The Analysis of International Standards in the Field of Safety Regulation of Highly Automated and Autonomous Vehicles

A. M. Ivanov
Moscow Automobile and Road Construction State Technical University (MADI)
Moscow, Russia
ivanov-am@madi.ru

S. S. Shadrin
Moscow Automobile and Road Construction State Technical University (MADI)
Moscow, Russia
shadrin@madi.ru

D. A. Makarova
Moscow Automobile and Road Construction State Technical University (MADI)
Moscow, Russia
dariamakarova.madi@gmail.com

2022 Systems of Signals Generating and Processing in the Field of on Board Communications | 978-1-6654-0635-2/22/$31.00 ©2022 IEEE | DOI: 10.1109/IEEECONF53456.2022.9744341

***Abstract*— This article examines the safety structure of highly automated vehicles (HAV), substantiates the problems of assessing and ensuring the safety of automated driving systems. It presents the main initiative groups at the international level engaged in the development of a safety regulation system for highly automated and autonomous vehicles. The main international standards that currently exist and those, that develop and can potentially serve as a basis for a safety regulation system development for highly automated and autonomous vehicles, are considered and analyzed in the article. The aspects of an integrated approach for the development of a safety regulation system of HAVs are formulated.**

***Keywords*— highly automated vehicles, autonomous vehicles, safety standards, ISO 26262, ISO/PAS 21448.**

I. INTRODUCTION

The deployment of an autonomous vehicle into the transportation sector and industrial infrastructure is an inevitable stage of the smart transport systems development. The advantages of the autonomous vehicles integration include: the perspective of reducing traffic accidents with fatal outcomes; effective roads usage due to centralized traffic management; increased mobility opportunities for people without driver's licenses, disabled people, underage groups; saving personal time due to the ability of doing business during the trip; an exclusion of the human factor while transporting highly dangerous cargo or doing assignments in war zones and natural disaster areas. Today, the largest manufacturers in the field of transportation industry together with IT developers and other interested organizations around the world are actively developing vehicles with the possibility of fully autonomous driving. It is important to mention that today there are no cars with the 5th level of automatization existing in the world. According to the SAE J3016 scale such cars are fully autonomous vehicles and can be operated in any conditions without requiring a human safety driver. Currently there are many countries testing HAVs of the 3rd and 4th automatization levels on the public roads. At the same time, the HAVs usage takes place in limited conditions called operational design domains (ODD) and requires the presence of a human safety driver who can switch control to manual mode or, according to some rare recent practices, accompanying cars with the ability to switch control to remote mode.

The key factor that is determining the development and introduction of HAVs into the industrial and transportation structures is to ensure the safety of their usage. In addition, the issues of responsibility and public approval are significant.

However, despite the obvious advantages of the HAVs integration, it is associated with a number of complicated problems, and the main one is to ensure the safety on the roads. This is a key factor, determining the further development and time slots of HAVs complete integration to public roads. Firstly, ensuring the safety of HAVs by manufacturers requires a system of standard requirements and evaluation methods, using an integrated approach. The safety regulation system for highly automated and autonomous vehicles is currently being developed [1,2,3].

This article will overview the international standards that currently exist and can serve as a basis to create the regulation system for the highly automated and autonomous vehicles safety.

II. HAV SECURITY STRUCTURE

The safety of a vehicle is a set of constructional and operational features that are supposed to ensure the safe functioning of the DCRE complex (driver – car – road – environment), which implies the saving of human life and health by reducing the possibilities of accidents and the severity of their consequences and also limiting the negative impact on the environment.

978-1-6654-0635-2/22/$31.00 ©2022 IEEE

The holistic vehicle safety for the convenient record of its individual aspects is conventionally divided into active, passive, post-accident and environmental safety. Information security should also be added to the list of HAVs' complex security components along with the ones that have already been mentioned, due to the smart systems included in HAVs' structure [2,3].

Information Security – is a set of the highly automated vehicle's software features that is supposed to eliminate an unauthorized use of the smart vehicle systems. These features include [8,9]:

- confidentiality of users' personal data;
- data integrity (protection against electronic jamming, protection against software viruses, protection against interception of vehicle control);
- availability (correct response of the smart system to the operator's requests).

Ensuring the information security of highly automated vehicles is one of the most important factors in their development, due to the direct impact on the safety of the functioning of the DCRE system. The problem of cybersecurity will tend to be even more urgent when the number of highly automated vehicles grow, because there will be a risk of unauthorized use of the car groups. The presentation of high demands to the information security of HAVs requires research in this area and the development of new methods to ensure it.

Passive safety - the construction features that reduce the severity of consequences after road accidents for the operator, passengers and cargo [4,5].

The passive safety of the car can be divided into an external and internal one. The main requirement of external passive safety is to ensure the design of the exterior surfaces and the elements of the car, that in case of an accident, would minimize the probability of damage and severity of injuries to pedestrians, cyclists and passengers of the other vehicles involved.

There are two main requirements for the internal passive safety of the car:

– creating conditions when a person could safely handle the significant overloads;

– minimizing the injuries of the driver and the passengers inside the vehicle in case of an accident.

The trends in the development of modern vehicles determine the availability of internal passive safety tools that are more effective, including: energy-absorbing structural elements, safety frames and active seat headrests, that can also be used in the highly automated vehicle designs.

The modern system of ensuring the external passive safety is a pedestrian protection system designed to reduce the consequences of a pedestrian collision with a car in a traffic accident. This system is manufactured by TRW Hodings Automotive (Pedestrian Protection System, PPS), Bosch (Electronic Pedestrian Protection, EPP), Siemens and since 2011 has been installed into serial passenger cars of European manufacturers of the higher-priced category. The concept of operation of the pedestrian protection system is based on opening the hood when a vehicle collides with a pedestrian, which increases the space between the hood and the engine parts and, accordingly, reduces the human injuries. In fact, the raised hood works like an airbag.

Along with this system, the following design solutions are used in the modern vehicles to protect the pedestrians and to reduce the injuries in case of an accident: a "soft" hood, frameless brushes, a soft bumper, a sloping incline of the hood and the windshield, an increased distance between the engine and the hood.

All the systems and the elements of external and internal passive safety that were mentioned above should be included in the design of highly automated vehicles, due to the increased requirements for their safety caused by the social aspects as well. Besides, the designs of highly automated vehicles are distinguished by the presence of a large number of electrical equipment that also causes the increased requirements for fire safety.

Active safety is a complex of technical and operational features that is supposed to ensure the safe interaction of a highly automated vehicle with other elements of the transport system on the road (other vehicles, pedestrians, infrastructure elements) by reducing the possibility of road accidents and eliminating their preconditions related to the design features of the vehicle [2,3].

The operational features of active safety for the highly automated vehicles include dynamic features, controllability and stability. The design features of active safety for the highly automated vehicles include weight and size characteristics of the vehicle, external informativeness (shape, color, lighting devices), reliability of the components and the aggregators. The determining factors of the active safety of a highly automated vehicle are the designed and the operational reliability and correctness of its systems and aggregates that affect safety (Fig.1).

- monitoring systems or systems of perception of the surrounding space by the vehicle;
- a control system that analyzes the data received from sensors and detectors and composes an algorithm of action;
- executive systems and units functionally related to the implementation of the maneuver based on the commands of the control system;
- redundant control circuits;
- security monitoring system.

In addition, an important aspect of the safety of the HAVs together with what has already been mentioned is the reliable situational awareness and the programmed correct response of the automated system to any situations that may happen on the road.

III. The Most Important Initiative Groups in the Field of Developping a Safety Regulation System of HAVs

The World Forum on the Harmonization of the Rules Related to Vehicles and Their Systems and Units WP.29, is a global forum for open discussions on the requirements to be followed by the automotive industry worldwide.

Within WP.29 there are six permanent working groups, divided by the subject. The GRVA Working Group works with automated and connected vehicles. This working group actively amends and develops new UNECE regulations in the field of regulating the safety of HAVs and ADAS systems. The latest important documents developed by GRVA were the rules on cybersecurity UN Regulation No. 155 and UN Regulation No. 156, UN Regulation No. 157 "Automated Lane Keeping System" (these documents will be discussed in detail later), amendments were also made to UN Regulation No. 79 regards to steering equipment, which contains requirements for testing automated control systems of different autonomy levels [6]. At the same time, the rules have not yet been developed for fully autonomous systems that can independently make a maneuver decision and carry out a maneuver depending on the traffic situation.

ISO is an international organization for standardization, whose technical committees prepare international standards. ISO cooperates closely with the International Electrotechnical Commission (IEC) on all issues of electrotechnical standardization. International governmental and non-governmental organizations participate in the development of international standards, which may be submitted to the committee.

Technical Committee ISO/TC 204 works with the system and infrastructure aspects of the smart transport systems, and includes 26 working groups on narrowed topics.

The Society of Automotive Engineers SAE International is a global association for the development of standards in the transport industry with a focus on mobility. SAE members include more than 138,000 engineers in the transportation industry worldwide. Thus, SAE standards represent the optimal technical content developed in a transparent, open and collaborative process.

In 2019, SAE International created the Consortium for the Safety of Automated Vehicles. This committee develops standards in the field of safety regulation of HAVs both separately and together with other international organizations, for example, with the ISO/TC 204 technical committee.

While some countries, mainly the countries of the European Union that use the type approval system, participate in the creation of the safety regulation system for HAVs, contributing to the development of international standards, some other countries prefer self-certification. Today Australia, Germany, China and the USA have the most developed national system for regulating the safety of HAVs.

IV. ISO 26262 "Road Vehicles – Functional Safety"

The ISO 26262 standard describes the requirements and the methods for assessing the functional safety of electrical and/or electronic systems related to vehicle safety. The standard was developed by the Technical Committee ISO/TC 22/SC 32 "Electrical, electronic components and types of general purpose systems", consists of 12 parts, the last edition was released in 2018 [7].

In a broad sense, functional safety ensures that the system has the ability to sufficiently reduce the risk of failure in case of identified hazards.

The amount of mitigation measures required depends on the severity of the potentially dangerous situation, the severity of its consequences and the possibility to avoid it due to the actions of the driver or the other road users. These factors are combined into the Vehicle Safety Integrity Level (ASIL) according to a pre-established risk table. The designated ASIL determines which technical and technological measures should be applied, including certain design and analysis tasks. ISO 26262 (Fig.1) conforms to safety standards, like IEC 61508, regarding such aspects as:

- Defines a basic process model based on the V-model;
- Considers software, hardware and system aspects using integrity levels;
- Includes life cycle topics such as production, operation, support and tools;
- Defines a security approach that includes hazards, security objectives and ASIL;
- Defines methods of analysis, design and verification based on ASIL.

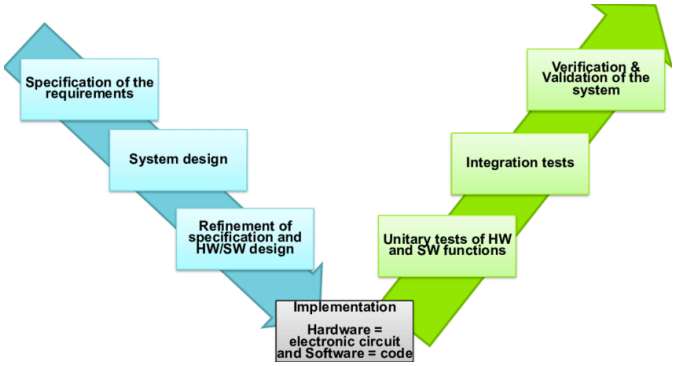

Fig. 1. The Structure of ISO 26262 "Road vehicles – functional safety"

Thus, ISO 26262 standard focuses on preventing design errors and mitigating the consequences of equipment failures during it's work. However, ISO 26262 does not count other security threats that may arise in the absence of system failures that are relevant for the operation of automated control systems. An example of such a situation is incorrect recognition of the road situation by the HAVs sensors, which in turn leads to incorrect behavior of the HAVs that can cause an accident. To work with such cases, ISO released the ISO/PAS 21448 standard in 2019, that relatively easy integrates with ISO 26262 [8].

V. ISO/PAS 21448 «ROAD VEHICLES - SAFETY OF THE INTENDED FUNCTIONALITY»

ISO/PAS 21448 (Fig.2), commonly called SOTIF (Safety of intended functionality) covers previously problematic areas for ISO 26262 related to the safety of the target functions.

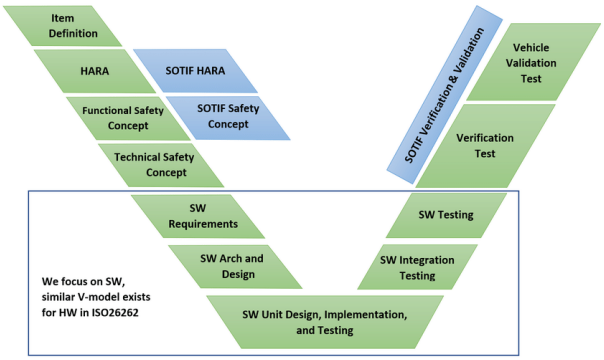

Fig. 2. The Structure of ISO/PAS 21448 «Road vehicles - safety of the intended functionality»

The purpose of SOTIF is to guarantee the safety of the functioning of the vehicle in the absence of the system failures. This standard covers such aspects as: predicted improper operation, problems of human-machine interaction, problems arising in connection with operational conditions (weather, infrastructure, etc.), as well as insufficient situational awareness, which is based on sensors and processing algorithms; (for example, active safety braking systems or adaptive cruise control).

Thus, the ISO 21448 standard expands the scope of the ISO 26262 standard to cover the functionality of ADAS systems and can be applied to the vehicles of the 1st and the 2nd driving automation levels on the SAE J3016 scale.

Together, ISO 26262 and ISO 21448 form the basis for the development of a safety regulation system for autonomous vehicles. However, in order to assess and ensure the integrated security of HAVs from 3rd to the 5th automation level, these standards need to be supplemented with risk acceptance criteria for automated control systems, more advanced modeling and analysis methods, as well as coordinated integration with new standards for automated control systems, which will be discussed further.

The publication of an updated version of the ISO/PAS 21448 standard, that is supposed to count the aspects above and will be applicable to the vehicles of the 3rd and 4th automation levels, is scheduled for 2022.

VI. THE LATEST STANDARDS IN THE FIELD OF HAVS SECURITY

It is worth mentioning the new descriptive standard, published in August 202, ISO/SAE PAS 22736:2021 "Taxonomy And Definitions Of Terms Related To Driving Automation Systems For Road Vehicles" [9]. This document was developed by the ISO/TC 204 Technical Committee, Intelligent Transport Systems together with the SAE Committee on Automated Driving on the Roads. There is another document, technically similar to this one, except a small number of editorial amendments, that was developed separately by the SAE on the Road, Automatic Driving Committee and published in July 2021 by SAE J3206-202, "Systematics and definition of safety principles for an automated driving system (ADS)" [10]. These documents provide definitions and classification of the safety principles of automated driving systems, in cases where an automated system performs one or more dynamic driving tasks for a long time. In other words, these standards do not apply to active security systems, since these systems operate for a short period of time. These standards are descriptive and do not cover all the aspects of automated control systems' integrated safety, including problems of interaction with other road users. As automated control systems develop, these standards will be revised and the scope of coverage will be expanded.

ISO 22737:2021 "Intelligent Transport Systems - Low-Speed Automated Driving (LSAD) Systems", published in July 2021 For Predefined Routes - Performance Requirements, System Requirements And Performance Testing Procedures" [11], which also defines system requirements, describes performance testing methods and requirements for the field of regular operation. The requirements of this standard are applied to HAVs of the 4th automation level operated within a closed low-speed environment of regular operation - operational design domains (ODD) along with a given route, for example, closed territories of enterprises. The gap in this standard is the lack of consideration of the sensors' impact..

The latest publication of the document SAE J 3018-2020 "Safety guidelines for road tests of a prototype automated driving system (ADS)-apparatus" [12] in December 2020 describes the methods and requirements for testing HAVs from the 3rd to the 5th driving automation levels, that are tested on public roads. This document also contains a safety guide for human-safety driver and is currently fundamental for regulating the safety of road tests.

In addition, the standards regulating the requirements and describing the procedure for testing intelligent ADAS transport systems are currently being actively developed and updated, which can be partially used to create a system for regulating the safety of HAVs, since they are their components. These standards include [13, 14,15]:

- ISO 22078:2020, Intelligent transport systems — Bicyclist detection and collision mitigation systems (BDCMS) — Performance requirements and test procedures
- ISO 19237:2020, Intelligent transport systems — Pedestrian detection and collision mitigation systems (PDCMS) — Performance requirements and test procedures
- ISO 15622:2018 Intelligent Transport Systems - Adaptive Cruise Control Systems - Performance Requirements And Test Procedures and other earlier standards.

VII. UNECE standards

The UNECE UN Regulation No. 157 "Automated Lane Keeping System" adopted by the UNECE's World Forum for Harmonization of Vehicle Regulations (WP.29) and started being effective in January 2021, are the first mandatory

international rules for regulating the safety of highly automated vehicles of the 3rd automation level[16].

The Regulations set out clear technical requirements for production that must be followed by car manufacturers before vehicles equipped with ALKS can be sold in countries where these regulations apply. The UNECE stated that these rules will be working in the European Union when being effective. The decision-making authorities of Germany and Japan, who led the development of this regulation, as well as the delegations from Canada, the Netherlands and France who participated in the development, have already applied these rules in their countries.

Activation of the Automated Lane Keeping System, according to these rules, is limited when driving up to 60 km/h and can be carried out in those areas of public roads where there is no presence of pedestrians and cyclists, and there is a physical separation from oncoming traffic.

In addition, the standard includes requirements for the human-machine interface, the required compliance criteria for the Automated Lane Keeping System, for testing these systems, for monitoring the technical condition and for reporting.

UN Regulation No. 157 imposes requirements for the implementation by manufacturers of the Automated Lane Keeping System, the so-called black box, and the human-safety driver presence and status recognition system. In addition, these rules describe the requirements for transferring control to manual mode and for switching to minimum risk mode, in the case when a human-safety driver cannot take control.

Based on UN Regulation No. 157, the ISO 22735:2021 standard "Road Vehicles - Test Method To Evaluate The Performance Of Lane-Keeping Assistance Systems" was updated, which was published in May 2021 [17]. This standard contains the requirements and describes the methods for testing and evaluating the performance of lane-keeping assistance systems.

Automated Lane Keeping Systems must also comply with the UNECE Cybersecurity Regulations UN Regulation No. 155 "Cyber Security and Cyber Security Management System" and UN Regulation No. 156 "Software Update and Software Update Management System", which were adopted on the same day [18,19].

The basis for the development of UN Regulation No. 155 was the ISO/SAE 21434 standard "Road Vehicles - Cybersecurity Engineering" [20]. UN Regulation No. 155 entered into force in January 2021, and from July 2022 will be mandatory for the official approval of all new types of vehicles in countries that are members of the European Union, and from July 2024 these rules will apply to all vehicles.

UN Regulation No. 156, as well as the above standard, entered into force in January 2021 and from 2022 will become mandatory for the approval of new types of vehicles. Both of these standards are aimed at reducing the growing risk associated with the expansion of the functionality of developing automated driving systems.

The ISO/TR 4804:2020 technical report "Road Vehicles - Safety And Cybersecurity For Automated Driving Systems - Design, Verification And Validation", published in December 2020, is also important in the field of cybersecurity of automated control systems. This document was developed on the basis of data from publications on a given topic around the world [21]. The main source for this document was the principles described in the white paper with the title "Safety First for Automated Driving" (SaFAD), published in 2019 by Daimler together with leading companies in the automotive industry [22].

ISO/TR 4804 is applicable to HAVs 3 and 4 levels of driving automation, and contains recommendations for reducing cybersecurity risks during development and during operation, as well as methods for evaluating and validating cybersecurity parameters in the context of integrated security of HAVs. It is expected that this standard will be finalized taking into account the UN Regulation No. 155 and No. 156 that were released after its publication.

VIII. SO TS 5083 «ROAD VEHICLES – SAFETY FOR AUTOMATED DRIVING SYSTEMS –DESIGN, VERIFICATION AND VALIDATION»

At the 11th session of the UNECE on the 28th of September 2021, the goals and stages of the development of the safety standard for automated driving systems planned for 2023 called ISO TS 5083 "Road Vehicles – Safety for automated driving systems –Design, verification and validation" were discussed, which will combine all the standards related to special topics of automated driving and will determine the whole picture using a holistic approach to safety for automated driving systems of SAE level 3 and 4. The basis for the development of this standard will primarily be the ISO 26262 (functional safety) and ISO 21448 (SOTIF) standards, as well as the above-mentioned cybersecurity standards. The development of ISO TS 5083 is carried out by the Technical Committee ISO/TC 22 Road vehicles Subcommittee SC 32 Electrical and electronic components and general system aspects working group WG13 "Safety for driving automation systems". The current structure of work under this standard is shown in Figure 3.

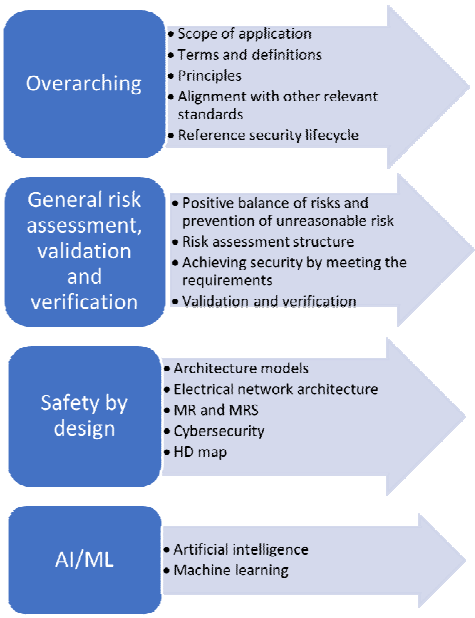

Fig. 3. The Current Structure of Work on Developing the Standard ISO TS 5083 «Road Vehicles – Safety for automated driving systems –Design, verification and validation».

IX. Conclusion

For the further development and implementation of highly automated and autonomous vehicles in the road transport infrastructure, the need to create a safety regulation system for such vehicles is urgent.

The standards discussed in this article, along with the standards currently being developed, will be applied to create a system for regulating the safety of HAVs for the 3rd - the 5th automation levels [23].

An integrated approach to the creation of a regulatory system will have to combine both general and specific safety components, characterizing the scope of the application field, to generalize the accumulated experimental experience using a multi-level approach to feedback, which includes an independent assessment, and to be updated according to the development of technologies in the field of intelligent transport system.

To ensure the safety of the developed and operated HAVs, the developer companies should follow the requirements and the recommendations specified in the listed standards while the integrated safety regulation system of HAVs is under development, and to continuously monitor the technical condition of the systems and the units that affect the safety.

References

[1] UNECE, “New Assessment/Test Method for Automated Driving (NATM) Master Document (Final Draft),” 2021, GRVA-09-07

[2] Koopman, Philip & Ferrell, Uma & Fratrik, Frank & Wagner, Michael. (2019). A Safety Standard Approach for Fully Autonomous Vehicles. 10.1007/978-3-030-26250-1_26.

[3] Dasom Lee, David J. Hess, Regulations for on-road testing of connected and automated vehicles: Assessing the potential for global safety harmonization, Transportation Research Part A: Policy and Practice, Volume 136, 2020, Pages 85-98, ISSN 0965-8564, https://doi.org/10.1016/j.tra.2020.03.026.

[4] A. M. Ivanov and S. S. Shadrin, «System of Requirements and Testing Procedures for Autonomous Driving Technologies», IOP Conference Series: Materials Science and Engineering. *International Automobile Scientific Forum, IASF 2019 "Technologies and Components of Land Intelligent Transport Systems"*, Moscow, October 16-18, 2019. Moscow: Institute of Physics Publishing, 2020. P. 012016. DOI 10.1088/1757-899X/819/1/012016.

[5] S. S. Shadrin and A. M. Ivanov, "Testing Procedures and Certification of Highly Automated and Autonomous Road Vehicles," *2021 Systems of Signals Generating and Processing in the Field of on Board Communications*, 2021, pp. 1-5, doi: 10.1109/IEEECONF51389.2021.9416103.

[6] European Commission, (WP.29/GRVA) Working Party on Automated/Autonomous and Connected Vehicles (11th session) sept-2021.

[7] ISO 26262:2018 "Road vehicles – Functional safety".

[8] ISO/PAS 21448:2019 «Road Vehicles - Safety Of The Intended Functionality».

[9] ISO/SAE PAS 22736:2021 «Taxonomy And Definitions For Terms Related To Driving Automation Systems For On-Road Motor Vehicles».

[10] SAE J3206-2021 «Taxonomy And Definition Of Safety Principles For Automated Driving System (ADS)».

[11] ISO 22737:2021 «Intelligent Transport Systems - Low-Speed Automated Driving (LSAD) Systems For Predefined Routes - Performance Requirements, System Requirements And Performance Test Procedures».

[12] SAE J 3018-2020 «Safety-Relevant Guidance For On-Road Testing Of Prototype Automated Driving System (ADS)-Operated Vehicles».

[13] ISO 22078:2020, Intelligent transport systems - Bicyclist detection and collision mitigation systems (BDCMS) - Performance requirements and test procedures.

[14] ISO 19237:2020, Intelligent transport systems - Pedestrian detection and collision mitigation systems (PDCMS) - Performance requirements and test procedures.

[15] ISO 15622:2018 Intelligent Transport Systems - Adaptive Cruise Control Systems - Performance Requirements And Test Procedures.

[16] UN Regulation No. 157 «Automated Lane Keeping System», 2021

[17] ISO 22735:2021 «Road Vehicles - Test Method To Evaluate The Performance Of Lane-Keeping Assistance Systems».

[18] UN Regulation No. 155 «Cyber Security and Cyber Security Management System», 2021.

[19] UN Regulation No. 156 «Software Update and Software Update Management System», 2021.

[20] ISO/SAE 21434:2021 «Road Vehicles - Cybersecurity Engineering».

[21] ISO/TR 4804:2020 «Road Vehicles - Safety And Cybersecurity For Automated Driving Systems - Design, Verification And Validation».

[22] Daimler, Aptiv, Audi, Baidu, BMW, Continental, Fiat Chrysler Automobiles, HERE, Infineon, Intel and Volkswagen, «Safety first for automated driving», July 02, 2019.

[23] UNECE WP.29 GRVA, ISO TS 5083 «Road Vehicles – Safety for automated driving systems – Design, verification and validation» / Report.11th session, Web Meeting, 28-Sep-2021.