performance (SCQ02), 32: 8(2012), CLSI, Wayne, Pa., U.S.A., 2012

Proceedings of the 21st international technical conference on the enhanced safety of vehicles ESV (2009) Proceedings of the 21st international technical conference on the enhanced safety of vehicles ESV, 2009

Rasmussen, J.: Human Performance Models (1983)
Rasmussen, Jens: Skills, Rules, and Knowledge; Signals, Signs, and Symbols, and Other Distinctions in Human Performance Models, in: IEEE Transactions On Systems, Man, and Cybernetics (3), SMC-13, p. 257–266, 1983

Reichart, G.: Diss., Zuverlässigkeit beim Führen von Kraftfahrzeugen (2001)
Reichart, Günter: Menschliche Zuverlässigkeit beim Führen von Kraftfahrzeugen, Dissertation Technische Universität München, Fortschritt-Berichte, Nr. 7, VDI-Verl., Düsseldorf, 2001

Reschka, A. et al.: Entwicklungsprozess von Kollisionsschutzsystemen für Frontkollisionen (2015)
Reschka, Andreas; Rieken, Jens; Maurer, Markus: Entwicklungsprozess von Kollisionsschutzsystemen für Frontkollisionen: Systeme zur Warnung, zur Unfallschwereminderung und zur Verhinderung, in: Winner, H. et al. (Eds.): Handbuch Fahrerassistenzsysteme, 3. Edition, Vieweg-Teubner-Verlag, 2015

Reschka, A.: Diss., Fertigkeiten- und Fähigkeitengraphen (2016)
Reschka, Andreas: Fertigkeiten- und Fähigkeitengraphen als Grundlage des sicheren Betriebsvon automatisierten Fahrzeugen im öffentlichen Straßenverkehr instädtischer Umgebung (Unpublished), Dissertation Technischen Universität Carolo-Wilhelmina zu Braunschweig, 2016

Reschka, A.: Safety Concept for Autonomous Vehicles (2016)
Reschka, Andreas: Safety Concept for Autonomous Vehicles, in: Maurer, Markus et al. (Eds.): Autonomous Driving: Technical, Legal and Social Aspects, Springer Berlin Heidelberg, Berlin, Heidelberg, 2016

Richards, D. C.: Relationship between speed and risk of fatal injury (2010)
Richards, D. C.: Relationship between speed and risk of fatal injury: pedestrians and car occupants, Department for Transport, London, 2010

Rieken, J. et al.: Development Process of Forward Collision Prevention Systems (2016)
Rieken, Jens; Reschka, Andreas; Maurer, Markus: Development Process of Forward Collision Prevention Systems, in: Winner, Hermann et al. (Eds.): Handbook of Driver Assistance Systems: Basic Information, Components and Systems for Active Safety and Comfort, Springer International Publishing, Cham, 2016

Rosen, E. et al.: Literature review of pedestrian fatality risk vs. impact speed (2011)
Rosen, Erik; Stigson, Helena; Sander, Ulrich: Literature review of pedestrian fatality risk as a function of car impact speed, in: Accident Analysis & Prevention (1), Issues 43, p. 25–33, 2011

Rumar, K.: Transport safety visions, targets and strategies: beyond 2000 (1999)
Rumar, Kåre: Transport safety visions, targets and strategies: beyond 2000, in: 1st European Transport Safety Lecture. European Transport Safety Council, Brussels, Tech. Rep, 1999

SAE: International Standard J3016 (2014)
Society of Automotive Engineers: International Standard J3016: Taxonomy and Definitions for Terms related to On-Road Motor Vehicle Automated Driving Systems, SAE International, 2014

Savage, I.: Comparing the fatality risks in United States transportation across modes and over time (2013)
Savage, Ian: Comparing the fatality risks in United States transportation across modes and over time, in: Research in Transportation Economics (1), Issues 43, p. 9–22, 2013

Schittenhelm, H.: Real World effectiveness (2013)
Schittenhelm, Helmut: Advanced Brake Assist–Real World effectiveness of current implementations and next generation enlargements by Mercedes-Benz, in: Proceedings of the 23rd International Technical Conference on the Enhanced Safety of Vehicles (ESV), Seoul, South Korea, 2013

Schnieder, E.; Schnieder, L.: Verkehrssicherheit (2013)
Schnieder, Eckehard; Schnieder, Lars: Verkehrssicherheit: Maße und Modelle, Methoden und Maßnahmen für den Straßen-und Schienenverkehr, Springer-Verlag, 2013

Schoettle, B.; Sivak, M.: Real-World Crashes Involving Self-Driving Vehicles (2015)

Schoettle, Brandon; Sivak, Michael: A Preliminary Analysis of Real-World Crashes Involving Self-Driving Vehicles, 2015

Schöner, H.-P. et al.: Testing with coordinated automated driving (2009)
Schöner, Hans-Peter; Neads, Stephen; Schretter, Nikolai: Testing and verification of active safety systems with coordinated automated driving, in: Proceedings of the 21st international technical conference on the enhanced safety of vehicles ESV, 2009

Schöner, H.-P.; Hurich, W.: Testing with Coordinated Automated Vehicles (2016)
Schöner, Hans-Peter; Hurich, Wolfgang: Testing with Coordinated Automated Vehicles, in: Winner, Hermann et al. (Eds.): Handbook of Driver Assistance Systems: Basic Information, Components and Systems for Active Safety and Comfort, Springer International Publishing, Cham, 2016

Schuldt, F. et al.: Effiziente systematische Testgenerierung (2013)
Schuldt, F.; Saust, F.; Lichte, B.; Maurer, M.; Scholz, S.: Effiziente systematische Testgenerierung für Fahrerassistenzsysteme in virtuellen Umgebungen, in: Automatisierungssysteme, Assistenzsysteme und eingebettete Systeme für Transportmittel (AAET), Braunschweig, 2013

Seeck, A. et al.: GIDAS project (2009)
Seeck, A.; Gail, J.; Sferco, R.; Otte, D.; Zwipp, H.; Bakker, J.: Development of the accident investigation and data handling methodology in the GIDAS project, in: Proceedings of the 21st international technical conference on the enhanced safety of vehicles ESV, 2009

Seeger, C.: MEM - eine Konstante? (2013)
Seeger, Carsten: Das tolerierbare Grenzrisiko nach MEM - eine Konstante?, 6. Workshop zu Fragen von Risiko und Sicherheit im Verkehr, Braunschweig, 2013

Sefati, M.: Benefit Analysis of Automated Safety Systems, Report Project Ko-KOMP (2013)
Sefati, Mohsen: Benefit Analysis of Automated Safety Systems, Report Project Ko-KOMP, 2013

Shorack, G. R.: Probability for statisticians (2000)
Shorack, Galen R.: Probability for statisticians, Springer texts in statistics, Springer, New York, 2000

Singh, S.: Critical Reasons for Crashes (2015)
Singh, Santokh: Critical Reasons for Crashes Investigated in the National Motor Vehicle Crash Causation Survey, Washington, D.C., 2015

Sivak, M.; Schoettle, B.: Road safety with self-driving vehicles (2015)
Sivak, Michael; Schoettle, Brandon: Road safety with self-driving vehicles: general

limitations and road sharing with conventional vehicles, Report No. UMTRI-2015-2, University of Michigan, Ann Arbor, Transportation Research Institute, 2015

Smith, B. W.: Regulation and the Risk of Inaction (2015)
Smith, Bryant W.: Regulation and the Risk of Inaction, in: Maurer, Markus et al. (Eds.): Autonomes Fahren, Springer Berlin Heidelberg, 2015

Smith, B. W.: How Governments Can Promote Automated Driving (2016)
Smith, Bryant W.: How Governments Can Promote Automated Driving; http://ssrn.com/abstract=2749375, 2016, Access 24.09.2016

Sokolov, D. A.: heise.de - Danke dass Sie das Auto von morgen testen (2015)
Sokolov, Daniel A. J.: http://www.heise.de/newsticker/meldung/Autonome-Autos-Danke-dass-Sie-das-Auto-von-morgen-testen-2760591.html, 2015, Access 13.09.2016

Soublet, B. G.: Autonomous Vehicles in California (2016)
Soublet, Brian G.: Autonomous Vehicles in California, in: American Association of Motor Vehicle Administrators Workshop & law institute, Cincinnati, USA, 2016

Ständer, T.: Diss., Modellbasierte Methode zur Objektivierung der Risikoanalyse (2011)
Ständer, Tobias: Eine modellbasierte Methode zur Objektivierung der Risikoanalyse nach ISO 26262, Dissertation Technischen Universität Carolo-Wilhelmina zu Braunschweig, 2011

statista.de: Audi AG - Statista-Dossier
statista.de: Audi AG - Statista-Dossier; https://de.statista.com/statistik/studie/id/7296/dokument/audi-ag-statista-dossier/, Access 22.09.2016

statista.de: BMW Group - Statista-Dossier
statista.de: BMW Group - Statista-Dossier; https://de.statista.com/statistik/studie/id/7319/dokument/bmw-group-statista-dossier/, Access 22.09.2016

statista.de: Daimler AG - Statista-Dossier
statista.de: Daimler AG - Statista-Dossier; https://de.statista.com/statistik/studie/id/7431/dokument/daimler-ag-statista-dossier/, Access 22.09.2016

statista.de: Sterbetafel: Deutschland, Jahre, Geschlecht,Vollendetes Alter (2013)
statista.de: Sterbetafel: Deutschland, Jahre, Geschlecht,Vollendetes Alter; https://www-gene-sis.destatis.de/genesis/online/data;jsessionid=06C3C45E2F9F02CD74266ED33E17B88F.tomcat_GO_2_3?operation=abruftabelleAbrufen&selectionname=12621-0001&levelindex=1&levelid=1473423773217&index=1, 2013

statista.de: Durchschnittliches Alter von Pkw in Deutschland 1960 bis 2016 (2016)
statista.de: Durchschnittliches Alter von Pkw in Deutschland in den Jahren 1960 bis 2016; http://de.statista.com/statistik/daten/studie/154506/umfrage/durchschnittliches-alter-von-pkw-in-deutschland/, 2016, Access 06.05.2016

Statistik Austria: Straßenverkehrsunfälle Österreich (2016)
Statistik Austria: Straßenverkehrsunfälle Jahresergebnisse 2015, Wien, 2016

Steininger, U.; Wech, L.: Wie sicher ist sicher genug? (2013)
Steininger, U.; Wech, L.: Wie sicher ist sicher genug? Sicherheit und Risiko zwischen Wunsch und Wirklichkeit, in: 9. VDI-Tagung Fahrzeugsicherheit, 20. - 21. November 2013

Streit, T. et al.: Deutsches Mobilitätspanel Bericht 2013/2014 (2015)
Streit, Tatjana; Chlond, Bastian; Weiß, Christine; Vortisch, Ing P.: Deutsches Mobilitätspanel (MOP)-Wissenschaftliche Begleitung und Auswertungen Bericht 2013/2014: Alltagsmobilität und Fahrleistungen, Forschungsprojekt FE-Nr. 70.0864/2011, Karlsruhe, 2015

Tatar, M.; Mauss, J.: Systematic Test and Validation of Complex Embedded Systems (2014)
Tatar, Mugur; Mauss, Jakob: Systematic Test and Validation of Complex Embedded Systems, in: Embedded Real Time Software and Systems (ERTS), Toulouse, 2014

Tesla Motors Inc.: Model S - Owners guide 7.1
Tesla Motors Inc.: Model S - Owners guide 7.1 r20160112; https://www.teslamotors.com/sites/default/files/model_s_owners_manual_touchscreen_7.1_das_ap_north_america_r20160112_en_us.pdf, Access 08.09.2016

Tesla Motors Inc.: SOFTWARE RELEASE NOTES v7.1
Tesla Motors Inc.: Model S Software Release Notes v7.1; https://www.tesla.com/sites/default/files/pdfs/release_notes/tesla_model_s_software_7_1.pdf, Access 05.08.2016

Tesla Motors Inc.: Upgrading Autopilot Release Notes v8 (2016)
Tesla Motors Inc.: Upgrading Autopilot: Seeing the World in Radar; https://www.tesla.com/de_DE/blog/upgrading-autopilot-seeing-world-radar?redirect=no, 2016, Access 13.09.2016

Tesla Motors Inc.: A Tragic Loss (2016)
Tesla Motors Inc.: A Tragic Loss; https://www.tesla.com/blog/tragic-loss, 2016, Access 08.09.2016

Thomeczek, C. et al.: Critical incident reporting system (CIRS) (2012)
Thomeczek, C.; Rohe, J.; Sanguino Heinrich, A.: Critical incident reporting system (CIRS), in: Notfall + Rettungsmedizin (1), Issues 15, p. 25–29, 2012

Thomopoulos, N.; Givoni, M.: The autonomous car—a blessing or a curse (2015)
Thomopoulos, Nikolas; Givoni, Moshe: The autonomous car—a blessing or a curse for the future of low carbon mobility? An exploration of likely vs. desirable outcomes, in: European Journal of Futures Research (1), Issues 3, p. 1–14, 2015

Trafikanalys: Road traffic statistics Sweden (2016)
Trafikanalys: Vägtrafikskador 2015, Stockholm, 2016

Trottenberg, P.; Belenky, P.: Valuation of travel time in economic analysis (2011)
Trottenberg, P.; Belenky, P.: Revised departmental guidance on valuation of travel time in economic analysis, in: US Department of Transportation, Washington, DC, 2011

U.S. DOT: Federal Automated Vehicles Policy (2016)
U.S. Department of Transportation: Federal Automated Vehicles Policy, Accelerating the Next Revolution In Roadway Safety, 2016

UN: Protection and Promotion of the Rights and Dignity of Persons with Disabilities (2006)
United Nations: General Assembly: Final report of the Ad Hoc Committee on a Comprehensive and Integral International Convention on the Protection and Promotion of the Rights and Dignity of Persons with Disabilities, HeinOnline, 2006

UN/ECE: Regulation Nr. 13-H (2010)
Wirtschaftskommission der Vereinten Nationen für Europa Regelung Nr. 13-H - Einheitliche Bedingungen für die Genehmigung von Personenkraftwagen hinsichtlich der Bremsen

van Zanten, A.; Kost, F.: Brake-Based Assistance Functions (2016)
van Zanten, Anton; Kost, Friedrich: Brake-Based Assistance Functions, in: Winner, Hermann et al. (Eds.): Handbook of Driver Assistance Systems: Basic Information, Components and Systems for Active Safety and Comfort, Springer International Publishing, Cham, 2016

VDA: Automatisierung (2015)
Verband der Automobilindustrie: Automatisierung - Von Fahrerassistenzsystemen zum automatisierten Fahren;
https://www.vda.de/de/services/Publikationen/automatisierung.html, 2015, Access 08.09.2016

Viscusi, W. K.; Aldy, J. E.: The value of a statistical life (2003)
Viscusi, W. K.; Aldy, Joseph E.: The value of a statistical life: a critical review of market estimates throughout the world, in: Journal of risk and uncertainty (1), Issues 27, p. 5–76, 2003

Voigt, C.; Adamy, J.: Formelsammlung der Matrizenrechnung (2012)
Voigt, Christian; Adamy, Jürgen: Formelsammlung der Matrizenrechnung, Technik 10-2012, Oldenbourg, München, 2012

Volti, R.: Cars and culture: The life story of a technology (2006)
Volti, Rudi: Cars and culture: The life story of a technology, JHU Press, Baltimore, 2006

Vorndran, I.: Unfallstatistik-Verkehrsmittel im Risikovergleich (2010)
Vorndran, Ingeborg: Unfallstatistik-Verkehrsmittel im Risikovergleich, in: Wirtschaft und Statistik (12), p. 1083–1088, 2010

Wachenfeld, W. et al.: Use Cases for Autonomous Driving (2016)
Wachenfeld, Walther; Winner, Hermann; Gerdes, Chris; Lenz, Barbara; Maurer, Markus; Beiker, Sven A.; Fraedrich, Eva; Winkle, Thomas: Use Cases for Autonomous Driving, in: Maurer, Markus et al. (Eds.): Autonomous Driving, Springer-Verlag, Berlin, Heidelberg, 2016

Wachenfeld, W.; Winner, H.: VAAFO (2015)
Wachenfeld, Walther; Winner, Hermann: Virtual Assessment of Automation in Field Operation. A New Runtime Validation Method, in: UNI DAS e.V (Ed.): 10. Workshop Fahrerassistenzsysteme, 2015

Wachenfeld, W.; Winner, H.: Do Autonomous Vehicles Learn? (2016)
Wachenfeld, Walther; Winner, Hermann: Do Autonomous Vehicles Learn?, in: Maurer, Markus et al. (Eds.): Autonomous Driving, Springer-Verlag, Berlin, Heidelberg, 2016

Wachenfeld, W.; Winner, H.: The new role of road testing. (2016)
Wachenfeld, Walther; Winner, Hermann: The new role of road testing for the safety validation of automated vehicles, in: Horn, Martin; Watzenig, Daniel (Eds.): Automated Driving: Safer and More Efficient Future Driving, Springer International Publishing, 2016

Wachenfeld, W.; Winner, H.: The Release of Autonomous Vehicles (2016)
Wachenfeld, Walther; Winner, Hermann: The Release of Autonomous Vehicles, in: Maurer, Markus et al. (Eds.): Autonomous Driving, Springer-Verlag, Berlin, Heidelberg, 2016

Ward, R. B.: Revisiting Heinrich's law (2012)
Ward, R. B.: Revisiting Heinrich's law, in: Chemeca, Wellington, New Zealand, 2012

Ward's Automotive Group: Ward's world motor vehicle data (2007)
Ward's Automotive Group: Ward's world motor vehicle data, 2007. Edition, Southfield, MI, 2007

Weitzel, A. et al.: Absicherungsstrategien für Fahrerassistenzsysteme (2014)
Weitzel, Alexander; Winner, Hermann; Peng, Cao; Geyer, Sebastian; Lotz, Felix; Sefati,

Mohsen: Absicherungsstrategien für Fahrerassistenzsysteme mit Umfeldwahrnehmung, Berichte der Bundesanstalt für Strassenwesen - Fahrzeugtechnik (F), Issues 98, Wirtschaftsverl. NW Verl. für neue Wissenschaft, Bremerhaven, 2014

Wikipedia: Safety (2015)
Wikipedia: Safety; https://en.wikipedia.org/wiki/Safety, 2015, Access 28.12.2015

Wikipedia.de: Wirtschaftszahlen zum Automobil
Wikipedia.de: Wirtschaftszahlen zum Automobil;
https://de.wikipedia.org/wiki/Wirtschaftszahlen_zum_Automobil, Access 18.09.2016

Winner, H.: Einrichtung zum Bereitstellen von Signalen in einem Kraftfahrzeug (2002)
Winner, H.: Einrichtung zum Bereitstellen von Signalen in einem Kraftfahrzeug, Patent WO 2002058975 A1, 2002

Winner, H. et al.: Handbuch Fahrerassistenzsysteme (2015)
Winner, H.; Hakuli, Stephan; Lotz, F.; Singer, Ch. (Eds.) Handbuch Fahrerassistenzsysteme, 3. Edition, Vieweg-Teubner-Verlag, 2015

Winner, H.: Quo vadis, FAS? (2015)
Winner, Hermann: Quo vadis, FAS?, in: Winner, H. et al. (Eds.): Handbuch Fahrerassistenzsysteme, 3. Edition, Vieweg-Teubner-Verlag, 2015

Winner, H.: ADAS, Quo Vadis? (2016)
Winner, Hermann: ADAS, Quo Vadis?, in: Winner, Hermann et al. (Eds.): Handbook of Driver Assistance Systems: Basic Information, Components and Systems for Active Safety and Comfort, Springer International Publishing, Cham, 2016

Winner, H.: Fundamentals of Collision Protection Systems (2016)
Winner, Hermann: Fundamentals of Collision Protection Systems, in: Winner, Hermann et al. (Eds.): Handbook of Driver Assistance Systems: Basic Information, Components and Systems for Active Safety and Comfort, Springer International Publishing, Cham, 2016

Winner, H. et al.: Handbook of Driver Assistance Systems (2016)
Winner, Hermann; Hakuli, Stephan; Lotz, Felix; Singer, Christina (Eds.) Handbook of Driver Assistance Systems: Basic Information, Components and Systems for Active Safety and Comfort, Springer International Publishing, Cham, 2016

Winner, H.; Schopper, M.: Adaptive Cruise Control (2016)
Winner, Hermann; Schopper, Michael: Adaptive Cruise Control, in: Winner, Hermann et al. (Eds.): Handbook of Driver Assistance Systems: Basic Information, Components and Systems for Active Safety and Comfort, Springer International Publishing, Cham, 2016

Winner, H.; Wachenfeld, W.: Absicherung automatischen Fahrens (2013)
Winner, Hermann; Wachenfeld, Walther: Absicherung automatischen Fahrens, Vortrag 6. Tagung Fahrerassistenz, München, 2013

Winner, H.; Weitzel, A.: Die Freigabefalle des autonomen Fahrens (2011)
Winner, Hermann; Weitzel, Alexander: Die Freigabefalle des autonomen Fahrens, in: TU Darmstadt (Ed.): Mensch und Fahrzeug, Darmstadt, 2011

Winner, H.; Wolf, G.: Quo vadis, FAS? (2009)
Winner, Hermann; Wolf, Gabriele: Quo vadis, FAS?, in: Winner, Hermann; Hakuli, Stephan; Wolf, Gabriele (Eds.): Handbuch Fahrerassistenzsysteme, Springer, 2009

Own Publications

2016

Conferences and Workshops:

Wachenfeld, W.; Junietz, P.; Wenzel, R.; Winner, H.: The worst-time-to-collision metric for situation identification, in: IEEE Intelligent Vehicles Symposium (IV), 2016

Wachenfeld, W.; Junietz, P.; Winner H.; Themann, P.; Pütz, A.: Safety Assurance Based on an Objective Identification of Scenarios – One Approach of the PEGASUS – Project; Presentation TRB-AUVSI-Automated Vehicle Symposium, San Francisco, 2016-07-20

Winner, H.; Wachenfeld, W.: Validation of Automated Driving – Strategies and Challenges, Presentation SafetyUpdate, Aschaffenburg, 2016-05-11

Winner, H.; Wachenfeld, W.; Junietz, P.: (How) Can Safety of Automated Driving be Validated? Presentation Symposium Virtual Vehicle, Graz, 2016-05-24

Winner, H.; Wachenfeld, W.; Junietz, P.: Safety Assurance for Highly Automated Driving – The PEGASUS Approach; Presentation TRB-AUVSI-Automated Vehicle Symposium, San Francisco, 2016-07-20

Books and Journals:

Junietz, P.; Wachenfeld, W.; Schönemann, V.; Domhardt, K.; Tribelhorn, W.; Winner, H.: Gaining Knowledge on Automated Driving's Safety – The risk-free VAAFO tool. In: Proceedings 1st Workshop on Development, Testing and Verification of ADAS and ADF, Linz, 2016 (in publication)

Wachenfeld, W.; Winner, H.: The new role of road testing for the safety validation of automated vehicles. In Horn, M.; Watzenig, D.: Automated Driving – Safer and more efficient future driving; Springer International Publishing AG, 2016

Wachenfeld, W.; Winner, H.: Do Autonomous Vehicles Learn?, in: Maurer, Markus et al. (Eds.): Autonomous Driving, Springer, 2016

Wachenfeld, W.; Winner, H.: The Release of Autonomous Vehicles, in: Maurer, Markus et al. (Eds.): Autonomous Driving, Springer, 2016

Wachenfeld, W.; Winner, H.; Gerdes, Chris; Lenz, Barbara; Maurer, Markus; Beiker, Sven A.; Fraedrich, Eva; Winkle, Thomas: Use Cases for Autonomous Driving, in: Maurer, Markus et al. (Eds.): Autonomous Driving, Springer, 2016

2015

Conferences and Workshops:

Wachenfeld, W.; Winner, H.: Virtual Assessment of Automation in Field Operation – A New Runtime Validation Method. In: 10. Workshop Fahrerassistenzsysteme Uni-DAS e.V., Walting im Altmühltal, 2015-09-28

Wachenfeld, W., Winner, H.: Der Sicherheitsnachweis für autonome Fahrzeuge. In: Hilgendorf, E., Hötitzsch, S., Lutz, L.S. (Hrsg.) Rechtliche Aspekte automatisierter Fahrzeuge. Beiträge zur 2. Würzburger Tagung zum Technikrecht im Oktober 2014, 1st edn. Nomos Verlagsgesellschaft; Nomos, Baden-Baden ,2015

Winner, H.; Graupner, M.; Wachenfeld, W.: How to Address the Approval Trap for Autonomous Vehicles. In: Vortrag ITSC (Keynote), Gran Canaria, 2015-09-17

Books and Journals:

Cao, P., Wachenfeld, W., Winner, H.: Perception sensor modeling for virtual validation of automated driving. it-Information Technology 57(4), 243–251 (2015)

Wachenfeld, W., Winner, H.: Die Freigabe des autonomen Fahrens. In: Maurer, M., Gerdes, J.C., Lenz, B., Winner, H. (Hrsg.) Autonomes Fahren, pp. 439-464. Springer Berlin Heidelberg , 2015

Wachenfeld, W., Winner, H.: Lernen autonome Fahrzeuge? In: Maurer, M., Gerdes, J.C., Lenz, B., Winner, H. (Hrsg.) Autonomes Fahren, pp. 465-488. Springer Berlin Heidelberg , 2015

Wachenfeld, W., Winner, H., Gerdes, C., Lenz, B., Maurer, M., Beiker, S.A., Fraedrich, E., Winkle, T.: Use-Cases des autonomen Fahrens. In: Maurer, M., Gerdes, J.C., Lenz, B., Winner, H. (Hrsg.) Autonomes Fahren, pp. 9-37. Springer Berlin Heidelberg , 2015

Winner, H., Wachenfeld, W.: Auswirkungen des autonomen Fahrens auf das Fahrzeugkonzept. In: Maurer, M., Gerdes, J.C., Lenz, B., Winner, H. (Hrsg.) Autonomes Fahren, pp. 265-285. Springer Berlin Heidelberg , 2015

2013

Conferences and Workshops:

Winner, H.; Wachenfeld, W.: Absicherung automatischen Fahrens, Vortrag 6. Tagung Fahrerassistenz, München, 2013-11-28

Supervised Theses

Zizer, A.: Systematische Bewertung und prototypische Nutzung von für die automatische Fahrt nicht zugänglichen Informationen für die Bewertung der automatischen Fahrt. Master-Thesis Nr. 605/16, 2016

Wenzel, R.: Implementation und Bewertung des Konzepts „Minimale Zeit bis zur Kollision“ zur Kritikalitätsbewertung der Fahrt im Straßenverkehr. Bachlor-Thesis Nr. 1251/15, 2016

Koch, S.: Retrospektive Schwereschätzung eines virtuellen Unfalls auf Autobahnen in CarMaker. Bachlor-Thesis Nr. 1234/15, 2015

Hein, E.: Vereinheitlichung der monetären retrospektiven Bewertung von identifizierten Gesetzesübertretungen für die Autobahnfahrt. Bachlor-Thesis Nr. 1233/15, 2015

Zaman, Z.: Retrospektive Zerlegung und Klassifikation von Situationen für die Fahrt auf Autobahnen in CarMaker. Bachlor-Thesis Nr. 1228/15, 2015

Nix, J.: Initialisierung und Anreicherung einer virtuellen Parallelwelt in CarMaker. Bachlor-Thesis Nr. 1227/15, 2015

Bobev, G.: Engineering on driving behaviour inter-dependencies for the purpose of safe autonomous vehicles. Master-Thesis Extern Informatik (Janssen), 2015

Selvalingam, J.: Bewertung aktueller Testmethoden sowie Entwicklung einer neuen Testmethode für die Absicherung automatisierten Fahrens. Bachlor-Thesis Nr. 1176/14, 2014

Möller, T.: Identifikation der Anforderungen für die Anwendung von Maschinellem Lernen bei sicherheitsrelevanten Systemen. Bachlor-Thesis Nr. 1175/13, 2013

Steinhaus, T.: Entwicklung eines Fahrzeugkonzepts des autonomen Fahrens mit Verfügbarkeitsfahrer. Bachlor-Thesis Nr. 1170/13, 2013

Leupold, F.: Fahrzeugkonzepte für fahrerloses Fahren. Bachelor-Thesis Nr. 1167/13, 2013

Danksagung

Es ist geschafft. Ich möchte mich für die zahlreiche Unterstützung bedanken:

Professor Winner, Sie haben mich als Sparringspartner mit viel Erfahrung und kritischem Hinterfragen aktueller Herausforderungen unterstützt.

Professor Grunwald, Sie haben meinen Horizont für die Fragen zur Technikfolgenabschätzung erweitert und mich durch ihre Rückmeldungen zur Arbeit unterstütz.

Projektpartner des Projektes „Villa Ladenburg – Autonomes Fahren“ der Daimler und Benz Stiftung und des „PEGASUS“-Projekts des BMWI, Sie haben mir den Blick über den Tellerrand ermöglicht.

Meine Kollegen und Studenten der FZD-Zeit, Ihr habt mich fachlich und menschlich vielseitig unterstützt und geprägt.

Philipp und Alex, Ihr habt mir mit wertvollen Rückmeldungen zu Arbeitsständen geholfen.

Meine lieben Eltern, Ingrid und Walter, Ihr seid mein persönlicher Rückhalt in jeglicher Situation. Ihr habt es nie kritisiert und mir immer Rat und positive Energie gegeben.

Meine Liebe, Kaddi, Du verstehst, verarbeitest und gehst gemeinsam mit mir.

Danke.