White Paper

Cybersecurity will decide the digital future of the automotive industry

Vehicle Cyber Security

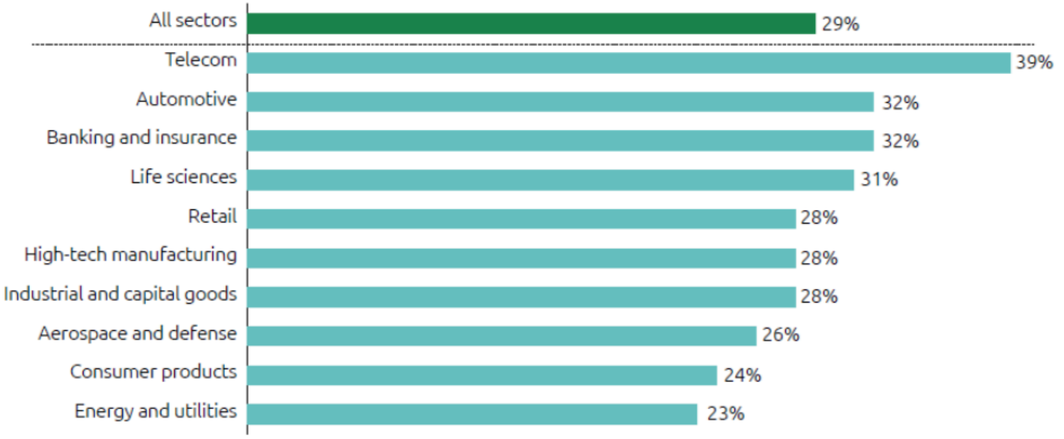
Over-the-air applications, digital services and assistance systems are fundamentally changing the nature of production and maintenance in the automotive industry. Software applications and reliable vehicle cybersecurity (VCS) are becoming core functions in vehicle manufacture. In July 2022 the EU introduced a requirement for a comprehensive Cyber Security Management System (CSMS) in every new class and type of vehicle. From July 2024, the requirements are set to become much more exacting. Every newly registered vehicle must then have a CSMS.

The networking of the electrical and electronic (E/E) systems in vehicles now extends along the entire supply chain up to and including maintenance, meaning that automobile manufacturers are increasingly focussing their strategy on software-based digital services. Vehicles are contacted directly over the air and refreshed with the latest updates and functional enhancements. The future of automobility will be determined by climate-neutral drive systems, but data will also play a major role. In 2023, Ola Källenius, CEO of Mercedes Benz, said in Silicon Valley: "We are on a journey to also become a software company. Supercomputer-like performance will need to be installed in every single vehicle, each with its own operating system and chip-to-cloud architecture."

Digital services becoming a major **competitive factor**

The automotive industry is currently investing around 20 per cent of its R&D expenditure in software projects for the integration of digital services. Today's production vehicles incorporate more than 150 electrical and electronic units, with the accompanying software containing at least 100 million lines of program code. The systems for built-in road safety assistance and for networking with devices and infrastructures (Internet of Things, IoT) now require enormous computing power, in some cases involving artificial intelligence.

According to a study by Capgemini, 47 per cent of the 1,500 companies surveyed worldwide from all sectors expect to become software providers in three to five years' time. Software-based revenue shares are set to almost quadruple by 2030. Accounting for a forecast share of 32 per cent, the automotive sector will then be second only to the telecommunications industry in terms of software-related sales.



Source: Capgemini Research Institute, Software-driven transformation survey, June-July 2023, N = 1,350 organizations that have/are building a strategy to become a software-driven organization, focusing on software-defined products/services.

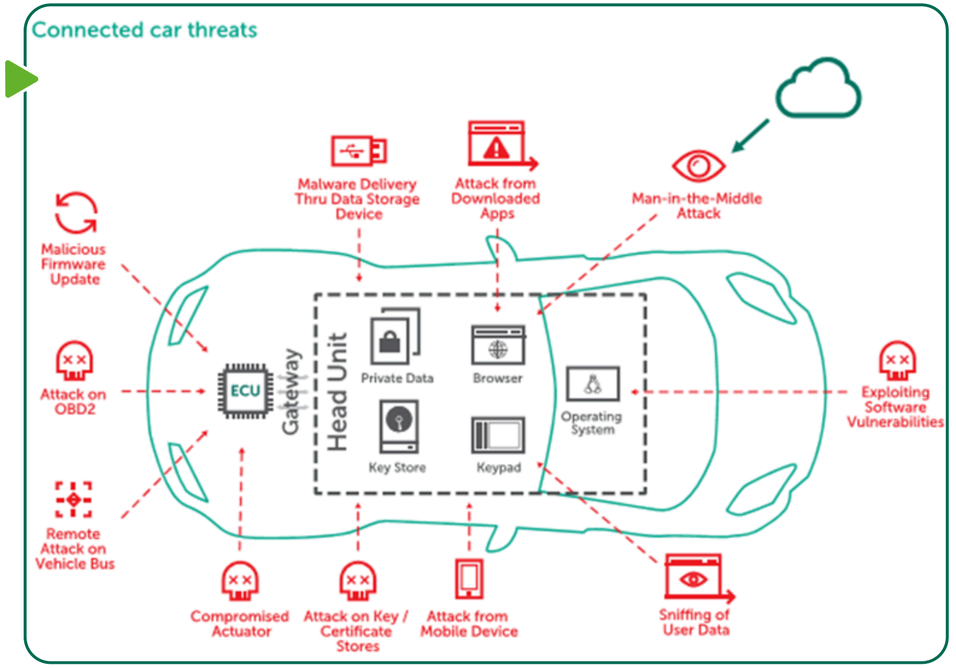
Vehicle Cyber Security

Vehicles as communication platforms

The mobility systems of the future will be able to network not only vehicles and public transport infrastructures, but all road users – including pedestrians – via their mobile devices. This will bring about highly varied communication channels, data relationships and security requirements:

- Vehicle-to-Vehicle (V2V): Vehicles communicate with each other, exchanging data on driving functions, location, real-time traffic information, etc.
- Vehicle-to-Infrastructure (V2I): Vehicles communicate with public infrastructures such as traffic guidance systems, traffic lights, car parks, charging stations, etc.
- Vehicle-to-Pedestrian (V2P): Vehicles communicate with pedestrians' mobile devices.
- Vehicle-to-Network (V2N): Vehicles are connected to cloud services, e.g. for maintenance, updates, customisable functions, extra equipment, etc.

Such an IoT environment will interconnect millions of components that communicate with each other via heterogeneous operating systems and cloud-based data storage technologies. At the same time, security concepts must also keep up with the latest developments. The possibilities opened up by machine-to-machine communication and automation are leaving the systems wide open to manipulation. For example, the actual intention of cyberattacks on some infotainment units has reportedly been to gain access to the control systems of the braking and steering units. And attackers have been able to use manipulated firmware in the remote control key to gain access to the diagnostic software and start the vehicle.



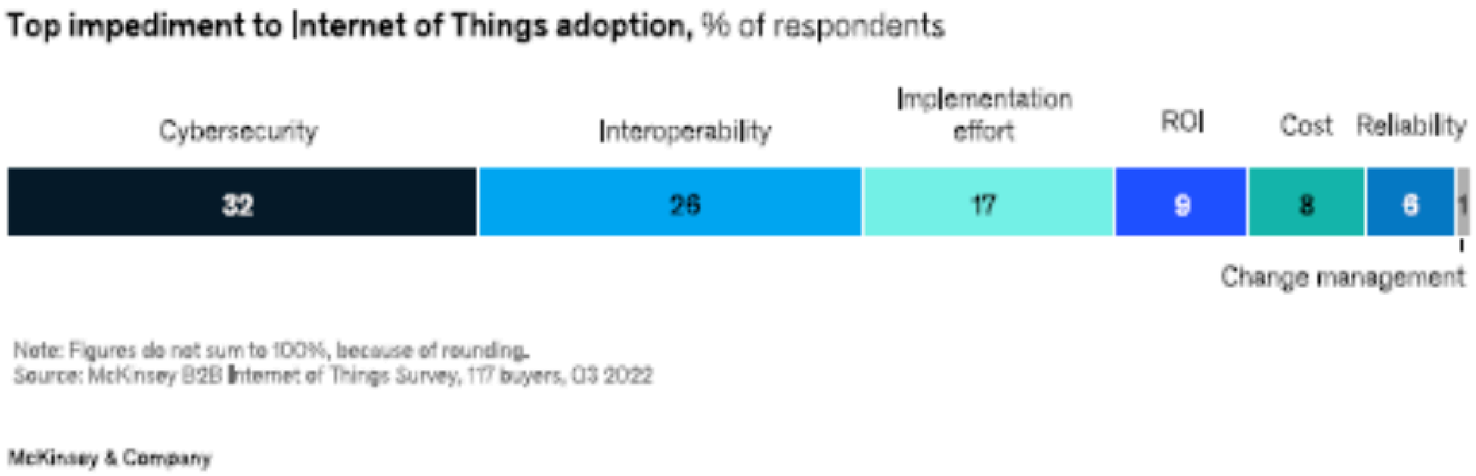
Vehicle Cyber Security

Cyber and data security: Core vehicle production functions

The extensive networking of vehicle control, regulation and monitoring functions, as well as of remote access systems pose significant risk management challenges in defending against cyber threats. Furthermore, previous security barriers between companies' own information technology and the operational IT in their production are becoming easier to overcome. This makes it easier for malware to infiltrate an entire organisation. Back in 2022, analysts from McKinsey discovered that companies regard cybersecurity as the greatest challenge in setting up the Internet of Things – and not the investment costs.
The extensive networking of vehicle control, regulation and monitoring functions, as well as of remote access systems pose significant risk management challenges in defending against cyber threats. Furthermore, previous security barriers between companies' own information technology and the operational IT in their production are becoming easier to overcome. This makes it easier for malware to infiltrate an entire organisation. Back in 2022, analysts from McKinsey discovered that companies regard cybersecurity as the greatest challenge in setting up the Internet of Things – and not the investment costs.

Effective cybersecurity is essential to ensure that the data platforms for over-the-air applications remain continuously available. It is becoming an integral part of the overall value chain. The entire supply structure with its ever-shorter product and innovation cycles must be considered here: from the design phase, component and prototype development, production and operation right through to post-production updates and decommissioning or scrapping.

Practical experience shows that cyber risks can only be managed effectively if the processes along the entire supply chain are controllable. This is why non-transparent supply structures harbour major cyber risks, as each supply stage is in turn the node of a further structure. New components or interfaces can provide new targets for cyber criminals. Furthermore, the vehicles themselves generate highly sensitive sets of data. Examples include biometric information on driving behaviour: this is linked to the chassis number and may still be available even after the vehicle has been decommissioned.



Vehicle Cyber Security

The Cyber Security Management System (CSMS)

From July 2024, it will be mandatory for manufacturers in the EU to prove that IT and information security levels are being upheld. This will take the form of a Cyber Security Management System (CSMS) in each and every newly registered vehicle – not just for the vehicle class, vehicle type or individual components.

The approval authorities therefore scrutinise not only the requirements pertaining to the manufacturers' organisation, development and production, but also those stipulated for every newly registered vehicle on the road. UNECE R-155 for cyber security provides the regulatory framework for this. It is specified in greater detail in ISO/SAE 21434. In addition, there are the UNECE R-156 provisions concerning software updates, the implementation of which is set out in the ISO 24089 standard.

ISO/SAE 21434 "Road vehicles - Cyber Security Engineering" was introduced in 2021 as a comprehensive security standard. It provides the basis for structured and regular reassessment of digital vehicle security risks. The standard is aimed specifically at cybersecurity in the development of electrical and electronic (E/E) systems in road vehicles. The technical requirements are determined by the organisational structures of the manufacturer and its suppliers over the entire life cycle of the vehicle. The standard is based on the requirements of the World Forum for Harmonization of Vehicle Regulations (WP.29) of the United Nations for Europe (UNECE) and is a globally applicable set of regulations.

In addition, the VDA is developing the TISAX® VCS (Vehicle Cyber Security) standard in conjunction with the ENX Association. The TISAX standard and ISO 27001 relate to the protection of data and information within an organisation, whereas ISO/SAE 21434 and TISAX® VCS extend manufacturers' responsibility to the product level throughout its life cycle.

TISAX VCS is therefore also aligned with ISO/SAE 21434. However, the ISO standard is not accredited, meaning that the ENX approach to assessing CSMSs based on TISAX VCS could potentially become established worldwide.

Vehicle Cyber Security

ISO/SAE 21434: Regulations for comprehensive cyber security

Even though ISO/SAE 21434 does not yet include a certification scheme, its field-proven regulations support the implementation of comprehensive cyber security. All assets, structures and supply relationships that are vulnerable to considerable damage from a cyberattack and could jeopardise continued operations are evaluated.

- Hardware and software are taken into account, as are all data-based components and the interfaces to suppliers. Examples: control systems for the electronics of doors, locks, brake systems, airbags, power steering, displays, etc. An algorithm for a driver assistance system is thus also considered a critical asset.

- A comprehensive risk assessment must be drawn up for each vehicle component and its interactions with other components. All external systems must be taken into account, as must known cyber risks within the organisation. The company must also gain expertise in forensic data analyses in order to recognise any patterns in the attacks and be able to respond effectively in future.

- A further focus is on technology partnerships and suppliers as well as on all downstream aftermarket services with regard to maintenance, repairs, upgrades based on software applications, storage of accessories, etc.

Evaluation audit as effective starting point

A CSMS audit is an important prerequisite for effective application of the main CSMS security requirements in operational processes. It constitutes an effecting starting point for a comprehensive security approach based on the life cycle concept contained in the regulations, which can then be continuously reviewed. The TISAX VCS audit, which is primarily aimed at the automotive industry, is based on ISO/SAE 21434, ISO/PAS 5112 and the established TISAX audit framework of the ENX Association.

In the audits, the independent DEKRA auditors take into account the external contractual relationships, programs and processes of the suppliers as well as their potential negative impact if areas of responsibility are not clearly defined, for example. Cyber security incidents and the measures taken are also evaluated. Experience to date clearly shows how a CSMS raises the overall effectiveness of systems and processes, and improves compliance with regulatory requirements. Manufacturers and suppliers can create resilient structures to protect their value chain from cyber risks, but such a management system is also an essential prerequisite for safeguarding the growth potential from digital services in the automotive sector.

DEKRA

DEKRA
Audit Services

DEKRA Audit is your partner for audits and certifications according to recognized international, national and house standards. We are holding over 200 accreditations for the certification of quality management systems, health safety and environment (HSE) and information security management systems (ISMS). Our offer includes independent audits and assessments as well as personnel certifications for various industries. DEKRA Audit operates with around 560 in-house experts and 1,200 external industry-experienced auditors and partners in 18 countries.

www.dekra.com

Would you like more information?

Contact Us!