Reconsidering the Cybersecurity Framework in the Road Transportation Domain

Mohammed Obaid[*], Zsolt Szalay, Árpád Török

Department of Automotive Technologies, Faculty of Transportation and Vehicle Engineering, Budapest University of Technology and Economics, Műegyetem rkp. 3, 1111 Budapest, Hungary; obaid.mohammed@mail.bme.hu, zsolt.szalay@gjt.bme.hu, arpad.torok@auto.bme.hu

Abstract: The Automotive Industry has advanced significantly and this process is constantly continuing. Cars are controlled by hundreds of electrical units, which affects directly numberless safety and security related risk factors, especially considering incidents realized in the cyberspace. Due to the increasing number of connected cars, new testing facilities and methods need to be established, to support the solutions, for these novel challenges. For this reason, the Hungarian government has founded the Zalaegerszeg test track, and its special purpose is to provide space for the validation of future vehicles. The overview focused on the presently applied validation methods and processes has highlighted, that cybersecurity related testing methods – from a scientific point of view – are only slightly detailed in the sector of Automobile Industry. In a sector specific term, the lack of a holistic approach, may result a relevant barrier, in the future, for providing a socially tolerable level of cybersecurity. Accordingly, this paper aims to introduce a comprehensive cybersecurity reference model, to provide a solid basis for describing attack patterns and characterizing malicious intervention profiles.

Keywords: Security-and-Privacy; Physical-Layer; Autonomous-Driving-and-Communication; Vehicle-to-vehicle/roadside/Internet-communication; vehicular-security; cybersecurity-reference-space

1 Introduction & Related Work

Automobile technology has greatly developed in the last decades and is still relentlessly developing; consider the introduction of driverless cars. Vehicles are now controlled by hundreds of electrical units (ECUs) that form an internal network of devices within the vehicle. This development has raised questions about the vulnerability of the transport system, especially considering safety and security issues influenced by cyberattacks [1].

The growing proportion of automated and connected vehicles makes it necessary to establish new testing facilities and methods supporting the solutions of these novel challenges. For this purpose, the Hungarian government has founded the Zalaegerszeg test track [2] called ZalaZone, which beyond the conventional test issues, especially focuses on the validation of future vehicles. ZalaZone ensures not only validation facilities for conventional vehicles, but it also makes it possible to implement different components of the approval process of autonomous and electric vehicles. To support this objective, ZalaZone has started various research projects in the field of cybersecurity of connected and autonomous vehicles (CAV). The working group, providing the foundational evaluation of the presently applied validation methods and processes, has recognized, that cybersecurity-related testing methods – from a scientific point of view – are slightly detailed in the automobile industry. In a sector-specific term, the lack of a holistic approach seems to be a relevant shortcoming, which may cause a serious barrier to achieve a plausible cybersecurity level, which could be cost-efficiently provided, in light of the available resources. On the other hand, the application of state-of-the-art testing methods is common in the field of informatics [3]. However, they do not necessarily suit the safety and security requirements of the automotive industry.

Following this – summarizing the result of the evaluation carried by the working group of ZalaZone – the paper aims to introduce the most important general cybersecurity approaches, based on the models applied in fundamental robotic systems. As a result of the analysis, new classification categories, and possible synergies between the related scientific fields are going to be introduced and explained. First, the most important research and literature references are presented regarding the investigated scientific field of automobile-related cybersecurity sector.

Eiza et al., give a well-constructed illustration of vehicle network architectures and how different hacking processes can threaten different architectures [4]. Monostori has further developed the concept of cyber-physical production systems and some related research challenges [5]. Khalid and others have given a general description of the cybersecurity characteristics of a collaborative robotic cyber-physical system (CRCPS), and the proposed a general security framework [6]. The study has also stated that there should be an option about CRCPS to change the operation to manual mode if the current industrial scenario makes it necessary. The study written by Khalid and his colleagues, is quite holistic and well-adaptable for the field of autonomous transport systems, since many autonomous transport systems related research studies just ignore important parts of the holistic approach. However, there are still other important system components that should be covered by an overall cybersecurity framework. The overall concept has to aim to cover the whole process network [7] related to the automobile industry and the transportation system. For example, during the formation of vehicle industry related cyber-security framework, the network [8] of the related processes should contain the processes of production, the processes of the operation phase, especially considering mobility, service and reparation processes and technical inspection related processes.

Gratian et al. emphasize that humans are often identified as the weak link in cyber-security, since any system containing human-robot collaboration can be dramatically influenced by human error [9]. For example, as a result of their research, certain social groups differentiated by age, gender, and other demographic property can be characterized by weaker cybersecurity properties. They proved to have less intention of password generation, updating, and proactive awareness. Accordingly, this kind of social groups can be identified as a demographic group needed additional cybersecurity training and guidance [9].

M. Alali et al. present an implementation of a fuzzy-based risk assessment model in cybersecurity, applying a probability approach [10]. However, it has to be emphasized that their study focuses on a very specific slice of the scientific field without aiming to have a holistic approach. In accordance with this, further analysis is required to provide a general interpretation of their research results. Guerrero-Higueras et al. presented in their study, that cyber-attacks on real-time location systems can be protected by a supervised learning detection [11]. Furthermore, they show that some type of cyber-attacks on real time location systems, specifically denial of service and spoofing, can be detected by special machine learning techniques. The paper articulates the importance of sensor proofing in robotics, which should also be adopted by the automobile industry.

Rizvi et al. analyze the denial of service attack and replay attacks within a car network. The study proposes a hybrid security system that consists of multiple security layers [12]. The structure of the study is acceptable, but the general framework of the article is not complete, especially focusing on the partly automated and autonomous vehicles, dispensing with the discussion of the production phase, malicious bug generation, or the importance of sensor disturbance. The paper of De La Torre et al. presents a categorized summary of security methodologies considering secure sensing, positioning, vision, and network technologies that can be equipped in driverless-vehicles [13]. The study is well-adaptable, and the discussed security fields are investigated in a quite detailed manner; however, the connections of the introduced security components are not clarified in a satisfying way. The journal of "Intelligence in Theory and in Practice" introduces a new organizational component in intelligence service which can be involved in the detection, prevention and treating process related to different type of cyberattacks as well. It also introduces the definition of the unknown-unknowns security elements, which can result in significant benefits in the security field. This approach can be efficiently adopted in cyberspace as well, especially in case of automated systems [14].

El Mrabet et al. analyze the basic pillars of cybersecurity, focusing on the classification of cyberattacks, demonstrating the practical applicability of their theory in the case of a smart grid system [15]. They propose a cybersecurity strategy composed of three phases: pre-attack, under attack, and post-attack. The paper includes a description of the relevant published solutions in terms of security protocols, security technology, cryptography, and other cyberattack countermeasures. The study is well adaptable to autonomous transport systems; since many previously formed autonomous transport system related studies ignore the importance of operation management and process analyzing approach. Axon et al. study the application possibilities of blockchain theory in cybersecurity [16]. They provide a detailed and prudential analysis. However, the introduced models are presented through quite specific demonstrations, and therefore general representations of the methods in an overall autonomous vehicle cybersecurity framework would be expedient. This study can exemplify the importance of a common classification framework since without a general reference space, this solution does not seem to be easily applied in other fields of automotive cybersecurity.

Ding et al. give a good insight into the challenges and possibilities of security control and attack detection, which is well adaptable to autonomous transport systems [17]. Mascareñas Stull and Farrar study the conditions and requirements of the precision immobilization technique (PIT) with an autonomous car [18].

Hasrouny, Samhat, Bassil, and Laouiti, present a general overview of the most important security challenges [19] related to vehicular ad-hoc network (VANET) and their causes and current solutions in a general way.

Based on the revealed potential development scopes, the paper aims to unify, join, harmonize, and complement the currently applied cybersecurity framework structure.

Accordingly, the identification of the novel automotive cybersecurity reference space will contribute to the more accurate characterization of cyberattacks. The evaluation of the incidents based on the newly developed reference space makes it possible for security experts to develop more efficient prevention methods and defense mechanisms. In light of this, the scientific aim of the investigation is to test and validate the suggested evaluation factors, especially considering their independence.

In accordance with this, in the next section, the basic methodology of the framework developing process is presented, in the third section, the main result of the framework reconsideration process is summarized, while in the fourth section the components and the related processes are discussed in a more detailed form.

2 Proposed Methodology

To identify the relevant factors for the characterization of the automotive sector related cyberattacks, other relevant related researches are reasonable to be analyzed. Several research studies [20] have already focused on the characterization of different cyberattacks. However, most of these studies [21] have focused on general cyberattack patterns instead of automotive industry related attacks, which reasonably narrow their applicability in case of a certain problem.

On the other hand, it has to be mentioned as well, that the reviewed literature has rather focused on a very specific research problem instead of drawing a more general conclusion regarding automotive industry related attack pattern composition. Researchers have already analyzed incidents according to harmonization, organization, extension, control, thoroughness, purposefulness, and resource demand of the specific cyberattack. [22] Conversely, this kind of study does not evaluate the basic time and space-related properties of event-based approaches [23]. However, time and space-related aspects should be the first step in characterizing malicious cyber-incidents targeting certain parts of the mobility processes. Some of the performed researches take into account spatiotemporal patterns [24] of cyberattacks; however, these researches rather focus on the geographical location and time-dependent predictability of cyberattacks [25]. Contrary to this, to have a more general result, it seems to be reasonable to investigate the relationship of the perpetrator and the target in time and space, since this approach could be applied to characterize the investigated sample on a more general level.

Additionally, it seems to be reasonable to test the strength of the relationship among the evaluation factors to validate their applicability, which final step has been left in most cases. The reason for the emphatic importance of the relationship among the evaluation factors is the possible risk of unfavorable effects, which can influence the conclusions drawn from the analyzed dataset if a strong dependence is identified among the factors.

In accordance with the achieved results, besides other basic evaluation factors like the targeted object or the involved OSI layer, the current research has to focus on the relationship of the perpetrator and the target in time and space and beside this; the selected variables have to be tested with regard to the strength of their relationship. Based on the findings of the research group and the evaluated references, it has been found to be expedient to introduce a new general framework for cybersecurity, which is applicable to distinguish cybersecurity-related issues based on temporal, spatial, and structural aspects. Temporal aspects are investigated in our study by characterizing attacks according to their relationship to past, present, and future. Spatial aspects are evaluated in our paper by defining the relationship of the attacker and the target in space. Structural aspects related to the transportation sector are considered through four main system components: vehicle, production, road infrastructure environment and the targeted OSI layer. In accordance with the considerations mentioned above, this section presents the main concepts behind the developed framework structure. In other words, the below-presented approach can assist the reader in understanding the endpoints of the possible cyber-attack paths and channels that can significantly influence the safety and the security of the road transport system.

2.1 Structural Aspects

In this section, we introduce a novel representation methodology for describing and classifying cybersecurity incidents. This concept makes it possible to analyze new aspects of cyberattacks and analysts should be able to identify new prevention techniques aimed at reducing the risk of specific attack paths that target influencing the operability and safety of transportation processes. Accordingly, the novel representation framework differentiates the vehicle component, the production process, the transportation infrastructure as possible objects of a malicious intervention focusing on the transport system and the importance of the ISO-OSI layers in the current framework. After presenting the most relevant target objects, in the next sections, we introduce the factors of the newly developed reference framework that can be applied to characterize, classify, and evaluate the analyzed attack types.

2.1.1 Vehicle Component

The security and safety level of the road transport system is seriously affected by the operation reliability of the vehicles. Since many vehicular control processes are electronically coordinated in vehicles nowadays, they are equipped with numerous electronic control units (ECU) supervising important vehicle functions [26]. The direct connection required for different services, diagnostic and driver activities is provided by the human-machine interface (HMI) control panel. Processes related to short-range information exchange can be ensured by local area wireless communication (e.g., Bluetooth, WiFi, NFC) units and several different types of sensors, for example, the radar sensor, the LIDAR sensor, the image sensor [12] providing information channels within and between the vehicles and its environment [27]. Wide area networks (e.g., cellular, satellite connection) can ensure the medium of long-range communication and online connection. To handle the cybersecurity system of a vehicle as a whole, - beside the communication, perception and detection components - human factor, the related private data and key database also have to be considered as critical factors in the overall security environment. In accordance with the recommendations of ENISA [28], the complex communication and electronic architecture of modern vehicles are illustrated in Figure 1. However, it has to be emphasized that the detailed description of high-level CAV architecture and external CAV interfaces is not in the focus of this analysis.

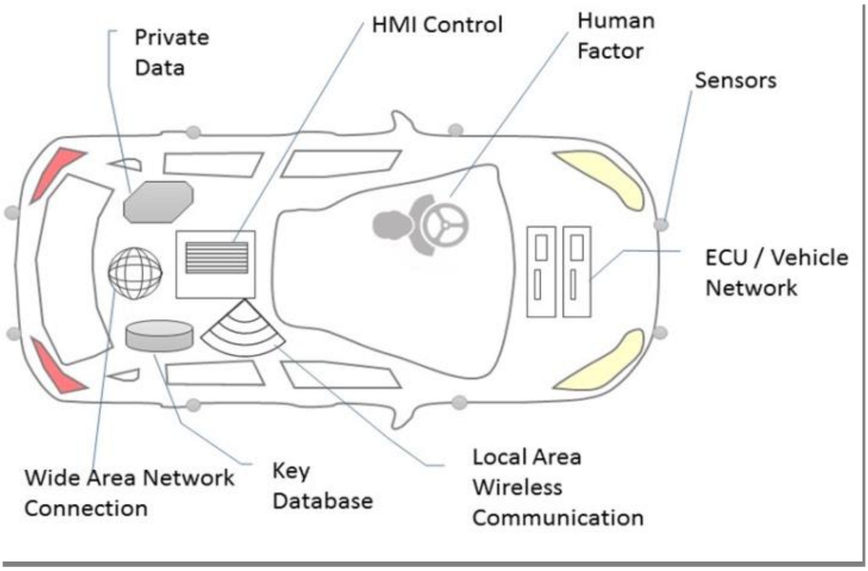

Figure 1
Vehicle components

2.1.2 Production Process Component

It is generally accepted that traditional operation factors and circumstances of connected transportation systems - such as protecting communication channels of connected vehicles, providing the integrity of basic transportation processes, or ensuring reliable authentication methods - influence the cybersecurity of road transport significantly. However, it seems reasonable, to extend the reference space of cybersecurity in the field of transportation, and so, fit the security system to product life-cycle theory. Therefore, cybersecurity-related issues should be investigated during the production phase. Besides this, in the production phase, the human components frequently cooperate with the physical machine components. Thus it is crucial to ensure a safe and secure environment for the production processes. During the production phase, malicious interventions can be implemented by either intruding from the cyberspace or by spoofing sensors at short range or by connecting directly on the internal network. [6].

In the case of a normal operation mode, the control unit receives information from the human and the physical components of the production process by sensing their locations and movements. Besides this, the operating production program can be modified from the cyberspace through a certified and authenticated communication channel. In the next step, information can be processed, and commands can be sent to the actuators and the physical components. Figure 2 illustrates the production process component.

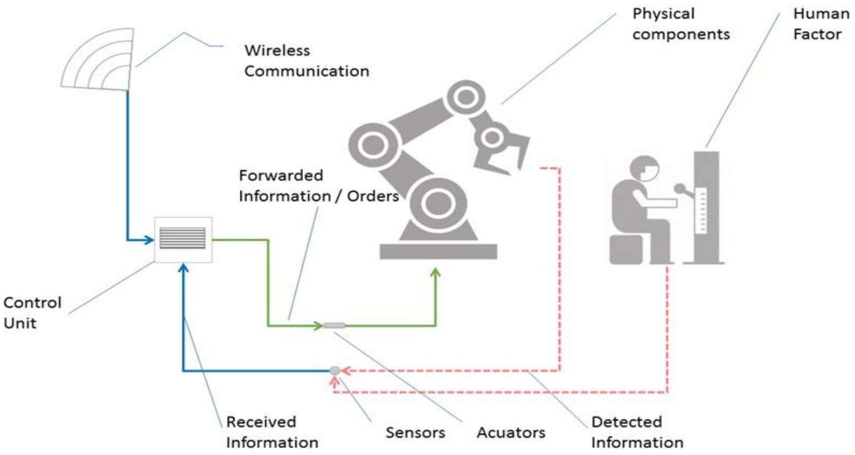

Figure 2
Production process component

2.1.3 Infrastructure Components

As mentioned earlier, ZalaZone has started different research in the field of cybersecurity of connected and autonomous vehicles (CAV). According to the findings of the research group, one of the most efficient components of the protection concept is the reduction of vulnerabilities. This purpose can be significantly supported by improving the ability of the system to protect itself. Beyond the continuous development of protection systems and the adaptation to the latest attack solutions, it is also an extraordinarily important task to inspect the possible and expected effects of relevant cyberattacks. In the automotive industry, in the first part of the inspection, it is more reasonable to perform the demonstrative cyberattacks separately from public traffic, preferably on a test track dedicated to these kinds of tasks, equipped by object-specific modules. ZalaZONE, the Hungarian proving ground, is planned, based on the introduced approach.

Accordingly, the proving ground has several test modules, which can provide a wide range of test circumstances. The concept of the new test track has been developed in accordance with the recommendations of the most important industrial actors and scientific institutions in Hungary. The test track has the technical modules: High-speed oval, Dynamic surface, Braking surfaces, Handling courses, Motorway section, Rural road, Smart City Zone. The proving ground is going to be built on a 260-hectare area from 130 million EUR.

From a cybersecurity point of view, it has to be mentioned, that the proving ground will also provide active test modules including intelligent traffic control [29], V2I communication and cellular 5G communication system, which provides a unique possibility to test different attack channels related to the automated and connected vehicles. Beyond the automotive testing facilities, the test track will be equipped by a special telecom and IT test environment. Besides this, it will also include an automotive cybersecurity test and certification center.

In accordance with the results of the working group, the proving ground will be capable to evaluate the security level of the infrastructure and vehicle connections.

The transportation process's safety and security are strongly affected by cooperative intelligent transport systems (C-ITS) allowing connected and automated vehicles to communicate with each other, with traffic signals, with roadside infrastructure components, and also with other road users. In accordance with this, the road infrastructure is equipped with sensors, detectors, and communication devices, making it possible to collect data from the road environment, traffic and road users as well as to share information with the actors of the transportation process. These components are connected to the cyberspace; they exchange information between each other and send it to the involved parties (traffic organizations, vehicle). Figure 3 illustrates the infrastructure components.

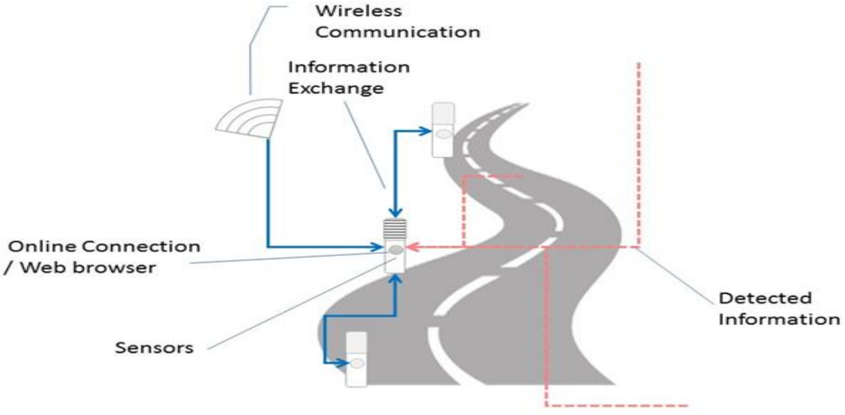

Figure 3
Infrastructure components

2.1.4 Cyberattacks classified based on ISO-OSI Layers related to the Automotive Industry

The definition of open systems interconnection (OSI) model is well known in the field of cyber-sciences. OSI model consists of seven layers. To make the basis and the context of the following conclusions related OSI layers clear, the applied definitions are summarized briefly. The first one is the physical layer, which is responsible for hosting and conveying information. It transforms the binary information codes into physical signals, which can be - among others - radio wave, electrical signals as well as optical signals [30]. The second level is the data link layer performing data transmission between the linked devices. It perceives and, if necessary, repairs failures that is originated from the physical layer. The data link layer determines the protocol to set up and close a connection between two nodes connected physically. The data link layer defines the control between the two connected devices. The third one is the network layer, which is responsible for the process of transmitting different sized data packets. This level provides the capability of the system to be able to connect numerous nodes, ordering addresses to every connected device to be able to send messages to other devices. The transport layer is the fourth level, which makes it possible from a functional point of view to transmit different sized data packets. It is responsible for the reliability of an information channel applying flow control, partition, merging, and failure control. The next level is the session layer, which provides the capability for the system components to be able to establish and coordinate dialogues. The sixth level is the presentation layer, which turns network format into application format and vice versa. The seventh OSI layer is located closest to the human component of the system, and it provides the platform for the direct information exchange between the system and the user involving communicating software components, resource definition, and communication synchronization.

From a cybersecurity point of view, it is important to emphasize that some of the OSI layers do not play a crucial role in reference to the in-vehicle network communication in the conventional term. For example, transport, network, session, and presentation layers are mainly involved in the vehicle's external communication. Therefore, the vulnerability of these layers rather influences the v2x communication processes [31]. The physical layer can unequivocally be differentiated from the other layers of the in-vehicle network. The main vulnerability of this layer regarding the in-vehicle network is the possibility of distracting or preventing the communication with the modification or detachment of the internal network by manipulating the terminating resistors. In case of the data link layer the bitwise modification of the communication frame has to be defined as a serious sensitivity, even if, the protocol controller does not allow such interventions in normal circumstances. The most relevant attack type regarding the network layer can priory affect the v2x communication channels instead of the in-vehicle communication by allocating unexpected extra occupancy influencing the available network bandwidth. The sensitivity of the transport layer can similarly be described as in the previous case since the critical impact can be triggered by making the system reach its capacity constraint. The session layer's typical vulnerability can be exploited through distributed denial of service attacks, which can keep the system from providing switch management processes [32]. The presentation layer can be maliciously influenced by applying modified SSL requests, which can result e.g., in rejecting SSL connection. Regarding the application layer, serious vulnerabilities can be observed in both kinds of networks. Autonomous-transportation related communication processes are reasonably data-sensitive, which means that the malformed, spoofed, or maliciously generated data can cause significant hazards. Accordingly, the information gained from environment sensing (e.g., RADAR signal), dynamic data utilization (e.g., GNSS signal), static data utilization (e.g., HD mapping) or V2X communication channels have to be handled by considering strict confidence rules and reliable risk estimation processes.

Table 1

Cyber-incident relevancy in light of the targeted OSI layer

	Relevant External Accessibility		Considerable External Accessibility		Limited External Accessibility		
OSI Layer	LAN Conn.	WAN Conn.	Sensors/ Actuators	HMI Ctrl	ECU	Private Data	Key Datab.
App.	High	High	Medium	High	High	Medium	High
Pres.	High	High	Low	Low	n/a	Low	Low
Sess.	Medium	Medium	Low	Low	n/a	Low	Low
Transp.t	Medium	Medium	Low	Low	n/a	Low	Low
Net.	Medium	Medium	Low	Low	n/a	Low	Low
Data	Medium	Medium	Low	Medium	Medium	Medium	Average
Phys.	Low	Low	High	High	Medium	Medium	Average

As presented in Table 1, it can be concluded that channels characterized by relevant external network accessibility are more sensitive to network processes occurring in the higher OSI layers, since these processes can directly affect their operational efficiency.

On the other hand, vehicle components responsible for in-vehicle communication or one-directional data surveying are less sensitive to incidents, which target OSI layers located in the middle part of the table. This structure of the table can be explained based on the in-vehicle communication network framework, where transport, network, session, and presentation layers do not play an emphatic role in the communication process.

2.2 Spatial Aspects of Cyber-Attacks

Incidents intending to influence vehicle operation processes can be classified in three different groups based on their spatial characteristics. Incidents carried out through a direct connection can be ordered to the class of direct local attacks. Malicious interventions implemented at short range, for example, through Bluetooth, CALM, or DSRC can be classified into the group of indirect local attacks. Cyberattacks performed and coordinated remotely is classified in the group of remote attacks. The spatial aspects of different cyberattack types are demonstrated in Figure 4.

According to the aforementioned distinctions, the following figure represents the three different attack methods. In the first part of Figure 4 (a), the attacker (blue) is situated in the immediate surrounding area of the target (yellow) and has a direct connection to the specific object. In the second part of Figure 4 (b), the perpetrator (blue) is located considerably close to the target (yellow), but the object and attacker are connected through an indirect, wireless channel with each other. In the third case (c), the attacker is located considerably further from the target. Accordingly, the perpetrator has to use an indirect, remote channel to reach the target.

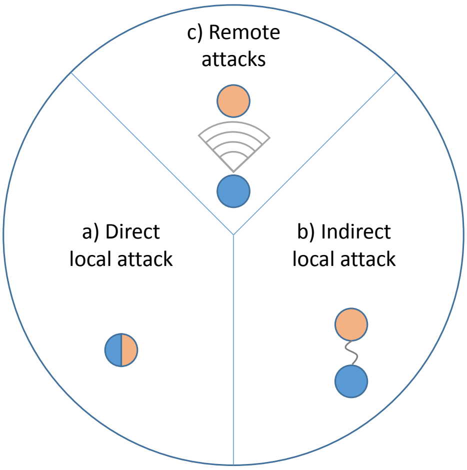

Figure 4
Spatial Aspects of Cyber-Attacks

2.3 Periodic and Time Related Aspects of Cyber Attacks

Preparation, implementation, and infection of malicious cyber-incidents may have different relations with the influenced transport process in time. A cyber incident can aim to affect stored, or archived data describing a process or activity carried out in the past. In this case, the object of the attack is a terminated occurrence; however even in this case, the target of the incident has significant effects on certain presently operating processes. Summing up, these kinds of attacks refer to a terminated occurrence. Hence, these malicious interventions are classified as cyberattacks targeting processes terminated in the past.

Of course, cyber-incidents can influence processes occurring presently. In this case, the prior objective of the malicious intervention is to modify the normal, safe operation of a system, mainly causing hazards affecting the integrity of safety, security, or data or, in some cases, public confidence negatively. The risks related to moving away from the safety state have been properly discussed in functional safety related research. Recently the scientific society completely accepted that these risks have to be treated emphatically in the applied analytical system engineering methods as mentioned for example by Sebron et al. [33].

Cyber incidents focusing on the infection of a process being implemented in the future can be similarly described as cyberattacks targeting processes being implemented in the present. These kinds of cyber incidents also aim to divert the targeted process from a safe and secure state, violating the required conditions of safety, security, privacy or possibly public confidence. However, the objective of this kind of malicious intervention is going to be realized in the future.

Besides the introduced time-related aspects of a given cyber incident, periodicity should also be discussed as an important property of the attacks implemented in the cyberspace. In the case of periodicity, the study differentiates three main clusters. A malicious intervention may affect the target as a one-time incident. Thus this type of incident is classified as single cyberattacks. A cyber-incident can influence its objective several times; repeatedly, this type of intervention is classified as multiple cyberattacks. Finally, there are incidents that aim to generate infection focusing on the target object continuously in a given interval.

In light of the introduced time-based representation of cyberattacks, the next figure represents the different relationships of the time and the cyberattacks. In accordance with this, compared to the perceived result of the interventions, attacks can be implemented in the past, in the present, and in the future. Thus, the perpetrator in the present (indicated by a blue dot on the time axis) can implement malicious intervention targeting a process in the past (Figure 5 a) in the present (Figure 5 b) or in the future (Figure 5 c). considering the periodic aspects of the attack, the perpetrator can perform the attack through a single (Figure 5 I), a multiple (Figure 5 II), or a continuous (Figure 5 III) intervention.

Periodic and Time-Related Aspects of Cyber Attacks are presented by the following figure.

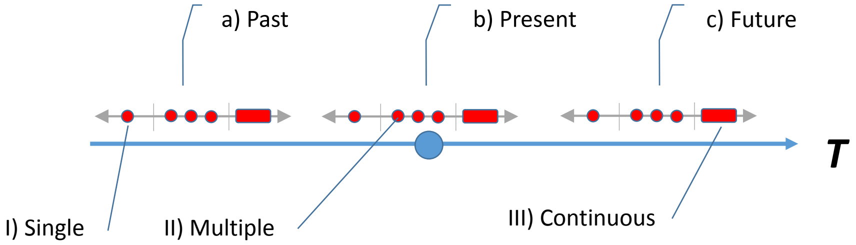

Figure 5
Periodic and Time Related Aspects of Cyber Attacks

3 Quantitative Validation of the Proposed Method

Cyberattacks mean a permanently intensifying threat to mobility processes, especially considering the spread of connected vehicles in road transportation [34]. The more accurate characterization of the discovered cyberattacks is essential for preparing an efficient prevention strategy against the different interventions. This rather risky competition has already stepped beyond the borders of the cyberspace. Hence prevention also needs to cover more and more phases of the activities related to cyberattacks. This concept is also in accordance with the approach of defense strategy identification [14]. Accordingly, it is reasonably important to gain as much information on the circumstances of the attacks as possible, including the targeted object, the spatial and time related aspects and the technical characteristics of the attack. Based on this consideration, the paper aims to build up a new cyberattack reference space framework constructed from the mentioned factors. In accordance with this, an important aim of this study is to analyze whether the new framework is applicable to properly characterize the cyberattacks in a comprehensive way or the suggested variables are not adequate to provide the required information without a significant amount of latent information overlapping.

To validate the new concept, based on practical experiments, a complex analytical framework has been developed to prove that the main elements of the reference space theorem (component, space, time, periodicity and OSI layer related properties) are applicable to characterize automotive industry related cyberattacks.

To do so, a complex database has been built, based on the data of Upstream Security [35] containing all the registered automotive industry related attacks performed during last twelvemonth. Following this, the registered attacks have been individually analyzed, and the data of the certain interventions have been defined containing the attacked component of the mobility system, the space, time and periodicity aspects of the specific attacks, the targeted OSI layer and the estimated cyber incident priority level [36] of the given intervention

In the next step, the applicability of the developed reference space is evaluated by analyzing the independence of the identified attributes. According to the applied assumption, if the reference space contains only such factors that cannot be explained by some of the other basic factors, then the newly developed representation framework includes only a marginal amount of overlapping information. Contrary to this, if the dependency among the applied attributes is strong, then the developed reference space cannot be accepted as a proper framework applicable to support the description of prior and latent relationships, tendencies, and patterns characterizing cyberattacks.

Since the introduced factors can be described as categorical variables, their dependency can be characterized by the application of the traditional Chi-Square test [37]. The independence of the investigated factors is analyzed through a pairwise comparison. Accordingly, every investigated factor has been compared to all the other factors in a pairwise evaluation. In the first step of the analysis, in case of a certain pairwise comparison, the relative frequencies related to the expected values of the independent scenario are calculated based on the below-presented equation:

$$f'_{ij} = \frac{\sum_i f_{ij} \cdot \sum_j f_{ij}}{(\sum_i f_{ij})^2} \tag{1}$$

Where,

i : is the index number of the nominal attributes representing the first categorical variable in case of the certain pairwise comparison;

j : is the index number of the nominal attributes representing the second categorical variable in case of the certain pairwise comparison;

fij : is the number of objects, characterized by attribute

f 'ij : is the expected number of objects in case of independence

After defining the independent case, it is possible to define the value of the test function, which can be defined by the following formula:

$$X^2 = \frac{(f_{ij}\text{-}f'_{ij})^2}{f'_{ij} \cdot \sum_{ij} f_{ij}} \tag{2}$$

If the investigated factor pairs are not independent, the strength of the association plays a key role in defining whether the two factors can be explained by each other. Therefore, the Cramer association coefficient is defined to evaluate the dependence.

$$C = \frac{X^2}{r \cdot \sum_{ij} f_{ij}} \tag{3}$$

Where,

r : is the smaller value from the number of rows reduced by one or the number of columns reduced by one;

In the case of dependence, the stronger the association between the analyzed factor pairs, the more significant information redundancy can be expected, which queries the applicability of the new reference space representation.

4 Results

During the evaluation, the factors regarding component, space, time, periodicity, and OSI layers related aspects have been pairwise compared by applying the Chi-square test. Accordingly, in the first step, the component factor, so the attacked component of the mobility system and the space-related aspects have been compared.

In the next step, the absolute frequencies related to the categories of the investigated nominal variables have been summarized by the contingency table below.

Table 2

Frequency data of the classified cyberattack sample

	Direct local attack	Indirect local attack	Remote Attack	Sum
Infrastructure	0	0	11	11
Production	1	0	4	5
Vehicle	9	44	8	61
Sum	10	44	23	77

Based on the absolute frequency values, it is possible to define the relative frequencies of the independent scenario, as follows.

Table 3

Relative frequency data of the classified cyberattack sample

	Direct local attack	Indirect local attack	Remote Attack
Infrastructure	0.019	0.082	0.043
Production	0.008	0.037	0.019
Vehicle	0.103	0.453	0.237

From the derived results, it is now possible to determine the elements of the X2 value, represented by the table below.

Table 4

Elements of the X2 value

	Direct local attack	Indirect local attack	Remote Attack
Infrastructure	1.429	6.286	18.112
Production	0.189	2.857	4.207
Vehicle	0.147	2.398	5.733

From this, it can be concluded that the value of the X^2 test is 41.36. The critical value of the given association concerning the degree of freedom of the problem is

0.091. The result is significant at $p < 0.05$; the two evaluated variables are not independent.

According to the introduced methodology, the next step is to identify the value of the Cramer association coefficient. If the association is proved to be strong, then the applicability of the new framework cannot be validated.

$$C = \sqrt{(41.36/2.77)} = 0.51 \tag{4}$$

Based on the performed calculation, the association between the components of the mobility system and the space-related aspects are proved to be moderate, which is higher than expected but still does not unequivocally queries the conformance of the introduced space reference approach.

To complete the investigation, all the factors have been compared, and in accordance with this, the result of the pairwise comparison is represented by the following table. Furthermore, the average value of the calculated coefficients has been defined related to certain variables to represent the average dependence of the specific factors.

Table 5

Comparison of the X2 values resulted by the association analysis

	Comp.	Spatial aspects	Timer related aspects	Period.	OSI	Aver.
Comp.	-	0.52	0.31	0.35	0.53	0.43
Spatial aspects	0.52	-	0.26	0.21	0.6	0.4
Timer related aspects	0.31	0.26	-	0.31	0.22	0.28
Period.	0.35	0.21	0.31	-	0.63	0.38
OSI	0.53	0.6	0.22	0.63	-	0.5

As observed, the results are more or less acceptable but still not completely satisfactory. However, if the output data is analyzed a little more detailed, it can be observed that variable related to the aspects of the OSI layers is represented by significantly higher association coefficients. If this variable is excluded from the comparison the results are much more convincing.

Table 6

Comparison of the X2 value resulted by the rationalized association analysis

	Comp.	Spatial aspects	Timer related aspects	Period.	Average without OSI
Comp.	-	0.518	0.313	0.346	0.392
Spatial aspects	0.518	-	0.262	0.213	0.331

Timer related aspects	0.313	0.262	-	0.309	0.295
Period.	0.346	0.213	0.309	-	0.289

According to the final results, the average values of the Cramer association coefficients are below 0.4, the investigated variables are dependent however the associations of the factors are weak moderate. This level of dependency can be expected in accordance with our baseline consideration, therefor cyber incidents are recommended to be characterized by the attacked component of the mobility system, the spatial, the time related, and the periodicity related aspects of the intervention.

Based on the evaluation of the applied classification approaches, it can be concluded that the different, more or less isolated segments of transport systems - including vehicles, production processes, connected infrastructure components, as well as, human factors - cannot answer all the cybersecurity related challenges by themselves. The reason for this is the significant probability related to the security risk of the high relevancy cyber-incidents targeting the transport sector as a whole.

To give an adequate answer to these issues it seems to be expedient to define the security requirements of the introduced components in light of their effect on the defensive competencies of the whole system.

In accordance with the above mentioned considerations it can be concluded that the introduced holistic aspects of cybersecurity related systems make it necessary to introduce a complex time, space and component based automobile industry related cyberattacks reference space. The newly introduced space is applicable to classify and represent different types of cyber-incidents, which allows us in the future to improve sector and threat specific cybersecurity solutions and to improve the efficiency of risk rate estimation.

Accordingly, we can classify the cyberattacks performed in the automotive sector in a three-dimensional reference space, where incidents can be characterized based on the type of targeted system component, the spatial relationship between the attacker and the target, and time and periodic aspects of the investigated intervention.

Where:

S axis represents the spatial relationship of the attacker and the target, including:

a) direct, local

b) indirect, local

c) indirect, remote attacks

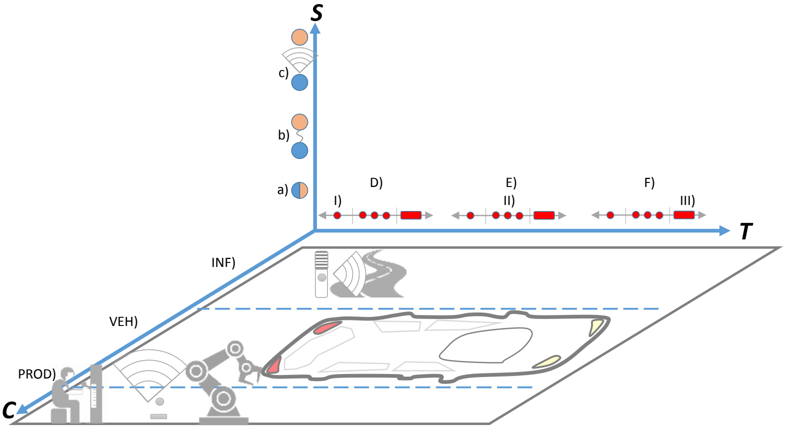

Figure 6
Time, space and component based automobile industry related cyberattack space

T axis represents the time and periodic aspects of the incident, including:

D) the attacker targets to influence a data describing a process in the past

E) the attacker targets to influence a data describing a process in the present

F) the attacker targets to influence a data describing a process in the future

I) the perpetrator performs the attack through a single intervention

II) the perpetrator performs the attack through multiple interventions

III) the perpetrator performs the attack through a continuous intervention

C axis represents the considered components of the transport system:

INF) the transport infrastructure

VEH) the moving unit of the system

PROD) the manufacturer of the system components.

As the main result of our concept, threats related to connected vehicles can also be classified based on the targeted OSI layer. However, while the introduced time, space and component related aspects, depend on the properties of the targeted process or object, the classification of cyber-incidents based on OSI layers is influenced by the type of the attack [38]. This approach can efficiently support the definition of the adequate protection concept; though, the detailed discussion of defensive strategies from a technical point of view does not comprise the subject of the study.

5 Discussion

Based on the reconsidered reference space of cyber-incidents, attacks can be classified based on their reference to the properties of the target. The evaluated system component, the time- and space-like properties of the investigated processes restrict the set of possibly relevant attack types. Accordingly, the typical characteristics of diverse attack types, can significantly vary from each other, strongly influencing the set of efficiently applicable defensive strategies.

Therefore, in the next step, the assumed profile of the possible perpetrators and targeted processes is defined based on the combination of the investigated classification factors. In light of the introduced classification factors (component, time, space) different motivations and objectives can be found behind the certain attack-types, their understanding might be critical in defining the adequate protection concept.

As the intelligence expert has summarized, the importance of understanding the surrounding world is crucial, from a security point of view. Therefore, conceptualization is a basic step in the process of defense strategy definition [14]. In other words, an effective and realistic representation of the expected security threats, can significantly improve our chance to apply the suitable prevention method. The clearer and more reliable the information we have about the security factors influencing the integrity of our system, the more an efficient prevention and reaction can be provided for the defense. To form a realistic model describing the security space of the environment, in which our system is located, it is relevant to specify the most important information gaps, which can be transformed into direct security questions. These predetermined security questions can be defined as the known-unknown components of the defense strategy. It is also substantially important to continuously provide a validation feedback about the information gained from the real world towards the model framework. This process is responsible for ensuring information about the space being uncovered by the constructed security strategy. In other words, the purpose of this system component is to answer questions which have not been asked yet. This approach can help us to detect the, so-called, unknown-unknown components of the security environment.

In view of the introduced conceptualization framework, the clear representation of motivations and objectives related to certain cyberattack types is considered to be primarily significant. Accordingly, in the next step, certain cyberattack class profiles are presented based on the combination of the introduced classification factors (component, time, space). Based on the introduced aspects related to cyber-attacks it is necessary to re-consider the traditionally applied reference-space in the field of automated vehicles related cyber-attack classification.

Introduction of Certain Cyberattacks Profiles Represented in the New Reference Space.

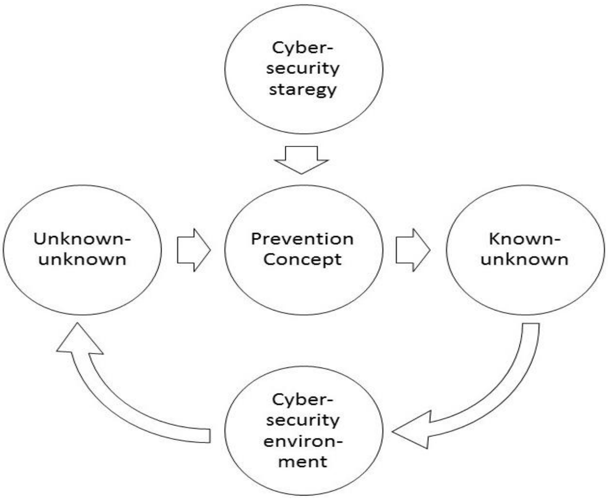

Figure 7

Conceptualization framework of cybersecurity related system

Investigating incidents in terms of time, attacks are classified into three main groups. Malicious interventions aiming to modify the recorded data of an object or process terminated in the past is classified in the first group. Influencing data related to an object or process recorded in the past can be important for attackers, due to its effect on present processes. The affected target group frequently involves specific official cases depending on data registered in official records or certain processes, which are subject to authorization. For example, in the transport sector, data of sales and purchase contract related processes, criminal cases related data or permission required activities are typical target objects of incidents intending to modify the official dataset recorded in the past. Cyberattacks performed in the present focusing on an object or processes influencing a real-time activity are ordered to the second group. This category of cyberattacks can affect a wide spectrum of the possible target objects or processes. Incidents characterized by this kind of validity period frequently aim at everyday life related processes like shopping, transportation or banking. Incidents influencing a future process or a future state of an object related to the attacked target are classified in the third group. Malicious interventions aiming to influence a process or an object in the future require well-founded, usually extremely well-founded and careful preparation. This kind of incidents are implemented frequently in an early stage of the affected project, not rarely during the strategic, planning or implementation phase. Cyber-incidents, which aim to affect a process or an object in the distant future, due to their significant resource demanding characteristic, often influence safety and security critical systems or processes strongly affecting national-security level. To discuss the characteristics and the main objective of the different attack types in light of periodicity, it is useful to form a realistic profiles related to the possible perpetrators. One-time cyber-incidents characterized as a single attack in time can involve quick intrusions targeting for example well protected objects to violate privacy or abstract private, public or national data. In case of a multi-time incidents, attacker can assume that the previously implemented interventions have not been detected. This means that the perpetrator estimates the differences between competencies to be significant, so interventions can be repeated several times without the risk of being discovered. Attacks carried out as continuous intervention, are often implemented to influence strongly safety critical systems by moving system state from safe and secured operational circumstances to a high risk operational domain [39]. These kind of incidents can be implemented for example by denial-of-service attacks in which the attacker aims to make a system resource ineffectual to the regular user for instance by flooding it from different sources [40].

Characterizing attacks based on their spatial relationship to the target, incidents are grouped in three classes. Cyber-incidents aiming to move a system from the safe and secured state, to violate privacy or private data through a direct connection, influencing the system from inside mean a reasonably challenging security issue. The reason for this is the undercover component of the attack, which may provide reliable information on the main vulnerabilities of the targeted system and can make the weak points of the defense strategy available for the attacker. This type of intervention might be based in numerous cases on a long-winded preparation process, hence this type of attack can rather be related to safety and security critical systems or processes, which may strongly affect national-security level. Cyber-incidents carried out through an indirect connection from the surrounding environment can be implemented by the application of one directional channels (e.g. influencing sensors or detectors) or by the application of bi- or multi-directional communication channels. This kind of cyberattacks can involve different sensor-spoofing interventions or incidents using the local area communication network. This group of cyberattacks frequently affects real-time, everyday life related processes, like shopping, transportation or banking. Remotely controlled attacks, which impact targets through the WAN (Wide Area Network) can influence almost all systems characterized by almost all kinds of dimensions and complexities.

To introduce the component based classification of cyberattacks, three main groups have been differentiated in the field of transportation related malicious interventions. Attacks aiming to influence the road infrastructure related system components can principally affect road traffic [41] either from a safety or from an efficiency point of view. These kinds of incidents can have an impact on a wide spectrum of traffic related parameters or factors, such as, speed, emission, unexpected events, accidents, bottlenecks, network vulnerability or emergency reaction performance. Incidents targeting the production component might aim to violate directly the safety or security integrity of the manufacturing process or the reliability of the type approval process [42]. In addition, attacks can influence the latter operation phase of the vehicle, affecting their safety characteristics or the conformance to their approved properties. This kind of incident can be well exemplified by the malicious modification of vehicles emission characteristics aiming to improve their performance. Malicious interventions related to the vehicle components mainly influence, directly, the transportation process. This kind of attack involve either the ramping of the decision making methods of the vehicle, by transmitting modified information to it, or the intrusion into the vehicle control unit network, taking control of the vehicle, stealing or modifying the private information related to the vehicle.

Conclusion

As observed, around the world, vehicle technology is continuously developing. This development results in numerous, challenging and novel questions, in reference to transport system security.

Accordingly, summing up the provided output, related to the investigation coordinated by ZalaZone, this work introduces the most relevant cybersecurity methodologies, based on the approaches used in the field of robotics and automation. First, the paper clarifies the applied definitions, the used models and the most relevant tendencies of the scientific community. Based on the investigation, the newly prepared classification theory and its benefits are interpreted in a detailed way. In the first section of this paper, the most relevant research results are introduced, as related to cybersecurity, in the Automotive Industry.

On the basis of the reviewed literature, it has been concluded that a new cybersecurity reference space has to be introduced, based on the discussed temporal, spatial and structural aspects. Accordingly, the next section of the paper presents the main ideas behind the developed architecture. Based on a novel method, the result of the different cyberattacks types can be highlighted from different point of views, which can substantially influence the safety and the security of the road transport system.

On the basis of the investigated classification methods, it can be summarized, that the different components of the transportation systems are not able to adequately reply all of the cybersecurity related questions by themselves.

On the contrary, the security system of transportation should be handled as a whole entity.

In conjunction with this and in accordance with the final results of the proposed validation method, cyberattacks are recommended to be characterized by the attacked component of the mobility system, the spatial, the time related and/or the periodicity related aspects of the intervention.

Furthermore, as a main output of this paper, hazarding factors, targeting autonomous transportation systems can be grouped based on the OSI layer. On the one hand, targeted systems can be classified based on the developed time, space and component dependent reference space, while on the other hand, attack paths and channels can be differentiated based on OSI layers.

To summarize the article's achievements, we can state, that our work herein, has managed to harmonize and complement the currently applied cybersecurity framework structure. Also, we have identified a novel automotive cybersecurity reference space, which contributes to a more accurate characterization of cyberattacks. The evaluation of incidents based on the newly developed reference space, makes it possible for security experts to develop more efficient prevention methods and defense mechanisms. In light of this, the investigation's scientific aim has been fulfilled through the validation of the suggested evaluation factors, particularly considering their independence.

Acknowledgement

The research reported in this paper was supported by the Higher Education Excellence Program of the Ministry of Human Capacities in the frame of Artificial Intelligence research area of Budapest University of Technology and Economics (BME FIKP-MI/FM).

The research reported in this paper was supported HAS (Hungarian Academy of Science) for providing the Janos BOLAYI Scholarship. Moreover, the authors are grateful for the support of New National Excellence Programme Bolyai+ scholarship.

References

[1] Macher, G., Armengaud, E., Kreiner, C., Brenner, E., Schmittner, C., Ma, Z., Martin, H., Krammer, M. (2018) Integration of security in the development lifecycle of dependable automotive CPS. In Solutions for Cyber-Physical Systems Ubiquity (pp. 383-423) IGI Global

[2] Szalay, Z., Tettamanti, T., Esztergár-Kiss, D., Varga, I., & Bartolini, C. (2018) Development of a Test Track for Driverless Cars: Vehicle Design, Track Configuration, and Liability Considerations. Periodica Polytechnica Transportation Engineering, 46(1), 29-35

[3] Hasanain, W., Labiche, Y., & Eldh, S. (2018, July) An Analysis of Complex Industrial Test Code Using Clone Analysis. In 2018 IEEE International Conference on Software Quality, Reliability and Security (QRS) (pp. 482-489) IEEE

[4] Eiza, M. H., & Ni, Q. (2017) Driving with sharks: Rethinking connected vehicles with vehicle cybersecurity. IEEE Vehicular Technology Magazine, 12(2), 45-51

[5] Monostori, L. (2014) Cyber-physical production systems: Roots, expectations and R&D challenges. Procedia Cirp, 17, 9-13

[6] Khalid, A., Kirisci, P., Khan, Z. H., Ghrairi, Z., Thoben, K. D., & Pannek, J. (2018) Security framework for industrial collaborative robotic cyber-physical systems. Computers in Industry, 97, 132-145

[7] Kreiner, C., & Messnarz, R. (2018) Effective Approaches to Training CPS Knowledge and Skills. In Solutions for Cyber-Physical Systems Ubiquity (pp. 111-135) IGI Global

[8] Jaskolka, J., & Villasenor, J. (2017) Identifying implicit component interactions in distributed cyber-physical systems

[9] Gratian, M., Bandi, S., Cukier, M., Dykstra, J., & Ginther, A. (2018) Correlating human traits and cyber security behavior intentions. computers & security, 73, 345-358

[10] Alali, M., Almogren, A., Hassan, M. M., Rassan, I. A., & Bhuiyan, M. Z. A. (2018) Improving risk assessment model of cyber security using fuzzy logic inference system. Computers & Security, 74, 323-339

[11] Guerrero-Higueras, Á. M., DeCastro-Garcia, N., & Matellan, V. (2018) Detection of Cyber-attacks to indoor real time localization systems for autonomous robots. Robotics and Autonomous Systems, 99, 75-83

[12] Rizvi, S., Willet, J., Perino, D., Marasco, S., & Condo, C. (2017) A Threat to Vehicular Cyber Security and the Urgency for Correction. Procedia Computer Science, 114, 100-105

[13] De La Torre, G., Rad, P., & Choo, K. K. R. (2018) Driverless vehicle security: Challenges and future research opportunities. Future Generation Computer Systems

[14] Intelligence In Theory And In Practice (2017) Joint Investigation Teams as a Response to the Big-Data Era: The Test of Practice

[15] El Mrabet, Z., Kaabouch, N., El Ghazi, H., & El Ghazi, H. (2018) Cyber-security in smart grid: Survey and challenges. Computers & Electrical Engineering, 67, 469-482

[16] Axon, L., Goldsmith, M., & Creese, S. (2018) Privacy Requirements in Cybersecurity Applications of Blockchain

[17] Ding, D., Han, Q. L., Xiang, Y., Ge, X., & Zhang, X. M. (2018) A survey on security control and attack detection for industrial cyber-physical systems. Neurocomputing, 275, 1674-1683

[18] Mascareñas D. L., D., Stull J., C., Farrar R. Ch. (2017) Autonomous execution of the Precision Immobilization Technique. Mechanical Systems and Signal Processing. 87, 153-168

[19] Hasrouny, H., Samhat, A. E., Bassil C., Laouiti, A. (2017) VANet security challenges and solutions: A survey. Vehicular Communications 7, 7-20

[20] Fava, D. (2007) Characterization of cyber attacks through variable length markov models

[21] Du, H., Liu, D. F., Holsopple, J., & Yang, S. J. (2010, August) Toward ensemble characterization and projection of multistage cyber attacks. In 2010 Proceedings of 19th International Conference on Computer Communications and Networks (pp. 1-8) IEEE

[22] Uma, M., & Padmavathi, G. (2013) A Survey on Various Cyber Attacks and their Classification. IJ Network Security, 15(5), 390-396

[23] Beard, K. (2006) Modelling change in space and time: an event-based approach. In Dynamic and Mobile GIS (pp. 83-104) CRC Press

[24] Jennifer, L., & Soor, S. (2018) Spatial and Temporal Patterns of Cyberattacks: Effective CYBERCRIME Prevention Strategies around the Globe

[25] Chen, Y. Z., Huang, Z. G., Xu, S., & Lai, Y. C. (2015) Spatiotemporal patterns and predictability of cyberattacks. PloS one, 10(5), e0124472

[26] SAE Vehicle Electrical System Security Committee. (2016) SAE J3061-Cybersecurity Guidebook for Cyber-Physical Automotive Systems. SAE-Society of Automotive Engineers

[27] Boštjančič Rakas, S., & Stojanović, M. (2019) A centralized model for establishing end-to-end communication services via management agents. Promet-Traffic&Transportation, 31(3), 245-255

[28] ENISA (2016): Cyber Security and Resilience of smart cars

[29] Olojede, O., Daramola, O., & Olufemi, B. (2017) Metropolitan transport safety and security: An African experience. Journal of Transportation Safety & Security, 9(4), 383-402

[30] Abedi, M. R., Mokari, N., Saeedi, H., & Yanikomeroglu, H. (2017) Robust resource allocation to enhance physical layer security in systems with full-duplex receivers: Active adversary. IEEE Transactions on Wireless Communications, 16(2), 885-899

[31] Iacovazzi, A., & Elovici, Y. (2017) Network flow watermarking: A survey. IEEE Communications Sfurveys & Tutorials, 19(1), 512-530

[32] Yan, Q., Huang, W., Luo, X., Gong, Q., & Yu, F. R. (2018) A multi-level DDoS mitigation framework for the industrial Internet of things. IEEE Communications Magazine, 56(2), 30-36

[33] Sebron, W., Tschürtz, H., & Krebs, P. (2018, September) The Shell Model– A Method for System Boundary Analysis. In European Conference on Software Process Improvement (pp. 68-79) Springer, Cham

[34] Lee, U., Jung, J., Jung, S., & Shim, D. H. (2018) Development of a self-driving car that can handle the adverse weather. International journal of automotive technology, 19(1), 191-197

[35] Upstream Security (2019) Upstream Security Global Automotive Cybersecurity Report, https://www.upstream.auto/

[36] NCCICI (2014) NCCIC Cyber Incident Scoring System. https://www.us-cert.gov/sites/default/files/publications/NCCIC_Cyber_Incident_Scoring_System.pdf

[37] Pearson, K. (1900) X. On the criterion that a given system of deviations from the probable in the case of a correlated system of variables is such that it can be reasonably supposed to have arisen from random sampling. The London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science, 50(302) 157-175

[38] Rosenberg, I., Shabtai, A., Rokach, L., & Elovici, Y. (2017) Generic black-box end-to-end attack against rnns and other api calls based malware classifiers. arXiv preprint arXiv:1707.05970

[39] Jelacic, B., Lendak, I., Stoja, S., Stanojevic, M., & Rosic, D. (2020) Security Risk Assessment-based Cloud Migration Methodology for Smart Grid OT Services. Acta Polytechnica Hungarica, 17(5), 113-134

[40] Chovancová, Eva, and Norbert Ádám. "A Clustered Hybrid Honeypot Architecture." Acta Polytechnica Hungarica 16.10 (2019)

[41] Li, S., Cao, D., Wu, J., Sun, T., & Dang, W. (2018) Traffic state evaluation and intersection-movement-based incidents detection of expressway network. Journal of Transportation Safety & Security, 1-19

[42] Zöldy M. (2018) Investigation of Autonomous Vehicles fit into Traditional Type Approval Process, Procedings of ICTTE 2018 Beograde, pp. 428-432