Organizational Aspects of Ensuring Information Security in the Framework of Creating an Intelligent Transport System in the Russian Federation

O M Pisareva\textsuperscript{1} and V A Alexeev\textsuperscript{2}

\textsuperscript{1}State University of Management, Moscow, Russia
\textsuperscript{2}RABUS (LLC), Moscow, Russia

E-mail: om_pisareva@guu.ru, vaalexeev@gmail.com

Abstract. Unmanned vehicle technology is the innovation that qualitatively transform the economic and social landscape of the modern state based on the concept of smart mobility. The widespread introduction of highly automated vehicles leads to additional risks that affect the level of quality and safety of functioning of many areas of public life. The increasing autonomy of unmanned vehicles and other vehicles causes a significant load on the infrastructure of communication networks of various types and creates new threats to the information security of cyberphysical systems. In this regard, the article addresses the issues of assessing and ensuring the security of information interaction between connected and autonomous cars with road infrastructure. The authors determine the requirements for the specification of the test site for testing unmanned vehicles taking into account the sources of threats and zones of vulnerability. The approaches to the design of landfills for testing unmanned vehicles existing in the world are described. Based on this, a possible scheme of the process of development and implementation of the test site project for testing the security of information interaction of the V2X technology platform in the Russian Federation is proposed. Recommendations are formulated on improving the regulatory system and certification of created systems and technologies for the information interaction of highly automated vehicles with road infrastructure. Recommendations are formulated on improving the regulatory system and certification of created systems and technologies for the information interaction of highly automated vehicles with road infrastructure.

1. Introduction: relevance of the study First Section

The creation of a national intellectual transport system and the development of unmanned automobile transport (public, commercial and state) is an important direction in the development of the digital economy in the Russian Federation (RF). As part of the work of the Supervisory Board of the Agency for Strategic Initiatives (September 18, 2019), the President of the Russian Federation V.V. Putin noted that new technologies have appeared that will change and are already changing our world. He highlighted artificial intelligence and unmanned vehicles among the ones. Under these conditions, the information security of the technological platform for the interaction of highly automated vehicles with road infrastructure is one of the key aspects in the large-scale spread of unmanned automobile traffic in Russia. An analysis of the organizational aspects of constructing landfills for testing the cybersecurity systems of unmanned vehicles, as well as the accumulated positive experience in this area, will
improve the organizational and methodological support of the substantiation of government programs and commercial projects for the development of unmanned technologies in the Russian Federation.

2. Background and purpose of the study

Information and communication technologies (ICT) are transforming the economic and social landscape of states. Against this background, specialists identify significant miscalculations in the work of digital technologies related to the development of the infrastructure of data transmission systems and ensuring information security. They are not yet designed for peak loads and large-scale protection of legally significant transactions. Moreover, a proliferation of unmanned technologies imposes additional requirements on the quality of information and communication solutions for processing and protecting large volumes of personalized data from owners, operators and users of the connected and automated vehicles (CAV) in an intelligent transport system (ITS) environment.

Efficient and reliable operation of highly automated vehicles for public and personal, state and commercial purposes depends on the security of unmanned logistics services. Given the hardware-software and information-analytical basis for the construction of ITS, maintaining reliability and reducing the risks of unmanned vehicles is associated primarily with the solution of cybersecurity problems [1]. The key point for ITS is to ensure the information security of the interaction of an unmanned vehicle with road infrastructure and other road users on various roads. To organize the implementation of ITS elements in the Russian Federation, it is important to evaluate:

- existing approaches to ensuring the security of CAV information interaction with ITS elements (technology platform - Vehicle-to-Everything, V2X);
- the current state of development in the design and creation of test sites for the comprehensive testing of methods and means of ensuring the safety of unmanned vehicles in various modes (conditions) of its operation.

3. Review of scientific publications and research

Research and development in the field of creating technologies for land, air and water unmanned vehicles have been conducted in the world for quite some time [2], [3]. Russian scientists, designers and engineers have their own original technical solutions [4], [5]. Technical, informational, technological aspects of the design and development of unmanned vehicles are described in [6], [7]. The legal, organizational, economic aspects of building the infrastructure of general and special roads for the operation of CAV are considered in [8, 9]. Tasks and methods for ensuring information security of CAV and ITS are presented in [10], [11], [12], [13]. A number of research studies analyze the vulnerability of models of transport systems with various levels of automation [14], for which a typology of remote attacks is determined depending on three categories of characteristics of unmanned vehicles: a zone for remote attack; cyber-physical features of the vehicle; network architecture used. In particular, in [15], seven main categories of remote attacks based on the analysis of the characteristics of 20 vehicle models were identified. This study identified an obvious upward trend in potential attack vectors for newer models of vehicles with Connected Automated Driving (CAD) technologies. The study [16] suggests a possible approach to building an integrated threat model for automated driving systems (including external attacks within the framework of the V2X platform) and to developing a method for assessing attacks through various telecommunication channels. This study summarized the first results of the SIP ADUS project in Japan based on a combination of clustering methods, statistical analysis and fuzzy sets (for structuring and identifying the level of threats in the nominal scale). However, you can find certain recommendations [17] on the use of subjective criteria for assessing the effectiveness of a test site (at the stages of its design and creation) based on a targeted collective discussion with the participation of representatives of academia, business and government officials. In [18], it is proposed to proceed with the development of the concept, layout, and specification of the test site from the generalized characteristics of many key traffic situations under various scenarios of unmanned vehicle operation in various weather conditions and behavior patterns of drivers of conventional vehicles. An attempt to apply quantitative metrics to assess various characteristics of a test site and verify the struc-
ture of its roads is presented in [19]. As a rule, it is proposed to use a non-parametric Bayesian training method based on experimental data sets with selective optimization to assess the compatibility of characteristics between different basic traffic scenarios. Most authors propose a general approach based on the description of typical cases of CAV operation and real-life driving events.

An additional empirical basis for the work was a wide range of various sources: regulatory legal and strategic planning documents, statistical data, scientific and specialized publications, reference and methodological materials of international organizations, including data from UN Internet sites (http://www.un.org), EAEU (http://www.eaeunion.org/), OECD (http://www.oecd.org), etc., reports on national and international scientific, practical and expert events. When studying the state and results of research in the subject area, the authors applied methods of content and semantic, logical and statistical, as well as comparative and expert analysis.

4. Research methodology and its results

On the one hand, large-scale automation is aimed at reducing risks during transportation; on the other hand, digitalization of cars and road infrastructure through the emergence of new zones of vulnerability of a combination of interacting cyber-physical systems leads to increased risks of autonomous (automated) the movement of vehicles. Therefore, the development of CAV-technologies needs to assess the consequences of use. This requires a comprehensive analysis of the structure of interconnections in the cyber-physical systems of intelligent automobile transport. With the transition to the next generation (5G) mobile communication protocols and devices, it became possible to create a single technological platform for high-speed electronic data exchange and the application of artificial intelligence methods in a common digital environment between a car and various elements. This is implemented in a holistic intelligent transport system with the support of dynamic communications for a complex of hardware and software solutions - V2X.

Under these conditions, it is necessary to intensify coordinated and comprehensive work in the field of technical regulation and support of innovative projects for the development of information technology solutions for Russian CAV prototypes. The synthesis of the best ideas, practices and technologies allows minimizing the costs and disadvantages of the experimental period for the development of ITS elements and infrastructure. In our opinion, the most representative and useful for analysis are official regulatory materials for planning the development of unmanned vehicles in the countries of the European Union, USA, China, Japan, South Korea and Singapore. The Table 1 provides a summary of initiatives in the field of unmanned automobile traffic and its safety. In each of the strategic decisions considered, issues of ensuring the safety of unmanned vehicles are given priority.

A review of possible approaches to the analysis of the reliability problems of CAV operation and the construction of the conceptual framework for ensuring information security in the ITS environment is presented in [20], [21]. The recommendations suggest structuring the task of ensuring information security of the V2X technology platform as part of the description of the strategic model of cyber-physical systems and vehicle infrastructure. The mechanism of interaction of an autonomous vehicle with physical and cyber-physical infrastructure is formed by the integrated use of technologies of intellectual mobility (Key Enabling Technologies of smart mobility): Automation; Digital user interface; Interconnectivity; Digital data. The reliability assessment of the V2X technological platform is associated with studies of the possibilities and consequences of the impact on the specified functional zones of automating the operation of automobile transport of threats from various sources and for various purposes. An analysis of the general practice of developing and testing CAV shows experts associate the main prospects for the construction and operation of national intelligent transport systems and international transport corridors with V2X platforms as part of the development of cellular network infrastructure new generation – 5G. At the same time, the creation of an effective ITS will require the use of a complex of communication technologies.

Testing the information security of unmanned vehicles, is carried out in two stages: 1) experiments with testing threats of accidental and intentional violation of the CAV information protection circuit in specialized laboratories; 2) reliability checks at test sites with the reproduction of various sections of
the road network and the surrounding urban and natural landscape.

Table 1. Information on national initiatives in the field of unmanned automobile traffic and its safety

| Country    | Base document                                                                 | Aspect / area of best practice                                                                 |
|------------|-------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|
| EU         | The European Union strategy on connected and automated mobility                | Structured and coherence of ITS strategic development initiatives                             |
| USA        | Intelligent Transportation System Strategic Plan 2015-2019                    | The breadth of planned changes and innovative solutions of the Society of Automotive Engineers, SAE, and The National Highway Traffic Safety Administration, NHTSA for standardizing unmanned vehicles, including the safety field |
| China      | The SAE China’s technology roadmap for energy-saving and new energy vehicles   | Proximity of initial development conditions and relative political accessibility of replicated unmanned transport technologies |
| Japan      | The Cross-ministerial Strategic Innovation Promotion Program: Automated Driving for Universal Services | Level of engineering, organizational and technological solutions for automating automobile traffic in an urbanized space |
| South Korea| The national master plan of the automotive industry development               | The pace of change and the degree of centralization of government decisions to mobilize and coordinate market participants for unmanned technologies and systems based on the National Strategy of the 4th Industrial Revolution |
| Singapore  | The Singapore autonomous vehicle initiative                                   | The complexity, compactness and completeness of the agreed solutions to approximate the “ideal” public image of ITS within the framework of the “Smart Mobility” project |

Our analysis of scientific publications and available informational materials showed that at present there is no uniform conceptual approach to the development of a test site design for CAV. This allows using optimization methods when designing a landfill using a limited number of road infrastructure elements to develop a reasonable judgment about the quality indicators of the tested specimens of intelligent vehicles for various purposes and the level of automation. In general one general situation can be distinguished: the starting point of the project development is to determine the main goal of the testing process, which should be decomposed according to the following key aspects of testing components and an automated driving system: operability and compatibility; reliability of operation; durability of operation; information security (cybersecurity); data integrity and privacy protection. The test site parameters and CAV test conditions should 1) take into account various problems when testing technologies, depending on the use cases, functions and selected levels of traffic automation; 2) reproduce deterministic or stochastic testing situations in a real or virtual environment; 3) provide the abil-
ity to test the automatic driving functions in a reproducible and effective way when solving the problems of state certification of CAV; 4) allow the assessment of liability and insure the risks of the owner/operator of the CAV.

In general, summarizing the provisions of [22], [23], [24], it can be noted that the specification of the landfill for assessing the information security of the V2X platform should include the ability to test the following components: general architecture of an autonomous vehicle; equipment of an automated driving system; software for automated driving systems. At the same time, testing should be carried out under conditions of simulation of threats both in the laboratory (Simulation Testing) and in motion (Driving Testing). In addition, the specification of the testing ground should provide testing of CAV vulnerabilities to evaluate the following functions: 1) perception; 2) decision making; 3) navigation; 4) action management. Regardless of the specific test methods, the CAV information security performance assessment process should include the following steps: defining Functional Testing Sets; substantiation of the composition and description of the design of testing procedures; preparation of simulation conditions and/or field tests; determination of the procedure for testing and accumulation of data of test results; determination of the processing and evaluation of test results; a description of the feedback mechanism and improvements to the testing procedures; formation of conclusions and recommendations.

The specification of the test site and the scheme of the testing process allow you to determine the time and cost parameters of the project development (composition and characteristics of the elements; composition and characteristics of equipment, composition and schedule, amount and structure of financing).

The information in Table 2 presents the organizational aspects of the design process of the test site (the notation used in the table are: IS - information security; WG# - working group (0 - Initiative group; 1 - Managing group; 2 - Expert group on IS; 3 - Transport Expert Group; 4 - Expert group on Infrastructure; 5 - Research Expert Group; 6 - Regulatory Expert Group; 7 - Construction Expert Group), Q# - quarter number).

### 5. Conclusions and recommendations

Summing up the preliminary results of the study, we can formulate the main conclusions.

1). Strategies for the development of CAV technologies and systems are integrated into the general logic of the development of national transport systems taking into account the intellectualization of infrastructure and services as well as determining priorities in the field of safe operation of highly automated vehicles.

| Table 2. Organizational aspects of the development and implementation of the design of proving ground for testing of the information interaction security of the V2X technology platform. |
|---|---|---|---|
| Stage (Work Content) | Development Object | Cast | Main result | Approximate period |
| 1 Initiating Designing an initiative structure, guidelines project | WG 0 | Project initiative | Q-0 |
| 2 Organizational Development plan and schedule of project Scope and characteristics of proving ground | WG 1 | Work schedule | Q-0 |
| 3 Predesign Draft and specification of proving: safety ground | WG 2 | Test goals and objects | Q-1 |
2). Creating a testing ground for assessing the state and substantiating information security measures of the “unmanned vehicle-road infrastructure” interaction system is a complex integrated project involving representatives of various parties: the state, business and science.

3) The successful implementation of the project depends on the correct determination of the goals of information security testing of the V2X technological platform and the differentiation of testing tasks for the specification of requirements for the landfill. Such tasks should be related to the implementation of the test plan for the individual functions of the automated driving system and CAV in a network communications environment.

4) It is necessary to synchronize the planning and implementation of the technical work of the project with the development of regulatory measures for the creation and operation of CAV.

5) The roadmap for creating a test site for assessing the information security of the V2X platform should be formed as a project for creating a specialized test site for laboratory and field tests in a lim-
ited area. It is necessary to provide for the possibility of virtual and real simulation of the road network and situations corresponding to the map and threat model for CAV communication.

6) The procedure and rules for testing information security of the V2X platform depend on the regulations for the use of the frequency spectrum by communication networks, which requires additional coordination of the frequency characteristics and parameters of the equipment used.

The recommendations presented may be useful in developing the concept and testing tools for the V2X technology platform.

6. References
[1] Cybersecurity Guidebook for Cyber-Physical Vehicle Systems SAE International http://standards.sae.org/j3061_201601/ last accessed 2020/06/21
[2] Autonomous Driving Technical, Legal and Social Aspects Eds. M Maurer, J Gerdes, B Lenz, H Winner (Springer, Berlin)
[3] Perspectives on the Use of New Information and Communication Technology (ICT) in the Modern Economy 2019 Springer International Publishing AG
[4] Nosov A G 2016 Economic and infrastructural aspects of the development of unmanned transport technologies Transport of the Russian Federation 5 21-25
[5] Kazanskaya L F, Savitskaya N V, Kamzol P P 2018 Prospects for the development of unmanned vehicles in Russia Bulletin of the results of scientific research 2 18-28
[6] Anderson J, Kalra N, Stanley K, Sorensen P, Samaras C, Oluwatola O 2016 Autonomous Vehicle Technology: A Guide for Policymakers (Rand Corporation, Santa Monica)
[7] Ivanov V V, Malinetskiy G G 2017 digital economy: myths, reality, perspective Russian Academy of Sciences (Moscow) (In Russ.)
[8] The Economic and Social Value of Autonomous Vehicles Compass Transportation and Technology, Inc. (Stackhouse)
[9] Clements L, Kockelman K 2017 Economic Effects of Automated Vehicles Transportation Research Record Journal of the Transportation Research Board 1 106-114
[10] Zhao D, Lam H, Peng H, Bao S, LeBlanc D, Nobukawa K, Pan C 2017 Accelerated Evaluation of Automated Vehicles Safety in Lane-Change Scenarios Based on Importance Sampling Techniques IEEE Trans. Intelligent Transportation Systems 18(3) 595-607
[11] Cui J, Sabaliauskaite G 2017 On the alignment of safety and security for autonomous vehicles In: Proceedings of the IARIA CYBER pp 1–6 (Barcelona)
[12] 2015 Digital Security in a Networked World (Wiley, Hoboken)
[13] Safety first for automated driving: a white paper 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 (2019)
[14] 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: Proceedings of the 20th USENIX conference on Security (SEC’11) pp 6–6 USENIX Association (Berkeley)
[15] Miller C, Valasek C 2014 A survey of remote automotive attack surfaces (Black Hat, USA)
[16] 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-ads: Project Reports Automated Driving for Universal Services pp 77-83 Publisher’s Office Cabinet Office (Government of Japan)
[17] 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 Polytechnical Transportation Engineering 46(1) 29–35
[18] Peng H 2019 MCity ABC Test: A Concept to Assess the Safety Performance of Highly Automated Vehicles University of Michigan, Ann Arbor
[19] 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 https://arxiv.org/pdf/1909.09079.pdf last accessed 2020/06/21
[20] Tokody D, Albini1 A, Ady L, Rajnai1 Z, Pongracz F 2018 Safety and Security through the Design of Autonomous Intelligent Vehicle Systems and Intelligent Infrastructure in the Smart City Interdisciplinary Description of Complex Systems 16(3-A) 384-396
[21] 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 45(3) 168-174
[22] Huang W, Wang K, Lv Y, Zhu F 2016 Autonomous Vehicles Testing Methods Review In: Proceedings of the IEEE 19th International Conference on Intelligent Transportation Systems pp 163-198 Rio de Janeiro https://www.researchgate.net/publication/311919670_Autonomous_vehicles_testing_methods_review last accessed 2020/06/21
[23] Joerger M, Jones C, Shuman V 2019 Testing connected and automated vehicles (CAVs): Accelerating innovation, integration, deployment and sharing results In Meyer G, Beiker S (eds.) Road vehicles Automation 5 pp 197-206 (Springer, Heidelberg)
[24] Huang W, Wen D, Geng J, Zheng N 2014 Task-specific performance evaluation of UGV’s: Case studies at the IVFC IEEE Transactions on Intelligent Transportation Systems 15(5) 1969-1979