Human-Computer Threats Classification in Intelligent Transportation Systems

Alexey Kashevnik*, Andrew Ponomarev*, Andrei Krasov†
*SPIIRAS, St. Petersburg, Russia
†Bonch-Bruyevich St. Petersburg State University of Telecommunications, St. Petersburg, Russia
{alexey.kashevnik, ponomarev}@iias.spb.su, krasov@inbox.ru

***Abstract*—Smart city concept becomes more and more popular last years for research and development. A lot of technologies appear every day that allows to automate the human life. Modern intelligent transportation systems provide possibilities to automate the driver process and increase the safety in the public roads. However, information and telecommunication technologies bring benefits as well as vulnerabilities that third parties can use for their own purposes. The paper presents comprehensive state-of-the art in the topic of human-computer threats detection for intelligent transportation systems. We discuss modern intelligent transportation systems and potential problems that appears due to interaction of human with computer. Then we consider in-cabin driver monitoring system as an example of intelligent transportation system to prove the developed classification.**

I. Introduction

The vulnerability of the traffic system in general and a ways to deal with potential risks associated with this critical infrastructure serving as a backbone of almost any city- or nationwide activity has been attracting the attention of researchers for a long time (see e.g., [1], [2]). Historically, most of the efforts in this area aim on the analysis of the transport network topology to identify critical parts of the network that can lead to disintegration of the network and make some areas not reachable.

This study is mostly focused on the threats that are associated with a) modern HMIs (possibly, leveraging AI techniques), b) attacks by authorized insiders (e.g., actions performed by an authorized car user that may affect the safety of the driver him-/herself and/or the safety of other participants of the transportation network). This contrasts our work from most of the current research in safety and security of the ITS, that consider mostly threats associated with software and communication protocols, employed in modern cars and road transportation infrastructures (e.g., [3]–[5]).

We consider human-computer interaction for intelligent transportation systems. Such interaction usually includes both implicit and explicit one. There are a lot of threats that can be caused during this interaction. We identify two main types of threats: threats related to human safety and threats related to "computer safety". Human safety is not the topic of this paper. This type of safety is related to cases then an intruder takes control on the computer system. In the paper we concentrate on "computer safety" case. This case is related to the situation when the human tricks the computer system while driving. We consider the intelligent transportation systems as computer systems. Suck tricks include threats that cause vulnerabilities for the driver, other drivers in the road or for society.

In the paper we consider related work in the topic of human-computer threats detection for intelligent transportation systems. We discuss the following aspects: transportation security, human-computer interaction, human as a consumer, and human as a provider. Then we discuss the driver monitoring system as a class of intelligent transportation systems. We identify main situations that human can use to trick the computer system. We called these situation as dangerous states. We identify main channels that driver monitoring system can use to detect such tricks. We discuss possible threats that are related to every dangerous situation.

The rest of the paper is organized as follows. State-of-the-art in the topic of human-computer threats detection for intelligent transportation systems is presented in Section II. Based on the state-of-the art analysis we identify the possible threats in Section III. Main results are summarized in Conclusion.

II. State-of-the-Art

A. Transportation security

Topological integrity of the transportation network is still an important component of transportation security ([6]–[9]). However, the proliferation of the information technologies has led to more "smart", but, at the same time, more complex transportation infrastructures and transportation means, that now include not only physical objects (e.g., roads) and appliances (e.g., vehicles), but also growing number of software modules exchanging information via multiple interfaces and protocols.

The fact that modern transportation infrastructure is a cyber-physical system that can be considered as a sum of its hardware and software based sub-components is widely recognized [10] and shapes modern research in the area of transportation security. In particular, any systematic security assessment must discover, understand, and address any vulnerabilities within each component (hardware and software) (e.g., with a help of the Common Vulnerability Scoring System [11]).

ISSN 2305-7254

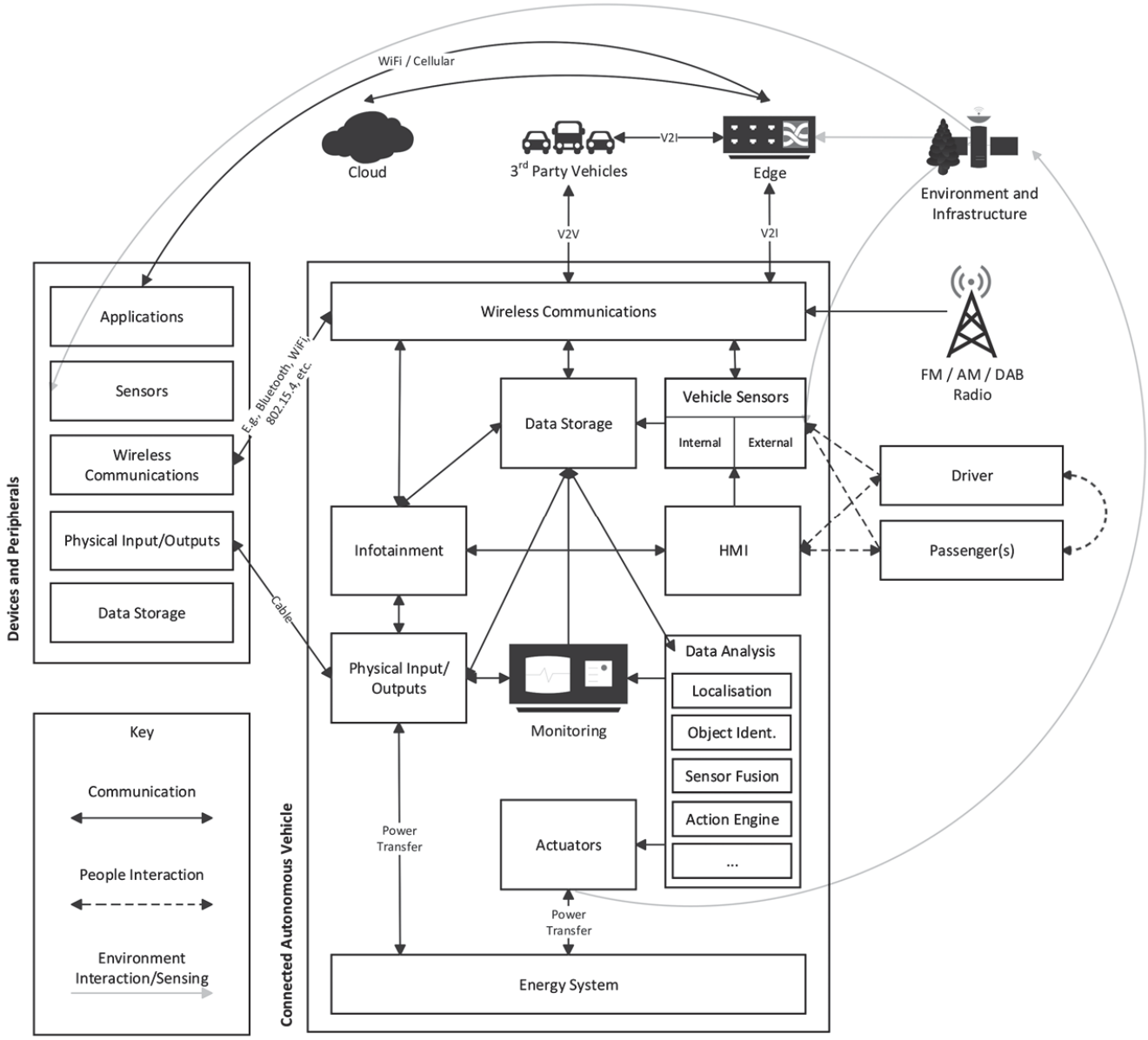

Fig. 1. Reference architecture of DAS (adopted from [12])

A particularly modern stream of work is related to specifically new threats that are introduced with the advent and proliferation of connected and autonomous vehicles. In the absence of connectivity, a physical access to the vehicle is required to exploit system vulnerabilities, and attack is localized to a single vehicle. However, with CAVs, the connection mechanisms (vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I) and vehicle-to-x (V2X)) may also be used for an attack and further weaponized to infect other vehicles. Besides, the connected infrastructure raises high requirements for the network infrastructure [13].

Research in this area is aimed on identification and classification of existing threats and vulnerabilities, development of risk assessment methodologies and proposing new technological and engineering countermeasures to the existing threats. It can be noted, that transportation cybersecurity is actively explored in at least two granularity levels: intra-vehicle level (dealing, e.g., with in-vehicle communication between components via CAN buses [3]), and inter-vehicle level (e.g., communications between various components of a large-scale intelligent transportation system [4], [5]). For example, the paper [14] proposes a proactive connected and autonomous vehicles cyber-risk classification model incorporating known software vulnerabilities contained within the US National Vulnerability Database (https://nvd.nist.gov/) into model building and testing phases. The model proposed by the authors employs Bayesian network to estimate quantitative risk score and qualitative risk level. The paper summarizes some fundamental cyber-attack types, vectors (or modes) and surfaces from the state-of-the-art literature.

The paper [12] explores the vulnerabilities of CAVs and proposes a reference CAV architecture tailored for attack surface analysis (Fig. 1). By using output from a threat

modelling, the identified goals, resources, capabilities, motivations and presence of an attacker can be used with a reference architecture to help understand how an attack could be executed (aimed mostly on L3-L5 autonomous vehicles.). The paper then uses this architecture to structure the attacks on the CAVs. The reference architecture proposed by the authors provides an abstracted view of the ecosystem, allowing developers of new products, services and infrastructure to see how a particular contribution fits into this system of systems. To identify and mitigate attacks using the reference architecture, the developer has to undertake three steps: instantiate the architecture with their particular use case; isolate the attack surface; and identify attack entry points in the boundary and internal interaction points.

Using the reference architecture from [12], our work can be positioned in People-Sensors and People-HMI interaction area. The following components and threats in HMI and Sensors area were identified by the architecture:

Sensors:

- maliciously manipulating sensor data to make the car software take incorrect decisions;
- eliminate the vehicle's ability to use certain sensors (e.g., by jamming GNSS signals or producing too much LIDAR interference for the data to be useful);
- to place additional sensors on the vehicle exterior or to subject the sensors to physical manipulation;
- interception of wireless communication with sensors (to leak identity, spoofing and replay).

Sensor security is itself a large area with several existing security assurance methodologies and practical solutions (e.g., ISO/IEC 15408 Common Criteria to solve specific security problems of sensors [15]).

HMI (any device or software that allows a person to *actively* interact with a machine, for passive interaction there are sensors – from a steering wheel to dashboard and feedback mechanisms):

- intercepting the signals from the HMI to prevent the vehicle doing something requested by the user;
- using the HMIs to report statuses that are incorrect to attempt to get the driver or passengers to perform certain actions.

The issue of cybersecurity of connected vehicles has also been addressed in the standardized guidelines documents that provide methodologies to systematically evaluate vehicle design decisions. Recent developments in this area are trying to account for both safety concerns and security concerns that are both crucial for transportation systems. In practice, in means that the so called HARA (hazard analysis and risk assessment) and TARA (threat analysis and risk assessment) has to be done jointly and may possibly intertwined. An important recent methodology in this area is SAE J3061 - guideline for cybersecurity engineering in the automotive domain, the first work related specifically to automotive cybersecurity. The questions of matching HARA and TARA are particularly addressed in [16] and [17]. In particular, the SAE J3061 suggests to apply the Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) approach, HEAling Vulnerabilities to Enhance Software Security and Safety (HEAVENS), and E-Safety Vehicle Intrusion Protected Applications (EVITA) approach. The authors of [17] point out several issues with these methodologies and also propose to adapt other approaches to do a systematic analysis of HARA and TARA: CORAS, STPA-SafeSec, SGM.

B. Human-computer interaction in ITS

Transportation system is a crucial part of any city, and therefore is actively addressed as a part of Smart City. Two major challenges of the transportation infrastructure are usually addressed in the context of a Smart City: 1) routing and congestion prevention, 2) safety. Approaches to these problems leveraging modern sensor and AI solutions are usually known under the umbrella term Intelligent Transportation Systems (ITS). ITS collects the data about current situation via multitude of heterogeneous sensors (stationary, mounted on the roadside, as well as cars playing the role of data providers), fuses it into a holistic representation of a traffic situation, employs various predictive models to estimate future situation, and (often) issues some strict or soft control instructions to change the situation to a more appropriate. Examples of strict control are changing the speed limits on road segments, length of traffic-light phases on crossroads etc. Soft control can be issued in a form of routing recommendations that balance the social and individual benefit.

Another type of systems that changes the experience of drivers is (Advanced) Driver Assistance Systems (ADAS, DAS). These systems are usually lower-level, they mostly provide assistance in routine driving operations, making them safer by either ensuring that the driver pays enough attention to the situation on the road, or by providing additional information to the driver. Typical functions of the DAS are antilock-breaking, adaptive cruise control, parking or lane change assistance, drowsiness monitoring etc. In some cases, DAS functions also include some "high level" recommendations, as navigation and routing, in this case there is some overlap between DAS and ITS. However, general distinction between these two kinds of systems is that ITS is mostly a "global" infrastructure endeavor, while DAS is mostly concentrated on the monitoring of a single driver and interaction with him/her. However, DAS and ITS recommendations might be delivered to the driver via the same HCI present in the car.

As it is currently understood, the role of a human in a modern Smart City environment is twofold. First of all, humans are end users (consumers) of Smart City services, making use of various functions (e.g., remote sensing, traffic state prediction, smart routing, maneuver assistance etc). Second, humans are providers of information for many of these systems, as many Smart City applications rely on what is called participatory sensing. These two types of interaction between a human and a Smart City infrastructure leverage different types of interactions and are analysed separately in this paper [18].

C. Human as a consumer

An important trend in analyzing human as a consumer of information provided by vehicle is the rapid change (and the lack of standardization) of the interfaces caused by new

"smart" features of the modern vehicles. As [19] points out, until the beginning of 21st century the composition of the physical buttons and mechanical gauge were more or less the same for any brand, while DAS, infotainment and navigation systems add a new layer of complexity and interactivity and dramatically change cognitive models.

Over last 40 years, a subsequent three layers control model proposed by Allen, Lunenfeld and Alexander [4] was used to analyses the driver vehicle interaction and description of driver tasks. These levels are: 1) Maneuvering level – basic control task including longitudinal and latitudinal movement control and control over vehicle accessories such as wipers and HVAC (severely affected by ADAS). 2) Tactical control – consists of tasks that require decision making in response to changing environment (affected by IVIS – in-vehicle information system) 3) Strategic level – includes highly demanding cognitive tasks, learning behavior, risk tacking and vehicle performance, driving style and preferences.

These changes require new standardized interface solutions, especially today, where young young urban inhabitant is moving away from car ownership towards "pay as you go" paradigm [19].

Here is the list of the modern technologies, which can potentially be implemented in near future to access the full potential of CC, Smart Cities and VAP technologies [19]:

- Haptic control (steering wheel, pedals).
- Embedded touch control.
- Gesture control with and without aural feedback.
- Soft interaction aid by computer vision (drowsiness detection, attention reduction).
- Touchscreens with possible haptic feedback.
- Voice control and feedback.
- Contextual information on secondary displays.

C. Human as a provider

Human sensor data – human-generated measurements (subjective observations on the environment, social media posts, mobile phone calls and text messages, and physiological measurements by wearable body sensors) [18]. This distinguishes human that generate data and humans that carry "ambient sensors" to measure external parameters (e.g., air quality with a smartphone). Paper [20] provides a nice bunch of examples of each kinds of sensors.

D. HCI in general

On the other hand, the problem of potential vulnerabilities in HCI in general has also received attention of researchers. A number of attempts to design a consistent technique for evaluation of the interfaces has been proposed.

Paper [21] states that to achieve end-to-end security, traditional machine-to-machine security measures are insufficient if the integrity of the HCI is compromised. It positions GUI flaws as a kind of software vulnerabilities that result from logic bugs in GUI design/implementation. The paper formulates the problem of GUI logic flaws and develops a methodology for uncovering them in software implementations (on an example of a web browser). Most of the effort here is dedicated to ensure that visual representation is consistent with the program (system) state. This consistency is basically achieved via a GUI model. To ensure this consistency a formal model was developed, describing system state, action sequences, execution context, and program logic. After these components are specified on the reasoning engine, formal reasoning can be applied to check if the user action sequence violates the program invariant. In [21] this task is resolved in the context of rewriting logic framework, with a help of Maude system.

An important direction here is formal evaluation of an interface to detect states that might result in misinterpretation of the system state by the user. Therefore, in [22] a formal model has been proposed to ensure the so-called full-control property.

F. Results analysis

It has already been widely recognized that modern ITS are cyber-physical systems, therefore potential threats for these systems can be associated with both software and hardware components. Likewise, security and safety assurance procedures should consider both worlds and their interaction.

However, we argue that the scope of safety and security assurance should be extended even more, because a) human driver is an inextricable part of any transportation system affecting the overall level of its security and safety, b) modern ITS actively interact with humans (in a number of ways). In fact, ITSs are socio-cyberphysical systems (or, cyber-physical-social systems). Therefore, an effort has to be undertaken to analyze ITS in this light, identify potential threats and vulnerabilities resulting from the inclusion of human into the system and human-computer interaction, possible countermeasures and ITS development methodologies allowing to systematically address these threats and vulnerabilities. This paper is making a first step in this direction by identifying and classifying human-related threats in such systems.

The human turn out to be involved into transportation system in several ways, and it naturally structures the threat analysis procedure:

1) Human driver is a part of a transportation system. He/she controls a car and human mistakes during this process can undermine safety of both the driver and other transportation system participants. Primary causes of driver mistakes are abnormal driver states (drowsiness, inattentiveness etc.).

2) Human is a part of a 'small cycle' information loop, implemented by various DAS that monitor human behavior and provide additional information to human driver. Threats here are associated with a) sensing and interpretation of human behavior, b) presentation of information to humans. For example, an attempt of a driver to disable some sensors of a monitoring system may result in malfunction of a DAS and therefore, threat road safety. On the other hand, ambiguous recommendations, or recommendations provided in an

inopportune moment may lower the attention of the driver and also threat road safety.

3) Human may be a part of a 'large cycle' information loop, providing information to other participants of transportation system via crowd- or participatory functions of modern ITS. For example, driver my falsely report traffic accidents or traffic congestion, that potentially results in lowering of effectiveness of routing.

III. Discussion

We consider driver monitoring systems (Fig. 2) as a typical ITS that is aimed at driver monitoring in real life and dangerous situation detection to prevent an accidents [23].

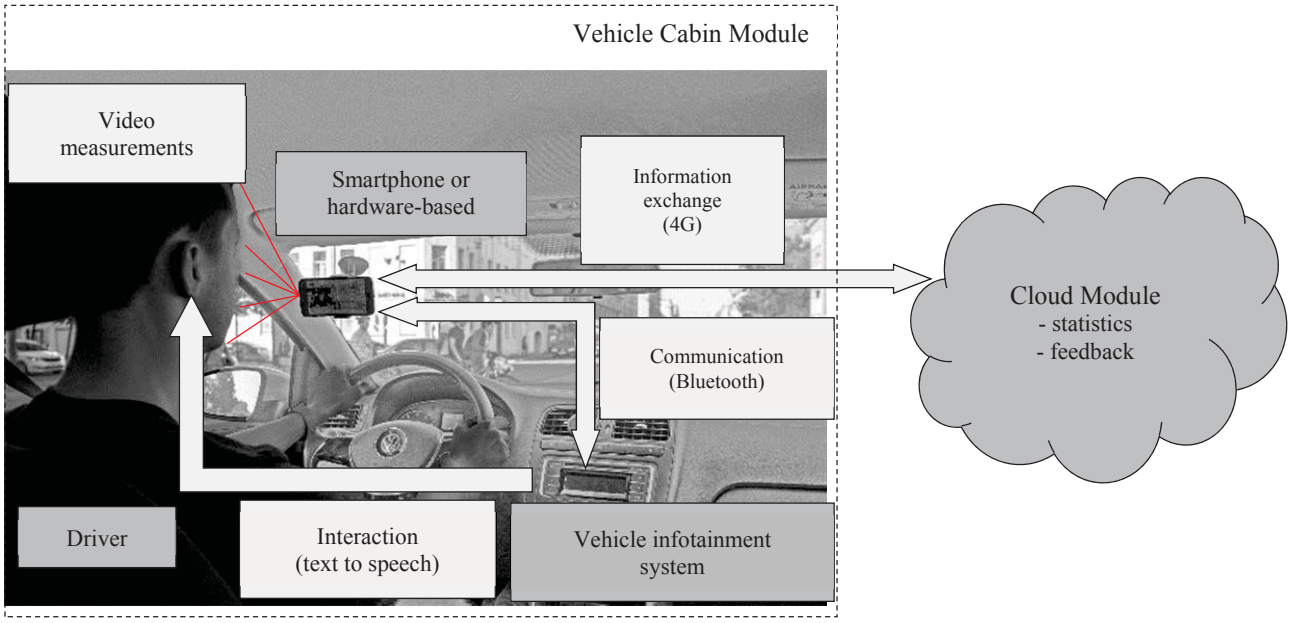

Fig. 2. Driver monitoring system

So, we consider the possible threads for the system operation if the driver tries to trick the system and driving process causes the dangerous situation. We classify possible threads that can be caused in driver monitoring system from the perspective (see Table I). The main goal of driver monitoring system is to predict dangerous states using one of possible communication channels. We identify visual channel, sensor channel, and audio channel.

We assume that the driver monitoring system use a camera that tracks driver face and analyses it to predict dangerous states. Analyzing the driver face images using the modern computer vision techniques, it is possible to predict different states that can cause the threads during the vehicle driving (such as sleeping, drowsiness, fatigue, distraction, mobile phone usage, eating, drinking, smoking, drunk driving, high heart rate, and etc.).

Sensor channel means analysis of such data as: coordinates, speed, accelerometer, gyroscope, magnetometer, light sensor that provide possibilities to detect such dangerous states as aggressive driving, traffic rules compliance as well as filter all other dangerous states that are not important for stopped vehicles (such as distracting, mobile phone usage, eating, drinking, smoking and etc.).

Audio channel allows proofing or indirectly detecting in case of visual channel unavailability such dangerous states as sleeping, drowsiness fatigue, distracting, mobile phone usage, eating, drinking, etc. Audio channel allows determining loudness level in the cabin as well as if the driver is silent or speaking, singing etc.

We discuss eight main dangerous states that are important for driver monitoring system and discuss possible threats they cause. Camera sabotaging is a situation when camera is switched off, or disactivated by some objects. In this situation visual channel is deactivated.

Driver sleeping, drowsiness or fatigue dangerous state is the dangerous state when the driving causes a risk of accident. If the driver continues the vehicle driving this causes the threat of increasing the accident level probability.

Driver distracting, mobile phone usage, eating, drinking, or smoking is the dangerous state when the driver loses the concentration on the road. This dangerous state can be caused by different factors but as the result the behavior causes the threat of increasing the accident level probability.

Drunk or drug driving dangerous state is also related to losing of the concentration on the road caused by taking of drugs or alcohol. Such situation also causes the threat of increasing the accident level probability.

IV. Conclusion

The paper presents comprehensive state-of-the-art in the topic of human-computer threats classification in intelligent transportation systems. Based on state-of-the-art we got the following results.

- Human driver is a part of a transportation system. He/she controls a car and human mistakes during this process can undermine safety of both the driver and other transportation system participants.
- Human is a part of a 'small cycle' information loop, implemented by various DAS that monitor human behavior and provide additional information to human driver.
- Human may be a part of a 'large cycle' information loop, providing information to other participants of transportation system via crowd- or participatory functions of modern ITS.

We consider driver monitoring systems as typical ITS that is aimed at driver monitoring in real life and dangerous situation detection to prevent an accident. We identified main dangerous states the human driver can cause that cause the possible threats in such systems.

TABLE I. THREATS CLASSIFICATION IN DRIVER MONITORING SYSTEMS

#	Dangerous States	Chanel	Possible Threats
1	Camera Sabotaging	Visual	Camera deactivation that causes impossibility of future driver monitoring in vehicle cabin.
2	Driver Sleeping, Driver Drowsiness, Driver Fatigue	Visual	Driving without concentration on the road increases the accident probability level.
		Sensor	
		Audio	
3	Distracting, Mobile Phone Usage, Eating, Drinking, Smoking	Visual	
		Sensor	
		Audio	
4	Drunk or Drug Driving	Visual	
5	Passenger Sleeping	Visual	Driving with sleeping passengers increase probability of sleep for the driver.
6	High Heart Rate	Visual	Driving in bad health condition or in aggressive state significantly increases the accident probability
7	Aggressive Driving	Sensor	
8	Vehicle Shaking	Sensor	Driving with high speed off-road causes the vehicle damage as well ass accident high probability level.
9	Traffic Rules Compliance	Visual	Traffic rules violation increases the accident probability.
		Sensor	

Future work will be concentrated on human-computer interaction interface development that is based on the presented threats classification and supported the identified dangerous states.

ACKNOWLEDGMENT

The presented results are part of the research supported by Russian Foundation for Basic Research project # 19-29-06099.

REFERENCES

[1] K. Berdica, "An introduction to road vulnerability: what has been done, is done and should be done," *Transport Policy*, vol. 9, no. 2, pp. 117–127, Apr. 2002.

[2] A. W. Evans, "Evaluating public transport and road safety measures," *Accident Analysis & Prevention*, vol. 26, no. 4, pp. 411–428, Aug. 1994.

[3] K. B. Kelarestaghi, M. Foruhandeh, K. Heaslip, and R. Gerdes, "Intelligent Transportation System Security: Impact-Oriented Risk Assessment of In-Vehicle Networks," *IEEE Intelligent Transportation Systems Magazine*, pp. 1–1, 2019.

[4] L. Ming, G. Zhao, M. Huang, X. Kuang, H. Li, and M. Zhang, "Security analysis of intelligent transportation systems based on simulation data," *Proceedings - 2018 1st International Conference on Data Intelligence and Security, ICDIS 2018*, pp. 184–187, 2018.

[5] N. Huq, R. Vosseler, and M. Swimmer, "Cyberattacks Against Intelligent Transportation Systems Assessing Future Threats to ITS," 2017.

[6] A. Pagani *et al.*, "Resilience or robustness: identifying topological vulnerabilities in rail networks," *Royal Society Open Science*, vol. 6, no. 2, p. 181301, Feb. 2019.

[7] T. Santos, M. A. Silva, V. A. Fernandes, and G. Marsden, "Resilience and Vulnerability of Public Transportation Fare Systems: The Case of the City of Rio De Janeiro, Brazil," *Sustainability*, vol. 12, no. 2, p. 647, Jan. 2020.

[8] Z. Zhu, A. Zhang, and Y. Zhang, "Measuring multi-modal connections and connectivity radiations of transport infrastructure in China," *Transportmetrica A: Transport Science*, vol. 15, no. 2, pp. 1762–1790, Nov. 2019.

[9] S. Mudigonda, K. Ozbay, and B. Bartin, "Evaluating the resilience and recovery of public transit system using big data: Case study from New Jersey," *Journal of Transportation Safety & Security*, vol. 11, no. 5, pp. 491–519, Sep. 2019.

[10] T. M. Keller, V. Wright, J. Benjamin, and B. Gold, "Vulnerabilities under the surface," in *Proceedings of the Fifth Cybersecurity Symposium on - CyberSec '18*, 2018, pp. 1–3.

[11] K. Scarfone and P. Mell, "An analysis of CVSS version 2 vulnerability scoring," in *2009 3rd International Symposium on Empirical Software Engineering and Measurement*, 2009, pp. 516–525.

[12] C. Maple, M. Bradbury, A. T. Le, and K. Ghirardello, "A Connected and Autonomous Vehicle Reference Architecture for Attack Surface Analysis," *Applied Sciences*, vol. 9, no. 23, p. 5101, Nov. 2019.

[13] M. Aamir, S. Masroor, Z. A. Ali, and B. T. Ting, "Sustainable Framework for Smart Transportation System: A Case Study of Karachi," *Wireless Personal Communications*, vol. 106, no. 1, pp. 27–40, May 2019.

[14] B. Sheehan, F. Murphy, M. Mullins, and C. Ryan, "Connected and autonomous vehicles: A cyber-risk classification framework," *Transportation Research Part A: Policy and Practice*, vol. 124, pp. 523–536, Jun. 2019.

[15] A. Bialas, "Vulnerability Assessment of Sensor Systems," *Sensors*, vol. 19, no. 11, p. 2518, Jun. 2019.

[16] G. Macher, R. Messnarz, E. Armengaud, A. Riel, E. Brenner, and C. Kreiner, "Integrated Safety and Security Development in the Automotive Domain," 2017-01–1661, 2017.

[17] J. Dürrwang, J. Braun, M. Rumez, R. Kriesten, and A. Pretschner, "Enhancement of Automotive Penetration Testing with Threat Analyses Results," *SAE International Journal of Transportation Cybersecurity and Privacy*, vol. 1, no. 2, pp. 91–112, Nov. 2018.

[18] B. Resch, "People as Sensors and Collective Sensing-Contextual Observations Complementing Geo-Sensor Network Measurements," in *Progress in Location-Based Services. Lecture Notes in Geoinformation and Cartography*, 2013, pp. 391–406.

[19] D. Rozhdestvenskiy and P. Bouchner, "Human machine interface for future cars. Changes needed," in *2017 Smart City Symposium Prague (SCSP)*, 2017, pp. 1–5.

[20] G. Sagl, B. Resch, and T. Blaschke, "Contextual Sensing: Integrating Contextual Information with Human and Technical Geo-Sensor Information for Smart Cities," *Sensors*, vol. 15, no. 7, pp. 17013–

17035, Jul. 2015.
[21] S. Chen, J. Meseguer, R. Sasse, H. J. Wang, and Y.-M. Wang, "A Systematic Approach to Uncover Security Flaws in GUI Logic," in *2007 IEEE Symposium on Security and Privacy (SP '07)*, 2007, pp. 71–85.
[22] S. Combefis, D. Giannakopoulou, C. Pecheur, and M. Feary, "A formal framework for design and analysis of human-machine interaction," in *2011 IEEE International Conference on Systems, Man, and Cybernetics*, 2011, pp. 1801–1808.
[23] A. Kashevnik, I. Lashkov, and A. Gurtov, "Methodology and Mobile Application for Driver Behavior Analysis and Accident Prevention," *IEEE Transactions on Intelligent Transportation Systems*, pp. 1–10, 2019.