Cybersecurity in automotive

Mastering the challenge

March 2020

Cybersecurity in automotive

Mastering the challenge

Authors
Ondrej Burkacky
Johannes Deichmann
Benjamin Klein
Klaus Pototzky
Gundbert Scherf

Acknowledgements
This study was conducted by McKinsey & Company, Inc. We wish to express our appreciation and gratitude to GSA and its members for their continued support and valuable contributions.

Contents

Introduction and key insights

The four ACES disruptions – autonomous driving, connected cars, electric vehicles, and shared mobility – have dominated the agenda of automotive industry leaders in recent years. These innovations, built on the digitization of in-car systems, the extension of car IT systems into the back end, and the propagation of software, turn modern cars into information clearinghouses. Hacking of connected cars by security researchers has made headlines over the past few years, and concerns about the cybersecurity of modern vehicles have become real. Lately, regulators have also started working on defining the minimum cybersecurity requirements for new cars. The UNECE WP.29[1] regulation on cybersecurity and software updates is on the horizon and will trigger a paradigm shift in the automotive industry in the UNECE member countries. Other countries like the US and China have issued best practices and frameworks but no regulations yet. Given the influence of UNECE, however, a broad adoption of its regulation across the world is expected.

With these first regulatory programs for cybersecurity and software updates in the automotive sector, the regulator will require automotive OEMs – the responsible parties for vehicle homologation – to demonstrate adequate cyber-risk management practices throughout development, production, and postproduction of their vehicles, including the ability to fix software security issues after the sale of vehicles and over the air.

In this context and based on our extensive research and analyses, we offer a perspective on three key questions for the automotive industry:

- What are the specific trends and drivers of cybersecurity in the automotive industry and why is this a paradigm shift for the industry?
- How are these drivers going to affect the automotive industry's long-established value chains?
- How can players inside and outside the industry prepare and position themselves for the upcoming market developments and anticipated segment growth?

While the following paragraphs provide a summary of our research, the remainder of the report will address these questions in detail.

Engine power, fuel consumption, driving comfort, and the precision of a car's chassis and body are just a few dimensions that define the quality of a car. With more and more core vehicle functions enabled by software running on specialized hardware chips, the security of those components – cybersecurity – will become yet another dimension of quality in the automotive industry, in much the same way that physical safety is a major concern and quality parameter today.

This measure of quality is underpinned by regulatory activities that impose minimum standards for managing cybersecurity risks and require OEMs to have the ability to fix security issues via software updates. Cybersecurity will become nonnegotiable for the industry.

In order to excel at cybersecurity, new processes, skills, and working practices along the automotive value chain will be required. This includes identifying cyber risks, designing secure software and hardware architectures, and developing and testing secure code and chips, ensuring that issues can be fixed – even years later – via software updates.

The rising need for cybersecurity will trigger investments over the next few years. We expect to see the market grow from USD 4.9 billion in 2020 to USD 9.7 billion in 2030, with software business representing half of the market by 2030. The strong growth of the market will create many new business opportunities for suppliers, established IT firms, specialist niche firms, start-ups, and many others, especially in the software development and services market. At the same time, the dynamics of the growing market will also challenge today's leaders in the market.

[1] UNECE, Proposal for a new UN Regulation on uniform provisions concerning the approval of vehicles with regard to cyber security and of their cybersecurity management systems; UNECE, Proposal for a new UN Regulation on uniform provisions concerning the approval of vehicles with regard to software update processes and of software update management systems.

1. Cybersecurity is becoming a new dimension of quality for automobiles

Software is one of the key innovations in modern vehicles

Software and electrical/electronic (E/E) components are and will continue to be among the key innovations in modern vehicles. The market is expected to grow from USD 238 billion in 2020 to USD 469 billion in 2030, corresponding to an annual growth of over 7 percent per year.[2]

This growth is driven to a large extent by software, which is becoming a key differentiator. Software is driving innovation in the four ACES categories:

— **Autonomous.** Autonomous cars, which have been the subject of fantasy for a long time, are becoming reality. Leading companies have already driven millions of miles on public roads with them, but so far always under the watchful eye of a human behind the steering wheel. The disengagement rate in field tests, i.e., how often the human driver needs to take over control, is rapidly declining, putting fully autonomous cars in reach within mere years. While the autonomous car offers great advantages, it comes with the risk of hackers interfering with steering or breaking. Such incidents would foster fear of autonomous cars and put the whole technology at risk.

— **Connected.** Cars are becoming more and more connected. The services enabled by connectivity today range from sending destination addresses to the vehicle, to receiving real-time traffic information, to parking the vehicle remotely via a smartphone app. However, the connectivity of cars is a potential attack vector for hackers to compromise a full fleet of cars, which is the worst nightmare of every OEM.

— **Electric.** The rise of electric cars started several years ago and they are gaining more and more traction as their range increases and their price decreases. Challenged by many start-ups, almost all incumbent OEMs have embarked on the journey to including electric cars in their product portfolios. The electric car per se is not more susceptible to sabotage than a conventional car, but attacks on charging infrastructure can have severe effects, from power outages to fires.

— **Shared.** Enabled by connectivity, new business models for transportation have become viable, such as car sharing and ride hailing. The trend in mobility is moving away from car ownership and towards shared-car solutions, which is significantly increasing vehicle utilization. This trend requires full protection of user data – a breach of sensitive data could foster massive distrust of the business model.

A deeper look into the connected car shows three types of software that will drive innovation in this area:

— In-vehicle services: All software within the vehicle that runs on electronic control units (ECUs) or domain control units (DCUs) within the car

— OEM back-end services: Cloud services for both the vehicle and user

— Infrastructure and third-party services: Software links between the vehicle and infrastructure, e.g., gas/charging, parking, insurance.

While the industry is investing in innovations across these types of software to enhance the customer experience and increase the value of modern cars, manufacturers must also build in cybersecurity from the beginning to avoid creating cyberattack-prone digital platforms and vehicles.

With every line of code, the cyber risk to modern vehicles increases, and security researchers have demonstrated its impact and cost

Over the last several years, modern cars have become data centers on wheels. Comparing the lines of code in modern connected cars with aircrafts and PCs provides a glimpse into the challenges of securing these vehicles. Today's cars have up to 150 ECUs and about 100 million lines of code; by 2030, many observers expect them to have roughly 300 million lines of software code. To put this into perspective, a passenger aircraft has an estimated 15 million lines of code, a modern fighter jet about 25 million, and a mass-market PC operating system close to 40 million.[3] This abundance of complex software code is a result of both the legacy of designing electronic systems in specific ways for the past 35 years and the growing requirements and increasing complexity of systems in connected and autonomous cars. This amount of code creates ample opportunity for cyberattacks – not only on the car itself but also on all components of its ecosystem (e.g., back end, infrastructure).

The cyber risk of connected cars has become clear over the past few years, as security researchers have revealed various technical vulnerabilities. In these scenarios, the "attackers" were not exploiting the vulnerabilities with bad intentions but rather

[2] Source: McKinsey, "Mapping the automotive software-and-electronics landscape through 2030," July 2019.
[3] Source: McKinsey, "The race for cybersecurity: Protecting the connected car in the era of new regulation," October 2019.

disclosing information to OEMs to help them fix those issues before malicious attackers caused actual harm. Some of the recently reported vulnerabilities are listed in Exhibit 1.

After becoming aware of the vulnerabilities, OEMs fixed the issues and provided software updates. But, depending on the affected car model, its E/E architecture, and the OEM's ability to provide software updates over the air, some software updates required visits to dealerships, resulting in much higher costs for carmakers.

Cybersecurity will be nonnegotiable for securing market access and type approval in the future

Unlike in other industries, such as financial services, energy, and telecommunications, cybersecurity has so far remained unregulated in the automotive sector – but this is changing now with the upcoming UNECE WP.29 regulations on cybersecurity and software updates.[4] Under this framework, OEMs in UNECE member countries (see Exhibit 2) will need to show evidence of sufficient cyber-risk management practices end to end, i.e., from vehicle development through production all the way to postproduction. This includes the demonstrated ability to deploy over-the-air software-security fixes even after the sale of the vehicle. Other countries like China and the US have so far not issued similar regulations, only guidelines and best practices. We expect the new UNECE regulation to become a de facto standard even beyond its members.

Looking at today's passenger car market volumes in only the ten largest countries regulated under UNECE WP.29, the new regulations will likely affect over 20 million vehicles sold worldwide. This does not even include commercial vehicles, or any other type of motor vehicle regulated under UNECE WP.29.

Exhibit 1

Software vulnerabilities have been observed across the entire digital car ecosystem

In-vehicle services

2018: Researchers demonstrated **>10 vulnerabilities in various car models,** gaining local and remote access to infotainment, telematics, and CAN buses

2018: Researchers exploited vulnerabilities of some **infotainment systems** and gained control of microphones, speakers, and navigation systems

2015: Researchers remotely sent commands to the **CAN bus of a specific car** that had an OBD2 dongle installed to control the car's windshield wipers and breaks

OEM back-end services

2019: Malware infected the **back end,** making laptops installed in police cars unusable

2019: Vehicle data exposed during registration allowed for remote denial-of-service attacks on cars

2015: Researchers demonstrated vulnerabilities within the back end, **gaining access to door control**

Infrastructure/third-party services

2018: EV home chargers could be **controlled** by accessing the home Wi-Fi network

2018: Security issues discovered in 13 **car-sharing apps**

2017: Rental car companies **exposed personal data**

Enterprise technology

2019: Memory vulnerability at a cloud provider **exposed data incl. passwords, API keys, and tokens**

2019: Hack of an OEM's **automotive cloud** via third-party services and tier-1 supplier network

2018: Cloud servers hacked and **used for cryptomining**

Production and maintenance systems

2019: A malware infection caused significant production disruption at a car parts manufacturer

2018: An ex-employee breached the company network and downloaded large volumes of **personal information**

2017: Ransomware caused the **stop of production** across several plants

Source: Press search

[4] UNECE, Proposal for a new UN Regulation on uniform provisions concerning the approval of vehicles with regard to cyber security and of their cybersecurity management systems; UNECE, Proposal for a new UN Regulation on uniform provisions concerning the approval of vehicles with regard to software update processes and of software update management systems.

What is UNECE's role in regulating automotive cybersecurity?

The World Forum for Harmonization of Vehicle Regulations (WP.29) is a worldwide regulatory forum within the institutional framework of the UN Economic Commission for Europe (UNECE). It establishes regulatory instruments concerning motor vehicles and motor vehicle equipment in over 60 markets globally, based on three UN agreements adopted in 1958, 1997, and 1998.

At the time of writing this report, UNECE is drafting a proposal for two new UN regulations. The first regulation is on uniform provisions concerning the approval of vehicles with regard to cybersecurity and cybersecurity management systems. The second regulation is on vehicle software update processes and software update management systems. For ease of readability, we'll refer to both regulations as the UNECE WP.29 regulations on cybersecurity and software updates throughout this report.

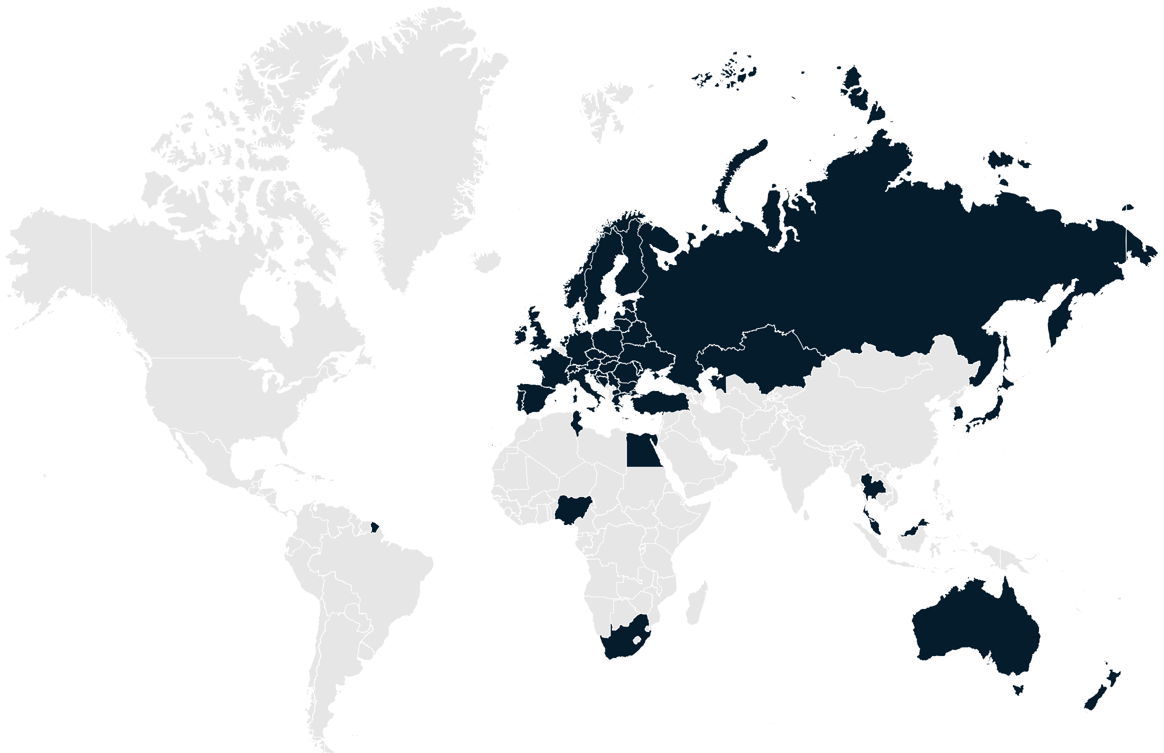
Once this proposal is accepted by UNECE and the regulations are adopted by its member countries, OEMs will be required to implement specific cybersecurity and software-update practices and capabilities for vehicle type approvals – effectively rendering cybersecurity a nonnegotiable component of future vehicles.

Exhibit 2

Cars in over 60 countries will be affected under the new World Forum for Harmonization of Vehicle Regulations framework on cybersecurity and software updates

World Forum for Harmonization of Vehicle Regulations (WP.29) under the UN Economic Commission for Europe (UNECE)

■ Countries party to the 1958 agreement[1] (as of December 2018)



[1] "Agreement concerning the Adoption of Harmonized Technical United Nations Regulations for Wheeled Vehicles, Equipment and Parts which can be Fitted and/or be used on Wheeled Vehicles and the Conditions for Reciprocal Recognition of Approvals Granted on the Basis of these United Nations Regulations" (original version adopted in Geneva on March 20, 1958)

Source: UNECE ECE/TRANS/WP.29/343/Rev.27 – Status of the Agreement, of the annexed Regulations and of the amendments thereto – Revision 27

2. The automotive industry is rethinking cybersecurity along the entire value chain

Getting cybersecurity right requires efforts from multiple parties along the value chain, for the entire digital lifecycle of modern vehicles

Ultimately, OEMs are responsible for the homologation of their vehicles and demonstrating their adherence to regulations and mandatory legal requirements. However, since OEMs source a large share of their vehicle components from suppliers and semiconductor manufacturers, their upstream value chain partners will also be required to follow and implement state-of-the-art practices to mitigate cybersecurity risks and produce vehicles that are secure by design. These partners must provide evidence of adhering to the regulations to support the type-approval process, which is the responsibility of the OEM. Looking at the current drafts of the UNECE WP.29 regulations on cybersecurity and software updates, it becomes evident that the value chain is affected across four areas (see Exhibit 3):

- **Cyber-risk management.** Automotive players must ensure end-to-end cyber-risk management and identify relevant cyber risks in their vehicle types (and in adjacent ecosystem components that might impact vehicle safety or security) and ensure that they implement measures to mitigate such risks. This includes reacting to evolving threats.

- **Security by design.** OEMs must develop secure vehicles from step one by adopting state-of-the-art practices in hardware and software engineering, and ensuring that vehicle types (and adjacent ecosystem components that might impact vehicle safety or security) are designed, built, and tested for security issues and any cyber risks are mitigated properly. Although OEMs are ultimately responsible for cybersecurity, all participants in the value chain need to contribute.

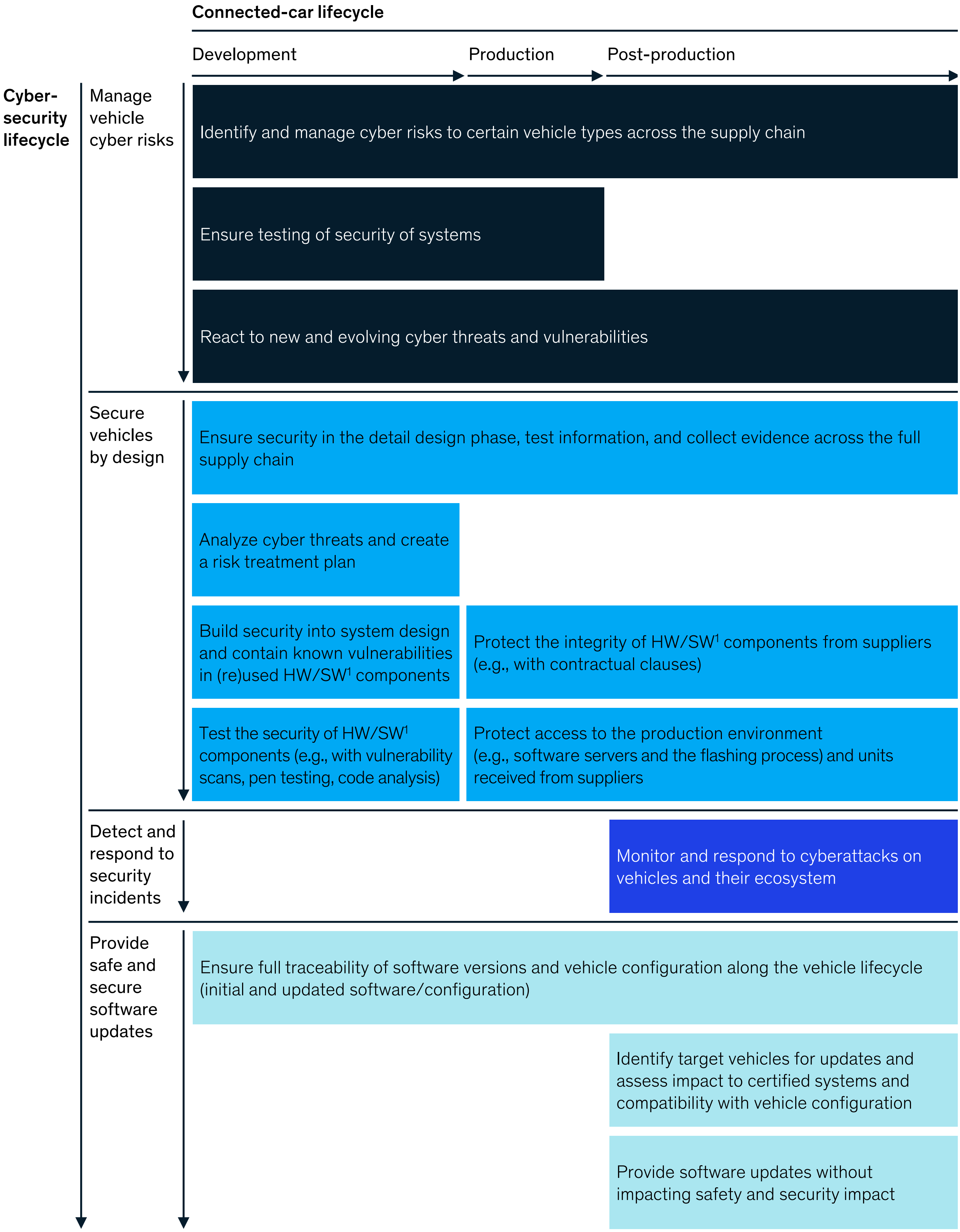
- **Detection and response.** Vehicle manufacturers must be able to detect technical vulnerabilities and security issues (e.g., cyberattacks) in their vehicles and adjacent ecosystem components (e.g., the back end or third-party services) that might impact vehicle safety or security.

- **Safe and secure updates.** Automotive players must be able to respond to any detected security event and provide software updates to fix security issues. To do so, they must systematically identify target vehicles for updates and ensure that software updates will not harm certified safety-relevant systems and are compatible with the vehicles' configuration.

Exhibit 3

The UNECE regulation is broken down into 4 concrete areas of cybersecurity and spans across the entire vehicle lifecycle

SIMPLIFIED



Connected-car lifecycle

Development → Production → Post-production →

Cyber-security lifecycle

Manage vehicle cyber risks

- Identify and manage cyber risks to certain vehicle types across the supply chain
- Ensure testing of security of systems
- React to new and evolving cyber threats and vulnerabilities

Secure vehicles by design

- Ensure security in the detail design phase, test information, and collect evidence across the full supply chain
- Analyze cyber threats and create a risk treatment plan
- Build security into system design and contain known vulnerabilities in (re)used HW/SW[1] components
- Protect the integrity of HW/SW[1] components from suppliers (e.g., with contractual clauses)
- Test the security of HW/SW[1] components (e.g., with vulnerability scans, pen testing, code analysis)
- Protect access to the production environment (e.g., software servers and the flashing process) and units received from suppliers

Detect and respond to security incidents

- Monitor and respond to cyberattacks on vehicles and their ecosystem

Provide safe and secure software updates

- Ensure full traceability of software versions and vehicle configuration along the vehicle lifecycle (initial and updated software/configuration)
- Identify target vehicles for updates and assess impact to certified systems and compatibility with vehicle configuration
- Provide software updates without impacting safety and security impact

[1] Hardware/software

Source: UNECE WP.29, "Draft Recommendation on Software Updates of the Task Force on Cyber security and Over-the-air issues," ISO/SAE 21434:2018 committee draft; McKinsey

While certain practices are already in place today, the upcoming regulations, higher levels of enforcement, and potential liability implications will require a much more explicit agreement between parties along the automotive value chain on what exactly is expected of each other. To adhere to this higher level of rigor, we are expecting automotive players to:

- Define clear roles and responsibilities for vehicle cybersecurity (not just enterprise cybersecurity) and establish interfaces and points of contact for vehicle cybersecurity between players
- Agree on a minimum set of cyber-risk management and cybersecurity practices in contractual agreements and derive measurable service levels similar to what has been good practice in other dimensions of vehicle quality (e.g., safety)
- Clarify organizational, technical, and legal (e.g., IP) prerequisites that allow security testing and attestation of vehicle software security of the entire E/E vehicle architecture or down to the individual ECU.

However, security does not stop at the production of vehicles – it is important throughout the entire vehicle lifecycle, as security vulnerabilities can be discovered at any given time. It will require OEMs and suppliers to continually detect and react to security issues until vehicles have reached their end of life, just as we expect aircraft or engine manufacturers to continuously monitor their aircrafts and engines to detect and fix any operational, safety, or security issues for as long as that equipment is in use by any owner.

New standards will raise the bar for vehicle cybersecurity and allow for independent attestation of an automotive company's security practices

Currently, only narrow standards and guidelines exist for specific technical procedures for securing hardware and software in vehicles, e.g., standards for hardware encryption or secure communication of ECUs (see Exhibit 4). While the UNECE WP.29 regulations on cybersecurity and software updates set an organizational framework and minimum requirements that impact all automotive players along the value chain, they do not provide any detailed guidance on operational practices. However, the new ISO/SAE 21434 standard, "Road vehicles – cybersecurity engineering," (still a working draft) is seen by industry experts as the first standard that lays out clear organizational, procedural, and technical requirements throughout the vehicle lifecycle, from development to production to after-sales. In parallel, the ISO/

Exhibit 4 (1/2)

Unlike in other industries, cybersecurity has remained unregulated in the automotive industry beyond general IT regulations

■ Regulation/law ■ Standard ■ Best practice/framework ◌ Draft/not published

<table>
<tr><td></td><td colspan="5"><b>Ecosystem component</b></td></tr>
<tr><td></td><td colspan="3">Operating technology ←</td><td colspan="2">→ Information technology</td></tr>
<tr><td><b>Organization</b></td><td>Connected car</td><td>OEM production OT</td><td>Vehicle infrastructure</td><td>OEM back-end services</td><td>Automotive player enterprise IT</td></tr>
<tr><td colspan="6">AUTOMOTIVE ENGINEERING</td></tr>
<tr><td>UNECE</td><td colspan="4">WP.29 regulation on cybersecurity and software updates ◌</td><td></td></tr>
<tr><td>NHTSA</td><td colspan="2">Cybersecurity Best Practices for Modern Vehicles</td><td></td><td></td><td></td></tr>
<tr><td></td><td>Automated Driving Systems 2.0</td><td></td><td></td><td></td><td></td></tr>
<tr><td>VDA</td><td></td><td></td><td></td><td></td><td>Information Security Assessment</td></tr>
<tr><td>IPA</td><td>Approaches for Vehicle Information Security</td><td></td><td></td><td></td><td></td></tr>
<tr><td>MIIT</td><td colspan="4">National Guidelines for Developing the Standards System of the Telematics Industry</td><td></td></tr>
<tr><td>AutoSAR</td><td>Secure Onboard Communications</td><td></td><td></td><td></td><td></td></tr>
<tr><td>ISO</td><td colspan="2">ISO 26262</td><td></td><td></td><td></td></tr>
<tr><td></td><td colspan="2">ISO/SAE 21434 ◌</td><td></td><td></td><td></td></tr>
<tr><td></td><td>ISO/AWI 24089 ◌</td><td></td><td colspan="2">ISO/AWI 24089 ◌</td><td></td></tr>
<tr><td>SAE</td><td colspan="2">SAE J3061</td><td></td><td></td><td></td></tr>
<tr><td></td><td colspan="2">SAE J3101</td><td></td><td></td><td></td></tr>
<tr><td>AUTOSIG</td><td>Automotive SPICE</td><td></td><td></td><td></td><td></td></tr>
<tr><td>Auto Alliance</td><td colspan="5">Consumer Privacy Protection Principles (CPPP) for Vehicle Technologies and Services</td></tr>
</table>

AWI 24089 standard, “Road vehicles – software update engineering,” is also currently under development. Although it is not dedicated to cybersecurity, we expect it to contain cybersecurity-related content. A first draft is expected by mid-2020 and some more time will be needed to finalize it.

These standards will allow the industry to implement common cybersecurity practices specific to vehicle development and manufacturing. They will also allow an assessment of adherence to those practices and attestation by third parties, which can be used between industry players to demonstrate adherence to the standards, for example, in contracts between OEMs and suppliers. The independent attestation of security practices will create a growing market for auditing, inspection, and certification companies (see Section 4). Legal experts also see this as the foundation for solving legal disputes and liability issues in case of cybersecurity-related vehicle incidents.

Exhibit 4 (2/2)

Unlike in other industries, cybersecurity has remained unregulated in the automotive industry beyond general IT regulations

■ Regulation/law ■ Standard ■ Best practice/framework ⁘ Draft/not published

Ecosystem component

Operating technology ← → Information technology

<table>
<tr><th>Organization</th><th>Connected car</th><th>OEM production OT</th><th>Vehicle infrastructure</th><th>OEM back-end services</th><th>Automotive player enterprise IT</th></tr>
<tr><td colspan="6">ELECTRICAL ENGINEERING</td></tr>
<tr><td>MIIT/SAC</td><td></td><td>Guideline on national intelligent manufacturing</td><td></td><td></td><td></td></tr>
<tr><td>IEC</td><td>SAE J3138</td><td>ISA/IEC-62443</td><td></td><td></td><td></td></tr>
<tr><td>IEEE</td><td colspan="4">Automotive ISAC Best Practices</td><td></td></tr>
<tr><td colspan="6">INFORMATION TECHNOLOGY</td></tr>
<tr><td>EU</td><td colspan="5">GDPR</td></tr>
<tr><td rowspan="2">USA</td><td colspan="5">California Consumer Privacy Act (CCPA)</td></tr>
<tr><td>California Connected Device Law</td><td></td><td></td><td></td><td></td></tr>
<tr><td>NIST</td><td></td><td colspan="4">Cybersecurity Framework (CSF)</td></tr>
<tr><td>China</td><td colspan="5">Cyber Security Law (CSL)</td></tr>
<tr><td rowspan="2">Singapore</td><td colspan="5">Cybersecurity Act 2018</td></tr>
<tr><td colspan="5">Personal Data Protection Act 2012</td></tr>
<tr><td>ITU</td><td></td><td></td><td></td><td colspan="2">PCI Data Security Standard</td></tr>
<tr><td>ISO</td><td></td><td colspan="4">ISO 27001</td></tr>
</table>

Source: McKinsey analysis

Securing hardware and software in modern vehicles will require new skills and talent for a true security-by-design approach

Other industries have already developed best practices for secure software development, including leading tech companies, aerospace and defense companies, and critical infrastructure companies. OEMs and all other automotive players can lean on these best practices and combine them with the upcoming standards for the automotive industry to develop the new capabilities required throughout the full development cycle – not only for hardware and software development (see Exhibit 5).

— Requirements: Define requirements such that cybersecurity is built into the system design and the security of hardware and software is tested.

— System design: Define requirements for confidentiality, integrity, and availability of data, and design systems in accordance to these requirements.

— Component design: Analyze the security requirements for software components and design them accordingly.

— Hardware/software development: Implement the security requirements into the hardware and software.

Exhibit 5

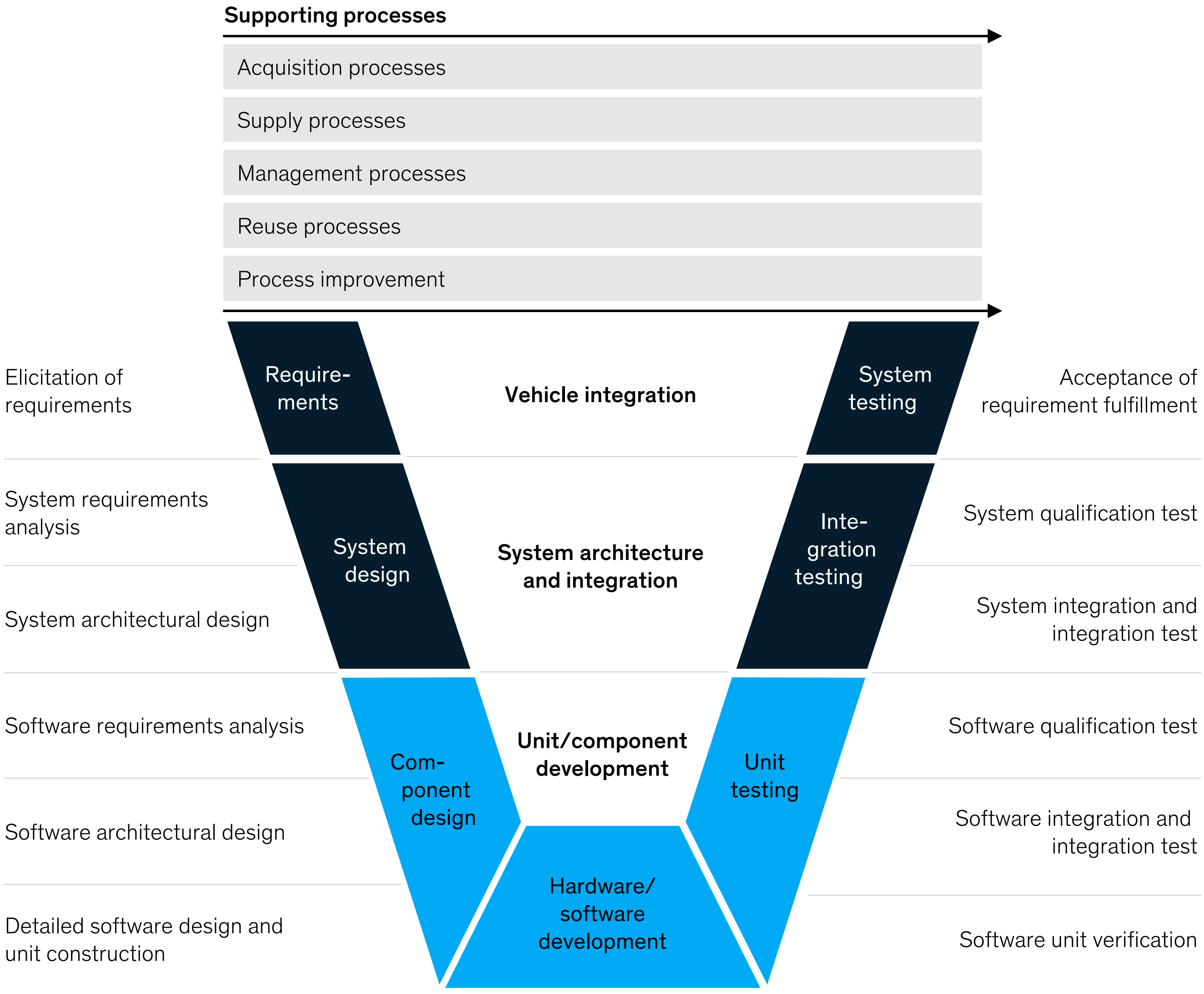
OEMs and suppliers will need to integrate cybersecurity measures throughout development – new talent and skills required

ILLUSTRATIVE

NON-EXHAUSTIVE

■ Development at vehicle level (OEMs)

🟦 Development at unit/component level (suppliers)


Supporting processes
Acquisition processes
Supply processes
Management processes
Reuse processes
Process improvement
Elicitation of requirements
Require-ments
Vehicle integration
System testing
Acceptance of requirement fulfillment
System requirements analysis
System design
System architecture and integration
Inte-gration testing
System qualification test
System architectural design
System integration and integration test
Software requirements analysis
Com-ponent design
Unit/component development
Unit testing
Software qualification test
Software architectural design
Software integration and integration test
Hardware/software development
Detailed software design and unit construction
Software unit verification

Source: McKinsey analysis, Automotive SPICE (A -SPICE®) framework

- Unit testing: Test the correct implementation of security requirements using software unit verification, software integration tests, and software qualification tests.
- Integration testing: Perform system integration and system qualification tests to ensure the correct implementation of the cybersecurity requirements.
- System testing: Perform acceptance testing of requirement fulfillment on the basis of a criteria catalog (e.g., derived from UNECE).

New capabilities and cybersecurity requirements along the development cycle will require significant reskilling and upskilling of the current workforce in many cases. The raising of skill requirements is also reflected in the market (see Section 4), where we see a variety of new products and services that all require new skills.

But even beyond the activities mentioned above, many other areas require upskilling. For example:

- The procurement of security components requires a more collaborative approach compared to the procurement of mechanical parts, e.g., chassis, powertrains, or batteries, where exact specifications can be detailed up front. Although specifications for security components can be laid out in the design phase, adjustments can be expected during the full development cycle. Due to the high complexity of cybersecurity, evaluating providers, especially for capabilities, will become much more challenging compared to sourcing physical parts or normal software.
- Project management must take security-by-design seriously and account for relevant cybersecurity-related activities and artefacts being part of the project, e.g., prioritizing cybersecurity in the product backlog.
- Dealerships, as the front line to automotive customers, will need to speak to cybersecurity matters (e.g., when reports of vulnerable cars or recent attacks are in the news) and must be able to assist in cybersecurity-related maintenance activities such as deploying software updates when over-the-air updates are not available.
- Customer communication teams will need to convey and communicate cybersecurity-related matters, like addressing public fears of cars being vulnerable to cyberattacks or navigating the challenging task of upholding external communication in case of a cybersecurity incident.

In the aviation industry, for example, some players have already built up new skills to address their cybersecurity needs. One leading aviation and defense company developed all of the above-mentioned skills internally. It has also built up SOCs to monitor its enterprise IT as well as its OT production. Going further, it’s even offering these services to the market, strengthening its position and credibility on the cybersecurity front.

3. Managing cyber risk throughout the vehicle lifecycle will require new working practices

Stricter cyber-risk management processes and compliance documentation

Stricter cyber-risk management processes and compliance documentation will need to be established. This includes management systems (cybersecurity management systems), and software update management systems, roles and responsibilities, and formal processes to assess and manage cyber risks for vehicles. Players should either adapt their existing management systems (e.g., quality management) or establish new systems, depending on their organizational structures and maturity.

So far, the role of vehicle cybersecurity (or product cybersecurity) has not yet been established by all OEMs in a way that fully reflects its multifaceted character at the intersection of quality, engineering, IT, software, procurement, and legal. The responsibility for cybersecurity is rather oftentimes assigned to functional domain owners, with basic functionality being provided by the OS and middleware. For enterprise IT, the role of a chief information and security officer overseeing the entire IT landscape is well established; a similar role is needed for vehicle cybersecurity. This can be achieved by either redefining the current information and security officer role or completely building a new cross-functional role.

Regulators, type-approval authorities, insurers, and business partners will likely demand more formal structures and processes, including diligent documenting. They will likely also require evidence of both the operational effectiveness of cybersecurity practices and OEM compliance with relevant regulatory requirements and standards (e.g., the UNECE WP.29 regulations or the ISO/SAE 21434 and ISO/AWI 24089 standards) in the future.

New ways of working and service levels between automotive value chain players ensure "security by design" for vehicles

As cybersecurity becomes relevant for type approval, OEMs will require their upstream partners, such as suppliers and semiconductor companies, to adhere to higher industry standards and follow new procedures. This will necessitate new contractual agreements. Adhering to regulatory requirements for process documentation will likely result in new forms of assessments, audits, and certifications; for example, independent third-party auditing of suppliers against emerging standards, such as ISO/SAE 21434 and ISO/AWI 24089. From a market perspective, this will likely create demand for implementation support as well as assessment and attestation services with respect to cybersecurity and software-update practices and their respective industry standards.

Ability to detect security incidents in the digital car ecosystem beyond the classical enterprise perimeter

OEMs will have to respond to security incidents as they occur. These incidents could take the form of everything from evidence of a new or potential vulnerability to even an actual attack on their vehicles. Automotive players will need new organizational, procedural, and technical capabilities to detect and respond to cybersecurity events in and around their vehicles:

- **Organizational capabilities** to embed cybersecurity in the DNA of the organization and establish practices to deal with cybersecurity topics in a diligent way.
- **Procedural capabilities** to monitor vehicles and the adjacent ecosystem components for security events based on the collection and analysis of log event data by a vehicle SOC and to respond to security events that cannot be resolved by typical tier-one and tier-two analysts inside the vehicle SOC.
- **Technical capabilities** for software inside vehicles and the digital car ecosystem that collects log events and feeds the vehicle SOC and security incident response team with information to detect anomalies and other adverse events (e.g., a vehicle intrusion detection system). Additionally, capacities for investigating root causes of anomalies need to be built up.

Furthermore, the blueprints of potential attacks will likely be sold by criminals to other criminals on the dark web. With this in mind, automotive players should also embrace the power and knowledge of global cybersecurity communities of white-hat hackers and security researchers and follow other industries in establishing bug bounty programs. Incentive and reward programs to encourage friendly hackers to report vulnerabilities they discover should be implemented to allow automotive players to fix issues before they are widely known and exploited with malicious intent.

As vehicles manufactured in one part of the world get sold in other parts, data privacy and privacy regulations must be accounted for. This leads to the potential requirement of region-specific versions of both software and vehicle SOCs.

The setup of vehicle SOCs and organizational anchoring is an open topic with no clear best practices as of now. For in-house vehicle SOCs, there are at least three options for anchoring the unit: (1) integrate it into the enterprise IT or OT SOC, (2) integrate it into the quality assurance unit, or (3) integrate it into the vehicle software R&D unit. Beyond these options, outsourcing the entire vehicle SOC either to an enterprise SOC service company or a dedicated vehicle SOC company is also an option. Lastly, there is also the option of creating a joint vehicle SOC service between multiple parties, increasing collective defense against cyber threats by sharing insights from recent attacks and joining forces to fight against potential future ones.

Time will tell which of these options will become the dominant setup. Initially, we believe that vehicle SOCs will be established internally to build up competencies and experiment with different models. Either way, we expect a growing market for vehicle SOC services over the next few years (see Section 4).

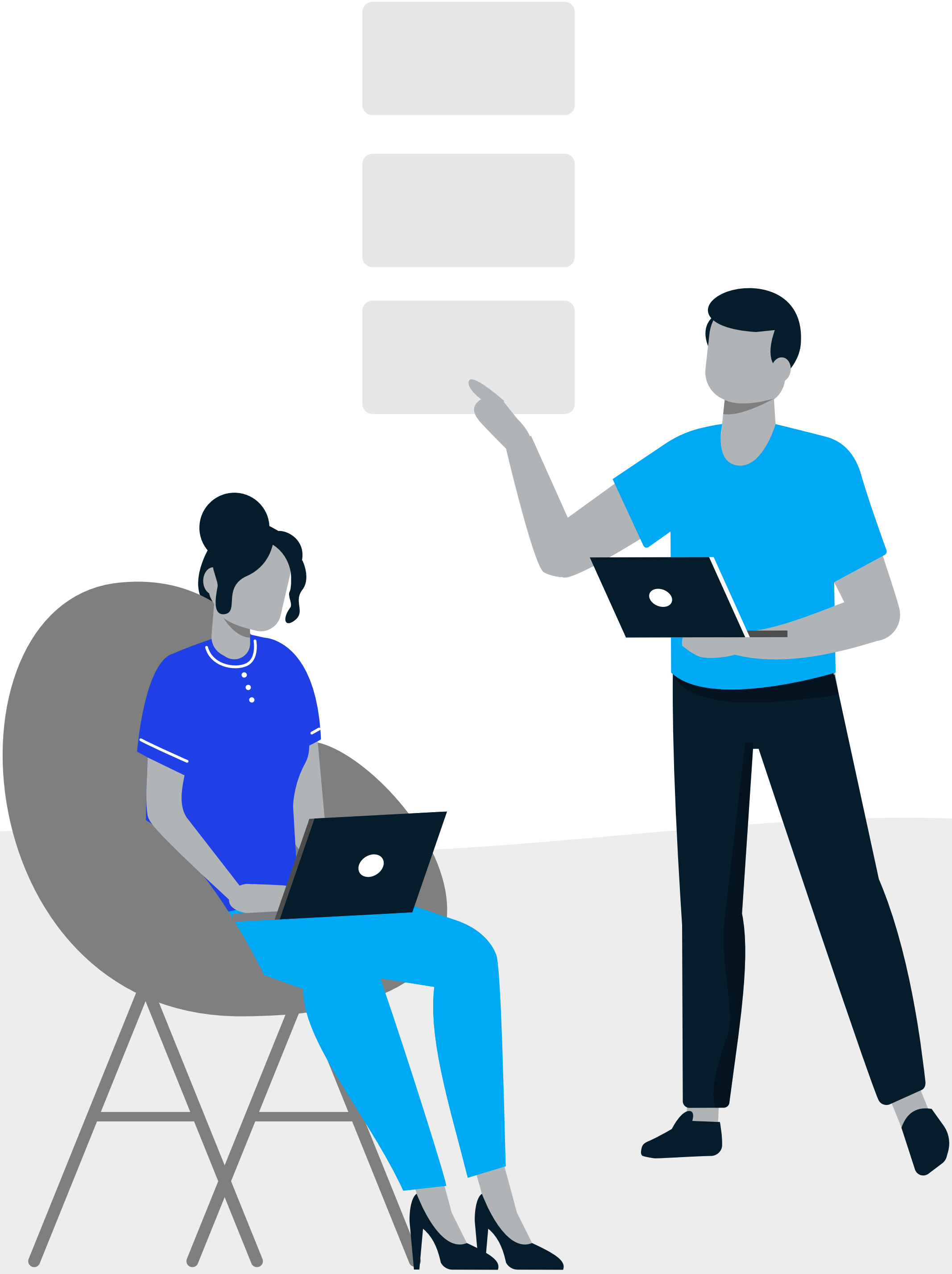
Service levels for providing security patches throughout the vehicle lifecycle

Providing security patches throughout the full vehicle lifecycle is essential for safe vehicle operation. Vehicles are often driven for ten years or even longer, requiring regular updates over a very long period. This makes vehicles more akin to aircrafts or vessels, which see software updates provided over longer periods, contrary to updates for consumer products like PCs, smartphones, tablets, or smart appliances.

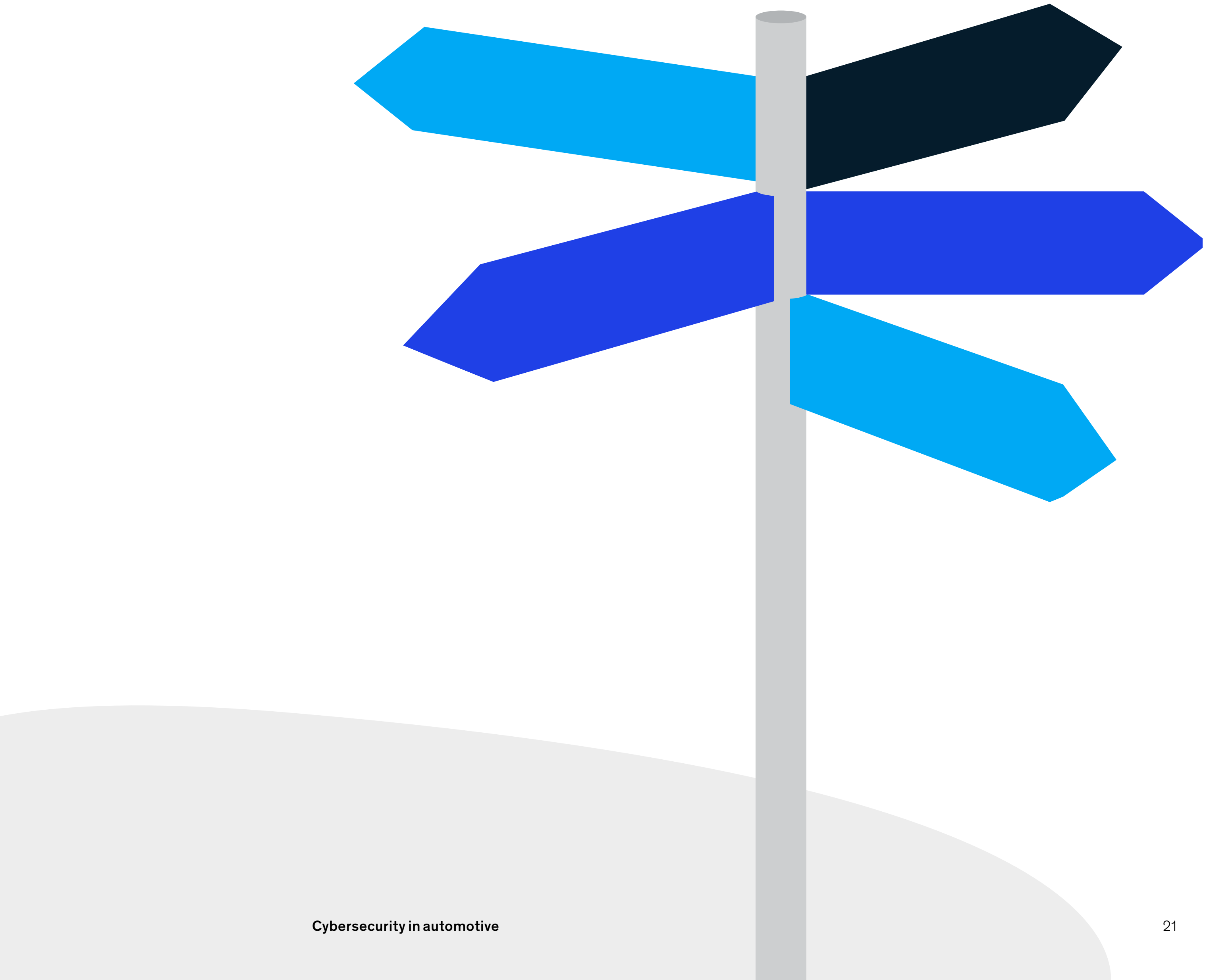
The industry will need to adapt to a long-life vehicle operating system and solid software architecture to master complexity and be able to provide new software releases and updates over many years. This means, for example, that the contractual relationship between OEMs and suppliers must clarify who is providing which software updates over which period. Work on the ISO/AWI 24089 standard, which will address software update management, has recently started and will provide guidance on update requirements.

Examples from the PC and smartphone business show that security updates are essential for safe device operation. Today, for example, the initial release of Windows XP is unsecure and infected within minutes after establishing an internet connection.[5] For cars, security updates are even more important since attacks could put the lives of drivers, passengers, and others at risk. In addition to the human cost, the price point of a vehicle is much higher than that of a smartphone, so consumer expectations of software patches throughout a vehicle's lifetime will likely be high.

[5] SANS Internet Storm Center, survival time. Retrieved from https://isc.sans.edu/survivaltime.html on March 9, 2020



4. Automotive executives should prepare their cybersecurity strategy



Perspectives on market size and opportunities for automotive cybersecurity

We have broken down the automotive cybersecurity market into three elements: cybersecurity hardware, cybersecurity-related software development efforts, and cybersecurity processes and solutions. Based on external expert interviews, McKinsey analysis, and predictive modeling of the automotive software market, we have created a market forecast for automotive cybersecurity until 2030. We expect the market to grow from USD 4.9 billion in 2020 to USD 9.7 billion in 2030, corresponding to annual growth of over 7 percent (see Exhibit 6). This is in line with the growth of the total market for automotive software and hardware. We expect to see a significant amount of change, in these areas in particular:

— **OEMs** are pursuing vertical integration, e.g., by building their own cybersecurity components or **even** software stacks.

— **Suppliers** are pushing their way up and down the value chain, e.g., by offering specialized cybersecurity consulting services.

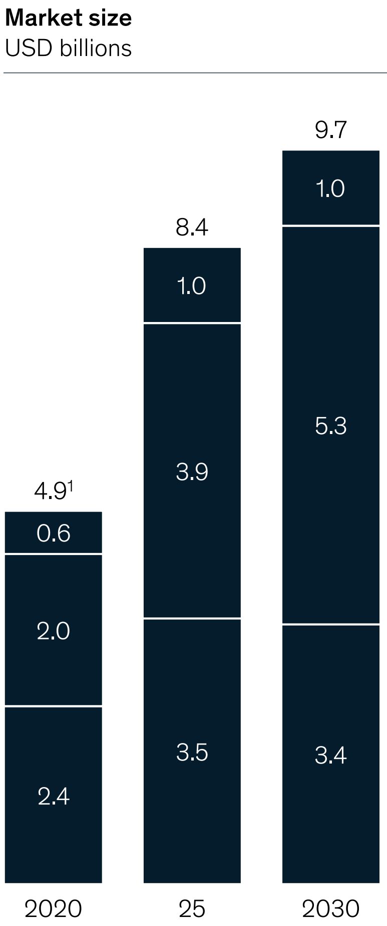
— **Start-ups** are entering the market with innovative solutions, e.g., specialized threat detection applications or vehicle SOCs as a service.

— **IT and OT companies** are expanding into the adjacent automotive cybersecurity market, e.g., by offering back-end solutions or cybersecurity components.

— **Semiconductor companies** are pushing their way up the value chain, e.g., by providing software that's optimized for their chips.

Exhibit 6

The cybersecurity market will grow significantly for automotive in the coming years



Submarket	CAGR 2020-30	
Total	7%	
Cybersecurity hardware components	6%	Dedicated security components for encryption and key storage (eHSM and TPM)
Cybersecurity-related software development efforts	10%	Implementation of cybersecurity components (e.g., encryption functionality) and requirements in functional domains Integration and testing of cybersecurity components and additional effort due to cybersecurity requirements in functional domains
Cybersecurity processes and solutions	4%	Efforts to implement new regulatory requirements Software traceability (inventory and compatibility management, and impact assessment) Risk management and incident response Vehicle monitoring using SOCs

[1] Sum does not add up due to rounding

Source: Analysis based on data from "Automotive software and electronics 2030 – mapping the sector's future landscape," McKinsey, 2019

Cybersecurity hardware components
There are currently two types of dedicated security components for security algorithms and key storage:

- Embedded hardware security module (eHSM): offers basic functionality
- Trusted Platform Module (TPM): provides more power and flexibility than an eHSM.

These hardware modules are already integrated into some ECUs. We expect an increasing penetration of these modules until 2024, when every ECU will have either an eHSM or a TPM. The choice between the two is determined by an ECU's required performance and flexibility. We note that the additional software requirements for security also lead to slightly higher needs for computing power and memory. This effect is excluded from our model since it increases the market for general chips, but has no effect on dedicated security elements.

The hardware security market is expected to grow until 2025 and then remain flat until 2030. This is driven by three predictions:

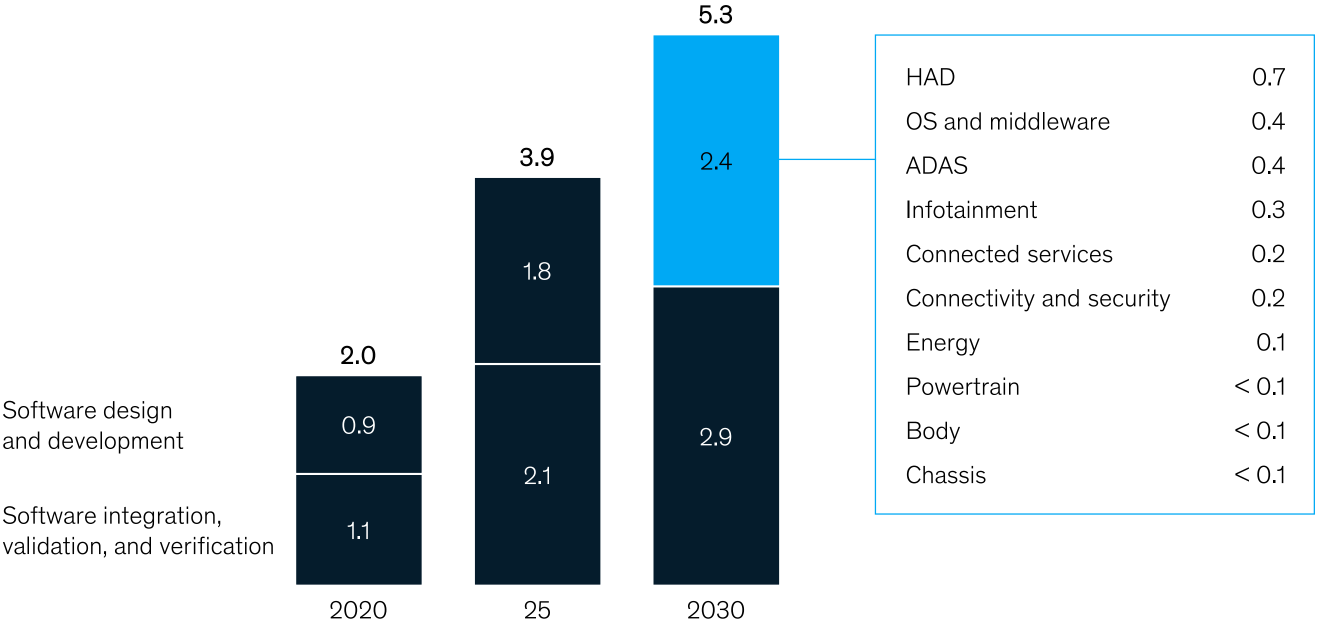
- **Higher ECU sales.** The total number of ECU sales will increase until 2025 and then remain flat afterwards. Increasing connectivity and software features will lead to an increase in the number of ECUs per car, while the consolidation of ECUs within the car balances the increase in the number of ECUs.
- **Security-module market saturation.** The penetration rate of hardware security modules will also reach saturation around 2025, corresponding to the expectation that the UNECE WP.29 regulations on cybersecurity and software updates will be enforced in 2024.
- **Modest increases in hardware prices.** The cost of security hardware is not expected to increase significantly. Higher performance and new features are expected to compensate price declines due to high volumes and optimized production.

We expect the market to stay in the hands of the incumbent semiconductor companies, but there are also opportunities for OEMs or suppliers to enter the market if hardware security modules become an important differentiating factor. Similar behavior has already been observed in other markets; for example, a leading automotive OEM has developed its own specialized chips for autonomous driving. In the consumer space, a few OEMs have developed their own system-on-chip – some systems-on-chips even include dedicated security components.

Exhibit 7

The software development market is expected to reach USD 5.3 bn by 2030, driven by ADAS/HAD but also OS and middleware

Cybersecurity-related software development effort market size
USD billions



HAD	0.7
OS and middleware	0.4
ADAS	0.4
Infotainment	0.3
Connected services	0.2
Connectivity and security	0.2
Energy	0.1
Powertrain	< 0.1
Body	< 0.1
Chassis	< 0.1

Source: Analysis based on data from "Automotive software and electronics 2030 – Mapping the sector's future landscape," McKinsey, 2019.

Cybersecurity-related software development
Software is the second key element for making cars secure. We describe our perspective on this aspect of the automotive cybersecurity market with two categories in mind:

- **Software design and development.** Market players must specify requirements and design components and develop the actual software for cybersecurity components as well as functional components for meeting security requirements.
- **Software integration, validation, and verification.** Market players must bring together software subsystems into a larger system (ECU/DCU but also at the vehicle level) and ensure that the developed functions meet specifications and fulfill their purposes consistently and reliably. This includes efforts for integrating and testing cybersecurity elements but also additional efforts for integrating and testing functional components due to enhanced security requirements.

For both categories, we look at two main subcomponents: operating systems and middleware, and functional domains.

Operating systems and middleware require the implementation of many security functionalities, including secure protocols, identity and access management, intrusion detection, and abstraction layers for crypto functions. These functionalities are then used by the functional domains (described below) to secure communications and avoid the creation of backdoors.

All **functional domains** need to be secured as well, but many of them can almost fully rely on the security functionality provided by the operating system and middleware. The most important areas needing additional security effort are ADAS and HAD, infotainment, and connectivity and security.

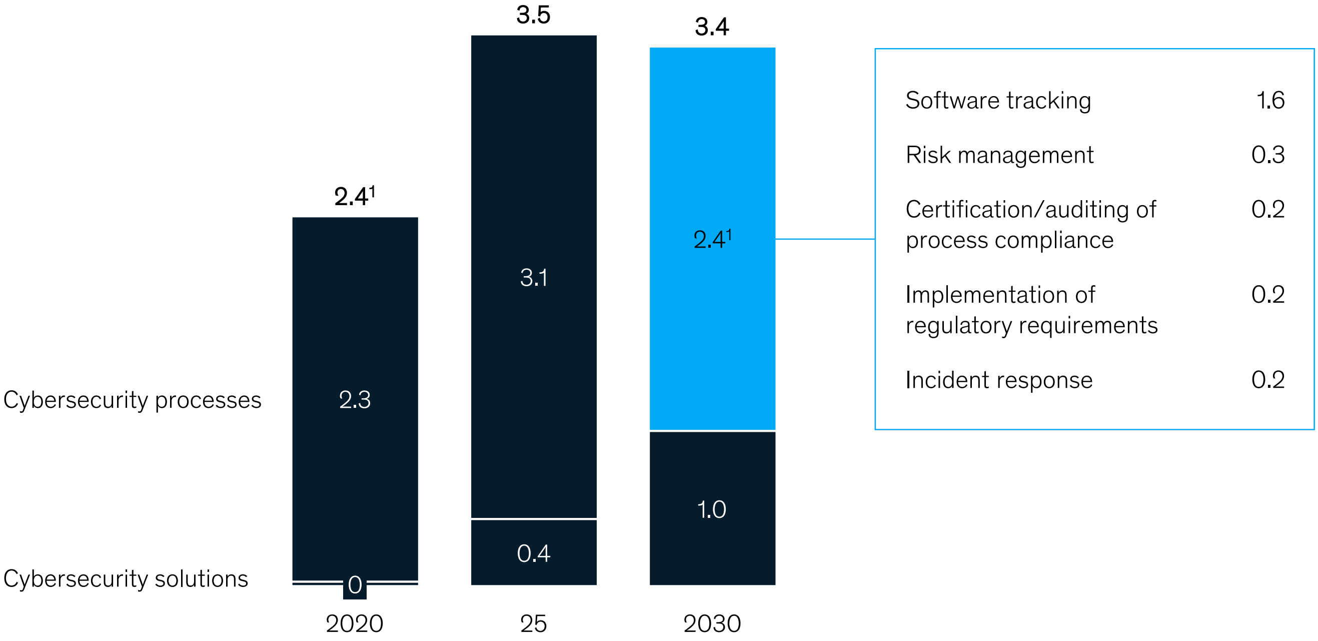
The software development market is expected to grow steadily at about 10 percent per year over the next few years to reach USD 5.3 billion in 2030 (see Exhibit 7). We expect to see a significant amount of competition – across player archetypes – related to ADAS and HAD in the automotive software market in general, and in the cybersecurity software market in particular.

Cybersecurity processes and solutions
Combined, the cybersecurity processes and solutions market – including both the personnel and tooling required to perform the activities – is expected to reach USD 3.4 billion by 2030 (see Exhibit 8). In the following, we break down this market into its two submarkets:

Exhibit 8

The cybersecurity processes and solutions market is mainly driven by software tracking; strong growth for vehicle SOCs is expected

Cybersecurity management and vehicle monitoring market size
USD billions



Software tracking	1.6
Risk management	0.3
Certification/auditing of process compliance	0.2
Implementation of regulatory requirements	0.2
Incident response	0.2

[1] Sum does not add up due to rounding

Source: Analysis based on data from "Automotive software and electronics 2030 – Mapping the sector's future landscape," McKinsey, 2019.

Cybersecurity processes includes activities related to software tracking, risk management, regulatory requirements, certification/auditing of process compliance, and incident response. The market size will peak around 2025, driven by customers, quality expectations, and increased cyber threats, but also by the new UNECE WP.29 regulations on cybersecurity and software updates. Following initial investments to achieve compliance, investment and scaling efforts are expected to go down.

- **Software tracking.** The regulation lays out three requirements regarding traceability: i) inventory management of components and all software versions for each component, ii) verification of compatibility between different component versions in light of a software update, and iii) assessment of impact on safety-relevant components in light of a software update.
- **Risk management.** The upcoming regulation and standards will lay the foundation for developing and implementing risk guidelines. Regular evaluations will be needed to ensure that employees are following risk-management guidelines.
- **Implementation of regulatory requirements.** Automotive players must operationalize and adhere to the minimum requirements laid out in the respective regulations (e.g., UNECE WP.29) and industry standards (e.g., ISO/SAE 21434 and ISO/AWI 24089). This results in higher rigor, more functional requirements, and bigger investments – both upfront and ongoing – along the development lifecycle. Action on this front will take the form of more robust engineering requirements and architectural design with inherent security features.
- **Certification/auditing of process compliance.** Certification bodies will testify OEM compliance with industry standards and regulations.
- **Incident response.** Responses include analyzing anomalies, triggering the resolution of issues by the software R&D team, pushing software updates to the vehicles or back end, and managing communication with affected car owners. We assume that issues can be fixed via over-the-air updates and that fleet recalls will not be necessary.

Cybersecurity solutions involve vehicle SOCs, which monitor anomalies in connected vehicles (see text box). OEMs can either build and run SOCs in house or source them through external vendors, e.g., as a managed service. Vehicle SOCs need specialized personnel to operate them and deal with car security incidents.

The cybersecurity processes and cybersecurity solutions markets offer many opportunities to create new business. The area of process compliance will offer opportunities for testing, inspection, and certification providers across all subcategories.

Monitor and monetize – the concept and business opportunity of vehicle SOCs

SOCs are already well-established concepts in the enterprise IT world, but a relatively new concept for automotive software. Vehicle SOCs monitor anomalies in car systems, which are detected by intrusion-detection sensors within the car.

These sensors can, for instance, inspect data traffic on communication buses, monitor software processes, or track input/output operations of ECUs. The SOC is alerted to any detected anomalies, which are analyzed by specialists to distinguish between real threats and false positives. Incident management is triggered in the event of a confirmed attack, with countermeasures taken if needed, e.g., over-the-air updates.

Vehicle SOCs are still in their infancy. Their development requires answers to many questions, especially around pricing and support periods. The cost for fixing vulnerabilities or defending against attacks can vary extremely and is part of the "incident response" category. For the end consumer, support by an SOC and regular security updates to their vehicle's software over its full lifetime will become essential.

The market will present a wide range of opportunities over the next few years: from providing expertise, to offering tool support, to operating SOCs as a service. Given the importance of security updates and the monitoring of vehicle ECUs and DCUs, OEMs might see SOCs as an opportunity for generating additional revenue by charging a yearly fee after some years. This would be in line with the pricing model of already existing subscription services like traffic information or premium connectivity. But it remains to be seen whether OEMs will take this path or choose to provide lifelong services at no additional charge.

Strategic partnerships bring different automotive players together, joining forces on a variety of capabilities

Cybersecurity is very complex, and no company will be able to do everything on its own. Thus, partnerships will become essential, and we already see various kinds. The capabilities at the heart of current partnerships between automotive players and cybersecurity firms include:

- Manage vehicle cyber risks
- Secure vehicles by design
- Detect and respond to security incidents
- Provide safe and secure software updates
- Penetration testing and consultant services.

Our analysis of over 20 partnerships reveals the following insights (see Exhibit 9):

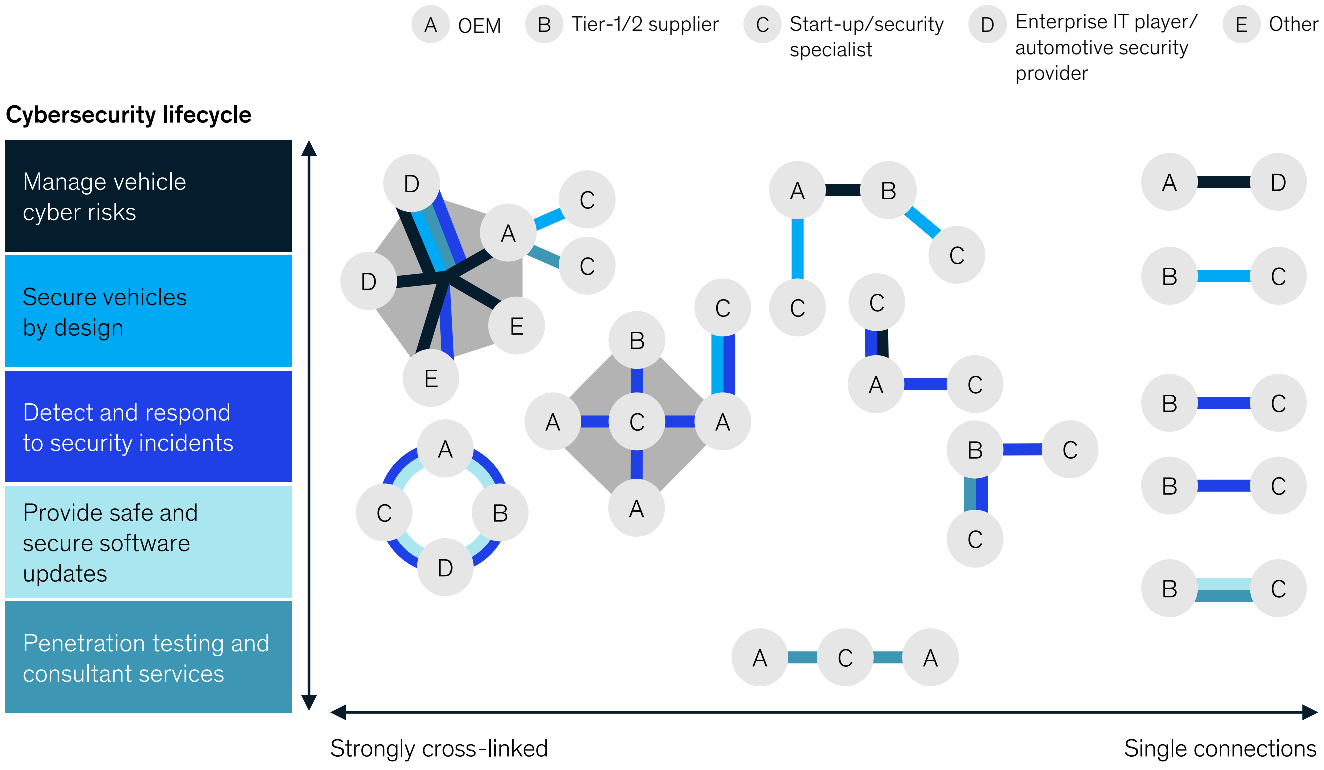
- Most partnership are between incumbent OEMs or tier-one/tier-two suppliers and start-up companies or security specialists.
- We don’t see and don’t expect large, interlinked networks, as is the case with autonomous driving.
- The partnerships cover all elements of cybersecurity capabilities.
- We see very few IT or OT cybersecurity companies entering the vehicle cybersecurity market. Possible reasons might be the latter’s much smaller market size compared to the IT and OT cybersecurity market, or limited synergies due to the very different approaches to cybersecurity on a detailed level.
- Cybersecurity hardware business seems to remain with the incumbent semiconductor players, since we are not seeing any cybersecurity chip companies.

These partnerships offer OEMs and tier-one/tier-two suppliers access to cybersecurity products, services, and skills, but it will be key for them to build up cybersecurity knowledge internally. Every player must have deep cybersecurity architecture knowledge for its area of business, and its applications need to be secured individually. This can only be achieved if cybersecurity becomes an integral part of the culture.

Exhibit 9

Today’s automotive cybersecurity landscape is interlinked with a broad variety of collaboration models

ONLY SELECTED PARTNERSHIPS SHOWN



A OEM
B Tier-1/2 supplier
C Start-up/security specialist
D Enterprise IT player/ automotive security provider
E Other
Cybersecurity lifecycle
Manage vehicle cyber risks
Secure vehicles by design
Detect and respond to security incidents
Provide safe and secure software updates
Penetration testing and consultant services
D
C
A
C
D
E
E
A
C
B
D
C
B
A
C
A
A
A
B
C
C
C
A
C
B
C
C
A
C
A
A
D
B
C
B
C
B
C
B
C
Strongly cross-linked
Single connections

Source: McKinsey analysis; press research

The need for partnerships is expected to open doors for start-ups, which normally would experience large market entry barriers; that is, the start-ups are too small for OEMs and tier-one suppliers to establish relationships with them. OEMs and tier-one suppliers often require a minimum size and business volume to ensure economic stability of business partners and keep the number of partners manageable.

We are already seeing many acquisitions, joint ventures, and collaborations between start-ups and OEMs/tier-one suppliers, and more are expected.

Getting started with navigating the changing industry landscape – pragmatic recommendations

For all players, it is important to get oriented early and define a strategy, but the strategic priorities, opportunities, and considerations will vary depending on where a company sits along the value chain. Potential pragmatic first steps for all players include:

Impact assessment. All automotive players should assess the impact of the new UNECE WP.29 regulations on their processes and business. This is necessary to ensure approvals of new vehicles types by OEMs after enforcement of the regulation begins (experts expect the EU to demand compliance starting in 2022 for new vehicle types and in 2024 for all vehicle types).

Capability mapping. Using a capability map, all players can identify areas of strength as well as areas for improvement, and define concrete needs. The needs can either be addressed by building up skills internally or sourcing them externally.

Prioritized implementation. Identified capability gaps need to be prioritized and critical paths for implementation must be outlined. In view of tight timelines, multiple new vehicle projects on the way, and numerous stakeholders, prioritization will be a key success factor, next to building up the required skills and workforce.

A company's understanding of both its internal strengths and the impact of regulation on its business set it up to identify potential business opportunities that arise from the evolution of cybersecurity. Potential opportunities include a range of products or offerings that could be developed and delivered to the market – this is especially true for suppliers. It is important to realize that not all aspects of the cybersecurity market will be accessible to all players. For example, the hardware business is expected to remain in the hands of semiconductor players for the foreseeable future.

In the following, we list selected areas which we believe will provide opportunities for a variety of players, including for those who have not yet been active in the automotive industry:

- **Vehicle SOCs.** The market for vehicle SOCs will emerge over the next few years. Similar to enterprise IT SOCs, we expect to see third-party vehicle SOCs, and software companies offering products to operate these SOCs.
- **Testing, inspection, and certification.** Like all other auditing, the cybersecurity auditing market will be in the hands of third parties. We expect to see a variety of companies become active in this market over the next few years, e.g., the big four accounting firms and firms specializing in auditing and certification.
- **Software components.** The whole industry will be in need of security components, e.g., encryption algorithms, key management, and intrusion detection. Since it will be difficult to develop them all from scratch, there will be a market for ready-to-use software components as well as innovative solutions.
- **Software engineering and lifecycle tooling.** The productivity of software developers and testers can be significantly increased with the right tooling, and given the efficiencies to be gained, companies would likely be willing to pay for excellent products. There is a variety of tools that can help security specialists, including penetration-testing tools, software version management tools, and software tracking tools.
- **Innovative start-ups.** These will also try to access these markets but will likely face significant barriers to entry. Due to their size, it will be hard for start-ups to approach OEMs directly. They need to search for other ways to get access to OEMs, such as going through OEMs' venture capital funds or by partnering with suppliers.

Outlook

Cybersecurity has already gained the attention of automotive companies and will trigger a paradigm shift as companies need to start now to address customer demands, meet quality expectations, manage increasing cyber risks, and become compliant with the UNECE WP.29 regulations on cybersecurity and software updates. This requires a rethinking of cybersecurity and new working practices along the value chain. Cybersecurity will become nonnegotiable in the long run, and these trends create opportunities for all players to either differentiate themselves or generate additional business with new offerings. We are excited to see many new partnerships, fresh trends, and innovative products and services.

Appendix

How we derived the insights presented in this report

The insights of this report were generated by closely linking qualitative and quantitative research. To gain qualitative insight, we conducted interviews with industry experts. These interviews were complemented by workshops jointly organized by the Global Semiconductor Alliance (GSA) and McKinsey. The insights were then used to create a market model for cybersecurity in automotive and served as a basis for our qualitative findings.

For our quantitative market insights, we built bottom-up market models for each of the core components within the automotive cybersecurity market:

- Hardware (embedded hardware security modules (eHSMs), Trusted Platform Modules (TPMs))
- Software development (operating systems and middleware, functional domains)
- Services (engineering services, process compliance services, vehicle security operations center (SOC) services)

Further details on and results of the market models are presented in Section 4. Details on the methodology are provided in this section.

Key aspects of the market model

Within these models, we distinguish between the following domains: ADAS, body, chassis, connected services, connectivity and security, energy, HAD, infotainment, middleware, OS, and powertrain.

The base data of all three models in our report builds on the data of a previous McKinsey report from 2019: “Automotive software and electronics 2030 – mapping the sector’s future landscape.”

We gained the quantitative market insights in this earlier report by building bottom-up market models for each of the core components within the automotive software and E/E market. In addition, we further validated our data and findings by integrating findings from market research companies such as Strategy Analytics and IHS Markit.

In the 2019 report, the number of vehicles produced each year is provided in a separate model, incorporating data from the latest McKinsey Center for Future Mobility market outlook and scenario analysis, and the McKinsey EV market model.

Cybersecurity hardware components market model
The hardware model uses the report’s prediction of the number of ECUs and DCUs installed by 2030. Each ECU will be assigned an eHSM and each DCU will be assigned a TPM. A ramp-up curve until 2024 ensures a smooth increase of numbers.

Cybersecurity-related software development efforts market model
The software development model uses total automotive software development spend as its main input. For each domain, we collaborated with industry experts to assess the share of cybersecurity within this market. The results are again modeled on a smooth ramp-up curve showing the increase in software development investments over the next several years.

Cybersecurity processes and solutions market model

Cybersecurity processes. This portion of the model analyzes software tracking, the implementation of regulatory requirements, risk management, incident response, and certification/auditing of process compliance. The scope of these buckets has been described above.

— Software tracking and the implementation of regulatory requirement buckets only contain efforts related to or caused by cybersecurity and are both calculated using the same logic as for engineering services, except that the ramp-up curve peaks at around 2021/2022 and saturates at a lower value, modeling the higher initial effort during those years.

— Risk management and incident response are calculated as a share of the software developer workforce. Again, a smooth increase over the next several years is assumed.

— The certification and audit efforts follow the same logic as incident management, except that we expect a peak in effort in the next few years with a lower steady state afterwards.

Cybersecurity solutions. The solutions market contains vehicle SOCs, and its market size is based on the total number of new vehicles, the monitoring cost per vehicle and year, and the adoption rate of vehicle SOCs. The total number of new vehicles is taken from the 2019 McKinsey report. Again, a smooth adoption rate with a steady state of 100 percent after 2024 is assumed. We estimated a service time frame of at least ten years; that is, no cars will reach the end of its lifetime until 2030.

To pressure-test the results of our modeling, we conducted a series of interviews with Global Semiconductor Alliance members in North America, Europe, and Asia. Based on their feedback, we iterated the models towards the version presented in this report.

List of abbreviations

ACES	Autonomous driving, connected cars, electric vehicles, and shared mobility
ADAS	Advanced driver-assistance systems
DCU	Domain control unit
ECU	Electronic control unit
eHSM	Embedded hardware security module
E/E	Electrical/electronic
HAD	Highly automated driving
IP	Intellectual property
IT	Information technology
OEM	Original equipment manufacturer
OS	Operating system
OT	Operations technology
R&D	Research and development
SOC	Security operations center
TPM	Trusted Platform Module
UNECE	United Nations Economic Commission for Europe

Contacts and authors

Ondrej Burkacky is a partner in
McKinsey's Munich office.
Ondrej_Burkacky@mckinsey.com

Johannes Deichmann is a partner in
McKinsey's Stuttgart office.
Johannes_Deichmann@mckinsey.com

Benjamin Klein is a specialist in
McKinsey's Berlin office.
Benjamin_Klein@mckinsey.com

Klaus Pototzky is an engagement manager in
McKinsey's Munich office.
Klaus_Pototzky@mckinsey.com

Gundbert Scherf is a partner in
McKinsey's Berlin office.
Gundbert_Scherf@mckinsey.com

The authors wish to thank Charlotte Mewes, Florian Haubner, Georg Doll, Patrick Keuntje, Stephanie Brauckmann, and Wolf Richter for their contributions.

Important notice

McKinsey is not an investment adviser, and thus McKinsey cannot and does not provide investment advice. Nothing in this report is intended to serve as investment advice, a recommendation of any particular transaction or investment, any type of transaction or investment, the merits of purchasing or selling securities, or an invitation or inducement to engage in investment activity.

Advanced Industries – Automotive & Assembly
March 2020

Designed by Visual Media Europe

www.mckinsey.com

@McKinsey
@McKinsey