via iD

September 2024

At the intersection of technology and cybersecurity: what are the challenges of connected mobility?

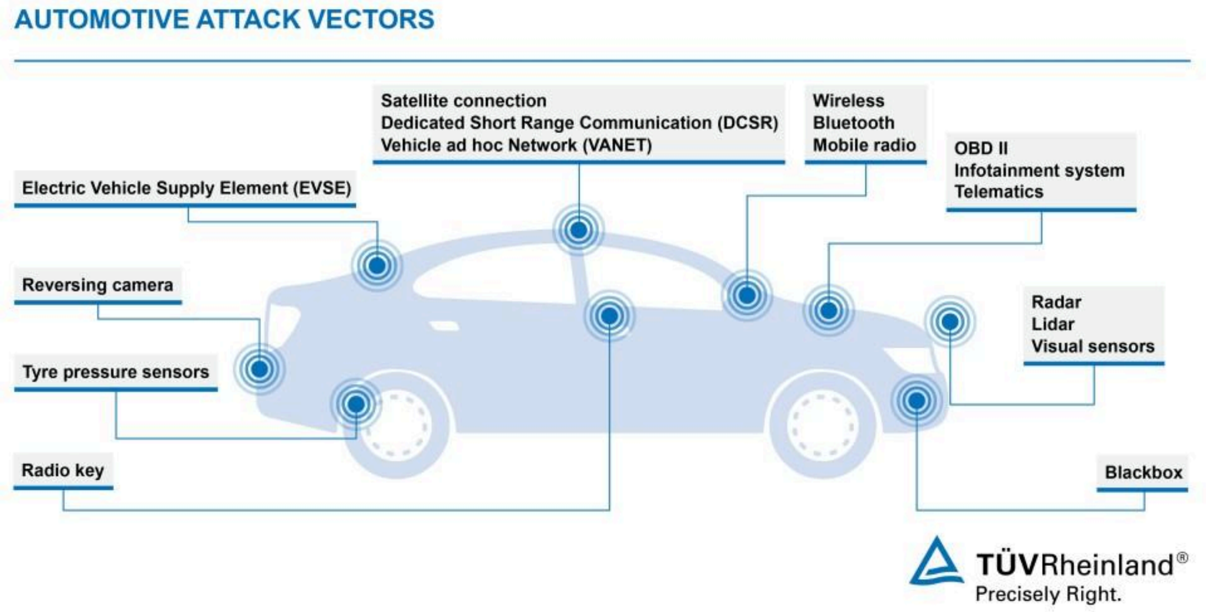
Romain LAFITTE
Managing Director at Via ID

Summary

In a world where technology and connectivity are reshaping the automotive industry, recent concerns raised by U.S. authorities regarding Chinese connected cars highlight the key issues at the intersection of mobility and cybersecurity. The evolution of these technologies raises essential questions about the safety and security of information and infrastructure in a world where every vehicle is a node in a vast, interconnected network.

Luca de Meo, CEO of the Renault Group, believes that "The Software Defined Vehicle represents the future of the automotive industry," signaling a spectacular rise in the connected vehicle[1] market. This transformation is not just a technological revolution but a paradigm shift in how we design, use, and interact with our means of transportation. However, **the promise of more efficient, personalized, and connected mobility comes with its own set of challenges**, particularly in the realm of cybersecurity.

The exponential growth of vehicle connectivity, while opening new horizons for innovation and enhancing the user experience, also introduces heightened vulnerability to cyber threats. Beyond protecting users' personal data, cybersecurity concerns also extend to the safety of transportation systems themselves, which could be targeted for disruption or immobilization. In response to this challenge, the connected mobility industry must strike a delicate balance between technological innovation and security imperatives, engaging in a constant battle to protect infrastructure and data from emerging threats.

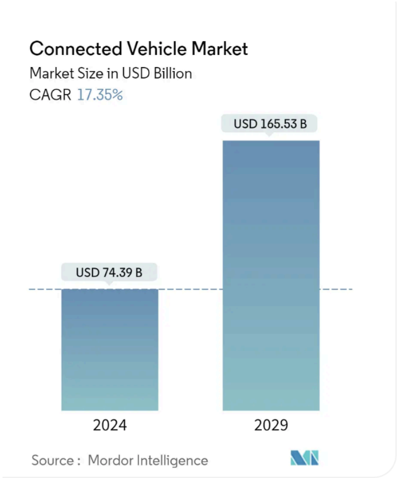


Source: TUV Rheinland

[1] A connected vehicle is a vehicle that integrates communication technologies to exchange data with other devices, thereby enhancing safety, efficiency, and comfort.

Accelerating into the future: current trends and market projections for connected vehicles

The rapid expansion of the connected vehicle market is revolutionizing the automotive industry, redefining the foundations of modern mobility. By 2027, the number of connected vehicles in service worldwide is expected to nearly double, growing from 192 million in 2023 to 367 million. This impressive growth is supported by a booming market, estimated to be worth USD 74.39 billion in 2024 and projected to reach USD 165.53 billion by 2029, with a remarkable compound annual growth rate (CAGR) of 17.35% over the 2024-2029 period.



This rapid development reflects increased global adoption, though the penetration rate of connected vehicles varies significantly from region to region. While Japan's rate is only 30%, countries like France and Germany boast much higher rates (71.8% and 84.3%, respectively). **These disparities highlight the diversity of approaches and strategies at the international level**.

Mary Barra, CEO of General Motors, encapsulates this transformation: "**The future of mobility will be defined by those who can successfully integrate connectivity, electrification, and autonomous driving**." This vision underscores the full potential of connected mobility, not just to revolutionize the automotive industry but to shape society as a whole. The implications extend beyond the vehicles themselves, **promising advances toward smarter, more efficient, and more sustainable cities**.

New entrants and massive investments in vehicle connectivity

This transformation has given rise to new companies specializing in vehicle connectivity, while tech giants like Google are investing heavily in the field. Waymo, a subsidiary of Alphabet (Google's parent company) that specializes in autonomous driving technologies, is at the forefront of this revolution. These tech companies offer solutions ranging from autonomous fleet management to advanced navigation, leveraging connectivity to provide safer, cleaner, and more efficient mobility.

Vehicles now have the ability to connect and communicate with their environment in various ways, revolutionizing road safety, fleet management, and energy efficiency. **Vehicle-to-infrastructure (V2I) connectivity provides vital safety and environmental data**. Between vehicles, **this exchange enhances safety and reduces traffic congestion**. Furthermore, cloud connectivity offers benefits in performance management and maintenance, while communication with pedestrians **aims to prevent accidents**. Lastly, interconnection with other devices opens up endless possibilities for integrating cars into the broader Internet of Things (IoT) network.

An infrastructure for optimal vehicle connectivity

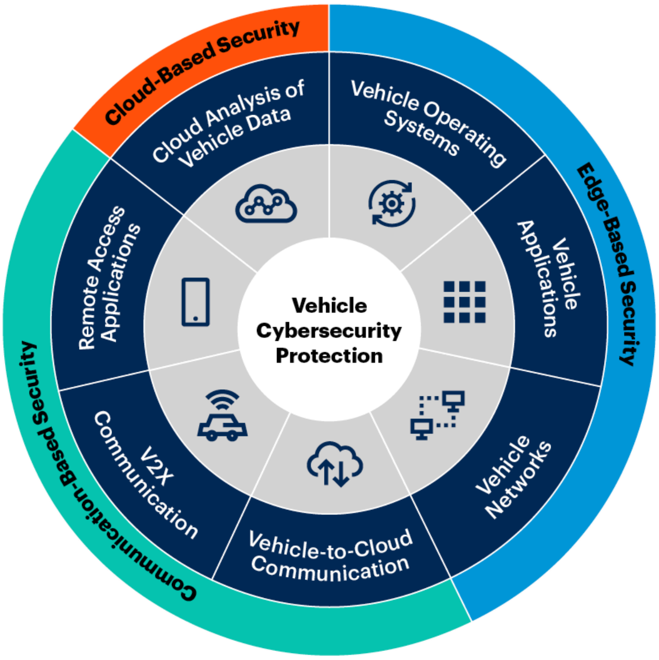
To meet the demands of connected cars, which generate millions of data points every day, internet connectivity needs to adapt. The arrival of 5G is a first step, but as Damien Garot, CEO of Stellar, points out, "it doesn't provide sufficient coverage across all of our roads." This is why the startup offers its automotive industry partners **an intelligent hybrid connectivity solution**. “A perfect internet connection on the road can only be achieved by combining all available wireless technologies (4G/5G cellular, Wi-Fi, and satellite) using advanced algorithms based on artificial intelligence and precise mapping of telecom networks on the roads.”

Emerging services and new business models

This era of connectivity promises not only to enhance the driving experience but also to introduce new business models. Data-driven services, such as pay-per-mile insurance or behavior-based insurance (using data to reward safe driving practices), are emerging. Predictive maintenance services are also gaining traction, where the analysis of operational data helps anticipate repair needs, improving vehicle reliability and reducing maintenance costs for owners. Additionally, in-car entertainment platforms leverage user preferences to offer personalized content, turning time spent in the car into a recreational experience. This shift towards connected and intelligent mobility represents both a major challenge and opportunity for the automotive industry, requiring swift adaptation to stay at the forefront of innovation. However, it also brings significant cybersecurity challenges.

Automotive cybersecurity: the challenges of responding to growing threats in a connected world

Seven Aspects of Connected Vehicle Cybersecurity Protection



Cloud-Based Security
Edge-Based Security
Communication-Based Security
Cloud Analysis of Vehicle Data
Vehicle Operating Systems
Vehicle Applications
Vehicle Networks
Vehicle-to-Cloud Communication
V2X Communication
Remote Access Applications
Vehicle Cybersecurity Protection

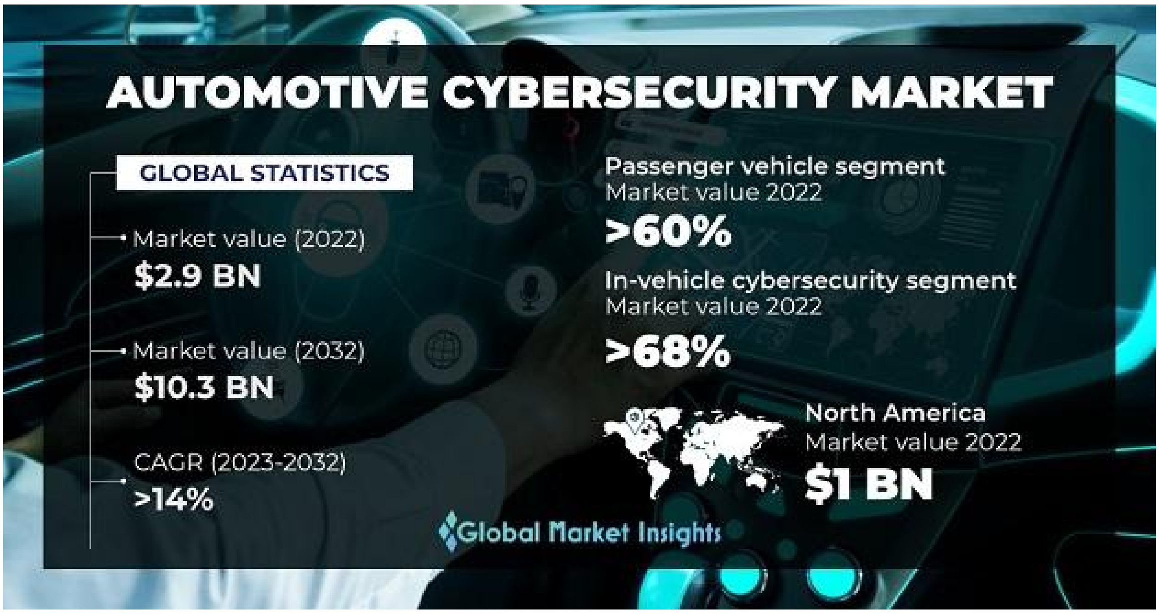
Source: Gartner
717045_C

Gartner

The risks of remote control of a connected vehicle

The crucial importance of cybersecurity in the field of road safety is highlighted by Chris Valasek, a recognized expert for his research on the vulnerability of vehicles to remote attacks. He emphasizes that "the security of connected vehicles transcends the mere protection of personal data to become a **foundation of road safety itself**." This statement underscores the indispensability of cybersecurity, not only for privacy but also as **a guarantor of the physical safety of occupants**. In the face of constantly evolving threats, the adoption of robust and adaptable defense strategies has become imperative.

This is why the automotive cybersecurity sector is experiencing exponential growth. Estimated at $2.9 billion in 2022, projections suggest it could reach $10.3 billion by 2032. This trend highlights the urgent need to develop advanced solutions to address the growing threats. Indeed, as automobiles become more integrated into the global digital network, they are exposed to increased risks of hacking and data theft.



Source: Global Market Insights

These risks of hacking and data theft primarily manifest in two critical forms: data protection and road safety. With the integration of infotainment systems and Electronic Control Units (ECUs) containing up to 40 million lines of code, connected vehicles are extremely vulnerable. These complex systems **can be exploited for personal information theft or, more dangerously, for remote control of vital functions such as braking or steering systems**. Thus, the increasing sophistication of connected vehicles, equipped with complex networks of sensors and algorithms, heightens their vulnerability to cyberattacks. Advanced Driver Assistance Systems (ADAS) use sensors like LiDAR, cameras, and radars to collect data about the vehicle's environment and make driving decisions. These systems rely on complex algorithms to process data and act accordingly, such as automatically adjusting speed, performing emergency braking, or assisting in lane-keeping. If a hacker manages to compromise these systems, they could disable emergency braking or manipulate the lane-keeping assistance system to cause an accident.

Similarly, **Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications are essential for the safety and efficiency of connected driving**. They allow vehicles to share information about their position, speed, and direction, as well as road conditions and traffic signals. This information helps avoid collisions and optimize traffic flow. However, a hacker could, for example, send false information to a vehicle, making it believe that an obstacle is in its path, thus prompting the vehicle to make an unnecessary and potentially dangerous evasive maneuver.

A concrete example of these vulnerabilities was demonstrated by security researchers who successfully took remote control of a Jeep Cherokee. By exploiting a vulnerability in the infotainment system connected to the vehicle's internet, they gained access to critical vehicle functions such as steering, acceleration, and braking, demonstrating the potential risks associated with the cybersecurity of embedded systems. **Journalist Andy Greenberg, who participated in the exercise, had a shocking experience**. While driving on a U.S. highway at 100 km/h, several onboard functions of the Cherokee activated by themselves. The ventilation blew at maximum, the radio turned on at full volume, the windshield washer emptied its reservoir, and the wipers went haywire. But that wasn't all... the researchers managed to disable the transmission and deactivate the brakes.

What solutions are there to strengthen cybersecurity for connected vehicles?

Facing this threat to the automotive industry, implementing robust security solutions and measures for connected vehicles has become a priority. The automotive sector is responding by adopting strict standards and regulations, as well as deploying advanced technologies to protect users and their data.

Several standards and regulations now structure cybersecurity in the automotive sector. These address all phases of the vehicle lifecycle, from design to maintenance, to be as effective as possible.

- For example, the ISO/SAE 21434 standard, resulting from a collaboration between the International Organization for Standardization (ISO) and the Society of Automotive Engineers (SAE), defines crucial guidelines for information security management. **It promotes thorough risk analysis and the adoption of appropriate protection measures**.
- The National Highway Traffic Safety Administration (NHTSA), the U.S. federal agency responsible for road safety, and the SAE J3061 standard, specific to cybersecurity in the automotive industry, **provide guidance for identifying and managing cybersecurity risks, emphasizing** the importance of remaining proactive against digital threats.
- These efforts are complemented by recommendations from WP.29, the global forum for harmonizing vehicle regulations of the United Nations, **which establishes principles for the security of connected vehicles and for Over-The-Air (OTA)** software updates. These OTA updates are crucial for quickly addressing vulnerabilities. In parallel, best practices from the Automotive Information Sharing and Analysis Center (Auto-ISAC) assist manufacturers and suppliers in strengthening their defenses against cyberattacks by promoting information sharing and collaboration in automotive cybersecurity.

These frameworks and guidelines play a vital role in preventing cyberattacks and protecting users in an ever-evolving technological landscape.

Opportunities for industry players

Automakers deploy innovative measures

In the wake of the regulations established by the standards and recommendations mentioned earlier, automakers are implementing innovative measures for cybersecurity. These efforts aim to effectively protect vehicles against cyber threats throughout their lifecycle.

- The adoption of **advanced encryption systems**, such as the **Advanced Encryption Standard (AES)**, secures vital communications. At the same time, as recommended by the UN, Over-The-Air (OTA) software updates enable rapid responses to vulnerabilities without the need for physical intervention.
- **Intrusion Detection Systems (IDS)** monitor system activities to identify and counterattack attempts, while the segmentation of internal networks

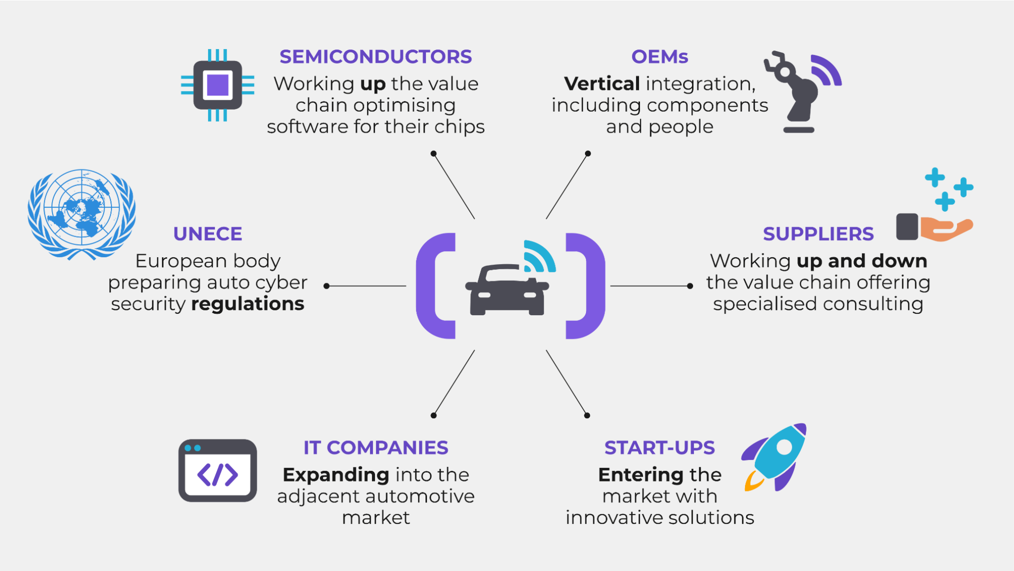
isolates critical functions from less sensitive ones, reducing the risk of exploiting vulnerabilities.

- Additionally, **the use of artificial intelligence** helps detect attack patterns, strengthening prevention against emerging threats.
- The commitment to proactive cybersecurity is also reflected in user awareness initiatives, informing them of best practices to minimize risks.

These initiatives illustrate automakers' commitment to keeping pace with and surpassing cybersecurity standards, combining regulatory compliance and innovation to ensure the safety of connected vehicles in an evolving digital environment.

In a context where connectivity in mobility is experiencing explosive growth, the importance of cybersecurity is becoming clearer than ever. The risks associated with data security and infrastructure in this rapidly expanding sector have prompted key players to take significant measures to counter growing threats. Companies, regulators, and standardization bodies are working together to develop robust and adaptive solutions that ensure the safety and protection of users and their data.

Emergence of new players/startups specializing in automotive cybersecurity


SEMICONDUCTORS
Working **up** the value chain optimising software for their chips
OEMs
Vertical integration, including components and people
UNECE
European body preparing auto cyber security **regulations**
SUPPLIERS
Working **up and down** the value chain offering specialised consulting
IT COMPANIES
Expanding into the adjacent automotive market
START-UPS
Entering the market with innovative solutions

Source: Expleo

Among the responses to these challenges, we are witnessing the emergence and development of companies specializing in automotive cybersecurity, such as Argus Cyber Security, C2A Security, Upstream Security, GuardKnox, ProvenRun, and SAIFLOW. These companies bring crucial technological innovations and tailored cybersecurity solutions to effectively address the unique challenges posed by the era of connected vehicles.

Argus Cyber Security, acquired by Continental in 2017 for $450 million, exemplifies the integration of advanced cybersecurity solutions into the automotive industry. This company works closely with renowned automakers **to integrate its security solutions**. Similarly, C2A Security emphasizes partnerships with AUTOSAR to develop cybersecurity standards and with Valeo to enhance the security of automotive systems **by integrating its security solutions directly at the hardware level**. Upstream Security, for its part, **has partnered with several major cloud platforms to enhance monitoring and data security for connected vehicles**. These collaborations perfectly illustrate how automotive cybersecurity companies work alongside traditional industry players and technology innovators to meet the unique challenges posed by the era of connected vehicles.

Emerging as essential players in the ecosystem, these startups are increasingly being watched by traditional companies in the sector. According to recent projections by McKinsey, **the increased importance of cybersecurity in the automotive sector is expected to lead to a significant rise in investments, from $4.9 billion in 2020 to nearly $9.7 billion by 2030**. This growth will be largely supported by the adoption of new regulations established by the United Nations, which will encourage a wave of innovation. This legislative context opens up new economic opportunities, particularly for automotive industry suppliers, tech companies, and specialized startups, especially in the areas of software development and associated services.

By forging links with leading companies and government entities, these startups strengthen the overall mobility ecosystem, **positioning the automotive cybersecurity market as an increasingly attractive investment area**. With the rise of data protection and road safety issues in a connected world, these strategic partnerships highlight the urgency and importance of investing in advanced cybersecurity solutions, heralding a promising future for the sector.

A promising sector for investors

I believe that the cybersecurity market in mobility represents a true market of the future, promising numerous investment opportunities. The demand for data protection solutions and the securing of mobility systems continues to grow, making this sector particularly attractive for investors looking for promising fields. Data protection, at the heart of users' and manufacturers' concerns, is becoming a major issue that defines the value and competitiveness of mobility solutions in the market.

I am keeping a close eye on this market, convinced of its significant potential. Automotive cybersecurity is not merely a protective issue; **it represents an opportunity for innovation and differentiation in a constantly evolving sector**. The companies that have developed in this field over the past few years, particularly in Israel, a recognized leader in cybersecurity innovation, illustrate the dynamics and growth potential of this market.

In conclusion, investing in automotive cybersecurity appears to be a strategic approach to anticipating the future needs of connected mobility and ensuring a technological lead in the field. The ability to effectively protect data and systems will be a key factor for success in the era of smart and connected mobility, offering unprecedented opportunities for visionary investors ready to help shape the future of mobility.

Contact us:

rlafitte@via-id.com

Romain Lafitte

Written by Romain LAFITTE
Managing Director at Via ID

Discover our website:

www.via-id.com

Follow us on social networks!