FUNCTIONAL SAFETY-ORIENTED RISK ANALYSIS OF HEAVY VEHICLE PLATOONING

Luboš Mikula*, Jan Famfulík

VSB - Technical University Ostrava, Faculty of Mechanical Engineering, Institute of Transport, Ostrava - Poruba, Czech Republic

*E-mail of corresponding author: lubos.mikula.st@vsb.cz

Luboš Mikula 0000-0003-2432-1047, Jan Famfulík 0000-0001-6500-1213

Resume

In this paper is presented platooning as a promising approach to reduce the greenhouse gas emissions, fuel consumption, and operation costs in heavy traffic. Attention is given to a risk assessment of vehicle-to-vehicle (V2V) communication in the context of ISO 26262, Edition 2: Road vehicles - Functional safety. [ISO 26262-2 2018] The analysis focuses on safety-related hazards associated with convoy driving of heavy vehicles, utilizing the principles of functional safety. It applies hazard analysis and risk assessment (HARA) to classify potential risks according to their severity, exposure, and controllability. Automotive safety integrity level (ASIL) is later determined for each risk. The results provide the ASIL levels of identified hazards, which can be used for developing and validating functional safety measures for cooperative truck driving.

Article info

Received 27 October 2025
Accepted 17 December 2025
Online 10 February 2026

Keywords:

truck platooning
functional safety
hazard analysis and risk assessment
automated driving
ISO 26262

Available online: https://doi.org/10.26552/com.C.2026.015

ISSN 1335-4205 (print version)
ISSN 2585-7878 (online version)

1 Introduction

Regardless of significant improvements in road safety, 18,786 fatalities occurred in the European Union in 2020, with 44.2% of passenger vehicle occupants, 3.5% of light commercial vehicles, and 2.3% of heavy trucks. Studies estimate [1] that most of these fatalities (67%) are caused by the driver's mistake or temporary driver disadvantage. At the same time, the road transport is responsible for 29% of EU CO_2 emissions (739.7 million tons in 2021) [2]. Together with limited economic efficiency, caused by driver availability and mandatory rest periods, the need for autonomous vehicles is increasing. However, the increase from SAE Level 2 autonomy to Level 3 brings a high safety risk due to the increased complexity of E/E systems, [3]. Appropriate and practical middle step for heavy vehicles is truck platooning, which can reduce aerodynamic drag, together with lower fuel consumption, emissions and driver demand, [4-5]. In this paper the focus was on the risks related to safety-relevant components of the truck platooning system according to ISO 26262 ed. 2, with particular focus on V2V communication and vehicle control functions.

2 Truck platooning and V2V communication

The concept of convoy driving has been significantly improved in recent years, due to rapid progress in electronic control systems and digitalization. In a typical platooning system, vehicles operate at different levels of automation, utilizing Vehicle-to-Vehicle communication. The leading truck is actively driven by a human driver, while the following vehicles are passively controlled based on the leader's behaviour. This arrangement is now referred to as a platoon. Multiple research projects have been held over the past decade by both vehicle manufacturers and scientists. These projects have emerged on various aspects of platooning, which can be separated into these main domains:

- Transport and logistics, with a focus on economic savings.
- Automation and autonomous driving, with technologies such as ACC, or CACC [7].
- Energy efficiency aiming to reduce drag and improve sustainability [8-9].
- Safety and legislation defining the regulatory framework.
- Telecommunications, ensuring reliable and safe

Figure 1 *Project ENSEMBLE [6]*

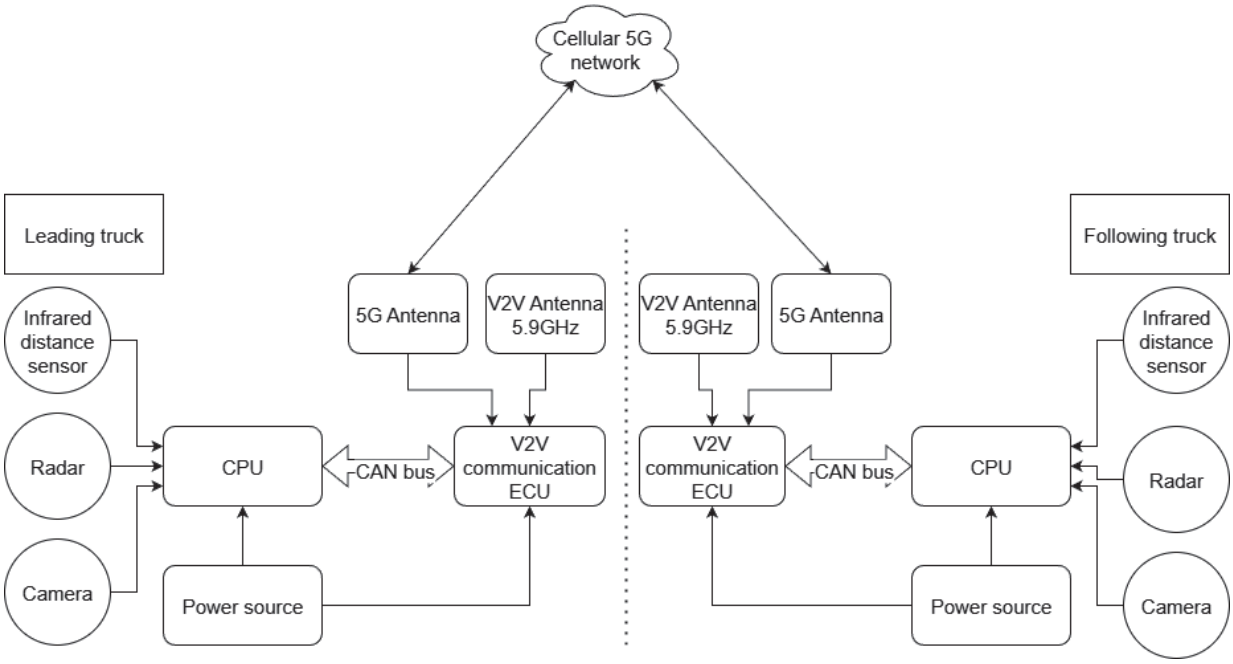

Figure 2 *Proposed V2V system architecture*

V2V communication.

- Real-world testing, validating theoretical benefits. [10-11].

The EU-funded project ENSEMBLE, shown in Figure 1. has been one of the significant projects, aiming to establish standards for the commercial deployment of platooning technology, [11], While the similar projects have been held in the United States by the National Highway Traffic Safety Administration. Both projects aim to bring technical standards and operational guidelines for manufacturers, operators, and drivers.

From an energy perspective, studies suggest that fuel consumption can be reduced up to 10% with truck platooning due to reduced drag. [12] Combined with design improvements such as digital side mirrors or aerodynamic body panels, drag can be reduced even more. [13] One of the most sensitive issues is still safety and legislation related to platooning, where the most critical attributes are response times and well-defined fallback strategies. While the legal frameworks are developed to allow autonomous vehicles operate on public roads, with compliance of safety standards.

The backbone of platooning and autonomous vehicles is communication. Communication can be realized as short-range Vehicle to Vehicle or cellular Vehicle to Cellular, where both approaches have advantages and disadvantages. Modern fifth-generation cellular networks offer low latency, high data throughput, and advanced security features; however, limitations lie in imperfect coverage in remote areas and latency drops in case of a high number of connected clients. Cross-border connectivity is another issue that limits the full-scale

use of 5G in autonomous vehicles, [14-15]. These are the reasons why the direct low-distance V2V communication is still primarily used. While this approach ensures low latency and independence from mobile infrastructure, it faces challenges in interoperability across different manufacturers and requires common standards to achieve widespread deployment. A critical concern in communication remains cybersecurity, where a potential attack may cause fatal road accidents. Ensuring authenticity, confidentiality, and integrity in communication is therefore vital for maintaining safety and a reliable system.

Pilot programs across the globe confirm that platooning can bring benefits in terms of efficiency and sustainability. Before the platooning can be evolved into fully autonomous automated systems with minimal human involvement, the already listed issues with safety and general user acceptance must be addressed. Based on the systems used in the above-mentioned platooning projects a simplified architecture as the subject of the safety assessment has been proposed. As shown in Figure 2, the system consists of multiple onboard sensors and cameras, that provide information used to control the vehicles. Connectivity is supplied by both 5G network and dedicated V2V 5.9 GHz antennas, where 5G is primarily designed for infrastructure communication, while the V2V antennas provide data transfer between the trucks.

3 Functional safety and ISO 26262 framework

The main objective of automotive systems functional safety is to reduce the risk of hazardous events caused by failures in vehicle systems and components. The automotive functional safety standard ISO 26262 builds on the generic standard IEC 61508, which defines the safety requirements for electronics across all industries. ISO 26262 uses these principles in specific conditions of road vehicles, with high production volumes, short development cycles, and complex operating environments. The second edition, published in 2018, extends to trucks, buses, and motorcycles and clarifies discrepancies from the first edition [16].

ISO 26262 ed.2 consists of twelve parts for the entire safety lifecycle, beginning with the concept and system development phase, followed by operation, service, and commissioning. The main section of this lifecycle is Hazard Analysis and Risk Assessment (HARA), which identifies potential hazards, defines safety goals, and ensures their correct implementation.

These safety goals are later translated into technical requirements, such as redundancy and fault detection. An emerging challenge within ISO 26262 is the integration of neural networks and machine learning into automotive systems. Although the standard categorizes them as software components subject to systematic faults, their inherently probabilistic and data-driven behaviour does not fit the traditional deterministic models. Errors may result from insufficient training, adversarial attacks, or sensitivity to minor input variations. Consequently, new approaches are being investigated to adapt functional safety methods to AI-based subsystems, particularly in perception and decision-making functions used in automated driving.

4 Methodology hazard analysis and risk assessment (HARA)

The Hazard Analysis and Risk Assessment (HARA) is a systematic process defined in ISO 26262 ed. 2, to identify potential hazardous events in road vehicles. At the same time, target is to evaluate associated risks and assess Automotive Safety Integrity Level (ASIL). Hara represents a fundamental part of functional safety analysis as its results are used to determine the safety goals that guide the technical design and validation requirements.

According to ISO 26262 ed.2, HARA is typically performed during the concept phase of the development and includes these steps:

- Identification of system functions and possible malfunctions,
- definition of hazardous events,
- risk assessment and
- definition of safety goals.

The first step is to define the system functions along with potential faults or failures. Possible hazards for each fault are determined for different driving scenarios. Each hazardous event is a unique combination of fault and specific operational conditions. Each event is assessed based on Severity (S), Exposure (E), and Controllability (C), where the standard provides guidance for the assignment of these values as follows:

a. Severity (S)
S1 - Light or no injuries
S2 - Moderate to severe injuries
S3 - Life-threatening or fatal injuries

b. Exposure (E)
E1 - Extremely rare operating conditions
E2 - Rare
E3 - Occasional
E4 - Frequent or permanent

c. Controllability (C)
C1 - Most drivers can control the situation
C2 - A limited number of drivers can control the situation
C3 - The situation is practically uncontrollable.

Based on the combination of these parameters, ISO 26262 defines the ASIL numbers in the following levels, while the process overview is shown in Figure 3:

- QM - general quality management processes are sufficient,
- ASIL A - low safety requirements, risk is limited and controllable,

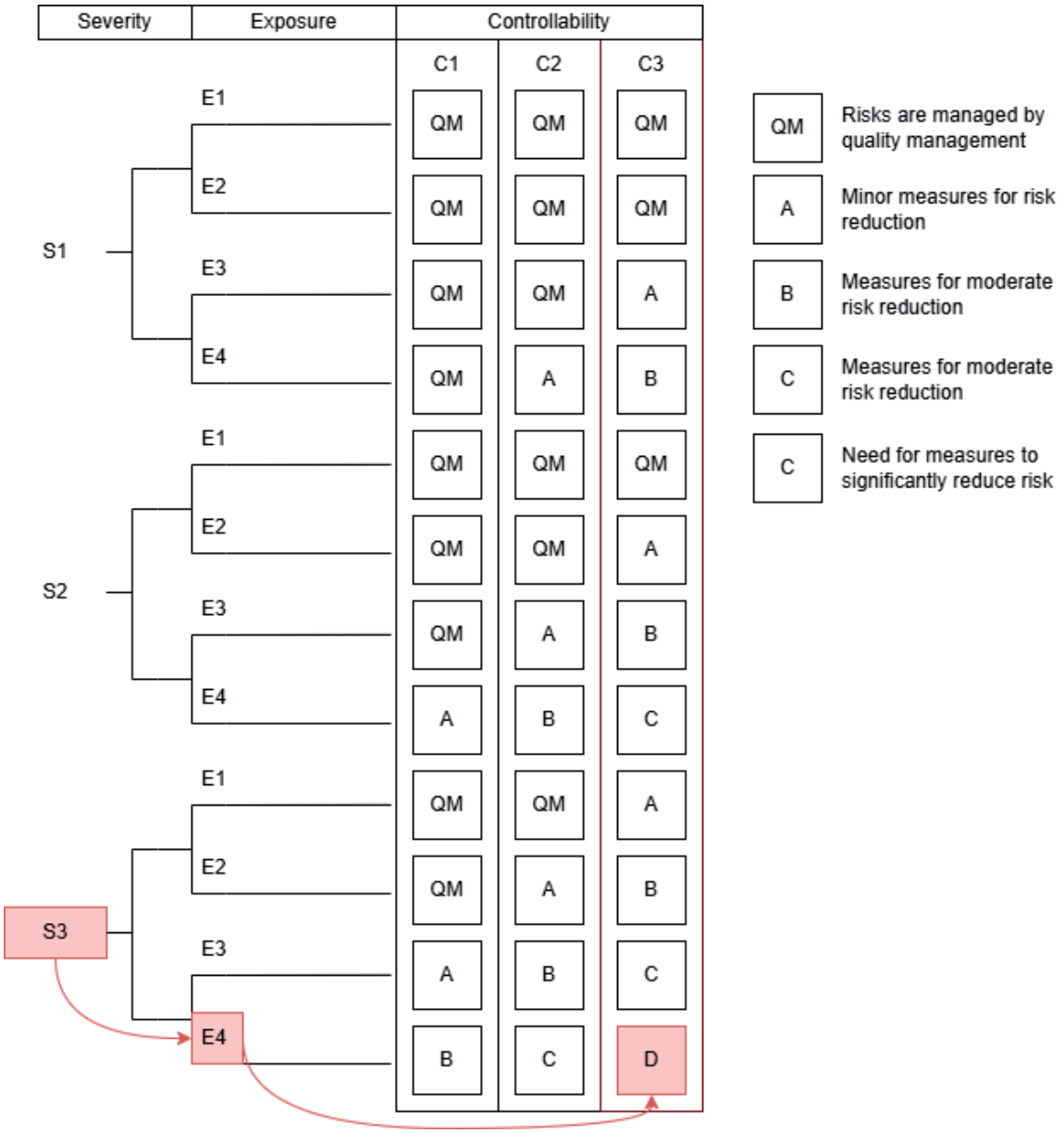

Figure 3 *HARA process overview*

- ASIL B - medium safety requirements, risks with higher severity or exposure,
- ASIL C - higher safety requirements, serious hazards with reduced controllability,
- ASIL D - highest safety requirements, most critical systems, where failures are fatal.

The list of identified hazards, together with their possible causes, and the result of the hazard assessment, is presented in Table 1. Each hazard is assigned a unique identification number. Possible hazard causes are also listed, along with Severity (S), Exposure (E) and Controllability (C) parameters as defined in ISO 26262 ed.2. Based on the combination of these parameters, ASIL level is derived for each hazard.

As an illustrative case, detailed HARA analysis for two scenarios of communication fault in a truck platoon is presented.

In the first case, the trucks travel at high speed (80 km/h) with minimal inter-vehicle distance. The complete loss of communication could lead to loss of convoy coordination, inadequate control response and increased risk of collision. As the trucks travel at similar speeds, collision severity is rated S2. Exposure is rated as E4, since communication issues may occur frequently, due to multiple reasons, such as software errors, hardware failures, or cyber-attacks. Controllability is rated C2 because, truck speeds are similar and total loss of communication could be easily detected. Based on the Figure 3, the combination of these parameters determines ASIL B for R.1.1 - Complete loss of communication, Table 2.

In the second scenario, the trucks operate at a constant speed of 80 km/h while maintaining a minimal inter-vehicle distance. Under these conditions, a

communication error may cause unpredictable responses of the following vehicles, significantly increasing the likelihood of a collision with severe consequences. Therefore, the severity of this hazard is assessed as S3, as unexpected braking or acceleration can result in life-threatening or fatal injuries. The exposure is again classified as E4, since communication disturbances can occur at any time during the platoon operation.

Table 1 *List of identified hazards and possible causes*

HAZARD NO.	HAZARD	POSSIBLE CAUSES	S/E/C ASIL
R.1.1	Complete loss of communication	Power supply failure, antenna hardware malfunction, excessive distance between vehicles, radio band interference, encryption error, hacker attack	S2/E4/C2 ASIL B
R.1.2	Erroneous communication	Antenna hardware failure, signal interference, encryption error, hacker attack	S3/E4/C3 ASIL D
R.2.1	Total loss of braking effect	Failure of wheel brake, retarder, or parking brake	S3/E4/C3 ASIL D
R.2.2	Reduced braking effect	Decreased efficiency of wheel brake, retarder, or parking brake	S2/E4/C3 ASIL C
R.2.3	Unintended braking	Incorrect brake activation without driver input	S3/E4/C3 ASIL D
R.2.4	Failure to release brakes	Malfunction of the wheel brake release mechanism	S2/E4/C1 ASIL A
R.3.1	Complete loss of tractive force	Powertrain failure	S2/E4/C2 ASIL B
R.3.2	Reduced tractive force	Reduced powertrain performance	S1/E4/C1 QM
R.3.3	Unintended tractive force	Malfunction in drive force regulation	S2/E4/C3 ASIL C
R.4.1	Complete unavailability of HMI (Human Machine Interface)	HMI power supply failure, hardware or software error	S2/E4/C2 ASIL B
R.4.2	Limited availability of HMI	Limited functionality due to hardware failure, software error, or cyberattack	S1/E4/C2 ASIL A
R.4.3	Unintended HMI commands	Incorrect inputs generated by system error or malicious attack	S3/E4/C2 ASIL C
R.5.1	Complete unavailability of control system	Power supply failure, ECU hardware failure, software error, or cyberattack	S3/E4/C3 ASIL D
R.5.2	False-positive control output	Incorrect signal from sensors or software fault triggering an unnecessary reaction	S2/E4/C3 ASIL C
R.5.3	False-negative control reaction	Failure to detect a critical situation due to incorrect evaluation of inputs	S3/E4/C3 ASIL D

Table 2 *Detailed analysis for Complete loss of communication*

HAZARD NO.	R.1.1
HAZARD	Complete loss of communication
POSSIBLE CAUSES	Power supply failure, antenna hardware malfunction, excessive distance between vehicles, radio band interference, encryption error, hacker attack
POSSIBLE CONSEQUENCES	Loss of convoy coordination, inadequate control response, increased risk of collision
SEVERITY	S2
EXPOSURE	E4
CONTROLLABILITY	C2
ASIL LEVEL	ASIL B
SAFETY GOAL	Detection of unavailable communication, fault signalling, transition to a safe state
SAFE STATE	Driver takeover, increased spacing between vehicles, controlled platoon dissolution

Table 3 *Detailed analysis of Erroneous communication*

HAZARD NO.	R.1.2
HAZARD	Erroneous communication
POSSIBLE CAUSES	Power supply failure, antenna hardware malfunction, excessive distance between vehicles, radio band interference, encryption error, hacker attack
POSSIBLE CONSEQUENCES	Antenna hardware failure, signal interference, encryption error, hacker attack
SEVERITY	S3
EXPOSURE	E4
CONTROLLABILITY	C3
ASIL LEVEL	ASIL D
SAFETY GOAL	Detect erroneous or corrupted communication, prevent unsafe control actions, and ensure reliable fallback operation.
SAFE STATE	Driver takeover with system alert, automatic platoon dissolution, and restoration of safe vehicle spacing

Due to the short spacing between vehicles and the limited ability to promptly recognize and compensate for the fault, the controllability is rated as C3. As illustrated in Figure 3 and summarized in Table 3, the combination of these parameters leads to an ASIL D classification for the communication subsystem. This assessment highlights that erroneous communication, whether caused by technical failures or malicious interference, represents one of the most critical hazards in platooning scenarios. Since the system may continue operating based on invalid data, the driver's ability to intervene is extremely limited. Consequently, hazards classified at ASIL D require the implementation of the most stringent safety measures, including subsystem redundancy, message authentication mechanisms, and plausibility checks to ensure acceptable risk levels.

5 Results and discussion

Using the aforementioned methods and approaches, the risks associated with the autonomous truck platoon are identified and evaluated using the ASIL scale. Table 1 summarizes these hazards for the key subsystems of the vehicles. The analysis covers communication between vehicles, braking components, powertrain, HMI, and the control system of the vehicle. These subsystems are highly connected, and their interaction is relevant to maintaining safe operation of the vehicle.

For each hazard, possible causes were analysed. These can be later used for subsequent development activities, such as safety mechanism specification, redundancy concepts, or monitoring concepts. This approach - linking hazards with possible causes, brings clear relation between identification and implementation of safety features.

A comparison between analysed hazards indicates that the most critical risks are directly leading to unpredictable vehicle or platoon behaviour. This includes erroneous communication, total loss of braking effect, unintended braking, unavailability of the control system, and false negative control reaction. All these hazards are evaluated as ASIL D, with high severity and limited controllability by the driver.

Generally, braking related hazards represent a significant safety concern, as both hazards may quickly change vehicle dynamics, which leads to rear end collisions in the case of vehicle platoons. Similarly, the powertrain related hazards may lead to changes in vehicle dynamics, however, differing from the braking, these changes are more gradual, making more time for the driver to react.

Hazards connected with the vehicle control system and HMI play an important role, as well. Unavailability of the control system or incorrect control decisions may lead to delayed or missing responses to critical situations. In highly automated driving modes, where the driver is only supervising the system, the ability to intervene could be reduced. The HMI-related failures may further delay driver awareness, increasing the overall risk during the fault conditions.

In contrast, hazards that lead to predictable failure are generally less critical. Complete loss of communication could be used as an example; despite its high exposure, it allows reliable fault detection and allows the human driver to take over the system.

Analysis shows that in terms of operational safety, a complete loss of communication is less critical than the communication with errors. In the cases when the communication is unavailable, the system can quickly and reliably detect the fault, alert the driver, and initiate the safe state. All the steps in this process are predictable, and residual risk mainly depends on the driver's skills. In contrast, the communication errors, may lead to false or inconsistent data transition, while the system operates as data are being valid. This may lead to unexpected convoy manoeuvres, with low opportunity for the driver to react.

6 Conclusion

In this paper is presented a functional safety assessment for vehicle-to-vehicle communication for truck platooning using the HARA methodology as defined in ISO 26262 ed. 2. The key hazards, connected to communication between vehicles, braking components, powertrain, HMI, and the global control system of the vehicle were identified, evaluated, and ASIL was assigned for them. The assessment shows how functional safety principles can be applied to cooperative driving scenarios of heavy vehicles with small inter-vehicle distances.

The results show that the highest safety requirements apply to hazards involving erroneous or corrupted communication between vehicles, total loss of braking effect, unintended braking, unavailability of the control system, and false negative control reaction. These may lead to unpredictable behaviour and cause severe accidents and were classified at the ASIL D level. Implementation of robust safety measures is required to ensure an acceptable risk level.

On the contrary, the total loss of communication has been evaluated as less safety critical in cases when the reliable malfunction detection and warning are ensured. Even though the total loss of communication can usually be classified as ASIL A, in the case of heavy vehicles traveling in a short distance platoon, it leads to a stricter classification as ASIL B in this paper.

Other subsystems described in the analysis may also independently or together affect the platoon's safety. While those hazards are typically local to individual vehicles, their impact can be bigger in a short distance platoon scenario. The results underline the need to consider the subsystem interactions when designing safety architectures for cooperative automated driving.

For the future work, simulation-based fault injection, experimental validation, and ASIL level comparison analysis can be presented. These will more precisely evaluate direct relations between the communication malfunctions and other safety-related subsystems. These extensions can lead to further development of platooning systems.

Acknowledgment

The authors received no financial support for the research, authorship and/or publication of this article.

Conflicts of interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] EUROSTAT. Greenhouse gas emissions by economic activity - transport [online] [accessed 2025-05-04]. Available from: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Greenhouse_gas_emissions_by_economic_activity

[2] EUROSTAT. Road accident fatalities - statistics by type of vehicle [online] [accessed 2025-05-04]. Available from: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Road_accident_fatalities_-_statistics_by_type_of_vehicle

[3] SAE International. Taxonomy and definitions for terms related to driving automation systems for on-road motor vehicles. Technical Report J3016_2021 [online] [accessed 2025-05-04]. Available from: https://www.sae.org/standards/content/j3016_202104

[4] MICHAUD, R., LEPAGE, P., FRENETTE, P., LETOURNEAU, D., GAUBERT, N. Coordinated manoeuvring of automated vehicles in platoons. *IEEE Transactions on Intelligent Transportation Systems* [online]. 2006, **7**(4), p. 437-447. ISSN 1524-9050, eISSSN 1558-0016. Available from: https://doi.org/10.1109/TITS.2006.883939

[5] LAMMERT, M. P., DURAN, A., DIEZ, J., BURTON, K., NICHOLSON, A. Effect of platooning on fuel consumption of class 8 vehicles over a range of speeds, following distances, and mass. *SAE International Journal of Commercial Vehicles* [online]. 2014, **7**(2), p. 626-639. ISSN 1946-391X, eISSN 1946-3928. Available from: https://doi.org/10.4271/2014-01-2438

[6] Volvo Group. Trucks on a European tour for platooning [online] [accessed 2025-05-04]. Available from: https://www.volvogroup.com/en/news-and-media/news/2016/mar/news-151 620.html

[7] MILANES, V., SHLADOVER, S. E., SPRING, J., NOWAKOWSKI, C., KAWAZOE, H., NAKAMURA, M. Cooperative adaptive cruise control in real traffic situations. *IEEE Transactions on Intelligent Transportation Systems* [online]. 2014, **15**(1), p. 296-305. ISSN 1524-9050, eISSN 1558-0016. Available from: https://doi.org/10.1109/TITS.2013.2278494

[8] CHOWDURY, H., JUWONO, R., ZAID, M., ISLAM, R., LOGANATHAN, B., ALAM F. An experimental study on the effect of various deflectors used for light trucks in the Indian subcontinent. *Energy Procedia* [online]. 2019, **160**, p. 34-39. ISSN 1876-6102. Available from: https://doi.org/10.1016/j.egypro.2019.02.115

[9] BARHOUMI, O., FARHANI, G., RAHMAN, T., ZAKI, M. H., TAHAR, S., ARAJI, F. Fuel consumption in platoons: a literature review. *arXiv* [online]. 2025, arXiv:2508.10891. eISSN 2331-8422. Available from: https://doi.org/10.48550/arXiv.2508.10891

[10] European Truck Platooning Challenge 2016. Brochure. The Hague: Government of the Netherlands, 2016 [online] [accessed 2025-05-04]. Available from: https://www.government.nl/binaries/government/documenten/leaflets/2015/10/06/leaflet-european-truck-platooning-challenge-2016/brochure-european-truck-platooning-challenge-2016.pdf.

[11] SCHMEITZ, A. Truck platooning projects, programs and cooperation groups. H2020 Project Ensemble, Deliverable D6.14. 2022.

[12] ZHANG, L., CHEN, F., MA, X., PAN, X. Fuel economy in truck platooning: a literature overview and directions for future research. *Journal of Advanced Transportation* [online]. 2020, **2020**, 2604012. eISSN 2042-3195. Available from: https://doi.org/10.1155/2020/2604012

[13] HABIBOVIC, A., ANDERSSON, J., MALMSTAIN LUNGREN, V., STAF, H. Replacing side view mirrors in trucks with integrated digital systems: prototype evaluation and potential fuel savings. Project Dreams. 2017.

[14] HAKAK, S., GADEKALLU, T. R., MADDIKUNTA, P. K. R., PRIYA, S., PARIMALA, M., DE ALWIS, C., LIYANAGE, M. Autonomous vehicles in 5G and beyond: a survey. *Vehicular Communications* [online]. 2022, **39**, 100551. eISSN 2214-210X. Available from: https://doi.org/10.1016/j.vehcom.2022.100551

[15] KOUSARIDIS, A., SCHIMPE, A., EULER, S., VILAJOSANA, X., FALLGREN, M., LANDI, G., MOSCATELLI, F., BARMPOUNAKIS, S., VÁZQUEZ-GALLEGO, F., SEDAR, R., SILVA, R., DIZAMBOURG, L., WENDT, S., MUEHLEISEN, M., ECKERT, K., HARRI, J., ALONSO-ZARATE, J. 5G cross-border operation for connected and automated mobility. *Future Internet* [online]. 2020, **12**(1), 5. eISSN 1999-5903. Available from: https://doi.org/10.3390/fi12010005

[16] International Organization for Standardization. Road vehicles - functional safety - ISO 26262, 2. ed. Geneva: ISO, 2018. ISBN 978-92-67-10667-2.