International Journal of Technology 12(7) 1407-1416 (2021)
Received October 2021 / Revised December 2021 / Accepted December 2021

International Journal of Technology

http://ijtech.eng.ui.ac.id

Justification of an Integrated Approach to Ensuring Information Security of Unmanned Vehicles in Intelligent Transport Systems

Ivan Babkin[1*], Olga Pisareva[2], Andrey Starikovsky[2], Makhmudova Guljakhon[3], Yulia Anoshina[4]

[1]*Peter the Great St. Petersburg Polytechnic University, Polytechnicheskaia Street, 29, Saint Petersburg, 195251, Russia*
[2]*The State University of Management, Ryazanskiy Prospect, 99, Moscow, 109542, Russia*
[3]*National University of Uzbekistan named after Mirzo Ulugbek, 4 Universitetskaya Street, Tashkent, 100174, Uzbekistan*
[4]*Moscow State University of Technology and Management 117418, Russia, Moscow, Novocheremushkinskaya Street, 69*

Abstract. The economic and social infrastructure of countries is improving under the growing influence of digital transformation, within which unmanned transportation technologies are being developed. The increased risks involve the driverless vehicle control and interaction mechanism, which determines the significance of information security analysis and support in the automated traffic environment. The technical aspect is considered in terms of a conceptual approach to identifying a comprehensive threat model for evaluating the security of information communications on the "driverless vehicle–road infrastructure" technological platform. The organizational aspect embraces the requirements and objectives related to the designing of test sites that should address a range of problems that are concerned with the information security of automated vehicles. The legal aspect is seen from the perspective of building a national certification system for driverless cars and active elements of road infrastructure. This promising research area includes work in the field of technical solutions, technological standards, and organizational guidelines to ensure the information security of automated transport.

Keywords: Automated transport; Intelligent transport system; Information security; Threat model; Unmanned technology validation

1. Introduction

One significant effect of the digital transformation of the economy is the spread of connected and automated vehicles (CAVs), including automobiles. The transfer to 5G mobile communication and modernized solutions for 4G with the use of «Long Term Evolution» (LTE) communication protocols has created a single technological platform of information communication between CAVs and various elements of the external environment in an integral digital transport system called Vehicle-to-Everything (V2X), which is based on high-speed data exchange and artificial intelligence methods.

This is an important stage in the full deployment of intelligent transport systems (ITS) with automated vehicles and related road infrastructure (RI) in urbanized spaces. To form

*Corresponding author's email: ivan.babkin@spbstu.ru, Tel.: +007 -812- 534-73-31
doi: 10.14716/ijtech.v12i7.5399

a national ITS, a number of technical, organizational, and legal problems must be resolved so that the general safety of CAVs can meet the acceptable level. If the system is to be fully deployed, new transport vulnerability zones must appear together, along with a new traffic control and management system and active RI items.

The growing number of threats to the normal operation of CAVs means that it is essential to change the standards and requirements that regulate the creation and operation of driverless cars. The functional capabilities of automated vehicles can be implemented, primarily if the problems of information security (IS) are studied in the context of the digital environment of innovative technical solutions for automobiles, transport infrastructure, and information communications systems for traffic organization and management. Consequently, the core of the testing problem changes because IS is assessed when CAVs and ITS elements are validated and verified in the commissioning process. As of today, the evolution, state, and prospects of highly automated vehicles have been discussed by Maurer et al. (2016). In addition, the potential of digital technology has been analyzed by Leviäkangas (2013), Ilin et al. (2018), Bataev and Aleksandrova (2020), Ivankova et al. (2020), and Tashenova et al. (2020), while the technical aspects of testing the IS of CAVs have been covered by Berger (2010), Barus et al. (2016), and Childress et al. (2016). Some original technical solutions have been proposed by Russian scientists as well, including Chikrin et al. (2019), who introduced CAV positioning algorithms. The correlation between CAV technology's effectiveness and value and the analysis of CAVs' effects have been presented by Hassn et al. (2016) and Economic and Social Value of Autonomous Vehicles (2018). The safety problems associated with unmanned technologies have also been in the spotlight. The general approaches to this theme are specified in *Safety First* for Automated Driving: A White Paper (2019). The problems and methods of providing IS for CAVs in the ITS environment were presented by Cui and Sabaliauskaite (2017). The matters of risk assessment for digital technologies in cyberphysical systems have been discussed by Grishunin et al. (2020), and the concept of a CAV test site was validated and solutions to its planning were presented by Szalay et al. (2017).

However, the analysis of the state and results of the research area shows that no solutions have been found to the problems of comprehensive risk analysis for the entire range of information communications of CAVs in ITS. The purpose of our work is to determine a system approach to providing IS for CAVs that would combine technological, organizational, and legal aspects in organizing and regulating the process of their design, development, creation, introduction, and operation. The research study implies building a structural risk model for CAV IS for the further development of risk assessment methods and the creation of testing tools for protecting the information communications of CAVs.

2. Methods

To achieve the goal and objectives of the research study, a set of content, comparison, logic, and system analysis methods must be applied for: (1) studying the national and global practice of developing and introducing CAV technology; (2) generalizing the legal regulation experience in the IS of CAVs; and (3) characterizing the testing schemes for the IS of the CAV-ITS technological platform. The sources of information include scientific publications, analytical materials from research centers for developing ITS technology and equipment, legal documents and statistics on CAV development, testing, and an introduction to IS. The work resulted from: (1) an analysis of the state and trends of autonomous automobile traffic projects within national and intercountry strategic initiatives in this field; (2) an evaluation of the general range of research studies currently carried out in the area of automated automobile traffic; and (3) the characteristics of approaches and solutions to testing automated vehicle systems given the IS of the V2X technological platform and the progress of information communication technology and intelligent RI elements.

3. Results

At the Global Forum for Road Traffic Safety (2018), the UN Economic Commission for Europe adopted a Resolution on the Deployment of Highly and Fully Automated Vehicles. It documented a new status for autonomous vehicles in road traffic and opened a new stage of ITS development. Fundamental and applied research and development in the field of unmanned transport are ongoing, but the objectives of introducing unmanned technologies in road traffic are becoming increasingly important. Technical and technological solutions for CAVs and ITS are being developed by the world's leading carmakers: China, the United States, Japan, Germany, and South Korea. However, according to a study carried out by KPMG International in 2019, only the United States was among the top five best prepared for introducing driverless vehicle technologies (see Table 1). This can be explained by a comprehensive assessment of the factors that are crucial for the success of CAV and ITS development and deployment projects.

Table 1 Leaders in the ranking of countries given the Autonomous Vehicles Readiness Index (AVRI)

Overall ranking	Country	Technology and innovations	Policy and legislation	Infrastructure	Consumer acceptance
1	Netherlands	10	5	1	2
2	Singapore	15	1	2	1
3	Norway	2	7	7	3
4	USA	3	9	8	6
5	Sweden	6	10	6	4

Source: Developed by the authors based on Threlfall (2019)

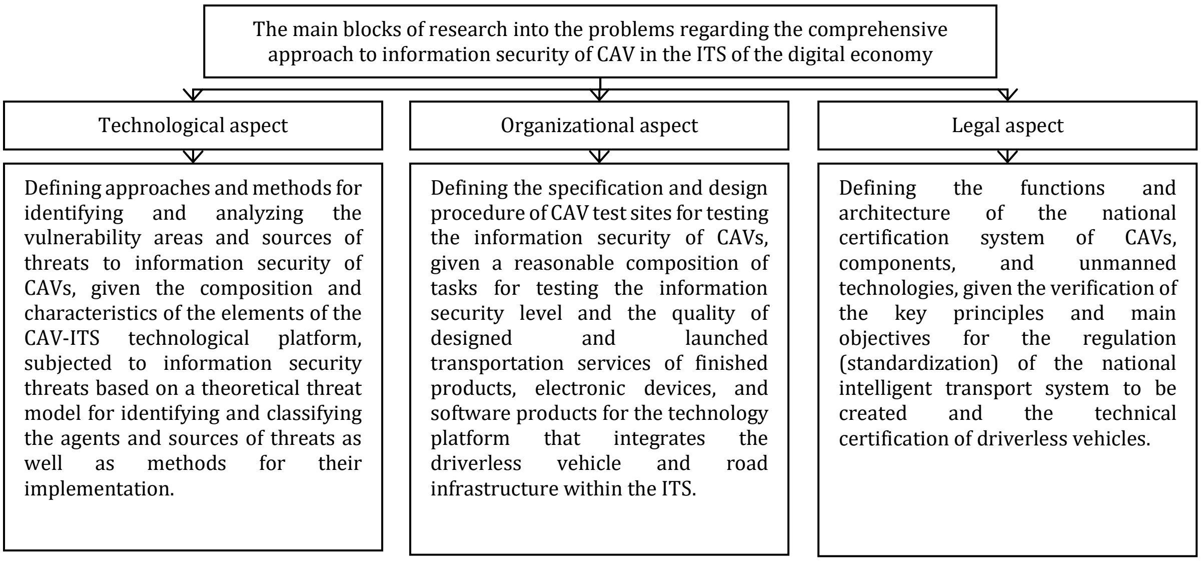
According to the analysis, there are some areas that contribute to the introduction of autonomous vehicles. They have the following characteristics: (1) *innovations* determine the state of the scientific, engineering, and manufacturing basis for developing and implementing a wide range of unmanned transport innovations; (2) *infrastructure* determines the state of the transport infrastructure for using the connected and automated transport (CAT); (3) *institutions* determine the state of the legislation regulating and encouraging the development, testing, implementation, and operation of CAVs and ITS; and (4) *consumers* define how unmanned technologies and CAVs are perceived by society in view of the dominance of the principle of public benefit, while safety and security (including IS) dictate technical and organizational solutions for adapting the functional and economic parameters of CAVs. A significant factor in introducing CAVs is the qualification aspect. Unmanned technologies are becoming increasingly dependent on a skilled workforce. Thus, additional staff training and development are important for manufacturers and operators of CAVs.

KPMG International ranked the Russian Federation, one of the top 10 carmakers in 2020, as 22nd out of 25 countries using the AVRI index. Russia has a good starting position for creating a national ITS. The government of the country clearly understands the importance of digital technologies, wireless communications, robotic systems, and artificial intelligence methods for increasing the competitiveness and efficiency of the national economy. According to Order No. 3821 issued on July 22, 2011, by the Gosstandart of Russia, a technical committee called TK 57, Intelligent Transport Systems, was set up and authorized to control the standardization of unmanned transport to be designed and commissioned. Unmanned technologies are also tackled in national projects, such as Digital Economy and Safe and Quality Roads, as well as in the state programs Information Society, Development of the Transport System, and Science and Technology in the Russian Federation. The administrative, financial, and legal support of unmanned technologies provided by the state has a significant impact on the pace and scale of strategic initiatives taking place in this field.

The growing use of driverless vehicles involves the need to ensure their safety, including protected information interaction between CAVs, road users, RI elements, traffic management centers, and the logistics control centers of the owners/operators of automated vehicles. For this reason, additional research must be carried out to analyze and tackle a number of problems in related areas, as illustrated in Figure 1.

Due to the transition to 5G mobile communications, driverless cars, road users, and active RI elements should be able to exchange digital information at a high speed. Thus, for their information interaction in the V2X environment, a single technological platform must be created, while artificial intelligence needs to be applied in the electronic complexes of automated driving and traffic management for the rapid analysis of data about all road users and the external environment. The interconnectivity of mobile systems would enable the use of this new computing environment for processing big data and controlling traffic in real time, which would optimize power consumption and create associated benefits. This is a critical step in the widespread deployment of ITS with automated driving objects and connected RI.

However, it is essential that CAVs are safe as they integrate into public, commercial, and personal transportation processes. Also, we must handle the problem of cyber security for CAT.



The main blocks of research into the problems regarding the comprehensive approach to information security of CAV in the ITS of the digital economy

Technological aspect

Defining approaches and methods for identifying and analyzing the vulnerability areas and sources of threats to information security of CAVs, given the composition and characteristics of the elements of the CAV-ITS technological platform, subjected to information security threats based on a theoretical threat model for identifying and classifying the agents and sources of threats as well as methods for their implementation.

Organizational aspect

Defining the specification and design procedure of CAV test sites for testing the information security of CAVs, given a reasonable composition of tasks for testing the information security level and the quality of designed and launched transportation services of finished products, electronic devices, and software products for the technology platform that integrates the driverless vehicle and road infrastructure within the ITS.

Legal aspect

Defining the functions and architecture of the national certification system of CAVs, components, and unmanned technologies, given the verification of the key principles and main objectives for the regulation (standardization) of the national intelligent transport system to be created and the technical certification of driverless vehicles.

Figure 1 Areas of comprehensive IS of CAVs
Source: Developed by the authors.

According to the general structure of the model of cyberphysical systems presented, for example, in Li et al. (2016), it is possible to identify the elements in CAVs and active RI elements in the ITS environment that are most vulnerable to attack and to determine the methods of cyberattacks. A vulnerability analysis of CAVs with different levels of automation was conducted by Checkoway et al. (2011), where a typology of remote attacks was proposed depending on: (1) information impact zones; (2) cyberphysical specifics of the vehicle design; and (3) the network architecture of the information communications in the ITS. Miller and Valasek (2014) highlighted the categories of remote attacks based on the analysis of the features of representative models of vehicles with AD functions. There has been a clear upward trend of potential attack vectors for the latest CAV technologies. This shows evidence of the need for additional research into the security of the V2X platform that would rely on effective means of protection against threats posed by intentional and accidental negative impacts in the digital ITS environment. Algorithmic and technological solutions that consider the characteristics of perspective and expected methods for hacking the cyberphysical security loop of CAV systems were presented by Ivanov et al. (2018).

We believe that a proper CAV IS threat model should be formed by taking into account the specifics of the ITS network communications architecture. Figure 2 offers a variant of the reference architecture scheme of the V2X communication network based on 5G or LTE-V2X protocols. It uses the following designations: User Equipment (UE), subscriber equipment of communication network in the ITS; Evolved Universal Terrestrial Radio Access Network (E-UTRAN), enhanced wireless interface; V2X Control Function, a logical function used for actions related to the network configuration and management to provide the functioning of V2X; Home Subscriber Server (HSS), a subscriber data server network; and Mobility Management Entity (MME), a cellular network mobility management node. The channels of information interaction in the CAV-ITS technology platform are defined as follows: V1 is the communication channel between the V2X application and the V2X application server; V2 is the communication channel between the V2X application server and the V2X control function in the operator's network (the V2X application server can connect to V2X control functions belonging to multiple networks); V3 is the communication channel between the V2X-enabled UE and the V2X control function in the operator's network; V4 is the link between HSS and the V2X control function in the operator's network; V5 is the link between V2X applications; V is the link between V2X control functions; LTE-Uu is the link between V2X-enabled UE and E-UTRAN; and PC5 is the link between V2X-enabled UE for V2V, V2I and V2P services.

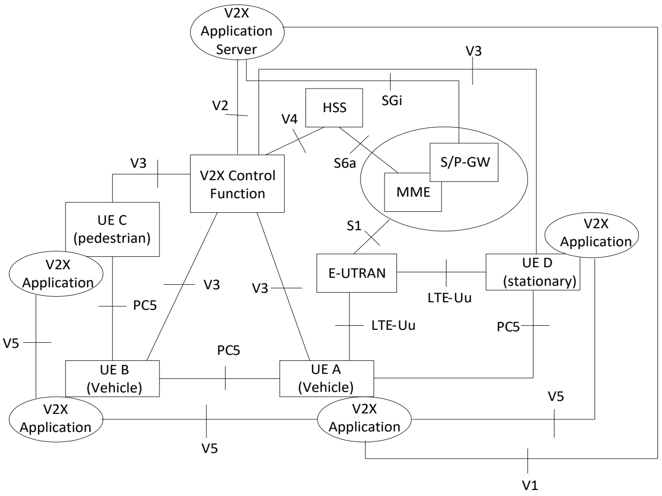


Figure 2 Possible reference architecture scheme of the V2X communication network (graphic elements on the ITS information and communication infrastructure diagram: oval – physical objects; rectangular – cybernetic objects)
Source: Compiled by the authors.

Communication between V2X system objects can be tampered with, reproduced, or intercepted by various actors if security risks occur during information interactions in ITS. The typology of offenders posing cybersecurity threats to CAVs, including the characteristics of the methods and motives of malicious actions, determines the possible approaches to building a threat model and choosing a method for assessing attacks for autonomous driving systems within the V2X platform. For example, Okuyama (2019) considered the range of possible external information impacts and the type of digital communication channels.

4. Discussion

The comprehensive model of threats presented by the authors and built on the basis of the structure of CAV information interaction channels, invariant to the ITS architecture, predetermines the methods to be developed for assessing the risks to the IS of CAVs and the formation of the structure and mechanism for testing unmanned transport and intelligent RI elements. IS technologies and AD control devices should be evaluated experimentally when different conditions of CAV operation are reproduced, together with a range of threats of accidental and intentional violation of the IS loop. Laboratories and test sites should be used to simulate different weather conditions and various states of road network infrastructure in order to build the road network and organize the surrounding landscape. The application of quantitative metrics for evaluating the testbed structure has been discussed by Chen et al. (2019). Recommendations for using subjective criteria for assessing the performance of test sites can be found in Szalay et al. (2018). The literature analysis showed that there is no single approach to designing test sites for evaluating the IS of CAVs. Tools for assessing and testing CAVs are created according to the V-shaped model and the ITS safety testing and analysis procedure discussed by Schmittner et al. (2014). The approaches proposed by, for example, Okuyama (2019) show that it is important to proceed from a fixed composition of active threats of deliberate violation of the IS loop of CAVs when building the testing model and validating the testing methodology. Summarizing the reviewed materials (see, e.g., Huang et al., 2016, and Joerger et al., 2019), it should be noted that, in order to analyze the IS of the V2X platform, the test site structure must be suitable for testing and include the following: (1) the general architecture of the driverless vehicle; and (2) the hardware and software of the AD system. The correct model of threats to the IS of CAVs that is based on the above scheme of wireless communication channels can be used to validate organizational decisions: (1) to create test sites for testing the protection of information and communication systems in the ITS; and (2) to form a national system of mandatory certification of the IS of CAVs.

Mass launching of a CAV fleet into the transportation services market means that there should be state certification procedures for driverless vehicles and components of unmanned technologies. The certification should be aimed at determining the degree of compliance of the V2X technology platform of an unmanned vehicle with the requirements of the national IS standard. Figure 3 presents the structure of the tasks related to the testing and certification of the IS of CAVs based on the mechanism of the interaction of the vehicle with the physical and cyberphysical infrastructure.

Verifying that an intelligent vehicle meets the IS requirements of the CAV-RI platform is a multilevel and multistage process (Pisareva et al., 2021). State control of CAV technology safety should use testing strategies that focus on the entire automatic driving system. The aims and functions of certification define the structure of the certification system to include the following: a state CAV certification body, authorized certifying organizations, and authorized testing laboratories. The objectives and methods of certification determine the verification mechanism—the testing scheme must envisage both sanctioned and periodic inspection controls.

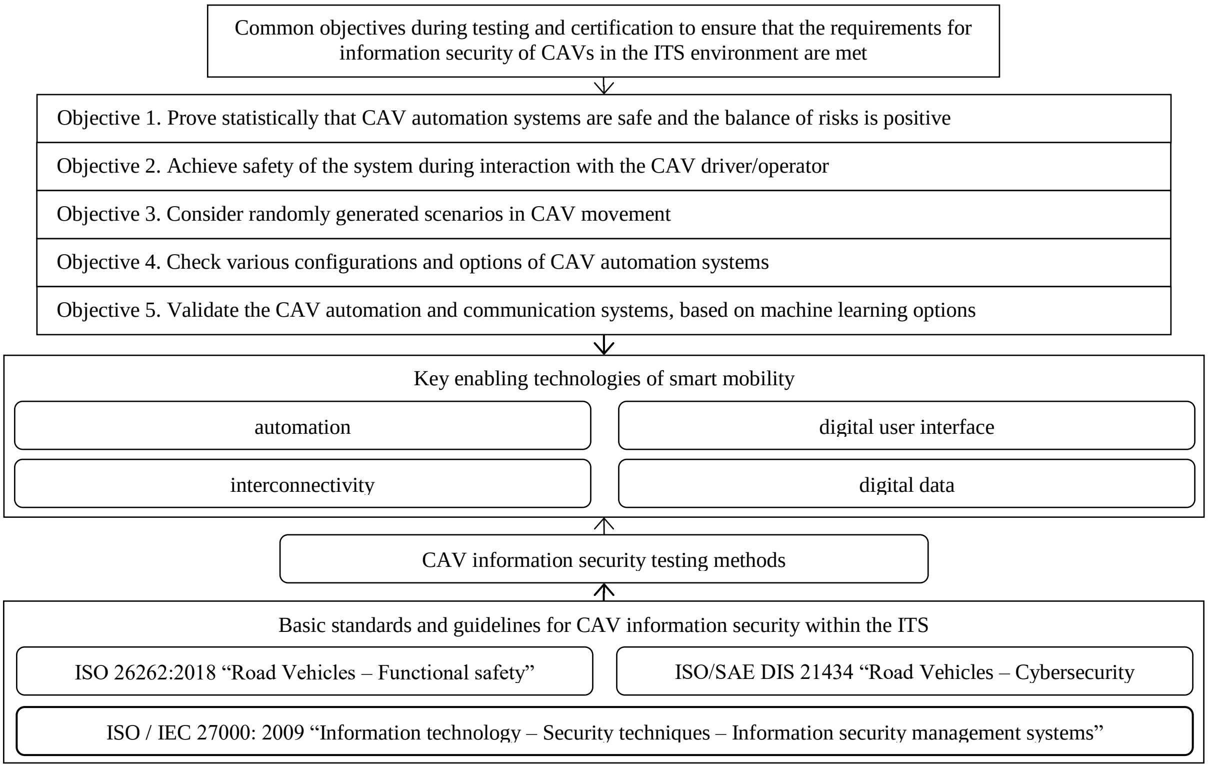

Common objectives during testing and certification to ensure that the requirements for information security of CAVs in the ITS environment are met
Objective 1. Prove statistically that CAV automation systems are safe and the balance of risks is positive
Objective 2. Achieve safety of the system during interaction with the CAV driver/operator
Objective 3. Consider randomly generated scenarios in CAV movement
Objective 4. Check various configurations and options of CAV automation systems
Objective 5. Validate the CAV automation and communication systems, based on machine learning options
Key enabling technologies of smart mobility
automation
digital user interface
interconnectivity
digital data
CAV information security testing methods
Basic standards and guidelines for CAV information security within the ITS
ISO 26262:2018 “Road Vehicles – Functional safety”
ISO/SAE DIS 21434 “Road Vehicles – Cybersecurity
ISO / IEC 27000: 2009 “Information technology – Security techniques – Information security management systems”

Figure 3 Areas for ensuring comprehensive IS of CAVs
Source: Developed by the authors.

The basic principle of the certification system and certification tests is the independence of the testing laboratory and that of the certifying organization controlling the results obtained by the testing laboratory. The state certification body should conduct regular external audits of the activities of the certifying organization and testing laboratories and should assess the completeness and quality of functions performed by them. From our point of view, the scope of work on creating a CAV certification system within the ITS should cover the following areas: improving the legislative framework for verification and validation of ITS systems and technologies; forming a functional state certification body and its territorial infrastructure; creating a mechanism for licensing, accreditation, and certification of the participants in the testing process; and organizing the design, development, and production of hardware and software packages for test platforms to assess the level of IS of CAV technologies in the V2X environment. According to Article 25 of Russia’s Federal Law “On Technical Regulation” No.184-FZ, dated December, 27, 2002, in order to certify driverless vehicles and ITS technologies, the equipment used and the services provided are included in the Unified List of Products and are subject to mandatory certification. The technological operation guidelines should define the necessity of compulsory confirmation of compliance with established safety requirements and quality characteristics. It is vital to ensure cooperation between departments and organizations in the field of CAV standardization. Given the specifics of the objective related to assessing the information vulnerabilities within the CAV-RI technology platform, it is necessary to choose the form of cooperation between the Federal Service for Supervision of Transport and the State Traffic Safety Inspectorate with government bodies authorized in the field of information protection.

This research study made it possible to substantiate the key provisions of the conceptual approach to ensuring the IS of the “driverless vehicle–road infrastructure” technological platform based on a comprehensive threat model that considers the structure and characteristics of information interaction channels in the digital environment of the ITS. This contributes to the harmonization of regulatory requirements and objectives concerning the test sites to be used for testing the IS of unmanned technologies, as well as for building a national certification system of the IS for CAVs and active elements of RI.

5. Conclusions

The top priority of the implementation stage of unmanned transport is to ensure the security of the CAV technology platform. This unlocks the potential of CAVs, reduces total costs, and results in additional effects due not only to the optimization of traffic routes, the control of fuel consumption, and the lessened impact on the environment but also to the decrease in accidents and reduction of financial losses. The study shows that, given the CAV design and ITS architecture, the overall safety level of unmanned transport cannot be improved unless IS objectives are achieved. Thus, according to the purpose of the study, the work proposes a comprehensive approach to ensuring the IS of CAVs based on the end-to-end use of the threat model in the process of development, testing, and certification and to taking into account various aspects related to the construction of the ITS. In the course of solving the tasks that had been set, the following scientific results were obtained: (1) the areas, factors, and conditions that contribute to the successful introduction of autonomous vehicles were identified; (2) the technological, organizational, and legal aspects were identified and specified for the comprehensive approach to solving the problem of IS of CAVs when a national ITS is created in the digital economy; (3) based on the architecture of information interaction in the ITS presented by the authors, a comprehensive threat model was formed to predetermine the elaboration of the risk profile for the IS of CAVs; (4) the specification and development of a CAV testing site was carried out to supplement the security testing tasks and check how reliable the protection of the V2Xtechnological platform is; and (5) the composition of objectives and schemes was determined for building a national certification system for the IS of CAVs and RI elements in the ITS environment.

Further research in this area should be dedicated to the system of national standards for the ITS and methods for testing CAVs. This involves the assimilation of national and international requirements not only to ensure CAV safety, but also to comply with the principles of interoperability and multimodality of CAV devices and technologies for the “seamless” building of global transport corridors to be used for various types of transportation.

Acknowledgements

The research is partially funded by the Ministry of Science and Higher Education of the Russian Federation under the strategic academic leadership program Priority 2030 (Agreement 075-15-2021-1333 dated 30.09.2021).

References

Barus, L.S., Flores, H.M., Hadiwardoyo, S.P., Batoz, J.L., 2016. Intercity Mode Choice Modelling: Considering the Intracity Transport Systems with Application to the Jakarta-Bandung Corridor. *International Journal of Technology*, Volume 7(4), pp. 581–591

Bataev, A.V., Aleksandrova, A.I., 2020. Digitalization of the World Economy: Performance

Evaluation of Introducing Cyber-Physical Systems. *In:* The 9th International Conference on Industrial Technology and Management, ICITM 2020, pp. 265–269

Berger, C., 2010. *Automating Acceptance Tests for Sensor- and Actuator-based Systems on the Example of Autonomous Vehicles*. Shaker Verlag, Aachener Informatik-Berichte, Software Engineering, Aachen, Germany

Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H., Savage S., Koscher, K., Czeskis, A., Roesner, F., Kohno, T., 2011. Comprehensive Experimental Analyses of Automotive Attack Surfaces. *In:* The Proceedings of the 20th USENIX Conference on Security (SEC'11). USENIX Association, Berkeley, CA, USA

Chen R., Arief M., Zhang W., Zhao D., 2019. How to Evaluate Proving Grounds for Self-Driving? A Quantitative Approach. *arXiv preprint*, arXiv: 1903.08352. Available Online at https://arxiv.org/pdf/1909.09079.pdf, Accessed on July 14, 2021

Chikrin, D.E., Savenkov, P.A., Shagiev, R.I., 2019. The Integrated Systems of High-Tech Satellite-Local-Inertial Navigation in the Problems of Unmanned Vehicle Control. *Nanoindustry*, Volume 89(5), pp. 49–56

Childress, S., Nichols, B., Charlton, B., Coe, S., 2016. Using an Activity-Based Model to Explore Possible Impacts of Automated Vehicles. *Journal of the Transportation Research Board*, Volume 2493(1), pp. 99–106

Cui J., Sabaliauskaite G., 2017. On the Alignment of Safety and Security for Autonomous Vehicles. *In:* Proceedings of IARIA CYBER, Barcelona, Spain, November, pp. 1–6

Economic and Social Value of Autonomous Vehicles, 2018. Compass Transportation and Technology, Inc., Stackhouse, USA. 58 p. Available Online at URL: https://avworkforce.secureenergy.org/wp-content/uploads/2018/06/Compass-Transportation-Report-June-2018.pdf

Grishunin, S., Suloeva, S., Burova, E., 2020. Developing a Mechanism for Assessing Cyber Risks in Digital Technology Projects Implemented in an Industrial Enterprise. *Communications in Computer and Information Science*, Volume 1273, pp. 3–18

Hassn, H.A.H., Ismail, A., Borhan, M.N., Syamsunur, D., 2016. The Impact of Intelligent Transport System Quality: Drivers' Acceptance Perspective. *International Journal of Technology*, Volume 7(4), pp. 553–561

Huang, W., Wang, K., Lv, Y., Zhu, F., 2016. Autonomous Vehicles Testing Methods Review. *In:* IEEE 19th International Conference on Intelligent Transportation Systems, pp. 163–198

Ilin, I.V., Iliashenko, O.Y., Klimin, A.I., Makov, K.M., 2018. Big Data Processing in Russian Transport Industry. *In:* Proceedings of the 31st International Business Information Management Association Conference, pp. 1967–1971

Ivankova, G.V., Mochalina, E.P., Goncharova, N.L., 2020. Internet of Things (IoT) in logistics. *IOP Conference Series: Materials Science and Engineering*, Volume 940(1), pp. 1–7

Ivanov, M.A., Roslyj, E.B., Starikovskiy, A.V., Krasnikova, S.A., Shevchenko, N.A., Shustova, L.I., 2018. Non-Binary Pseudorandom Number Generators for Information Security Purposes. *In*: 8th Annual International Conference on Biologically Inspired Cognitive Architectures, BICA 2017, *Procedia Computer Science*, Volume 123, pp. 203–211

Joerger, M., Jones, C., Shuman, V., 2019. Testing Connected and Automated Vehicles (CAVs): Accelerating Innovation, Integration, Deployment and Sharing Results. *In*: Road Vehicles Automation, Volume 5, Meyer, G., Beiker, S., Shpringer (eds.), pp. 197–206

Leviäkangas, P., 2013. Intelligent Transport Systems-Technological, Economic, System Performance and Market Views. *International Journal of Technology*, Volume 4(3), pp. 288–298

Li, L., Huang, W., Liu, Y., Zheng, N., Wang, F., 2016. Intelligence Testing for Autonomous

Vehicles: A New Approach. *IEEE Transactions on Intelligent Vehicles*, Volume 1(2), pp. 158–166

Miller, C., Valasek, C., 2014. *A Survey of Remote Automotive Attack Surfaces*, Black Hat, USA

Maurer, M., Gerdes, J., Lenz, B., Winner, H., (eds.), 2016. *Autonomous Driving: Technical, Legal and Social Aspects*, Springer, Berlin, Germany

Okuyama, K., 2019. Formulation of a Comprehensive Threat Model for Automated Driving Systems Including External Vehicular Attacks such as V2X and the Establishment of an Attack Evaluation Method through Telecommunication. *In:* SIP-adus: Project Reports, 2014–2018— Automated Driving for Universal Services. Publisher's Office Cabinet Office, Japan, pp. 77–83

Pisareva, O.M., Alexeev, V.A., Mednikov, D.N., Starikovsky, A.V., Kurguzov, V.B., 2021. Creating a National Certification System for Unmanned Vehicles: Tasks of Information Security Testing. *St. Petersburg State Polytechnical University Journal. Economics*, Volume 14(2), pp. 63–80

Safety First for Automated Driving: A White Paper, 2019. Aptiv Services US, LLC; AUDI AG; Bayrische Motoren Werke AG; Beijing Baidu Netcom Science Technology Co., Ltd; Continental Teves AG & Co oHG; Daimler AG; FCA US LLC; HERE Global B.V.; Infineon Technologies AG; Intel; Volkswagen AG

Schmittner, C., Ma, Z., Gruber, T., 2014. Standardization Challenges for Safety and Security of Connected, Automated and Intelligent Vehicles. *In:* The 3rd International Conference on Connected Vehicles & Expo (ICCVE 2014), pp. 941–942

Szalay, Z., Nyerges, A., Hamar, Z., Hesz, M., 2017. Technical Specification Methodology for an Automotive Proving Ground Dedicated to Connected and Automated Vehicles. *Periodica Polytechnica Transportation Engineering*, Volume 45(3), pp. 168–174

Szalay, Z., Tettamanti, T., Esztergar-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*, Volume 46(1), pp. 29–35

Tashenova, L., Babkin, A., Mamrayeva, D., Babkin, I., 2020. Method for Evaluating the Digital Potential of a Backbone Innovative Active Industrial Cluster. *International Journal of Technology*, Volume 11(8), pp. 1499–1508

Threlfall R., 2019. *Autonomous Vehicles Readiness Index*, KPMG International. Amstelveen, Netherlands Available Online at https://assets.kpmg/content/dam/kpmg/xx/pdf/2019/02/2019-autonomous-vehicles-readiness-index.pdf