13th Graz Symposium Virtual Vehicle (GSVF) 2020

Macroscopic Safety Requirements for Highly Automated Driving in Urban Environments

Christian Amersbach, Timm Ruppert, Niclas Hebgen and Hermann Winner

Abstract — **The release of automated vehicles is only possible if their safety is ensured. Thus, acceptable safety requirements for all stakeholders have to be defined. The scope of this work is a traceable proposal of a definition of macroscopic safety requirements for highly automated driving in urban environments.**

Firstly, relevant stakeholders are identified. These are the society in general, the users of automated vehicles and other road users, which are further divided into subgroups, depending on their type of traffic involvement. Secondly, the available statistical data for Germany is analyzed. Hereby the domestic annual mileage is identified as the most suitable parameter to relate the stakeholder-specific accident numbers to. The quotients of accidents of different stakeholders and the driven distance represent the current risks of manual driving in urban environments, which are used as exemplary safety reference. Thereafter, existing risk acceptance principles from other domains such as the railway industry are used to determine the acceptable risks for each stakeholder group, which can be directly used as macroscopic safety requirements.

Among other analytics, it is shown that the users of automated vehicles are attributed to the highest risk tolerance, while other road users are the most critical stakeholder group in terms of safety requirements.

Keywords — **Automated Driving, Safety Requirements, Risk Analysis**

I. Introduction

One of the major challenges for the release of highly automated vehicles (HAV, Level 3 and higher according to [1]) is their safety approval. The major question “How safe is safe enough?” has not yet been answered in detail. In this context, the term "safe enough" refers to a situation in which the risk emanating from a product is lower than the marginal risk that is still tolerated by society and legislative. It seems evident that safety requirements are no less relevant in requirements engineering than purely functional requirements. Furthermore, a strict separation of the two types of requirements is not always possible. For example, the correct functioning of the steering system of motor vehicles is a prerequisite for the avoidance of damage events whose severity may contribute to exceeding the tolerated risk.

In order to take account of the functional safety of road vehicles, ISO 26262 [2] provides guidelines in the form of (safety) processes to be carried out or methods to be applied, which serve to avoid the corresponding risks. In connection with the question of whether a new technology has reached the required maturity for its market launch, the application of methods such as those proposed in ISO 26262 forms a necessary basis for argumentation and decision-making. However, following the standard is not sufficient to answer this question. There are several reasons for this. Firstly, ISO 26262 refers to functional safety, which is only a subset of the overall system safety. Secondly, the standard focuses on electrical and/or electronic (E/E) systems. Consequently, hazards such as chemical reactions, fire or electric shock are not part of the scope of ISO 26262, unless they are due to malfunction of E/E systems. [3, pp. 11-12] In addition, methods proposed by the standard - for example the "Failure Mode and Effects Analysis" (FMEA) - only offer the possibility of their application if the system to be analyzed has already been specified to a sufficiently high level of detail. This is the case, for example, if the system and its elements can be represented as a function block diagram. [4, pp. 6-7] However, in order to define safety requirements for automated driving in general, there is no functional structure of a tangible system and the feasibility of analysis methods such as FMEA is not given.

For these reasons, a macroscopic approach is chosen, which does not aim to define safety requirements for a specific system, its assemblies or even its individual components. Nor does it address special driving or hazardous situations in road traffic. Rather, the focus is on the quantitative requirements such as a maximum number of fatal accidents per inhabitant, per time interval or per distance travelled. These are referred to as so-called macroscopic safety requirements. [5]

A definition of macroscopic safety requirements for automated driving on motorways has already been carried out by Junietz et al. [5] The aim and scientific contribution of this work is to transfer the considerations made with regard to motorway driving to the inner-city traffic situation, i.e. to define macroscopic safety requirements for automated driving within urban environments.

The research leading to these results is partly funded by the German Federal Ministry for Economic Affairs and Energy (BMWi) within the project “VVM - Verification & Validation Methods for Automated Vehicles Level 4 and 5”.

C. Amersbach and N, Hebgen were and T. Ruppert and H. Winner are with the Institute of Automotive Engineering at Technical University Darmstadt, GERMANY (e-mail: christian.amersbach@gmail.com, timm.ruppert@tu-darmstadt.de, n.hebgen@live.de, hermann.winner@tu-darmstadt.de).

II. RELATED WORK

A. Risk Acceptance Principles

Macroscopic safety requirements such as a maximum number of accidents per travelled kilometer are risk indicators. [5] Risk is generally defined as the product of the two factors: predicted amount of damage and frequency of occurrence of a damage event. [6, p. 187] Therefore, whether a quantifiable risk is below or above a tolerable limit, depends just on these two parameters. This fact is also evident from the risk graph shown in Figure 1.

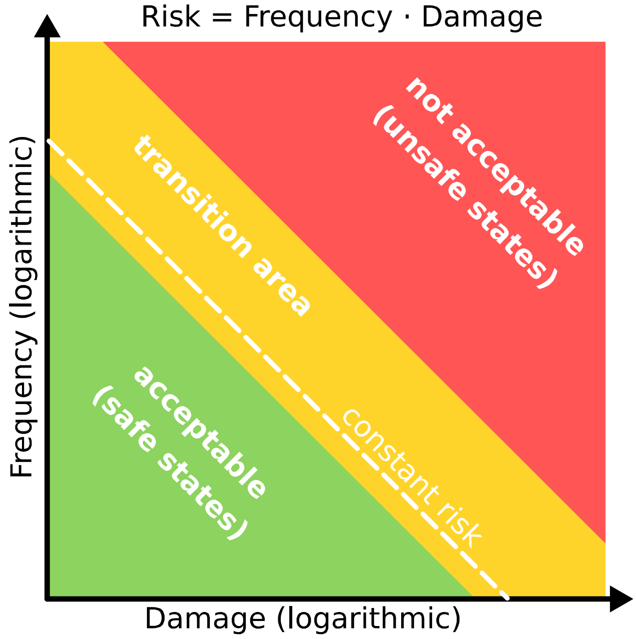

Figure 1:Risk graph based on Steininger et al. [7]

The green area at the bottom left of Figure 1 marks the range of accepted risks. If the risk emanating from a technical system is found there, the system is considered safe. In contrast, the red area in the upper right-hand corner marks the area of unaccepted risks and thus signals the uncertainty of the system. The border between accepted and unaccepted risks or between safe and unsafe systems is not exactly defined. Instead, there is a blurred transition area denoted in yellow. [5] In order to be able to formulate and quantify clear safety requirements for systems or technologies despite this diffusion, various risk acceptance principles or risk acceptance criteria have been developed. They originate from railway applications, explained in EN 50126, and have been transferred to road traffic within the scope of research. [5, 8] The following sections are discussing the three principles for the definition of accepted (limit) risks.

1) As Low as Reasonably Practicable (ALARP)

The risk of being struck by lightning is about 10^{-7} per person per year. Risks emanating from activities, technologies or events below this threshold are generally considered negligible and therefore acceptable. In contrast, the risk of fatal injury in a road traffic accident is higher. In Germany and other industrialized countries, it is in the order of 10^{-4} per person per year. In most cases higher risks are only accepted for voluntary exposures, such as in the case of extreme sports. In the transition zone between 10^{-7} and 10^{-4}, general statements on risk acceptance are not possible without further analysis. Rather, cost-benefit analyses are to be carried out within this range in order to quantify the risk that is still feasible in a specific application - taking into account technical, economic and social aspects. This means that a specific risk must be kept *as low as reasonably practicable*. [5] [8, pp. 58-59]

Quantitative cost-benefit analyses of road safety technology are only possible if the subject of discussion is a tangible system with defined elements, such as assemblies or components and quantifiable values or costs. However, this work does not aim at a specific automated vehicle but addresses automated driving independently of specific realizations. Cost-benefit analyses are therefore - at least in the narrower sense - not feasible. Accordingly, a risk acceptance principle requires higher levels of abstraction. This leads to the two principles "Minimum Endogenous Mortality" (MEM) and "Globalement au moins aussi bon" (GAMAB), which are explained in the following sections.

2) Minimum Endogenous Mortality (MEM)

Minimum endogenous mortality is based on age-specific mortality rates. Although the absolute values of these rates are not constant for all ages, there is a distinct minimum of $5{\cdot}10^{-5}$ deaths per person per year for the group of 5-15 year old children. It should be noted that the corresponding standards, still partly anticipated mortality rates from the 1980s. In the case of EN 50126 and similar standards, the assumption is made that an individual person is exposed to multiple (normed to 20) systems at the same time. According to MEM, the maximum risk, MEM/20, therefore calculates to $2{\cdot}10^{-4}$ deaths per person per year. Irrespective of which numerical value is regarded as decisive for a risk acceptance study, the MEM principle requires that the additional risks arising from a new technical system does not exceed the respective MEM/20 value or tolerable risks derived from it. Using MEM is particularly predestined for its use as criteria for risk acceptance analysis when a completely new technology is introduced that does not intend to replace an existing system. [8, p. 58] [9]

3) Globalement au moins aussi bon (GAMAB)

GAMAB is a risk acceptance criterion frequently used especially in France. The term GAMAB is derived from the French expression "Globalement au moins aussi bon", which translates as "at least as good in general". Based on the designation it is already clear that GAMAB requires the existence of a reference system. The principle implies the assumption that the risks posed by the already existing system are generally accepted. These risks define the current safety level and thus, at the same time the minimum safety requirement for a new system which means that the new system must not pose higher risks than the existing system. [7, p. 58]

4) Correlation and suitability of risk acceptance principles

Figure 2 visualizes the risk acceptance principles along with their respective marginal risks. For the quantitative classification of GAMAB, the current risk of fatal accidents on German motorways was used as a reference. The other risk acceptance principles and their respective limit values are valid independently of technical reference systems and / or locations. The graph also shows that the level of a still tolerated risk depends not least on whether the risk exposure is voluntary, occupationally, involuntary or due to large-scale technologies. While the willingness to accept risks is virtually unlimited if the exposure is voluntary - for example within the framework of leisure activities - the tolerance limit is much lower in the case of large-scale technologies such as nuclear energy. It corresponds approximately to the lower limit of the ALARP principle, which is defined by the risk of succumbing to a lightning strike. Remaining (borderline) risks can be found between these two extremes. [5]

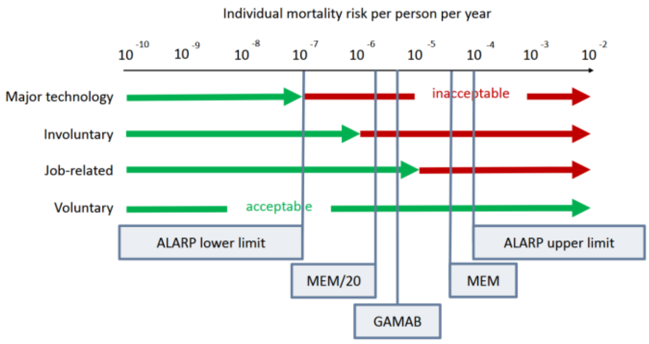

Figure 2: Risk acceptance principles and respective marginal risks [5]

The fact that the feasibility of cost-benefit analyses as part of the ALARP principle is not given in the context of automated driving in general has been explained above. Furthermore, knowing that a reference system exists in the form of the current traffic situation motivates the application of GAMAB rather than MEM for automated driving. In this context, the German Ethics Committee "Automatisiertes und vernetztes Fahren", appointed by the Federal Ministry of Transport and Digital Infrastructure (BMVI), demands the following: "The approval of automated systems is only justifiable if they promise at least a reduction of damage in the sense of a positive risk balance compared to human driving performance". [10] However, the requirement of a positive risk balance, i.e “at least as good” as a human driver is quite vague. So far it is not clear, how much better an automated driving function has to be compared to its reference. For example, Junietz et al. [5] state that a Highway-Chauffeur has to be better by a factor of 1.3, while Liu et al. conclude, that this factor is between 4 and 5 [11]. Furthermore, if a technical solution is existing, that is significantly better than the current reference, it has to be taken as new reference.

Taking this into account, the use of a risk acceptance principle based on a reference system seems not only appropriate but also mandatory even if the required improvement factor is not known. Another argument for the use of GAMAB is that MEM - as described above - is based on mortality rates. Thus, while this principle is predestined as a risk acceptance criterion for accidents involving fatalities, it is only of limited suitability for accidents of other categories, such as those involving serious injuries. Thirdly, the definition of the tolerable risk according to MEM does not differentiate between different interest groups nor between different severities. As stated above, this work focuses on the definition of safety requirements for individual interest groups specifically for urban traffic. This aspect argues against the use of MEM for the introduction of automated driving. In summary, according to the stated reasons, the focus in the further course of this work will be on GAMAB.

B. Location as a disaggregation characteristic of traffic engineering analyses

In order to determine the accepted risks of automated driving in a given location, the current risks of the existing reference system in the same location must first be identified in accordance with the GAMAB principle. [5]

Moreover, it is necessary to resort to traffic statistical surveys of different institutions. Examples are the traffic accident statistics for Germany of the Federal Statistical Office (Destatis) and the mileage surveys of the Federal Highway Research Institute (BASt). However, there is one major drawback when using accident statistics as reference: Traffic participants that tolerate a higher risk than others are more likely involved in accidents or suffer more serious injuries (e.g because of not wearing a seatbelt or speeding). Thus, accident statistics overestimate the reference risk for traffic participants in average. Nevertheless, they are used here as a reference, as the overestimation cannot be quantified and there is no better reference available.

Furthermore these sources distinguish only between three localities: urban, extra-urban (excluding motorways) and motorway. [12, 13] A further differentiation for example into "town", "municipality" and "rural group settlements", is not made. This is due to the significant differences in traffic law between the three official localities. This becomes particularly clear when comparing motorways with other localities based on the legal framework conditions:

- Motorways may only be used if the maximum design speed of the motor vehicle used is greater than 60 km/h. [14]
- Pedestrians are not allowed to enter motorways. [14]
- Level crossings must not be present on motorways. [15]
- Motorways must be equipped with special junctions for access and exit. [15]

Correspondingly sharp legal demarcations such as those described above exist between the three locations "in towns", "outside towns" and "on motorways", but not within them. This means that supposedly urban traffic situations such as intersections, traffic lights or pedestrian scenarios may occur not only in cities but also in rural areas and vice versa. Therefore, the approach of the institutions mentioned above, to not further break down localities in the context of traffic statistics surveys, is justified.

For the present study, however, this means that the definition of macroscopic safety requirements - in the absence of the necessary data material - cannot be made specifically for automated driving in cities, but only more generally for automated driving within built-up areas.

III. METHODOLOGY

Before the current risks can be quantified, it is necessary to discuss which of these risks are representative of the local traffic situation and which risks can be quantified in general. This means, for example, that the following questions must be addressed:

- Is it sufficient to consider accidents with fatalities within built-up areas or should other categories such as accidents with serious injuries be considered as a supplement?
- Are accident figures, on the one hand, or casualty figures, on the other hand, more suitable for quantifying risks?
- Which interest groups are characteristic of urban traffic and how do they differ from those on motorways?
- Which variables other than for e.g. mileage are suitable to relate accident or casualty figures to them?

These questions are discussed in the following sections.

A. Determination of an observation level for the severity of accident consequences

The German Federal Statistical Office (Destatis) distinguishes between six accident categories, which are listed in the following hierarchical structure (see Figure 3). [12, p. 20]

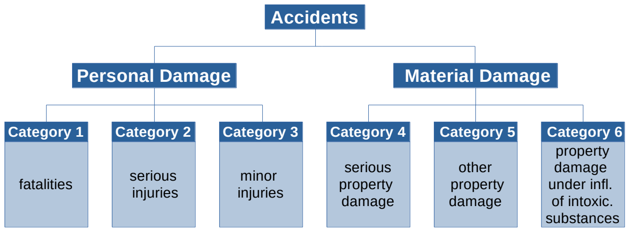

Figure 3:Classification of accidents (according to Destatis [12, p. 20])

The classification of accidents into one of these categories is always based on the most serious consequences of the accident. An accident is classified in category 1 if at least one person involved in the accident dies within 30 days. The criterion for distinguishing between minor and serious injuries is whether an inpatient hospital stay is required immediately after the accident. If there are no injured persons, but at least one motor vehicle involved is no longer roadworthy and the cause of the accident was also a criminal offence or an administrative offence, this is classified as a "*serious accident involving damage to property in the narrower sense*" (category 4). If, on the other hand, all involved motor vehicles are still roadworthy and the persons involved were under the influence of intoxicating substances such as alcohol, the accident is classified in category 6: "*other property damage accident under the influence of intoxicating substances*". All remaining property damage accidents are classified in category 5, "*other property damage accidents*". [12]

1) Accidents with fatalities (category 1)

Human life has an outstanding protection status by law. This is already evident from Article 2 of the Basic Law of the Federal Republic of Germany, according to which every person has "*the right to life*". [16] Based on this, an ethics committee, which was convened by the Federal Ministry of Transport and Digital Infrastructure, published 20 ethical rules in one of its reports, which are aimed at automated and networked vehicle traffic. The need for protection of human life is manifested in the standards of this ethics committee. For example, the second of the rules mentioned is: *"The protection of people takes precedence over all other considerations of utility"*. [10] Based on these legal and ethical principles, it is not possible to define macroscopic safety requirements for automated driving solely based on material damage accidents, for example. In contrast, it is mandatory to consider fatal accidents.

This is also shown in the macroscopic safety requirements for automated driving on motorways presented by Junietz et al. [5] who take fatal accidents into account. Nonetheless, the hypothesis exists that the distribution over the categories stated above differs significantly between motorways and built-up areas. For example, the higher (average) speeds on motorways lead to the assumption that accidents on motorways tend to be more fatal and that the percentage of minor accidents is lower than in built-up areas. If this hypothesis is correct, it should be discussed whether accident categories that are more prevalent in built-up areas should be used in addition to the mandatory category of fatal accidents when defining macroscopic safety requirements.

2) Accidents involving damage to property and accidents involving minor injuries (categories 3-6)

To test the above hypothesis accident data from the Federal Statistical Office for the year 2018 [12, pp. 56-58] and a ten-year observation period (2009 to 2018) was used, both allowing a differentiated analysis by location and accident category. Comparing the stated accident data, it becomes clear that the percentual category distribution for the two localities differ only marginally. Once again, the differences in the accident category distribution between build-up areas and motorways are smaller than expected. The picture that was already apparent in the 2018 study alone is confirmed and the hypothesis presented at the beginning is thus further questioned.

There are several possible explanations for the phenomenon that the distribution of accidents involving property damage, injuries and fatalities does not differ significantly between the two locations compared here - despite the higher speeds on motorways:

In comparison to inner-city roads, motorways have more construction measures, which serve to reduce harm and avoid fatal consequences of accidents. For example, protective barriers or similar measures are prescribed on motorways to maintain "*separate lanes for directional traffic*". According to the law, motorways must also be "*free of junctions at the same level*". [15]

Furthermore, the Road Traffic Regulations (StVO) [14] restrict the types of traffic permitted on motorways compared to other localities. For example, motorways may not be entered by pedestrians and cyclists are excluded from traffic on motorways. This means that within the built-up areas, the proportion of unprotected or at most lightly-protected road users is higher. If representatives of these groups are involved in an accident, the probability that it will end in more than just material damage is apparently greater than, for example, in the case of accidents involving only one type of vehicle. This is confirmed by the surveys of the Federal Statistical Office, according to which the majority of intra-urban fatalities in 2017 were among the weaker road users. [17]

In summary, various factors on and for motorways exist that mitigate the consequences of accidents and help compensate for the fatal effects of higher speeds. These factors provide an explanation for the nearly congruent distribution of the two locations.

In the course of the location-dependent comparison of accident distributions - in addition to the accident mitigating factors on motorways mentioned above - it is also necessary to consider how the accident data was collected. In this concern, the Federal Statistical Office makes the following statement: "*According to law, the police stations whose officers recorded the accident are obliged to provide information. It follows that the statistics only record accidents for which the police were called in; these are mainly those with serious consequences. In particular, a relatively large proportion of traffic accidents with only material damage or with only minor injuries are not reported to the police*." [12, p. 10] Accordingly, there is a discrepancy between the actual accident figures on the one hand and the numbers of accidents recorded by the police on the other - the so-called dark figure. [18]

It is generally assumed that the estimated number of unrecorded accidents involving serious injuries and fatalities both on motorways and in built-up areas is negligible, as there is an obligation to report these two categories. [12] The unrecorded figures for the remaining accident categories 3 to 6, on the other hand, are firstly higher and secondly differ depending on the location of the town or the type of road. In other words, the estimated number of unreported accidents involving property damage and minor injuries is lower for motorways than that for other localities. [18] One explanation for these different estimates is that the police are increasingly intervening on motorways even in the case of less serious accidents since minor accidents as well can have a massive impact on the traffic situation. [19, p. 6]

Irrespective of the reasons for the higher number of unreported accidents involving property damage and minor injuries in built-up areas, the following conclusions can be drawn from the distributions: The actual distributions will differ from them in that the proportion of property damage accidents will no longer be 88 to 89 per cent, but will be even higher within built-up areas and on motorways. In addition, the real proportion of property damage accidents will be higher within built-up areas than that on motorways. This circumstance is in line with the hypothesis set above.

Estimates suggest that the true accident figures for property damage accidents could be more than seven times higher than the recorded numbers. In the case of accidents involving minor injuries, the corresponding factor is over 4.5. [18] It remains questionable how high the number of unreported cases actually is and whether it is even possible to quantify them realistically. On the other hand, it seems undisputed that accident figures associated with such a large degree of uncertainty do not provide a solid data basis for defining macroscopic safety requirements for automated driving. For this reason, accidents in categories 3 to 6 will not be included in the further course of the present study - neither on their own nor in addition to the accidents with fatalities that will be definitively considered.

3) Accidents with serious injuries (category 2)

Seriously injured persons are included in the official statistics if they are "*immediately admitted to hospital for in-patient treatment (at least 24 hours)*" and do not succumb to the accident-related injuries within 30 days. If death occurs within 30 days of the accident event, the injured are counted as fatalities. In the event of death later, they continue to be considered as seriously injured only - even if the death is undoubtedly due to the accident or its consequences. [12]

If the definition of macroscopic safety requirements for automated driving within built-up areas were based solely on the number of fatalities - according to the above definition - then the safety requirements would not take into account fatally injured persons whose death occurred later than 30 days after the accident. However, from a moral philosophical point of view, it makes no difference whether a person dies because of an accident 29 or 31 days after the accident.

Furthermore, there are two existing ways to reduce the number of fatal accidents. Firstly, a complete avoidance of a fatal accident event without the occurrence of any accident. Secondly, an accident that could not have been avoided occurs, but its severity was mitigated: E.g. an accident with fatalities becomes one with serious injuries. This implies that minimizing the risk of fatal accidents entails an increase in the risk for other categories. Wachenfeld and Winner emphasize that when automated driving functions are released *"not only a reduction in the number of accidents must be demonstrated, but also an accepted relationship [...] between avoided [...] and additionally caused risks [...]"*. [20, p. 442] If a fatal accident is transformed into an accident with serious injuries by automated driving functions, this corresponds to the minimization of one risk while increasing another at the same time. In order to address the relationship between the two types of risk - as demanded by Wachenfeld and Winner - the definition of safety requirements based exclusively on fatal accidents is not sufficient.

In addition, with approximately 0.1 percent, fatal accidents make up only a marginal proportion of all accidents within built-up areas and are therefore - purely in terms of their number - not representative of all accidents. [12] In order for the macroscopic safety requirements to cover a larger share of the total number of accidents within built-up areas, at least one additional accident category must be added to the definition of safety requirements. Accidents involving material damage in the categories 4 to 6 and accidents involving minor injuries (category 3) are not suitable due to the high number of unreported cases. Consequently, only accidents with seriously injured persons (category 2) remain as a supplementary option.

Therefore, in summary to the arguments stated above, the category of serious injuries should not be ignored when defining safety requirements. Accidents with serious injuries (category 2) should therefore also be taken into account when defining macroscopic safety requirements for automated driving in built-up areas. However, it has to be mentioned that increasing the number of safety levels considered for indicating macroscopic safety requirements, results in a similar proportional increase of workload for the safety approval itself. Nonetheless, from an ethical point of view, it seems at least questionable whether and to what extent the use of the workload as an argument is permissible with regard to the methodology of the procedure here, since the definition of macroscopic safety requirements focuses on the need to protect human life and not on an economic aspect. [10]

B. Combination Methods for multiple accident categories

In the previous section, it was motivated why two accident categories have to be considered for the determination of macroscopic safety requirements: Accidents with fatalities (category 1) and those with serious injuries (category 2). A question that now needs to be addressed is how to combine the data from the two categories, as several possibilities exist.

A first potential option is the establishment of a summative limit value. This must not be exceeded by the sum of accidents involving fatalities and serious injuries. On the one hand, addressing the so-called problem of small numbers appears to be advantageous. Behind this problem lies the fact that although the numbers of fatal accidents are not small in absolute terms, in special cases they may still not be sufficiently large enough to make statistically significant statements. By adding accidents with serious injuries, the statistical data is expanded, thus making it possible to reduce the problem of small numbers.

On the other hand, a summary consideration of the two accident categories implies that a fatal accident has the same consequences as an accident with serious injuries. However, it seems evident that the accepted marginal risks of both categories differ and that the implicit equality with regard to the severity of accidents does not reflect the real risk acceptance of the population.

In order to take into account that a fatal accident is apparently more serious than one with severe injuries, a second approach consists in offsetting accidents from both categories against each other could be considered. This means, for example, that it could be determined and then defined that one fatal accident (category 1) corresponds to 10 serious injuries (category 2) in terms of severity of consequences. [5] This would in theory make it possible to generate a single limit value that covers both accident categories, as is already the case with the summative approach. However, the Ethics Committee on Automated and Networked Driving prohibits the offsetting of traffic accident victims. [10] Furthermore, it is not clear which factor should be used to convert one accident category into another. Therefore, the approach of converting accidents in one category into those in another category is also ruled out for the further procedure.

The option remains of determining a separate, still-tolerated limit value for both fatal accidents and accidents with serious injuries. This means that the number of accidents from category 1 must be below the limit value for accidents involving fatalities. In coexistence, the number of accidents from category 2 must not exceed the limit value for accidents with serious injuries. In contrast to the two previous approaches, two limits must therefore always be observed independently. Thus, there is no reduction to a common limit value for both accident severity levels. This increases the amount of work that has to be performed in the course of the statistical verification of the required safety. However, the amount of work is not doubled, since, for example, the step of converting accidents of one category into accidents of another category is no longer necessary. In addition, the procedure discussed here also enables more differentiated analyses than the two possible combinations of accident categories 1 and 2 as discussed above. For example, if an automated vehicle would not initially meet its macroscopic safety requirements. In this case, the existence of individual limit values opens up the possibility of assessing which accident severity level is more likely to require addressing by appropriate measures in order to achieve approval.

Due to the implicit equality of both accident categories that must be avoided, the ethical boundary conditions and the potential for differentiated analyses, the variant presented last will be further pursued.

C. Trade-off between accident and casualty figures

In its publications on traffic accidents, the Federal Statistical Office relates both accident and casualty figures to various reference values. [12] Therefore, in the further course of this work, it must be considered whether it is more appropriate to consider accidents on the one hand or casualties on the other to define macroscopic safety requirements for automated driving within built-up areas.

A single accident may cause several victims and/or injured parties who are linked to the one accident and are therefore not independent in terms of the causing event. The casualty figures may vary for different accidents with the same event, as the casualty figures are depending on multiple boundary conditions that might not be possible to be conceived for a statistical analysis.

In special cases, however, accidents also pose the problem of dependency. The following scenario illustrates this: an accident with personal injury occurs at an inner-city intersection involving the need of the police to control the traffic that is obstructed by the accident. Meanwhile, one of these officers is hit by a car and fatally injured. The subsequent accident would not have happened if the first accident that initiated the deployment of the police had not occurred. In this specific case, there is not only a dependency between the injured parties, but also between the two accidents.

According to the Federal Statistical Office, scenarios such as the one described above however, belong to a category, which claims fewer than five per cent of fatal accidents within built-up areas in 2018. This also includes accidents involving road workers who are not involved in an accident, but who are on the roadway for work reasons, or accidents involving occupants of breakdown vehicles. [12] This means that the actual number of subsequent accidents outlined above will be even lower than the share of just under five percent as mentioned earlier. This supports the thesis that accidents with mutual dependency are exceptional rather than regular situations.

In conclusion, it can be stated that the accident figures have the potential to represent the one event that leads to at least one or more fatalities better than causality figures and are therefore preferable. Thus, the approach of using accident numbers instead of fatalities is used for the work described in this paper.

D. *Identification of relevant stakeholder groups*

Automated vehicles pose a risk to various groups of road users. The individual groups differ in terms of the risks they accept. [5] Accordingly, macroscopic safety requirements should not be defined for road users in general, but rather for specific groups. As a basis for this group-specific definition of macroscopic safety requirements, the first step is to identify the relevant stakeholder groups for automated driving within built-up areas.

According to [5], it is possible to divide all stakeholders of automated driving into three general groups: *the users of automated vehicles*, *other road users* and *society*. Although it can be argued that *users* and *other road users* also belong to *society, society* here denotes that part of the population which is not directly affected by the accident-related fate of an individual, but for which only the total number of accidents is relevant. In the further course of this work, the focus will be on the interest group of *other road users* and their sub-groups, which are yet to be determined, since *the users of automated vehicles* are attributed higher tolerated border risks in the relevant literature. The latter assumption is based on two factors. Firstly, although every newly introduced technology carries a new and/or additional risk, this is accepted by its users because they hope to gain a profit from its use in other respects. Secondly, commercial, i.e. work-related, or even involuntary use of automated vehicles is not to be expected in typical cases of application in the short to medium term. It is assumed that the use of automated driving functions is almost exclusively voluntary. [5] In cases of voluntary risk exposure the tolerated limit risks are always higher than for occupational or involuntary exposure. [5] Consequently, *other road users* who may potentially be involved in accidents with automated vehicles constitute a more critical stakeholder group than the *users* themselves. Furthermore, they represent the majority of society. These arguments justify the non-exclusive but concentrated analysis of *other road users* as the most important stakeholder group with respect to macroscopic safety requirements for automated driving.

The range of *other road users* is wider within built-up areas than on motorways, as there are several limiting factors for participation in motorway traffic. For example, according to § 18 of the German Road Traffic Regulations (StVO), vehicles on motorways are only allowed if maximum design speed of the vehicle is greater than 60 km/h. [14] In order to take this diversity into account, the top level group classification according to [5] is further differentiated. This is done with the help of a list from the German Federal Statistical Office, which provides information on the current existing types of traffic participation. [12, pp. 18-19]

However, the performance of risk acceptance analyses at the level of the finest granularity of the classification of stakeholders in road traffic is associated with a statistical problem, the before mentioned so-called law of small numbers. [23] An example that illustrates this problem: In 2018, there was just one fatal accident in German build-up areas involving an S-pedelec. [12] It seems evident that a single accident does not provide a sufficiently large data basis to make statistically significant statements about the tolerated risk. For this reason, single stakeholders are grouped into interest groups.

To overcome the statistical problem of the small numbers, the minimum number of accidents has to be identified that expresses the statistical significance of the minimum group size in order to form such interest groups. We suppose to estimate this number based on an approach to approximate the minimum sample size for a given margin of error e, the so called Z-Score $z_{1-\alpha/2}$ and the variance σ^2 of the underlying probability distribution according to [22, p. 218]:

$$n = \left(\frac{z_{1-\alpha/2} \cdot \sigma}{e}\right)^2$$

As supposed in section III.A, this work differentiates between accidents with fatalities (index 1) and accidents with serve injuries (index 2). The minimum group size for both categories n_1 and n_2 is calculated independently and the more restrictive result is considered for accumulating different types of road users into interest groups.

To determine n, the accident statistics for the period from 2009 to 2018 are utilized and modelled as a multinomial distribution. Data before 2009 is not considered as multiple factors, e.g. safety increasing regulations, are increasing the road safety continuously, like for example a framework directive of the European Union (EU) on the mandatory equipping of new vehicles in various classes with lane departure warning systems and emergency brake assistants has only been in existence since 2009. [26, p. 6] . For this reason, it is not considered expedient to use data older than ten years when modelling the occurrence of accidents In contrast, however, it is also not sufficient to consider only statistics for the most recent or most recently evaluated year, as accident figures are subject to fluctuations.

This fluctuation is shown by the variance σ^2 which can be calculated directly from the accidents numbers from 2009 to 2018 for both categories independently. [27] This variance of the overall accident numbers is used to conservatively approximate the variance of the accident numbers of the individual interest groups that should be identified. The yearly overall fluctuation is likely to be bigger than the variance of a single stakeholder but not guaranteed as fluctuations of single interest group may vary in size and could even compensate themselves when added to the overall number of accidents.

As stated by the equation above, to calculate n, the error e has to be defined as well. We propose an approximation by utilizing the mean value error $\sigma_{\bar{\mu}} = \sqrt{\mu/m}$ to achieve a definition within a plausible order of magnitude. While m being the number of measurements (10 years), μ is the overall expectation value for the number of accidents observed in the observed span of 10 years and is therefore different for accidents of category 1 and 2. Utilizing the statistical data from Destatis, the resulting mean errors $\sigma_{\bar{\mu},1} = \sqrt{1008/10} = 10$ and $\sigma_{\bar{\mu},2} = \sqrt{33267/10} = 57.7$ are used to approximate the errors by rounding $\sigma_{\bar{\mu}}$ to the next lower number of ten to $e_1 = 10$ and $e_2 = 50$. This approach is a conservative approximation for the minimum sample size n, as a lower value of e leads to a higher value of n.

Lastly, the Z-Score $z_{1-\alpha/2}$ can be read from tables depending on the significance level α. [24, p. 3] For the further course of this work, the significance level is defined to the typical value $\alpha = 5\ \%$ in order to achieve a balance between the statistical errors of the so called first and second type. [22, p. 225] [29]

Finally, this leads to $n_1 = 230$ for accidents of category 1, which is the annual number of fatal accidents in built-up areas that must be present at least when individual stakeholders are grouped to form a statistically significant interest group. For accidents of category 2 (with serious injuries) the minimum number of accidents is $n_2 = 1833$ accordingly. If the group-internal number of accidents for the corresponding categories is smaller than n_1 or respectively n_2, other stakeholders or types of traffic involvement have to be added to the affected group until the stated minimum numbers for fatal as well as accidents with serve injuries is reached.

The fact that there is only a factor of about 8 between n_1 and n_2 seems paradoxical at first glance since the factor between the expected values of both accident categories is 33. According to [24, p. 2], however, this is a typical phenomenon of sampling theory. For example, "*the sample size hardly changes if the stratum from which the sample is drawn contains 2,000 or 20,000 units [...]*."

It needs to mentioned, that other ways to calculate the minimum sample size exist, which are specialized for multinomial distributions and need to be evaluated in the future, e.g. those summarized in [27]. Respecting on the minimum number of accidents that must be considered when aggregating stakeholders into sufficiently large interest groups, two different approaches are discussed:

1. On the one hand, a stakeholder under consideration, e.g. the type *bus*, which does not meet the requirement of statistical significance for accidents with fatalities (21 in 2008), can be bundled with another stakeholder that on its own already meets the requirements for minimum accident figures. This is the case, for example, with *passenger cars* (554 fatal accidents in built-up areas in 2018) [12] One argument in favor of combining *buses* and *passenger cars* is that both means of transport primarily serve to transport passengers. By contrast, the similarities in terms of spatial dimensions and masses favor combining *buses* and *cargo road transport vehicles*.

2. On the other hand, another possibility is to combine several types of traffic participation, which all on their own do not fulfill the statistically required minimum number of accidents, but in total represent a significant group. As examples - in addition to the *buses* already mentioned - *railway vehicles, trams, tractors, good transporters, other motor vehicles and other and unknown vehicles* can be mentioned as well, where fewer than the required number of accidents with fatalities within built-up areas occurred in 2018. [12] By combining the mentioned types the statistical problem of small numbers can be circumvented. In addition to the stochastic motives, a further argument in favor of this grouping is that there is a higher degree of similarity between these types of traffic participation in terms of their construction-related characteristics and the resulting transport volumes than, for example, between *trams* and *passenger cars*.

For both methods, the grouping should take into account the extent to which individual types of traffic participation are protected from the influence of a potential accident opponent. The adjective *protected* here does not mean protection by law and/or written safety requirements, but rather direct, physical protection by helmets, protectors, airbags, etc. In this context, official road accident statistics repeatedly refer to "*unprotected road users*".

Based on the above arguments, the second methodology of grouping is used in calculating the exemplary safety reference in the following sections. However, in any case there is a certain degree of arbitrariness left for every combination. Also is should be noted that due to the usage of different types of road users to create groups, accidents are most likely counted multiple times in the overall perspective. E.g. if a *car* and a *pedestrian* are involved in fatal accident, this accident is represented in both total numbers of accidents for this type of road users. Also as *cars* might be involved in accidents without any other type of road user, this is almost never true for accidents with pedestrians. Nonetheless, an accident that is counted in more than one group of road users created a risk for more than this one group and therefore has a certain (but not unquestionable) degree of validity to be represented in multiple safety requirements indices.

In addition to the one interest group already explained in the example, further interest groups are grouped in a similar way. Finally, the group classification method explained above leads to five different interest groups as subgroups of *other road users* who are one of the three *stakeholder groups explained in section III.D*. These are summarized in Figure 4:

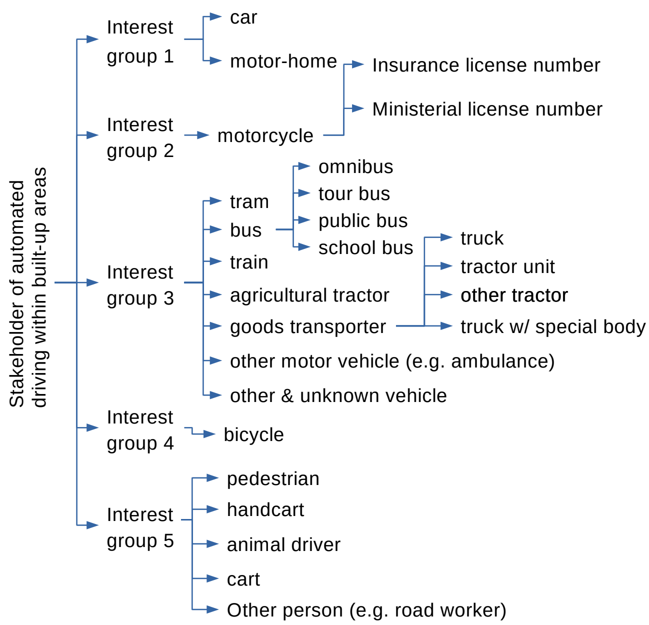

Figure 4: Interest groups, based on [12, pp. 18-19]

E. Determination of a suitable reference value for accident figures

In its publications on road accidents, the German Federal Statistical Office addresses various reference values, which are used to relate accident figures to them, resulting in accident indicators. [12] In domains other than road transport - rail vehicle technology and aviation for example - certain reference parameters have emerged particularly suitable for their respective mode of transport. [5] In the following section, these reference values are analyzed with regard to their suitability in the context of this work.

An intuition-based assumption regarding the causality between the number of vehicles and the frequency of accidents is that a larger number of vehicles also lead to an increase in the number of accidents. However, the statistics [12] show that a corresponding positive correlation is not given across the board.

Since the inner-city road network is not exclusively used by motor vehicles, but also by non-motorized road users, the road length as a reference value aims at a larger number of types of road users than, for example, the total number of vehicles. In contrast, the risk of a road accident on a road exists only when the road is actually used - similar to the fact that a motor vehicle only poses an immediate risk when it is used in traffic. One way to address this problem is to use traffic density as a reference, which is defined as the number of vehicles per section of road. [30] Traffic density is thus based on the length of the road, but in contrast to this, it also allows a statement to be made as to whether and to what extent the infrastructure is used. However, as length figures for the same road can differ significantly depending on the road length definition on which the survey is based, there is a risk of misunderstanding and/or wrong assumptions when using the road length or the traffic density - which is based on it - as a reference for accident figures.

In Germany, the registration of residents in a defined geographical area is regulated by law, namely by the Federal Registration Act. [31] The fact that registration registers are kept by the registration authorities, and consequently the population figures are based on a law, this parameter has an advantage over other potential reference variables such as the above mentioned road length. The surveys are unambiguous due to their legally regulated recording. Additionally, in the context of other domains, the maximum tolerated risks are also often given per person per year. This is for example the case for occupational risks or within the risk analyses of large-scale technologies such as nuclear energy. [5] The use of the population figures as a reference value has therefore the advantage that it allows risks to be compared across different domains. Contrarily, statements about traffic volumes can only be made to a limited extent based on population figures. It cannot be ruled out that individual members of the population may only contribute to a negligible extent to the traffic volume. For individuals, however, an immediate risk arises only through actual participation in traffic events. This argues in the favor of preferring reference values that are inevitably linked to traffic participation and thus the resulting exposure to risk.

In aviation, the majority of accidents happen during take-off or landing. Additionally, longer travel distances are covered compared to ground-based traffic. The combination of these two circumstances and the fact, that each flight can either end with an accident or not, justifies the approach to use the number of flights rather than the distance as a reference value for accident rates. [5] An analogous approach for automated driving within built-up areas would be to use the number of trips as a reference value for traffic accidents. The counterpart to accidents during take-off or landing in aviation is the accident type "*collision with another vehicle that starts, stops or is stationary*" [12]. However, in contrast to aviation this particular accident type does not dominate road traffic within built-up areas. In 2018, for example, the proportion of accidents with another vehicle involving injuries was only 7.8%. In relation to accidents with fatalities, the figure was only 2.4 %. [12]

In the context of railway safety, tolerated marginal risks are defined by means of a maximum number of errors per hour. [32] The reference value used is therefore a time interval. The procedure of relating errors, accidents or damage to rail vehicles not to a spatial but to a temporal distance can be justified as follows: Railway vehicles are already more closely connected with their infrastructure than road vehicles. Consequently, technical faults, which have the potential of safety-critical states, can be located not only in the rail vehicle itself, but also on the railway infrastructure. Therefore, the requirement for a reference value for faults in railway safety systems suggests that a part of the risk results from stationary installations. This makes the use of a time interval seem an adequate solution. In road transport however, there is no sophisticated level of communication or networking between vehicles and the infrastructure.

In the previous remarks, it has already been mentioned that values representing actual participation in traffic should be preferred as only the traffic participation causes the risk exposure. While the driven distance meets this requirement, it can be argued that, although it implies actual participation in traffic, this only applies to motor vehicles and not to pedestrians, cyclists or any other possible types of traffic participation. However, although the driven distance, does not allow statements to be made for all stakeholders about actual participation features, still has the advantage of taking some (even the major) participation in transport in to account. Furthermore, only the driven distance within built-up areas allows the comparison with other existing research results on automated driving to be made, as it has already been used as a reference value when defining macroscopic safety requirements for automated driving on motorways. [5]

In passenger transport, transportation performance is defined as the product of the mileage performed and the number of passengers transported within a specific observation period. It is used, for example, in the context of studies on safety in public transport, where a large number of people are transported per vehicle. According to [33] the average car occupancy rate in Germany in 2016 was only 1.46 persons per vehicle. Consequently, a method transfer from public transport to automated driving is not considered necessary here. In addition, two input variables are required to calculate the transport performance. Therefore, there are also two potential sources of inaccuracies in data collection

After weighing up the discussed advantages and disadvantages of all potential reference values that are summarized in Table 1, the driven distance proves to be the most suitable.

Table 1: Advantages and disadvantages of pot. reference values

Possible reference values / evaluation criteria for reference value	Number of motor vehicles	Road length	Traffic density	population	Population density	Number of trips	Time interval / operating time	driven distance	Passenger-distance
data for different localities exists	-	+	+	○	○	-	-	+	-
implies traffic participation	-	-	+	-	-	+	○	+	+
addresses different kind vehicle typs in use	○	+	+	+	+	○	○	○	○
is unambiguous	+	-	-	+	+	-	○	+	○
allows comparison with other domains	-	-	-	+	○	-	○	-	○
allows comparison with req. for AD on highway	-	-	-	-	-	-	-	+	-
motivation of use in other domains is valid in built-up areas	○	○	○	+	○	-	-	+	-

F. *Quantification of the driven distance as reference value*

The survey of the German Federal Highway Research Institute (BASt) is used to quantify the driven distance as a reference value. [34] The BASt distinguishes between "*resident mileage*" and "*domestic mileage*". *Resident mileage* is the total mileage of motor vehicles registered in Germany. Not only distances travelled in Germany are included in the surveys, but also the distances travelled on foreign roads. In contrast, the total mileage performed on domestic, i.e. German, roads is included in the statistics as *domestic mileage*, irrespective of the origin of the vehicles responsible for this mileage. [34, p. 17]

The macroscopic safety requirements to be defined represent key figures where accident figures are reflected in the numerator and driving performance in the denominator. To ensure that the numerator and denominator have the same spatial reference, the accident figures are not to be set in relation to *resident mileage*, but rather in relation to *domestic mileage*.

The BASt points out that there are two different concepts for determining such key figures [34, pp. 77-78]:

The first concept involves breaking down both numerator and denominator of the key figure according to the same characteristic (such as street class, location, vehicle type, vehicle nationality, etc.). As this concept is the most logical as it expresses the direct risk for each stakeholder, this breakdown concept is only practicable if data is available for accident figures and in the survey of mileage (within built-up areas) for each single type of road user. This means for example that the driven distance by bicylcle within build-up areas would be needed, which differs from the overall driven distance, that is included in statistic, as bicycles are quite often used outside built-up areas as well.

The second concept is that the numerator of the risk indicator is disaggregated, while the denominator - irrespective of the characteristic value in the numerator - always remains constant.

For the definition of macroscopic safety requirements for automated driving within built-up areas, a mixture of both variants is used, since two differentiating characteristics are distinguished, namely the location and the type of traffic involvement and only limited data for the expression of the mobility usage of an individual interest group or even single type of road user exists.

The type of vehicle or traffic involvement represents the second differentiating characteristic, since the macroscopic safety requirements have to be defined for different interest groups. With regard to this feature, the second presented concept is used, since the available statistical data does not allow a distribution of the mileage among the different interest groups. In other words, the accident figures of different stakeholders are related to the same mileage value, i.e. the total mileage produced by all types of road transport operators together. This averages to 193.5 billion kilometers per year in urban areas. [34, pp. 67-68]

IV. RESULTS

The findings from the previous sections are combined to derive the macroscopic safety requirements for automated driving within built-up areas. Therefore, the previously determined interest groups and driving performance data are used and presented individually in the following section:

A. *Safety requirements of other road users*

Based on the accident statistics for 2014-2018 [12, 35–38] and the average mileage in urban areas over the same period [34], Table 2 shows the safety requirements in terms of the calculated performance indicators for the interest groups defined in section III.D. According to the GAMAB principle (cf. II.A.3)), these correspond to the macroscopic safety requirements for automated driving in urban environments from the perspective of *other road users*.

Table 2: Macroscopic safety requirements of other road users

Interest Group	**1**	**2**	**3**	**4**	**5**
Accidents with fatalities per year	582	166	272	253	367
Accidents with serious injuries per year in thousands	23.4	6.6	3.6	12.5	7.5
aggregated driving performance in km per year	$193.5 \cdot 10^{9}$				
Max value: Accidents w/ fatalities per aggregated km	$3.0 \cdot 10^{-9}$	$0.9 \cdot 10^{-9}$	$1.4 \cdot 10^{-9}$	$1.3 \cdot 10^{-9}$	$1.9 \cdot 10^{-9}$
Max value: Accidents w/ serious injuries per aggregated km	$12 \cdot 10^{-8}$	$3.4 \cdot 10^{-8}$	$1.9 \cdot 10^{-8}$	$6.5 \cdot 10^{-8}$	$39 \cdot 10^{-8}$

B. Safety requirements of society

In section III.D, society was defined as that part of the population which is not directly affected by the accident-related fate of an individual, but for which only the total number of accidents is relevant. For this reason, the annual totals of all fatal accidents as well as the annual totals of all accidents with serious injuries within urban areas are used to define macroscopic safety requirements for this interest group. Analogous to the requirements of other road users defined in section IV.A, the following safety requirement for the society results in, according to the GAMAB risk acceptance principle, less than $5.0 \cdot 10^{-9}$ accidents with fatalities and simultaneously a maximum of $1.7 \cdot 10^{-7}$ accidents with serious injuries per kilometer.

C. Safety requirements of users of automated vehicles

The users of automated vehicles are attributed borderline risks that exceed the current risks of manual driving, as they voluntarily expose themselves to the risk. The risk acceptance principle GAMAB, which was used for the risk acceptance analyses of the other interest groups, only reflects current risks. [8] In order to derive the higher marginal risks of the users of automated vehicles from the current risks of manual driving, a surcharge factor or an additive risk surcharge is required. In connection with the MEM risk acceptance principle, [8] specifies risk values by which an existing risk may be maximally increased by the introduction of a new technology or a new transport system. The MEM principle thus provides the necessary additive risk surcharges. For this reason, the two principles GAMAB and MEM are combined below. This means that the tolerated marginal risks of the automated vehicles users are given by the sums of the marginal risks from the GAMAB and MEM principles:

$$R_{\mathrm{U,s}} \leq R_{\mathrm{GAMAB,s}} + \frac{R_{\mathrm{MEM,t}}}{\bar{d}}$$

This approach was also followed by [5] to define macroscopic safety requirements for automated driving on motorways. In the equation above, R is the general symbol for a risk. The index U is an abbreviation for the users of automated vehicles while the index s indicates that the risks are given in terms of distance and the index t indicates a time-based risk figure. While R_{GAMAB} represents the current risks of manual driving according to the GAMAB principle, R_{MEM} here does not refer to the minimum endogenous mortality itself, but to the additive risk surcharges that are derived from it and can be taken from standards or tables. [8, p. 59]

In [8], which defines the MEM principle, the values for $R_{\mathrm{MEM,t}}$ are time-related and correspond to $1/20^{\mathrm{th}}$ of the minimum endogenous mortality MEM/20 (cp. section II.A.2) . Since in section III.E the mileage was selected as the reference value for accident figures, the values given per person and year from [8] must be converted into distance-related values. For this reason, a division is made by the distance $\bar{d}$ that a person per year travels on average within urban environments in Germany. For the first summand $R_{\mathrm{GAMAB,s}}$, the accepted limit risk from the point of view of society is used (cf. section IV.B), since the future users of automated vehicles cannot be assigned to a specific interest group as defined in section III.D.

The values for $R_{\mathrm{MEM,t}}$ used in the second summand are derived from [8]. For fatal accidents (category 1), the standard specifies a maximum value of 10^{-5} fatalities per person per year. For accidents with serious injuries (category 2), the maximum value is 10^{-4} seriously injured persons per person per year. However, these limit values address casualties and not accident figures. Since the latter was selected as the preferred parameter in section III.C, the maximum number of casualties from [8] have to be converted into maximum accident figures. The factors required for this are derived by dividing the accident figures by causality figures (for the years 2014-2018, using data from [12]) to 0.977 for category 1 accidents and 0.938 for category 2 accidents. Thus, the values to be used for $R_{\mathrm{MEM,t}}$ are $0.977 \cdot 10^{-5}$ fatal accidents per person per year and $0.938 \cdot 10^{-4}$ accidents with serious injuries per person per year.

The average travel distance $\bar{d}$ within urban areas per person per year is estimated with 3,360 km, based on [34].

This results in the following macroscopic safety requirements for users of automated vehicles:

Less than $7.9 \cdot 10^{-9}$ accidents with fatalities and at the same time a maximum of $2.0 \cdot 10^{-7}$ accidents with serious injuries per aggregated kilometer occur.

D. Discussion of results

The marginal accepted safety requirement of *other road users* ranges from $2.6 \cdot 10^{-10}$ to $3.0 \cdot 10^{-9}$ accidents with fatalities per aggregated kilometer, depending on the type of *other road users*. The *society's* marginal risk is higher than that of *other road users* by factors of 1.7 to 19.2. The *users of automated vehicles* even tolerate risks that exceed the marginal risk of the society by a factor of 1.6. Figure 5 illustrates these conditions.

In section III.D, it was argued that the group of *other road users* are the most critical stakeholders and that, in contrast, *users of automate vehicles* are the ones with the highest tolerated marginal risks. This theory is supported by the above-mentioned conditions as illustrated in Figure 5.

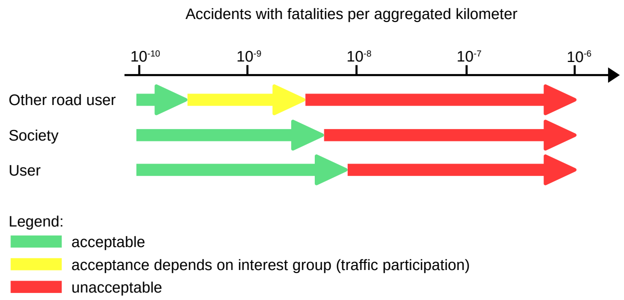

Figure 5: Comparison of inner urban marginal risks for accidents with fatalities

When comparing the marginal risks of *other road users* with those of the other two superordinate interest groups, it should be born in mind that the former has been divided into sub interest groups. The probability of being specifically involved in an accident as a representative of one of these sub interest groups is always lower than that of being involved in an accident at all. Since the probability of occurrence is by definition a factor in the risk, in addition to the amount of damage, the safety requirements of the *other road users* are consequently lower than in the summative analyses of *society* and the *users of automated vehicles*. This observation applies not only to the accidents with fatalities as discussed above, but also to accidents with serious injuries, which are illustrated in Figure 6.

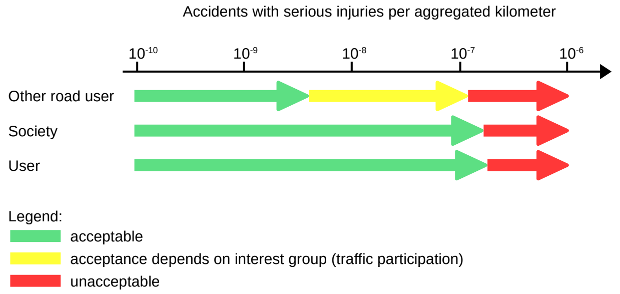

Figure 6: Comparison of inner urban marginal risks for accidents with serious injuries

Once again, the users of automated vehicles present themselves as the interest group with the highest tolerated risks, while other road users represent the most critical interest group. A comparison of Figure 5 and Figure 6 indicates that the numbers of accepted accidents with serious injuries per interest group are higher than the corresponding numbers of accepted accidents with fatalities, which meets the expectations.

Macroscopic safety requirements or tolerated limit risks for automated driving on motorways are only derived for accidents with fatalities by [5]. Accordingly, the possibility of a direct comparison of inner urban and motorway-related marginal risks for accidents with serious injuries is not given. For this reason, the following explanations refer exclusively to accidents with fatalities.

Figure 7 illustrates that the inner urban marginal risks exceed those of motorway traffic. This means that within built-up areas, higher numbers of fatal accidents per kilometer are assigned to the acceptable risks. This situation is in line with expectations since motorways are considered the safest of the three locations compared to built-up areas and out-of-town roads - especially if accidents per kilometer serve as a reference. [5]

With regard to the *users of automated vehicles*, the risks still tolerated in built-up areas exceed those of motorway traffic by a factor of 3.6. For *society*, motorway-related marginal risks are indicated in relation to predicted field proportions of automated vehicles in [5]. Consequently, it is not possible to determine a single risk factor as in the case of *users of automated vehicles*. Instead, depending on the assumed field share, marginal risks are attributed to the *society*, which within built-up areas are 2.8 to 17.2 times higher than their motorway-related counterparts. For *other road users*, there is an additional dependency on which of the sub interest groups formed is considered. Depending on the assumed field share and sub interest group, the factors between the marginal risks on motorways and those within built-up areas amount to up to 47.6. [5]

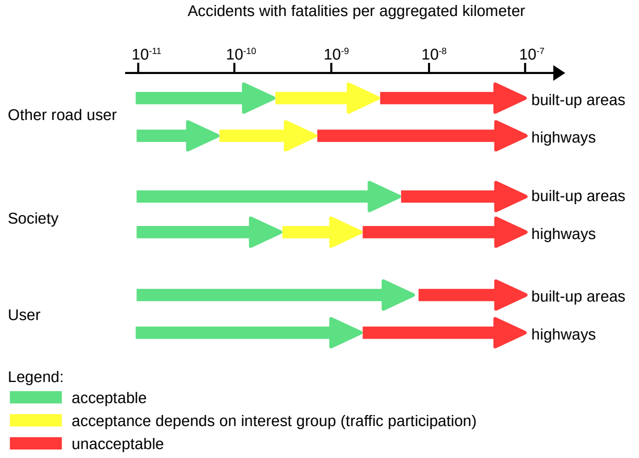

Figure 7: Comparison of inner urban and motorway-related marginal risks (based on [5])

ISO 26262 recommends assigning an "Automotive Safety Integrity Level" (ASIL) to each potentially hazardous event. [2] This assignment is made on the basis of the three parameters "severity", "probability of exposure" and "controllability". Depending on their constellation, one of the five levels QM, ASIL A, ASIL B, ASIL C or ASIL D results.

ASIL D represents the highest safety requirement and addresses life-threatening as well as fatal injuries. In this respect, ASIL D goes hand in hand with the accident categories 1 (accidents with fatalities) and 2 (accidents with serious injuries), which are considered in the context of the present work.

For ASIL D systems, the required probability of error or failure per operation hour is less than 10^{-8}. [2] Using average vehicle speeds, this can be converted into maximum numbers of acceptable errors per kilometer. According to [39], the average speed is 24.1 km/h within built-up areas. This results in an inner urban limit value for ASIL D systems of $4.1 \cdot 10^{-10}$ severe errors per kilometer. A comparison of this limit value and the values stated in Figure 5 shows that it is within the range in which the risks posed by automated vehicles are already no longer accepted by all stakeholders. If, as a consequence, it should become necessary in the future to prove sufficient safety, according to ASIL D, not only for individual components and/or (sub) systems, but also for entire vehicles, the complexity of the safety proof of automated driving is already apparent from this circumstance. However, due to dilution effects, the safety requirements will be lower during the introduction phase of automated vehicles due to lowered exposure, until a significant market share is reached. [cp. 5]

V. Conclusion

The primary objective of the present work was the definition of macroscopic safety requirements for automated driving within built-up areas.

For the future market introduction of automated vehicles, the macroscopic risk is significantly influenced by (local) market penetration. The example of the automated DB shuttle buses in the Bavarian town of Bad Birnbach shows that the probability of encountering automated vehicles there and - as a consequence - the risk of an accident is currently significantly higher. Nevertheless, this effect cannot be statistically recorded due to the absolute low number of events. Meanwhile, the risks of a traffic accident in the rest of Germany remain unaffected by the pilot project. [40] Since the marginal risks were determined within the framework of the present analysis based on reference values that result as average values from localities throughout the Federal Republic of Germany, their direct transferability to individual localities, in particular, is not yet given. Not least in order to establish the possibility of such a transfer, the influences of local market penetration on the inner-local risk acceptance are to be examined in further work.

Furthermore, automated vehicles are not designed for exclusive distribution or exclusive use in only one country. Just as the macroscopic safety requirements in Germany can only be transferred to singular localities to a limited extent, their internationalization in the form of a comparison with reference values of today's urban traffic from countries other than the Federal Republic of Germany is also required.

Additionally, the Federal Statistical Office distinguishes between three locations: urban areas, rural areas (excluding motorways) and motorways. For the latter, macroscopic safety requirements were defined by [5]. The inner urban counterpart was the subject of the present study. In order to cover all locations, macroscopic safety requirements for automated driving in rural areas have to be determined. Subsequently, it has to be discussed how the location-specific individual results could be combined.

Regardless of the location under consideration, it must be considered that a hypothetical decrease in the number of accidents could result in lower tolerated limit risks and thus in higher safety requirements in the future. [5] Accordingly, macroscopic safety requirements must be continuously versioned and adapted to the current state of road safety.

Even though all of the questions still open are potentially answered or dealt with in following research contributions, one aspect always needs to be taken into account when dealing with macroscopic safety requirements: There is no guarantee that risk limits that have been established will actually be accepted in individual cases. Despite this fact, it seems obligatory to deal with this topic as part of a comprehensive safety argumentation in order to enable the market introduction of automated driving functions at all. Hereby, the derived macroscopic safety requirements are not to be understood as design goals. Instead, they are intended to be used as reference values during safety approval.

Acknowledgement

We thank Claus Pastor from the Federal Highway Research Institute (BASt) for the comments on an earlier version of the manuscript and the valuable discussion that improved this paper.

References

[1] *J3016: Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems, J3016, 2018*

[2] *ISO 26262: Road vehicles – Functional safety, 2018*

[3] *H.-L. Ross, Funktionale Sicherheit im Automobil: ISO 26262, Systemengineering auf Basis eines Sicherheitslebenszyklus und bewährten Managementsystemen. München, Wien: Carl Hanser Verlag, 2014*

[4] *DIN EN 60812 - Analysetechniken für die Funktionsfähigkeit von Systemen, DIN EN 60812:2006 (IEC 60812:2006), 2006*

[5] *P. Junietz, U. Steininger, and H. Winner, "Macroscopic Safety Requirements for Highly Automated Driving", Transportation Research Record: Journal of the Transportation Research Board, vol. 2673, no. 3, pp. 1–10, https://journals.sagepub.com/eprint/9NjEFpXRdJjp3NrtbDSA/full, 2019*

[6] *U. Lindemann, Handbuch Produktentwicklung. München: Carl Hanser Verlag, 2016*

[7] *U. Steininger, Schöner, Hans-Peter, Schiementz, Mark, and J. Mazzega, "Validation of assisted and automated driving systems.", . crash.tech, München, 2016.*

[8] *E. CENELEC, "50126: Railway applications-The specification and demonstration of Reliability", Availability, Maintainability and Safety (RAMS), 2001*

[9] *U. Steininger and L. Wech, "Wie sicher ist sicher genug? Sicherheit und Risiko zwischen Wunsch und Wirklichkeit", VDI-Berichte, no. 2204, 2013*

[10] *Ethik-Kommission Automatisiertes und Vernetztes Fahren, "Bericht Juni 2017", Bundesministerium für Verkehr und digitale Infrastruktur, Berlin, Jun. 2017. [Online] Available: https://www.bmvi.de/SharedDocs/DE/Publikationen/DG/bericht-der-ethik-kommission.html. Accessed on: Oct. 15 2019*

[11] *P. Liu, R. Yang, and Z. Xu, "How Safe Is Safe Enough for Self-Driving Vehicles?", Risk analysis, 2018*

[12] *Statistisches Bundesamt, "Verkehrsunfälle 2018: Fachserie 8 Reihe 7", Statistisches Bundesamt, Wiesbaden Artikelnummer: 2080700187004, Jul. 2019. [Online] Available: https://www.destatis.de/DE/Themen/Gesellschaft-Umwelt/Verkehrsunfaelle/_inhalt.html. Accessed on: Oct. 15 2019*

[13] *Bundesanstalt für Straßenwesen (BASt), Ergebnisse Fahrleistungserhebung 2014: Erhebung der Inländerfahrleistung und der Inlandsfahrleistung. [Online] Available: https://www.bast.de/BASt_2017/DE/Verkehrssicherheit/Fachthemen/u2-fahrleistung-2014/u2-Fahrleistung-2014-ergebnisse.html. Accessed on: Oct. 29 2019*

[14] *Straßenverkehrs-Ordnung: StVO, 2019*

[15] *Bundesfernstraßengesetz: FStrG, 2018*

[16] *Grundgesetz für die Bundesrepublik Deutschland, 1949*

[17] *Statistisches Bundesamt, Unfallentwicklung auf deutschen Straßen 2017: Begleitmaterial zur Pressekonferenz am 12. Juli 2018 in Berlin. Wiesbaden, 2018*

[18] *W. Matthews, "Unfall- und Unfallkostenraten im Strassenverkehr", . Forschungsauftrag VSS 2000/343 auf Antrag des Schweizerischen Verbands der Strassen- und Verkehrsfachleute VSS, Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation UVEK, Nov. 2009. [Online] Available: https://ethz.ch/content/dam/ethz/special-interest/baug/ivt/ivt-dam/vpl/vss-ek/2000-343.pdf. Accessed on: Oct. 18 2019*

[19] *P. M. Junietz, "Microscopic and Macroscopic Risk Metrics for the Safety Validation of Automated Driving", Technische Universität, 2019*

[20] W. Wachenfeld and H. Winner, "Die Freigabe des autonomen Fahrens", in Autonomes Fahren: Technische, rechtliche und gesellschaftliche Aspekte, M. Maurer, J. C. Gerdes, B. Lenz, and H. Winner, Eds., Berlin, Heidelberg: Springer-Verlag GmbH Berlin Heidelberg, 2015, pp. 439–464

[21] E. Papadimitriou, G. Yannis, F. Bijleveld, and J. L. Cardoso, "Exposure data and risk indicators for safety performance assessment in Europe", in Accident Analysis & Prevention, M. A. Abdel-Aty, Ed.: Elsevier, 2013, pp. 371–383

[22] H.-F. Eckey, R. Kosfeld, and M. Türck, Wahrscheinlichkeitsrechnung und Induktive Statistik: Grundlagen - Methoden - Beispiele. Wiesbaden: Betriebswirtschaftlicher Verlag Dr. Th. Gabler/GWV Fachverlage GmbH, 2005

[23] L. Bortkewitsch, Das Gesetz der kleinen Zahlen. Leipzig: Teubner, 1898

[24] P. von der Lippe, Wie groß muss meine Stichprobe sein, damit sie repräsentativ ist?: Wie viele Einheiten müssen befragt werden? Was heißt "Repräsentativität"? [Online] Available: http://www.von-der-lippe.org/dokumente/Wieviele.pdf. Accessed on: Sep. 02 2019

[25] W. H. K. Wachenfeld, "How stochastic can help to introduce automated driving", Technische Universität Darmstadt, 2017

[26] E. Petersen, "Notbrems-Assistenzsysteme für Nutzkraftwagen: Wissenspapier", Landesverkehrswacht Niedersachsen e.V., Sep. 2016. [Online] Available: https://www.landesverkehrswacht.de/fileadmin/user_upload/ALLGEMEIN_FILES/LVW_Wissensblatt/LVW-Wissensblatt-18_Notbrems-Assistenzsysteme-fuer-Nutzkraftwagen.pdf. Accessed on: Nov. 10 2019

[27] Steven K. Thompson, "Sample Size for Estimating Multinomial Proportions", The American Statistician, vol. 41, no. 1, pp. 42–46, http://www.jstor.org/stable/2684318, 1987

[28] H. Winner, S. Hakuli, F. Lotz, and C. Singer, Eds., Handbuch Fahrerassistenzsysteme: Grundlagen, Komponenten und Systeme für aktive Sicherheit und Komfort, 3rd ed. Wiesbaden: Springer Vieweg, 2015

[29] W. Hemmerich, Signifikanz, Signifikanzniveau. [Online] Available: https://matheguru.com/stochastik/signifikanz-signifikanzniveau.html. Accessed on: Nov. 16 2019

[30] D. Schäfer and N. Blagojevic, "Ermittlung der Kapazität von Straßen durch Fahrzeugmessungen im Verkehrsfluss", . Studienarbeit, Hochschule Ulm, Ulm, 2010

[31] Bundesmeldegesetz: BMG, 2019

[32] M. Leining, "Ausgewählte Elemente der Leit- und Sicherungstechnik", . Darmstadt, Nov. 27 2018.

[33] Deutscher Bundestag, "Drucksache 19/1162: Trend zu schweren, schnellen und leistungsstarken Autos und Einhaltung von Klimaschutzzielen", . Antwort der Bundesregierung auf Drucksache 19/777, Deutscher Bundestag, Berlin 19/1162, Mar. 2018. [Online] Available: http://dip21.bundestag.de/dip21/btd/19/011/1901162.pdf. Accessed on: Nov. 07 2019

[34] Bundesanstalt für Straßenwesen (BASt), "Fahrleistungserhebung 2014: Inlandsfahrleistung und Unfallrisiko", Bundesanstalt für Straßenwesen (BASt), Bergisch Gladbach, Berichte der Bundesanstalt für Straßenwesen V 291, Aug. 2017. [Online] Available: https://bast.opus.hbz-nrw.de/opus45-bast/frontdoor/deliver/index/docId/1775/file/BASt_V_291_barrierefreies_Internet_PDF.pdf. Accessed on: Oct. 29 2019

[35] Statistisches Bundesamt, "Verkehrsunfälle 2014: Fachserie 8 Reihe 7", Statistisches Bundesamt, Wiesbaden Artikelnummer: 2080700147004, Jul. 2015. [Online] Available: https://www.destatis.de/GPStatistik/servlets/MCRFileNodeServlet/DEHeft_derivate_00018327/2080700147004_Korr15022016.pdf. Accessed on: Oct. 28 2019

[36] Statistisches Bundesamt, "Verkehrsunfälle 2015: Fachserie 8 Reihe 7", Statistisches Bundesamt, Wiesbaden Artikelnummer: 2080700157004, Jul. 2016. [Online] Available: https://www.destatis.de/GPStatistik/servlets/MCRFileNodeServlet/DEHeft_derivate_00026296/2080700157004.pdf;jsessionid=BB70F55B2BFECD4F631D684A7EE4A96A. Accessed on: Oct. 28 2019

[37] Statistisches Bundesamt, "Verkehrsunfälle 2016: Fachserie 8 Reihe 7", Statistisches Bundesamt, Wiesbaden Artikelnummer: 2080700167004, Jul. 2017. [Online] Available: https://www.destatis.de/GPStatistik/servlets/MCRFileNodeServlet/DEHeft_derivate_00035071/2080700167004_Korr16042018.pdf. Accessed on: Oct. 28 2019

[38] Statistisches Bundesamt, "Verkehrsunfälle 2017: Fachserie 8 Reihe 7", Statistisches Bundesamt, Wiesbaden Artikelnummer: 2080700177004, Jul. 2018. [Online] Available: https://www.destatis.de/DE/Themen/Gesellschaft-Umwelt/Verkehrsunfaelle/Publikationen/Downloads-Verkehrsunfaelle/verkehrsunfaelle-jahr-2080700177004.pdf?__blob=publicationFile&v=4. Accessed on: Oct. 28 2019

[39] Statistisches Bundesamt and Umweltbundesamt, "Umwelt, Haushalte und Konsum: Daten zur Umwelt", Statistisches Bundesamt (Destatis); Umweltbundesamt, Wiesbaden, Dessau-Roßlau, 2015. [Online] Available: https://www.destatis.de/DE/Themen/Gesellschaft-Umwelt/Umwelt/Publikationen/Querschnitt-Sonstiges/Broschuere_UBA_Daten_Zur_Umwelt.pdf?__blob=publicationFile. Accessed on: Nov. 03 2019

[40] U. Baumann, "Autonomer Bus in Bad Birnbach", 08 Oct., 2019, https://www.auto-motor-und-sport.de/elektroauto/autonomes-shuttle-bad-birnbach-deutsche-bahn-ioki/