

# Review of Computer Engineering Research

2022 Vol. 9, No. 3, pp. 200-208.

ISSN(e): 2410-9142

ISSN(p): 2412-4281

DOI: 10.18488/76.v9i3.3148

© 2022 Conscientia Beam. All Rights Reserved.



## A MODEL FOR THE SAFETY RISK EVALUATION OF CONNECTED CAR NETWORK

 **Thalakola Syamsundararao**<sup>1+</sup>

 **Badugu Samatha**<sup>2</sup>

 **Praveen Kumar Pinjala**<sup>3</sup>

 **Nagarjuna Karyemsetty**<sup>4</sup>

<sup>1</sup>Department of Computer Science and Engineering, Kallam Haranadhareddy Institute of Technology (A), Chowdavaram, Guntur, India.

Email: [syamsundar@khitguntur.ac.in](mailto:syamsundar@khitguntur.ac.in)

<sup>2</sup>Department of Computer Science and Engineering, Vignan's Foundation for Science, Technology and Research, Vadlamudi, Guntur, India.

Email: [drbs\\_cse@vignan.ac.in](mailto:drbs_cse@vignan.ac.in)

<sup>3</sup>Department of Information Technology, Vignan's Institute of Information Technology (A), Visakhapatnam, India.

Email: [pk.pinjala@gmail.com](mailto:pk.pinjala@gmail.com)

<sup>4</sup>Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, India.

Email: [nagarjunak@kluniversity.in](mailto:nagarjunak@kluniversity.in)



(+ Corresponding author)

### ABSTRACT

#### Article History

Received: 4 July 2022

Revised: 31 August 2022

Accepted: 16 September 2022

Published: 3 October 2022

#### Keywords

Autonomous vehicles

Internet of vehicles

Privacy

Risk prediction

Safety

Security.

The automobile industry is preparing for what is now anticipated to be a big transition toward linked and autonomous vehicles. This introduces significant dangers both to individuals' privacy and to the intricate workings of electrical and electronic systems. Currently, the automotive industry has well-established and government-mandated safety risk management methods. They present an improved risk assessment methodology and demonstrate its validity with a real-world use case to facilitate the derivation of safety procedures and safety solutions for automotive integrated devices. This should make it simpler to ensure the safety of integrated vehicles. Some of the significant factors are the accessibility of functional safety to individuals who are not trained in safety and the appropriateness of existing techniques for said functional safety. The methodology that is used to assess the risks posed by properties and capacities includes a risk analysis as an essential component. The next step in the process of managing risks involves determining both the degree of risk and the magnitude of the potential impact. In this step, various different rules and requirements that are already in place are utilized to make any necessary adjustments. After much deliberation, a level of security has been settled on in order to facilitate the formulation of high-level security objectives. Due to the fact that this design has a good convergence with contemporary principles and criteria, it ought to be capable of being adequately suited to the prerequisites of the automotive sector.

**Contribution/Originality:** This research focuses on safety and security levels of connected networks and predicts the degree of risk in dynamic moving vehicles.

## 1. INTRODUCTION

Cars have traditionally been viewed as lonely, immobile, and closed systems, but recently, a paradigm shift toward connected and autonomous vehicles has begun. Cars are becoming increasingly individualized while also becoming gradually more connected to the Internet of Things (IoT). According to a market survey [1-3] by the year 2022, 85 percent of all vehicles will be connected to the Internet. [Citation needed]. In the cars of the future, the usage of technology and the complexity of electrical systems and components will both continue to increase, which will result in the introduction and potential vulnerability to new threats to safety and protection. When it comes to the automotive industry, safety is regarded as a consideration that cannot be compromised [4]. An example of a

methodology and process that has been created and regulated to attain an acceptable level of protection during the implementation of safety-critical components is the operational safety requirement for road cars known as ISO 26262. This requirement, which would be based on the more general safety requirements [5] would be an excellent illustration of a methodology and process. However, despite the fact that security threats against transport might put the safety of drivers, passengers, and other road users at risk [6], the automobile industry has recently begun to place a greater emphasis on safety as security threats have hardly been addressed in an appropriate manner. Researchers have already demonstrated that it is possible to commit acts of violence that put a significant amount of one's security in jeopardy. As a result, consideration should be given to safety problems and potential hazards in order to improve the protection offered by automobiles.

An example of a methodology and procedure that has been created and regulated to achieve an acceptable level of protection during the implementation of safety-critical components is the operational safety regulations for road cars, known as International Standard Organization (ISO) 26262. These regulations would be based on the more general safety requirements, which would make them a good example of a methodology and accompanying procedure. Despite the fact that vulnerabilities in a transport pose a threat to the safety of its drivers, customers, and other users of the road [6] the security of the automotive industry has only recently begun to receive attention, and approaches to addressing the matter of vehicular security have been largely inadequate. Due to this, consideration must be given to safety problems and potential dangers for the sake of enhancing the protection offered by automobiles. Because the criteria are typically exercised by contractors, one of the development goals was to design an architecture that is easy to use because the outcomes are easy to grasp. This was accomplished by making the criteria as straightforward as possible. We define the "degree of safety", which is a phrase that is fundamentally connected to the "level of vehicle safety integrity" as described in International Standard Organization (ISO) 26262 [7]. The "Security Level" would be a risk-based measure that is unique to the automotive industry. It has been used to describe the degree of risk reduction that must be applied while developing automotive systems when handling security threats [8-10]. We make adjustments to various industry standards in order to determine the potential impact that a threat could have on particular security goals. When calculating the threat level, they do not take into account the amount of time that has passed since the last incident as a separate parameter, as opposed to what it seen in earlier standards and protocols [11], despite the fact that it is possible to infer it from other components of the same framework, such as the available technology and the level of skill possessed by the attacker. The perpetrator's intention is not recognized as a distinct feature either [12] due to the fact that it is inherent in other features and extremely difficult to model.

## 2. RELATED WORK

Given the importance of safety engineering processes to the vehicle engineering process, one of the goals should be to ensure that they can be easily integrated to pre-existing safety manufacturing practices. The procedure for our method is depicted in Figure 1, beginning with the analyzed system specification [13-16]. Many levels of specificity could be correlated to a network, depending on what needs to be investigated, such as the entire electrical and electronic infrastructure, a motor performance that is implemented using multiple electronic control devices, a specific Engine Control Unit (ECU), ECU hardware, or an ECU programme. They call the "system" that is currently being examined (the "platform") in order to keep things as simple as possible. As soon as the platform has been determined, the risk assessment, which will be a two-stage procedure, may begin. The question of which parts of the system are essential and call for certain precautions to be taken should be the motivating factor behind asset identification.

We considered information that is vital to the protection of individuals, such as the specifics of an individual's automobile or the individualized programming found on a given ECU. The second step was to detect potential threats and involved comparing each piece of property to a pool of probable dangers. As soon as risks were identified for any and all resources, the created risk combinations were incorporated into the process of putting those plans into action.

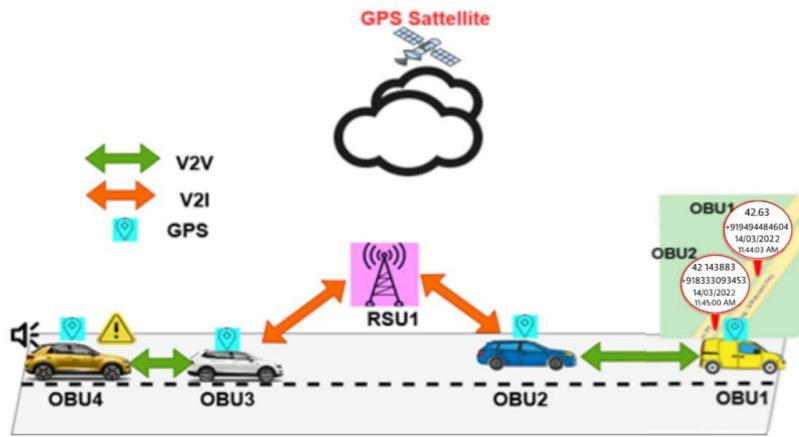


Figure 1. Connected car network.

During the risk assessment, the likelihood of an impact or the magnitude of an effect caused by a combination of an activity and a threat are both taken into consideration as shown in Figure 2. These two duties are known as the hazard rating and the effect rating [17]. The danger level provides an estimation of the likelihood that an attacker will carry out a risk against an asset while the impact level provides an estimation of the possible damage that may be incurred by stakeholders. After determining the risk level and the extent of the impact that the risk poses, the next step would be to compute the safety level by taking into account both the alert level and the possible effect. Figure 3 shows the levels of threat security in connected dynamically moving cars.

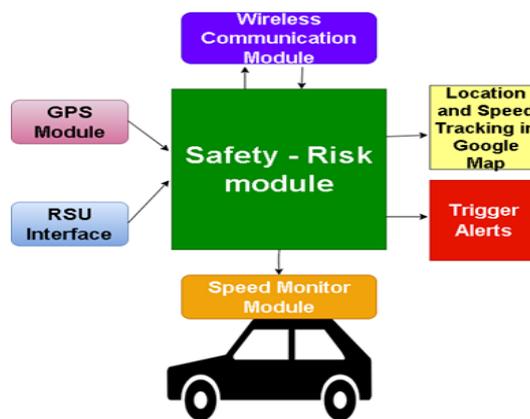


Figure 2. Model of safety- risk module.

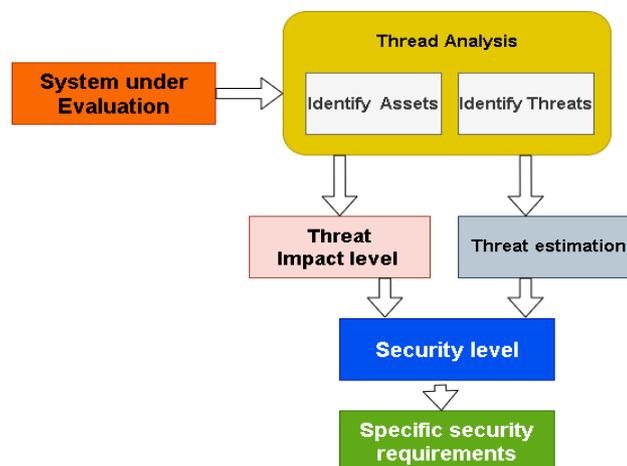


Figure 3. Threat analysis in connected cars.

### 3. PROPOSED SYSTEM AND EVALUATION OF THE RISKS

STRIDE's primary objective is to catalogue all of the possible uses for various network services. Tools that enable users to describe the flow of data over a network by drawing data flow diagrams are examples of what could be utilized for automatic hazard recognition with Spoofing identity, Tampering with data, Repudiation threats, Information disclosure, Denial of service, and Elevation of privileges (STRIDE). The data flow diagrams are the source of a risk assessment that includes a list of the risk pairings. Threats do not immediately match vulnerabilities [18], but risks take use of and exploit their flaws and weaknesses. It's possible for a single vulnerability to be the source of multiple dangers, whereas a single incident could potentially attack multiple hazards. The Vulnerability Assessment Simulation Tool 2014 is used to locate all of these connections. They apply this strategy to the velocity restrict use-case and produce the data flow diagram that is displayed in Figure 4. It is substantially more detailed and tangible than the control strategy that had been devised in the past because the Data Flow Diagram (DFD) enables operations for an Aftermarket instrument that could be used by a Human Consumer to alter the settings of the Regional Screen Level (RSL). The tool will then provide a threat report that describes the various attributes and dangers associated with the threat. At some point in time, individuals will extract asset matches from the document in order to initiate the process of risk management.

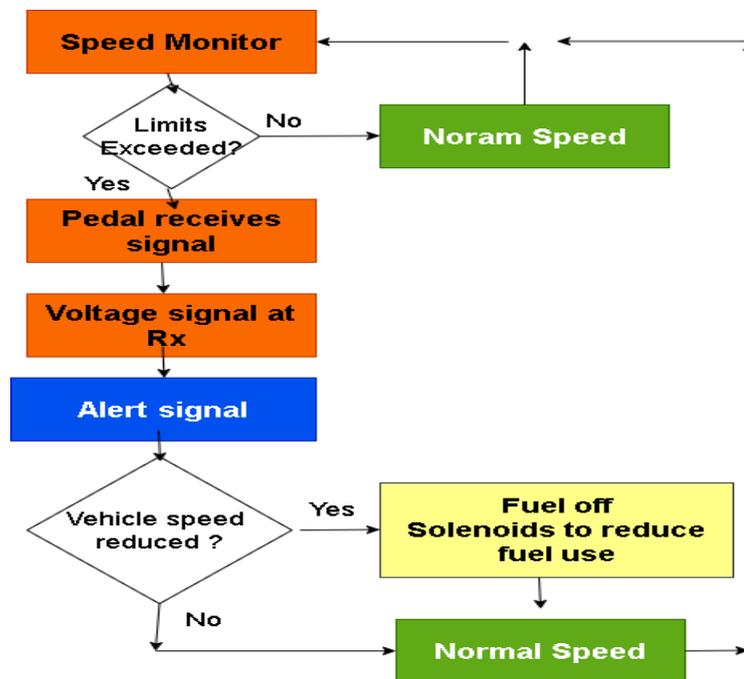


Figure 4. shows the data flow for the speed limiter.

A connection between a threat and an action is shown in Table 1. As a consequence of this, the correction factor that is being sent from the tacho to the RSL-ECU is a piece of digital data. As such, its authenticity is susceptible to being compromised if it is altered or tampered with while it is en route. According to this, it is possible for an unauthorised individual to make a fake version of the ParameterChangeRequest, that an Aftermarket product might then submit to the RSLECU, in order to change the limit that is displayed. Even though there are undoubtedly a lot of different permutations of resources, these two components only ought to be sufficient to explain the process. The results of the risk assessment of the speed limit are presented in Table 1.

Table 1. Risk assessment of speed limit.

ID	Assesst	Threat	Security Concern
1	Conversion factor	Tampering	Integrity
2	Variable change Rq	Spoofing	Authenticity

After each danger has been identified for each resource, the risk assessment process helps prioritise the hazards that need to be addressed. The threat assessment consists of three steps: determining the amount of hazard, evaluating the level of effect, and finally integrating all three to define secure communication [19]. First, identify the level of hazard. The standards for acceptable levels of risk dictate the level of protection that must be provided. The level of alert, the level of impact, and the level of safety are each discussed in further detail in the next three subheadings.

The number of hazard level parameters is listed in Table 2.

Table 2. Hazard level parameters

Expertise Value	Knowledge value - Target	Window value	Experiment value
Zero -0	Public -0	Unlimited -0	Standard-0
Proficient -1	Restricted -1	Large-1	Specialized-1
Experience-2	Sensitivity -2	Medium-2	Bespoke-2
Expert- 3	Critical -3	Small-3	Multiple Bespoke-3

The danger level offers a forecast on the likelihood that a particular threat will occur. As can be seen in Table 2, each variable has a total of four phases, and each step has a value associated with it. As parameter values go up, so does the likelihood of a potentially catastrophic occurrence happening. They employ a linear scale for each variable, which is different from designs and thus makes it easier to reason consistently about the numerous components and compute the risk level for a particular hazard couple. Designs use a logarithmic scale. The scales can very easily be modified in order to cater to particular needs. Before going into further detail regarding the significance of each individual step, a human being would first provide a concise explanation of the danger level calculation's processes and outcomes. To compute a danger level when all of the parameter values for a particular hazard have just been approximations, the following straightforward linear Equation 1 could be utilized:

$$T_{sum} = W_x T_x + W_k T_k + W_y T_w + W_z T_z \tag{1}$$

where the variables x, k, w, and e correspond to the four variables, respectively, and wi and ti are the value and predicted threat level values of characteristic i. where x, k, w, and e are the variables that correspond to the four variables. Under the assumption that all of the variables have the same level of importance, wi = 1, the formula or Equation 2 can be shortened to:

$$T_{sum} = T_x + T_k + T_w + T_z \tag{2}$$

Weights can be adjusted in order to fulfil the specific requirements of an organization. A qualitative indicator of the level of risk has been offered by our method in the form of one of five levels: none, low, medium, strong, or critical. These levels are as follows: After the Tsum value has been calculated, the level of threat is lowered using a predefined system, as illustrated in Table 3.

Table 3. An estimate of the level of danger.

Variable Sum	Threat Level	Value
>9	None	0
7 - 9	Low	1
4 - 6	Medium	2
2 - 3	High	3
0 -1	Critical	4

The effect threshold is an evaluation of the potential losses that would be incurred by a variety of stakeholders in the event that a particular investment couple was realized. Each of the four variables can be assigned one of the following four levels: zero, low, medium, or high. The data shown in Table 4 indicates that there is a numerical value that corresponds to each level. Before delving into the specifics of each of the four facets of the impact, we would begin by providing a concise explanation of the steps that were done and the findings of the impact level estimation. After

each of the impact parameters has been evaluated to establish the level of influence that will arise, the following simple linear Equation 3 can be utilized to compute the entire sum of those parameters' effects:

$$M_{sum} = W_x M_x + W_k M_k + W_y M_w + W_z M_z \tag{3}$$

where the indicators f, o, and p stand for the factors Security, Economic, Functional, Security, and Regulatory, respectively, and w<sub>j</sub> and i<sub>j</sub> are the weight as well as the projected effect level of characteristic j, where the indicators f, o, and p stand for the factors Security, Economic, Functional, Security, and Regulatory, respectively.

Table 4. Results for impact level parameters.

Safety	Operational	Financial	Privacy & Leglitive	Value
N	N	N	N	000
L	L	L	L	001
M	M	M	M	010
H	H	H	H	100

It was possible to adjust the weights so that they corresponded more closely to the desired level of alertness. The weights that are assigned to the effect variables in standard parameters are not consistent. Taking into account that the effects of the operational, privacy, and financial implications are relatively minor, it is possible that the effects of the security and economic implications will result in the most severe repercussions for stakeholders. For example, passengers in cars could be killed, and businesses could go out of business. Because of this, we recommend that.

$$W_s = W_f = 10 \quad \text{and} \quad w_o = w_p = 1$$

As a consequence of this, the formula Equation 4 can be simplified as follows:

$$X_{sum} = 10 ( X_s + X_f ) + X_o + X_p \tag{4}$$

After then, the extent of the overall influence would be determined by calculating the resultant average, as shown in Table 5.

Table 5. Current analysis of the effect level.

Variable Sum	Threat level	Value
0	None	0
0 - 19	L	1
20 -99	M	20
100 - 999	H	3
> 1000	C	4

#### 4. DEGREE OF SECURITY

The level of protection that is required, as well as the choice of safeguards, is determined by the security requirements that are placed on the system. The formula for determining the safety level, which takes into account both the hazard level and the effect level, is presented in Table 6. Comparable to the practice of allocating different degrees of vehicle safety integrity in terms of objectives and procedures is the following: What should be stressed, however, is that due to the ever-changing nature of the threat level, the security level is significantly more fluid. There are five progressively higher degrees of security to be recommended: Four levels of quality control: critical, low, medium, and high. The phrase "quality assurance" comes from the international standard ISO 26262, and it denotes that the necessary quality controls are sufficient and do not call for any further controls as a means of risk reduction. This suggests that investment pairings with a Quality Monitoring (QM) security level would not be required to have any additional security measures taken on their behalf. For the next four layers of security, comprehensive security requirements need to be drafted. It is important to keep in mind that the level of safety does not have any bearing on the stringency of the criterion at this stage. It is possible to link a single asset to several hazards, which would result in the element having multiple degrees of security [20]. If this scenario were to play out,

the asset's current level of security would be the most stringent that could possibly be required for this piece of property.

Calculating the level of security based on the affects and the risks is shown in [Table 6](#).

**Table 6.** Security and risk levels.

Security Level (SL)		Q0	Q1	Q2	Q3	Q4
Threat Level (TL)	Q0	0	0	0	0	1
	Q1	0	1	1	1	2
	Q2	0	1	2	2	3
	Q3	0	1	2	3	3
	Q4	0	2	3	3	4

After the risk and hazard assessment has been carried out, the determination of the maximum safety criteria for the investment combinations that have been found will still require the assistance of a human. It should be underlined that more acceptable technical safety measures should be developed at a later period, even though doing so is outside the scope of this work; nonetheless, it should be noted that this work is outside the scope of this work. At this point in time, the protection had no connection to the high-level security standards that were being created. The only thing that the security level indicates is that there needs to be a developed security requirement: The security level is understood or translated into countermeasures at the time that the architectural, hardware, or software security requirements are defined. It needs to be underlined once more that property combinations that have a safety level of QM do not have any security processes at all, but that high-level criteria need to be set for all of the other investment pairings.

Because threat assessment and risk assessment are often carried out during the concept stage of the development lifespan, operational specifics are frequently lacking at this stage [21]. This is because the development lifespan begins with the concept stage. As a consequence of this, it is probable that it will not always be possible to specify the exact security measures that need to be put in place in order to fulfil the high-level security needs. Nevertheless, all through the product development stage of the product's lifecycle, the anticipated security level for each investment combination, in conjunction with its high-level security requirement, should be utilized to identify a suitable security mechanism to meet the requirements for a specific security level. Even though the subject of security assurance is not addressed in our architecture, the application of common criteria is possible whenever it is required.

## 5. CONCLUSIONS

The ongoing paradigm shift toward autonomous and connected vehicles, as well as the rising utilization and complexity of E/E technology, will undoubtedly result in the emergence of new concerns pertaining to the protection of personal information, privacy, and security. In the past, the automotive industry was largely devoid of any form of safety risk management. Today, however, safety risk management is both more prevalent and more regulated. This study puts forward a framework for analysing threats and determining levels of risk in order to more effectively address safety concerns, which provide a method that can be used to determine a "security level" and formulate high-level security requirements. This has a number of distinct benefits: it is simple to use, even for individuals who are not knowledgeable in the field of safety. Due to the fact that it is in outstanding agreement with ISO 26262, it is straightforward and easy to comprehend for automobile engineers. The extremely secure standards that were developed as a result align with operational safety regulations, and the four different security arrangements can be compared to different levels of automotive safety integrity. Because subcontractors frequently comply with requirements, the terms governing them must be clear.

**Funding:** This study received no specific financial support.

**Competing Interests:** The authors declare that they have no competing interests.

**Authors' Contributions:** All authors contributed equally to the conception and design of the study.

## REFERENCES

- [1] M. Ashjaei, L. L. Bello, M. Daneshlab, G. Patti, S. Saponara, and S. Mubeen, "Time-Sensitive Networking in automotive embedded systems: State of the art and research opportunities," *Journal of Systems Architecture*, vol. 117, p. 102137, 2021. Available at: <https://doi.org/10.1016/j.sysarc.2021.102137>.
- [2] R. Jabbar, M. Shinoy, M. Kharbeche, K. Al-Khalifa, M. Krichen, and K. Barkaoui, "A model for detecting tiredness in drivers, built with techniques from convolutional neural networks and intended for use in an android application," presented at the The IEEE International Conference on Informatics, Internet of Things, and Enabling Technologies (ICIOT) will take place in the year 2020. IEEE, 2020.
- [3] C. Schmittner and G. Macher, "The relationship between cybersecurity standards and an overview of the automotive industry," presented at the Within the Framework of the International Conference on Computer Safety, Reliability, and Security. Springer, Cham, 2019.
- [4] B. Karnan, A. Kuppusamy, T. P. Latchoumi, A. Banerjee, A. Sinha, A. Biswas, and A. K. Subramanian, "Multi-response optimization of turning parameters for cryogenically treated and tempered WC-co inserts," *Journal of The Institution of Engineers (India): Series D*, vol. 103, pp. 263–274, 2022. Available at: <https://doi.org/10.1007/s40033-021-00321-x>.
- [5] F. Pascale, E. A. Adinolfi, S. Coppola, and E. Santonicola, "Cybersecurity in automotive: An intrusion detection system in connected vehicles," *Electronics*, vol. 10, p. 1765, 2021. Available at: <https://doi.org/10.3390/electronics10151765>.
- [6] X. Zhang and S. Mahadevan, "Bayesian network modeling of accident investigation reports for aviation safety assessment," *Reliability Engineering & System Safety*, vol. 209, p. 107371, 2021. Available at: <https://doi.org/10.1016/j.res.2020.107371>.
- [7] T. P. Latchoumi, G. Kalusuraman, J. F. Banu, T. L. Yookesh, T. P. Ezhilarasi, and K. Balamurugan, "The application of the Grey-Fuzzy and LK-SVM approaches to the improvement of production systems," presented at the IEEE International Conference on Intelligent Systems, Smart and Green Technologies (ICISSGT) . IEEE, 2021.
- [8] A. Venkatesh, T. Latchoumi, S. Chezhian Babu, K. Balamurugan, S. Ganesan, M. Ruban, and L. Mulugeta, "Multiparametric optimization on influence of ethanol and biodiesel blends on nanocoated engine by full factorial design," *Journal of Nanomaterials*, pp. 1-9, 2022. Available at: <https://doi.org/10.1155/2022/5350122>.
- [9] S. Arabi, A. Haghighat, and A. Sharma, "A system for detecting construction vehicles that is based on computer vision and uses deep learning," *Computer-Aided Civil and Infrastructure Engineering*, vol. 35, pp. 753-767, 2020.
- [10] H. Olufowobi, C. Young, J. Zambreno, and G. Bloom, "Saiducant: Specification-based automotive intrusion detection using controller area network (can) timing," *IEEE Transactions on Vehicular Technology*, vol. 69, pp. 1484-1494, 2019.
- [11] A. L. Dakwat and E. Villani, "System safety assessment based on STPA and model checking," *Safety Science*, vol. 109, pp. 130-143, 2018. Available at: <https://doi.org/10.1016/j.ssci.2018.05.009>.
- [12] L. T. Pugazhendhi, R. Kothandaraman, and B. Karnan, "Implementation of visual clustering strategy in self-organizing map for wear studies samples printed using FDM," *Signal Processing*, vol. 39, pp. 531-539, 2022. Available at: <https://doi.org/10.18280/ts.390215>.
- [13] I. Studnia, E. Alata, V. Nicomette, M. Kaâniche, and Y. Laarouchi, "A language-based intrusion detection approach for automotive embedded networks," *International Journal of Embedded Systems*, vol. 10, pp. 1-12, 2018. Available at: <https://doi.org/10.1504/ijes.2018.10010488>.
- [14] J. Martins, A. Tavares, M. Solieri, M. Bertogna, and S. Pinto, "Bao: A lightweight static partitioning hypervisor for modern multi-core embedded systems," presented at the Workshop on Next Generation Real-Time Embedded Systems, 2020.

- [15] M. W. Anwar, M. Rashid, F. Azam, M. Kashif, and W. H. Butt, "A model-driven framework for design and verification of embedded systems through systemVerilog," *Design Automation for Embedded Systems*, vol. 23, pp. 179-223, 2019. Available at: <https://doi.org/10.1007/s10617-019-09229-y>.
- [16] P. Munk and A. Nordmann, "Model-based safety assessment with SysML and component fault trees: Application and lessons learned," *Software and Systems Modeling*, vol. 19, pp. 889-910, 2020. Available at: <https://doi.org/10.1007/s10270-020-00782-w>.
- [17] S. Mubeen, E. Lisova, and A. Vulgarakis Feljan, "Timing predictability and security in safety-critical industrial cyber-physical systems: A position paper," *Applied Sciences*, vol. 10, p. 3125, 2020. Available at: <https://doi.org/10.3390/app10093125>.
- [18] L. L. Bello, R. Mariani, S. Mubeen, and S. Saponara, "Recent advances and trends in on-board embedded and networked automotive systems," *IEEE Transactions on Industrial Informatics*, vol. 15, pp. 1038-1051, 2018. Available at: <https://doi.org/10.1109/tii.2018.2879544>.
- [19] P. R. Garikapati, K. Balamurugan, T. P. Latchoumi, and G. Shankar, *A quantitative investigation into the processing of small datasets utilizing agglomerative hierarchical clusters and K-medoids emerging technologies and biomedical systems are discussed in the following article*. Singapore: Springer, 2022.
- [20] R. Jabbar, M. Shinoy, M. Kharbeche, K. Al-Khalifa, M. Krichen, and K. Barkaoui, "An urban traffic monitoring and modelling system is one application of internet of things technology that can be used to make roads safer," presented at the The Internet of Things, Embedded Systems, and Communications International Conference (Iintec) will take place in 2019. IEEE, 2019.
- [21] W. Wu, R. Li, G. Xie, J. An, Y. Bai, J. Zhou, and K. Li, "A survey of intrusion detection for in-vehicle networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 21, pp. 919-933, 2019.

*Views and opinions expressed in this article are the views and opinions of the author(s), Review of Computer Engineering Research shall not be responsible or answerable for any loss, damage or liability etc. caused in relation to/arising out of the use of the content.*