Development of a Novel Automotive Cybersecurity, Integrity Level, Framework

Árpád Török, Zsolt Szalay, Balázs Sághi

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

Abstract: As automated driver assistance functions are getting more and more popular, they will surly have a significant impact on our life especially considering security and the expected serious effects of malicious interventions. In light of the introduced aspects, the Test Field of Zalaegerszeg has started a research to evaluate the required professional and scientific framework to prevent transport systems from malicious external intervention. With regard to this aspect, the homologation system has been analyzed. In accordance with this the main objective of the article is to develop integrity level structure related to transport systems especially focusing on security issues. In this context the paper reconsiders the structure of ASIL to provide a proper framework focusing on the outstandingly important issues of cybersecurity. To develop a novel SIL framework a tailor-made method is identified to define risk parameter values related to certain SIL categories. At the end of the research, the investigation has determined the acceptable hazard rates related to the S&SIL architecture.

Keywords: cybersecurity integrity level; automotive safety integrity level; clustering model; tolerable hazard rate; hazard classification category

1 Introduction

Currently the significance of the secured and well-protected cyberspace is continuously increasing. By this time, online connections have become as important as personal relationships, everybody uses the internet to keep in touch with the surrounding environment. On the one hand, everybody feels that the digital development facilitates the formation and the maintenance of social networks. Everything is getting closer, goods can be easily purchased from the other side of the world and people from different continents can easily meet each other on the internet. These new possibilities extremely increase the effectiveness of communication related processes. New methods like fifth generation cellular network technology [1] and intelligence demonstrated by machines [2] will

probably revolutionize the recent world. However, on the other hand our online dependency is going to strongly influence the security of the society. In light of the introduced trends, data integrity, privacy, data security, individual safety and even public safety can be threatened. To summarize, the spread of connected devices and the growing influence of the cyberspace on our life will make it necessary to improve the protection of safety and security.

Beside this, the spread of self-driving cars can provide additional advantages through the concept of connected vehicles by utilizing the possibilities of real time information exchange. However, this new mode of transportation will surly generate new vulnerabilities related to mobility processes influencing the safety of our everyday life. In light of this, attack detection is going to be one of the main objectives to provide the proper safety and security of the transportation system [3]. Since the increasing number of connecting devices in highly automated cars can lead to serious vulnerabilities, which can be exploited by malicious intruders influencing safety and security of everyday mobility processes. On the other hand, moral considerations can also not be forgotten, which in many cases make the cybersecurity related development processes even more difficult [4].

In accordance with this, the proper and acceptable security level of highly automated vehicles has to substantially be evaluated. For this purpose, it is crucial to perceive and remove those factors in the system which increase security risk. To consider safety and security together, even during the earliest stages of the design procedure, researchers have developed a new method for the automotive industry [5]. In light of the introduced development processes, the Test Field of Zalaegerszeg [6] has started a research to evaluate the required professional and scientific framework to prevent transport systems from malicious external intervention. Since nowadays it seems to be an outstandingly important research objective to identify the homologation framework of automotive cybersecurity, the gap between the classical methods of automotive standardization and validation and the quickly changing informatics field has to be bridged [7]. Considering that the methods followed by the two mentioned segments are considerably different, this purpose seems to be a difficult task. Since if classical functional safety related audit methods and the high-tech cybersecurity related analytical background are compared, we can find significant differences.

In accordance with this, the main objective of the evaluation coordinated by the Test Field of Zalaegerszeg Research Committee is to identify the foundations of a novel integrity level architecture taking into account both safety and security related aspects. In the first step related works have been reviewed to get a clear picture about the recently applied most up-to-date methods and models, which can support the development of a novel complex integrity level architecture. Even the functional safety characteristics of microchips and circuits can have a serious impact on security of highly automated vehicles, hence the work of Belotti et al. has to be thoroughly investigated to build up a comprehensive methodological framework [8]. Their paper introduces in details the integrity level frame work

applied by the automobile industry, on the other hand the paper does not do further steps to propose development orientations related to the recently applied integrity level architecture. Chang and other researchers have also analyzed the effect of automotive functional safety standards on the applied microchips [9]. Their paper provides a comprehensive safety investigation in case of the analyzed automobile elements. However, it has to be emphasized that the paper does not focus on security related problems or issues [10]. Other important automotive industry related forums like SAE proposes different approaches to evaluate the security level of highly automated cars. These proposals are in accordance with the most important automotive industry related standards (e.g. ISO 26262). One of the most known methodological framework is HEAVENS, beside this, EVITA is also a well-structured model environment [11]. On the other hand, it needs to be considered that theses frameworks do not combine the aspects of safety and security, which should be a key issue in the automotive sector. Beyond this, the mentioned models place much less emphasis on the investigation of acceptable level of cybersecurity risk than it would be reasonable. According to the results of the relevant researches related to the combined evaluation of safety and security in the automotive sector [12], it is now obvious that accident risk of highly automated vehicles cannot be analyzed without the comprehensive evaluation of automotive cybersecurity [13]. In accordance with this, when safety integrity level of automotive systems [14] are investigated, security vulnerabilities and the related preventive interventions are also necessary to be analyzed in details. To present the newly developed S&SIL (combined safety and security integrity level) architecture, the relevant risk parameters have been evaluated, especially considering severity, probability and controllability [15]. In light of the introduced considerations, this work focuses on the identification of the novel integrity level framework, especially considering the relevant risk parameters, which need to be taken into account. In accordance with this, the paper covers the following main topics: interpretation of the used models, introduction of the main findings and the explanation of the most important outputs of our investigation.

2 Applied Models

To identify the novel integrity level framework, the proper terms should be identified and well described. For this purpose, the collection and description of the most important definitions related to the integrated model of safety and security should be the first and foremost step. In accordance with the introduced field, the most relevant terms are necessary to be defined. During our model development process hazard is defined as the alignment of the possible conditions and circumstances, which can lead to harm. Therefore, the investigation of potential hazards has to be followed by further analysis. In the following phase, it has to be evaluated whether the identified hazards affect system vulnerabilities or

not. In light of this, vulnerability can be defined as the ability to be affected by an investigated hazard. The term of impact reflects to relationship between vulnerability and hazard. If a hazard is getting activated, its impact on the system depends strongly on the system vulnerability with regard to the given hazard. Furthermore, the definition of risk can be derived by the terms of probability and its possible impact through multiplying the two factors by each other. Beside this, the term of threat represents the alignment of the above mentioned negative factors. Accordingly, if there is a relevant hazard, a strongly related serious vulnerability and the expected impact seems to be significant, then the investigated system is considerably threatened. Accordingly, the figure below (Figure 1) represent the introduced processes.

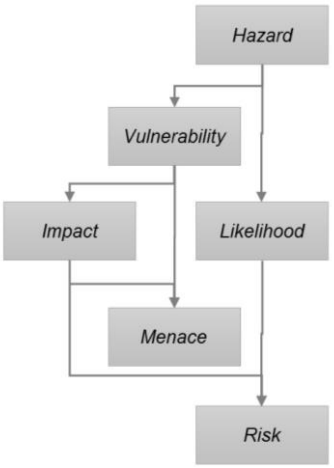

Figure 1
The connection among the introduced terms in the integrated fields of safety and security

Safety hazards are described by many popular models, such as GAMAB, ALARP and MEM. The above-introduced methods investigate the level of acceptable and tolerable hazards. Their aim is to describe if certain hazards in relation to their derived risk can or cannot be accepted on the level of the society. The main approach of the paper is in accordance with the GAMAB model, applying the main concept of integrity level framework to develop a novel architecture, which fits to the requirements of the integrated fields of safety and security. Tithe outcomes of this concept can lead to complex and holistic representation with regard to the analyzed functions. This added value can be outstandingly important from the viewpoint of safety and security, since the newly generated information on system characteristics can strongly influence the applied analytical methods and the efficiency of the investigation during the product lifecycle. [16]. Integrity level framework can support the investigation in describing the ability of the system to stay in a safe and secured operation mode. In light of this, the goal of the analysis is to determine if the derived risk level in case of a certain hazard is

tolerable or not. Accordingly, Kreiner et al. have shown that safety and security of highly automated systems have an outstanding importance especially if they have been built-up from strongly interrelated hardware and software components [17].

The acceptable risk level in case of safety critical system can be determined considering the related risk category. In this regard, the applied model - as mentioned above – takes into account the severity, probability and controllability. Accordingly, the demanded safety and security characteristic of the investigated safety critical system is determined based on the acceptable risk level of the society. In light of this, the demanded safety and security characteristic of a safety critical system is determined as the level of the acceptable risk [18]. It has to be kept in mind that the article aims to discuss safety and security related issues of the automotive segment, in accordance with this, the new integrity level framework is derived from the ASIL concept [19]. The expected likelihood of an effective malicious intervention, is difficult to be estimated, especially with acceptable prediction accuracy. In accordance with this, during our investigation the method introduced by Dudrov et al. is used to determine the probability of the investigated malicious intervention types [20].

3 Results

The primary outcome of the completed investigation is the understanding, the interpretation and the demonstration of the timeliness of a novel model, in case of the combined fields of safety and security. Firstly, it has to be understood that the set of consequences are not the same in case of safety and cybersecurity. While safety mainly focuses on human severity, cybersecurity has to consider also information security related aspects as well. On the other hand, classical cybersecurity risk classification models primarily investigate privacy, data protection and national security related issues. Accordingly, if the aim is the development of a common framework, safety and security related consequences have to be reduced to a common denominator. Furthermore, the applicability of controllability as a risk parameter should be reconsidered, since this ability of the system fundamentally depends on the relationship of the system and the investigated attack, namely, how efficiently can the given system detect and then treat the investigated malicious intervention. Accordingly, detectability (D1, D2, and D3) and treatability (T1, T2, and T3) should be among the most important risk parameters in the newly developed model focusing on the integrated fields of safety and security. In light of the introduced findings a novel S&SIL architecture is developed, which covers private data security (PR-S), public data security (PU-S), national security (NS) and also safety integrity. The following table describes the new integrity level framework representing the field of safety and security (Table 1). In Table 1, QM refers to issues, which can be solved by the tools of

quality management and S&SIL A..D refer to issues, which have to be investigated by the tools of safety and security assessment methodologies (Tab. 1).

Table 1
Representation of S&SIL framework

		T1			T2			T3		
		D1	D2	D3	D1	D2	D3	D1	D2	D3
B-S-PR	E1	QM	QM	QM	QM	QM	QM	QM	QM	QM
	E2	QM	QM	QM	QM	QM	QM	QM	QM	S&SIL A0
	E3	QM	QM	QM	QM	S&SIL A0	QM	QM	S&SIL A0	S&SIL A1
M-S-PR	E1	QM	QM	QM	QM	S&SIL A0	QM	QM	S&SIL A0	S&SIL A1
	E2	QM	QM	QM	S&SIL A0	S&SIL A1	QM	S&SIL A0	S&SIL A1	S&SIL A2
	E3	QM	QM	S&SIL A0	S&SIL A1	S&SIL A2	S&SIL A0	S&SIL A1	S&SIL A2	S&SIL B0
B-S-PU	E1	QM	QM	S&SIL A0	S&SIL A1	S&SIL A2	S&SIL A0	S&SIL A1	S&SIL A2	S&SIL B0
	E2	QM	S&SIL A0	S&SIL A1	S&SIL A2	S&SIL B0	S&SIL A1	S&SIL A2	S&SIL B0	S&SIL B1
	E3	S&SIL A0	S&SIL A1	S&SIL A2	S&SIL B0	S&SIL B1	S&SIL A2	S&SIL B0	S&SIL B1	S&SIL B2
M-S-PU	E1	S&SIL A0	S&SIL A1	S&SIL A2	S&SIL B0	S&SIL B1	S&SIL A2	S&SIL B0	S&SIL B1	S&SIL B2
	E2	S&SIL A1	S&SIL A2	S&SIL B0	S&SIL B1	S&SIL B2	S&SIL B0	S&SIL B1	S&SIL B2	S&SIL C0
	E3	S&SIL A2	S&SIL B0	S&SIL B1	S&SIL B2	S&SIL C0	S&SIL B1	S&SIL B2	S&SIL C0	S&SIL C1
M-NS	E1	S&SIL A2	S&SIL B0	S&SIL B1	S&SIL B2	S&SIL C0	S&SIL B1	S&SIL B2	S&SIL C0	S&SIL C1
	E2	S&SIL B0	S&SIL B1	S&SIL B2	S&SIL C0	S&SIL C1	S&SIL B2	S&SIL C0	S&SIL C1	S&SIL C2
	E3	S&SIL B1	S&SIL B2	S&SIL C0	S&SIL C1	S&SIL C2	S&SIL C0	S&SIL C1	S&SIL C2	S&SIL D0
C-NS	E1	S&SIL B1	S&SIL B2	S&SIL C0	S&SIL C1	S&SIL C2	S&SIL C0	S&SIL C1	S&SIL C2	S&SIL D0
	E2	S&SIL B2	S&SIL C0	S&SIL C1	S&SIL C2	S&SIL D0	S&SIL C1	S&SIL C2	S&SIL D0	S&SIL D1
	E3	S&SIL C0	S&SIL C1	S&SIL C2	S&SIL D0	S&SIL D1	S&SIL C2	S&SIL D0	S&SIL D1	S&SIL D2

The following investigation focuses on the definition of the currently acceptable risk level related to the combined fields of safety and security. In the next step, the defined risk level is going to be implemented in case of the newly introduced architecture. The acceptable risk level is derived from the estimated number of connected tools and instruments, from the expected number of malicious interventions arriving from the cyberspace and from the expected likelihood of efficient interventions [20].

$$L = \frac{N \cdot \sum_{i=1}^{n} r_i \cdot l_i}{M} \tag{1}$$

L: expected likelihood of efficient interventions,

N: expected number of malicious interventions arriving from the cyberspace in 2020,

M: estimated number of connected tools and instruments in 2020,

li: expected likelihood of efficient interventions regarding the i^{th} attack type,

ri: is the ratio of the i^{th} intervention type, and

n: number of intervention types.

Based on the ASIL framework, in light of the derived acceptable risk level, the novel S&SIL rating scale can be introduced as follows (Table 2):

Table 2
S&SIL rating

	S&SILs	Probability of succ. incident
1	S&SIL A	<10-7
2	S&SIL B	<10-8
3	S&SIL C	<10-8
4	S&SIL D	<10-9

4 Discussion

The development of the combined architecture of safety and security integrity levels should start with identification of the main consequence classes. At this stage it is a basic aspect with regard to the novel architecture to integrate the classes considered by ASIL, ENISA [21] NCCIC framework. Taking into account the mentioned models, the primary goal of the analysis is to combine the introduced risk evaluation methods. ASIL [8] actually includes three different types of possible consequences, ENISA [21] classifies the investigated functions and processes based on three different evaluation assurance level (EAL), and NCCIC categorizes the malicious interventions in seven groups. The framework applied by the automotive sector considers primarily those kind of hazards, which can be dangerous to life, in accordance with the applied risk categories refer to the severity of the expected injury. On the contrary, ENISA uses a much simpler approach and hazards are classified into basic, substantial and high risk groups. This simpler model primarily considers the vulnerability of the evaluated function or process. In case of the ranking system used by NCCIC the classification of the investigated hazard is primarily influenced by the assumed attack vector. According to the applied methodology, the threat class of a given malicious

intervention is determined as legible if the expected effect of the given attack is marginal. The priority of an attack is defined as minor if the hazard related to the given incident to have impact on public health or national security is reasonably low. An attack is classified into the low priority group if it cannot be assumed to significantly influence public health or national security. When the evaluated attack can have an effect on public health or national security it should be classified into the medium-risk group. If the investigated incident is likely to influence public health or national security it should be assigned to the high-risk group. When a malicious intervention can have significant impact on public health or safety and national security it is defined as a severe priority incident. When a malicious intervention menaces critical infrastructure, national security or human lives it is defined as emergency. In accordance with the introduced risk ranking methods it is possible to develop an overall evaluation concept covering the most important considerations of the mentioned models. It has been introduced that a fundamental criteria of the development process of the new integrity architecture combining the fields of safety and security to be reconcilable with the automotive safety concept. In case of this criterion, the most important goal has been to provide the mutual interoperability between the integrity level frameworks of the classical automotive sector and the newly developed architecture of safety and security. In order to ensure interoperability between the classical automotive approach and the newly developed integrity level framework, it is expected to have the same structure with regard to their lines and columns. In light of this, the numbers of lines and columns of the novel architecture should be the integer multiple of the numbers of columns and lines used in case of the integrity level framework of the automotive sector. Based on the introduced considerations, the developed risk evaluation framework includes six different risk groups, which are mainly derived from the incident scoring system of NCCIC. The number of baseline risk levels are contracted to one group. At the same time, the risk groups used in the novel concept are also in accordance with the severity categories of the automotive safety integrity levels. In accordance with this the definitions of the risk groups contain descriptions related to effects possibly resulting personal injury as well as information damage or theft. Due to the introduced considerations the following levels can describe the risk group structure related to the developed cybersecurity integrity level architecture (Table 3).

In light of Table 3 it is obvious that beyond the mentioned cybersecurity related approach of NCCIC and the introduced automotive sector related framework; the newly developed concept also refers to the presented evaluation assurance level applied by the ENISA. In accordance with this, the first two risk groups of S&SILs are related the basic assurance level of ENISA, the second two groups of S&SILs are related to the substantial assurance level of ENISA, while the third two risk groups are related to the high assurance level of ENISA. With regard to the likelihood of the investigated attacks, classical likelihood approach based groups are re-clustered into three groups.

Table 3
Representation of cybersecurity significance level

Risk group	Description
Threatening either basic safety or security of private data (B-S-PR)	The attacks in this class cause less relevant menace to private data or slight personal injuries.
Threatening either moderate safety or security of private data (M-S-PR)	Malicious interventions in this group can lead to moderately relevant menace to private data or moderate injuries.
Threatening either basic public safety or public data security (B-S-PU)	Attacks in this class cause less relevant menace to public data or severe personal injuries.
Threatening either moderate public safety or public data Security (M-S-PU)	Malicious interventions in this group can lead to moderately important menace to public data or life-threating personal injuries.
Threatening national security (M-NS)	Attacks in this class cause moderately relevant menace to national security or fatal injury.
Critical threatening national security (C-NS)	Malicious interventions in this group lead to critical menace to national security or numerous fatal injuries.

Based on this classification, incidents can be less (L1), moderately (L2) or critically (L3) likely to cause threatening. In case of the safety and security related combined integrity level framework in light of the classical automotive sector related architecture, the factor of controllability becomes more complex, since the controllability of a security incident is strongly affected by its detectability and treatability. [22]. Actually, in case of the combined field of safety and security, with the detection and the treatment of a given attack the whole control process can be performed. Accordingly, in the first step the investigated attack should be recognized and only then that attack can be averted. Based on this, with regard to detectability as well as treatability, attacks can be assigned to three classes (Table 4).

Table 4
S&SIL risk parameters

	Detectability levels	Definition		treatability levels	Definition
1	D1	Basic level of detectability	1	T1	Basic level of treatability
2	D2	Moderate level of detectability	2	T2	Moderate level of treatability
3	D3	Critical level of detectability	3	T3	Critical level of treatability

Based on the application of the previously interpreted correspondences, the novel integrity level framework combining the aspects of safety and security can be built up. (table 1). In this matrix lines include the levels of the described risk groups (B-S-PR, M-S-PR, B-S-PU, M-S-PU, M-NS, C-NS). The likelihood to detect or treat incidents is described by the columns of the investigated matrix. Based on the classical safety integrity level model applied by the automotive sector, if the occurrence probability and the expected effect of the malicious interventions related to the analyzed function or module are low and its detectability and treatability are high then the related issues can be solved by quality management related processes. The objective of the next development step is to fit the novel framework to the classical automotive safety integrity architecture. In light of this, the assignment process between hazard classes (ASIL QM, A, B, C, D) and risk parameter groups (the combinations of severity, probability and controllability) are represented by a specific optimization problem. The aim of the method is to assign the proper hazard class to a certain combination of risk parameters. To do so the adequate estimation function has been selected, which can estimate the proper hazard class based on the risk parameters as input variables. Accordingly, the objective of the optimization problem is to define the coefficients of the estimation functions by minimizing the differences between the values of the classical automotive framework and the newly developed architecture. Input data has been generated by using risk parameter levels as integer input values (e.g. if the level of severity is S1 S=1). To identify the considered factors of the estimation function, the matrix of the safety integrity level framework has been investigated. The mentioned matrix includes the related parameters of severity, probability and controllability in two dimension, so practically both severity and probability are included by the lines of the table. This has inspired the contraction of the introduced two parameters in the estimation function. In light of this, during the estimation process severity (S) and probability (P) are taken into account in an

integrated form by generating risk values (R) through multiplying their scale parameters.

$$R = S \cdot P \tag{2}$$

With this, the further clustering method has used two fundamental classification parameters risk (R) and controllability (C). To conclude the main goals of the developed model, the primary objective has been to build up a framework which applies the parameters of the classical automotive integrity level architecture and which can generate a cluster structure considering the aspects of automotive safety and security in an integrated way. During the development process three different models have been developed including linear, exponential and a mixed model. The objective of the evaluation has been to analyze the efficiency of the classification models (Class) and to identify safety integrity levels unequivocally based on the function values of the classification models.

$$Class_{lin} = a \cdot R + b \cdot C \tag{3}$$

$$Class_{exp} = R^{\alpha} \cdot C^{\beta} \tag{4}$$

$$Class_{mix} = R^{\omega} + C^{\gamma} \tag{5}$$

where

a, b: linear coefficients,

α, β, ω, γ: are non-linear coefficients.

The next step to define the most efficient clustering method, the table of classical safety integrity framework (Table 5) is represented by the clustering model function in light of the interrelated input values (Table 6).

It can be seen in the presented matrix (Table 6) that in case of the applied clustering models, the input variables and the possible combination of the input parameters have discrete values. In light of this, using the presented input parameter combinations, the results of the clustering models can be systematically connected to a certain integrity level class. Accordingly, integrity levels are represented in Table 6 by the characters in the lower indexes.

To select the adequate approach for the clustering process the below presented optimization model was applied. The aim of the introduced method has been to identify the best model which results the minimum values of overlapping in comparison of the resulted cluster boundaries.

$$max: \sum_{k} Min\left(Class(R_{k+1}, C_{k+1})_{ASIL_{k+1}}\right) - \left(Max\left(Class(R_k, C_k)_{ASIL_k}\right)\right) \tag{6}$$

Table 5
Basic ASIL framework

		Level of Controllability		
Level of Severity	Likelihood of the incident	C1	C2	C3
S1	P1	QM	QM	QM
	P2	QM	QM	QM
	P3	QM	QM	ASIL A
	P4	QM	ASIL A	ASIL B
S2	P1	QM	QM	QM
	P2	QM	QM	ASIL A
	P3	QM	ASIL A	ASIL B
	P4	ASIL A	ASIL B	ASIL C
S3	P1	QM	QM	ASIL A
	P2	QM	ASIL A	ASIL B
	P3	ASIL A	ASIL B	ASIL C
	P4	ASIL B	ASIL C	ASIL D

The solution of this optimization problem provides the minimum overlapping between the sum of upper boundary of the k-th and the lower boundary of the k+1-th neighboring ASIL clusters. Based on the introduced model, it has become obvious that the mixed model can provide the best results (5) In case of this formula coefficients have been chosen ω=0,7 and γ=1,075. Based on the introduced clustering model S&SIL architecture has been be identified, and its compatibility with classical automotive integrity architecture is ensured. To define the necessary clustering parameters, first parameter is derived based on formula (2) and the second clustering parameter is identified according to formula (7).

$$C' = T \cdot D \tag{7}$$

Table 6
Result of the estimation function depending on the input variables EST (D,C)

			2nd risk parameter group (C)		
		1st risk parameter group (R)	1	2	3
S1	P1	1	CLASS (1,1)QM	CLASS (1,2)QM	CLASS (1,3)QM
	P2	2	CLASS (2,1) QM	CLASS (2,2) QM	CLASS (2,3) QM
	P3	3	CLASS (3,1) QM	CLASS (3,2) QM	CLASS (3,3) A
	P4	4	CLASS (4,1) QM	CLASS (4,2) A	CLASS (4,3) B
S2	P1	2	CLASS (2,1) QM	CLASS (2,2) QM	CLASS (2,3) QM
	P2	4	CLASS (4,1) A	CLASS (4,2) QM	CLASS (4,3) A
	P3	6	CLASS (6,1) QM	CLASS (6,2) A	CLASS (6,3) B
	P4	8	CLASS (8,1) A	CLASS (8,2) B	CLASS (8,3) C
S3	P1	3	CLASS (3,1) QM	CLASS (3,2) QM	CLASS (3,3) A
	P2	6	CLASS (6,1) QM	CLASS (6,2) A	CLASS (6,3) B
	P3	9	CLASS (9,1) A	CLASS (9,2) B	CLASS (9,3) C
	P4	12	CLASS (12,1) B	CLASS (12,2) C	CLASS (12,3) D

Formula (7) describes the integration of detectability and treatability in one unique parameter. The deliberate malicious attack or unintentional failures of automotive functions and components that has been assigned to a white colored field of the following matrix can be handled by quality management. Spotted cells describe A level functions or components, striped cells describe B level functions or components, checked cells refer to C level functions or components, while grey colored fields refer to D class functions or components (Table 7).

Table 7
Representation of S&SIL architecture

		T1			T2			T3		
		D1	D2	D3	D1	D2	D3	D1	D2	D3
B-S-PR	E1									
	E2									
	E3									
M-S-PR	E1									
	E2									
	E3									
B-S-PU	E1									
	E2									
	E3									
M-S-PU	E1									
	E2									
	E3									
M-NS	E1									
	E2									
	E3									
C-NS	E1									
	E2									
	E3									

For the following phase of the architecture development task, the aim of the investigation has been to define the accepted risk level related to the combined field of safety and security. Based on the introduced methodology, if expected number of malicious interventions and the expected likelihood of efficient interventions and estimated number of connected tools and instruments are definable, then the expected likelihood of efficient interventions can be estimated (8).

$$L = \frac{N \cdot \sum_{i=1}^{n} r_i \cdot l_i}{M} \tag{8}$$

The next step of the investigation is to identify the expected distribution of the certain intervention types. In case of our investigation, the distribution of the different intervention types is estimated to be uniform. In accordance with the mentioned expectation, the previously interpreted formula can be modified as follows:

$$L = \frac{N \cdot \sum_{i=1}^{n} \frac{l_i}{n}}{M} \tag{9}$$

In the following phase of the analysis, the estimated likelihoods of effective malicious interventions - introduced by the colleagues City University London - are applied [20]. Through estimating the likelihood of effective interventions, the expected value of effectively attacked objects can be defined. In the evaluation phase the most relevant attack surfaces of the vehicle industry are taken into account (direct intervention, intervention performed via Bluetooth connection, interventions performed via cellular network, connection and messaging and via phising and planting) [20].The number of malicious interventions is assumed to reach the eight hundred thousand in the United States of America according to the data published by Brooks statistics, at the same time, the number of online objects is expected to reach the fifty billion in the world [21]. The number of malicious interventions has been modified in accordance with the ratio of the world and the US population. In light of the interpreted aspects, it is possible to identify the annual accepted risk level of effectively implemented malicious interventions targeting online objects based on the below presented equation.

$$L = \frac{N \cdot \sum_{i=1}^{n} \frac{l_i}{n}}{M} = (8/10^5) \cdot (23/5) \cdot (0.63 + 0.52 + 0.33 + 0.76 + 0.6)/50/10^9 \tag{10}$$

In light of the introduced data describing the actual trend of the world's cybersecurity, based on the previously defined annual accepted risk level of effectively implemented malicious interventions, the hourly accepted risk level related to cyber incidents is assumed to be under 10 effective attacks. The identified hourly risk level has to be primarily interpreted as a mean value describing the society as a whole. In light of this, of course attack frequencies and their acceptance level can vary over the world. Hence, according to our interpretation the identified average value should be the central element of the developed rating scale. In accordance with this rating scale of the newly developed S&SIL architecture can be completed, and it is going to be correspond well to the classical framework of the automotive industry (Table 8):

Table 8
Saftey and security integrity levelrating scale

	ASILs	Likelihood of failure		S&SILs	Likelihood of succ. incident
1	ASIL A	$<10^{-6}$	1	S&SIL A	$<10^{-7}$
2	ASIL B	$<10^{-7}$	2	S&SIL B	$<10^{-8}$
3	ASIL C	$<10^{-7}$	3	S&SIL C	$<10^{-8}$
4	ASIL D	$<10^{-8}$	4	S&SIL D	$<10^{-9}$

On the other hand, the defined level of risk clusters shall be handled cautiously, because due to the expected quick development of the field, the number of attacks related to automated driver assistance systems is estimated to increase dynamically. The introduced trends are expected to completely modify the attitude of society to the risk of cyber threats. In accordance with this the frequency of malicious interventions, the ratio of remote interventions on vehicles are expected to increase dynamically in the close future. In light of the above-mentioned considerations the likelihood of efficient malicious interventions can achieve critical levels, which is likely to influence the sensitivity of society with regard to the combined field of safety and security in the automotive industry. Then, the operation efficiency of vehicle systems dealing with cybersecurity will need to be considerably improved. Accordingly, in case of formula (10), ten times more efficiently performed cyberattack can raise the hourly risk level to the value of 10^{-7}. This would definitely make necessary intelligent, targeted and strong international actions in the security field to make the average risk decrease under the acceptable value.

5 Summary

The aim of the article is to develop a novel integrity level framework in the combined field of automotive safety and security. In light of this, the paper discusses the most relevant terms related to the integrated field of safety and security, especially considering clustering parameters, and integrity levels. The investigation utilizes the approach of Safety Integrity Levels (SIL) to develop the novel integrity level framework suiting the combined field of automotive safety and security. In the article integrity levels are built up primarily according to the approach of the GAMAB model. It is important to emphasize that the study considers the aspects of automotive sector in an accentuated way, so the novel frame work is compatible to classical integrity level architecture of the automotive

industry [9]. To define the summarized likelihood of the possible remote interventions, the approach of Dudorov et al. is adopted [20]. This novel model takes controllability into account, as covering detectability and treatability. The novel S&SILs comprise a wide range of safety and security aspects. The last phase of this investigation was focused on current accepted risk levels of society, in the field of cybersecurity, which makes it possible to identify rating scale values, related to this newly developed S&SIL framework.

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).

References

[1] Alzenad, M., Shakir, M. Z., Yanikomeroglu, H., & Alouini, M. S. (2018) FSO-based vertical backhaul/fronthaul framework for 5G+ wireless networks. IEEE Communications Magazine, 56(1), 218-224

[2] Briand, L. C., Labiche, Y., and Liu, X., "Using machine learning to support debugging with tarantula," In Proceedings of the 18th IEEE International Symposium on Software Reliability, Washington DC, USA, 2007, pp. 137-146

[3] Rosenberg, I., Shabtai, A., Elovici, Y., & Rokach, L. (2018) Low Resource Black-Box End-to-End Attack Against State of the Art API Call Based Malware Classifiers. arXiv preprint arXiv:1804.08778

[4] Baldini, G., Botterman, M., Neisse, R., & Tallacchini, M. (2018) Ethical design in the internet of things. Science and engineering ethics, 24(3), 905-925

[5] 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

[6] 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

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

[8] Bellotti, M., & Mariani, R. (2010) How future automotive functional safety requirements will impact microprocessors design. Microelectronics Reliability, 50(9-11), 1320-1326

[9] Chang, Y. C., Huang, L. R., Liu, H. C., Yang, C. J., & Chiu, C. T. (2014, April) Assessing automotive functional safety microprocessor with ISO 26262 hardware requirements. In VLSI Design, Automation and Test (VLSI-DAT), 2014 International Symposium on (pp. 1-4) IEEE

[10] Jaskolka, J., & Khedri, R. (2016) Mitigating covert channels based on analysis of the potential for communication. Theoretical Computer Science, 643, 1-37

[11] Cheah, M., Shaikh, S. A., Bryans, J., & Wooderson, P. (2018) Building an automotive security assurance case using systematic security evaluations. Computers & Security, 77, 360-379

[12] Gheraibia, Y., Djafri, K., & Krimou, H. (2018) Ant colony algorithm for automotive safety integrity level allocation. Applied Intelligence, 48(3), 555-569

[13] Guiochet, J., Machin, M., & Waeselynck, H. (2017) Safety-critical advanced robots: A survey. Robotics and Autonomous Systems, 94, 43-52

[14] Miller, C., Kassie, J., & Poston, D. (2017) Assessing and Computing the Safety Integrity Level (SIL) for Turbo Machinery Protection. In Proceedings of the 46th Turbomachinery Symposium. Turbomachinery Laboratory, Texas A&M Engineering Experiment Station

[15] Kaczor, G., Młynarski, S., & Szkoda, M. (2016) Verification of safety integrity level with the application of Monte Carlo simulation and reliability block diagrams. Journal of Loss Prevention in the Process Industries, 41, 31-39

[16] 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

[17] 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

[18] Fülep, T. (2007) Design methods of safety-critical systems and their application in electronic brake systems

[19] Chuck Brooks (2017) Keep Calm and… Here Is a List of Alarming Cybersecurity Statistics. URL: https://www.itspmagazine.com/from-the-newsroom/keep-calm-and-here-is-a-list-of-alarming-cybersecurity-statistics

[20] Dudorov, D., Stupples, D., & Newby, M. (2013, August) Probability analysis of cyber attack paths against business and commercial enterprise systems. In Intelligence and Security Informatics Conference (EISIC), 2013 European (pp. 38-44) IEEE

[21] E. Commission, Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on ENISA, the ”EU

Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act"), 2017

[22] Guerrero-Higueras, Á. M., DeCastro-García, N., Rodríguez-Lera, F. J., & Matellán, V. (2017) Empirical analysis of cyber-attacks to an indoor real time localization system for autonomous robots. Computers & Security, 70, 422-435

[23] Tarnai G., Sághi B.: Hazard and Risk Analysis of Human-Machine Interfaces of Railway Interlocking Systems. 7th World Congress on Railway Research. 4-8.June, 2006, Montréal, Canada