

Case Report

Open Access

Artificial Intelligence in Vehicles: Standardization perspectives

Nahid Heidari ¹, Mohammad Mahdi Share Pasand ^{2*}

1- Department of Electrical and Computer Engineering, Faculty of Engineering, Kharazmi University, Karaj, Iran.

2- Electrical Engineering Research Group, Research Center of Technology and Engineering, Standard Research Institute, Karaj, Iran.

Abstract

The integration of Artificial Intelligence (AI) in automotive technology, particularly in the context of driverless vehicles, presents significant opportunities and challenges that necessitate a comprehensive approach to standardization, safety, cybersecurity, and ethical considerations. This paper explores the implications of AI in vehicle systems, emphasizing the need for robust regulatory frameworks to address the complexities introduced by intelligent functionalities such as automatic emergency braking, driver drowsiness detection, and automatic vehicle navigation. The selected intelligent features studied in this paper are those known to have significant safety implications. Key issues discussed include the legislative and technical issues regarding the quality of training data, the interplay between AI and cybersecurity, ethical concerns regarding algorithmic decision-making, and the evolving landscape of liability in autonomous systems. The findings underscore the importance of collaboration among industry stakeholders, researchers, and regulatory bodies to foster public trust and ensure the safe integration of AI technologies into everyday transportation.

Keywords Regulation of artificial intelligence, Security and privacy, ethics, discrimination, Liability.

Introduction

Artificial Intelligence (AI) is an important emerging topic in vehicle standardization. Many vehicular sub-systems may use AI for normal operations as well as safety functions. The AI development has been freely admitted with no or little regulatory control [1] and may lead to insufficient performances in vehicle application [2]. There are several aspects according to which a vehicle could be categorized as intelligent. These aspects include automatic emergency breaking, driverless features, driver eye status monitoring, automatic speed control, etc. The core

concept in intelligent vehicles is to replace human factor by a sufficiently mature machine program. The process of making the vehicles intelligent may be accomplished by conventional automation based on human-generated codes or it may use deep learning techniques leading to artificial intelligence. While the first method can be tailored to minimize safety risks, comply to regulations and standards and avoid specific hazardous decisions, the latter can't be customized since it is generated by deep learning and there is no coded program to be changed or customized. This poses challenges and risks which are to



© The Author(s) 2023. **Open Access** This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

* Correspondence:
sharepasand@standard.ac.ir

be addressed by researchers and engineers.

The main topic of concern is the safety of driver and occupants as well as the pedestrians. However, security issues may intervene making the situation unpredictably unsafe [3]. When large numbers of intelligent driverless vehicles enter the streets, additional challenges will emerge. This requires more sophisticated processes defined for design, test and homologation process [4]. Those vehicles using components for which a kind of machine learning procedure is applied, may be subjected to more restrictions regarding the machine learning process [5]. The uncertainties of the machine learning based software and its behavior in specific marginal situations which may not be well covered in the training data, are to be identified and addressed [6, 7]. The trustworthiness and ethical compliance of artificial intelligence is still an open problem with several challenging issues [8]. These challenges rapidly grow when it comes to smart traffic control and other aspects of smart cities which require integration of the intelligent vehicles in the city [9, 10]. Another complication is the cybersecurity which may be well treated in human-operated environment but needs to be revisited in driverless and intelligent vehicles [11]. The field of industrial automation can be viewed as a pioneer field in the integration of artificial intelligence, functional safety and cyber security in complex interactive systems [12]. Therefore, the vehicle industry sector may benefit those experiences in its own journey towards integrated intelligent cities. The International Standardization Organization (ISO) has published a series of standards regarding functional safety [13]. The ISO 2622 series has been a popular and reliable standard in functional safety of road vehicles for more than a decade. However, these standards barely addressed the role of artificial intelligence in this essential field. This partially motivated the introduction of ISO 8800 [2] which draw attention to the quality and diversity of training data for machine learning procedures in which safety is important [2]. The cyber security standard ISO 21434 [14] discusses cyber security requirements but fails short to adequately address the interaction between artificial intelligence and cyber security. Intelligent vehicles are being viewed as a solution to increasing demands for mass transportation [15]. This implies that the growth of the intelligent vehicles is inevitable. However, the outcomes of utilizing these vehicles can be catastrophic if safety, ethics and legal issues are not well addressed before vast implementation. The desired outcomes of homologation of intelligent vehicles can be achieved only if they are used under pre-planned conditions with safety as a top priority [15]. In the next section we examine some critical aspects in standardization for intelligent functions of modern vehicles and intelligent vehicles.

Standardization topics and challenges

Standardization is a dynamic and iterative process during which risks of undesirable performance are identified, assessed and treated by introducing new test methods and acceptance criteria. Therefore, complete standardization is achieved only after the product is extensively used and additional information including customer feedbacks are acquired. This poses little problem for mature technological sectors in which the pace of change is slow. However, the artificial intelligence is evolving very fast nowadays. This means that standardization activities should adapt the processes and procedures in such a way that the standards do not lose track of the rapidly evolving field. In the following the most important aspects of intelligent vehicles are discussed.

1. Driver drowsiness detection

Driver Drowsiness Detection System (DDDS) is a system made of camera or sensors as well as auditory alarm to prevent accidents caused when the driver is drowsy. These accidents constitute at least 20% of road accidents [16]. The DDDS may use steering pattern, lane camera, driver eye/ face pattern or driver physiological condition (acquired via body sensors) to recognize the drowsiness of the driver.

Future DDDSs may use machine learning for the recognition of the pattern attributed to drowsy driving. European regulation (EU) 2019/2144 [16] regulates the DDDS. This regulation pays attention to two important issues:

- a. DDDS shall not interfere with warning systems (specifically Advanced Driver Distraction Warning System (ADDWS) which will be introduced later).
- b. DDDS shall not keep any personal information of the driver and shall delete any personal data after processing. DDDS shall not share that information with a third party. The aforementioned requirements are of utmost importance in terms of safety and privacy. However, [16] does not address cybersecurity, artificial intelligence and their mutual interaction. Specifically, it is important to ensure that DDDS keeps working with proper accuracy after any foreseeable cybersecurity attack. It is also of importance that a DDDS which is trained by machine learning conform to the aforementioned requirements. This may necessitate inclusion of additional training data to ensure proper reaction of the artificial intelligence in these situations and similar scenarios where privacy or safety are jeopardized.

2. Advanced driver distraction warning system

ADDWS warns the driver when it detects that he/she is distracted and does not pay attention to the road traffic ahead. As per (EU) 2019/2144, [16] the ADDWS is legislated as mandatory for new types of some types of cars.

ADDWS monitors the driver's gaze which is the direction towards which the driver is looking. If the driver's gaze is fixed towards an area beyond the road ahead, then ADDWS will make an alarm and inform the driver to pay attention to the road.

As mentioned earlier, it is essential that ADDWS does not interfere with DDDS. Specifically, only one of the two alarms should be activated at a moment. ADDWS may also use artificial intelligence to detect driver distraction. Therefore, challenges of using artificial intelligence for this system are the same as those for DDDS.

3. Advanced emergency braking system

Advanced Emergency Braking System (AEBS) is a system which autonomously brakes when an imminent accident is detected. UN ECE Regulation 131 [17] requires a system that can automatically detect a potential forward collision and activate the vehicle braking system to decelerate a vehicle to avoid or mitigate a collision. UN ECE regulation 152 mandates that deceleration can be 5 meters per second squared [18].

AEB acts independently of the driver to avoid or mitigate the accident by applying the brakes in critical situations of imminent crash. AEB should act only in the emergency situation for which it is designed. Otherwise, it can cause unnecessary collisions.

4. Emergency steering function

Emergency Steering Function (ESF) is an automated steering function that detects a potential collision and automatically activates the steering system for a limited duration to avoid or mitigate a collision. ESF is described by regulation 79 of UN ECE [20]. ESF has some limitations including the following:

- ESF may cause the driver to unconsciously intervene by steering or braking.
- ESF depends on the sensors to check whether the adjacent lane is clear. In the cases where the sensor is faulty, reliability measures should be implemented to avoid unsafe decisions. In some cases, it may not be sufficient to check the clarity of the adjacent lane. The ESF system may need to check incoming cars if those cars have high speeds.

5. Collision avoidance system

The Collision Avoidance System (CAS), also known as forward collision warning system or collision mitigation system, is designed to prevent or reduce the severity of vehicle collisions. Principally CAS measures the vehicle speed and its distance to the next vehicle in the same lane. If the vehicles become too close to each other, CAS will cause an alarm with which it warns the driver of the imminent crash. CAS may include pedestrian and obstacle

warning as well. In its simplest form, CAS is not likely to use artificial intelligence to detect imminent crash. However, when combined with other emergency functions such as AEBS and ESF it may become feasible to use artificial intelligence and machine learning for the decision-making process. In particular, when an accident is detected to be imminent, the intelligent system or vehicle should decide between the following:

- To activate CAS (only warning)
- To decelerate
- To activate AEBS
- To activate ESF
- To active AEBS and then ESF

Other choices are also plausible in some scenarios. The choice between AEBS, ESF or both depends on several factors including vehicle speed, time to crash and whether the adjacent lane is clear or not.

This decision may be delegated to artificial intelligence. This means the training data must be diverse and informative to prevent the system from causing catastrophic damages. If this decision is delegated to artificial intelligence, ethical concerns arise in scenarios where the decision-making process can lead to not-braking for instance to avoid crash from following vehicles. There are also cybersecurity concerns regarding cyber attacks that make the artificial intelligence to come to incorrect conclusions regarding the vehicle situation. These attacks can hypothetically cause the vehicle to brake in non-emergency situations or to steer to the adjacent lane when it is not clear. There are also concerns regarding electromagnetic susceptibility. For these intelligent functions may be interfered by electromagnetic waves coming from utility power cables, adjacent vehicles, etc. The electromagnetic interference can have catastrophic safety consequences for vehicles with AEBS or ESF because the interference may temporarily intervene with the decision-making process described above.

Another concern in the CAS is the liability. Liability is a legal concern in artificial intelligence decision-making. The liability problem is to determine who is responsible for consequences of a wrong decision.

6. Automatic Vehicle Navigation

In fully autonomous vehicles, navigation is conducted through an Automatic Vehicle Navigation System (AVNS) without the need for a human driver. These driverless vehicles must adhere to various requirements, including those outlined in ISO standards that emphasize functional safety and cybersecurity ([21]). These stipulations encompass compliance with safety regulations, type-approval protocols, and the integration of advanced technologies to ensure functional safety and environ-

mental sustainability. Specifically, adherence to directives that govern the performance of systems such as the Advanced Emergency Braking System (AEBS) and Lane Departure Warning System (LDWS) is mandated, as these systems are essential for maintaining safety on roadways. Furthermore, the vehicles are obliged to undergo thorough testing and evaluations to verify their adherence to EU type-approval standards, thereby ensuring that they meet the necessary technical and administrative requirements prior to their introduction into the marketplace. The incorporation of Artificial Intelligence (AI) within these navigation systems markedly enhances their capability to perceive and react to the dynamic nature of environmental fluctuations; however, this advancement simultaneously presents complex challenges that necessitate extensive and rigorous efforts toward standardization to ensure smooth operation and safety ([2], [3]).

A significant challenge that emerges in the field of automated vehicle navigation relates to the necessity of ensuring the dependability and safety of the AI algorithms employed in critical decision-making processes. These algorithms must undergo comprehensive training on a diverse array of datasets to adeptly manage a multitude of driving situations, which is essential for alleviating risks that may arise from unpredictable and unforeseen circumstances encountered during operation ([4], [5]). Moreover, the ethical ramifications surrounding AI-driven decision-making in high-stakes scenarios, such as those involving potential collisions or accidents, necessitate the formulation and establishment of explicit guidelines and standards aimed at promoting accountability and fostering public trust in the technology ([8], [12]).

In addition to the previously mentioned considerations, cybersecurity emerges as an equally critical dimension within the framework of automated vehicle navigation. As vehicles become progressively interconnected within

an expansive digital ecosystem, they concurrently face an increased risk of cyber threats that could jeopardize their navigation systems and overall operational safety, thereby endangering both passengers and pedestrians ([11], [14]). Established standards, such as ISO/SAE 21434, offer a foundational framework to address these cybersecurity challenges; however, it is crucial to integrate these standards into the core of functional safety protocols to develop a comprehensive safety and security strategy that encompasses all dimensions of vehicle operation ([3], [14]). Furthermore, the homologation process for autonomous vehicles must undergo substantial transformation to effectively address the distinctive challenges posed by AI and automated systems. Traditional methods of testing and approval may prove inadequate in thoroughly evaluating the safety and performance metrics of these innovative technologies, thereby underscoring the urgent necessity for the development of novel testing environments and methodologies that can accurately simulate real-world conditions and scenarios ([4], [10]). This includes the establishment of specialized proving grounds designed to replicate authentic driving conditions, which will serve to validate the effectiveness and reliability of automated vehicle navigation systems in practical applications ([9], [10]).

Automatic car navigation systems have a lot of promise to increase transportation safety and efficiency in a number of ways. But achieving these potential calls for a thorough and multidimensional approach to standardization that takes into account crucial elements like cybersecurity, functional safety, ethical issues, and creative testing techniques. For fully autonomous vehicles to be successfully deployed and integrated into public roads, industry players, university researchers, and regulatory agencies must work together effectively. Future transportation will be safer and more effective as a result of this cooperative effort ([2], [4], [10]). The following table summarizes the discussed requirements.

Table 1: Summary of AI in intelligent vehicles

Intelligent feature	Regulation	Relevance of AI	Concerns
DDDS	[16]	Very relevant	Privacy and personal data Interference with other warning functions
ADDWS	[16]	Very relevant	Interference with DDDS
AEB	[17]	Less relevant	Unnecessary brake and collision
ESF	[20]	Relevant	Driver unconscious intervention Unsafe action due to sensor fault
CAS	[16]	Relevant	Collision due to delayed action Unnecessary brake Electromagnetic susceptibility Liability
AVNS	[21]	Very relevant	Electromagnetic susceptibility Liability

Conclusion

The incorporation of Artificial Intelligence (AI) technologies within the automotive industry, with a particular emphasis on the realm of Autonomous Vehicles (AVs), reveals a multifaceted landscape characterized by considerable obstacles alongside substantial opportunities for innovation and development. This process of integration demands a comprehensive and holistic methodology that thoroughly encompasses various critical components, including but not limited to standardization practices, safety protocols, cybersecurity measures, and ethical considerations, as evidenced by the illuminating insights extracted from the existing body of literature on the subject.

Robust Standardization: The swift and ongoing evolution of AI technologies implemented within vehicles accentuates the pressing necessity for the establishment of robust and comprehensive standardization frameworks that can adequately address the unique challenges posed by these advanced systems. Current standards, such as ISO 26262, primarily emphasize functional safety; however, they frequently fall short in addressing the intricate complexities and nuances introduced by AI systems, as noted in several scholarly sources ([2], [13]). The introduction and subsequent adoption of ISO 8800 represent a significant advancement in the endeavor to enhance the quality and variety of training data that is crucial for the effective functioning of machine learning applications, which is fundamentally essential for guaranteeing the safety and reliability of AI-driven vehicles on the roads ([2]).

Cybersecurity Vulnerabilities: As vehicles evolve towards increased interconnectivity, they are subsequently exposed to an expanding spectrum of cybersecurity threats that could potentially compromise their operational integrity. The ISO/SAE 21434 standard delineates the necessary cybersecurity measures that need to be implemented; however, it also emphasizes the critical importance of adopting a more integrative approach that fully considers the dynamic interplay between AI functionalities and the requisite cybersecurity protocols that govern them ([14]). Such integration is of paramount importance in order to effectively mitigate the myriad risks associated with potential cyberattacks that could jeopardize the overall safety and functionality of vehicles in real-world scenarios ([11], [14]).

Ethical and Legal Implications: The advent and deployment of AI technologies within vehicles engender profound ethical and legal dilemmas, particularly in relation to issues of liability and accountability in the event

of accidents involving autonomous systems. The current absence of clear and definitive guidelines concerning accountability significantly complicates the regulatory landscape, thereby necessitating the urgent establishment of comprehensive frameworks that explicitly delineate responsibilities and procedural protocols for conducting thorough accident investigations ([8], [12]). Proactively addressing these ethical concerns is of critical importance for nurturing and fostering public trust in the emerging landscape of autonomous technologies.

Dynamic Testing and Validation: The conventional methodologies employed for testing may prove inadequate when faced with the intricate and multifaceted behaviors exhibited by AI-driven vehicles that operate in complex environments. Therefore, the development and implementation of innovative testing environments and methodologies, such as advanced simulation techniques and dedicated proving grounds, are absolutely essential for accurately assessing the performance and reliability of AI systems under a diverse range of operational conditions ([4], [5]). Such an approach ensures that vehicles are capable of safely navigating real-world scenarios, which may include encountering adverse weather conditions and unexpected obstacles that could impede their operation.

Collaboration and Continuous Improvement: The multifarious challenges that arise from the integration of AI into vehicle systems necessitate a sustained and ongoing collaboration among various industry stakeholders, researchers, and regulatory authorities. Continuous feedback loops and iterative improvements in standards and practices are absolutely vital to maintaining alignment with the rapid pace of technological advancements while simultaneously ensuring the safety and well-being of the public at large ([9], [10]).

In conclusion, although the integration of AI into vehicle navigation systems presents immense potential for significantly enhancing both transportation efficiency and safety, it concurrently requires the formulation and implementation of a comprehensive strategy that encompasses rigorous standardization practices, effective cybersecurity measures, ethical considerations, and dynamic testing methodologies. Addressing these multifaceted challenges through collaborative efforts and the establishment of robust regulatory frameworks is fundamentally essential for the successful deployment and operation of intelligent vehicles on public roadways. The insights and recommendations derived from the literature underscore the critical importance of adopting a proactive and integrated

approach in order to successfully navigate the complexities and intricacies associated with the application of AI technologies within the automotive industry.

Funding

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Declarations

Ethics approval and consent to participate

Not applicable.

Consent for publication

Not applicable.

Competing interests

The authors declare that they have no competing interests.

Received: Dec. 2024 Accepted: Jan. 2025

Published online: Jan. 2025

DOI: 10.22034/ASAS.2025.495087.1070

References:

- [1] Henrique Sousa Antunes, Pedro Miguel Freitas, Arlindo L. Oliveira, Clara Martins Pereira, Elsa Vaz de Sequeira, Luís Barreto Xavier (Editors), *Multidisciplinary Perspectives on Artificial Intelligence and the Law*, Springer Cham, Dec. 2023, Cham, Switzerland.
- [2] ISO/DPAS 8800: Road vehicles — Safety and artificial intelligence, ISO, 2024.
- [3] Li, Y., Liu, W., Liu, Q., Zheng, X., Sun, K. and Huang, C., 2024. Complying with ISO 26262 and ISO/SAE 21434: A Safety and Security Co-Analysis Method for Intelligent Connected Vehicle. *Sensors*, 24(6), p.1848.
- [4] Zöldy, M., Szalay, Z. and Tihanyi, V., 2020. Challenges in homologation process of vehicles with artificial intelligence. *Transport*, 35(4), pp.447-453.
- [5] Radlak, K., Szczepankiewicz, M., Jones, T. and Serwa, P., 2020, December. Organization of machine learning based product development as per ISO 26262 and ISO/PAS 21448. In *2020 IEEE 25th Pacific Rim International Symposium on Dependable Computing (PRDC)* (pp. 110-119). IEEE.
- [6] Vasudevan, V., Abdullatif, A., Kabir, S. and Campean, F., 2022. A framework to handle uncertainties of machine learning models in compliance with iso 26262. In *Advances in Computational Intelligence Systems: Contributions Presented at the 20th UK Workshop on Computational Intelligence*, September 8-10, 2021, Aberystwyth, Wales, UK 20 (pp. 508-518). Springer International Publishing.
- [7] Falcini, F. and Lami, G., 2017. Deep learning in automotive: Challenges and opportunities. In *Software Process Improvement and Capability Determination: 17th International Conference, SPICE 2017, Palma de Mallorca, Spain, October 4–5, 2017, Proceedings* (pp. 279-288). Springer International Publishing.
- [8] Charter, R., 2022. Ethical and trustworthy Artificial Intelligence.
- [9] Englund, C., Aksoy, E.E., Alonso-Fernandez, F., Cooney, M.D., Pashami, S. and Åstrand, B., 2021. AI perspectives in Smart Cities and Communities to enable road vehicle automation and smart traffic control. *Smart Cities*, 4(2), pp.783-802.
- [10] Tokody, D., Albin, A., Ady, L., Rajnai, Z. and Pongrácz, F., 2018. Safety and security through the design of autonomous intelligent vehicle systems and intelligent infrastructure in the smart city. *Interdisciplinary Description of Complex Systems: INDECS*, 16(3-A), pp.384-396.
- [11] Ward, D. and Wooderson, P., 2021. *Automotive Cybersecurity: An Introduction to ISO/SAE 21434*. SAE International.
- [12] Zhao, W., 2021. Artificial Intelligence and ISO 26000 (Guidance on Social Responsibility). In *AI and Learning Systems-Industrial Applications and Future Directions*. IntechOpen.
- [13] ISO 26262 series: Road vehicles — Functional safety, ISO, 2018.
- [14] ISO/SAE 21434: Road vehicles — Cybersecurity engineering, ISO, 2021.
- [15] ISO 38171: Road vehicles — Smart community infrastructures — Smart transportation by autonomous vehicles on public roads, ISO, 2022.
- [16] Moradi, A., Nazari, S.S.H. and Rahmani, K., 2019. Sleepiness and the risk of road traffic accidents: A systematic review and meta-analysis of previous studies. *Transportation research part F: traffic psychology and behaviour*, 65, pp.620-629.
- [17] European Parliament, EU Regulation 2144. 2019. Type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, as regards their general safety and the protection of vehicle occupants and vulnerable road users. EU. 2019.
- [18] United Nations Economic Commission for Europe, UNECE Addendum: 130 - Regulation: 131: 2019. Uniform provisions concerning the approval of motor vehicles with regard to the Advanced Emergency Braking Systems (AEBS). UNECE. 2019.
- [19] United Nations Economic Commission for Europe, UNECE Addendum: 130 - Regulation: 152: 2020. Uniform provisions concerning the approval of motor vehicles with regard to the Advanced Emergency Braking System (AEBS) for M1 and N1 vehicles. UNECE. 2020.
- [20] United Nations Economic Commission for Europe, UNECE Addendum: 78 - Regulation: 79: 2024. Uniform

provisions concerning the approval of vehicles with regard to steering equipment. UNECE. 2024.

[21] European Parliament, EU Regulation 858. 2018. vehicles produced in unlimited series, vehicles produced in small series, fully automated vehicles produced in small series and special purpose vehicles, and as regards software update. EU. 2018.

Submit your manuscript to Advances in the standards and applied sciences journal and benefit from:

- ▶ Convenient online submission
- ▶ Rigorous peer review
- ▶ Open Access: articles freely available online
- ▶ High visibility within the field
- ▶ Retaining the copyright to your article

**Submit your next manuscript at:
journal.standards.ac.ir**