CONNECTIVITY, INTELLIGENCE AND MOBILITY: THE ROLE OF INTERNET OF THINGS AND INTERNET OF VEHICLES IN THE AUTOMOTIVE INDUSTRY

CONECTIVIDADE, INTELIGÊNCIA E MOBILIDADE: O PAPEL DA INTERNET DAS COISAS E DA INTERNET DOS VEÍCULOS NA INDÚSTRIA AUTOMÓVEL

10.29073/e3.v11i1.1011

Receção: 01/06/2025. Aprovação: 21/06/2025. Publicação: 29/06/2025

Carlos Costa [1]; Daniel Azevedo [2]; Romeu Sequeira [3]; Pedro Lopes [4]; Damiana Guedes [5]

[1] School of Technology and Management of Lamego, Polytechnic Institute of Viseu, Portugal, ccosta@estgl.ipv.pt; [2] Polytechnic Institute of Viseu, Portugal, azevedo21@gmail.com; [3] School of Technology and Management of Lamego, Polytechnic Institute of Viseu, Portugal, nsequeira@estgl.ipv.pt; [4] School of Technology and Management of Lamego, Polytechnic Institute of Viseu, Portugal, plopes@estgl.ipv.pt; [5] School of Technology and Management of Lamego, Polytechnic Institute of Viseu, Portugal, dguedes@estgl.ipv.pt;

ABSTRACT

The digitalization of the automotive industry has accelerated the adoption of the Internet of Things (IoT) and the Internet of Vehicles (IoV), fostering new solutions for safety, efficiency, and sustainable mobility. This article, developed within the scope of the IDT – PIVOT project, Incentive System for Business Research and Development – Individual Operations, aims to critically analyze the role of IoT and IoV in the automotive sector, exploring practical applications, conceptual architectures, and implementation challenges. The methodology consisted of a critical review of scientific and technical literature (2010–2025), complemented by institutional reports and industrial case studies, structured into four axes: IoT applications, communication networks, IoT/IoV architectures, and the evolution towards IoV. The results highlight clear benefits, such as accident reduction through V2X communication, improved efficiency via predictive maintenance, and environmental gains in intelligent mobility systems. However, significant limitations remain, including interoperability issues, latency, cybersecurity risks, costs, and social acceptance. Future perspectives point to the integration of 5G/6G networks, edge intelligence, and Mobility as a Service (MaaS) models, requiring robust public policies and global communication standards. It is concluded that IoT and IoV are strategic pillars for the transition towards connected, autonomous, and cooperative mobility.

Keywords: IoT, IoV, Automotive industry, Connected mobility, Cybersecurity.

RESUMO

A digitalização da indústria automóvel tem acelerado a adoção da Internet das Coisas (IoT) e da Internet dos Veículos (IoV), promovendo novas soluções para a segurança, eficiência e mobilidade sustentável. Este artigo, desenvolvido no âmbito do projeto IDT – PIVOT, Sistema de Incentivos à Investigação e Desenvolvimento Empresarial – Operações Individuais, tem como objetivo analisar criticamente o papel da IoT e da IoV no setor automóvel, explorando aplicações práticas, arquiteturas conceptuais e desafios de implementação. A metodologia consistiu numa revisão crítica da literatura científica e técnica (2010–2025), complementada por relatórios institucionais e estudos de caso industriais, estruturada em quatro eixos: aplicações da IoT, redes de comunicação, arquiteturas IoT/IoV e a evolução rumo à IoV. Os resultados evidenciam benefícios claros, como a redução de acidentes através da comunicação V2X, o aumento da eficiência via manutenção preditiva e ganhos ambientais em sistemas de mobilidade inteligente. Contudo, persistem limitações significativas, incluindo problemas de interoperabilidade, latência, riscos de cibersegurança, custos e aceitação social. As perspetivas futuras apontam para a integração de redes 5G/6G, inteligência de periferia (edge computing) e modelos de Mobilidade como Serviço (MaaS), exigindo políticas públicas robustas e normas globais de comunicação. Conclui-se que a IoT e a IoV são pilares estratégicos para a transição rumo a uma mobilidade conectada, autónoma e cooperativa.

Palavras-chave: IoT, IoV, Indústria automóvel, Mobilidade conectada, Cibersegurança.

1. INTRODUCTION

The digitization of the automotive industry has accelerated the adoption of emerging technologies aimed at increasing the safety, efficiency and sustainability of mobility. In this context, the Internet of Things (IoT) and the Internet of Vehicles (IoV) play a pivotal role in enabling the interconnection of vehicles, infrastructure, users and services. This creates dynamic, collaborative digital ecosystems (Lee, Gerla & Pau, 2016).

In the automotive sector, the IoT enables real-time data collection and analysis, facilitating applications such as predictive maintenance, intelligent traffic management, and personalized infotainment services (Lin et al., 2017). As a specialized subdomain, the IoV focuses on specific communication networks —Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I) and Vehicle-to-everything (V2X) — which facilitate cooperation between vehicles and urban infrastructure elements. These networks are supported by advanced communication technologies such as Automotive Ethernet, 5G and, in the future, 6G (Shrestha, Bajracharya, Nam & Kim, 2020).

Prepared as part of the IDT-PIVOT project (Incentive System for Business Research and Development – Individual Operations), this article aims to conduct a critical review of the role of the IoT and the IoV in the automotive industry. It explores their practical applications, conceptual architecture and implementation challenges. The article seeks to contribute to the systematization of current practices and offer recommendations for the adoption of secure, scalable, and interoperable solutions in the automotive sector.

2. LITERATURE REVIEW

2.1. INTERNET OF THINGS APPLIED TO THE AUTOMOTIVE SECTOR

The IoT is playing a pivotal role in the digital transformation of the automotive industry by enabling vehicles to evolve from isolated systems into active nodes in a global data network (Lin et al., 2017). Smart sensors, Electronic Control Units (ECUs) and communication platforms allow for the continuous monitoring of vehicle performance and environmental conditions, facilitating the development of new applications in the areas of safety, efficiency and user experience.

One of the most notable examples of the practical application of IoT in the automotive sector is predictive maintenance. Manufacturers such as Tesla and BMW use sensors distributed across critical components, such as the engine, brakes and tires, to collect data which is analyzed using cloud and edge computing platforms. This approach enables early detection of anomalies, reducing operating costs and avoiding unexpected failures (Zhang, Mao, Leng, He & Zhang, 2017).

Another use case is the integration of the IoT into Intelligent Transport Systems (ITS), enabling real-time traffic data collection and sharing between vehicles and urban infrastructure. Pilot projects in cities such as Hamburg and Singapore demonstrate that these solutions help to reduce congestion and optimize mobility flows (European Commission, 2021). Thus, the IoT forms the technological basis for the development of the IoV, expanding automotive connectivity to collaborative and intelligent scenarios.

2.2. CONNECTIVITY AND COMMUNICATION NETWORKS

Connectivity is the structuring element of both the IoT and the IoV, ensuring the transmission of data between vehicles, infrastructure, and digital services. Specific applications are supported by

different network layers, ranging from internal vehicle control to large-scale communication with other systems (Lee, Gerla & Pau, 2016).

At the intra-vehicle level, technologies such as the Controller Area Network (CAN) bus, the Local Interconnect Network (LIN), FlexRay and Automotive Ethernet facilitate communication between sensors, actuators and ECUs. These protocols are essential for systems such as automatic braking, stability control and engine management to function properly (Papadimitratos, La Fortelle, Evenssen, Brignolo & Cosenza, 2009).

At short range, standards such as Bluetooth, Wi-Fi and Ultra-Wideband (UWB) are used for convenience applications, such as integration with mobile devices, digital key systems, and local vehicle monitoring.

Long-range networks, on the other hand, are the strategic foundation of the IoV. Technologies such as 4G-LTE and 5G, and in the future 6G, enable critical, low-latency applications such as V2V, V2I and V2X communication. Organizations such as the 5G Automotive Association (5GAA) have developed pilot projects demonstrating the potential of 5G to support cooperative traffic management and autonomous driving in urban environments (5GAA, 2021).

Additionally, paradigms such as cloud, edge and fog computing reinforce decentralized processing, thereby increasing resilience and reducing latency in safety-critical applications (Zhang, Mao, Leng, He & Zhang, 2017).

2.3. Internet of Things applications in the automotive industry

The application of IoT in this industry covers several key areas, including road safety, predictive maintenance and smart mobility.

In terms of safety, the IoT is supporting the development of Advanced Driver Assistance Systems (ADAS) that are moving towards cooperative solutions based on V2X technology. These systems facilitate the exchange of information between vehicles and infrastructure, enabling the anticipation of collisions or the adjustment of speed at dangerous intersections (Papadimitratos et al., 2009). One example is Volvo's system which communicates slippery road conditions via the cloud, enabling other vehicles to adjust their driving in real time (Shrestha, Bajracharya, Nam & Kim, 2020).

In the field of predictive maintenance, smart sensors continuously collect data on the condition of vehicle components. Tesla and General Motors have implemented remote diagnostic systems that can predict failures and perform over-the-air software updates, thereby reducing costs and increasing reliability (Lin et al., 2017).

In the field of smart mobility, IoT enables vehicles to integrate with ITS. Cities such as Hamburg and Barcelona already use IoT-based solutions to manage adaptive traffic lights and optimize urban traffic, achieving proven reductions in congestion and emissions (European Commission, 2021).

Thus, the IoT increases operational efficiency and safety while enhancing the user experience with connected, personalized services.

2.4. Conceptual platforms and Internet of Things / Internet of Vehicles architectures

Implementing the IoT and the IoV in the automotive industry requires conceptual architectures that can integrate different layers of data collection, transmission, and analysis. These

architectures are typically structured in four levels: sensors and actuators; connectivity; data processing; and applications (Lin et al., 2017).

At the sensor level, sensors installed in critical components, such as tires, engines and brakes, collect real-time data. One practical example is the Tire Pressure Monitoring System (TPMS), which is already mandatory in several countries and monitors tire pressure, automatically reporting safety deviations (European Commission, 2021).

The communication layer uses different protocols to ensure connectivity, ranging from CAN bus and Automotive Ethernet for internal communication to 5G and NB-IoT networks for external interconnection. Projects by the 5GAA demonstrate how the low latency of 5G enables cooperative maneuvers between vehicles on motorways (5GAA, 2021).

Data processing takes place in cloud computing environments and, increasingly, in edge and fog computing. These technologies bring analysis closer to where the data is generated, thereby reducing latency in critical applications. Machine Learning (ML) and Deep Learning (DL) algorithms applied in edge units, for example, allow driving patterns to be identified and risk scenarios to be predicted, eliminating the need to send all data to the cloud (Zhang, Mao, Leng, He & Zhang, 2017).

The application layer then makes these results available to drivers, manufacturers or authorities via dashboards, mobility services or fleet management platforms. Despite their potential, standardisation and cybersecurity challenges still need to be overcome for this architecture to be adopted on a large scale.

2.5. Evolution towards the Internet of Vehicles

The IoV is a natural extension of the IoT to the automotive sector. It expands vehicle connectivity to collaborative networks that include other vehicles, infrastructure, pedestrians, and smart urban systems (Lee, Gerla & Pau, 2016). Unlike the general IoT, it adopts specific vehicle communication protocols such as V2V, V2I and V2X. These protocols enable real-time information exchange, directly impacting mobility, safety and efficiency (Papadimitratos et al., 2009).

In practice, IoV is already being tested in various scenarios. For example, the European Union's Cooperative ITS (C-ITS) program has implemented test corridors on cross-border motorways where vehicles from different manufacturers communicate with each other to coordinate overtaking, adjust speeds, and reduce congestion (European Commission, 2021). Similarly, companies such as Audi and Volkswagen have launched V2I communication services that enable vehicles to synchronize with smart traffic lights in cities such as Las Vegas and Ingolstadt, thereby optimizing fuel consumption and reducing emissions (5GAA, 2021).

Despite these advances, the IoV still faces significant challenges. The lack of interoperability between manufacturers, universal standardization and cybersecurity risks continue to limit its implementation. Furthermore, the social acceptance of connected mobility raises issues of privacy and trust, necessitating transparent public policies and regulations (Raza, Wallgren & Voigt, 2017).

Therefore, the IoV is emerging as a strategic pillar for cooperative driving and the progressive transition towards autonomous vehicles, the success of which will depend on technological and regulatory consolidation in the coming years.

3. METHODOLOGY

This article forms part of a critical review of scientific and technical literature concerning the application of IoT and the IoV within the automotive industry. A qualitative and exploratory approach was adopted to systematize the state of the art, identify patterns of technological evolution, and discuss the main challenges associated with implementing these paradigms.

Bibliographic data was collected from high-impact databases, including IEEE Xplore, Scopus, Web of Science, ScienceDirect and SpringerLink. This was supplemented by institutional reports from organisations such as the European Commission, the European Telecommunications Standards Institute (ETSI) and the 5GAA. Documents published between 2010 and 2025 were examined, with a particular focus on more recent publications (2018–2025) due to the dynamic nature of this field (Lin et al., 2017; European Commission, 2021).

The following were considered as inclusion criteria: (i) peer-reviewed articles directly relevant to the IoT and IoV in the automotive sector; (ii) industrial case studies with practical applications; and (iii) technical reports describing implementations in real environments. Documents that were purely promotional or lacked an explicit methodology were excluded.

The analysis employed a narrative synthesis approach, categorizing the findings into four themes: (i) the application of IoT to the automotive sector; (ii) connectivity and communication networks; (iii) the practical applications of IoT; and (iv) conceptual architectures and the evolution towards IoV. This approach enabled the integration of academic and industrial perspectives, providing a comprehensive overview of the subject (Shrestha, Bajracharya, Nam & Kim, 2020; Zhang, Mao, Leng, He & Zhang, 2017).

4. RESULTS AND DISCUSSION

4.1. IDENTIFIED BENEFITS

The integration of the IoT and IoV in the automotive industry has demonstrated significant benefits in three key areas: road safety, operational efficiency, and sustainable mobility.

In terms of safety, for example, the IoV supports the implementation of V2X communication systems, enabling real-time data exchange between vehicles and infrastructure. These systems can provide early collision warnings, coordinate lane changes and optimize traffic flow at intersections, thereby reducing the likelihood of accidents. For instance, C-ITS projects funded by the European Union have reduced the risk of incidents in dense traffic scenarios by up to 30% (European Commission, 2021).

Secondly, the IoT contributes to operational efficiency through predictive maintenance solutions. Manufacturers such as Tesla use ML algorithms to continuously monitor vehicle condition and issue alerts for imminent failure, thereby avoiding unexpected breakdowns and reducing repair costs (Lin et al., 2017).

Finally, the IoV promotes environmental and social benefits by supporting smart, sustainable mobility. Integrating connected vehicles into urban traffic management systems, as demonstrated in projects such as those in Hamburg and Barcelona, has been shown to reduce congestion and CO_2 emissions. This highlights the positive impact on urban quality of life (5GAA, 2021).

Therefore, IoT and IoV are key technologies for enhancing safety, reducing costs, and making transport systems more sustainable.

4.2. Current limitations

Despite the identified benefits, the implementation of IoT and IoV in the automotive industry faces several limitations that hinder large-scale adoption.

One of the main barriers is limited interoperability. The coexistence of multiple manufacturers, technology providers and communication protocols makes it challenging to establish a consistent ecosystem. For instance, the absence of a universal V2X standard means vehicles from different brands may struggle to communicate effectively in cooperative environments (Papadimitratos et al., 2009).

Another relevant limitation is communication latency. Although 5G networks have reduced response times, critical applications such as cooperative breaking require latencies of less than 1ms. Recent studies indicate that network congestion in dense urban scenarios can compromise the reliability of V2X, thereby endangering safety (Shrestha, Bajracharya, Nam & Kim, 2020).

Cybersecurity is also a key challenge. Connected vehicles are vulnerable to potential cyberattacks that could compromise critical systems such as infotainment, steering and braking controls. Real-life cases, such as the remote hacking of a Jeep Cherokee in 2015, have demonstrated the vulnerability of these systems and reinforced the need for robust security measures (Raza, Wallgren & Voigt, 2017).

Finally, implementation costs remain high. Installing sensors, communication modules and support infrastructure requires significant investment, limiting adoption in market segments with lower purchasing power (European Commission, 2021).

Thus, IoT and IoV still face structural obstacles that need to be overcome before they can be disseminated globally.

4.3. Implementation challenges

Implementing IoT and IoV in the automotive sector presents challenges that extend beyond technical limitations to encompass regulatory, social, and ethical considerations.

One of the biggest obstacles is the lack of technical standardization. Currently, various communication protocols (DSRC, C-V2X and 5G) coexist, and there is no global consensus on which should prevail. This fragmentation compromises interoperability between vehicles from different manufacturers and hinders large-scale adoption (Papadimitratos et al., 2009). Organizations such as the 5GAA have proposed standardization efforts, but convergence is still in its infancy (5GAA, 2021).

Another critical challenge is the integration of autonomous vehicles. Although the IoV is considered essential for cooperative driving, its implementation requires ultra-low latency, high reliability and system redundancy. Without these, the safe coordination of maneuvers between autonomous vehicles may be compromised (Shrestha, Bajracharya, Nam & Kim, 2020).

From a social perspective, issues related to privacy and public acceptance arise. The large-scale collection of geolocation data and driving patterns raises concerns about surveillance and the misuse of information. To mitigate these issues, the creation of specific cybersecurity certification

centres for connected vehicles is suggested, to ensure that manufacturers comply with minimum protection standards (Raza, Wallgren & Voigt, 2017).

Finally, the absence of a clear regulatory framework in certain countries impedes the expansion of the IoV. National connected mobility strategies and incentives for fleet modernization could accelerate the transition to cooperative systems.

4.4. Future prospects

The future of the IoT and the IoV points towards ever deeper integration between vehicles, infrastructure, and smart cities. The introduction of 5G technology, and ongoing development of 6G, promises to reduce latency to below 1 millisecond. This will enable the real-time coordination of autonomous vehicles and cooperative transport systems (Shrestha, Bajracharya, Nam & Kim, 2020).

Technologically, the trend is towards expanding edge intelligence by combining edge computing with ML and DL algorithms. This paradigm will allow data to be processed locally, either in vehicles or in nearby base stations, thereby reducing dependence on the cloud and increasing resilience. Toyota, for instance, has invested in hybrid cloud-edge architectures to enhance traffic forecasting and optimize energy usage (Lin et al., 2017).

Another area of development will be the convergence of the IoV with ITS and Mobility as a Service (MaaS) models. Cities such as Helsinki and Vienna are already testing integrated platforms through which connected vehicles, public transport and micro-mobility services can share real-time data, thereby increasing the overall efficiency of urban mobility (European Commission, 2021).

However, these prospects will only be realized if cybersecurity, standardization and social acceptance challenges are overcome. Therefore, the future of the IoV depends on technological advances as well as the creation of robust public policies and social trust to support autonomous and cooperative mobility.

5. Conclusions

This article's analysis confirms that IoT and IoV are strategic pillars for the digital transformation of the automotive industry. These technologies enable real-time communication between vehicles, infrastructure and urban systems, and have been shown to deliver significant benefits in terms of road safety, operational efficiency and sustainable mobility (European Commission, 2021; Lin et al., 2017).

However, structural limitations remain that constrain their widespread adoption. These include issues of interoperability between manufacturers, latency in critical applications, cybersecurity and implementation costs (Papadimitratos et al., 2009; Raza, Wallgren & Voigt, 2017). Resolving these issues requires coordinated efforts between industry, regulators, and standardization bodies.

The outlook points to increasingly connected, autonomous and cooperative mobility based on 5G/6G networks and edge intelligence, as well as integration with MaaS models (Shrestha, Bajracharya, Nam & Kim, 2020). To accelerate this transition, the following are recommended:

1. Adopting global V2X communication standards to promote interoperability.
2. The creation of automotive cybersecurity certification centres to strengthen social trust.
3. Definition of public policies to encourage the renewal of the connected fleet and the implementation of smart infrastructure.

In summary, the IoT and the IoV should not merely be seen as technological innovations, but as catalysts for structural change in mobility. The success of their implementation will depend on technological advancement, robust regulation and social acceptance converging.

REFERENCES

5GAA – 5G Automotive Association. (2021). *C-V2X use cases, security requirements and 5G roadmap for connected vehicles*. 5GAA White Paper.

ETSI – European Telecommunications Standards Institute. (2019). *Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Definitions*. ETSI TR 102 638.

European Commission. (2021). *On the road to automated mobility: An EU strategy for connected and automated mobility*. Publications Office of the European Union. https://doi.org/10.2838/411077

Lee, E. K., Gerla, M., & Pau, G. (2016). Internet of vehicles: From intelligent grid to autonomous cars and vehicular clouds. *Proceedings of the IEEE, 104*(5), 1127–1168. https://doi.org/10.1109/JPROC.2015.2503118

Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., & Zhao, W. (2017). A survey on Internet of Things: Architecture, enabling technologies, security and privacy, and applications. *IEEE Internet of Things Journal, 4*(5), 1125–1142. https://doi.org/10.1109/JIOT.2017.2683200

Miller, C., & Valasek, C. (2015). *Remote exploitation of an unaltered passenger vehicle*. Black Hat USA. https://ioactive.com/wp-content/uploads/2018/05/remote-exploitation-of-an-unaltered-passenger-vehicle.pdf

Papadimitratos, P., La Fortelle, A., Evenssen, K., Brignolo, R., & Cosenza, S. (2009). Vehicular communication systems: Enabling technologies, applications, and future outlook. *IEEE Communications Magazine, 47*(11), 84–95. https://doi.org/10.1109/MCOM.2009.5307471

Raza, S., Wallgren, L., & Voigt, T. (2017). Security and performance analysis of IoT networks under various attacks. *IEEE Access, 5*, 437–448. https://doi.org/10.1109/ACCESS.2017.2648799

Shrestha, R., Bajracharya, R., Nam, S. Y., & Kim, S. H. (2020). A new type of vehicular networking: Internet of vehicles for autonomous driving. *International Journal of Distributed Sensor Networks, 16*(6), 1–14. https://doi.org/10.1177/1550147720926965

Wu, G., Talwar, S., Johnsson, K., Himayat, N., & Johnson, K. D. (2015). M2M: From mobile to embedded Internet. *IEEE Communications Magazine, 53*(9), 36–43. https://doi.org/10.1109/MCOM.2015.7263369

Zhang, K., Mao, Y., Leng, S., He, Y., & Zhang, Y. (2017). Mobile-edge computing for vehicular networks: A promising network paradigm with predictive off-loading. *IEEE Vehicular Technology Magazine, 12*(2), 36–44.

ETHICAL PROCEDURES

Conflict of interest: nothing to declare. **Funding**: nothing to declare. **Peer review**: Double anonymous peer review.