Investigating Safety Effects of PKI Authentication, in Automotive Systems

Zsombor Pethő[1], Tamás Márton Kazár[1], Roland Kraudy[2], Zsolt Szalay[1] and Árpád Török[1]

[1] Department of Automotive Technologies, Budapest University of Technology and Economics, Műegyetem rkp. 3, 1111 Budapest, Hungary; E-mail: zsombor.petho@edu.bme.hu, kazar.tamas@kjk.bme.hu, szalay.zsolt@kjk.bme.hu, torok.arpad@kjk.bme.hu

[2] Microsec Software Management and Consulting ltd., Ángel Sanz Briz út 13, 1033 Budapest, Hungary; E-mail: roland.kraudy@microsec.com

Abstract: Our study analyses the safety effects of Public Key Infrastructure (PKI), based authentication mated, related to certain wireless communication based automotive functions. The first part of the article focuses on quantifying the safety effect of quality of service (QoS) parameters in the case of wireless communication based automotive functions. Based on this concept, the paper discusses two scenarios: in the first case, there is no authentication process applied during the communication, and in the second case, the communication is secured by PKI authentication. This concept allows us to evaluate the safety effect of the security overhead caused by the additional computation demand related to the authentication process. Considering the results of our research, it becomes possible to define the requirements and expected conditions, regarding the operational circumstances.

Keywords: automotive safety; public key infrastructure; safety risk; V2X; network performance

1 Introduction

Our paper aims to evaluate how Public Key Infrastructure-based security solutions (PKI) affect communication service quality and, thus, traffic safety. The reason why we need to analyze the PKI authentication process in detail is the fact that the available computational resources of the automotive systems are limited. Therefore, we need to find an acceptable trade-off between allocating our resources to improve the functionality and safety of the coordinated automotive applications or increasing the security of our system [1] [2]. Wireless communication between the components of the transportation system (e.g., vehicles, pedestrians, central management system, etc.) can significantly contribute to improving safety [3] [4] since the actors

of the cooperative intelligent transportation systems (C-ITS) will be able to exchange real-time information on their positions, velocities, accelerations, and planned trajectories. In certain cases, this information can be available sooner than the data collected by an environment perception module, especially in the case of some non-line-of-sight scenarios, where other sensor systems cannot detect the other actors in time.

Different types of messages exist in cooperative, connected and automated mobility (CCAM) systems that contain data used by safety-related applications. Cooperative Awareness Message (CAM) is a widely used massage type that contains information on the vehicle's position and dynamics parameters by default. Therefore, it is well applicable for safety-related purposes [5].

To prevent malicious actors from joining the communication related to CCAM processes, the system must be capable of checking the authorization of the participants. CCAM systems use the PKI security solution to ensure authenticated, reliable communication, especially considering non-repudiation, integrity, and the freshness of the messages. X.509 PKI frameworks apply digital signatures, timestamps, hash functions and pseudonym certificates to sign messages. This provides both authenticity for CAMs and privacy for the users since the end-user identities do not contain any identifying data. Furthermore, the different authorization levels of CCAM system actors (such as police or normal driver) must also be handled. This results in further computational tasks that need to be performed beyond the processes of the classical automotive functions.

If it is not possible to assign additional computational capacity, the PKI authentication process can increase the delay / latency of the message transfer process. In everyday traffic scenarios, the extra computational demand needed for the authentication does not cause any difficulties since efficient algorithms (such as ECC – Elliptic Curve Cryptography) and application-specific hardware components support the procedure.

However, for example in case of sub-optimal network performance even the slight overhead introduced by PKI authentication can affect the system’s ability to appropriately assess a safety-critical situation and react to it in time.

Therefore, the trade-off must be considered during the automotive development processes to find an optimal balance between safety and security [6] [7], especially considering automotive functions influencing high-risk processes such as braking, steering, etc.

Network performance can be affected by several external and internal factors (such as buildings, the weather, speed conditions, the number of actors participating in the communication process, or the applied security solutions). On the other hand, it must be emphasized that a malicious attack [8] or an unintentional error can considerably decrease network service quality.

Note that Public Key Infrastructure frameworks are also widely applied in other domains to provide an acceptable security level of the systems (e.g., the energy or the financial sector) [9] [10]. Many other research papers focused on the impact of authentication on communication delay [11], the effectiveness of Credential Management Systems related to CCAM solutions [12-15], and the security overhead of different coding algorithms [16]. Following the studied related works, we found that PKI authentication's safety effect in automotive systems has not yet been investigated in detail and needs further research.

To define the limits and boundaries where specific CCAM systems can be applied in a safe way, developers should pay attention to identify the expected risk level of the system related to particular combinations of the influencing factors. In that case, the system can be operated in the safe interval of the influencing factors, staying on the safe side. Accordingly, if the quality of service (QoS) decreases significantly, either because of an attack or an error, the controllable influencing factors can be modified to drive the system in a safe state [17-19].

2 Methods

This article investigates the expected effects of specific malicious interventions or random errors related to wireless communication based automotive functions taking into account the severity and probability of the considered unexpected event. Based on this, the applied risk estimation concept is introduced in the first part of the section, and in the next step, the probability estimation model is described [19].

2.1 Investigation Concept

During the evaluation, we investigated six cases focusing on intersecting vehicle movements [20]. All investigated cases included two cars (Target Vehicle – TV, Subject Vehicle – SV) where the neighboring legs of the junction meet at a 90-degree angle. Table 1 includes the velocities of the vehicles.

Table 1
Investigated cases and the applied velocities

Test case	TC1	TC2	TC3	TC4	TC5	TC6
v_{TV} [*km/h*]	20	50	20	50	20	50
v_{SV} [*km/h*]	40	70	70	100	100	130

In order to guarantee that the two vehicles are on a collision course, the starting position of both vehicles are chosen accordingly. The test scenarios were built using the Cohda VSIM simulation framework. In the test setup two Cohda MK5 On-Board Units (OBUs) are used to facilitate wireless communication between the two vehicles using CAM messages. The VSIM software simulates the vehicles following their respective paths and generates a GNSS (Global Navigation Satellite System) data stream for both. This data stream is then fed to their respective OBUs via TCP/IP (Transmission Control Protocol/Internet Protocol) connection. The architecture of the test system is shown on Figure 1.

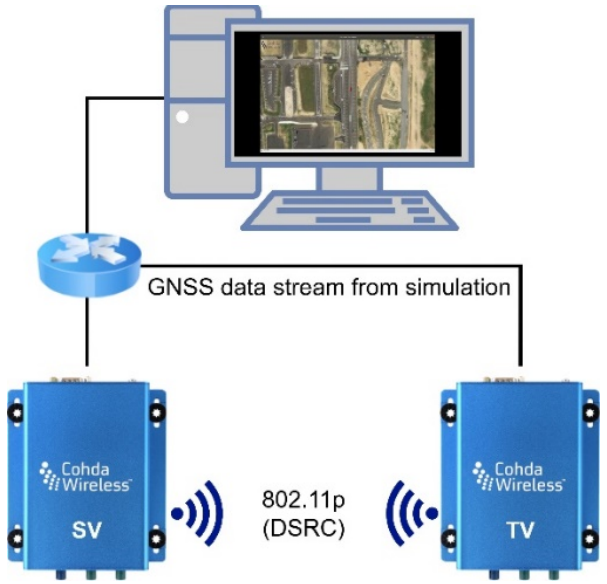


Figure 1
Test system architecture

The test cases were implemented in the virtual model of the ZalaZONE test field to provide the possibility for the real test-based verification of the experimental results [21]. The below presented laboratory setup was used to carry out the measurements.

Figure 2
Measurement laboratory setup

2.2 Representing Safety Risk

The below-presented part of the article describes the indicator applied to characterize safety risk. Beyond the vehicle generally applied dynamics parameters, the developed Safety Risk Index (SRI) considers the relevant QoS parameters, such as packet delivery ratio (PDR) or end-to-end latency (E2E). During the analysis, the stopping distance (denoted by d_{crit}) was evaluated to characterize the safety level of a specific scenario.

When CAMs do not arrive before the following vehicle approaches the front vehicle to the stopping distance (d_{crit}), the following car will not have enough distance to decelerate to a safe speed and avoid the accident.

In light of the above, if a CAM arrives to the following vehicle before the critical point, the car can prevent the collision. However, we also need to emphasize that it is not advantageous if the CAM arrives too early since the situation will not be classified as a hazardous event. Following this, we can identify a warning period (t_{warn}) in which the CAM should arrive. If the speeds of the cars are higher, the warning period has to be longer.

Accordingly, in the development procedure of ADAS/ADS (Advanced Driver-Assistance System/Automated Driving System) applications, we must consider the proportion of the warning and the critical period. If the proportion is smaller, the application will become more effective, but the risk related to the application will also be larger.

The indicator describing safety risk is defined by multiplying the estimated occurrence and severity values in the case of specific scenarios due to the delayed arrival of cooperative awareness massages.

The occurrence value related to the delayed arrival of cooperative awareness messages in a specific scenario is calculated by subtracting the arrival timestamp (t_{TS}) from the center point of the warning period (t_{TS_CENT}).

According to our concept, we estimate severity based on the collision energy. In light of this, it can be derived from the kinetic energy of the colliding vehicles. Following these assumptions, in the case of a longitudinal scenario, severity is proportional to the difference between the squares of velocities. In that case, risk can be represented by the following formula:

$$SRI = \left(t_{TS} - t_{TS\_CENT}\right) \cdot d_{crit} \tag{1}$$

Based on Eq. 1. we calculated the risk values related to the implemented test scenarios. Following this, it became possible to identify the polynomial regression function (Eq. 2.) capable of estimating the risks in the case of specific combinations of the considered input variables, such as the values of the investigated vehicle dynamics and QoS parameters:

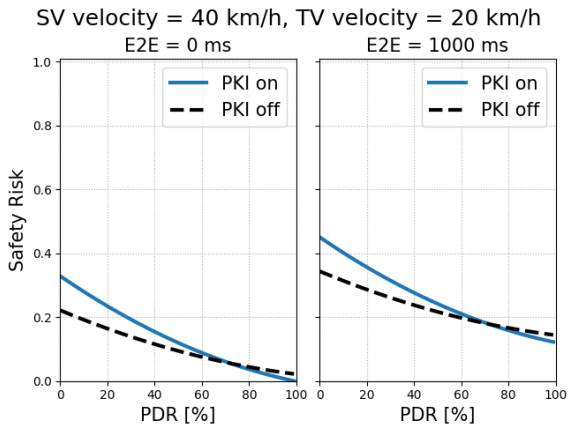
$$\hat{y} = \beta_0 + \beta_1 x_1 + \beta_2 x_2 + \cdots + \beta_{12} x_1 x_2 + \beta_{13} x_1 x_3 + \cdots \quad (2)$$

3 Results

This section focuses on the outcomes of the executed measurements. The safety risk of the V2V test cases is analyzed by applying the presented safety risk index. The below-presented figure pairs compare the risk functions. The left side of the figures show a low-latency scenario with minimal (~0 ms) E2E latency, the right side shows a high-latency (1000 ms) scenario. Each figure contains the results of two measurements, one with PKI authentication turned on (blue continuous line) and one with PKI turned off (black dashed line). Due to applying polynomial regression to the calculated SRI values the resultant safety risk values are normalized.

3.1 Test Case TC1

In the first test case, the subject vehicle moves at 40 km/h while the target vehicle moves at 20 km/h. Due to the relatively low velocities, the expected risk level is relatively low. In both low- and high-latency cases the risk function is steeper when the PKI authentication is switched on.



Safety Risk function for TC1 test case

Table 2
Safety Risk values for TC1 test case

PDR	E2E	Without PKI	With PKI
10%	0 ms	0.193	0.281
	500 ms	0.254	0.342
	1000 ms	0.315	0.403
50%	0 ms	0.095	0.121
	500 ms	0.156	0.182
	1000 ms	0.218	0.243
100%	0 ms	0.022	0
	500 ms	0.083	0.061
	1000 ms	0.145	0.122

3.2 Test Case TC2

In the following test case, the subject vehicle moves at 70 km/h, while the target vehicle moves at 50 km/h. We can recognize that the safety impact of the PKI authentication process is not emphatic, only a small difference can be observed at extremely low PDR levels (under 20%).

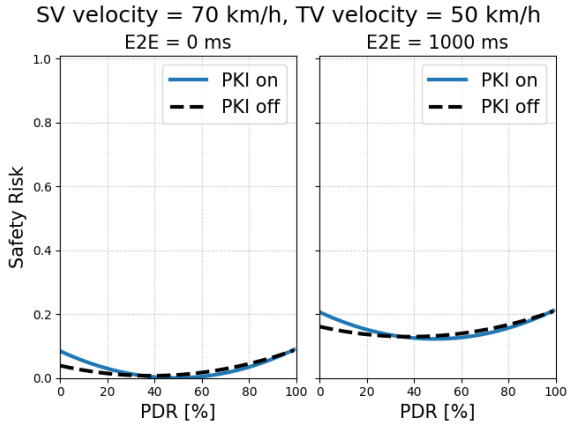


Figure 4
Safety Risk function for TC2 test case

Table 3
Safety Risk values for TC2 test case

PDR	E2E	Without PKI	With PKI
10%	0 ms	0.066	0.095
	500 ms	0.127	0.156
	1000 ms	0.188	0.217
50%	0 ms	0.051	0.042
	500 ms	0.113	0.103
	1000 ms	0.174	0.164
100%	0 ms	0.131	0.134
	500 ms	0.192	0.195
	1000 ms	0.253	0.256

3.3 Test Case TC3

In the third test case, the target vehicle moves at 20 km/h while the subject vehicle moves at 70 km/h. Due to the more considerable difference in velocities, the safety risk takes larger values when the quality of service becomes lower. On the other hand, we have to emphasize that the packet delivery ratio has a more significant influence on the safety risk. Comparing the safety risk of the systems with and without PKI authentication, the maximum value of the system with PKI is ~0.1 larger than that of the system without PKI.

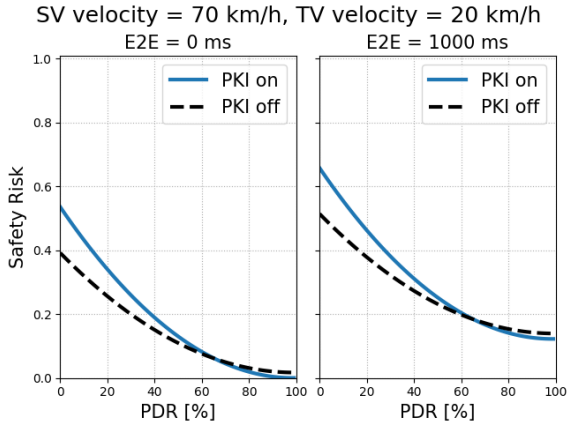


Figure 5
Safety Risk function for TC3 test case

Table 4
Safety Risk values for TC3 test case

PDR	E2E	Without PKI	With PKI
10%	0 ms	0.389	0.501
	500 ms	0.45	0.562
	1000 ms	0.511	0.623
50%	0 ms	0.178	0.198
	500 ms	0.239	0.26
	1000 ms	0.3	0.321
100%	0 ms	0.086	0.069
	500 ms	0.147	0.13
	1000 ms	0.208	0.191

3.4 Test Case TC4

Regarding the fourth test case, the target vehicle moves at 50 km/h while the subject moves at 100 km/h. Similar to the previous test case, the more significant difference in the velocities results in larger safety risk values in the case of lower quality of service levels. Besides this, we can also observe that the packet delivery ratio considerably impacts the safety risk. Comparing the safety risk of the systems with and without PKI authentication, the maximum value of the system with PKI is about the same as the system without PKI.

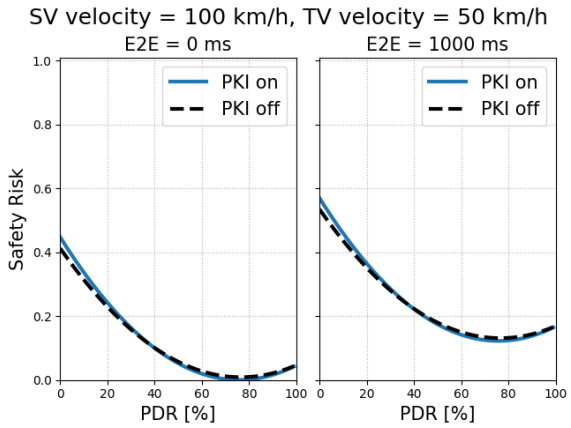


Figure 6
Safety Risk function for TC4 test case

Table 5
Safety Risk values for TC4 test case

PDR	E2E	Without PKI	With PKI
10%	0 ms	0.372	0.396
	500 ms	0.433	0.457
	1000 ms	0.495	0.518
50%	0 ms	0.116	0.11
	500 ms	0.177	0.172
	1000 ms	0.238	0.233
100%	0 ms	0.105	0.104
	500 ms	0.166	0.165
	1000 ms	0.228	0.227

3.5 Test Case TC5

Analyzing the TC5 test case, the target vehicle moves at 20 km/h while the subject vehicle moves at 100 km/h. In this test case, the large difference between the vehicles' velocity increases the safety risk significantly, especially when PDR is under ~30%. Besides, we can also observe that the packet delivery ratio considerably impacts the safety risk. The maximum safety risk in the case of the system with PKI approaches the value of 0.8 when the latency is relatively high.

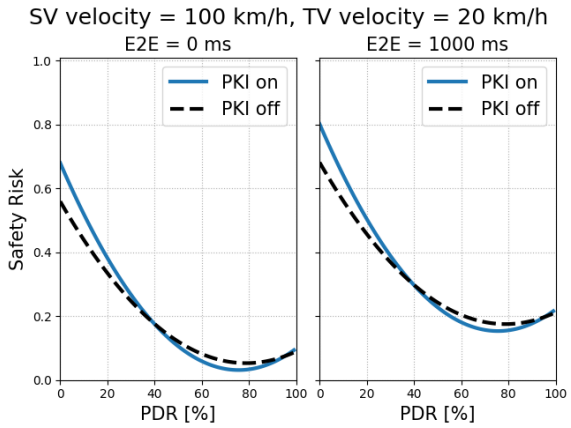


Figure 7
Safety Risk function for TC5 test case

Table 6
Safety Risk values for TC5 test case

PDR	E2E	Without PKI	With PKI
10%	0 ms	0.513	0.593
	500 ms	0.574	0.654
	1000 ms	0.635	0.716
50%	0 ms	0.194	0.179
	500 ms	0.255	0.24
	1000 ms	0.317	0.301
100%	0 ms	0.163	0.173
	500 ms	0.225	0.234
	1000 ms	0.286	0.295

3.6 Test Case TC6

Regarding the most dangerous test case, the vehicles travel with 50 km/h and 130 km/h. In accordance with the above, we can observe the highest safety risk values among the examined scenarios in this test case. We can also conclude that the safety risk function changes steepest in this test case as a function of the packet delivery ratio.

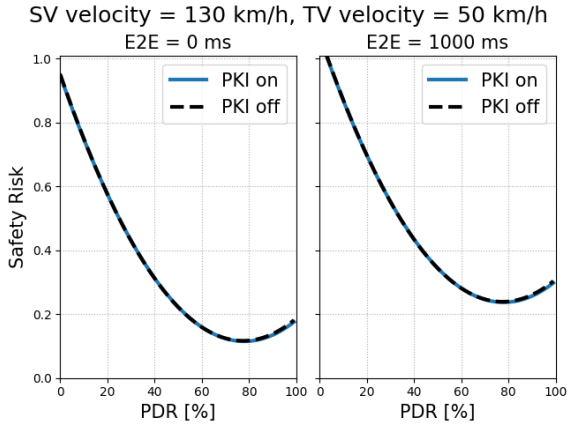


Figure 8
Safety Risk function for TC6 test case

Table 7
Safety Risk values for TC6 test case

PDR	E2E	Without PKI	With PKI
10%	0 ms	0.824	0.822
	500 ms	0.885	0.883
	1000 ms	0.946	0.945
50%	0 ms	0.295	0.296
	500 ms	0.356	0.357
	1000 ms	0.418	0.418
100%	0 ms	0.261	0.255
	500 ms	0.322	0.316
	1000 ms	0.383	0.377

Conclusions

Our article investigates the impact of Public Key Infrastructure (PKI) based authentication processes, on the safety risk caused by the increased processing time in the case of different QoS parameter levels.

To evaluate the quantified risk values of the investigated test cases and to analyze the behavior of the system depending on different vehicle dynamics, we investigate the relationship between the change in the analyzed QoS parameters and the risk level related to the test cases.

When the packet delivery ratio is low, the value of the safety risk becomes outstandingly high, above 0.9. If we focus on the test cases with PKI switched on, we can observe that when the PDR is low, the risk values are generally larger than without the PKI. Tough the differences vary the maximum difference is ~0.11.

When the packet delivery ratio gets higher, the risk levels related to the test cases with and without PKI get closer. Accordingly, if the packet delivery ratio is close to 100%, the overhead of the PKI process becomes negligible.

Based on our outcomes, the safety impact of Public Key Infrastructure based authentication is insignificant. The increased processing time can only result in unsafe cases if the quality-of-service decreases below an unacceptable level.

To solve this difficulty, we need to consider case-dependent resource allocation and make further computational resources available to our automotive systems in the case of critical situations when the QoS parameters make it necessary to reduce the processing time of the authentication process.

To reduce the mentioned risks, adaptive security-related solutions or detailed system limitations can be applied. System limitations must be validated to approve if the investigated applications can be operated safely by controlling system parameters between the pre-defined limits.

Based on the concluded outcomes of the research, we can formulate the following key messages:

- Packet loss has stronger effect on safety risk than latency.
- In the case of normal QoS levels, PKI has negligible effect on safety risk.
- If QoS reduces, PKI's negative effect on safety risk becomes more pronounced. In this case, adaptive, risk-reducing measures should be implemented and applied.

Acknowledgements

The research was supported by the Ministry of Innovation and Technology NRDI Office within the framework of the Autonomous Systems National Laboratory Program.

This work was supported by the ÚNKP-22-3-II-BME-53 and ÚNKP-21-5 new national excellence program of the Ministry for Innovation and Technology from the source of the National Research, Development and Innovation Fund.

References

[1] M. Zöldy, "Legal barriers of utilization of autonomous vehicles as part of green mobility," in International Congress of Automotive and Transport Engineering. Springer, 2018

[2] H. Tschürtz and A. Gerstinger, "The safety dilemmas of autonomous driving," in 2021 Zooming Innovation in Consumer Technologies Conference (ZINC) IEEE, 2021

[3] Z. Szalay, D. Ficzere, V. Tihanyi, F. Magyar, G. Soós, and P. Varga, "5g-enabled autonomous driving demonstration with a v2x scenario-in-the-loop approach," Sensors, Vol. 20, No. 24, 2020

[4] D. Grimm, M. Stang, and E. Sax, "Context-aware security for vehicles and fleets: A survey," IEEE Access, 2021

[5] T. Sipos, A. Afework Mekonnen, and Z. Szabó, "Spatial econometric analysis of road traffic crashes," Sustainability, Vol. 13, No. 5, 2021

[6] T. Bécsi, Á . Szabó, B. Kővári, S. Aradi, and P. Gáspár, "Reinforcement learning based control design for a floating piston pneumatic gearbox actuator," IEEE Access, Vol. 8, 2020

[7] C. Csiszár and D. Földes, "System model for autonomous road freight transportation," Promet-Traffic&Transportation, Vol. 30, No. 1, 2018

[8] B. Nagy, P. Orosz, T. Tóthfalusi, L. Kovács, and P. Varga, "Detecting ddos attacks within milliseconds by using fpga-based hardware acceleration," in NOMS 2018-2018 IEEE/IFIP Network Operations and Management Symposium. IEEE, 2018

[9] J. Csatár and A. Dán, "Novel load flow method for networks with multipoint-grounded-neutral and phase-to-neutral connected equipment," International Journal of Electrical Power & Energy Systems, Vol. 107, 2019

[10] C. Krasznay and G. Gyebnár, "Possibilities and limitations of cyber threat intelligence in energy systems," in 2021 13th International Conference on Cyber Conflict (CyCon) IEEE, 2021

[11] B. Fernandes, J. Rufino, M. Alam, and J. Ferreira, "Implementation and analysis of ieee and etsi security standards for vehicular communications," Mobile Networks and Applications, Vol. 23, No. 3, 2018

[12] B. Brecht and T. Hehn, "A security credential management system for v2x communications," in Connected Vehicles. Springer, 2019

[13] H. Qiu, M. Qiu, and R. Lu, "Secure v2x communication network based on intelligent pki and edge computing," IEEE Network, Vol. 34, No. 2, 2019

[14] I. Agudo, M. Montenegro-Gómez, and J. Lopez, "A blockchain approach for decentralized v2x (d-v2x)," IEEE Transactions on Vehicular Technology, Vol. 70, No. 5, 2020

[15] M. Rumez, D. Grimm, R. Kriesten, and E. Sax, "An overview of automotive service-oriented architectures and implications for security countermeasures," IEEE access, Vol. 8, 2020

[16] A. Fazzat, R. Khatoun, H. Labiod, and R. Dubois, "A comparative performance study of cryptographic algorithms for connected vehicles," in 2020 4th Cyber Security in Networking Conference (CSNet) IEEE, 2020

[17] Torok, A., & Pauer, G. (2022) Safety aspects of critical scenario identification for autonomous transport. Cognitive Sustainability, 1(3)

[18] Török, Á. (2020) A novel methodological framework for testing automated vehicle functions. European Transport Research Review, 12(1), 1-9

[19] Nyerges, L. Á., & Zöldy, M. (2023) Ranking of four dual loop EGR modes. Cognitive Sustainability, 2(1), 51-72