Software-Defined Vehicles: Digital Infrastructure, Data Spaces, and AI as Drivers

From Vehicle to Digital Service – Europe's Path to Trustworthy and Scalable Mobility

By Juan I. Hahn, founder of HAHN Network and Leader of the eco Mobility Competence Group at the eco Association of the Internet Industry. The Competence Group brings together experts from the automotive, digital and mobility sectors to promote innovative projects.

At IAA Mobility 2025 in Munich, sessions such as "Software-Defined Vehicle Platform" and smart infrastructure demonstrations focusing on 5G corridors will showcase the future of mobility. In parallel, on 12 September, the EU Strategic Dialogue on the Automotive Industry will discuss how Europe can remain competitive in the digital transformation. The proximity of these events highlights the close connection between the two: the collaboration between the automotive and digital industries is a key driver of this transformation.

Digital Transformation of the Automotive Industry

The automotive industry is currently undergoing a dual transformation: electrification and digitalisation. The software-defined vehicle (SDV) is increasingly shifting value creation from hardware to software, data and digital services. Functions can be expanded after the sale via over-the-air (OTA) updates, and vehicles are becoming integral components of digital ecosystems.

In short: The SDV transforms the vehicles into digital end devices that generate revenue from software and data.

For users, this leads to increased comfort and safety, from new OTA features to personalised driving experiences. For manufacturers, it opens up new revenue streams through data-driven services. According to S&P Global Mobility (2024, "Connected Vehicle Data: Volume and Value Report"), connected vehicles generate around 25 gigabytes of data per hour, sourced from over 100 sensors and systems. However, this potential can only be fully realised if networks, the cloud, data spaces, interoperability, AI and cybersecurity work together in a holistic manner.

Networks and Connectivity as the Foundation

A powerful digital infrastructure is a prerequisite for SDV. Many autonomous functions cannot operate optimally without fast and stable Internet connections, and updates and services require real-time communication. The expansion of broadband and 5G networks is therefore crucial. Already today, vehicles regularly exchange data with cloud servers, for example to update navigation maps or for predictive maintenance.

In short: Without high-performance networks, there can be no reliable SDV functions.

With the expansion of 5G campus networks and, looking ahead, 6G from 2030, the importance of connectivity will continue to grow, especially for safety-critical applications such as Vehicle-to-Everything (V2X) communication. Grand View Research (2025, "Vehicle-to-Everything Market Size Report") forecasts an average annual growth rate (CAGR) of 42.2% for the V2X market between 2025 and 2030. Other studies, such as MarketsandMarkets (2023), place the figure at around 50% over a similar time frame, reflecting differences in segment definition and methodology.

Cloud and Data Spaces: Central SDV Infrastructure

The cloud is central to SDV. It processes large volumes of data in real time and enables new services. Safety-critical OTA updates are centrally controlled from the cloud, software versions of vehicle fleets are managed and tested with digital twins. Allied Market Research (2024, "Automotive Cloud Market Outlook") and Frost & Sullivan expect a compound annual growth rate (CAGR) of 14–16% for the automotive cloud market by 2032.

Data sovereignty is becoming increasingly important. The Data Act strengthens user access to vehicle data. The European Commission (COM(2025)95 "Industrial Action Plan for the European automotive sector") is reviewing sector-specific regulations for vehicle interfaces. Decentralised, federated data spaces such as the Mobility Data Space promote user-centric services. In addition, multi-cloud strategies and exit clauses should reduce dependencies.

Interoperability and Open Platforms

For SDVs to reach their full potential, isolated silo solutions must be overcome. Current operating systems and platforms are often incompatible, leading to inefficient structures and barriers to innovation.

Open standards such as AUTOSAR Adaptive, Eclipse SDV (2025, "Blueprint Release"), COVESA or SOAFEE provide solutions here. Interoperability fosters innovation, comparable to smartphone ecosystems in which apps work across manufacturers. Open interfaces and standardised profiles facilitate the development of manufacturer-independent services, while certifications and regular audits address security concerns.

Examples of successful initiatives and partnerships: BMW and Microsoft are working on connected car platforms on Azure. Bosch is investing over 2.5 billion euros in AI capabilities by 2027 (Bosch Tech Day 2025). SAP supports production and logistics processes with RISE with SAP. Siemens provides industrial-edge platforms for AI-based mobility applications.

AI as a Driver of Innovation

Without AI, the SDV concept is hardly conceivable. AI controls automated driving functions, from lane departure warning systems to autonomous driving, and enables intelligent cockpits, predictive maintenance and personalised services. Edge computing allows AI decisions to be made directly in the vehicle, for example for emergency brake assist systems where milliseconds are crucial. Current studies predict strong growth for the automotive AI market. Grand View Research (2025) expects a compound annual growth rate (CAGR) of 23.4% between 2025 and 2030. NextMSC (2024) even sees a CAGR of 29.2%. MarketsandMarkets (2025) is somewhat more conservative at 15.3% for the same period. This range illustrates the dynamics and uncertainties in market development. Sovereign AI models, trained on European data spaces such as the Mobility Data Space, could make SDV functions less dependent on global hyperscalers (COM(2025)95).

In short: AI is the "brain" of the SDV, making driving functions smarter and Europe more competitive.

An example: Connected car data enables predictive maintenance through cloud-based AI analysis. Wear is detected early, and car repair shops receive automatic appointment suggestions. Pilot projects show that diagnostics are becoming more precise and downnewtime is decreasing (Deloitte 2025, "Future of Automotive Workforce").

Cybersecurity and Trust

The more digital vehicles become, the more important cybersecurity becomes. SDVs offer many benefits, but they are also more vulnerable to hacker attacks. More software means a larger attack surface.

In short: More software means more attack surface; trust requires end-to-end cybersecurity.

Since July 2022, new cybersecurity and update standards have applied in Europe (UNECE R155, R156, as well as ISO/SAE 21434 and ISO 24089). Structured risk analyses, regulated update processes and verifiable compliance along the supply chain are essential. AI-supported attack detection and end-to-end encryption protect SDVs from threats. SBOM also ensures transparency in the supply chain and minimises security risks. In addition, companies should build crypto-agility and prepare for the introduction of post-quantum secure procedures – for example, through migration paths, key rotation and test environments for post-quantum cryptography.

Reality Check: Hurdles and Trade-offs

Despite all opportunities, the SDV transformation also presents considerable challenges:

- **Costs and complexity.** The transition to zonal E/E architectures, new software platforms and OTA toolchains requires high upfront investment. In the short term, TCO and organisational complexity increase, while ROI depends on the market penetration of software-based revenues.
- **Dependencies.** Cloud solutions create speed, but also increase the risk of lock-in effects. Multi-cloud strategies, exit clauses and open interfaces are key countermeasures.
- **Trade-offs.** OTA speed collides with safety approvals, data monetisation with data protection, openness with IP protection. These tensions require transparent governance and clear guardrails.

Global Competitive Dynamics

Europe competes with the US and Asia. In the US, tech companies are driving forward SDV stacks, cloud ecosystems and chips in tight integration. In China, integrated software and hardware platforms are growing rapidly, also due to economies of scale. Europe's areas of differentiation are trustworthiness, security, data sovereignty and interoperability. Partnerships across industries and countries remain crucial.

Risks and Countermeasures

Risk	Countermeasure
Data protection	Privacy by design, transparent consent processes, pseudonymisation
Proprietary lock-in	Open interfaces, multi-sourcing, interoperability requirements
Financing	Blended financing, CEF, national, private, prioritised sections, milestone monitoring
Skills shortage	Upskilling programmes, targeted recruitment, automotive specialisation for IT professionals
EU coordination	Pilot-first approach, standard processes, accelerated legislation

Hyperscaler dependency	Multi-cloud, exit scenarios, data portability, open interface profiles
Legacy complexity	Migration path to zonal E/E, product line roadmap, clear sunset criteria
Safety vs. agility	Staged rollouts, feature flags, blue-green-OTA, SBOM, coordinated approval processes
TCO and business case	Stage-gate process with NPV and payback criteria, service attach rate, end-to-end cost accounting
Crypto-agility	PQC roadmap, crypto inventory, key rotation, hybrid procedure

---

Recommendations with Measurement Points

- **Open interfaces** (Commission and Parliament): EU legal act by 2026; KPI: 60% of new vehicle types with certified API according to uniform profile from 2027
- **Data spaces** (Commission and industry consortia): Governance framework by 2026; KPI: doubling of productive datasets by 2028
- **5G on TEN-T** (Member States and network operators): 75% by 2027, 90% by 2029; KPI: coverage per route section, availability >99%, average latency <20 ms, packet loss <0.1%
- **Cross-border sandboxes** (Commission and Member States): 5 pilot projects by 2027; KPI: published evaluations, derived standards, integration into regulations
- **SME involvement** (industry alliances and regulators): Open specifications by 2026; KPI: increase the share of smaller companies in SDV alliances from currently under 20% to over 35%
- **Financing path** (EU, Member States, industry): blended finance via CEF, IPCEI and private funds with milestones; KPI: share of projects with blended financing and payback in 3 to 5 years
- **EU reference profile SDV APIs v1.0** (industry and standardisation): Uniform minimum profiles for vehicle, data and security interfaces; KPI: at least three compliant reference implementations by 2027
- **AI-supported API development** (industry and research): Use of AI tools for automated analysis and optimisation of SDV interfaces; KPI: pilot project with AI-generated API profiles by 2028
- **PQC roadmap** (industry and regulators): migration path to post-quantum secure procedures in backends, OTA and V2X; KPI: two productive pilot paths by 2028, including crypto-agility playbook

Conclusion: Collaboration as the Key to Success

The automotive industry provides indispensable domain expertise, while the Internet and digital economy provides technologies such as networks, cloud, data spaces, interoperability, AI and cybersecurity. Only together can they exploit this potential and thus create the conditions for SDV to scale reliably in Europe and safeguard long-term competitiveness.

Glossary of Key Technical Terms

- **OTA (Over-the-Air-Updates):** Wireless software updates for vehicles, without workshop visits.
- **V2X (Vehicle-to-Everything):** Communication of vehicles with other vehicles, infrastructure, or devices.
- **CAGR (Compound Annual Growth Rate):** Average annual growth rate over a period of time.
- **SBOM (Software-Bill-of-Materials):** List of all software components, ensuring transparency and security.
- **PQC (Post-Quantum-Cryptography):** Encryption methods that are also resistant to attacks by quantum computers.
- **Crypto-agility:** Ability to flexibly switch cryptographic methods in order to respond to new threats.

Methodology and Sources

CAGR values vary depending on segment definition, region and observation period. Where ranges are given, they reflect the range of different studies.

Sources: 1. EU Commission: COM(2025)95, “Industrial Action Plan for the European automotive sector”, 5 March 2025, EUR-Lex. 2. UNECE: Regulations R155/R156 on cybersecurity and software updates, application from 07/2022 and 07/2024. 3. ISO/SAE: ISO/SAE 21434:2021 (Cybersecurity Engineering) and ISO 24089:2023 (Software Update Processes). 4. S&P Global Mobility (2024): “Connected Vehicle Data: Volume and Value Report”. 5. Grand View Research (2025): “Vehicle-to-Everything Market Size Report”. 6. MarketsandMarkets (2023): “Automotive AI Market Forecast”. 7. Allied Market Research (2024): “Automotive Cloud Market Outlook”. 8. Frost & Sullivan (2024): Automotive Cloud Forecasts. 9. Deloitte (2025): “Future of Automotive Workforce”. 10. Bosch: Tech Day 2025, investments >2.5 billion euros in AI Software by 2027. 11. SAP: RISE with SAP for manufacturing and logistics processes, example BMW Group 2025.12. Siemens: Industrial edge platforms for real-time analytics and AI in industrial and mobility applications. 13. Eclipse Foundation (2025): “SDV Blueprint and API Framework”.14. SDVoF Roadmap (2025): EU initiative for the development of common SDV building blocks and interfaces.