Scenario-based definition of technical safety requirements for autonomous road vehicles

O Kirovsky \textsuperscript{1,3} and K Byakov\textsuperscript{2}

\textsuperscript{1}ZF North America, 34605 W 12 Mile Rd, MI 48033, Farmington Hills, USA
\textsuperscript{2}Bauman Moscow State Technical University

\textsuperscript{3}E-mail: Oleg.Kirovskii@trw.com

Abstract. The article provides a brief overview of the standards ISO 26262 and ISO 21448 and the safety life cycle defined therein. A method for technical requirements development based on road situation statistics is proposed. Possibilities for improvement of safety life cycle for autonomous vehicles using traffic data are considered. An outlook towards the implementation of traffic scenarios into the safety lifecycle is briefly described.

1. Introduction
The automotive industry is undergoing perhaps the most important changes since Henry Ford launched the conveyor belt. Over the last hundred years, engineers have been working to improve the vehicles driven by humans. Today, the direction of development is changing. More and more systems now take over the functions previously performed by human drivers. These systems are called Driver Assistance Systems (DAS). Already developed and launched in the series are systems like automatic emergency braking (AEB) \cite{1–4}, lane keep assist (LKA) \cite{5–9}, signage assistance systems (SAS) \cite{10–15} and many others \cite{16–18}.

However, car manufacturers are not going to limit themselves and focus on driver assistance systems only. For example, Tesla Motors (USA) developed the “Autopilot” system (Figure 1A). According to the company, this system can fully take over the control of the vehicle in some cases. Other car manufacturers are developing similar systems \cite{19–22}.

The main barrier to the widespread introduction of autonomous driving technologies is posed by safety issues. Tesla Motors’ cars with activated Autopilot system have already caused a number of accidents (Figure 1B). Similar incidents have also occurred with vehicles of other manufacturers (e.g. Uber). According to the Fatality Analysis Reporting System (FARS), seven people have already died in autonomous car accidents. The indicator of the number of fatalities per 100 km driven is higher for Tesla cars than the average for cars of the same class (p<0.05). Investigations of the various accidents confirm the potential danger of autonomous driving.

It is believed that the methods of dealing with the threats related to the operation of vehicles on public roads are different for autonomous and non-autonomous systems.
Figure 1. Tesla Model S with activated Autopilot
A — Functioning “Autopilot” system
B — Autopilot-induced collision with a fire vehicle (Culver City, California, USA, January 2018)

2. Autonomous systems: Methods for safety lifecycle
The safety methods used in the development of vehicle systems cannot fully protect passengers, drivers and other road users from hazards associated with autonomous vehicles on public roads. ISO 26262 is the standard for the vehicle systems safety. It does not cover hazards not related directly to system component failures.

The newly developed ISO 21448 "Safety of the Intended Functionality" deals with hazards caused by environmental factors. Such factors include e.g. the illumination that affects the functionality of systems based on camera. In addition, it also covers unintentional errors committed by the driver or operator of the vehicle. The distinction between ISO 26262 and ISO 21448 is shown in Figure 2.

Figure 2. Methodologies to ensure the safety of vehicle systems [23, 24]
The number of failure modes of the system components is finite. At the same time, the number of different traffic situations, taking into account different variants of parameterization, is infinite. Therefore, ISO 26262 methods (inductive and deductive system analysis, testing and validation of specifications) do not fully cover the safety needs of AD and ADAS systems. Comparison of safety life cycles according to ISO 26262 and ISO 21448 is presented in [23, 24]. There one can also find a definition of the scenario for the description of the traffic situation. In the next section we will consider the differences between the hazard analysis for the systems of zero level of autonomy and subsequent levels.

3. Methods

3.1. Hazard analysis

According to ISO 26262 and ISO 21448, a hazard is a potential source of risk. The purpose of the hazard analysis and risk assessment (HARA) is to identify and categorize the hazards associated with the operation of the system under analysis, as well as to determine the safety goals required to deal with those threats.

3.1.1. Non-autonomous systems. The HARA for non-autonomous systems in accordance with ISO 26262-3 is carried out according to the scheme presented in Figure 3.

![Figure 3. Hazard analysis for non-autonomous systems](image)

Here $f$ is the list of functions of the system under study, $M$ is the list of functional failures (malfunctions). By analyzing the behavior of a car with different types of failures in different scenarios, possible negative consequences are determined. This is followed by a classification of these consequences by severity ($S$), the time that the driver and passengers spend in the state where the consequences may occur (exposure time, $E$), and the driver's ability to avoid the consequences ($C$). The table from ISO 26262-3 is then used to determine an ASIL – the safety integrity level suitable to this failure in the selected scenario. The result of the analysis is a list of safety targets with corresponding ASIL levels. Scenarios are described here in natural language, classifications $S$, $E$ and $C$ are estimated.

3.1.2. Additional aspects for autonomous systems. For hazards caused by component failures in autonomous systems, the HARA is performed in the same way as for non-autonomous systems (see Figure 2). Due to the more diverse nature of the events that can cause autonomous systems to fail, classification by $S$, $E$, and $C$ parameters, as well as finding a common ASIL level, is meaningless. Instead, the probability of consequences of various degrees of severity is determined, which can then be compared to accident statistics. If the overall probability of severe consequences does not increase due to the operation of an autonomous system, the system remains safe [23, 24].

To determine the probability of the occurrence of certain negative consequences, Monte Carlo simulation based on parameterized scenarios is used.
3.2. Parameterization of scenarios

According to ISO GTC 21448, the following information is included in the scenario definition:

- Scene (information about nearby objects)
  - Dynamic elements (other cars, pedestrians, cyclists, etc.)
  - Static elements (road infrastructure, trees, etc.)
- Actions and events occurring during the scenario performance
- Objectives and indicators defining the safety of the scenario, quality of driving, compliance with the requirements of the road traffic regulations and other evaluation factors (KPI)

Static and dynamic elements of the scene are determined by numerical parameters. These parameters cannot be specified unambiguously, they have some probability distribution. For example, let's consider a scenario where two cars follow each other along a straight road section (Figure 4). This scenario is important for designing an autonomous emergency braking system (AEB).

![Figure 4. Scenario «car following»](image)

Figure 4 shows the following scenario. On a straight stretch of road, two cars follow each other at a distance \( d \) in one direction and at the same speed \( v \). The front car is equipped with an AEB system. At a certain point in time \( t_0 \), the AEB system is activated in the front car. This results in a maximum negative acceleration braking \( a \). The negative consequence of this situation is that the rear car is hitting the vehicle in front of it because the driver of the rear car may not be able to respond to a sudden change in speed. The result of such collision may be human casualties.

Let's assume that the maximum braking acceleration of both cars is the same. The second car starts to brake in time \( \tau \) after the first one because of the delay in the driver's reaction. After braking starts, the distance between the two vehicles is determined by the formula:

\[
d(t) = d - \frac{a\tau^2}{2} - a\tau t
\]

(1)

The collision time (i.e. the moment when \( d(t) \) becomes zero) is determined by the formula:

\[
t_c = \frac{d - a\tau^2/2}{a\tau}
\]

(2)

Vehicle speed difference at the moment of collision \( \Delta v = a\tau \). The difference in speed determines the severity of injuries to drivers and passengers of both vehicles during the collision.

3.3. Probabilistic modelling

From the traffic data [25], the distributions of drivers' response time to sudden changes in situation (\( \tau \)) as well as the time distance \( d_t = d / v \) are known. The corresponding distributions are shown in Figure 5.

Negative acceleration \( a \) was assumed to be constant and equal to 9 m/s\(^2\).

A Monte Carlo simulation was performed using the Markov property, i.e. each subsequent pair of random variables did not depend on the previous results. In addition, random \( d_t \) and \( \tau \) values were considered as independent.
4. Results
As a result of modeling the dependence between initial velocity and probability of realization of various negative consequences has been received. Avoidance of a collision or a non-injury collision (S0 according to ISO 26262 classification), minor (S1), moderate (S2), or severe (up to fatal) injuries were chosen as possible implementations. The result is shown graphically in Figure 6.

By using the risk graph from ISO 26262-3, it can be established that the required level of integrated safety in this scenario is ASIL B. There are various ways to reduce this level. One possibility is to reduce the maximum speed at which the AET system is active to 20 m/s. Another way is to change the system so that the AEB system is deactivated if a vehicle equipped with the system is followed by
another vehicle at a dangerous distance. This will require the installation of additional sensors and software components.

These results characterize vehicles driven by human drivers. They can be used as a benchmark for writing specifications for stand-alone vehicles. It can be claimed that in order to lower the injuries and fatalities in the considered scenario, an autonomous vehicle would need to have a lower response time than the driver. If it is not possible to do in case the situation corresponding to the considered scenario is detected, the autonomous vehicle will have to initiate an evasive maneuver. The development of such a maneuver will require consideration of additional scenarios and creating simulation similar to that discussed in this paper.

5. Conclusions

The article describes a method for elicitation of requirements for autonomous vehicle control systems based on parameterized traffic scenarios. As an example, the "car following" scenario (Figure 4) was chosen. This scenario was parameterized using two values - trail distance $d_t$ and driver reaction time $\tau$. Based on the available statistics, probability distributions were created for both parameters (Figure 5). This was followed by a Monte Carlo simulation, which resulted in a probability of various possible negative consequences in the "car-following" scenario (Figure 6).

It should be noted that in reality, $d_t$ and $\tau$ parameters seem to be dependent on each other and on the speed. Drivers with longer reaction times (e.g. people of advanced age) would be more likely to maintain a longer trailing distance than drivers showing good reaction time (e.g. young sports car drivers). In addition, when the flow rate is reduced, the distance between vehicles on the road is usually shortened. Consequently, simulation methods need to be improved to take these dependencies into account.

Scenario, parametrization, creation of parameter distribution and modeling in this paper were performed using MathWorks MATLAB and Microsoft Excel software products. As the level of autonomy of the systems under consideration increases, the number of scenarios to be simulated grows rapidly [23, 24]. Further it seems necessary to use formal or semi-formal language for scenario description together with an interpreter capable to create necessary models and distributions in an automated mode in a form acceptable for using in simulation software.

References

[1] Miholjic D, Fabbroni M and Robinson R 2019 A Study of the Performance of Automatic Emergency Braking (AEB) Systems Equipped on Passenger Vehicles for Model Years 2013 to 2018 SAE Tech. Pap. 2019 April
[2] Ariyanto M, Haryadi G D, Munadi M, Ismail R and Hendra Z 2019 Development of Low-Cost Autonomous Emergency Braking System (AEBS) for an Electric Car Proc. — 2018 5th Int. Conf. on Elec. Vehic. Techn. pp 167–171
[3] Lee D H, Kim S K, Kim C S and Huh K S 2014 Development of an autonomous braking system using the predicted stopping distance Int. Journ. of Aut. Techn. 15 (2) pp. 341–346
[4] Jin P F, Kim J H and Kim J H. 2015 Design of unmanned vehicle advanced braking system using smart motor 12th Int. Conf. on Ubiquit. Rob. and Amb. Intell. pp 167–171
[5] Tominaga K, Takeuchi Y, Tomoki U, Kameoka S, Kitano H, Quirynen R, Berntorp K and Cairano S 2019 GNSS based lane keeping assist system via model predictive control SAE Tech. Pap. 2019 April
[6] Cerone V, Chinu A and Regruto D 2002 Experimental results in vision-based lane keeping for highway vehicles Proc. of the Amer. Contr. Conf. 2 pp 869–874
[7] Cerone V, Milanese M and Regruto, D 2009 Combined automatic lane-keeping and driver's steering through a 2-DOF control strategy IEEE Transact. on Contr. Syst. Techn. 17 (1) pp 135–142
[8] Beglerovic H, Schloemicher T, Metzner S and Horn M 2018 Deep learning applied to scenario classification for lane-keep-assist systems Appl. Scienc. (Switzerland) 8(12)
[9] Hsu J Y, Ku K L, Jhang T K, Lin H P and Yeh C J 2017 Integration and implementation of a lane keeping system with vehicle dynamics control Int. Autom. Contr. Conf. 2017 November pp 1–6
[10] Stallkamp J, Schlipsing M, Salmen J and Igel C 2012 Man vs. computer: Benchmarking machine learning algorithms for traffic sign recognition Neur. Netw. 32 pp 323–332
[11] Sermanet P and Lecun Y 2011 Traffic sign recognition with multi-scale convolutional networks Proc. of the Int. Joint Conf. on Neur. Netw. pp 2809–2813
[12] Bahlmann C, Zhu Y, Ramesh V, Pellkofer M and Koehler T 2005 A system for traffic sign detection, tracking, and recognition using color, shape, and motion information IEEE Intel. Vehicl. Symp., Proc. pp 255–260
[13] Maldonado-Bascón S, Lafuente-Arroyo S, Gil-Jiménez P, Gómez-Moreno H and López-Ferreras F 2007 Road-sign detection and recognition based on support vector machines IEEE Trans. on Intel. Transp. Syst. 8(2) pp 264–278
[14] Shadeed W G, Abu-Al-Nadi D I and Mismar M J 2003 Road traffic sign detection in color images Proc. of the IEEE Int. Conf. on Electr., Circ., and Syst. 2 pp 890–893
[15] Loy G and Barnes N 2004 Fast shape-based road sign detection for a driver assistance system IEEE/RSJ Int. Conf. on Intel. Robots and Syst. 1 pp 70–75
[16] Kotiev G O, Butarovich D O and Kositsyn B B 2018 Energy efficient motion control of the electric bus on route IOP Conf. Ser.: Mat. Sci. and Eng. 315(1)
[17] Medvedev V, Butarovich D and Smirnov A 2019 Prototyping of the remote monitoring system of battery condition of the electric vehicle Journ. of Phys.: Conf. Ser. 1177(1)
[18] Sarach E, Kotiev G and Beketov S 2018 Methods for road microprofile statistical data transformation MATEC Web of Conf. 224
[19] Rao S J, Seitz T, Lanka V R R and Forkenbrock G 2019 Analysis and mathematical modeling of car-following behavior of automated vehicles for safety evaluation SAE Techn. Pap. 2019-April
[20] Yakusheva N, Proletarsky A and Basarab M 2018 Pedestrian-Vehicle Collision Avoidance Strategy for NLOS Conditions 26th Telecom. For. — Proc.
[21] Munir F, Azam S, Hussain M I, Sheri A M, Jeon M 2018 Autonomous vehicle: The architecture aspect of self driving car Proc. — IEEE INFOCOM 2018 April pp 72–80
[22] Osipkov V, Ksenevich T I, Belousov B, Karasev O, Sokolov S, Rudynets M, Skalyga M, Naumov S, Stepnov V and Klimachkova A 2016 Intelligent Transport Systems: Revolutionary Threats and Evolutionary Solutions SAE Techn. Papers April
[23] Kirovskii O M and Gorelov V A 2019 Driver assistance systems: tests and the safety case. ISO 26262 and ISO PAS 21448 IOP Conf. Ser.: Mat. Sci. and Eng. 534(1)
[24] Kirovskii O 2019 Determination of Validation Testing Scenarios for an ADAS Functionality: Case Study SAE Techn. Pap. 2019-April
[25] Christopher Kober 2018 Stochastische Verkehrsflussimulation auf Basis von Fahrerverhaltensmodellen zur Absicherung automatisierter Fahrfunktionen Springer Vieweg, (Stuttgart) p 162