https://doi.org/10.31891/csit-2024-2-8
UDC 004.72

Mykyta BOIKO, Vasyl YATSKIV
Khmelnytskyi National University

SURVEILLANCE CYBER-PHYSICAL SYSTEM AS A PART OF INTERNET OF VEHICLES

Integration of cyber-physical surveillance systems (CPSS) into the Internet of Vehicles (IoV) paradigm represents a transformative approach to enhancing transportation safety and efficiency. This article discusses the design, implementation, and application of CPSS as part of IoV ecosystems. Leveraging advancements in sensor technologies, communication protocols, and data analytics, CPSS within IoV enables real-time monitoring, analysis, and response to road conditions, incidents, and emergencies. Our research explores the architecture and functional capabilities of CPSS, including sensor deployment, data fusion, anomaly detection, and decision support mechanisms. We investigate the synergistic interaction between CPSS and IoV platforms, facilitating seamless data exchange, collaboration, and compatibility between automotive and infrastructural domains. Additionally, we discuss potential applications of CPSS in traffic management, law enforcement, emergency response, and urban planning, emphasizing its role in enhancing transportation safety, optimizing resource allocation, and preventing congestion and accidents. Through empirical evaluations and thematic studies, we demonstrate the effectiveness, scalability, and societal impact of integrating CPSS into IoV ecosystems. This research contributes to the development of intelligent transportation systems and underscores the transformative potential of CPSS within the IoV context.

This article explores the potential of Cyber-Physical Systems (CPS) in the realm of the Internet of Vehicles (IoV), particularly within the context of surveillance systems in the IoV network. It proposes an approach to designing CPS, examining existing technical and systemic solutions for their creation. The article delves into the network architecture, the system's time cost model, and the possible positioning of CPS within vehicles.

The aim of this article is to investigate the possibilities of utilizing CPS in the IoV sphere and to initiate a discussion on their implementation and potential benefits for the development of transportation infrastructure and road safety. It opens up new perspectives for improving transportation systems and creating effective monitoring and control mechanisms, thereby promoting safer and more efficient transportation usage.

Keywords: cyber-physical system, Internet of Vehicles, intelligent transportation systems, edge computing.

Микита БОЙКО, Василь ЯЦКІВ
Хмельницький національний університет

СИСТЕМА КІБЕР-ФІЗИЧНОГО СПОСТЕРЕЖЕННЯ ЯК ЧАСТИНА ІНТЕРНЕТУ ТРАНСПОРТНИХ ЗАСОБІВ

Інтеграція кіберфізичних систем спостереження (КФСС) у парадигму Інтернету транспортних засобів (IoV) представляє трансформаційний підхід до підвищення безпеки та ефективності транспортування. У цій статті розглядається дизайн, впровадження та застосування КФСС як частину екосистем IoV. Використовуючи досягнення в сенсорних технологіях, протоколах зв'язку та аналітиці даних, КФСС в рамках IoV дозволяє здійснювати моніторинг, аналіз і реагування на дорожні умови, інциденти та надзвичайні ситуації в реальному часі. Наше дослідження вивчає архітектуру та функціональні можливості КФСС, включаючи розгортання датчиків, об'єднання даних, виявлення аномалій та механізми підтримки прийняття рішень. Ми досліджуємо синергетичну взаємодію між платформами КФСС та IoV, сприяючи безперебійному обміну даними, співпраці та сумісності між автомобільними та інфраструктурними доменами. Крім того, ми обговорюємо потенційні застосування КФСС в управлінні дорожнім рухом, правоохоронній діяльності, реагуванні на надзвичайні ситуації та міському плануванні, підкреслюючи його роль у підвищенні безпеки транспортування, оптимізації розподілу ресурсів і запобіганню заторів і аварій.

За допомогою емпіричних оцінок і тематичних досліджень ми демонструємо ефективність, масштабованість і вплив на суспільство інтеграції КФСС в екосистеми IoV. Це дослідження робить внесок у розвиток інтелектуальних транспортних систем і підкреслює трансформаційний потенціал КФСС в контексті IoV.

У цій статті досліджується потенціал кіберфізичних систем (КФС) у сфері Інтернету транспортних засобів, зокрема в контексті систем спостереження. Запропоновано підхід до проектування КФС, розглянуто існуючі технічні та системні рішення для їх створення. У статті розглядається архітектура мережі, модель часових витрат системи та можливе розміщення КФС в транспортних засобах.

Мета цієї статті - дослідити можливості використання КФС у сфері інтернету транспортних засобів та ініціювати дискусію щодо їх впровадження та потенційних переваг для розвитку транспортної інфраструктури та безпеки дорожнього руху. Це відкриває нові перспективи для вдосконалення транспортних систем і створення ефективних механізмів моніторингу та контролю, що сприятиме безпечнішому та ефективнішому використанню транспорту.

Ключові слова: кіберфізична система, інтернет транспортних засобів, інтелектуальні транспортні системи, периферійні обчислення.

Introduction

Internet of Vehicles (IoV) is a system of loosely connected heterogeneous or homogeneous devices capable of receiving, transmitting, and processing information among each other. Mostly discussed alongside the use of Intelligent Transportation Systems (ITS) to create safe and reliable automated vehicle control technology [1]. This technology is equipped with embedded sensors based on automotive devices while simultaneously connected to environments, people, and systems [2]. The development of new vehicles is already being done with consideration for IoV and ITS technologies, which are integrated at the design and assembly stages of the vehicle. The future will

be defined by the interactions between entities, sensors, smartphones, and vehicles, which are not exceptions in this context. Thus, considering potential methods of creating cyber-physical systems in the Internet of Things (IoT) network becomes crucial.

Figure 1 illustrates the general conceptual scheme of CPSS in the IoV network, which can ensure driver safety through a cyber security service center and utilize its monitoring devices to gather useful information and disseminate it within or even beyond the IoV. Computers play a significant role in this system, as many smart vehicles have become intelligent due to advancements in technology and computational power of devices. Currently, smart cars have added stability control, optimal mileage, fuel injection, navigation, and theft prevention [3]. However, there is almost no discussion or development in the field of individual portable cyber-physical systems that can be involved in IoV usage, not only for safe vehicle control but also for collecting and disseminating useful information such as road traffic accidents, road conditions, or monitoring fuel prices at gas stations. Similar to the technological use of smartphones, a portable cyber-physical system (CPSS) for vehicles can add a lot of functionality based on the data it can accumulate and analyze.

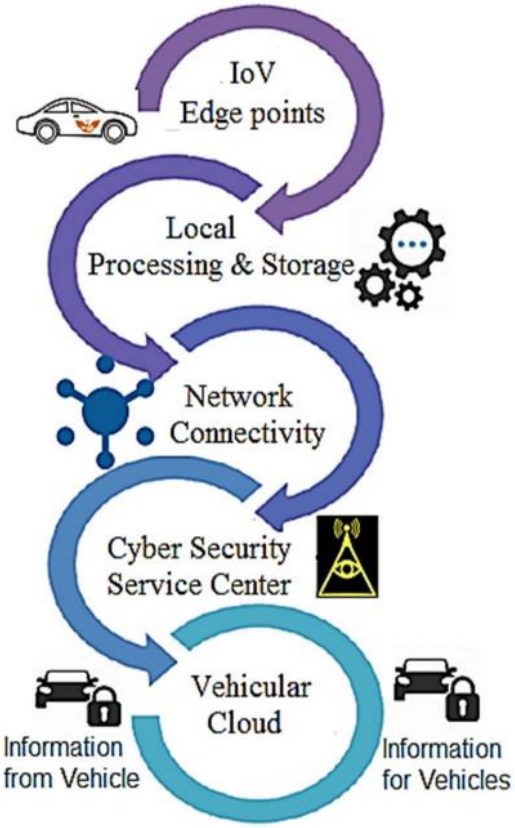

Fig.1. Concept of a secure Internet of vehicles [1]

In this article, we present an approach to designing the proposed CPSS model as part of IoV. We will consider available technical and system solutions for creating such a system. We will develop the network architecture and build a time cost model of the system. In the final section, we will discuss possible positioning of CPSS in the vehicle and the components it should consist of, describing them as a mathematical model.

Related works

In the Internet of Things (IoV), computational capabilities and storage of video surveillance fall under edge computing. Although the capacity of surveillance systems is strengthened by edge computing, there are still some challenges that arise, namely: time costs, task offloading, and confidentiality preservation in edge computing are being investigated according to recent research.

Task offloading aims at proper distribution of computational tasks and their efficient allocation to neighboring computing devices. From the perspective of task offloading, an effective real-time video system with an efficient resource provisioning strategy and low latency video cluster scheduler has been developed in [4]. The architecture of collaborative video processing to balance the limited network bandwidth and task offloading has been investigated in [5]. Both approaches effectively address the issue of limited resources. However, it is also important to consider the efficiency of task offloading.

In [6], the author proposed an algorithm using hypergraph segmentation to minimize network load of

systems with an optimal way of considering the non-obligatory case. Taking into account the offloading capacity, a new network offloading scheme has been developed in [7] to enhance the power of edge computing by maximizing constant productivity while ensuring energy expenditure with constant constraints. A task offloading model has been proposed in [8] to enhance long-term utility based on a powerful distributed offloading model during various wireless connections.

Additionally, in terms of time costs, a distributed smart surveillance system has been introduced in [9], which offloads computational burdens to alleviate high communication overheads and provides low-latency video analysis solutions using deep learning algorithms. A strategy of collective video processing has been proposed in [10] to achieve multimedia tasks with time-sensitive reactions and improve human detection accuracy through edge computing.

However, none of these approaches take security aspects into account. Peripheral nodes in video surveillance face challenges in confidentiality preservation. A paradigm supporting secure communication and preserving confidentiality has been presented in [11]. A new protocol has been developed in [12] to provide desired security features. Strategies for optimizing task offloading and data confidentiality protection are presented in [13] and [14].

However, current research on task offloading in edge computing mainly focuses on the efficiency of implementing computational tasks, neglecting the drawbacks of unbalanced service placement. In this article, we will consider the placement of the peripheral device system by moving them from the surrounding environment to vehicles.

System Model

In this section, the network architecture and time cost model for our CPS are developed and presented. The main system notations are provided in Table 1.

Table 1

Notations and Definitions

Notations	Definitions
N	Number of vehicles with a cyber-physical system
S	Set of peripheral systems, where *S = {s1, s2, … sN}*
L	Number of virtual machines in *S*N
J	Number of executed tasks
VN	Set of virtual machines in *SN*, where *VN = {vn, 1, vn, 2, … vn, L}*
T	Set of executed tasks, where *T = {t1, t2, … tJ}*
Ttotal	Total time spent on tasks

In this article, we utilize edge computing technology in the video surveillance system. As shown in Figure 2, an architecture of video surveillance with edge computing is proposed, where observation terminals are installed in vehicles, and generated video data is offloaded directly to the base station using LTE communication. Peripheral nodes with powerful computational capabilities (vehicles with CPS) take on computational tasks. Then, the computation results are sent from peripheral nodes to the cloud environment via base stations. In this scenario, along the road, there are *N* vehicles, each equipped with CPS for video surveillance, denoted as *S = {s1, s2, … sN}*. The CPS device set consists of two components: peripheral nodes and access points. Let *T = {t1, t2, … tJ}* denote a set of *J* computational tasks generated from nodes. Peripheral nodes have powerful computational capabilities and preprocessing capacity, consisting of virtual machines (VM). There are *L* virtual machines in sw, defined as *VN = {vn, 1, vn, 2, … vn, L}*.

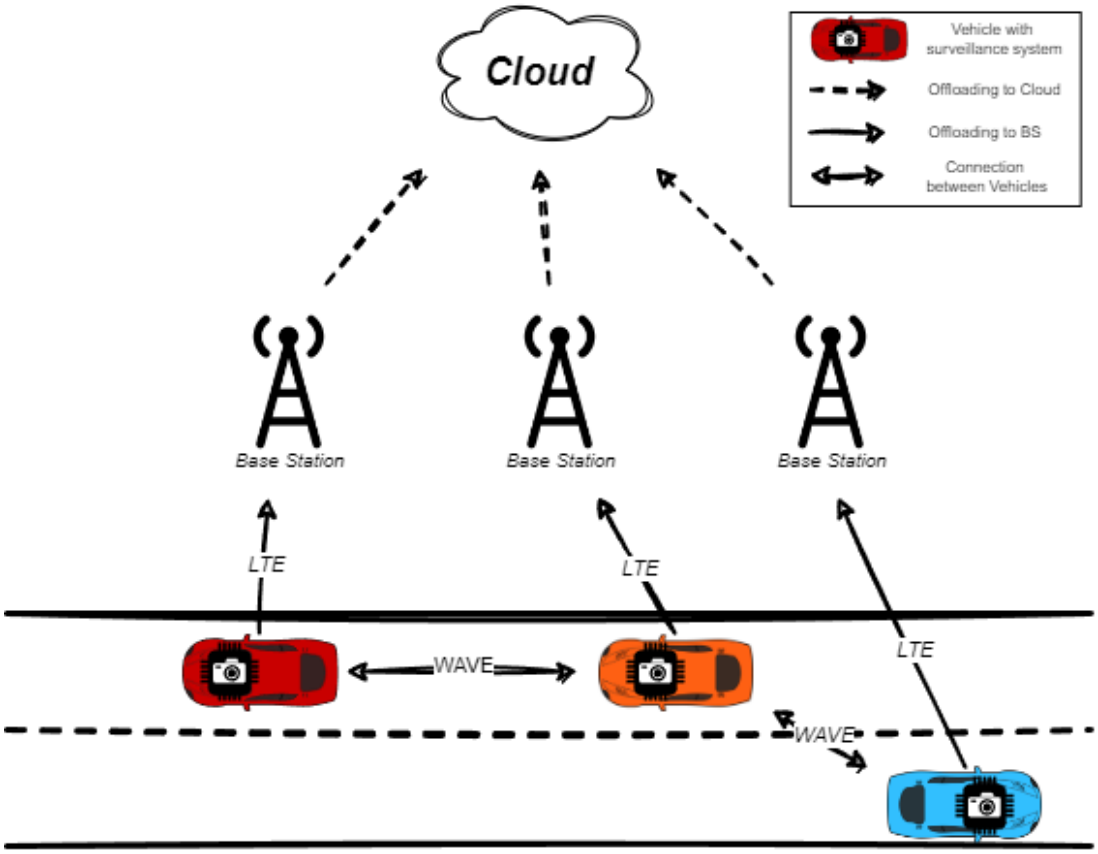

Fig. 2. Architecture of video surveillance with edge computing located in vehicles

The next time cost model will be developed based on the work type [15], in which the authors also developed a time cost model, load balance model, and entropy model for the offloading system based on static objects for monitoring vehicle traffic.

Time costs consist of computation time at the respective peripheral node and offloading time. Time costs are an important parameter that determines the quality of real-time service on monitoring devices. When video tasks are sent to the image processing device, the CPS should provide virtual machines for computation. The computational capacity of peripheral nodes is associated with the number of available virtual machines. Thus, the number of available virtual machines in *sn* is denoted as *xn*, and the operational capacity of each virtual machine is denoted as φ. Suppose the video task with duration *F*j is processed in *sn*, and the computation time of *s*n is expressed as (1):

$$h_j = \sum_{n=1}^{N} k_{j,n} \frac{F_j}{x_n \cdot \varphi} \quad (1)$$

, where *kj,n* = 1 if the data *tj* arrived at *sn*, otherwise 0.

Once the video processing in *sn* is completed, the computed result is offloaded from the peripheral devices to the cloud center. The offloading time of the computation result *tj* with weight *fj,output* can be calculated as (2):

$$o_j = \sum_{n=1}^{N} k_{j,n} \left(\frac{f_{j,output}}{\eta} + \frac{f_{j,output}}{\lambda} \right) \quad (2)$$

where η represents the transmission speed between peripheral nodes and base stations, and λ denotes the transmission speed between base stations and the cloud data processing center.

With the calculated two components, the total time costs for task execution can be determined by the following formula (3):

$$T_{total} = \sum_{j=1}^{J} (h_j + o_j) \quad (3)$$

Structure of CPSS

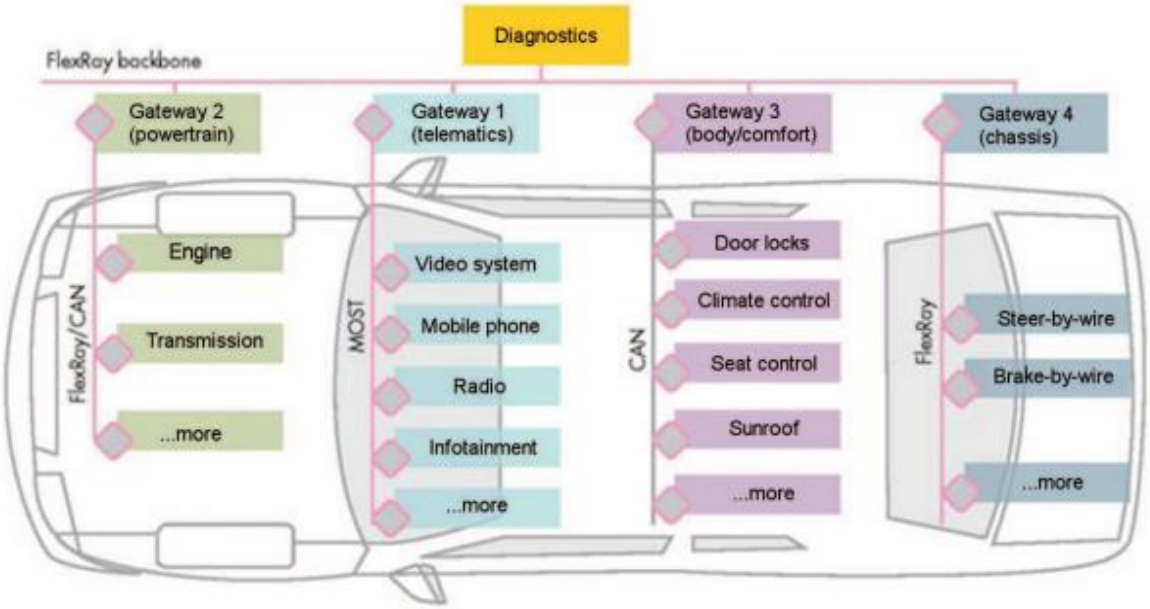

Fig. 3. Topology of the automotive network [16]

Before developing the CPS, it is necessary to determine which part of the automotive network our system belongs to. According to [17], the automobile topology can be divided into four parts, each with its own diagnostic gateways: telematics, powertrain, body/comfort, and chassis. In this topology, telematics is best suited for integrating our CPS, as it combines telecommunications, automotive technologies, electrical engineering, and informatics of the vehicle, and it utilizes the Media Oriented Systems Transport (MOST) communication protocol.

Let's define the subsystems of this system and describe them in the form of a mathematical model:

1. Communication module (*S*). At the initial stages, a smartphone can be used as an access point providing communication between the system and a remote server via the Internet.

Parameters: communication state (*Sstate*), data transmission speed (*Sspeed*), network access time (Saccess_time).

2. GPS module (*G*). Determines the location of our system (vehicle) and provides coordinates that can be used for various purposes such as navigation or location determination.

Parameters: Coordinates (*x, y*), location determination accuracy (*Gaccuracy*), update time (*Gupdate_time*).

3. Surveillance camera (*C*). Designed to gather information about events on the road.

Parameters: Resolution (*Cresolution*), frame rate (*Cframe_rate*), processing delay time (*Cprocessing_time*).

4. Power source (P). Provides power supply for the entire peripheral system.

Parameters: Voltage (*Pvoltage*), Power (*Ppower*).

5. Single-board computer (R). Responsible for image processing, interaction with the GPS module, and data transmission to the remote server.

Parameters: Memory size (*Rmemory*), processor speed (*Rprocessor_speed*), load level (*Rload*).

Thus, the our CPSS can be described as the following set (4):

$$CPSS = \{S, G, C, P, R\} \quad (4)$$

The mentioned subsystems represent the key components of our CPS in IoV for surveillance, each responsible for specific functionality and having its own parameters that determine their efficiency and productivity. Developing a mathematical model of the system has allowed for a better understanding of its operation and component interaction, which is crucial for the successful implementation and optimization of the system's functioning in real operating conditions.

Conclusion

This article explores the potential of Cyber-Physical Systems (CPS) in the realm of the Internet of Vehicles (IoV), particularly within the context of surveillance systems in the IoV network. It proposes an approach to designing CPS, examining existing technical and systemic solutions for their creation. The article delves into the network architecture, the system's time cost model, and the possible positioning of CPS within vehicles.

The aim of this article is to investigate the possibilities of utilizing CPS in the IoV sphere and to initiate a discussion on their implementation and potential benefits for the development of transportation infrastructure and

road safety. It opens up new perspectives for improving transportation systems and creating effective monitoring and control mechanisms, thereby promoting safer and more efficient transportation usage.

References

1. Singh, D., Tripathi, G., Shah, S. C., & da Rosa Righi, R. (2018). Cyber physical surveillance system for Internet of Vehicles. 2018 IEEE 4th World Forum on Internet of Things (WF-IoT). doi:10.1109/wf-iot.2018.8355218

2. F. Yang, S. Wang, J. Li, Z. Liu and Q. Sun, "An overview of Internet of Vehicles," in China Communications, vol. 11, no. 10, pp. 1-15, Oct. 2014.

3. D. George, P. Demestichas. "Intelligent transportation systems." IEEE Vehicular Technology Magazine 5.1 (2010): 77-84

4. P.-H. Wu, C.-W. Huang, J.-N. Hwang, J.-Y. Pyun, and J. Zhang, "Video-quality-driven resource allocation for real-time surveillance video uplinking over OFDMA-based wireless networks," IEEE Trans. Veh. Technol., vol. 64, no. 7, pp. 3233–3246, Jul. 2015.

5. J. Wang, L. Zhao, J. Liu, and N. Kato, "Smart resource allocation for mobile edge computing: A deep reinforcement learning approach," IEEE Trans. Emerg. Topics Comput., early access, Mar. 4, 2019, doi: 10.1109/TETC.2019.2902661.

6. N. Tziritas et al., "Data replication and virtual machine migrations to mitigate network overhead in edge computing systems," IEEE Trans. Sustain. Comput., vol. 2, no. 4, pp. 320–332, Oct. 2017.

7. L. Chen, S. Zhou, and J. Xu, "Computation peer offloading for energyconstrained mobile edge computing in small-cell networks," IEEE/ACM Trans. Netw., vol. 26, no. 4, pp. 1619–1632, Aug. 2018.

8. T. Quang Dinh, Q. Duy La, T. Q. S. Quek, and H. Shin, "Learning for computation offloading in mobile edge computing," IEEE Trans. Commun., vol. 66, no. 12, pp. 6353–6367, Dec. 2018.

9. J. Chen, K. Li, Q. Deng, K. Li, and P. S. Yu, "Distributed deep learning model for intelligent video surveillance systems with edge computing," IEEE Trans. Ind. Informat., early access, Apr. 9, 2019, doi: 10.1109/TII.2019.2909473.

10. L. T. Tan and R. Q. Hu, "Mobility-aware edge caching and computing in vehicle networks: A deep reinforcement learning," IEEE Trans. Veh. Technol., vol. 67, no. 11, pp. 10190–10203, May 2018.

11. J. Kang, R. Yu, X. Huang, and Y. Zhang, "Privacy-preserved pseudonym scheme for fog computing supported Internet of vehicles," IEEE Trans. Intell. Transp. Syst., vol. 19, no. 8, pp. 2627–2637, Aug. 2018.

12. U. L. N. Puvvadi, K. D. Benedetto, A. Patil, K.-D. Kang, and Y. Park, "Cost-effective security support in real-time video surveillance," IEEE Trans. Ind. Informat., vol. 11, no. 6, pp. 1457–1465, Dec. 2015.

13. M. Liu, F. R. Yu, Y. Teng, V. C. M. Leung, and M. Song, "Distributed resource allocation in blockchain-based video streaming systems with mobile edge computing," IEEE Trans. Wireless Commun., vol. 18, no. 1, pp. 695–708, Jan. 2019.

14. X. Li, S. Liu, F. Wu, S. Kumari, and J. J. P. C. Rodrigues, "Privacy preserving data aggregation scheme for mobile edge computing assisted IoT applications," IEEE Internet Things J., vol. 6, no. 3, pp. 4755–4763, Jun. 2019.

15. Xu, X., Wu, Q., Qi, L., Dou, W., Tsai, S.-B., & Bhuiyan, M. Z. A. (2020). Trust-Aware Service Offloading for Video Surveillance in Edge Computing Enabled Internet of Vehicles. IEEE Transactions on Intelligent Transportation Systems, 1–10. doi:10.1109/tits.2020.2995622

16. R. ALLAN. Automotive networks strive to satisfy safety and bandwidth needs. illustration. Electronic Design, 57(21):28 – 33, 2009.

17. Pohlmann, U., Meyer, M., Dann, A., & Brink, C. (2014). Viewpoints and Views in Hardware Platform Modeling for Safe Deployment. Proceedings of the 2nd Workshop on View-Based, Aspect-Oriented and Orthographic Software Modelling - VAO '14. doi:10.1145/2631675.

Mykyta BOIKO **Микита БОЙКО**	bachelor, Khmelnytskyi National University, Khmelnytskyi, Ukraine, e-mail: nikita2000223@gmail.com	бакалавр, Хмельницький національний університет, Хмельницький, Україна.
Vasyl YATSKIV **Василь ЯЦКІВ**	Doctor of Technical Science, Professor, Western Ukrainian National University, Ternopil, Ukraine. e-mail: jazkiv@ukr.net https://orcid.org/0000-0001-9778-6625, Scopus Author ID: 27468042400,	доктор технічних наук, професор, завідувач кафедри кібербезпеки, Західноукраїнський національний університет, Тернопіль, Україна.