TRANSPORT
ISSN 1648-4142 / eISSN 1648-3480
2020 Volume 35 Issue 4: 447–453
https://doi.org/10.3846/transport.2020.12904

CHALLENGES IN HOMOLOGATION PROCESS OF VEHICLES WITH ARTIFICIAL INTELLIGENCE

Máté ZÖLDY*, Zsolt SZALAY, Viktor TIHANYI

Dept of Automotive Technologies, Faculty of Transportation Engineering and Vehicle Engineering, Budapest University of Technology and Economics, Hungary

Received 1 November 2018; revised 21 May 2019, 5 July 2019; accepted 25 July 2019

Abstract. The traditional automotive homologation processes aim to ensure the safety of vehicles on public roads. Autonomous Vehicles (AV) with Artificial Intelligence (AI) are difficult to account for in these conventional processes. This research aims to map and attempt to close the gaps in the areas of testing and approval of such automated and connected vehicles. During our research into the homologation process of traditional vehicles; functional safety issues, challenges of AI in safety critical systems, along with questions of cyber security were investigated. Our process focuses on the integration of the already existing functions and prototypes into new products safely. As a key result, we managed to identify the main gaps between Information and Communication Technology (ICT) and automotive technology: the rigidity of the automotive homologation process, functional safety, AI in safety critical areas and we propose a solution.

Keywords: autonomous vehicle, safety critical systems, artificial intelligence, functional safety, homologation.

Notations

AI – artificial intelligence;
ALS – ambient light sensor;
ASIL – automotive safety integrity level;
AV – autonomous vehicles;
DEKRA – German Motor Vehicle Inspection Association (in German: *Deutscher Kraftfahrzeug-Überwachungs-Verein*);
FOTA – firmware over the air;
ICT – information and communication technology;
IT – information technology;
OEM – original equipment manufacturer;
SAE – Society of Automotive Engineers;
TÜV – Technical Inspection Association (in German: *Technischer Überwachungsverein*);
UNECE – United Nations Economic Commission for Europe.

Introduction

The traditional automotive homologation processes aim to ensure the safety of vehicles on public roads. AV with AI are difficult to account for in these conventional processes. This research aims to map and attempt to close the gaps in the areas of testing and approval of such automated and connected vehicles. During our research into the homologation process of traditional vehicles; functional safety issues, challenges of AI in safety critical systems, along with questions of cyber security were investigated. Our process focuses on the integration of the already existing functions and prototypes into new products safely. The next stage in the development process is to create a complete instrument chain, including criteria and measures for driving task assessment, quality levels, test catalogues and centralized methods and processes to secure and enable highly automated driving functions.

The current homologation and self-evaluation methods were used as a basis of the study, taking into consideration the special circumstances of automated driving. At this stage of the research, a definition of the main problems is expected, in order to identify focal areas and possible avenues of solution.

1. Background materials

1.1. The homologation process of road vehicles

The main driver of the traditional homologation process is ensuring that only safe vehicles are allowed to be part of

*Corresponding author. E-mail: *mate.zoldy@auto.bme.hu*

public road traffic (Martins 2010). In order to put a vehicle in a specific market, manufacturers must prove or confirm officially that it meets or exceeds all relevant regulatory standards and specifications. Worldwide there are three existing methods (Zöldy 2018) to formally show that a vehicle meets regulatory standards and specifications as presented in Table.

With international participation, the *World Forum for Harmonization of Vehicle Regulations* (WP.29) was held in 1958. With the presence of the most important internal combustion engine vehicle manufacturing countries the WP.29 drafted a standalone structure for harmonized regulations on vehicles on a global level (GlobalAutoRegs 2020). Such deeply harmonized regulations had a tangible positive effect on traffic safety as well as environmental protection, and even in trade. The WP.29 group manages type approval/homologation type methods.

The UNECE approach is an independent third-party approved homologation process (type approval), while on the other end of the spectrum we find the OEM declared self-certification. The OEM, as the manufacturer of the vehicle declares that the vehicle conforms/complies with the list of regulations and declares that it is safe for public road traffic.

Type approval process is carried out by an OEM independent organization, typically TÜV or DEKRA, who certify the component/product fulfils the applicable regulations and can go to market. It is mainly used in the EU, India and China.

Self-certification concerns product liability, and is more frequently used in the US. It is based on a certificate provided by the producer that guarantees that the product meets all relevant standards.

Table. Official methods to indicate that a vehicle meets the regulatory standards (Zöldy 2018)

Method name	Certificatory/approver	Country
Type approval/ homologation	Government	EU, China, India
Self-certification	Manufacturer	US, Canada
Combined self-certification and type approval	Combined	Brazil

1.2. Functional safety

A typical state-of-the-art vehicle has more coding lines than a jumbo jet (Edelstein 2015). Even moderately sophisticated automobiles contain longer codebases with higher complexity than similar vehicles from couple of years ago. The emergence of multi-featured infotainment systems, the variety of driver-assist technologies, and electronically supported safety features are now typical components – even in low cost economy models – all adding up to the increasing role of computing in the vehicle industry.

1.3. Safety critical systems

State-of-the-art deep neural networks, such as those utilized in AV, necessitate an enormous amount of computational power. Computational capability is increasing continuously; a single computer used for testing and developing purposes today outpaces the computational performance of the world's leading supercomputers in 2010.

The increasing demand for calculation performance is especially relevant in case of safety critical systems, like self-driving vehicles. The need for precise detection in case of autonomous cars is definitely greater than in other industries. These systems are expected to function perfectly irrespective of road surface quality, visibility or weather conditions (Pinchon *et al.* 2019).

Neural networks could be trained on representative datasets to achieve this level of performance. Databases must contain samples of all potential driving, traffic, situational- and meteorological conditions. Based on the preliminary calculations, the needed storing capacity could even reach the more hundred petabyte (Grzywaczewski 2017). Furthermore, deep neural networks should have an appropriate number of parameters to be able to learn from enormous databases without losing their own previous experience (Goodfellow *et al.* 2016). As an example, if the database size is increased by a factor of n, in the same second calculating resources will growth by a factor of n^2, generating a real multifarious engineering challenge. Teaching on a single graphics processing unit could take several months to complete the training process for a traffic situation based on its high complexity, depending on the internal design of the neural network. Not only should the teaching/learning process be taken into consideration but also networking, storage and algorithms (Wang *et al.* 2018).

1.4. Cyber security

It is becoming more and more evident as the technology for autonomous cars develops, that cyber security is a critical subject, which will impact on public trust and acceptance of driverless cars. This is not a new concept by any means, and manufacturers, as well as those involved in the supply chain, are treating cyber security with the utmost priority as they embark on the journey towards AV (Valasek, Miller 2014).

Self-driving and connected vehicles are called as cyber-physical system by researchers, as these contain parts not only in the real world but virtually as well. It is clear that these systems have to be protected, which posits a significant challenge for the automotive industry: to provide the required safety level of intelligent vehicle transportation.

1.5. Certification issues

There are still a high number of challenges to be regular part of the everyday mobility for AV, from technical feasibility and legal background to general acceptance by the public. From the automotive industry's point of view, the main question is how to guarantee safety (Reschka 2016).

As discussed previously, traditional vehicles have their own validation process through either homologation or

self-certification. In case of AV, software is an element, which must fulfil high-quality criteria and should be independently certified. Traditional tests are not able to measure software elements, and the neural networks of AV in an acceptable timeframe (Tettamanti *et al.* 2016).

1.6. Outlook on other transportation systems

The homologation process and safety/security related questions of increasing autonomy are relevant in other transportation systems as well.

Digitalization will become more and more important in railway traffic as well (Esser, Schindler 2016). Completely driverless, automated metro systems are in operation for instance in Nuremberg (Germany) (Maurer *et al.* 2016) and Budapest (Hungary) (Fraszczyk *et al.* 2015). There is a legally self-contained traffic space for rail travel; in addition, logic-based systems and external monitoring are used to avoid collision between two trains. Only in closed industrial railways and tramway systems is autonomous driving feasible. In all cases, further assistance systems can increase the safety, reliability and efficiency of railway traffic (Esser, Schindler 2016). AV already exist in railway traffic; they can be part of existing system, the main issue is to increase the acceptance of driverless trains.

Commercial air travel automation does not currently provide any examples of full automation (Maurer *et al.* 2016). Even if pilots only occasionally perform flying tasks, they are still present in a supervising and operating role. Air traffic is also operated in a legally self-contained space; collision-warning systems are mandatory, and air traffic control provides an external monitoring of operations. Civilian aviation regulations are starting to account for cyber security issues as well but threats remain a continuously evolving topic needing continual care and updating. Air traffic has implemented security controls like access control, contingency planning, and physical security measures to support against potential cyber-attacks. Retention of back-ups, mitigation against spoofing, built-in cross-checks of surveillance data and encryption provide assurance that the move to integrated modular avionics will maintain a similar level of cyber security as that of earlier generation digital air traffic, while conferring added functionality and benefits (Andreades *et al.* 2017). Civilian aviation is not fully automated, pilots and air control are involved in the process. As air traffic systems become redundant, the appearing cyber security questions can be better managed.

Remote controlled and autonomous ships, without crew on-board, are in focus of research and development in the last decades. Key arguments for the support of these technological transitions are increased safety, fuel saving and emission reduction and the possibility of creation of new, interesting careers. Research is focusing on the question of, without the presence of crew, the lack of ship sense; without the crew to feel wave and wind conditions as well as engine and ship noises, and make navigational decisions accordingly (Wahlström *et al.* 2019).

2. Current challenges

2.1. Homologation process of road vehicles

The main challenge is in the homologation of new technologies to integrate IT based system components into the traditionally rigid automotive validation system. Contradictions in the type approval in the early stages of development are that there is lack of knowledge about the technology on the authority and regulatory side. There are no commonly accepted testing methodology and clarified processes with key scenarios, etc., that would allow the type approval. Restrictive regulation could result in the blocking of innovation (Zöldy 2018). New test procedures should be developed and implemented so as to merge the different automotive and IT validation frameworks.

2.2. Functional safety

ISO 26262 is the standard (9 parts) that defines the framework for automotive functional safety. It defines the ASIL classification to differentiate the severity of automotive products. On top of this, the increasing role of AV technology and connected vehicles that function as internet-of-things systems on public roads will result in even greater codebases with increased complexity.

The advancement of IT takes place in the automobile industry, increasing fears over reliability, security, and safety of electronic systems utilized in vehicles. These concerns are right, given that the supply chain of the automotive software is a complex and long system of third-party providers bridging numerous tiers. Often specific microcontroller developed software is integrated by a third-tier provider into a component that is transported to a tier level two manufacturer, and so on – until as the last step the composite component is delivered for final assembly by the producer of the car (Zöldy 2018).

2.3. Challenges of AI in safety critical systems

The calculation requirements of deep neural networks utilized in autonomous and connected vehicles are gigantic. Calculations rounding down on data volumes (Grzywaczewski 2017) show that in self-driving vehicles' car related development and research a high number of graphics processing units are needed.

Luckily, we are faced with this enormous calculation need in a moment when, for the first time in history, the necessary computing performance is ready for utilization in such complex problems as neural networks decision-making in self-driving vehicles. Calculation performance and capability is only one part of the necessary resources. A deep cooperation is needed to optimize deep neural networks and automotive data acquisition and utilization opportunities.

As Figure 1 shows, a deeply merged process is necessary to combine AI and automated vehicles. Understanding deep neural networks internal composition and

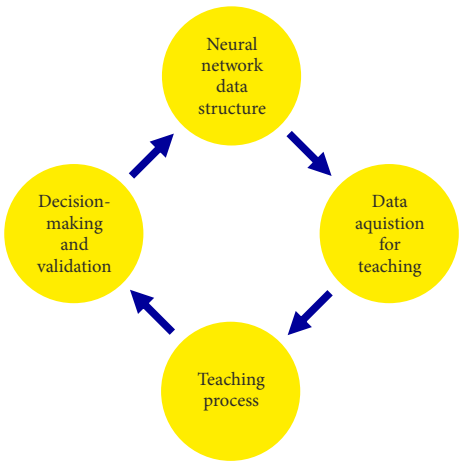

Figure 1. Merged process of utilization of neural networks in self-driving cars

opportunities is the key to setting up efficient training datasets. On field, acquired data is the basis of teaching of neural networks and well trained networks ensure safe and good decisions on the roads.

2.4. Cyber security

Connected and self-driving vehicles are more vulnerable to cyber-attacks and online threats and more sensitive to the dangers and injuries that frequently disrupt software networks, like economic and personal data theft, incorrect information from drivers, and denial-of-service type attacks that are aiming to shut down computers or even attempt stopping the vehicle itself (Shabtai *et al.* 2009). On top of this, new types of threats, unique to automated vehicles are emerging – hackers aiming to take over the control of the vehicle, or thieves who instruct a self-driving car to relocate itself to the local market (Buttyán *et al.* 2015).

Finally, the AV will connect with a numerous wireless network to arrange parking or toll paying or to get ALS from cameras, traffic lights or sensors. Homologation of AV from a cyber security point of view is not on the agenda today. On the EU level the *European Cyber Security Act* (EC 2020) has only just been completed, aiming to establish a European cyber Security certification and a standardization framework for ICT products and services.

2.5. Certification issues

It has long been clear that it is impossible to test systems thoroughly enough to ensure an ultra-dependable system operation (Török, Pauer 2018). For instance, take a theoretical fleet of one million vehicles, each tested one hour per day – that would mean 106 operational h/day. If the safety target of this fleet is to have about only one catastrophic computing failure every 1000 days, then the safety goal is a mean time between catastrophic failures of 109 h, which is comparable to aircraft permissible failure rates (Koopman, Wagner 2016). The likelihood used in the calculation means that catastrophic computing failures will happen more often during the life of the fleet of vehicles. To measure and standardize inspections, the procedures must be developed and extended.

As a first step of the inspection process, development of automotive vehicles should be classified. There are more classifications in use; one of the most used is the SAE classification that is presented in Figure 2 (Hirz, Walzel 2018).

Figure 2 shows that with increasing automation more and more complex systems are involved in the environment detection and decision-making process.

The roles of AI and neural networks are increasing as vehicles are more and more self-driving. It is an easy trend to track, as software roles are also higher and higher with increasing SAE levels (Godoy *et al.* 2015; Li *et al.* 2015). It means that this tendency should be followed as well into the regulation and homologation process. The growing role of software will naturally increase the effect of program updates on vehicle behaviour in traffic and based on that the measurement, validation and quality assurance of each software update. As result of this, increased reliance on version verification solutions of informatics should be a next step in the development of automotive vehicles and make them more suitable for the market.

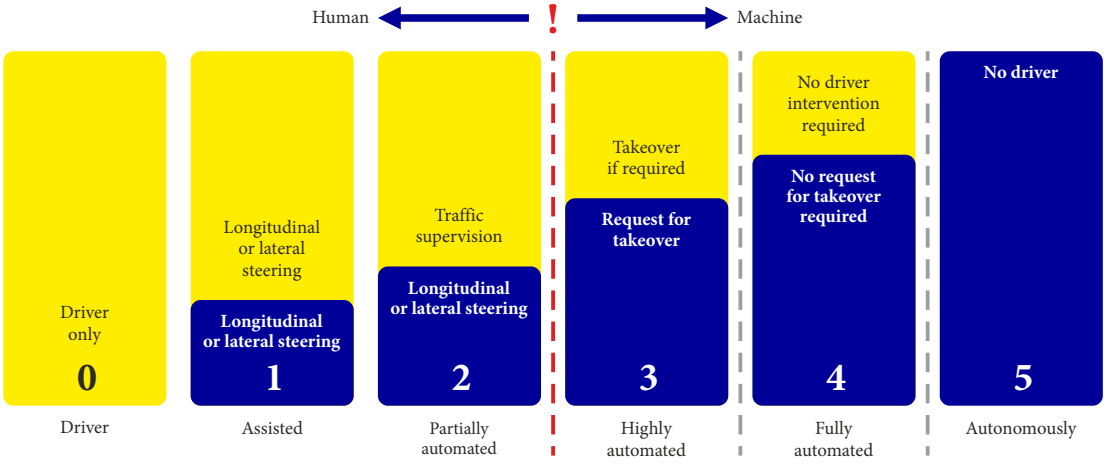

Figure 2. AV SAE classification (Hirz, Walzel 2018)

3. Proposed solutions

3.1. Homologation process of road vehicles

In fact, innovative industrial players competing with each other in the time-to-market race know that not having a universal regulatory framework may affect public safety. One approach would be to allow industrial companies to innovate - within a safe regulatory framework. This is what happened in Hungary in 2017 (Tettamanti *et al.* 2016).

A proposed special intermediate approach in Hungary was to enable self-certification in the early phase to support technological innovation until the testing methodology of the technology can be admitted into the type approval process. Since April 2017 in Hungary AV functions are allowed for testing purposes. Though Hungary also uses type approval, the testing of a hybrid solution has already been started.

3.2. Functional safety

While not all of the software utilized in the automotive industry is safety-critical, codes that carry out functional safety operations must be reliable, secure, and safe. Software quality and quality related process controls should be implemented carefully and in harmonization with the regulation of development of safety critical software. It is a functional safety standard for automotive software. It delivers guidelines on processes associated with software development for electrical and/or electronic systems in vehicles. The aim of ISO 26262 is to reduce hazards connected with software for safety functions to an acceptable level by providing feasible requirements and processes (Trujillo, Dunlop 2016).

As the main regulation for automotive software development ISO 26262 should cover the main elements of functional safety standard such as requirements definition and specification, design aspects, frame of implementation, integration with other tools, verification and validation process, and configuration. It provides guideline with the list presented on Figure 3 regarding automotive safety lifecycle activities.

3.3. Challenges of AI in safety critical systems

Testing AV in public roads is limited in Europe in accordance with the *Convention on Road Traffic: Done at Vienna on 8 November 1968* (ECOSOC 1968), which prescribes that a human driver should be in the vehicle at all times, able to take control of the vehicle. Testing and developing vehicles in a testing ground context is a common solution for automotive testing and developing purposes, but these traditional test grounds are mainly focused on conventional vehicles and do not have the special setup to challenge self-driving vehicles. According to Szalay *et al.* (2018), only one public available proving ground exists in the US (MCity) and another is just opened in Europe (ZalaZONE).

AI was born in the IT industry, and its merge with autonomous driving means it should be compatible with the prerequisites of safety critical systems as well. It is a huge gap that should be abridged and it is one of the major challenges to implement AI systems in automotive industry.

Beyond such issues is the fact that weather conditions still pose a major challenge for self-driving vehicles. Sensors in the vehicles, like human eyes, do not work properly in fog, rain or snow. Testing self-driving vehicles in such special circumstances can be solved using specialized datasets that are account for extraordinary weather conditions as well.

3.4. Cyber security

It will be a general rule; automotive specialties like safety criticality should have an increasing role. In case of automotive homologation, process safety-critical requirements should be an inevitable part due to the complexity of the electric systems.

3.5. Certification issues

The aim of the new certification process is to have certification for the security level of individual vehicle types and to provide benchmarking potential for the customers for the different vehicle models. In the meantime, a certification is an investigation snapshot of the actual status, at the time of the certification. IT related systems, however, change continuously in their lifecycle (software upgrades and updates). This is especially important in case of cyber security aspects. Similar phenomena can also be expected for the vehicle systems by using FOTA. This would mean that a cyber security certified vehicle could change its characteristics after a FOTA security update, without requiring an additional certification process.

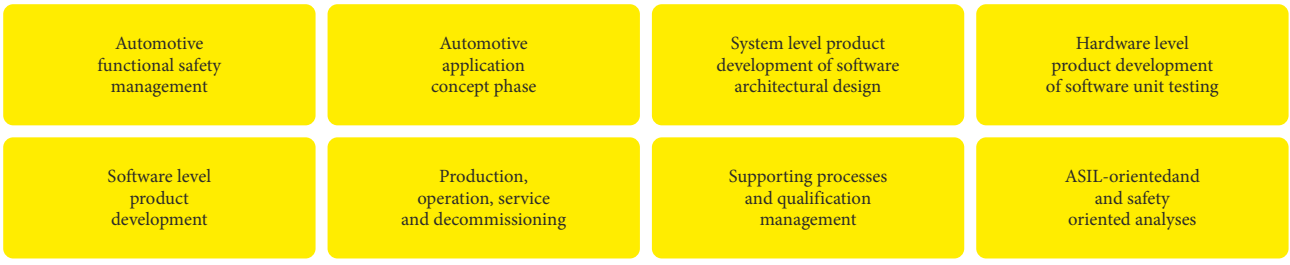

Figure 3. ISO 26262 guidelines for automotive safety critical software's

Conclusions

The integration of AV and affiliated AI into the traditional homologation and self-certification process needs further efforts. To reach complete integration, one must let AV out on the road only when they are as safe as traditional vehicles, and as key areas we define the following research fields:

Environmental consciousness of AV: with the rising popularity of AV, the detection of signalling systems and the environment, together with the control of the vehicle, may be transferred to the vehicle in certain circumstances. The aim of the research is to examine actual and newly developed autonomous systems and their impact on traffic, as well as to find the necessary factors to create the most accurate and appropriate systems of self-driving; based on weaknesses of human drivers and previous systems; explore traffic situations that can cause problems with autonomous systems and use the test environment to look for development opportunities to solve problems.

Further development of trajectory following algorithms in AV is a key area as well. With studying the vehicle dynamics, better models can be created and more precise corresponding controllers can be developed. Better understanding and modelling of vehicle dynamics are key parameters to increase the role and reliability of simulations to decrease the real life testing.

Normal traffic test times of AV can be kept on a moderate level with extended and merged utilization of proving grounds and simulations. As a solution with a close cooperation of the newest test centers, dedicated to AV is to develop several test areas such as city zones, highways, rural roads and imaging in simulation environment. It gives the opportunity after the simulations to get real data from testing, which can be validated.

The testing ground is not only a place for a wide range of vehicles and traffic test scenarios for conventional, connected and automated vehicles but also their capabilities will cover prototype testing, and will be used for type-approval procedure developments and educational purposes. One of the potential utilization options will be the testing autonomous driving (i.e. SAE level) from a residential home to a metropolitan office together with self-driving parking (public domestic road, highway traffic, residential area, downtown environment with continuous transition) (Szalay 2016).

As part of the proving ground, a cyber security test center is also under development. As a member of the EU cyber security certification framework an evaluation center for cyber security criteria and requirements, so that it could be fed back to the testing and validation process. The new test center would enable promote/improve information sharing among industry actors, share best practices, enable separation and clarification of cyber security liability. It will be a complete vehicle testing and validation center for automotive cyber security functions, focusing not only on known–known but known–unknown and unknown–unknown vulnerabilities. It will have the capacity to develop dedicated penetration tests to address unknown vulnerabilities and potential new vulnerabilities.

Acknowledgements

The paper has been supported by the EU, co-financed by the European Social Fund EFOP-3.6.2-16-2017-00002.

Author contributions

Máté Zöldy, Zsolt Szalay and Viktor Tihanyi put together the main research path.

Máté Zöldy was responsible to collect the details of state of art homologation process and define the challenges of autonomous vehicles.

Zsolt Szalay presented the functional safety and together with Máté Zöldy the utilization of AI in safety critical environment.

Viktor Tihanyi was brought together the cyber security related main challenges of AV.

Based on the statement a joint effort of Máté Zöldy, Zsolt Szalay and Viktor Tihanyi was to define the proposed solutions.

Disclosure statement

Authors are not have any competing financial, professional, or personal interests from other parties.

References

Andreades, C.; Kendrick, J.; Poresky, C.; Peterson, P. 2017. *Cyber Security in Civilian Aviation: Insights for Advanced Nuclear Technologies*. UCBTH-17-001 Department of Nuclear Engineering, University of California, Berkeley, US. 10 p. Available from Internet: http://fhr.nuc.berkeley.edu/wp-content/uploads/2017/04/UCB-TH-17-001-Cybersecurity-in-Civilian-Aviation.pdf

Buttyán, L.; Szijj, A.; Szalay, Z. 2015. *Hacking Cars in the Style of Stuxnet*. https://doi.org/10.5446/18858

EC. 2020. The EU Cybersecurity Act. European Commission, Brussels, Belgium. Available from Internet: https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act

ECOSOC. 1968. *Convention on Road Traffic: Done at Vienna on 8 November 1968*. Economic and Social Council (ECOSOC), United Nations.

Edelstein, S. 2015. *Ford's New GT has More Lines of Code than a Boeing Jet Airliner*. Digital Trends, Designtechnica Corporation. Available from Internet: https://www.digitaltrends.com/cars/the-ford-gt-uses-more-lines-of-code-than-a-boeing-787

Esser, F.; Schindler, C. 2016. Assisted, automated and autonomous driving ("Triple A") for railway traffic, in *XVII Scientific-Expert Conference on Railways RAILCON'16*, 13–14 October 2012, Niš, Serbia, 17–20.

Fraszczyk, A.; Brown, P.; Duan, S. 2015. Public perception of driverless trains, *Urban Rail Transit* 1(2): 78–86. https://doi.org/10.1007/s40864-015-0019-4

GlobalAutoRegs. 2020. *WP.1 Agreement: 1968 Vienna Convention on Road Traffic*. Available from Internet: https://globalautoregs.com/rules/157-1968-vienna-convention-on-road-traffic

Godoy, J.; Pérez, J.; Onieva, E.; Villagrá, J.; Milanés, V.; Haber, R. 2015. A driverless vehicle demonstration on motorways and in urban environments, *Transport* 30(3): 253–263. https://doi.org/10.3846/16484142.2014.1003406

Goodfellow, I.; Bengio, Y.; Courville, A. 2016. *Deep Learning*. MIT Press. 800 p.

Grzywaczewski, A. 2017. *Training AI for Self-Driving Vehicles: the Challenge of Scale*. Available from Internet: https://devblogs.nvidia.com/training-self-driving-vehicles-challenge-scale

Hirz, M.; Walzel, B. 2018. Sensor and object recognition technologies for self-driving cars, *Computer-Aided Design and Applications* 15(4): 501–508. https://doi.org/10.1080/16864360.2017.1419638

ISO 26262. *Road Vehicles – Functional Safety*.

Koopman, P.; Wagner, M. 2016. Challenges in autonomous vehicle testing and validation, *SAE International Journal of Transportation Safety* 4(1): 15–24. https://doi.org/10.4271/2016-01-0128

Li, Z. R.; Chitturi, M. V.; Yu, L.; Bill, A. R.; Noyce, D. A. 2015. Sustainability effects of next-generation intersection control for autonomous vehicles, *Transport* 30(3): 342–352. https://doi.org/10.3846/16484142.2015.1080760

Martins, H. 2010. *Type Approval Homologation and Self Certification*. Ford Motor Company. 9 p. https://doi.org/10.13140/RG.2.2.31708.39041

Maurer, M.; Gerdes, J. C.; Lenz, B.; Winner, H. 2016. *Autonomous Driving: Technical, Legal and Social Aspects*. Springer. 706 p. https://doi.org/10.1007/978-3-662-48847-8

Pinchon, N.; Cassignol, O.; Nicolas, A.; Bernardin, F.; Leduc, P.; Tarel, J.-P.; Brémond, R.; Bercier, E.; Brunet, J. 2019. All-weather vision for automotive safety: which spectral band?, in J. Dubbert, B. Müller, G. Meyer (Eds.). *Advanced Microsystems for Automotive Applications 2018: Smart Systems for Clean, Safe and Shared Road Vehicles*, 11–12 September 2018, Berlin, Germany, 3–15. https://doi.org/10.1007/978-3-319-99762-9_1

Reschka, A. 2016. Safety concept for autonomous vehicles, in M. Maurer, J. C. Gerdes, B. Lenz, H. Winner (Eds.). *Autonomous Driving: Technical, Legal and Social Aspects*, 473–496. https://doi.org/10.1007/978-3-662-48847-8_23

Shabtai, A.; Moskovitch, R.; Elovici, Y.; Glezer, C. 2009. Detection of malicious code by applying machine learning classifiers on static features: a state-of-the-art survey, *Information Security Technical Report* 14(1): 16–29. https://doi.org/10.1016/j.istr.2009.03.003

Szalay, Z. 2016. Structure and architecture problems of autonomous road vehicle testing and validation, in *Proceedings of the 15th Mini Conference on Vehicle System Dynamics, Identification and Anomalies: VSDIA2016*, 7–9 November 2016, Budapest, Hungary, 229–236.

Szalay, Z.; Tettamanti, T.; Esztergár-Kiss, D.; Varga, I.; Bartolini, C. 2018. Development of a test track for driverless cars: vehicle design, track configuration, and liability considerations, *Periodica Polytechnica Transportation Engineering* 46(1): 29–35. https://doi.org/10.3311/PPtr.10753

Tettamanti, T.; Varga, I.; Szalay, Z. 2016. Impacts of autonomous cars from a traffic engineering perspective, *Periodica Polytechnica Transportation Engineering* 44(4): 244–250. https://doi.org/10.3311/PPtr.9464

Török, Á.; Pauer, G. 2018. Optimization of linear traffic distribution problem in terms of the road toll structure assuming an autonomous transportation system, *International Journal for Traffic and Transport Engineering* 8(1): 112–124. https://doi.org/10.7708/ijtte.2018.8(1).08

Trujillo, A.; Dunlop, C. 2016. *ISO 26262 Software Compliance with Parasoft: Achieving Functional Safety in the Automotive Industry*. Parasoft Corporation, Monrovia, CA, US, 11 p. Available from Internet: https://blog.parasoft.com/hs-fs/hub/69806/file-15282344-pdf/docs/iso_26262_software_compliance.pdf

Valasek, C.; Miller, C. 2014. *A Survey of Remote Automotive Attack Surfaces*. IOActive, Inc. 90 p. Available from Internet: https://ioactive.com/a-survey-of-remote-automotive-attack-surfaces

Wahlström, M.; Forster, D.; Karvonen, A.; Puustinen, R.; Saariluoma, P. 2019. Perspective-taking in anticipatory maritime navigation – implications for developing autonomous ships, in *18th Conference on Computer and IT Applications in the Maritime Industries COMPIT'19*, 25–27 March 2019, Tullamore, Ireland, 191–200.

Wang, M.; Cui, Y.; Wang, X.; Xiao, S.; Jiang, J. 2018. Machine learning for networking: workflow, advances and opportunities, *IEEE Network* 32(2): 92–99. https://doi.org/10.1109/MNET.2017.1700200

Zöldy, M. 2018. Investigation of autonomous vehicles fit into traditional type approval process, in *ICTTE 2018: International Conference on Traffic and Transport Engineering*, 27–28 September 2018, Belgrade, Serbia, 428–432.