KOŠICKÁ BEZPEČNOSTNÁ REVUE

KOSICE SECURITY REVUE

Vol. 15, No. 2 (2025), p. 65 – 81

ISSN 1338-4880 (print ver.), ISSN 1338-6956 (online ver.)

Predict future advances in car connectivity development with a focus on safety

Predikcia budúceho pokroku vo vývoji konektivity automobilov so zameraním na bezpečnosť

Jozef KOČÍK[1]

[1]*University of Security Management in Košice*

The manuscript was received on 28.10.2025 and was accepted after revision for publication on 30.10.2025

Abstract:

The article analyzes the current state and future development of vehicle connectivity with a focus on safety. It describes technologies such as V2X communication, 5G/6G networks, edge computing, artificial intelligence, satellite connectivity, blockchain, and digital identity, which significantly transform how vehicles interact with their environment. It discusses challenges in cybersecurity, data privacy, standardization, and ethics of autonomous systems. Based on technological trends and pilot projects, the article predicts that by 2035, vehicles will operate as fully connected digital nodes capable of autonomous decision-making and adaptive safety. It concludes with recommendations for the secure and trustworthy development of automotive connectivity.

Keywords: *vehicle connectivity, V2X communication, cybersecurity, digital identity, autonomous vehicles, edge computing, blockchain, intelligent infrastructure, security-as-a-service*

Abstrakt:

Článok analyzuje súčasný stav a predikciu budúceho vývoja konektivity v automobilovom priemysle so zameraním na bezpečnosť. Popisuje technológie ako V2X komunikácia, 5G/6G siete, edge computing, umelá inteligencia, satelitné pripojenie, blockchain a digitálna identita, ktoré zásadne menia spôsob interakcie vozidiel s okolím. Diskutuje výzvy v oblasti kybernetickej bezpečnosti, ochrany osobných údajov, štandardizácie a etiky autonómnych systémov. Na základe technologických trendov a pilotných projektov predpovedá, že do roku 2035 budú vozidlá fungovať ako plne prepojené digitálne uzly, schopné autonómneho rozhodovania a adaptívnej bezpečnosti. Záverom sú formulované odporúčania pre bezpečný a dôveryhodný rozvoj konektivity.

Kľúčové slová: *konektivita vozidiel, V2X komunikácia, kybernetická bezpečnosť, digitálna identita, autonómne vozidlá, edge computing, blockchain, inteligentná infraštruktúra, bezpečnosť ako služba*

Introduction

The automotive industry has been undergoing rapid transformation over the past decades, faster than ever before. Traditional mechanical systems are giving way to digital technologies that fundamentally change how vehicles operate, communicate, and interact with their surroundings. One of the most prominent trends in this transformation is the growing importance of connectivity—the ability of a vehicle to remain continuously connected to the internet, other vehicles, infrastructure, and even users' personal devices. This connectivity brings numerous benefits, ranging from enhanced convenience and efficient maintenance to improved road safety.

Safety is among the most critical aspects influenced by connectivity. Thanks to technologies such as V2X (Vehicle-to-Everything), 5G networks, advanced sensors, and artificial intelligence, vehicles are becoming capable of predicting hazards, communicating with other traffic participants, and responding in real time to changing conditions. These capabilities can significantly reduce traffic accidents, improve traffic flow, and enhance the protection of vulnerable road users such as pedestrians and cyclists.

On the other hand, increasing digital interconnectivity introduces new challenges. Vehicle systems are becoming more complex and vulnerable to cyberattacks. Data protection, secure communication, and the reliability of software updates are emerging as key concerns not only for automakers but also for regulators and technology developers. This creates a need to balance innovation with a strong emphasis on safety and user trust.

The aim of this article is to examine the current state of automotive connectivity, analyze the main technological trends shaping its future, and predict how these changes will impact safety. We will focus on technologies with the potential to fundamentally influence future mobility while highlighting the challenges that must be overcome to ensure connectivity becomes not only a tool for progress but also a guarantee of safety.

1. Current state of vehicle connectivity

Connectivity has become one of the main pillars of the modern automotive industry. While a decade ago internet access in vehicles was a privilege of luxury models, today digital interconnection is standard even in mid-range cars. Automakers are investing billions in developing systems that enable vehicles to communicate with their surroundings, share data in real time, and provide drivers and passengers with new services. This chapter offers an overview of current technologies, their functions, and the associated security challenges. [1]

Connectivity Type	Usage
Wi-Fi	Infotainment, hotspot for passengers
Bluetooth	Connecting mobile devices, hands-free
4G LTE	Basic mobile connectivity, OTA updates
5G	Low latency, autonomous systems, V2X
V2X	Communication with infrastructure and other vehicles
Satellite Connectivity	Global coverage, low-orbit communication

Tab. No.1 Types of connectivity and their uses [1,2,3]

1.1. Key connectivity technologies

Mobile Networks (4G LTE and 5G): Most new vehicles today are equipped with a SIM card or eSIM module that enables connection to mobile networks. While 4G LTE remains the most widespread technology, an increasing number of manufacturers are transitioning to 5G, which offers lower latency and higher data transfer speeds. For example, BMW introduced 5G-enabled models in 2021, allowing faster OTA updates and advanced real-time services.

Wi-Fi and Bluetooth: These technologies primarily serve to link mobile devices with the vehicle's infotainment system. Apple CarPlay and Android Auto allow drivers to control navigation, music, and messaging directly via the vehicle's touchscreen. Some models, such as Tesla Model 3, even offer a Wi-Fi hotspot for passengers.

GPS and GNSS Systems: Global navigation satellite systems form the foundation for location-based services, navigation, and geofencing. Combined with mapping platforms (e.g., HERE, TomTom, Google Maps), they enable precise vehicle positioning and real-time route optimization.

V2X Communication (Vehicle-to-Everything): V2X technology encompasses communication between vehicles (V2V), infrastructure (V2I), pedestrians (V2P), and networks (V2N). Although its deployment remains limited, pilot projects are underway in the U.S., Europe, and Asia. For instance, Toyota is testing V2V communication in Japan, where vehicles share information on position, speed, and direction to reduce collision risks at intersections. [1,2,3]

1.2. Functions enabled by connectivity

Infotainment and Digital Services: Modern infotainment systems offer a wide range of online services—from music streaming and voice assistants to personalized driver profiles. Mercedes-Benz's MBUX system supports voice control ("Hey

Mercedes") and smart home integration. Volvo uses Google's Android Automotive platform, providing native apps such as Google Maps and Google Assistant

Telematics and Remote Monitoring: Telematics units enable real-time monitoring of vehicle health, driving habits, and location. Services like Škoda Connect or Hyundai Bluelink provide information on battery status, tire pressure, and remote locking/unlocking via mobile apps.

Safety Systems and eCall: Since 2018, the EU has mandated the eCall system, which automatically contacts emergency services in case of an accident. Connectivity also enables advanced driver assistance systems (ADAS), which use data from cameras, radars, and sensors to warn of collisions, maintain lane position, and adjust speed via adaptive cruise control

OTA Updates (Over-the-Air): One of the most significant benefits of connectivity is the ability to update vehicle software remotely. Tesla pioneered this feature, but today brands like Ford (BlueCruise), Volkswagen (ID. Software), and Hyundai also offer OTA updates. These updates allow not only bug fixes but also the addition of new features without visiting a service center. [1,2,3]

1.3. Security challenges of current connectivity

Cybersecurity Threats and Attacks: With growing digitalization comes an increased risk of cyberattacks. Past incidents have shown that hackers can remotely control vehicles—for example, in 2015 researchers demonstrated how they could take control of a Jeep Cherokee over the internet, including braking and steering. Manufacturers are therefore implementing security layers such as firewalls, encrypted communication, and separation of critical systems from infotainment.

Data Privacy: Vehicles now collect vast amounts of data—location, driving style, voice commands, and user preferences. While these data are valuable for service development, they also pose a risk of misuse. Legislation such as the EU's GDPR emphasizes transparency and user consent for data processing.

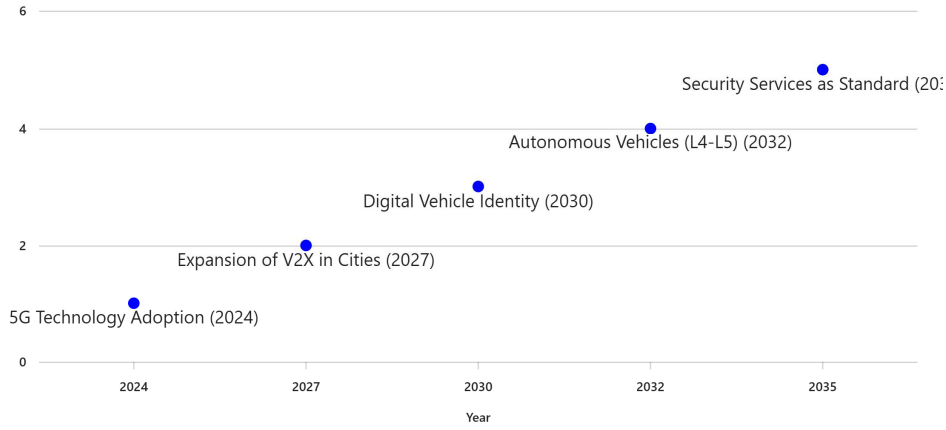
System Complexity and Interoperability: Modern vehicles contain dozens of electronic control units (ECUs) that must cooperate in real time. Ensuring flawless communication, updates, and compatibility is technically challenging. Moreover, different manufacturers use different standards, complicating integration into broader transportation systems.

Connectivity already fundamentally influences how vehicles operate and communicate. A rigorous approach to security and data protection is essential. [1,2,3]

2. Future trends in connectivity

The development of automotive connectivity shows no signs of slowing down. On the contrary, the coming years are expected to bring a surge of innovations that will fundamentally change how vehicles communicate, make decisions, and respond to their environment. These changes will be driven not only by technological progress but also by growing demands for safety, efficiency, and sustainability in

transportation. This chapter examines the most significant trends shaping the future of automotive connectivity and analyzes their potential impact on road safety



Graf. No.1 Timeline of development trends up to 2035[4,5]

2.1. 5G and the emergence of 6G: Foundations for autonomous mobility

5G technology already enables faster and more reliable communication between vehicles and infrastructure. With latency below 10 ms and high data transfer rates, 5G provides an ideal foundation for autonomous driving systems and V2X communication. In the future, the advent of 6G networks is expected to deliver even lower latency (around 1 ms), higher capacity, and the ability to connect millions of devices per square kilometer.

Example: Audi, in collaboration with Ericsson, is testing 5G networks both in manufacturing plants and real-world traffic conditions. The goal is to enable vehicles to communicate with traffic signs, signals, and other vehicles in real time, reducing accident risks and improving traffic flow [4,5]

2.2. Expanded V2X communication and intelligent infrastructure

V2X technologies will continue to evolve and expand. Beyond vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication, increasing attention is being paid to V2P (Vehicle-to-Pedestrian) and V2N (Vehicle-to-Network). The aim is to create a comprehensive ecosystem where all traffic participants including pedestrians, cyclists, and transportation systems are interconnected and able to share information in real time..

Examples: In the Netherlands, a pilot project equips traffic lights with sensors and communication units that "talk" to vehicles. When an ambulance or bus approaches, the system adjusts signals to allow uninterrupted passage, reducing fuel consumption, emissions, and improving safety.

Honda's "Smart Intersection" system in Marysville, Ohio, enables vehicles to communicate with traffic signals and cameras at intersections to "see around corners" and predict collisions.

Volkswagen's Car2X technology in Golf and ID.3 models exchanges information on accidents, traffic jams, and emergency vehicle movements within an 800-meter radius.

Cohda Wireless in Australia is developing V2X solutions that allow vehicles to communicate with cyclists and pedestrians via mobile apps and wearable devices. [4,5]

2.3. Edge computing and artificial intelligence in vehicles

With the growing volume of data generated by vehicles, sending all information to the cloud becomes inefficient. The solution is edge computing—processing data directly in the vehicle or nearby. Combined with artificial intelligence (AI), this enables faster decision-making, risk prediction, and autonomous responses without requiring constant internet connectivity.

Examples: NVIDIA's DRIVE Orin platform processes up to 254 trillion operations per second, enabling simultaneous evaluation of camera, radar, and LIDAR data to predict and respond to hazards.

Volvo collaborates with Qualcomm to develop infotainment systems with smartphone-level computing power for in-vehicle sensor data processing.

Waymo uses proprietary AI models to process LIDAR and camera data in real time without continuous internet access.

ZF Friedrichshafen develops AI-based control units that predict the behavior of other road users and adjust autonomous driving accordingly. [4,5]

2.4. Satellite connectivity and global coverage

In areas without mobile signal, satellite connectivity offers a solution. Companies such as SpaceX (Starlink) and Amazon (Project Kuiper) are building low-earth orbit satellite networks to provide global internet coverage—critical for freight transport, remote routes, and emergency services.

Examples: Tesla plans to integrate Starlink into its vehicles, enabling uninterrupted connectivity even in remote areas—important for navigation and safety functions such as eCall or remote monitoring.

General Motors announced a partnership with SpaceX in 2023 to integrate Starlink into vehicles for remote regions of North America.

Land Rover Defender offers satellite connectivity for expeditions in areas without mobile coverage, essential for off-road safety.

Toyota tests satellite connectivity in Australia for vehicles operating in hard-to-reach areas to ensure communication in emergencies.

2.5. Digital identity and blockchain in automotive systems

As connectivity grows, the need for secure and verifiable digital vehicle identity becomes critical. Blockchain technology can ensure transparent and immutable records of vehicle history, maintenance, ownership, and insurance events—enhancing trust among manufacturers, service providers, and customers.

Examples: The MOBI (Mobility Open Blockchain Initiative) consortium, including BMW, Ford, GM, and Renault, works on standardizing digital vehicle identities through decentralized systems.

Renault developed a prototype using blockchain to record vehicle maintenance history, improving transparency in used car sales.

Bosch and Fetch.ai test decentralized marketplaces where vehicles autonomously pay for parking, charging, or tolls using digital identity.

Daimler Mobility experiments with blockchain for real-time management of leasing and insurance contracts. [4,5]

2.6. Security-as-a-service

In the future, cybersecurity is expected to become a dedicated service offered by manufacturers or third parties via subscription. These services will include real-time threat monitoring, automatic patches, encrypted communication, and digital certificate management..

Examples: Upstream Security provides a cloud platform analyzing telemetric data to detect anomalies indicating cyberattacks—especially important for autonomous vehicle fleets.

Continental develops a cloud platform for real-time threat monitoring and automatic security patch distribution.

Karamba Security offers solutions protecting ECUs from unauthorized access and detecting firmware manipulation attempts.

Cisco and Panasonic collaborate on secure gateways protecting data communication between vehicles and the cloud..

The future of automotive connectivity is closely tied to safety. Technologies such as 5G, edge computing, V2X, and blockchain have the potential to significantly reduce accidents, improve traffic efficiency, and protect user data. At the same time, they impose high demands on system robustness, interoperability, and regulatory frameworks. [4,5]

3. Safety as a priority in the era of vehicle connectivity

As vehicles become increasingly digitalized and interconnected, safety emerges as one of the most critical aspects of automotive technology development. While connectivity offers numerous benefits—from comfort and efficiency to new business models—it also opens the door to new types of risks. These risks include not only technical failures but also cyberattacks, data breaches, and misuse of personal information. This section analyzes the main security challenges associated with connectivity and presents current approaches to addressing them.

3.1. Cybersecurity as a fundamental requirement

Modern vehicles are equipped with dozens of electronic control units (ECUs) that communicate via internal buses (e.g., CAN, LIN, Ethernet) and are simultaneously connected to external networks (mobile networks, Wi-Fi, V2X). This architecture creates potential entry points for cyberattacks. Real-world examples, such as the well-known Jeep Cherokee incident (2015), demonstrate that unauthorized access to a vehicle can lead to complete loss of control over its functions.

To mitigate these risks, several measures are being implemented:

- **System segmentation:** Separation of safety-critical functions (e.g., braking, steering) from less sensitive ones (infotainment).
- **Encrypted communication:** Use of protocols such as TLS, IPsec, and VPN to protect data.
- **Authentication and authorization:** Deployment of digital certificates and security tokens.
- **Anomaly detection:** Implementation of IDS/IPS systems (Intrusion Detection/Prevention Systems) to monitor network traffic.

Example: Tesla's Vehicle Security platform combines hardware security modules (HSM) with regular OTA updates and a bug bounty program for ethical hackers. [6,7,8]

3.2. Data privacy and regulatory compliance

Vehicle connectivity involves collecting and processing large volumes of user data including location, driving habits, biometric identifiers (voice, facial recognition), and preferences. While these data enable personalized services, they also represent sensitive content from a privacy perspective

In compliance with regulations such as GDPR (General Data Protection Regulation), manufacturers must ensure::

- **Transparency:** Clear information for users about what data are collected and for what purpose.

- **Consent:** Active user confirmation before data collection begins.
- **Right to erasure and data portability.**
- **Data minimization:** Collection of only essential data and their anonymization..

Example: Volvo Cars processes most data locally within the vehicle and allows users to manage privacy settings via a mobile application. [6,7,8]

3.3. Security architecture and standardization

The security architecture of modern vehicles must be designed to withstand failures and attacks. Key elements include:

- **Zonal architectures:** Division of the vehicle into functional zones (e.g., powertrain, comfort, infotainment) with dedicated security policies.
- **Redundant systems:** Backup components for critical functions (e.g., dual power supply, dual sensors).
- **Secure boot and software integrity checks.**

Standards play a crucial role in this area

- **ISO/SAE 21434:** International standard for automotive cybersecurity, defining processes throughout the vehicle lifecycle.
- **UNECE WP.29:** UN regulation requiring all new vehicles (since 2022) to implement software update management and cybersecurity systems. [6,7,8,11,12]

3.4. Artificial intelligence in cybersecurity

AI is increasingly used to detect and prevent security incidents. By analyzing large volumes of data in real time, AI can:

- Identify anomalies in vehicle or user behavior,
- Predict component failures (predictive maintenance)
- Automatically classify and respond to cyber threats.

Examples: Upstream Security and Karamba Security develop AI platforms for the automotive sector, capable of monitoring vehicle fleets and detecting suspicious behavior in real time. [6,7,8]

4. Prediction of development up to 2035

The evolution of automotive connectivity over the next decade will be shaped by a combination of technological innovations, regulatory requirements, and societal expectations. By 2035, vehicles are expected to function as fully integrated digital nodes within a broader ecosystem of intelligent mobility. This section outlines key development directions and their anticipated impact on safety, infrastructure, and user experience.

Technological Area	Expected Timeframe	Sources / Prediction Basis	Examples of Manufacturers / Projects
5G Connectivity	2023–2030	Standardization 5G (2019), models BMW, Ford; development of 6G	BMW, Ford, Huawei, SAIC Motor
V2X Communication	2025–2030	Pilot projects in EU, USA, Japan; UNECE support	Volkswagen Car2X, Honda Smart Intersection, Cohda Wireless
Digital Vehicle Identity	2028–2035	MOBI initiative, blockchain networks, EU digital identity	Renault, MOBI consortium, Bosch, Daimler Mobility
Autonomous Vehicles (Level 4–5)	2030–2035	Testing by Waymo, Cruise, Baidu; SAE autonomy definitions	Waymo, Cruise, Tesla, Baidu Apollo
Security-as-a-Service	2027–2035	Development of cloud security platforms (Upstream, Karamba)	Continental, Cisco, Karamba Security, Upstream Security
Intelligent Infrastructure	2025–2035	Smart City projects; EU and Asia; RSU deployment	Toyota, Audi, municipalities in EU and Asia
AI and Edge Computing in Vehicles	2023–2035	Development by NVIDIA, Qualcomm; AI for safety and processing	Volvo, NVIDIA, ZF, Bosch, Qualcomm

Tab. No.2 Analysis of baseline assumptions for automotive connectivity development up to 2035 [4,5,11,12,13,14]

4.1. Fully connected and autonomous vehicles

By 2035, most new vehicles are expected to be equipped with advanced autonomous driving systems (SAE Level 4 and 5), requiring continuous and reliable connectivity.

These vehicles will be capable of:

- Communicating with other vehicles and infrastructure in real time (V2X).
- Receiving and processing large volumes of data from cloud and edge devices.
- Responding autonomously to traffic situations without driver intervention.

Forecast: In cities with advanced infrastructure (e.g., Singapore, Shanghai, Munich), autonomous vehicles will become a standard component of public transport and shared mobility. [4,5,12,13, Tab. č.2]

4.2. Digital identity and vehicle trustworthiness

With the growing number of digital interactions between vehicles and external systems, implementing a secure digital identity for each vehicle will be essential.

This identity will serve to::

- Authenticate vehicles during communication (e.g., V2V data exchange).
- Manage the vehicle lifecycle (maintenance, insurance, ownership).
- Ensure trust in transactions (e.g., automated payments for charging or parking).

Forecast: By 2035, digital identity will be standardized at the EU level and integrated into every new vehicle, leveraging technologies such as blockchain and decentralized identifiers (DID). [4,5,12,13, Tab. č.2]

4.3. Security services as part of mobility

Cybersecurity will evolve from a passive feature into an active service offered by manufacturers and mobility providers as part of subscription packages.

These services will include::

- Continuous threat and anomaly monitoring.
- Automatic updates of security protocols.
- Remote diagnostics and intervention in case of incidents.

Forecast: Vehicles will be equipped with AI-based security agents capable of autonomously responding to intrusion attempts or system manipulation. [4,5,12,13, Tab. č.2]

4.4. Intelligent transportation infrastructure

Connectivity development will depend on parallel progress in intelligent infrastructure.

By 2035, it is expected that:

- Traffic lights, signs, and intersections will be equipped with roadside communication units (RSUs).
- Cities will use digital twins to simulate and optimize traffic flows.
- Transportation systems will predict congestion and accidents based on vehicle data.

Forecast: Under Smart City initiatives, municipalities will invest in integrating transportation infrastructure with vehicles, enhancing safety and traffic efficiency. [4,5,12,13, Tab. č.2]

4.5. Personalized and adaptive safety

Thanks to advanced analytics and AI, vehicles will tailor safety functions to individual users.

This will include:

- Adaptive configuration of assistance systems based on driving habits.
- Biometric driver authentication (voice, facial recognition, fingerprint).
- Predictive warnings based on behavior and context (e.g., fatigue, stress).

Forecast: By 2035, vehicles will recognize individual users and automatically adjust safety settings to their profile and current conditions. [4,5,12,13, Tab. č.2]

4.6. Challenges and success factors

Despite technological progress, successful implementation of these trends will depend on several factors::

- Interoperability among manufacturers and infrastructure.
- Regulatory frameworks that support innovation while protecting consumers.
- Public trust in new technologies and their safety.
- Education and training of specialists in automotive cybersecurity.

The prediction for 2035 indicates that connectivity will become an inseparable component of safety, mobility, and user experience. Manufacturers, technology firms, and public institutions must collaborate closely to ensure that this development is not only innovative but also trustworthy and secure. [4,5,12,13, Tab. č.2]

5. Challenges and recommendations for secure connectivity development

The advancement of connectivity in the automotive sector represents a fundamental technological shift with the potential to transform how vehicles interact with their environment, infrastructure, and users. Despite its undeniable benefits, this evolution is accompanied by systemic challenges that require a multidisciplinary approach and coordinated action from industry, academia, regulatory bodies, and society as a whole.

Challenge	Recommendation
Technology Fragmentation	Harmonization of Standards
Cybersecurity Risks	Security by Design
Privacy Protection	Transparency and Data Control
Investment Costs	PPP and Pilot Projects
Ethical Dilemmas	Interdisciplinary Legislation

Tab. No.3 Challenges and recommendations [9,10,11,12,13,14]

5.1 Key challenges

5.1.1 Technological fragmentation and interoperability

The absence of unified standards for communication protocols, data formats, and security mechanisms leads to technological fragmentation. This incompatibility among systems from different manufacturers limits effective implementation of V2X communication and reduces the potential for scalable solutions within intelligent transportation infrastructure. [9,10,11,12,13,14]

5.1.2 Cybersecurity and liability

Increased connectivity exponentially raises the risk of cyberattacks on vehicles, their control units, and communication channels. Unclear legal frameworks regarding liability for security incidents complicate responses to threats and hinder effective enforcement of corrective measures. [9,10,11,12,13,14]

5.1.3 Data protection and digital trust

The collection, processing, and transmission of personal data within vehicle connectivity raise fundamental questions about privacy, transparency, and user consent. Insufficient control over data can lead to loss of public trust in digital automotive services. [9,10,11,12,13,14]

5.1.4 Infrastructure and investment barriers

Implementing intelligent transportation infrastructure requires substantial investment in physical and digital components (e.g., RSU units, 5G networks, data centers). Lack of coordination between public and private sectors may slow development and geographically limit service availability. [9,10,11,12,13,14]

5.1.5 Ethical and legal dilemmas of autonomous systems

Decision-making by autonomous vehicles in critical situations, management of digital identity, and cross-border data transfer introduce new ethical and legal challenges that demand interdisciplinary discussion and updates to existing legislative frameworks. *[9,10,11,12,13,14]*

5.2 Strategic recommendations

5.2.1 Harmonization of standards and open protocols

Support for international standardization initiatives (e.g., ISO/SAE, ETSI, UNECE) is essential to ensure system interoperability. Open protocols enable transparency, auditability, and reduce entry barriers for innovative stakeholders. *[9,10,11,12,13,14]*

5.2.2 Integration of security into system design

The concept of “security by design” should be a fundamental principle in connectivity development. This includes implementing security mechanisms during the design phase, regular penetration testing, update management, and real-time threat monitoring. *[9,10,11,12,13,14]*

5.2.3 Strengthening user data sovereignty

Users should have the ability to manage their data through transparent interfaces, including granting or revoking consent, accessing processing history, and exercising the right to erasure. These mechanisms must comply with regulations such as GDPR and ePrivacy. *[9,10,11,12,13,14]*

5.2.4 Support for research and education

Connectivity development requires new expertise in cybersecurity, data ethics, AI, and systems engineering. Interdisciplinary research projects, academic programs, and industrial Ph.D. initiatives should be supported. *[9,10,11,12,13,14]*

5.2.5 Pilot implementations and public-private partnerships

Testing technologies under real-world conditions through pilot projects helps identify technical, legislative, and societal barriers. Public-private partnerships are key to effective financing and scaling of solutions. *[9,10,11,12,13,14]*

Conclusion

Vehicle connectivity represents one of the most transformative elements of current and future mobility. Its development is moving toward the creation of a comprehensive digital ecosystem in which vehicles will continuously communicate with their surroundings, infrastructure, other traffic participants, and cloud services. This trend not only introduces new possibilities for comfort, efficiency, and personalization but fundamentally reshapes the paradigm of road safety.

The analysis indicates that by 2035, we can expect the emergence of fully connected and partially to fully autonomous vehicles utilizing advanced technologies such as 5G/6G networks, V2X communication, edge computing, artificial intelligence, and digital identity. However, these technologies simultaneously create new challenges in cybersecurity, data protection, legal liability, and system interoperability.

Successful implementation of connectivity into practice therefore requires a systemic approach encompassing not only technological innovation but also a robust regulatory framework, standardization, infrastructure investment, and careful consideration of ethical and societal aspects. Cross-sector collaboration among manufacturers, technology companies, academia, and public institutions will play a crucial role.

From a safety perspective, it is essential that system and data protection become an integral part of vehicle and transportation solution design. Only then can connectivity serve not merely as a tool for progress but as a guarantor of trustworthy, secure, and sustainable mobility for the future.

Glossary of Abbreviations:

5G / 6G – Fifth / Sixth generation of mobile networks
V2X – Vehicle-to-Everything: communication between a vehicle and all external entities (vehicles, infrastructure, pedestrians, network)
V2V – Vehicle-to-Vehicle: communication between vehicles
V2I – Vehicle-to-Infrastructure: communication with traffic infrastructure

V2P – Vehicle-to-Pedestrian: communication with pedestrians
V2N – Vehicle-to-Network: communication with the network
OTA – Over-the-Air: wireless software update
AI – Artificial Intelligence
ECU – Electronic Control Unit
ADAS – Advanced Driver Assistance Systems
GNSS – Global Navigation Satellite System
eCall – Emergency Call: automatic emergency call in case of an accident
HSM – Hardware Security Module
GDPR – General Data Protection Regulation (EU)
ISO/SAE 21434 – International standard for vehicle cybersecurity
UNECE WP.29 – UN regulation for cybersecurity and software updates in vehicles
PPP – Public-Private Partnership
DID – Decentralized Identifier
API – Application Programming Interface

References

Books:

[1] VLK, František. *Automobilová elektronika 1: Asistenční a informační systémy.* Brno: František Vlk, 2006. 308 s. ISBN 80-239-7062-3.

[2] VLK, František. *Automobilová elektronika 2: Systémy řízení podvozku a komfortu.* Brno: František Vlk, 2007. 312 s. ISBN 80-239-7063-1.

[3] REIF, Konrad. *Automotive Mechatronics: Automotive Networking, Driving Stability Systems, Electronics.* Wiesbaden: Springer Vieweg, 2014. 512 s. ISBN 978-3-658-03897-2.

[4] RAJKUMAR, R., et al. *Cyber-Physical Systems: Principles of Design.* Cambridge: MIT Press, 2016. 280 s. ISBN 978-0-262-03301-7.

[5] KHAN, M. I., & KHAN, M. A. *Connected Vehicles in the Internet of Things: Concepts, Technologies and Frameworks.* Boca Raton: CRC Press, 2020. 350 s. ISBN 978-0-367-34392-0.

Journals:

[6] LI, Yufeng et al. Complying with ISO 26262 and ISO/SAE 21434: A Safety and Security Co-Analysis Method for Intelligent Connected Vehicles. In: *Sensors*, Vol. 24, No. 6, 2024. MDPI. [online] [cit. 19-9-2025] available from: https://www.mdpi.com/1424-8220/24/6/1848

[7] PAPADIMITRATOS, P. et al. Vehicular Communication Systems: Enabling Technologies, Applications, and Future Outlook on Intelligent Transportation. In: *IEEE Communications Magazine*, Vol. 47, No. 11, 2009. IEEE. ISSN 0163-6804.

[8] PETIT, J., & SHLADOVER, S. E. Potential Cyberattacks on Automated Vehicles. In: *IEEE Transactions on Intelligent Transportation Systems*, Vol. 16, No. 2, 2015. IEEE. ISSN 1524-9050.

Data, Reports, Thesis:

[9] SCHMIEDECKER, M. *A Hacker's View to ISO/SAE 21434*. BruCON Conference, 2019. [online] [cit. 19-9-2025] available from: https://files.brucon.org/2019/03-Martin-Schmiedecker-ISO21434.pdf

[10] MVEACOM. *Digitalizace a konektivita v moderních vozidlech: Bezpečnostní a etické otázky*. Veacom.cz, 6. 7. 2025. [online] [cit. 19-9-2025] available from: https://www.veacom.cz/cs/blog/digitalizace-a-konektivita-vmodernich-vozidlech-bezpecnostni-a-eticke-otazky-41

[11] SGS. *ISO/SAE 21434 certifikace – Řízení kybernetické bezpečnosti silničních vozidel*. SGS.com, 2024. [online] [cit. 19-9-2025] available from: https://www.sgs.com/cs-cz/services/iso-sae-21434-certifikace--systemu-kyberneticke-bezpecnosti-silnicnich-vozidel

[12] UNECE. *WP.29 – World Forum for Harmonization of Vehicle Regulations.* UNECE.org, 2023. [online] [cit. 19-9-2025] available from: https://unece.org/transport/vehicle-regulations

[13] NVIDIA. *NVIDIA DRIVE: AI Platform for Autonomous Vehicles.* Nvidia.com, 2025. [online] [cit. 19-9-2025] available from: https://www.nvidia.com/en-us/self-driving-cars/drive-platform/

[14] ETSI. *Intelligent Transport Systems (ITS); Vehicular Communications.* ETSI.org, 2024. [online] [cit. 19-9-2025] available from: https://www.etsi.org/technologies/intelligent-transport

Author:

[1]**Jozef Kočík –** external doktorand, University of Security Management in Košice, Košťová 1, Košice, Slovakia, email: jozefkocik@seznam.cz