Automotive iQ

STATE OF AUTOMOTIVE CYBER SECURITY, CONNECTIVITY & SOFTWARE-DEFINED VEHICLES REPORT

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

EXECUTIVE SUMMARY

The automotive sector is currently experiencing a profound shift towards software-defined vehicles (SDVs) with cloud-based operating platforms and over-the-air (OTA) updates becoming standard. According to recent forecasts by multiple studies, SDVs are expected to account for most vehicles sold by the end of this decade. This transformation is driving significant R&D efforts as legacy companies look to remain competitive in an increasingly digital era. According to estimates by Deloitte, investments in the design and development of SDVs reached over US$4 billion in 2024. OEMs are also prioritising investments in digital technologies such as artificial intelligence (AI), machine learning (ML), digital twins, and internet of things (IoT), as they assume critical importance in augmenting vehicle intelligence, personalisation, and autonomous driving capabilities.

This evolution has enabled novel opportunities for data monetisation, with additional revenues available to suppliers expected to grow to around US$700 billion by 2035. Monetising features such as better navigation, infotainment, and safety functions gives OEMs an opportunity to diversify their revenue streams beyond traditional vehicle sales. The key monetisation strategies being employed by SDV OEMs include features as a service, services around a vehicle, and data monetisation.

Even though the shift towards SDVs brings unprecedented opportunities for innovation, monetisation, customer experience, and operational efficiency, it also exposes manufacturers and suppliers to a rapidly evolving cyber threat landscape. In fact, the complexity of achieving comprehensive cyber security has already increased to such a level that even large OEMs are struggling to keep up with evolving threats. According to a 2024 Gartner study, vehicle cyber threats have increased by 600% over the past four years, with attacks now targeting everything from infotainment systems to remote vehicle takeovers and critical ECUs. Therefore, SDV manufacturers have started adopting novel technologies, processes, and business models to curb costs, while ensuring vehicle safety and security. These include edge AI, cyber security standards such as ISO 21434 and UNECE R155/R156, cyber security management systems (CSMS), the zero-trust model, and adherence to security by design principles.

AI and edge computing are by far the most suitable solutions that OEMs are increasingly adopting to detect and respond to threats autonomously, reducing dependency on the cloud and lowering operational costs. Notably, the AI-based cyber security is projected to be a US$135 billion market by 2030.

COMPLIANCE UPDATES

International automotive cyber security regulation is becoming increasingly harmonised and comprehensive, shaping compliance requirements and product development strategies. The foundation is laid by ISO 21434, which mandates end-to-end cyber security risk management throughout the vehicle lifecycle, from concept to decommissioning. Compliance is now a prerequisite for market access in most regions, with a second edition expected by 2028 to address evolving threats. Complementing this, UNECE R155/R156 regulations require all vehicles produced from July 2024 onward to incorporate Cyber Security Management Systems (CSMS) and Software Update Management Systems (SUMS). Special-purpose and small-series vehicles must comply by July 2026.

At a broader digital product level, the EU Cyber Resilience Act (CRA) expands obligations for secure software development, vulnerability handling, and incident reporting for connected vehicles. This is reinforced by the updated Product Liability Act, which holds OEMs accountable for software defects and cyber security breaches, with only limited legal exemptions.

Meanwhile, China's GB 44495 regulation integrates elements of ISO 21434 and UNECE R155 but adapts them to national priorities, forming a localised cyber security framework with mandatory compliance.

STRATEGIC FOCUS AREAS

To meet growing consumer demand for faster vehicle delivery without compromising product integrity and security, OEMs are adopting agile, parallel development

models like "shift-left" and "software-first." These allow software to be developed and tested virtually before hardware is finalised, significantly accelerating time-to-market. Central to this transformation is the integration of AI into daily product development. AI models are now embedded throughout the software lifecycle, from code generation and static analysis to real-time anomaly detection, enhancing cyber security by continuously assessing vulnerabilities, performing predictive diagnostics, and enabling secure over-the-air (OTA) updates.

AI's role is even more critical in autonomous vehicles, where machine learning and deep learning algorithms improve sensor data interpretation, support real-time threat detection, and ensure secure decision-making under unpredictable conditions. AI is also optimising cost and development time. GenAI-powered simulations that replicate real-world driving scenarios significantly reduce dependence on costly road testing. IBM estimates that these efficiencies could potentially shorten launch timelines by 21% and enhance productivity by nearly 40%.

These technologies also strengthen the safety of advanced driver assistance systems (ADAS) and automated driving, from AI-driven sensor fusion to platforms like Nvidia's DRIVE AGX. Supporting this is a transition from domain-centric to zonal-centric architecture, which simplifies wiring, reduces weight, and improves OTA update performance. Tesla and Volkswagen have leveraged zonal designs to halve production time and boost efficiency.

These advancements, from faster delivery and AI integration to enhanced safety architectures, are reshaping how value is delivered to the end user. Consequently, consumer perception is evolving, and buyers are increasingly willing to pay a premium for SDVs, not only for their intelligent features but for ongoing updates, better security, and a seamless digital experience. This shift is unlocking new monetisation avenues for OEMs through subscriptions, feature unlocks, and data services.

FUTURE PROSPECTS

The SDV industry is poised for exponential growth, driven by advancements in AI, 5G connectivity, and edge computing. By 2030, nearly 90% of vehicles are expected to feature software-defined architectures, reshaping the competitive landscape. Leading OEMs have already announced an ambitious SDV pipeline, including Hyundai's global SDV rollout by 2030, Volkswagen's Golf and Audi A4 e-tron by 2028–2029, and Scout Motors' zonal-architecture-based Traveler and Terra models in 2028. Other anticipated launches like the Lexus LF-ZC, Volvo EX60, and Tata's Avinya indicate strong momentum across Asia, Europe, and North America.

Cyber security will remain a critical differentiator, with prospects centred on quantum-resistant algorithms, AI-powered threat intelligence, and real-time system resilience. Regulatory alignment across global markets will intensify, compelling OEMs to embed cyber security from design through decommissioning. With evolving customer expectations and increasing willingness to pay for digital features, SDVs are set to become platforms for continuous innovation, personalised mobility, and recurring revenue models.

DRIVING COMPETITIVENESS, CUTTING COSTS & ENSURING VEHICLE SECURITY

HOW COMPANIES ARE CUTTING COSTS AND IMPROVING EFFICIENCY, SAFETY, AND SECURITY

According to a 2024 Gartner study, there is a 600% increase in vehicle cyber threats over the last four years. The exponential increase in the number of software-defined vehicles (SDVs) hitting the road further exacerbates this problem from a diagnostic and mitigation perspective. With most OEMs currently relying heavily on cloud-based detection and uploading vast amounts of data to the vehicle security operations centre (VSOC), transmission costs have escalated to around US$2.1 million per month, creating a significant financial strain. Moreover, as vehicles integrate complex software, effective troubleshooting becomes harder and more expensive for an industry that has traditionally been hardware focused.

SDV manufacturers have started adopting novel technologies, processes, and business models to curb costs, while ensuring vehicle safety and security.

- **Edge AI:** Many OEMs are utilising edge AI to reduce dependency on expensive cloud solutions. The technology essentially equips vehicles with the intelligence to autonomously learn, detect threats, and, if necessary, defend themselves. Each vehicle's architecture is integrated with the foundational capabilities of an entry-level VSOC, allowing it to detect threats directly at the edge using advanced computing resources like central processing units (CPUs), neural processing units (NPUs), or graphics processing units (GPUs). By minimising dependency on the cloud, edge AI reduces costs and ensures that data remains secure onboard. The reduction in data transmission also results in lower VSOC operational costs and integration and maintenance costs.

- **Cyber Security Standards:** Automotive industry standards such as ISO 21434, UNECE R155/R156, etc., and related principles such as Secure Software Development Life Cycle (SSDLC) and Security-by-Design play a key role in enabling a more secure and cost-effective smart mobility ecosystem. These standards were developed to ensure that OEMs and suppliers incorporate cyber security protocols and solutions at every step of the product lifecycle, from the concept phase to retirement. This ensures that potential vulnerabilities are detected and mitigated during the early stages, reducing the risk of costly recalls. Importantly, investing in measures such as ISO 21434 helps OEMs realise significant cost savings by preventing data breaches, system failures, regulatory fines, and potential litigation.

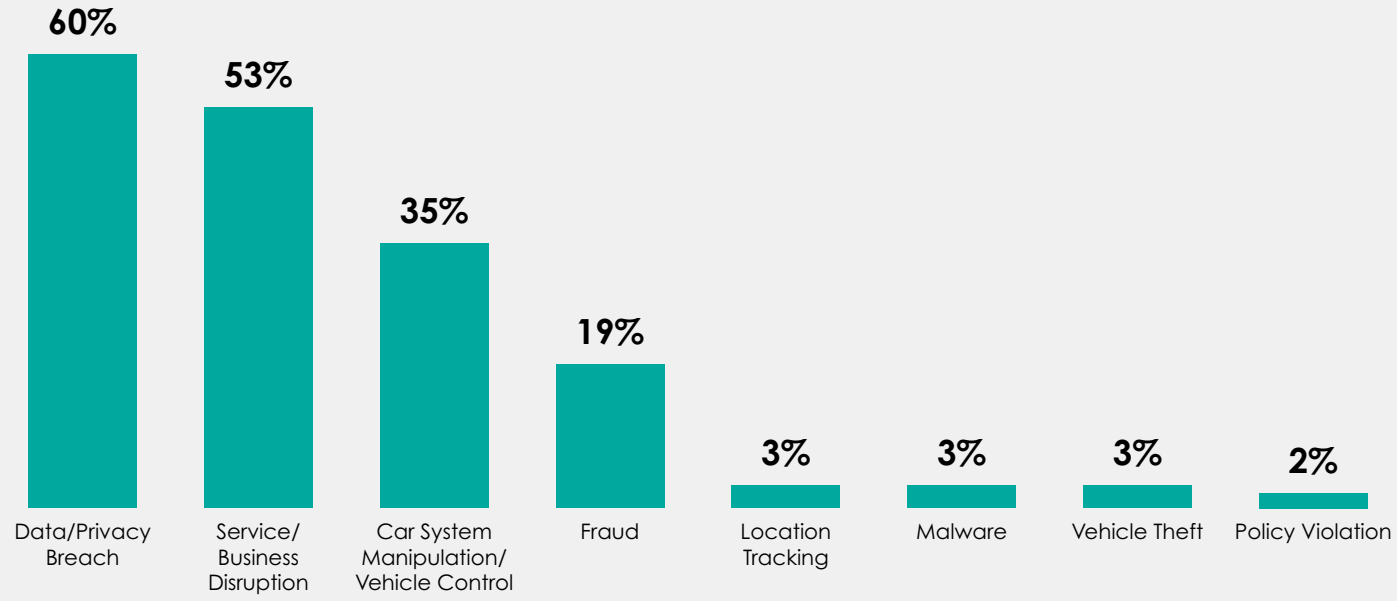
- **Cyber Security Management Systems (CSMS):** Under a recent regulation by the United Nations (UN), SDV OEMs are required to implement cyber security management systems (CSMS) to "guarantee vehicle safety and data protection through rigorous cyber security measures." One such solution is cyber security platforms such as the one offered by DevSecOps platform provider C2A Security to companies such as Daimler Trucks, BMW, Marelli, NTT Data, Siemens, and Valeo. These platforms automate cyber security features and implement efficient processes such as OTA updates, thereby facilitating cost-effective and efficient compliance with regulations.

- **Zero-Trust Model:** Zero-trust is a new cyber security model that replaces the traditional one by recommending continuous verification of users, devices, and applications, whatever their position or origin. OEMs are fastly recognising the benefits of adopting this model to reduce the attack surface and prevent lateral movement without relying on implicit trust. Adopting the zero-trust principle in Intelligent Transportation Systems (ITS), especially SDVs, presents an effective solution in the face of increasing threats. From a cost perspective, the model facilitates efficient network cost management in the form of high detection rates, low false positive rates, and reduced network costs in simulation results.

- **Security By Design with DevSecOps:** OEMs are fast recognising the benefits of integrating security measures early in the development process through the Development, Security, and Operations (DevSecOps) approach. This is because vulnerabilities detected during development are much easier to fix than those detected after the delivery of the vehicle. DevSecOps platforms speed up development and testing by adopting the shift-left and security-by-design concepts, that result in reduced time between updates, and reduced costs.

"According to a 2024 Gartner study, there is a 600% increase in vehicle cyber threats over the last four years. The exponential increase in the number of software-defined vehicles (SDVs) hitting the road further exacerbates this problem from a diagnostic and mitigation perspective."

FIGURE 1: AUTOMOTIVE-CYBER-ATTACK INCIDENTS IN 2024



Source: Upstream Security

STRATEGICALLY MEETING CONSUMER DEMAND FOR FASTER VEHICLE DELIVERY WITHOUT COMPROMISING PRODUCT INTEGRITY AND SECURITY

One of the primary goals of OEMs manufacturing SDVs is to shorten the time-to-market while augmenting the vehicle's safety and security features. A way to do this is by adopting cloud-native technologies such as continuous integration/continuous delivery/continuous testing (CI/CD/CT), containerisation, and APIs, and integrating them with virtualisation techniques. This facilitates the creation of digital twins of the vehicle's electronic control units (ECUs) in a simulated cloud-based environment prior to the physical, target hardware being available.

OEMs are able to deploy a parallel and iterative development process that is more efficient and less time-consuming than the conventional sequential method, which has a hardware-first approach. This process is the key tenet of the "shift-left" and "software-first" approach, which not only enhances overall test coverage and software quality but also streamlines the software development process, thereby allowing OEMs to get their vehicles to market faster without compromising product integrity and security.

"OEMs are able to deploy a parallel and iterative development process that is more efficient and less time-consuming than the conventional sequential method, which has a hardware-first approach. This process is the key tenet of the "shift-left" and "software-first" approach, which not only enhances overall test coverage and software quality, but also streamlines the software development process."

Another way OEMs are simplifying and accelerating vehicle software development and integration is by adopting modular designs and standardisation to reduce complexity and facilitate the reuse of software components across different models and brands. Modular software architectures also allow for easy updates and integration of new functionalities without the need for multiple versions.

AI-powered solutions are accelerating product design, engineering, testing, fine-tuning, and software deployment for SDV vehicles, thereby speeding up the entire software development lifecycle (SDLC).

LEVERAGING AI FOR AUTOMOTIVE CYBER SECURITY AND SDV DEVELOPMENT

LEVERAGING AI IN DAILY PRODUCT DEVELOPMENT TO ENHANCE AND ADVANCE CYBER SECURITY FRAMEWORKS

AI is becoming integral in the rapid evolution of automotive cyber security, transforming how manufacturers detect and mitigate threats in real time. After all, the technology's ability to process large volumes of data from connected systems enables it to identify anomalies, flag potential breaches, and even automate responses to emerging threats. A recent research report by Morgan Stanley estimated the global market for AI-based cyber security products to be valued as much as US$135 billion by 2030.

"AI is becoming integral in the rapid evolution of automotive cyber security, transforming how manufacturers detect and mitigate threats in real time. After all, the technology's ability to process large volumes of data from connected systems enables it to identify anomalies, flag potential breaches, and even automate responses to emerging threats."

One of the key areas of AI adoption to bolster cyber security in SDVs is the monitoring of critical vehicle systems like electronic control units (ECUs), which have been compromised consistently over the last few years by hackers attempting to corrupt data or take control of vehicle functions. In fact, according to a study by cyber security company Upstream, attempted breaches on ECUs already account for over 25% of all cyber security attacks on vehicles.

Another AI use case is protection against tampering with V2X systems, where attackers have been able to change road safety messages and traffic management systems, potentially causing hazardous situations for drivers.

Yet another vulnerability lies in compliance gaps where hackers aim to exploit any weaknesses in a vehicle's cyber security management system, particularly if certain components or processes are not secured by design.

AI-powered systems have demonstrated significant prowess in mitigating such threats in real-time by continuously monitoring and assessing systems for weaknesses, thereby significantly reducing the window of opportunity for hackers. These systems can also analyse historic incident patterns, established vulnerabilities, and global threat intelligence feeds, to help organisations anticipate future cyber-attacks.

Additionally, AI has proven to be very useful in penetration testing, which involves intentionally probing the defences of software and networks to identify weaknesses. By developing AI tools to target their technology, organisations can better identify their weaknesses before hackers can maliciously exploit them. This will not only stop breaches before they occur but also significantly lower IT costs for enterprises.

USE OF AI MODELS IN AUTONOMOUS CARS

Owing to their ability to process large amounts of sensor data and identify patterns, AI systems play a pivotal role in improving the security of autonomous vehicles by detecting anomalies, mitigating attacks, and ensuring smooth operations even in complex or adversarial conditions. Over the years, AI-driven technologies ranging from ML models that enhance predictive capabilities to deep learning algorithms that improve perception and decision-making have significantly reshaped the automotive landscape. Interestingly, these capabilities are integral for safeguarding both the vehicle's internal systems and interaction with the outside world.

The core AI technologies that are powering autonomous vehicles include GenAI, computer vision & object detection, machine & deep learning, sensor fusion & LiDAR, and edge AI & real-time processing. The key areas where AI is improving security are:

- **Real-Time Response to Threats:** The heavy reliance of autonomous vehicles on sensors like cameras, LiDAR, and radars to make sense of their surroundings makes the proper functioning of these systems imperative. However, these systems have proven vulnerable to cyberattacks such as spoofing, jamming, or data manipulation. AI models such as convolutional neural networks (CNNs) play a critical role in mitigating these threats due to their ability to analyse sensor inputs to identify inconsistencies. For example, if a GPS signal suddenly shows an unlikely location (e.g., jumping continents in seconds), the AI model can quickly compare this with wheel speed sensors or camera data to flag it as a spoofing attempt. Similarly, adversarial attacks involving the use of stickers on road signs often used to confuse object detection, can be mitigated by training AI models on diverse datasets that include similar manipulated scenarios. Apart from mitigating cyberattacks, GenAI systems improve sensor data processing by enhancing data quality, filling in gaps, and generating synthetic sensor data, resulting in better decision-making and safer driving.

- **Secure Decision Making:** AI systems such as reinforcement learning (RL) algorithms play a critical role in ensuring secure decision-making under unpredictable conditions. For example, if the data emanating from a camera feed is restricted due to dirt or hacking, the AI model could prioritise LiDAR data or reduce speed until the issue is resolved. Additionally, these systems conduct regular redundancy checks to ensure that critical systems such as braking or steering remain operational even if one component fails. A good example is Tesla's Autopilot feature that leverages multiple neural networks to cross-validate sensor data, reducing reliance on any single input source. This layered process mitigates the impact of possible breaches and maintains operational integrity.
- **Adaptive Learning:** AI models can be updated over-the-air (OTA) to address novel vulnerabilities such as malware targeting vehicle-to-infrastructure (V2I) communication. A good example of this is Waymo, which continuously integrates its training models with real-world data such as unusual pedestrian behaviour or road obstructions. Additionally, other manufacturers are using unsupervised learning-powered anomaly detection systems to detect unusual network traffic patterns within the vehicle's internal systems, flagging potential intrusions before they escalate.
- **Better Virtual Testing Environments:** GenAI tools help create a range of realistic virtual environments that mimic real-world driving conditions, allowing developers to test and refine their algorithms in a controlled environment. This ensures that autonomous vehicles are sufficiently trained on exhaustive datasets, making them well-prepared to function in the real world. It not only enhances the safety of autonomous vehicles but also reduces the time and costs associated with traditional testing methods.

ENSURING SAFETY AND SECURITY IN SDV PRODUCT DEVELOPMENT THROUGH AI

As a whole, AI maturity across the automotive sector is fairly advanced, with most OEMs having already made significant advancements in integrating AI in their production processes. Central to the evolution of SDVs is the successful integration of AI and ML, with the technologies playing a critical role in powering every facet of vehicle development, including autonomous driving, EV battery performance, predictive maintenance, advanced driver assistance systems (ADAS), and overall vehicle efficiency. In fact, AI and associated technologies are crucial to bridge the gap between legacy automakers and the software-driven future by streamlining development, optimising designs, and facilitating faster testing cycles.

"Owing to their ability to process large amounts of sensor data and identify patterns, AI systems play a pivotal role in improving the security of autonomous vehicles by detecting anomalies, mitigating attacks, and ensuring smooth operations even in complex or adversarial conditions."

AI also plays an important role in the flow of data from vehicles to OEMs and automotive suppliers, and vice versa. More specifically, AI models enable OEMs to execute both firmware over-the-air (FOTA) updates and software over-the-air (SOTA) updates. Additionally, the technology enables personalisation algorithms to help customise vehicle features and settings to individual driver preferences and usage patterns.

In the future, advanced AI models are expected to create more advanced iterations of today's existing vehicle features, like smarter and safer infotainment centres. Another example is fully automated parking in areas with no distinct parking lines or boundaries, a step up from current parking assistance capabilities. Moreover, AI advancements are also expected to drive higher levels of data fusion from multiple sensors as well as dynamic environmental modelling, enhanced anomaly detection, and fault tolerance algorithms.

The key use cases of AI in SDV development are:

- **Autonomous Driving:** The main role of AI, especially GenAI, in enhancing autonomous capabilities is to automate the creation of test scenarios, enhance test coverage, generate test data, and improve simulation accuracy. This has been shown to not only speed up the testing process but also reduce workload and costs. By leveraging GenAI, SDVs can navigate complicated scenarios and make intelligent decisions in real-time.
- **EV Battery Optimisation:** Various challenges in EV technologies, especially battery optimisation, are now being addressed by AI and quantum intelligence (QI). QI, a fusion of quantum computing and AI, drives material discovery by analysing large datasets from quantum simulations to optimise materials for conductivity, stability, and energy density. Additionally, AI-powered digital twins optimise EV battery performance, improve range efficiency, and extend battery life. According to a report by Tata Consultancy Services (TCS), AI and QI-enhanced batteries could potentially extend battery range from 300 to 500 kilometres (186 to 310 miles) per charge to 600 to 800 kilometres (370 to 500 miles). Additionally, enhancements in regenerative braking efficiency through AI could add an extra 10% to 15% to the driving range.

"AI also plays an important role in the flow of data from vehicles to OEMs and automotive suppliers, and vice versa. More specifically, AI models enable OEMs to execute both firmware over-the-air (FOTA) updates and software over-the-air (SOTA) updates."

- **Cyber Security:** AI-powered cyber security becomes incrementally important as vehicles become increasingly connected, owing to its ability to protect both vehicle data and operational integrity. GenAI-powered solutions can optimise the delivery of OTA updates by predicting maintenance needs, generating targeted updates, and enhancing security by identifying and mitigating potential threats.
- **Code Generation:** According to IBM's study "Automotive 2035", GenAI's ability to automate code generation can improve SDV development productivity by 39%. This can reduce the time required to launch new products and services by 21%, allowing companies to respond quickly to changing market dynamics and regulatory frameworks.

THE USE OF AI TO SPEED UP SOFTWARE DEVELOPMENT AND TESTING PROCESSES AND DECREASE COSTS

The automotive industry is undergoing a major transformation with the emergence of SDVs, where software plays a key role in vehicle functionality and user experience. In fact, vehicle software lines of code (LOC) already stand at around 100 million and are expected to grow rapidly in the future as well. In this scenario, the ability to rapidly iterate, update, and improve software and feature updates is seen as key to establishing a competitive advantage, and AI technologies are critical to do just that.

GenAI is transforming the software development process from software 1.0 to software 2.0, where AI models develop software and development teams have AI companions that assist, augment, or transform each phase of the development lifecycle. The technology's ability to facilitate domain-specific feature development, including advanced decision-making systems for autonomous driving, conversational assistants, predictive diagnostics, and cyber security enhancements, makes it a game-changer for OEMs. This accelerates SDV software development from requirement analysis to validation, enabling quicker updates, improved quality, and better handling of complex systems.

"GenAI is transforming the software development process from software 1.0 to software 2.0 where AI models develop software and development teams have AI companions that assist, augment, or transform each phase of the development lifecycle. The technology's ability to facilitate domain-specific feature development, including advanced decision-making systems for autonomous driving, conversational assistants, predictive diagnostics, and cyber security enhancements, makes it a game-changer for OEMs."

Key use cases of AI in software development are:

- **Requirement Analysis:** OEMs have struggled with requirement engineering for a while, often finding it hard to hire people with the required skills. GenAI has automated this process to a large extent by creating structured specification documents that clearly separate system requirements into subsystem and software-level requirements. Additionally, the technology can help in conducting ISO 26262 functional safety-specific analyses, which includes creating failure mode and effects analysis (FMEA) safety analyses.
- **Design and development:** GenAI helps in faster vehicle design and styling by transforming rough sketches into detailed models that can also integrate real-time modifications. While the technology is still not mature enough to create production-ready code, it can certainly refactor code and enhance its quality. For example, it can automatically fix static code analysis errors and ensure that the code is in line with required standards. In autonomous driving, AI models have proven their ability to augment object detection and decision-making, with studies showing an 18% improvement in labelling accuracy using GenAI compared to regular convolutional neural network (CNN) models.
- **Validation:** According to a study by Tata Consultancy Services (TCS), software validation involving multiple testing levels, including unit, feature, system, bench, and vehicle testing, accounts for over 33% of development efforts in the automotive manufacturing sector. In fact, one of the most labour-intensive and time-consuming tasks is generating test cases from structured/unstructured system requirements. GenAI models, especially generative adversarial networks (GANs), combined with regular automation, can help automate the process of test case and script generation, all customised for different domains and validation levels. This automation significantly reduces time and human effort while maintaining high accuracy and coverage.

REGULATORY UPDATES

The digitalisation of vehicles, including in-car gaming and entertainment, and autonomous navigation and driving capabilities, has increased the automotive sector's threat level from a cyber security point of view. International bodies have responded to this by forming various regulatory frameworks that proactively identify and mitigate cyber security risks.

The ISO 27001 and 27002 standards launched by the International Organisation for Standardisation (ISO) in 2005 (and revised in 2013) were the first of their kind frameworks, which detailed a systematic approach to information security management across sectors. In 2016, the U.S. Department of Transportation's National Highway Traffic Safety Administration (NHTSA) issued the "Cyber Security Best Practices for Modern Vehicles" guidelines to improve motor vehicle cyber security. Another one is the U.S. National Institute of Standards and Technology (NIST) Cyber Security Framework 1.0 (CSF 1.0), which was released in 2018 and covered the automotive sector as well.

"The digitalization of vehicles including in-car gaming and entertainment, and autonomous navigation and driving capabilities, has increased the automotive sector's threat level from a cyber security point of view. International bodies have responded to this by forming various regulatory frameworks that proactively identify and mitigate cyber security risks."

Europe released its own set of cyber security frameworks, the General Data Protection Regulation (GDPR) and the Network and Information Systems 1 (NIS1) directives, in 2018 as well. Both of them covered the automotive sector. This was followed by the ISO 21434 standard published in 2020, which focuses on the cyber security management and risk assessment of road vehicles over their entire lifecycle.

The ensuing period has witnessed the rise of fresh vulnerabilities and future possibilities that have resulted in new regulations, along with updates to existing ones. One of them is the EU-focused UN ECE R155/R156 frameworks that establish minimum cyber security standards for vehicles, including software systems. Another is the Cyber Resilience Act (CRA), which was introduced in the European Parliament in 2022. The CRA establishes mandatory cyber security requirements for hardware and software products throughout their whole lifecycle. Also in 2022, members of the European Parliament gave their assent to the Network and Information Systems 2 (NIS2) directive, which looks to implement cyber security practices such as risk analysis, information system security policies, and basic cyber hygiene guidelines across various sectors including automotive.

In September 2022, the U.S. NHTSA released the updated version of "Cyber Security Best Practices for the Safety of Modern Vehicles", which was along the lines of the ISO/SAE 21434 standard. The latest is the NIST Cyber Security Framework 2.0 (CSF 2.0) which was released in 2024. It builds on the NIST CSF1.0 framework to broaden sector inclusivity and establish cyber security as a key component of enterprise risk management.

China, which is one of the largest automobile markets and another prominent player in the automotive sector, released the National Cyber Security Law in 2017, which obligates all OEMs that utilise computers or other technology to gather, store, process, transmit, and distribute data, to adhere to specific cyber security standards. This was followed by the Data Security Law (DSL) and Personal Information Protection Law (PIPL) in 2021, both of which focus on providing regulations to ensure more comprehensive data protection. In October 2021, the Cyberspace Administration of China (CAC), published a guideline document called "Several Provisions on Vehicle Data Security Management", that outlined new requirements for manufacturers and operators of intelligent connected vehicles to protect personal information and 'important' data. The Chinese Ministry of Industry and Information Technology (MIIT) and the Standardisation Administration of China (SAC) have also issued regulations called the Guo Biao (national standard) or GB standards, that outline vehicle cyber security standards. Interestingly, they have several parallels to the tenets and requirements detailed in the UNECE R155/R156 regulations.

SCENARIO IN 2025

The R155/R156 regulations, in force across the EU since July 2022, are now fully applicable to all vehicles produced from July 2024 onwards. The deadline for compliance with R156 for special purpose or small-series vehicles remains July 2026. Japan and South Korea have also aligned with these frameworks and are progressing along similar implementation timelines.

The NIS2 directive has already been transposed into national laws across all EU member states as of October 2024, expanding the scope of cyber security obligations for connected vehicle manufacturers and suppliers.

The Cyber Resilience Act (CRA) entered its implementation phase in the second half of 2024. As of now, OEMs are expected to have established conformity evaluation mechanisms, with the August 2025 deadline for this milestone fast approaching. Additionally, the CRA's mandatory security vulnerability disclosure and cyber incident reporting requirements are set to take effect by November 2025. Looking ahead, the CRA is anticipated to be fully enforceable by late 2027, following the stipulated three-year transition window post-enactment.

In China, the Ministry of Industry and Information Technology (MIIT) and the Standardisation Administration of China (SAC) have mandated that all OEMs comply with baseline vehicle cyber security standards by the end of 2025. MIIT is also on track to roll out over 100 mandatory and voluntary standards related to automotive cyber security by the end of this year.

With these overlapping regulatory pressures and accelerated implementation timelines across global markets, the automotive industry in 2025 is experiencing intense activity as stakeholders race to ensure compliance, certification, and long-term cyber resilience.

NEXT EDITION OF ISO 21434

The ISO/SAE 21434 standard, which was first published in August 2021, is part of a global effort to create a unified approach to automotive and smart mobility cyber threats. It includes continuous monitoring, risk assessments, and response measures on all electrical and electronic systems and their vehicle components and interfaces, to ensure that vehicles remain secure even as new threats emerge. ISO/SAE 21434 builds on the ISO 26262 Road Vehicles - Functional Safety standard, covering the entire product lifecycle, including the concept phase, operating phase, maintenance phase, and ultimately decommissioning and the end of cyber security support. It provides OEMs and their suppliers with a comprehensive process for calculating asset risk, including RF communication threats, such as jamming, spoofing, and unauthorised access and recommends methods for calculating scores and prioritising vulnerability urgency. Despite its broad acceptance, industry stakeholders have highlighted several challenges to the existing version:

- **High Level of Abstraction:** The standard is often criticised for its abstract language, which can make practical implementation difficult for organisations seeking clear and actionable guidance.
- **Lack of Concrete Application Support:** Many users report a need for more detailed examples, tools, and templates to help translate the standard's requirements into specific processes and deliverables.
- **Rapid Technological Change:** The automotive landscape is evolving rapidly, with new connectivity features, software-defined architectures, and autonomous capabilities introducing novel cyber security risks that were not fully addressed in the first edition.

"The R155/R156 regulations, in force across the EU since July 2022, are now fully applicable to all vehicles produced from July 2024 onwards. The deadline for compliance with R156 for special purpose or small-series vehicles remains July 2026. Japan and South Korea have also aligned with these frameworks and are progressing along similar implementation timelines.

A second edition of the standard is expected to be published towards the end of this decade, possibly as early as 2028. Participating organisations have already started collecting feedback at a higher level of application. Even though the specifics of the updated version have not been discussed or released, market experts point to more weight being given to cyber security assessment issues, and those in out-of-context and off-the-shelf scenarios. According to John Krzeszewski, a Cyber Security & Functional Safety Senior Engineering Specialist at U.S.-based power company Eaton Corporation, the second edition will consider the inclusion of Agile methodologies and provide updates to the threat analysis and risk assessment (TARA) section, as current flexibility in attack feasibility ratings has led to inconsistencies. Eventually, the ISO/SAE 21434 is expected to become a management system standard corresponding to the ISO MSS structure.

TABLE 1: ISO/SAE 21434: CHANGES EXPECTED IN NEXT EDITION

ASPECTS	FIRST EDITION (2021)	EXPECTED IN NEXT EDITION (2028)
Practical Guidance	Limited	Enhanced with examples, tools
Technology Coverage	Basic connectivity	Advanced CV/SDV, AI, V2X, OTA
Industry Collaboration	Moderate	Increased engagement
Alignment with Other Standards	Partial	Stronger integration

Source: CYEQT Knowledge Base (2024), Parasoft (2025)

CHINESE CYBER SECURITY REGULATION GB 44495

In August 2024, China released GB 44495, a new standard in vehicle cyber security that incorporates elements of international standards such as UN Regulation No. 155 and ISO/SAE 21434:2021 but is tailored to the Chinese market. The standard applies to M (passenger), N (commercial), and O (trailers, including semi-trailers) vehicle types equipped with at least one electronic control unit (ECU). It sets out specific requirements for data protection, threat detection, and incident response. Key objectives of this regulations are:

- **Setting Mandatory Requirements:** Unlike voluntary international standards, GBg44495 is mandatory for all vehicles sold in China, ensuring a high level of compliance across the industry.
- **Aligning with Global Standards:** The regulation incorporates elements from UN Regulation No. 155 and ISO/SAE 21434, but tailors requirements to the Chinese market and regulatory environment.
- **Promoting Technological Sovereignty:** GB 44495 is part of China's strategy to assert greater control over technology standards and reduce reliance on foreign frameworks.

By January 2028, the regulation will become mandatory for all vehicle types. The primary areas of focus include:

- **Cyber security Management System (CSMS):** To ensure that automotive companies have the required capabilities in place to tackle cyber security risks across the entire vehicle lifecycle, from design to decommissioning. Each company must undertake a re-audit every three years to ensure that cyber security measures and processes are up to date.
- **Technical Requirements:** Lists a set of 27 tests to assess if a vehicle meets the required cyber security standards. These include external connection security, communication systems, software updates, data security, access control, Denial-of-Service (DoS) protection, network entry protection, malware detection, anomaly detection, cryptographic key management, end-of-life security, and DoS protection, among others.

TABLE 2: GB 44495 VS. INTERNATIONAL STANDARDS

Feature	GB 44495	UN R155	ISO/SAE 21434
Mandatory	Yes	Varies by region	Voluntary
Specific Test Cases	27 mandatory tests	Risk-based, no fixed tests	Risk-based, no fixed tests
Data Protection	Strict, local focus	General	General
Audit Frequency	Every 3 years	Not specified	Not specified

Source: CYEQT Knowledge Base (2024)

ISO/SAE CD PAS 8475 ROAD VEHICLES

ISO/SAE CD PAS 8475 is an under development new standard focused on Cyber Security Assurance Levels (CAL) and Targeted Attack Feasibility (TAF) for road vehicles. This standard is designed to complement ISO/SAE 21434 by providing a more granular approach to assessing and communicating cyber security risks. Its primary objective is to:

- **Define Cyber Security Assurance Levels (CAL):** These levels provide a structured way to assess the robustness of cyber security measures implemented in vehicles, helping stakeholders understand the degree of protection against cyber threats.
- **Assess Targeted Attack Feasibility (TAF):** TAF evaluates the likelihood of an attack being successfully executed against a vehicle system, considering the attacker's resources, motivation, and technical capabilities.
- **Support Risk-Based Decision Making:** By providing clear metrics for cyber security assurance and attack feasibility, the standard enables OEMs, suppliers, and regulators to make informed decisions about risk acceptance and mitigation.

Key Features and Benefits

- **Standardised Assurance Levels:** CAL provides a common language for communicating cyber security maturity, facilitating collaboration and benchmarking across the industry. There are typically four CAL levels (CAL1 to CAL4), with each increment corresponding to a higher assurance requirement.
- **Targeted Attack Feasibility Assessment:** TAF helps organisations prioritise security investments by identifying the most likely and impactful attack scenarios.

- **Integration with Existing Standards:** ISO/SAE CD PAS 8475 is designed to work alongside ISO/SAE 21434, providing additional detail and guidance for risk assessment and management.

Key Takeaways for OEMs and Suppliers

- **Monitor Standard Development:** Stay informed about the progress of ISO/SAE CD PAS 8475 and prepare for its adoption.
- **Integrate with Existing Processes:** Ensure that CAL and TAF assessments are integrated into existing cyber security management systems and risk assessment processes.
- **Leverage for Competitive Advantage:** Use CAL and TAF to demonstrate cyber security maturity and differentiate products in the market.

"ISO/SAE CD PAS 8475 is an under development new standard focused on Cyber Security Assurance Levels (CAL) and Targeted Attack Feasibility (TAF) for road vehicles. This standard is designed to complement ISO/SAE 21434 by providing a more granular approach to assessing and communicating cyber security risks."

Development Status and Timeline

The ISO/SAE CD PAS 8475 is currently under development, with the comment period recently closed. The standard is being developed by ISO/TC 22/SC 32 - the same technical committee responsible for ISO/SAE 21434. The first edition is expected to be published over the next couple of years with updates reflecting evolving threats and technologies.

CYBER RESILIENCE ACT (CRA)

The Cyber Resilience Act (CRA) was introduced in the European Parliament in 2022 and implemented in October 2024. It establishes mandatory cyber security requirements for hardware and software products throughout their whole lifecycle. Manufacturers will have to offer compliant products in the European market by 2027. Article 3(2) of the act covers all products in the market with digital elements that can be connected to a device or a network, including their building blocks (i.e., hardware and software), and solutions provided in Software as a Service (SaaS) mode, if they qualify as remote data processing solution.

For the automotive industry, products already regulated by sector-specific regulations such as Regulation (EU) 2019/2144 – also known as the General Safety Regulation (GSR)- are not covered by the CRA. However, automotive components with digital elements, particularly those produced by suppliers not regulated under GSR, fall under the CRA. These include electronic control units (ECUs) – telematics and infotainment systems (e.g. retrofit solutions); aftermarket components with internet access (e.g. diagnostic devices, dongles); firmware and software; connected charging infrastructure (V2G communication); cloud and back-end components that communicate with vehicle functions via APIs; and non-road vehicles, such as agricultural machinery, construction equipment and industrial transport vehicles.

"The Cyber Resilience Act (CRA) was introduced in the European Parliament in 2022 and implemented in October 2024. It establishes mandatory cyber security requirements for hardware and software products, throughout their whole lifecycle. Manufacturers will have to offer compliant products in the European market by 2027."

OEMs will incur additional costs to meet compliance requirements under the CRA regulation. The requirement to provide continuous monitoring and free security updates over a product's usage will result in the deployment of vulnerability management programs, incident reporting systems, and dedicated personnel, all of which will warrant additional expenditure. Also, offering free security updates for a certain length of time can lead to extended product support timelines and associated costs. Finally, in case of non-compliance, OEMs will be liable to pay substantial fines up to EUR15 million or 2.5% of global annual turnover. Interestingly, the impact of the CRA extends to OEMs and their partners located outside the EU, if they sell vehicles in the region. This includes authorised representatives, resellers, and distributors, all of whom will need to implement processes to comply with the regulations.

Manufacturers and suppliers of automotive components must comply with the guidelines mentioned below.

1. **Standard and Regulation Compliance:** Automotive manufacturers must comply with not only existing regulations like UNR-155 and GSR but also follow standards like ISO/SAE 21434 when it comes to vehicle architecture and connected platforms.
2. **Secure OTA Updates:** Manufacturers must ensure that their Over-the-Air (OTA) capabilities are secure and efficient, and vulnerabilities are patched in real-time.
3. **Regular Testing:** Manufacturers must conduct regular testing of the current architecture for vulnerabilities to analyse where mitigation is needed.
4. **V2X Security and Security Credential Management Systems (SCMS):** while an SCMS is not mandatory under the CRA, it is beneficial for manufacturers in terms of security best practices.

EUROPEAN PRODUCT LIABILITY ACT

The revised EU Product Liability Directive 2024/2853 was adopted on the 23rd of October 2024, replacing the 40-year-old Product Liability Directive 85/374/EEC. Relevant to all companies selling products in the EU market, the new directive aims to update the product liability rules to include the latest technologies, the circular economy, new business models, and globalisation of supply chains. It is also designed to make the process of seeking compensation for

"The revised EU Product Liability Directive 2024/2853 was adopted on the 23rd of October 2024, replacing the 40-year-old Product Liability Directive 85/374/EEC. Relevant to all companies selling products in the EU market, the new directive aims to update the product liability rules to include the latest technologies, and globalisation of supply chains."

defective products easier. Some of the amendments in the revised version include:

1. The definition of a 'product' now includes embedded and standalone software and AI-powered products, including those related to digital health.
2. Liability for manufacturers extends to damage resulting from missing or inadequate software updates or weak cyber security protection of products.
3. Allows claimants to sue for wider damage, including destruction or corruption of data. Also removes the current deductibles and maximum liability limits.
4. New liability risks for authorised representatives of the manufacturer, software developers, fulfilment service providers (i.e. storage, packaging and shipping service providers), distributors and online marketplaces operators.
5. Strict liability for companies that 'substantially modify' a product (regardless of fault).

From an automotive industry standpoint, the new directive's expansion of the term 'product' means that software updates and AI-supported systems in vehicles are also covered under product liability. Specifically, it considers cyber security errors to be potential product defects, which makes it even more pertinent in light of the increasing connectivity and autonomisation of vehicles. Additionally, according to the amendments mentioned above, the liability will not only be limited to manufacturers of automobiles but also extend to importers, fulfilment service providers, and retailers. All of these changes, along with the removal of maximum liability limits and retroactive liability for software updates, present big challenges for vehicle and car manufacturers and their suppliers.

While the revised PLA broadens liability, it also includes certain exclusions and limitations:

- **State of the Knowledge:** Manufacturers may not be held liable if they can demonstrate that the state of scientific and technical knowledge at the time of production did not allow for the detection of the defect.
- **Third-Party Modifications:** Liability may be limited if the defect was caused by unauthorised modifications or misuse by the user or third parties.
- **Statute of Limitations:** Claims must be brought within a specified period after the defect becomes known.

EU DATA ACT

The EU Data Act, adopted in 2023 and expected to be fully applicable by the end of 2025, introduces new rules for data sharing, accessibility, and security in the digital economy. For the automotive industry, the Data Act has significant implications, particularly as vehicles generate and process vast amounts of data.

Key Provisions of the EU Data Act

- **Data Accessibility:** The Data Act grants users (e.g., vehicle owners, fleet operators) the right to access data generated by their products, including connected vehicles.
- **Data Sharing:** Manufacturers may be required to share certain data with third parties, such as service providers, repair shops, and insurers, under specified conditions.
- **Data Security:** The act imposes strict requirements for the protection of personal and non-personal data, including encryption, access controls, and incident response measures.
- **Interoperability:** The Data Act promotes interoperability and standardised data formats to facilitate data sharing and reuse.

Implications For The Automotive Industry

The EU Data Act requires OEMs to enhance data transparency, implement robust cyber security measures, and adapt to data-driven business models such as predictive maintenance and usage-based insurance. Compliance poses challenges, requiring major updates to IT systems, processes, and contracts to meet regulatory standards and ensure user control over vehicle-generated data.

Strategies for Managing Data Accessibility, Security, and Compliance

The best strategy for OEMs is to adopt robust data governance frameworks, strengthen cyber security with encryption and monitoring, and create user-friendly data portals. They should also establish secure third-party data-sharing protocols and continuously monitor regulatory changes to maintain compliance with evolving Data Act requirements.

- **Implement Data Governance Frameworks:** Establish clear policies and procedures for data collection, storage, sharing, and deletion.
- **Enhance Cyber Security Controls:** Deploy advanced encryption, access controls, and monitoring tools to protect vehicle data.
- **Develop User-Centric Data Portals:** Provide users with secure, user-friendly interfaces for accessing and managing their data.
- **Engage with Third Parties:** Establish contractual and technical frameworks for secure data sharing with authorised third parties.
- **Monitor Regulatory Developments:** Stay informed about updates to the Data Act and related regulations to ensure ongoing compliance.

The EU Data Act, adopted in 2023 and expected to be fully applicable by the end of 2025, introduces new rules for data sharing, accessibility, and security in the digital economy. For the automotive industry, the Data Act has significant implications, particularly as vehicles generate and process vast amounts of data.

SECURING SECURITY FOR FUTURE VEHICLES

Solutions to Secure and Improve the Safety of Automated Driving and Advanced Driver Assistance Systems

Advanced Sensors:
Advanced driver assistance systems (ADAS) sensors such as LiDAR (Light Detection and Ranging) sensors, 360° camera systems and computer vision-powered tools, and radar sensors, contain ultramodern microprocessors and data processing technologies. They allow vehicles to process information on their surrounding environments at sub-second speeds using AI and ML algorithms. Examples of AI/ML in ADAS include deep learning algorithms for object recognition and predictive analytics to study drivers' behaviours.

Multi-Sensor Fusion and High-Resolution Sensing Layer:
The latest architectures in autonomous vehicles are equipped with AI-powered sensor fusion algorithms that dynamically adjust to changing road conditions, noise reduction and inaccuracies in real-time. A good example is Tesla's full self-driving (FSD) architecture which can process multiple video frames from integrated cameras, using networks that allow the system to estimate object trajectories. By fusing data derived from radars and onboard cameras, the FSD architecture minimises reliance on LiDAR.

High-Performance Computing (HPC):
Most OEMs producing autonomous vehicles use HPC units that contain GPUs, TPUs, or dedicated AI processors optimised for deep learning tasks, such as quick processing of sensor data and execution of driving algorithms. A good example is Nvidia's DRIVE AGX platform that is integrated in many autonomous vehicles due to its ability to effectively handle complex tasks such as perception, mapping, and path planning.

Adaptive Cruise Control (ACC):
The two main types of ACC technologies, radar-based and laser-based ACC systems, use sensors to maintain a safe distance between vehicles and surrounding objects.

Lane Departure Warning (LDW) and Lane Keep Assist (LKA):
LDW systems provide early warnings in the form of vibrations, dashboard visuals, or audio to indicate that a vehicle is about to cross over lane markings. On the other hand, LKA systems provide steering support to enable drivers to keep their vehicles within the lane.

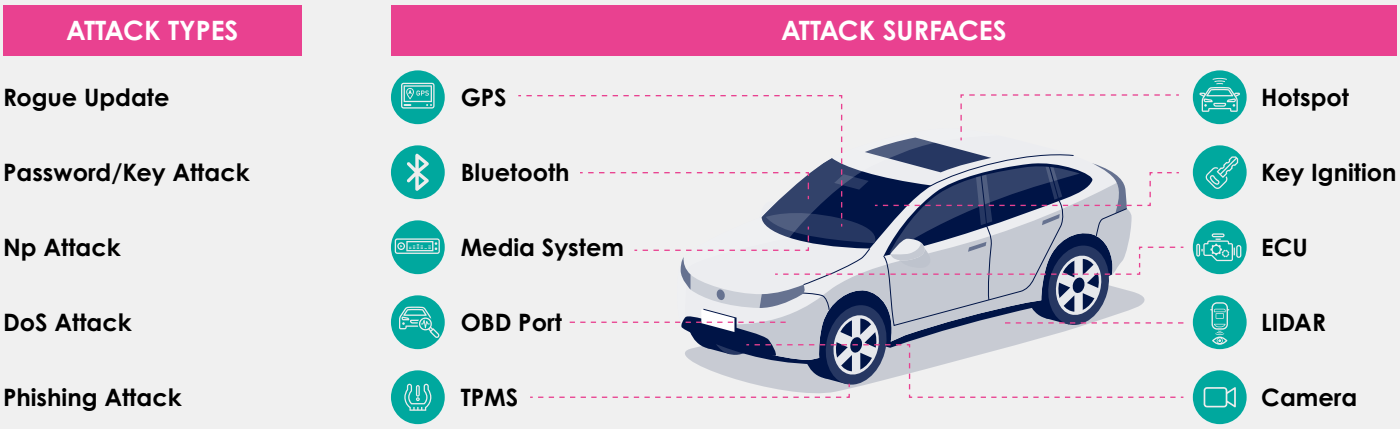
Autonomous Emergency Braking (AEB):
AEB technology uses forward-facing cameras and other sensors to inform the vehicle about an imminent crash, resulting in the automatic application of the brakes. According to a late 2024 study by the AAA automotive group, new 2024 model vehicles with AEB systems avoided 100% of forward collisions when tested at speeds up to 35 mph, in comparison to old (2017 – 2018) model vehicles, which only avoided collisions 51% of the time.

Blind Spot Detection (BSD): BSD systems leverage quasi-millimetre wave radar-based systems, ultrasonic sensors and cameras, that operate in tandem with blind spot monitors to transmit visual information of objects in blind spots to the driver's dashboard. They can also deliver warnings and alerts in the form of alarms or vibrations. Different types of neural networks and unsupervised learning algorithms are trained to recognise patterns in the sensor data and recognise accidental hazards.

CYBER SECURITY BY DESIGN: SECURING FUTURE-READY VEHICLES FROM THE GROUND UP

While all industries today grapple with cyber security risks, the stakes are particularly high in the automotive sector due to the potential impact on the safety and well-being of drivers, passengers, and the wider community. Moreover, innovations such as zonal computing, digital twins, and software-based feature monetisation, have heightened architectural risk.

FIGURE 2: ATTACK TYPES AND SURFACES



Source: Broadcom

For example, while zonal computing streamlines design, it also increases the attack surface through more entry points. The profound implications for human safety and novel architectural risks are driving the adoption of embedded security or security-by-design measures across the lifecycle of a vehicle, including design, partnerships, validation, and real-time defence. Without embedded security from the ground up, SDVs remain vulnerable to backdoor exploits, firmware poisoning, and OTA hijacks.

Security-by-design measures include the development of components and the associated software code (firmware) with adequate built-in security features such as robust electronic control unit (ECU) identity management, secure boot processes and communication channels, strong critical vehicle keys, and secure OTA update capabilities. Others include intrusion detection, secure diagnostics, and secure logging capabilities that enable the vehicle to continuously and automatically monitor and safeguard its vital systems.

Security-by-design measures include the development of components and the associated software code (firmware) with adequate built-in security features such as robust electronic control unit (ECU) identity management, secure boot processes and communication channels, strong critical vehicle keys and secure OTA update capabilities.

It is also equally important to extend the robust cyber security measures beyond just the physical vehicle to restrict the entry of exploit chains that are beyond OEM visibility. This includes cloud-based infrastructure that hosts vehicle services such as telematics, infotainment, OTA updates, web and mobile apps; network connectivity between the vehicle and hosting infrastructure; and the supplier ecosystem.

Additionally, considering the longer operational life of SDVs, manufacturers and other stakeholders must look beyond the existing and near-term threat landscape and consider future threats. Vehicles must be designed with built-in mechanisms for future updates that can effectively mitigate new threats. A good example is protection against quantum computing-based attacks that could emerge over the short to medium term. National Institute of Standards and Technology (NIST) standards have already started including quantum-safe algorithms in their scope, making it imperative for OEMs to adopt them in their development lifecycle.

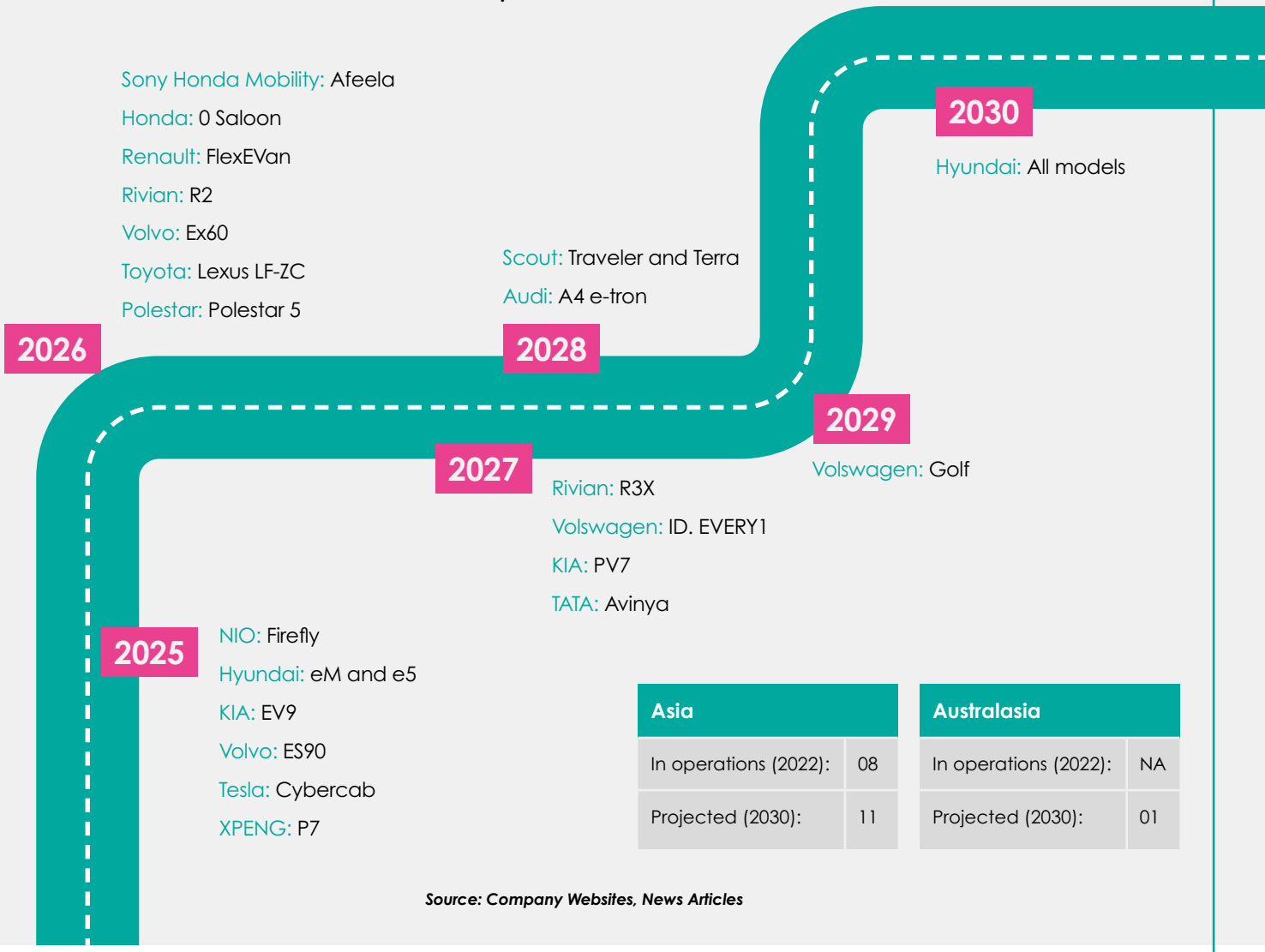
The last few years have witnessed the emergence of various standards and certifications that support security-by-design. One is the AUTOSAR standards, which have created a standardised software architecture for automotive ECUs and a common framework for software development to improve collaboration between OEMs and suppliers. Another is the Portable Operating System Interface (POSIX) that supports the development of secure vehicle software architectures for real-time operating systems, SDVs, and ECUs.

SDV ARCHITECTURE

SDV ARCHITECTURE

Year-end roundup of the SDV landscape, including a roadmap for 2026 and beyond.

FIGURE 3: SDV RELEASE ROADMAP, 2025-2030



Asia	
In operations (2022):	08
Projected (2030):	11

Australasia	
In operations (2022):	NA
Projected (2030):	01

Source: Company Websites, News Articles

TABLE 3: LIST OF SOFTWARE-DEFINED VEHICLES (SDVS)

Manufacturer	Model	Launch Year	Region availability	Tech specification
NIO	Firefly	2025	Asia and Europe	Over-the-Air & ADAS
Hyundai	eM and eS	2025	European and North American	Integrated Modular Architecture
Kia	EV9	2025	Europe	Over-the-Air
Volvo	ES90	2025	Europe	Superset tech stack, NVIDIA DRIVE AGX Orin, SPA2 platform
Tesla	Cybercab	2025	North America	Camera-only, Full Self-Driving system
Xpeng	P7	2025	China	Smart Electric Platform Architecture 2.0
Sony Honda Mobility	Afeela 1	2026	North America, Asia, and Europe	Liftback, Level 3 ADAS, Over-the-Air
Honda	0 Saloon	2026	North America	AI/ADAS
Renault	FlexEVan	2026	Europe	Ampere SDV
Rivian	R2	2026	Europe	Zonal SDV architecture, Over-the-Air support
Volvo	EX60	2026	Global	Superset tech stack, NVIDIA DRIVE AGX Orin, SPA3 platform
Toyota	Lexus LF-ZC	2026	Global	Arene OS interactive reality experience platform
Polestar	Polestar 5	2026	Asia and Europe	FlyMe OS, Geely's new SEA platform
Rivian	R3X	2027	Europe	Over-the-Air
Volkswagen	ID. Every1	2027	Europe	Zonal architecture; Over-the-Air; affordable AI
Kia	PV7	2027	Global	AI-based mobility platform
Tata	Avinya	2027	Asia	Software over the air
Scout Motors	Traveler, and Terra	2028	North America	Zonal software architecture, and Over-the-Air
Volkswagen	Audi A4 e-tron	2028	Europe	Scalable Systems Platform, and Over-the-Air
Volkswagen	Golf	2029	Europe	Scalable Systems Platform, and Over-the-Air
Hyundai	All Models	2030	Global	Over-the-Air and ADAS

Source: Company Websites, News Articles

FROM DOMAIN-CENTRIC TO ZONAL-CENTRIC ARCHITECTURES

The domain architecture approach in an SDV involves each functional element, such as the powertrain, safety systems, or infotainment systems, having its own domain controller connected from the power source to the electronic control unit (ECU). Vehicles with domain architectures typically have anywhere between 100 to 150 ECUs, each requiring its own dedicated wiring network. Even though this approach worked well for many years, the increasing complexity of SDVs is now causing convoluted wiring, undesirable performance, and scaling limitations.

These limitations are driving the shift towards zonal architecture, which involves the decentralisation of electric controllers to various hardware gateways located at different points throughout the vehicle. Since devices of various functions are strategically attached to the closest gateway or zonal controller, the wiring lengths are significantly shortened, and power transmission and software stacks are simplified.

TABLE 4: ZONAL VS. DOMAIN ARCHITECTURE: KEY DIFFERENCES

Feature	Domain-Based	Zonal
Structure	Function-oriented (e.g., infotainment, powertrain)	Location-oriented (e.g., front-left, rear-right)
ECU Distribution	Central ECUs per domain	Local ECUs per zone
Wiring	Point-to-point, extensive harnessing	Simplified with backbone Ethernet
Software Deployment	Distributed across ECUs	Centralised, abstracted from hardware
Scalability	Low, tight coupling between hardware & software	High, modular zones and central intelligence

Source: Promwad

The zonal architecture is a centralised architecture equipped with a powerful central CPU on which the software stack runs. This makes it easier for OEMs to update software by having all the functions on a SOAFEE (sustainable open architecture for embedded edge). According to McKinsey estimates, by 2030, the global share of vehicles with zonal architecture is estimated to reach around 18% and will continue to grow. Other benefits include:

- **Reduced weight:** Another benefit of adopting zonal architecture is a significant reduction in vehicle weight, which is detrimental to efficiency and performance. A good example is Tesla, which has reduced the cabling length for its Model 3 from 3 km to 1.5 km due to zonal architectures, resulting in an 85% drop in overall harness weight.
- **Secure OTA Updates:** The large number of ECUs used in domain architectures caused bottlenecks and complexity in OTA updates, leading to challenges from a safety, reliability, and regulatory compliance standpoint. However, zonal architectures not only mitigate these issues but also facilitate rollbacks when updates fail.
- **Hardware and Software Decoupling:** The adoption of zonal architectures results in the decoupling of both vehicle hardware and software, thus speeding up development times, enabling faster reengineering and adaptation, and boosting innovation.
- **Increased Data and Power Reliability:** In conventional architectures, vehicle systems are often heavily dependent on the operational environment, with connectors particularly vulnerable to the frequent shocks and vibrations inherent in daily vehicle use. In fact, the centralised layout of domain architecture makes the vehicle prone to comprehensive failure, where one malfunction can overwhelm the entire electrical network. However, zonal systems are integrated with fail-safe protocols to isolate malfunctions.
- **Support for 48-Volt Systems:** Zonal architecture also supports the current transition in the automotive industry from traditional 12-volt (V) systems to 48-V ones. 48-V systems allow for more power efficiency, less vehicle weight, and cost savings. In fact, it requires only 25% of the power needed to deliver the same power as a 12-V system, resulting in significant cost and weight savings.

FUTURE OF ZONAL ARCHITECTURES

According to Prashant Gulati, CEO of vehicle software marketplace SDVerse, "The promise of SDVs, a multi-trillion-dollar opportunity, can only be unlocked by moving over to zonal architectures." SDV OEMs are gradually transitioning from traditional distributed to advanced zonal architectures, with McKinsey estimating vehicles with zonal control modules to match those without by 2030.

Tesla is the global leader in zonal architecture, with 2023 research by S&P Global pegging the company to be at least five years ahead of its competition. This is one of the main reasons why it can build vehicles like the Model 3 in 10 hours, compared to its peers, who need around 20 hours for a similar outcome. Moreover, its proprietary zonal architecture technology has already resulted in savings of 50% in wiring, simplifying manufacturing, and lowering vehicle weight.

"Tesla is the global leader in zonal architecture with 2023 research by S&P Global pegging the company to be at least five years ahead of its competition. This is one of the main reasons why it can build vehicles like the Model 3 in 10 hours compared to its peers who need around 20 hours for a similar outcome."

In April 2024, Volkswagen announced a partnership with Chinese EV company XPeng Motors to develop a new zonal architecture called China Electrical Architecture (CEA) for its SDVs. The company plans to use it in locally developed VW-branded EVs from 2026. This is mainly to achieve a cost reduction target of 40% compared to its German-developed MEB platform, by reducing the number of control units.

FIGURE 4: SDV READINESS LEVELS: FOUNDATION TECHNOLOGIES

VEHICLE SDV READINESS LEVEL	Level 0 Not Connected	Level 1 Connected	Level 2 Basic Upgrades	Level 3 Efficient Upgrades	Level 4 Dynamic Upgrades	Level 5 Full Sdv
VEHICLE CAPABILITIES	Static features	Can update maps over the air	Can update, debug, and upgrade infotainment and ADAS, or powertrain	Can upgrade multiple domains efficiently in the same OTA update	OTA updates across 3+ domains, dynamic compute power and memory allocation, and 24/7 cyber security updates	Real-time updates and dynamic resource allocation across 4+ domains, ensuring future-proof adaptability to new hardware configurations

FOUNDATION TECHNOLOGY

OTA	Over-the-air (OTA)	No OTA	Basic OTA	Intermediate OTA	Full OTA	
SOFTWARE	Software architecture type	Signal type		Mix signal-service		Full service-oriented
SOFTWARE	Cyber security	Basic cyber security		Fully embedded cyber security	Fully embedded + cloud cyber security	
SOFTWARE	Unified Auto OS	Individual operating systems			Partially unified OS	Fully unified OS
HARDWARE	E/E architecture	Distributed or Domain		Basic Zonal		Advanced Zonal
HARDWARE	Backbone BUS	CAN				Ethernet

Source: S&P Global Mobility

CUSTOMER PERCEPTION: ASSESSING WHETHER CONSUMERS ARE WILLING TO PAY FOR SDVS

Deloitte estimates the global market for SDVs to be valued between US$400 billion and US$600 billion by 2030, with the category representing the vast majority of vehicles sold. A 2025 study by market intelligence firm IDTechEx estimates the market to grow to over US$700 billion by 2034, accounting for as much as 20% of the global car market. Yet another recent study by McKinsey involving over 1,600 automotive customers in China, Germany, and the U.S. found that over 90% of vehicles sold in 2030 will be connected, up from 50% today.

These numbers suggest not only a growing demand for SDVs but also increasing customer willingness to pay a premium for features such as autonomous driving, software-boosted performance, and enhanced infotainment, along with comfort features such as intelligent in-car ambiance and customisable interiors. According to a 2024 McKinsey study, 40-60% of the customers displayed a high willingness to pay a considerable premium for features such as autonomous driving, enhanced performance, infotainment, and comfort, in that order.

Moreover, a 2024 study by Cubic[3], a provider of SDV solutions, found that customer willingness to pay for in-car digital subscriptions is also likely to increase over the short to medium term. 25% of the consumers surveyed were already paying for digital services, with the number almost doubling (44%) for those in the 18-24 age bracket. On the other hand, only 20% of the consumers globally said that they wouldn't pay for monthly subscriptions for these services.

However, it is interesting to note that consumers are not willing to pay extra for all the features being offered by automotive companies. A good example is BMW's introduction of subscriptions for heated seat functionality and Apple CarPlay, both of which were met by a swift backlash from consumers, as they felt they were paying for services that were previously available free of charge.

It is also important to note that the market for SDVs is expected to grow significantly despite the higher manufacturing costs as compared to traditional vehicles. This is mainly due to investments in hiring specialised talent with expertise in various aspects of software development, from system architecture to coding and testing. Moreover, the costs associated with regular training and development to keep up with the latest technological advancements in AI, ML, edge computing, and connectivity are often significant. In fact, according to the 2024 Deloitte Global Survey, over 40% of automotive manufacturers spent more than US$1 billion on software development in 2023, with some investing over US$2.5 billion.

A study by McKinsey involving over 1,600 automotive customers in China, Germany, and the U.S. found that over 90% of vehicles sold in 2030 will be connected, up from 50% today. These numbers suggest not only a growing demand for SDVs but also increasing customer willingness to pay a premium for features such as autonomous driving, software-boosted performance, and enhanced infotainment, along with comfort features such as intelligent in-car ambiance and customisable interiors.

EMERGING SECURITY FEATURES TAILORED FOR NEXT-GENERATION SDV ARCHITECTURES

Zone Control Units (ZCUs): ZCUs play a key role in reducing SDV network complexity and costs by supporting centralised architectures and the increasing separation of software and hardware. They are also critical for continuous OTA updates, improvements, and function deployment services to support SDVs. Each ZCU has advanced processing power and high-performance computing unit (HPCU) advancements in chip technology that can handle the complex computations necessary for autonomous control within their designated units. This gives them the ability to rapidly analyse data, which is crucial for real-time decision-making and rapid responses. Moreover, ZCUs act as communication gateways, provide smart power distribution, and ensure the reliable execution of x-Domain real-time vehicle functions, such as audio, external sound, parking assistance, air conditioning, and suspension.

Encryption Techniques: OEMs are adopting three main encryption techniques to secure vehicle data: symmetric encryption, asymmetric encryption, and hybrid encryption. Symmetric encryption includes the Advanced Encryption Standard (AES), mostly integrated in vehicle-to-everything (V2X) applications to secure data related to location, speed, and direction. The AES functions in modes like Cypher Block Chaining (CBC) and Counter (CTR) because they can handle higher data volumes efficiently. Asymmetric encryption techniques include algorithms such as Rivest-Shamir-Adleman (RSA) and Elliptic Curve Cryptography (ECC) that are employed for secure key exchange and digital signatures. This is particularly useful to authenticate software updates and secure communications with infrastructure and other vehicles. Hybrid systems, which are a mix of the other two, are mostly used to achieve a certain level of balance between security and performance. For example, symmetric keys encrypt the actual data, while asymmetric keys encrypt the symmetric keys themselves for transmission.

Real-Time Operating Systems (RTOS): RTOS support zonal architectures by enabling ZCUs to react immediately to sensor data and actuator control within each zone, thereby facilitating rapid and decisive actions that are critical in such a dynamic environment. They are also essential to developing modules in a vehicle that are impenetrable to a cyber-attack. This is achieved by using hardware memory protection to isolate and protect drivers, third-party software, communications, and embedded applications. An advanced and secure RTOS ensures that a breach in any vehicle component does not affect other components.

Cameras, Radars and LiDAR Systems: Cameras, radars, and LiDAR systems deliver heightened sensory perception, allowing each zone to quickly adapt to changing conditions and make informed decisions for increased safety.

Redundancy: Redundancy is built into zonal architectures from the ground up to offer safeguards against potential failures. Backup components and systems act as a safety net, ensuring continued operations even if individual parts malfunction. This prioritises passenger safety and minimises the risk.

"Real-time operating systems (RTOS) support zonal architectures by enabling ZCUs to react immediately to sensor data and actuator control within each zone, thereby facilitating rapid and decisive actions that are critical in such a dynamic environment. They are also essential to developing modules in a vehicle that are impenetrable to a cyber-attack."

HOW AUTOMOTIVE OEMS ARE MONETISING SDVS

According to estimates by BCG, the SDV market, including automotive software and electronics, is expected to quadruple from US$320 billion in 2024 to US$1.2 trillion by 2035, with revenues available to suppliers growing to about US$700 billion. Interestingly, this market growth is driving a fundamental shift in automotive business models, with OEMs now having access to diverse revenue streams. These include subscription services, software upgrades, and data monetisation, among others. Furthermore, OEMs are experimenting with various pricing strategies for their digital services and features. These include value-based, usage-based, tiered, dynamic, flat rate, freemium, and subscription pricing.

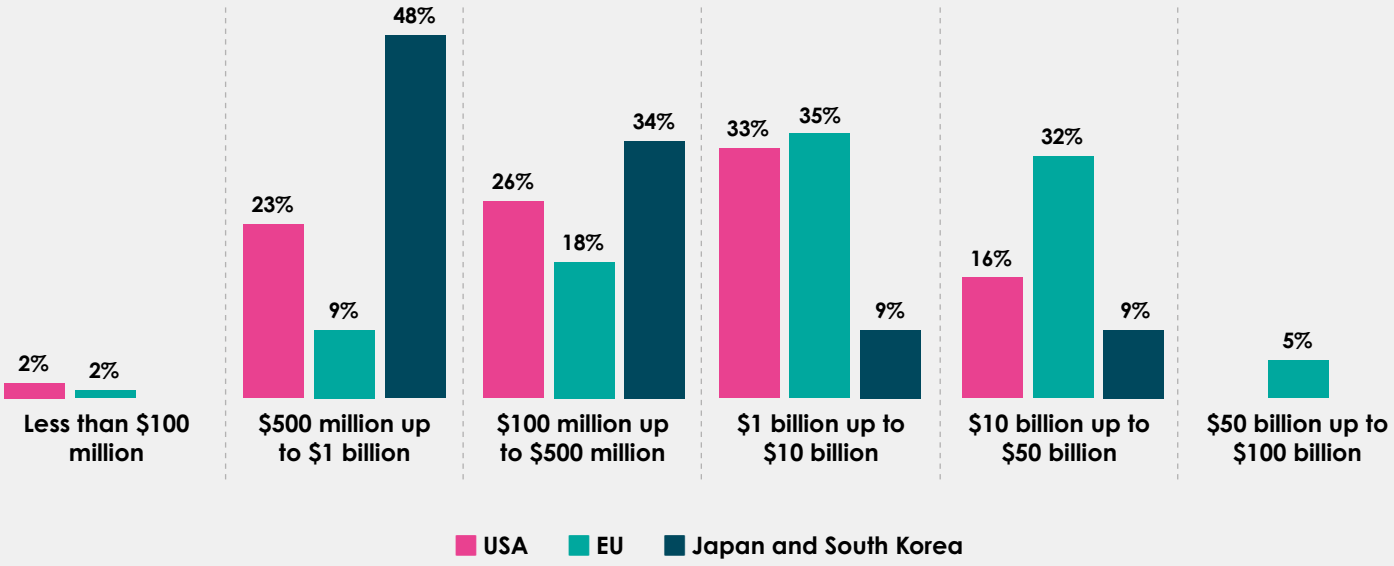
European automobile company Stellantis forecasts additional revenues of EUR20 billion from connected vehicles by 2030, while U.S.-based automakers General Motors and Ford expect US$25 billion in additional revenue each by the same year. While these targets are certainly aspirational and even optimistic, they underscore the increased attention these services are receiving, far removed from the once-niche revenue streams from Wi-Fi data plans. Monetising features such as better navigation, infotainment, and safety functions gives OEMs an opportunity to diversify their revenue streams beyond traditional vehicle sales. The key monetisation strategies being employed by SDV OEMs include:

- **Feature as a Service:** Instead of offering vehicles with a fixed set of features, OEMs now allow customers to subscribe to or purchase additional features through in-vehicle app stores. Exemplifying this model is Tesla with its OTA updates that not only offer new features such as autopilot improvements, enhanced infotainment systems, new safety systems, and advanced driver-assistance systems (ADAS), but also protection against potential cyberattacks. Another example is Ford, which offers a solution allowing fleet owners to track real-time locations, monitor fuel usage, and maintain alerts. Yet another is BMW, which offers features such as an adaptive M suspension, parking assistant, driving assistant, remote service, welcome light settings, and high beam assistant, all available through subscription. This model is fast gaining widespread acceptance, with a 2025 study by Cubic[3], a provider of SDV solutions, showing that 25% of consumers across all ages are already paying for digital services in their vehicles, a figure that almost doubles for those in the 18-24 age range.

"Instead of offering vehicles with a fixed set of features, OEMs now allow customers to subscribe to or purchase additional features through in-vehicle app stores. Exemplifying this model is Tesla with its OTA updates that not only offer new features such as autopilot improvements, enhanced infotainment systems, new safety systems, and advanced driver-assistance systems (ADAS), but also protection against potential cyberattacks."

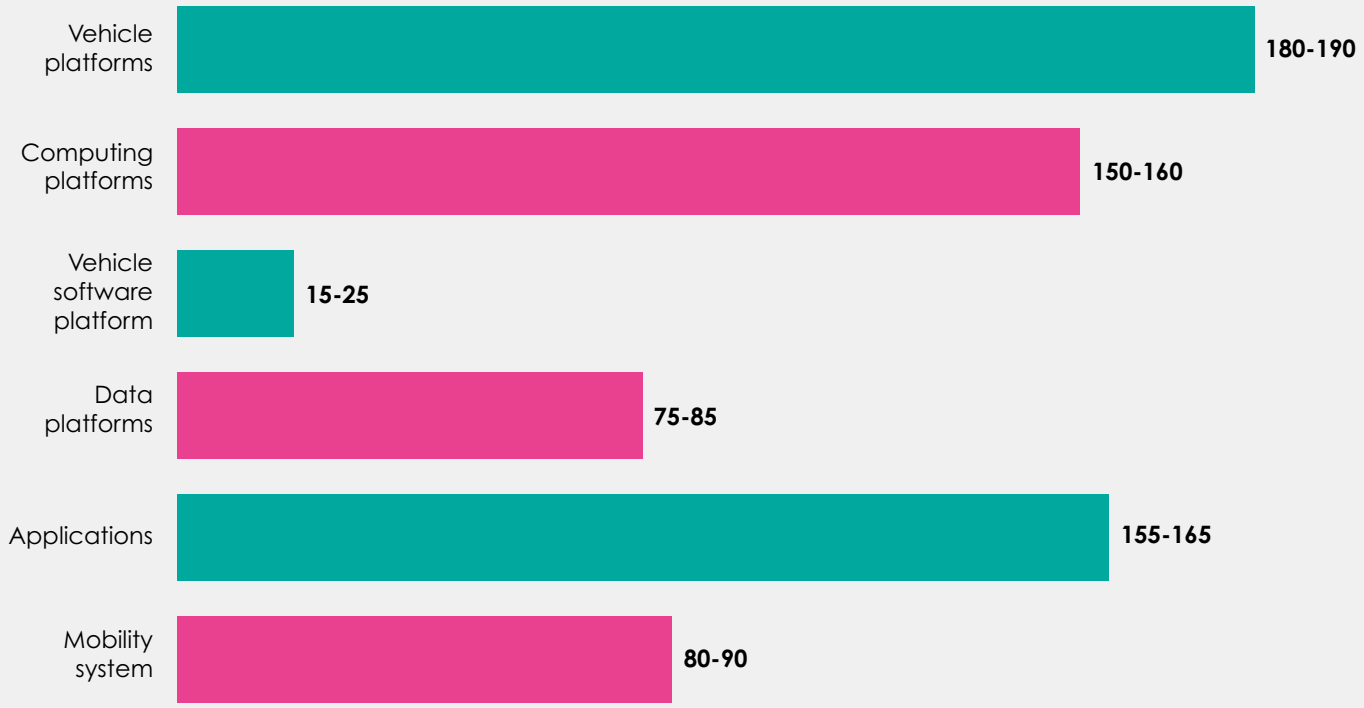
- **Services Around a Vehicle:** Another important monetisation strategy being employed by SDV OEMs is connecting data or vehicle functions to external services. These solutions include pay-per-use insurance, delivery-to-trunk services, or connecting a vehicle to home energy management to control charging. Apart from targeting only end customers beyond the initial vehicle sale, this strategy also includes partnerships with stakeholders in other industries to create an ecosystem of services around the APIs of a vehicle.
- **Data Monetisation:** Connected vehicles generate various kinds of data, such as external road and environmental conditions, the vehicle's technical status, vehicle usage, personal data and preferences, and direct communications from the vehicle. OEMs are using data analytics to offer innovative products such as intelligent route suggestions, traffic warnings, remote vehicle access for diagnosis and repair, autonomy, driving alerts and preventive actions, usage-based insurance policies, targeted advertising, and fleet management and maintenance. Another data monetisation strategy involves licensing vehicle data to third-party developers and service providers, who can use it to create innovative automotive solutions. To optimise their data monetisation strategy, OEMs will need to differentiate between creating value from data and realising that value as financial gain. A good way to do it is to package insights like targeted consumer behaviour analytics and sell them as high-value products. According to a 2024 Deloitte report, the average expected revenue for SDV OEMs from data monetisation is around US$720 million over the next five years.

FIGURE 5: PROJECTED REVENUE FROM DATA MONETISATION IN SDVS OVER THE NEXT FIVE YEARS



Source: Deloitte 2024 Global SDV Readiness Survey

FIGURE 6: SUPPLIER-ADDRESSABLE SDV MARKET IN US$ BILLIONS IN 2035



Asia	
In operations (2022):	08
Projected (2030):	11

Australasia	
In operations (2022):	NA
Projected (2030):	01

Source: BCG, Nov 2024

ACTIONABLE TAKEAWAYS AND FUTURE-LOOK

KEY TAKEAWAYS

The automotive industry is undergoing a significant transformation. As connected and SDVs become the new norm, automakers are navigating a complex web of innovation, regulation, and risk. This transformation is reshaping the market and the value proposition.

FUTURE OUTLOOK: 2026–2030

The automotive industry is racing toward a software-defined future in which vehicles evolve into digital platforms. With robust market projections and growing consumer demand for digital features, success will depend on mastering AI, cyber security, and talent acquisition.

- **Market Growth:**
  The SDV market is on a steep upward trajectory. Deloitte estimates a market size of US$400 to US$600 billion by 2030, with BCG projecting over US$1.2 trillion by 2035. AI-based cyber security alone is set to reach US$135 billion by 2030. Most global OEMs are aligning their R&D and business models with this software-first future.
- **Consumer Behaviour:**
  By 2030, over 90% of new vehicles sold will be connected. Consumers are showing a strong willingness to pay for advanced features, especially those related to autonomy, infotainment, and safety. However, poorly executed subscription models may still face backlash. The balance between innovation and perceived value will be critical for success.
- **Vehicles as Digital Platforms:**
  Vehicles are evolving into digital platforms, enabling continuous feature delivery, updates, and data-driven services. The future of automobiles is expected to be shaped more by software than by physical design changes.
- **Role of AI in All Aspects:**
  AI will influence every layer, from real-time decision-making in autonomous driving to synthetic data generation for virtual testing. It will also optimise energy use, personalisation, and anomaly detection at the edge.
- **Talent and Tools Gap:**
  With growth in demand, the competition for AI, cloud, and embedded systems talent will intensify. Upskilling, acquisitions, and partnerships will be essential to bridge the gap.

Vehicles are evolving into digital platforms, enabling continuous feature delivery, updates, and data-driven services. The future of automobiles is expected to be shaped more by software than by physical design changes.

OEM LANDSCAPE: SOFTWARE-DEFINED VEHICLE

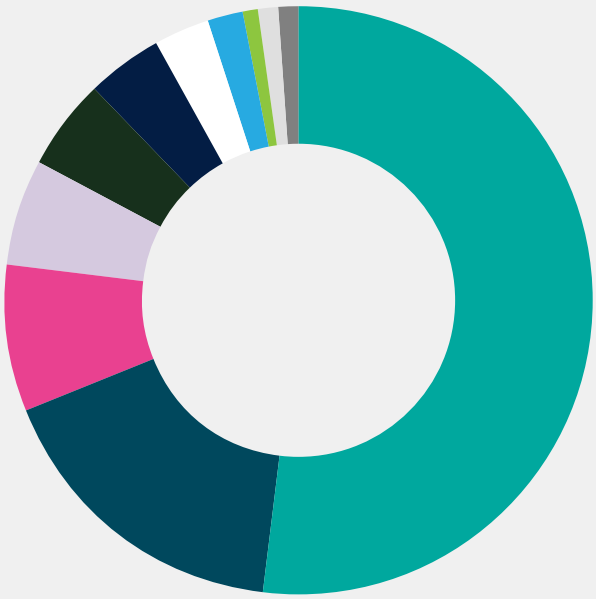
LEADING SOFTWARE-DEFINED VEHICLE OEMS

TABLE 5: LEADING OEMS: SOFTWARE-DEFINED VEHICLE

Vendors	Country	Expertise
BYD	China	Combines Nvidia-powered ADAS with DiLink smart cockpit and "God's Eye" autonomous safety system on mass-market EVs.
Li Auto	China	Pioneer in extended-range EVs with open-source Halo OS and advanced AD Max/Pro driver-assist systems.
Nio	China	Software-driven EV maker with NT 2.0 platform, "Adam" supercomputer, and advanced autonomous features.
Renault	France	Innovator in SDVs through partnerships with Google and Qualcomm, advancing OTA platforms via Ampere subsidiary.
Rivian	US	Developer of in-house Gen 2 zonal architecture and autonomous driving software delivering hands-free driving via OTA.
Stellantis	The Netherlands	Unified software leader with STLA Brain platform enabling connected, autonomous features and frequent OTA updates.
Tesla	US	Leader in fully integrated SDVs with Autopilot, Full Self-Driving, and AI-driven OTA updates.
Volvo	Sweden	Safety-focused automaker integrating Android Automotive OS and NVIDIA tech for evolving SDVs with Gemini AI assistant.
Xiaomi	China	New EV entrant leveraging proprietary HyperOS and Snapdragon chips to unify smartphone and vehicle ecosystems.
Xpeng	China	Smart EV innovator using SEPA 2.0 platform with AI-powered safety and voice assistants enhanced via OTA.
Zeekr	China	Premium EV brand using SEA platform and "Haohan" intelligent driving with continuous OTA improvements.

Source: Company Websites

FIGURE 7: LEADING OEMS BY SDV SALES MARKET SHARE 2024



Tesla Motors	52%	Other Chinese Manufacturers	5%	Geely Group	1%
BYD Auto	17%	Nio	4%	Xpeng	1%
Xiaomi	8%	SAIC Group	3%	Rivian	1%
GAC Group	6%	Other	2%		

Notes: Other Chinese Manufactures include Dayun HiPhi, Leapmotor, Li, Neta, and Seres

Source: Wards Intelligence

TESLA

Founded in 2003, Tesla is a global leader in electric vehicles and clean energy. Beyond hardware, Tesla is redefining what a car can be- turning it into a smart, software-driven machine. Its vehicles receive regular over-the-air (OTA) updates, improving performance, adding new features, and even enabling advanced driver assistance through its Autopilot and Full Self-Driving (FSD) software.

Tesla develops most of its vehicle software in-house, giving it full control over systems like battery management, infotainment, and autonomous driving. This makes Tesla one of the top companies in the software-defined vehicle space.

The company is also investing in its own AI supercomputer, Dojo, to improve its self-driving algorithms. Tesla's bold vision includes launching fully autonomous "robotaxis" by 2026, marking a shift toward cars that improve and evolve through software long after they leave the factory.

Founding year:	2003
Headquarters:	US
No of employees:	125,665 (Dec 2024)
CEO:	Elon Musk
Revenue:	US$97.7 Billion (Dec 2024)

BYD

BYD is one of China's leading electric vehicle makers, known for blending advanced software and hardware to build smart, connected cars. Their vehicles use powerful processors like Nvidia's DRIVE Orin, which support advanced driver-assistance systems (ADAS) with features such as hands-free highway driving and valet parking.

BYD's own DiLink system creates a user-friendly smart cockpit, offering voice control, navigation, and regular over-the-air (OTA) updates that keep the car's software current without needing to visit service centres. Their ADAS system, called God's Eye, is available even in entry-level models and combines cameras, radar, and sometimes Lidar sensors to deliver safety functions and autonomous driving capabilities.

Founding year:	1995
Headquarters:	China
No of employees:	968,900 (Dec 2024)
CEO:	Wang Chuanfu
Revenue:	US$106.4 Billion (Dec 2024)

NIO

Founded in 2014 by William Li, it is a leading electric vehicle company from China that focuses heavily on software-driven innovation. Its cars receive regular over-the-air (OTA) updates, which improve features like parking, navigation, entertainment, and driving controls.

Most Nio models are built on the NT 2.0 platform and run on a powerful system called "Adam," which includes four Nvidia Orin chips. This setup delivers high computing power and works with sensors like LiDAR, cameras, radar, and ultrasonic detectors to support advanced driver-assist features.

In late 2023, Nio introduced its own self-developed chip, the Shenji NX9031, designed to boost performance and efficiency, starting with its premium ET9 model. More recently, in June 2025, Nio partnered with ZF to test steer-by-wire technology, which replaces traditional steering parts with electronic controls. This allows for real-time adjustments and safety improvements through future OTA updates.

Founding year:	2014
Headquarters:	China
No of employees:	45,635 (Dec 2024)
CEO:	William Li
Revenue:	US$9 Billion (Dec 2024)

XIAOMI

Xiaomi Auto, founded in 2021 and based in Beijing, China, is a subsidiary of the tech giant Xiaomi. The company made its entry into the electric vehicle market with the launch of its first model, the Xiaomi SU7, in March 2024.

Central to Xiaomi's software-defined vehicle (SDV) approach is its own operating system, HyperOS, which unifies software across Xiaomi's smartphones, IoT devices, and cars. The SU7 features the Snapdragon 8295 in-car chip, enabling seamless integration with Xiaomi's ecosystem and supporting popular features like free-form screen mirroring, CarPlay, and Android Auto.

Beyond software, Xiaomi Auto has also invested in advanced manufacturing techniques such as Hyper Die-Casting to improve production efficiency and reduce costs.

Founding year:	2010
Headquarters:	China
No of employees:	43,688 (Dec 2024)
CEO:	Lei Jun
Revenue:	US$50.1 Billion (Dec 2024)

XPENG

Founded in 2014 and based in Guangzhou, China, is one of the leading smart EV makers. The company regularly enhances its vehicles through over-the-air (OTA) updates. Recent software versions like XOS 5.4 and 5.6 have introduced AI-powered safety features, multilingual voice assistants, smarter charging visuals, and more personalised cabin experiences.

Many of its models—such as the X9, P7+, G6, and G9—are built on the SEPA 2.0 platform and come equipped with advanced technology, including dual Nvidia Orin-X chips, LiDAR, mmWave radar, and multiple cameras. These systems support enhanced safety and autonomous driving features.

In 2024, Xpeng began expanding into Europe, supported by partnerships with companies like Volkswagen and Alibaba Cloud. Together, they are working on new vehicle platforms and digital systems, with plans to launch jointly developed EVs by 2026.

Founding year:	2014
Headquarters:	China
No of employees:	15,364 (Dec 2024)
CEO:	Xiaopeng He
Revenue:	US$5.6 Billion (Dec 2024)

RIVIAN

Rivian is an American EV company founded in 2009 and based in Irvine, California. Unlike many traditional automakers, Rivian builds most of its software and electronic systems in-house. As part of this approach, it has developed a new Gen 2 zonal architecture that reduces the number of electronic control units (ECUs) from 17 to just 7. This simplifies the vehicle's wiring, lowers cost and weight, and allows for faster, more efficient software updates.

This smart architecture powers Rivian's models like the R1T, R1S, and the upcoming R2. These vehicles are equipped with advanced hardware - high-performance computing, multiple cameras, radar, sensors, and Rivian's own self-driving software. Features such as hands-free driving (Enhanced Highway Assist) are delivered and improved through regular over-the-air (OTA) updates.

To further strengthen its software-defined vehicle strategy, Rivian formed a partnership with Volkswagen in late 2024. As part of the deal, Volkswagen is investing around US$5.8 billion to jointly develop next-generation vehicle platforms, starting with the R2 and future Volkswagen models.

Founding year:	2009
Headquarters:	US
No of employees:	14,861 (Dec 2024)
CEO:	RJ Scaringe
Revenue:	US$5.0 Billion (Dec 2024)

VOLVO

Volvo Cars, founded in 1927 and headquartered in Gothenburg, Sweden, is a well-known automaker recognized for its strong focus on safety and innovation. The company is advancing software-defined vehicles (SDVs) that continuously improve through over-the-air (OTA) updates, enhancing driver assistance, infotainment, and overall vehicle performance.

To support this, Volvo has partnered with Google to integrate the Android Automotive OS, which allows seamless app integration and regular software updates. Recently, this partnership expanded to include the Gemini AI assistant, set to deliver smarter voice control and enhanced in-car experiences starting in 2025.

In addition, Volvo works with NVIDIA to incorporate powerful onboard computing platforms that enable advanced autonomous driving features and improve vehicle safety systems.

Founding year:	1927
Headquarters:	Sweden
No of employees:	102,000 (Dec 2024)
CEO:	Martin Lundstedt
Revenue:	US$47.8 Billion (Dec 2024)

STELLANTIS

Stellantis is a major global automaker formed from the merger of PSA Group and Fiat Chrysler in 2021. The company has partnered with leading tech companies like Foxconn to develop a unified software platform called STLA Brain, which aims to centralize vehicle functions such as infotainment, navigation, and driver assistance. This platform allows frequent software updates that improve safety, comfort, and user experience.

Additionally, Stellantis has also collaborated with Qualcomm on digital cockpit technologies and powerful computing platforms that support autonomous driving and connected services.

Stellantis is accelerating its transition toward smarter, more connected electric vehicles through these efforts.

Founding year:	2010
Headquarters:	The Netherlands
No of employees:	248,243 (Dec 2024)
CEO:	Antonio Filosa
Revenue:	US$163.4 Billion (Dec 2024)

LI AUTO

Founded in 2015 by Li Xiang and headquartered in Beijing, China, it specialises in extended-range electric vehicles (EREVs) equipped with advanced smart features. A key milestone in its software-defined vehicle (SDV) journey was the development of its proprietary automotive operating system, Halo OS, which the company open-sourced in April 2025 - an industry-first move aimed at boosting performance, stability, and wider collaboration.

The company's SDV capabilities are most evident in its models, such as the L8, L9, L6, and Mega, which are equipped with its AD Max and AD Pro systems. These use high-performance Nvidia Orin-X or Thor-U chips, along with LiDAR, radar, and AI-powered Vision-Language-Action (VLA) models. Continuous over-the-air (OTA) updates enhance safety, autonomy, and user experience over time.

Founding year:	2015
Headquarters:	China
No of employees:	32,248 (Dec 2024)
CEO:	Li Xiang
Revenue:	US$19.8 Billion (Dec 2024)

ZEEKR

Launched by Geely Group in March 2021, it is a premium electric vehicle brand from China. It uses the advanced SEA (Sustainable Experience Architecture) platform, designed specifically for electric cars.

The company follows a software-first approach by regularly sending over-the-air (OTA) updates to its vehicles. These updates improve features like charging, driver assistance, navigation, entertainment, and in-cabin controls. For example, its OS 1.1 and 1.2 updates brought smarter charging, smoother driving support, and better navigation and infotainment.

Zeekr's popular models like the 001, 7X, and 007 are equipped with powerful hardware, including dual Nvidia Orin-X chips, LiDAR, radar, and cameras. These systems support Zeekr's advanced "Haohan" intelligent driving features, offering a smart and safe driving experience that gets better over time.

Founding year:	2021
Headquarters:	China
No of employees:	17,439 (Dec 2024)
CEO:	Conghui An
Revenue:	US$10.4 Billion (Dec 2024)

RENAULT

Renault Group is a leading global automaker driving innovation through advanced software and hardware integration. To boost its SDV technology, Renault has partnered with major tech companies. To give this some perspective, With Google, they are building a shared IT platform that enables smooth OTA updates and easy access to vehicle data. Their collaboration with Qualcomm involves the Snapdragon Digital Chassis, a system that centralizes vehicle controls and enhances in-car experiences. Valeo contributes by supplying key electronic components and supporting software development.

Renault's dedicated subsidiary, Ampere, plays a key role in creating SDV platforms, allowing new features to be delivered regularly via OTA updates, improving vehicle performance and user experience.

Founding year:	1898
Headquarters:	France
No of employees:	98,636 (Dec 2024)
CEO:	Luca de Meo
Revenue:	US$58.6 Billion (Dec 2024)

BIBLIOGRAPHY

1. AFP. "Cubic Research Finds Automotive OEMs View Connectivity as Crucial for Security as Half of Consumers Worry Their Car Can Be Hacked." April 29, 2025. https://www.afp.com/en/infos/cubic3-research-finds-automotive-oems-view-connectivity-crucial-security-half-consumers-worry.
2. Annabi, Malak, Zeroual, Abdelhafid and Messai, Nadhir. "Towards Zero Trust Security in Connected Vehicles: A Comprehensive Survey." Arxiv. https://arxiv.org/pdf/2504.05485.
3. Autocrypt. "Cyber Resilience Act Explained: What It Means for the Automotive Industry." April 29, 2025. https://autocrypt.io/cyber-resilience-act-explained-what-it-means-for-the-automotive-industry/.
4. Automotive World. "AI drives the future of software-defined vehicles." December 10, 2024. https://www.automotiveworld.com/articles/ai-drives-the-future-of-software-defined-vehicles/.
5. Automotive World. "SDVs require new zonal architecture ecosystems." December 12, 2024. https://www.automotiveworld.com/articles/zonal-architecture-ecosystems-deliver-the-promise-of-sdvs/.
6. Baule, Alexander, Bertoncello, Michele and Ellencweig, Ben. "Car connectivity: What consumers want and are willing to pay." Mckinsey. January 08, 2024. https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/car-connectivity-what-consumers-want-and-are-willing-to-pay#/.
7. Bezerra, Maite. "SDV Market Tracker: 2024 Analysis." Wardsauto. December 18, 2024. https://www.wardsauto.com/software-defined-vehicles/sdv-market-tracker-2024-analysis.
8. Boston Consulting Group.6r "Software-Defined Vehicles Will Create a More Than $650 Billion Value Potential for the Auto Industry by 2030." September 07, 2023. https://www.bcg.com/press/7september2023-software-defined-vehicles-create-650-billion-value-potential.
9. Burkacky, Ondrej, Deichmann, Johannes and Kellner, Martin. "Getting ready for next-generation E/E architecture with zonal compute." Mckinsey. June 14, 2023. https://www.mckinsey.com/industries/semiconductors/our-insights/getting-ready-for-next-generation-ee-architecture-with-zonal-compute.
10. Business Wire. "First Real-World Multisite Study Shows GenAI-Powered Mental Health Treatment Outperforms Standard of Care." March 10, 2025. https://www.businesswire.com/news/home/20250310848349/en/First-Real-World-Multisite-Study-Shows-GenAI-Powered-Mental-Health-Treatment-Outperforms-Standard-of-Care.
11. C R, Manoj and Kannan, Paduka. "Driving automotive software engineering 2.0 with generative AI." TATA Consultancy Services. https://www.tcs.com/what-we-do/services/iot-digital-engineering/white-paper/generative-ai-software-defined-vehicles.
12. Car Group. "IBM 'Automotive 2035' Study: Transformative Insights on AI and SDV." March 16, 2025. https://www.cargroup.org/automotive-2035/.
13. CB Insights. "State of AI Q1'25 Report." May 01, 2025. https://www.cbinsights.com/research/report/ai-trends-q1-2025/.
14. Cetin, Enver. "Agentic AI and the Future of Personalized Healthcare." Ciklum. May 19, 2025. https://www.ciklum.com/resources/blog/future-of-personalized-healthcare.
15. Continental. "New ECU Platform for Server-Zone Vehicle Architectures." https://www.continental-automotive.com/en/solutions/server-zone-architecture/zone-control-units.html.
16. Cybellum. "John Krzeszewski: What's Next for ISO/SAE 21434." https://cybellum.com/podcast/65-john-krzeszewski-safety-security-at-eaton/.
17. Dataspan. "GenAI in Manufacturing: 7 Real-World Use Cases." December 27, 2024. https://www.dataspan.ai/blog/7-use-cases-of-genai-in-manufacturing.
18. Dixon, Richard. "Can Carmakers Assail Tesla's Lead in E/E Architecture?." SP Global. February 10, 2023. https://www.spglobal.com/mobility/en/research-analysis/can-carmakers-assail-teslas-lead-in-ee-architecture.html.
19. Eur Lex. "Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on liability for defective products." September 28, 2022. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0495.
20. Funke, Janine. "EU Cyber Resilience Act: Implications for the Automotive Industry." UL. November 21, 2024. https://www.ul.com/sis/blog/eu-cyber-resilience-act-implications-automotive-industry.
21. Futureciso. "Partnership to strengthen automotive security and support EU Chips Act sovereignty goals." May 19, 2025. https://futureciso.tech/partnership-to-strengthen-automotive-security-and-support-eu-chips-act-sovereignty-goals/.
22. Garikapati, Divya. "Zonal Architectures for Future SDV Success." Mouser. May 17, 2024. https://www.mouser.com/blog/eit-2024-zonal-architectures-future-sdv-success?srsltid=AfmBOoqnSzab3YKKR9p0Eyskydd2qCjZDpl4HG0-2We971iavl8gUZyl.

23. Gnanasambandam, Chandra, Harrysson, Martin and Singh, Rikki. "How an AI-enabled software product development life cycle will fuel innovation." Mckinsey. February 10, 2025. https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/how-an-ai-enabled-software-product-development-life-cycle-will-fuel-innovation.
24. Goldberg, Jillian. "Data Monetization and the Evolution of Connected Car Technologies." Guard Knox. August 10, 2023. https://blog.guardknox.com/data-monetization-and-the-evolution-of-connected-car-technologies.
25. Hilal, Syed Sameer Bin, Chaudhary, Himanshu and Kundu, Raj Kumar. "Generative AI tools can transform educational experience." TCS. https://www.tcs.com/what-we-do/industries/education/white-paper/generative-ai-tools-transforming-education-sector.
26. Himes, Emily. "An Overview of ISO 21434 for Automotive Cyber security." PTC. December 16, 2024. https://www.ptc.com/en/blogs/alm/iso-21434-for-automotive-cyber security.
27. HIS Markit. "The Risks and Rewards of Automakers'." https://cdn.ihsmarkit.com/www/prot/pdf/1224/Risks-and-Rewards-of-SDVs.pdf.
28. Hörmann, Fabiane. "Generative artificial intelligence takes Siemens' predictive maintenance solution to the next level." Siemens. February 05, 2024. https://press.siemens.com/global/en/pressrelease/generative-artificial-intelligence-takes-siemens-predictive-maintenance-solution-next.
29. Hunnius, Jan-Peter von. "The Cyber Resilience Act (CRA) in the automotive industry: What carmakers and suppliers need to know." Cyeqt. April 04, 2025. https://www.cyeqt.com/en/cyber-resilience-act-cra-in-the-automotive-industry/.
30. InsightAce Analytic. "Software Defined Vehicle Market, Share & Trends Analysis Report, By SDV Type (Semi-SDV. SDV), E/E Architecture (Distributed, Domain Centralised, Zonal Control), Vehicle Type (Passenger Car and Light Commercial Vehicle), By Region, and Segment Forecasts, 2025-2034." April 15, 2025. https://www.insightaceanalytic.com/report/software-defined-vehicle-market/2671.
31. ISO. "ISO/SAE CD PAS 8475 Road vehicles — Cyber security Assurance Levels (CAL) and Targeted Attack Feasibility (TAF)." https://www.iso.org/standard/83187.html.
32. Juliussen, Egil. "Automotive Cyber security: More Than In-Vehicle and Cloud." EETimes. June 29, 2022. https://www.eetimes.eu/automotive-cyber security-more-than-in-vehicle-and-cloud/.
33. Kanmaz, Bugra. "Automotive Cyber security Regulations and Standards." Diconium. May 20, 2025. https://diconium.com/en/blog/automotive-cyber security-regulations-and-standards.
34. Kiefer, Christina and Herlitz, Laure. "Liability for software under the new European Product Liability Directive." Ibanet. April 30, 2025. https://www.ibanet.org/European-Product-Liability-Directive-liability-for-software.
35. Lucente, Ida. "Generative AI in Healthcare: Use Cases, Benefits, and Challenges." John Snow Labs. May 22, 2025. https://www.johnsnowlabs.com/generative-ai-healthcare/.
36. Maniar, Shweta. "How GenAI will transform life sciences in 2025." Pharma Phorum. January 07, 2025. https://pharmaphorum.com/digital/how-genai-will-transform-life-sciences-2025.
37. Martin,Carlos Pardo, Lamb, Jessica and Dahab, Amine. "Generative AI in healthcare: Current trends and future outlook." Mckinsey. March 26, 2025. https://www.mckinsey.com/industries/healthcare/our-insights/generative-ai-in-healthcare-current-trends-and-future-outlook.
38. McEvoy, Steve. "Comment: How AI is shaping automotive cyber security." The Engineer. October 03, 2024. https://www.theengineer.co.uk/content/opinion/how-ai-is-shaping-automotive-cyber security/.
39. Mender. "Lowering costs using the software-defined vehicle." March 19, 2024. https://mender.io/resources/reports-and-guides/lowering-costs-software-defined-vehicle.
40. Milvus. "What role does AI play in improving the security of autonomous vehicles?." https://milvus.io/ai-quick-reference/what-role-does-ai-play-in-improving-the-security-of-autonomous-vehicles.
41. Mohn, Tanya. "Automatic Emergency Braking Tech Gets Better, New Research Finds." Forbes. October 28, 2024. https://www.forbes.com/sites/tanyamohn/2024/10/28/automatic-emergency-braking-tech-gets-better-new-research-finds/.
42. Molex. "Zonal Architecture vs. Domain Architecture: Modular Automotive Infrastructure Face Off." https://www.molex.com/en-us/blog/zonal-architecture-vs-domain-architecture-modular-automotive-infrastructure-face-off.
43. Morgan Stanley. "AI and Cyber security: A New Era." September 11, 2024. https://www.morganstanley.com/articles/ai-cyber security-new-era.
44. Morrison, Paul. "Retail 2025: 6 Trends Re-defining the Future of Shopping." WNS. https://www.wns.com/perspectives/articles/retail-2025-6-trends-re-defining-the-future-of-shopping.
45. Mutschler, Ann. "Automotive Outlook 2025: Ecosystem Pivots Around SDV." Semiengineering. February 6, 2025. https://semiengineering.com/automotive-ecosystem-pivots-around-sdv/.
46. Mutschler, Ann. "Automotive OEMs Focus On SDVs, Zonal Architectures." Semi Engineering. November 07, 2024. https://semiengineering.com/automotive-oems-focus-on-sdvs-zonal-architectures/.
47. Neukirchner, Moritz. "SDVs create new markets for monetising software." Automotive World. October 20, 2023. https://www.automotiveworld.com/articles/sdvs-create-new-markets-for-monetising-software/.
48. Niehoff, Lena, Hilger, David and Howarth, Megan. "New Product Liability Directive 2024/2853: New product liability risks for products in the EU." Taylor Wessing. January 06, 2025. https://www.taylorwessing.com/en/insights-and-events/insights/2025/01/di-new-product-liability-directive.
49. Parasoft. "ISO/SAE 21434 Automotive Cyber security & Compliance." https://www.parasoft.com/solutions/iso-21434/.
50. Parthasarathy, Laksh and Purushothaman, Madhan Mohan. "Revolutionizing EV Batteries with AI and Quantum Technologies." TCS. https://www.tcs.com/what-we-do/industries/manufacturing/white-paper/ai-quantum-technologies-shaping-future-ev-batteries.
51. Pritsch, Elmar, Stefanis, Stavros and Walker, Lisa. "Software-defined vehicles Global manufacturer readiness study." Deloitte. https://www2.deloitte.com/content/dam/Deloitte/us/Documents/consumer-business/deloitte-2024-sdv-global-manufacturer-readiness-study.pdf.
52. Rawal, Dheeraj. "Securing the lifeblood of modern vehicles: OTA." T-Systems. February 21, 2025. https://www.t-systems.com/in/en/insights/newsroom/expert-blogs/over-the-air-automotive-security-1045062.
53. Riemer, Stiene, Coppola, Matteo and Rogg, Jürgen. "For Banks, the AI Reckoning Is Here." BCG. May, 2025. https://web-assets.bcg.com/3e/6f/9dfa63434eb7a00e1cf1cdcb3754/for-banks-the-ai-reckoning-is-here-may-2025.pdf.
54. Rinf Tech. "Advanced Driver Assistance Systems Development: Current Trends and Future Outlook." https://www.rinf.tech/advanced-driver-assistance-systems-development-current-trends-and-future-outlook/.
55. Robbins, Jacob. "Sequoia keeps the top spot in our generative AI investor rankings." Pitchbook. June 06, 2025. https://pitchbook.com/news/articles/top-generative-ai-vc-investors-list.
56. Roth, Felix. "Status quo ISO/SAE 21434: A look at the standard three years after publication." Cyeqt. July 30, 2024. https://www.cyeqt.com/en/status-quo-iso-sae-21434-a-look-at-the-standard-three-years-after-publication/.
57. Salgarkar, Rohan. "Top Companies in Software Defined Vehicle Industry." MarketsandMarkets. July 16, 2024. https://www.marketsandmarkets.com/ResearchInsight/software-defined-vehicles-market.asp.

58. Saunders, Joseph. "Building Resilient SDVs: Secure by Design in the automotive industry." Sae. March 18, 2025. https://www.sae.org/news/2025/03/secure-by-design.
59. SBD. "Securing the Software-Defined Vehicle." https://www.sbdautomotive.com/reports/securing-the-software-defined-vehicle.
60. Schädlich, Eric. "China's New Vehicle Cyber security Standard: GB 44495-2024." Dissec. September 2, 2024. https://dissec.to/general/chinas-new-vehicle-cyber security-standard-gb-44495-2024/.
61. Scheer, Steven. "Israeli firm C2A to supply cyber security platform for Daimler Trucks." Reuters. March 29, 2024. https://www.reuters.com/business/autos-transportation/israeli-firm-c2a-supply-cyber security-platform-daimler-trucks-2024-03-28/.
62. Subramanya, Ganesh. "A strategy to future-proof software-defined vehicles' cyber security." TCS. https://www.tcs.com/what-we-do/services/cyber security/white-paper/software-defined-vehicles-secure-by-design.
63. Thomas, Salice. "Generative AI And Self-Driving Vehicles: A Potential Future." Forbes. November 22, 2024. https://www.forbes.com/councils/forbesbusinessdevelopmentcouncil/2024/11/22/generative-ai-and-self-driving-vehicles-a-potential-future/.
64. Ungurean, Marius-Constantin. "Cyber security in Automotive: Current Trends, Regulations, and Future Paths." Rinf Tech. https://www.rinf.tech/cyber security-in-automotive-current-trends-regulations-future-paths/#elementor-toc__heading-anchor-6.
65. Upstream Security. "Automotive & Smart Mobility Global Cyber security Report." 2025 https://info.upstream.auto/hubfs/Security_Report/Security_Report_2025/Upstream_2025_Global_Automotive_Cyber security_Report.pdf.
66. UST. "Engineering the future of mobility." http://ust.com/en/insights/engineering-the-future-of-mobility.
67. Veronesi, Philipp. "Automotive Cyber security Trends 2025: 9 impulses for the future of vehicle security in challenging times." Cyeqt. January 08, 2025. https://www.cyeqt.com/en/automotive-cyber security-trends-2025/.
68. Veronesi, Philipp. "The new EU Product Liability Directive (2024/2853) vs Automotive Industry: Challenges and Opportunities." Cyeqt. January 28, 2025. https://www.cyeqt.com/en/new-eu-product-liability-directive-2024-automotive-industry/.
69. VicOne. "Driving Intelligence: How Edge AI Is Transforming Vehicle Threat Detection." January 28, 2025. https://vicone.com/blog/driving-intelligence-how-edge-ai-is-transforming-vehicle-threat-detection.
70. Weber, Thomas, Koster, Alex and Quinn, Mike. "As Auto Software Revs Up, Suppliers Need to Switch Gears." BCG. November 14, 2024. http://bcg.com/publications/2024/auto-software-revs-up-suppliers-switch-gears.
71. Wu, Sarah. "Volkswagen to roll out new architecture with Xpeng to cut China EV costs." Reuters. April 17, 2024. https://www.reuters.com/business/autos-transportation/volkswagen-roll-out-new-architecture-with-xpeng-cut-china-ev-costs-2024-04-17/.
72. Yousseef, Amal, Satam, Shalaka and Latibari, Banafsheh Saber. "Autonomous Vehicle Security: A Deep Dive into Threat Modeling." Arxiv. December 19, 2024. https://arxiv.org/html/2412.15348v1.
73. Zvi, Ran Ben. "DevSecOps for Automotive: Accelerating Development and Bolstering Cyber Security of Software-Defined Vehicles." Plaxidityx. May 8, 2024. https://plaxidityx.com/blog/cyber-security-blog/devsecops-for-automotive-accelerating-development-and-bolstering-cyber-security-of-software-defined-vehicles/.