

Pedal to the Metal – How to Navigate the Way to Automotive Cybersecurity

PwC's Global Automotive Cyber Security
Management System Survey 2022

Pedal to the Metal – How to Navigate the Way to Automotive Cybersecurity

Published by PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft

Survey Project Manager: Bennet von Skarczynski

Contribution by James Hunt, Johanna Jefremow, Henning Kruse, Tobias Franz Langkau, Joachim Mohs, Sebastian Nagel, Manuel Schulte, Maike Schulz, Bennet von Skarczynski, Phil Swarbrick, Grant Waterfall and Harald Wimmer

May 2022, 32 pages, 17 figures, soft cover

All rights reserved. This material may not be reproduced in any form, copied onto microfilm or saved and edited in any digital medium without the explicit permission of the editor.

This publication is intended to be a resource for our clients, and the information therein was correct to the best of the authors' knowledge at the time of publication. Before making any decision or taking any action, you should consult the sources or contacts listed here. The opinions reflected are those of the authors. The graphics may contain rounding differences.

PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft adheres to the PwC-Ethikgrundsätze/PwC Code of Conduct (available in German at www.pwc.de/de/ethikcode) and to the Ten Principles of the UN Global Compact (available in German and English at www.globalcompact.de).

© May 2022 PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft. All rights reserved. In this document, "PwC" refers to PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft, which is a member firm of PricewaterhouseCoopers International Limited (PwCIL). Each member firm of PwCIL is a separate and independent legal entity.



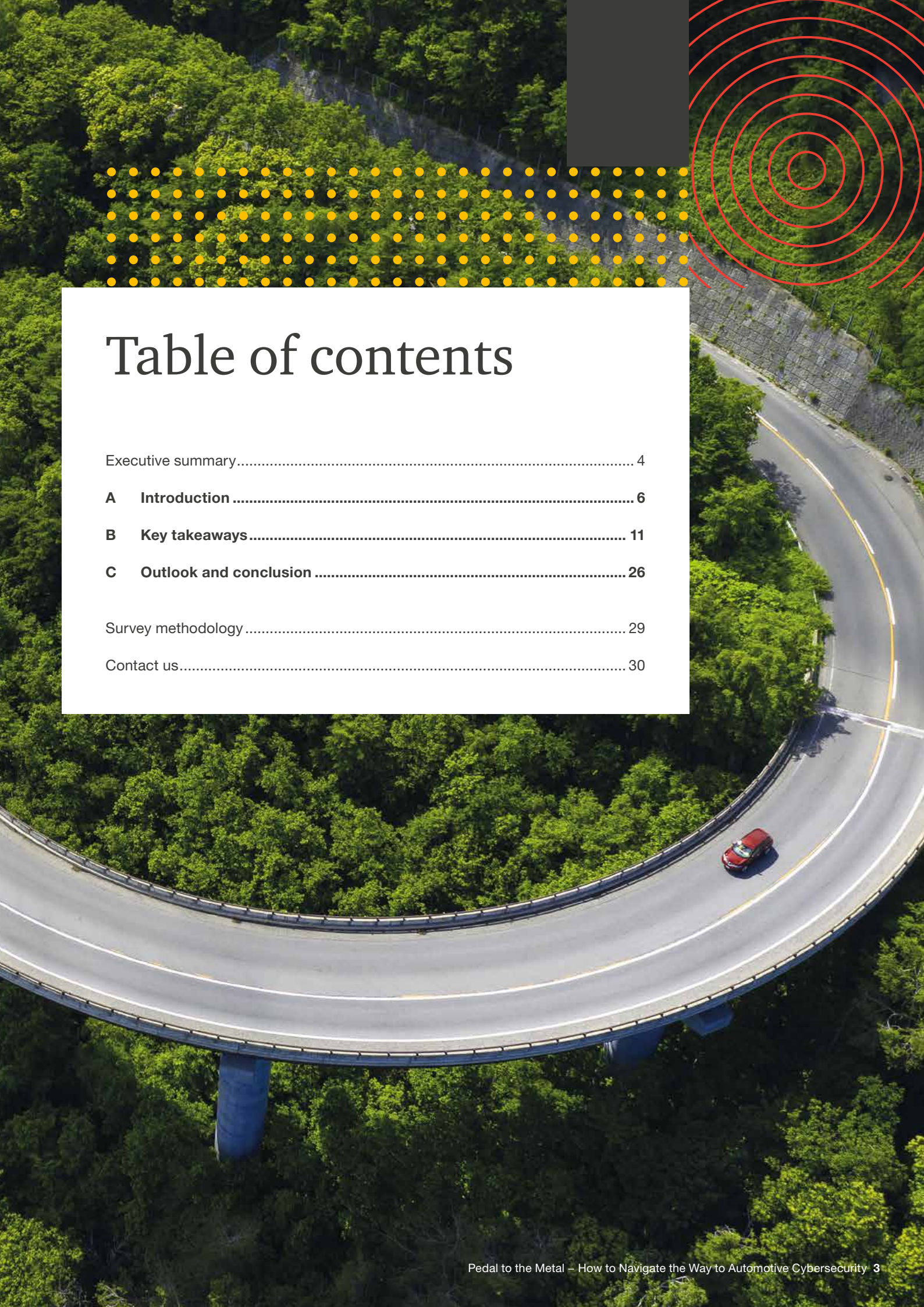
An aerial photograph of a winding asphalt road through a dense green forest. The road curves from the bottom left towards the top right. A red car is visible on the road. In the top left, there is a grid of yellow dots. In the top right, there are concentric red circles. A dark grey rectangle is also present in the top right area.

Table of contents

Executive summary.....	4
A Introduction	6
B Key takeaways.....	11
C Outlook and conclusion	26
Survey methodology	29
Contact us.....	30

Executive summary

100%

of interviewees expect cyberattacks on vehicles and the entire automotive ecosystem to increase dramatically.

91%

of respondents stated that security management systems from OEMs and suppliers must grow even closer together.

89%

of OEMs agree that high cybersecurity maturity will be a distinct competitive advantage for selling vehicles in the future.

Welcome to PwC's Global Automotive Cyber Security Management System (CSMS) Survey 2022. It provides a detailed and up-to-date benchmark of major trends, threats and technological solutions related to this topic in the automotive sector.

In March and April 2022, we interviewed representatives from across the automotive industry. This included interviewees from original equipment manufacturers (OEMs) and suppliers, along with market experts. The interviewees were based in 11 different countries, with roles ranging from product security to R&D and quality management, information security, production and IT – all actively involved in vehicle cybersecurity management. They shared real-world insights into how regulations and expectations are shaping measures to fight cybersecurity risks in the automotive sector. They also described their journeys so far, the problems they currently face, and their thoughts about the future.

Technological developments, as well as the rising popularity of connected and autonomous driving, is making people, vehicles and companies vulnerable in completely new ways. New regulations are seeking to prevent security concerns for the automotive vehicle ecosystem. However,

regulations vary across regions and often lack detail about exactly how to implement measures to tackle cyber threats. That's why more far-reaching guidelines, and above all a holistic business strategy that goes beyond them, are indispensable. And businesses that successfully anticipate and adapt will gain a significant advantage.

The results from this survey show that companies at every stage in the automotive value chain are now taking action to implement a CSMS – but mainly in design and with a low level of maturity. Moreover, these activities are placing big demands on time and money. There is a lack of transparency between players in this industry and approaches are inconsistent.

Respondents to our survey broadly agreed that connected and autonomous driving will lead to major changes in market share, with new players entering the market and established players forced to adapt quickly. Our survey demonstrates that the automotive ecosystem is threatened by cyber risks. A CSMS, however, protects the vehicle ecosystem, which is constantly growing in terms of scope, complexity and the parties involved. This makes the CSMS very business-critical from three points of view.

Firstly, a CSMS not only protects people but also the basis for substantial future revenues and new data- and service-driven business models centred around the new living and working place: the car.

Secondly, continuously operated cybersecurity has a significant impact on vehicle costs. A smart CSMS in combination with a modular and scalable software architecture will determine how cost-efficiently the ecosystem can be operated throughout its life cycle.

Thirdly, a CSMS is and will continue to be a basic requirement for vehicles to be registered and produced in many markets worldwide. Violation of compliance requirements can lead to the revocation of operating licences for entire vehicle fleets, and to the threat of fines and major legal disputes.

Despite all this, CSMS is just one milestone on the road to a successful digital transformation. OEMs and

suppliers will need to transform their cyber programs much more interconnected, while focusing on consumer trust.

The top priority of the management is to implement a culture that builds cybersecurity into the core of the business as well as embedding cyber risk management into corporate risk management.

Only those who combine a holistic view of regulatory requirements with a true business motivation will win the race.

The course has been set. Any company hoping to enjoy success in this market must keep up with the pace of the automotive transformation.

Overall, there's a long and winding road ahead to achieve secure and efficient automotive ecosystems – and it will take teamwork, speed and navigation skill to reach that destination.

PwC's Global Automotive CSMS Survey 2022 takes a close look at how businesses in this industry perceive the field of cybersecurity – and how they're responding. Find out what companies are doing now and how they're preparing for the future.

A | Introduction

The automotive industry is evolving rapidly. Consumers have embraced connected vehicles. And as related technologies develop, fresh expectations are developing too. Regulations for connected vehicles are emerging at different rates in different regions, markets and countries. This shift is creating a completely new set of guiding principles – and is reshaping the automotive sector.

OEMs and suppliers face unparalleled disruption, while also attempting to tap into incredible new opportunities for the future of mobility. Success will require fast and far-reaching changes to existing models of product development, supply chain and value chain management, and the way vehicles are maintained and serviced throughout their life cycles. Companies will need to embark on a journey of transformation for their production processes, digital technologies and workforces. Thus, the vehicle ecosystem is constantly expanding, generating new opportunities, but also growing in complexity and risk exposure.

People, vehicles and companies are now vulnerable in completely new ways. Hackers have already remotely seized control of door locks, brakes and accelerators in cars. Denial-of-Service (DoS) attacks have hit cars too, targeting key components and functions like the vehicle-distancing system, which stops cars from driving dangerously close to each other.

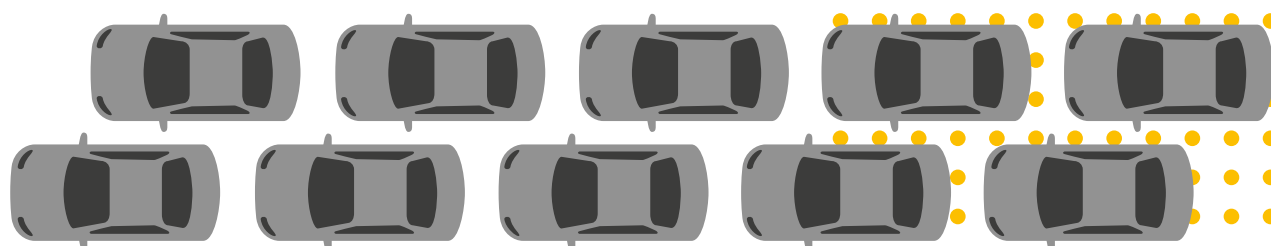
But what would happen if cyber criminals took control of a city's police fleet and committed a crime while officers were unable to respond? Or if cameras for driver anti-sleep devices were hacked and the victim's grumpy Monday-morning face got posted online? Or if a faulty update for an automated lane-keeping assistant got installed on thousands of vehicles?

New regulations are seeking to prevent security concerns like these. In some markets, there are already local regulations with a focus on cybersecurity management systems for vehicles. These regulations differ in their scope, level of detail and timings for implementation. The United Nations Economic Commission for Europe (UNECE) recently introduced regulation No. 155 (CSMS – Cyber Security

Management Systems) and announced regulation No. 156 (SUMS – Software Update Management System), which will be binding in 56 countries. Many producers are adopting the requirements of ISO/SAE 21434 (Road vehicles – Cybersecurity engineering), which covers cybersecurity for road vehicles. Other standards are under development, such as ISO/DIS 24089 (Road vehicles – Software update engineering).

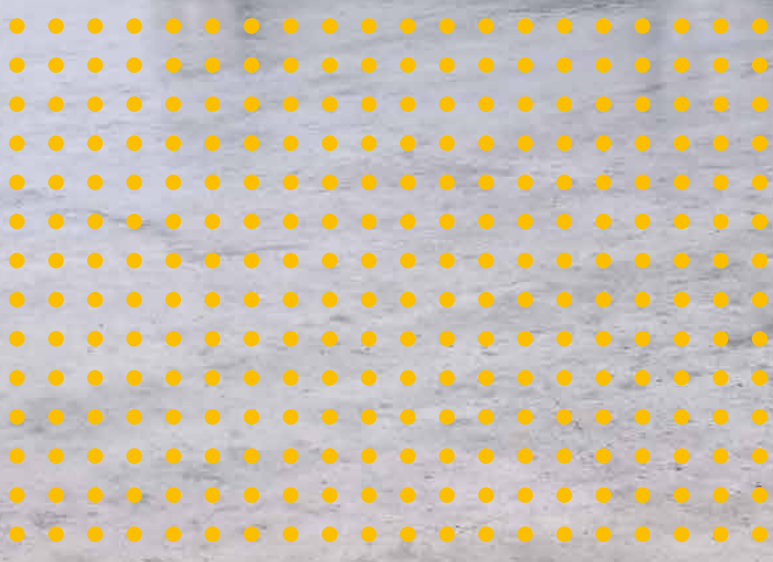
In many markets, however, legislation has yet to reach even the draft stage. Similarly, many OEMs and suppliers are unaware of how they compare to other market players in terms of CSMS technology and associated regulatory compliance.

Regulations focus on OEMs, although contractual obligations for partners and suppliers of software, services and vehicle components mean that these legal requirements for vehicle manufacturers are being passed on down the value chain and the supply chain. This relationship generates additional potential for inconsistency, as different stakeholders in global value chains are subject to different local and market-specific conditions.



Despite this lack of clarity, one thing is crystal clear: security and safety are absolutely essential for connected and autonomous driving. In line with this, market players are investing in cybersecurity within their automotive ecosystems. Governments will continue to introduce and tighten regulations. And companies are defining CSMS requirements in increasing detail.

Threats exist in every part of this ecosystem and at every stage in the vehicle's life cycle. Businesses in the automotive industry need to implement technical and organisational measures to protect their customers and their reputations – but also their vehicle ecosystems, which will create new business opportunities.



Opinions about automotive CSMS

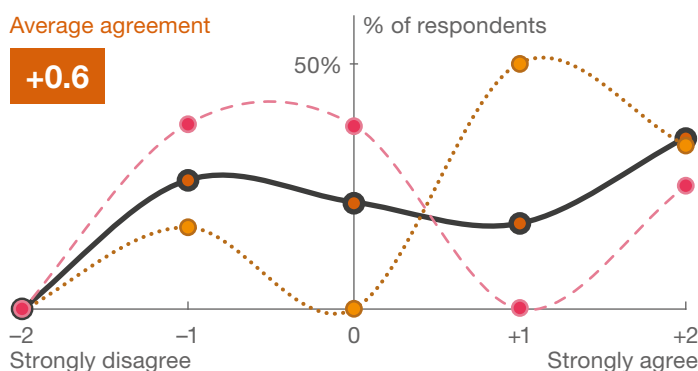
In detailed interviews, the respondents shared their opinions about key topics and trends related to CSMS. We asked them to rate a series of statements on a scale from -2 (strongly disagree) to +2 (strongly agree). We then created graphs to show the overall spread of responses. The thick black line shows the overall average, while the coloured lines show the averages among suppliers, OEMs and market experts.

Hypothesis no. 1

OEMs would have incurred the very high costs of meeting the CSMS requirements even without regulation because only secure vehicles can be successful in competition in the long term.

Average agreement

+0.6

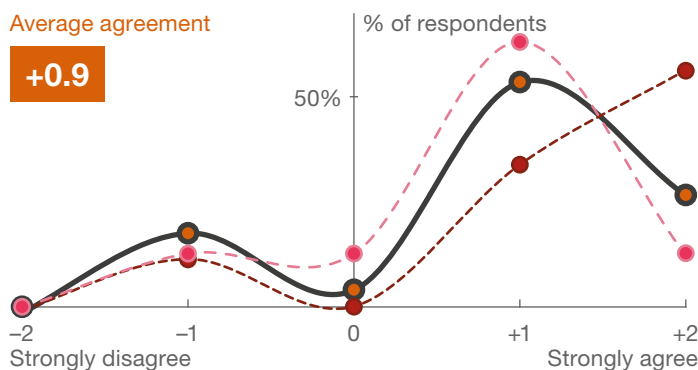


Hypothesis no. 2

High cybersecurity maturity will be a distinct competitive advantage for selling vehicles in the future.

Average agreement

+0.9

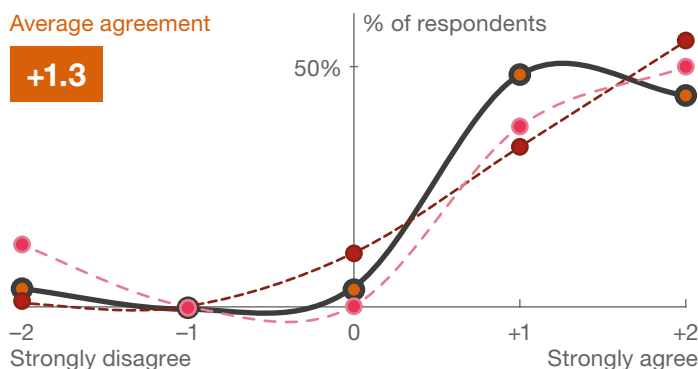


Hypothesis no. 3

Security management systems of suppliers and OEMs must grow even closer together to meet regulatory requirements.

Average agreement

+1.3

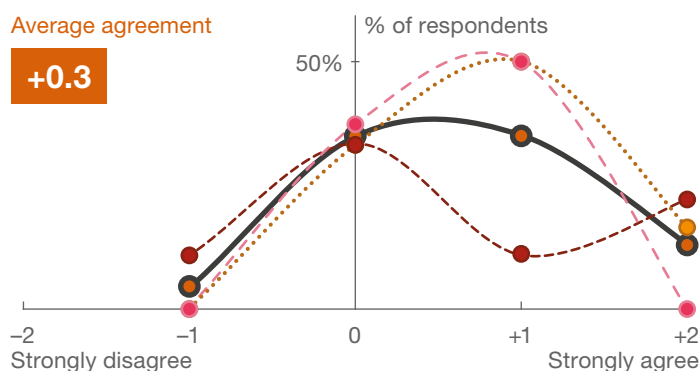


Hypothesis no. 4

For reasons of certifiability and risk segmentation, OEMs will limit their CSMS to the essentials and will not integrate them with other management systems to any great extent.

Average agreement

+0.3

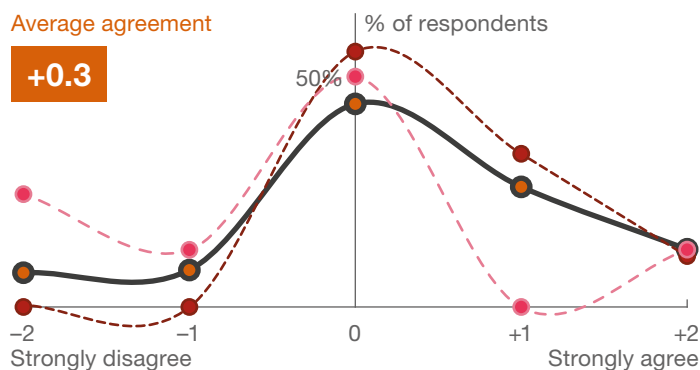


Hypothesis no. 5

OEMs will increasingly provide their own services and insource more and more parts of the automotive value chain.

Average agreement

+0.3

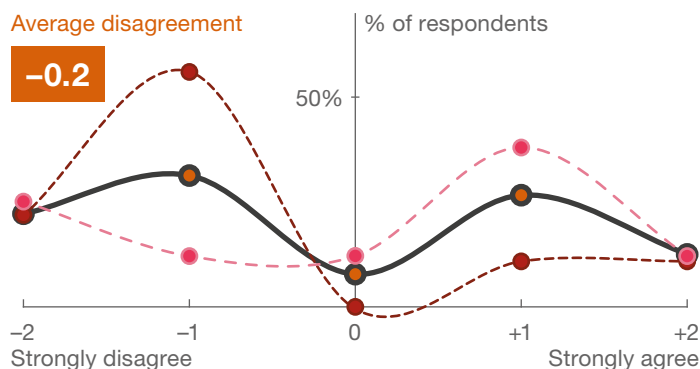


Hypothesis no. 6

It's impossible to fulfil CSMS requirements and document evidence for audits without delaying approval of new vehicle types.

Average disagreement

-0.2



Legend: All (thick black line), OEMs (dashed red line), Suppliers (dashed pink line), Market experts (dotted yellow line)

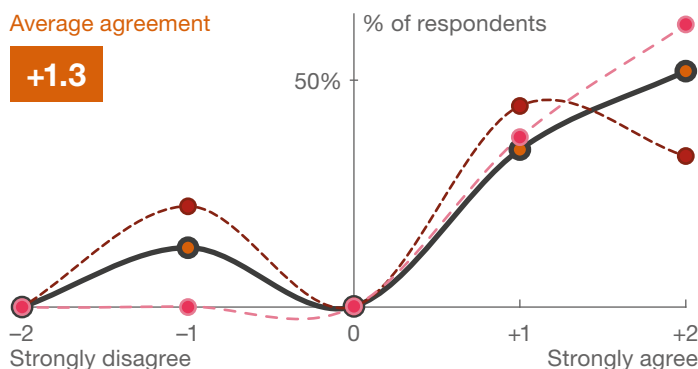


Hypothesis no. 7

Connected and autonomous driving is highly dependent on functioning national infrastructure and political/economic stability.

Average agreement

+1.3

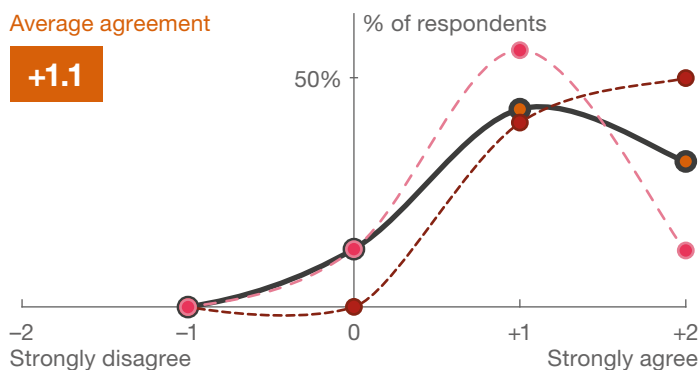


Hypothesis no. 8

UN Regulation No. 155 (CSMS) is absolutely necessary as it will lead to more secure vehicles.

Average agreement

+1.1

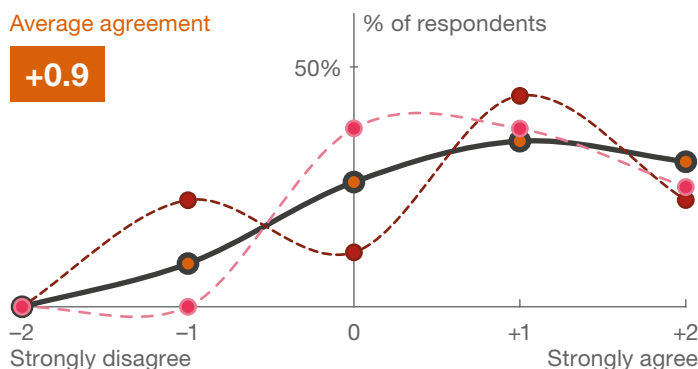


Hypothesis no. 9

Connected and autonomous driving will greatly change previous market shares.

Average agreement

+0.9

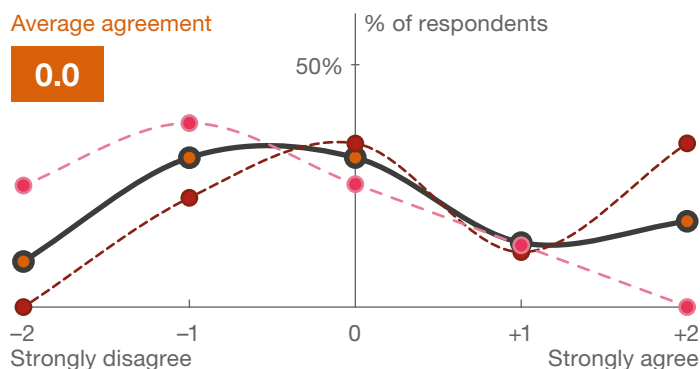


Hypothesis no. 10

OEMs provide comprehensive support to help their suppliers comply with contractual CSMS requirements (i.e. best practices, tools).

Average agreement

0.0

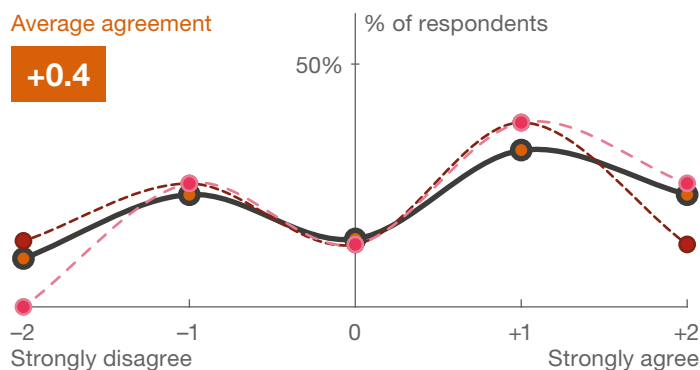


Hypothesis no. 11

Security-critical suppliers are clear about their contributions and importance to OEM value chains.

Average agreement

+0.4

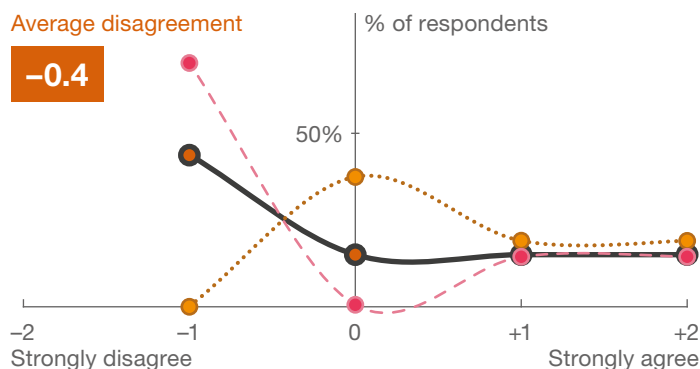


Hypothesis no. 12

Ultimately, vehicle security depends heavily on the behaviour of end users.

Average disagreement

-0.4



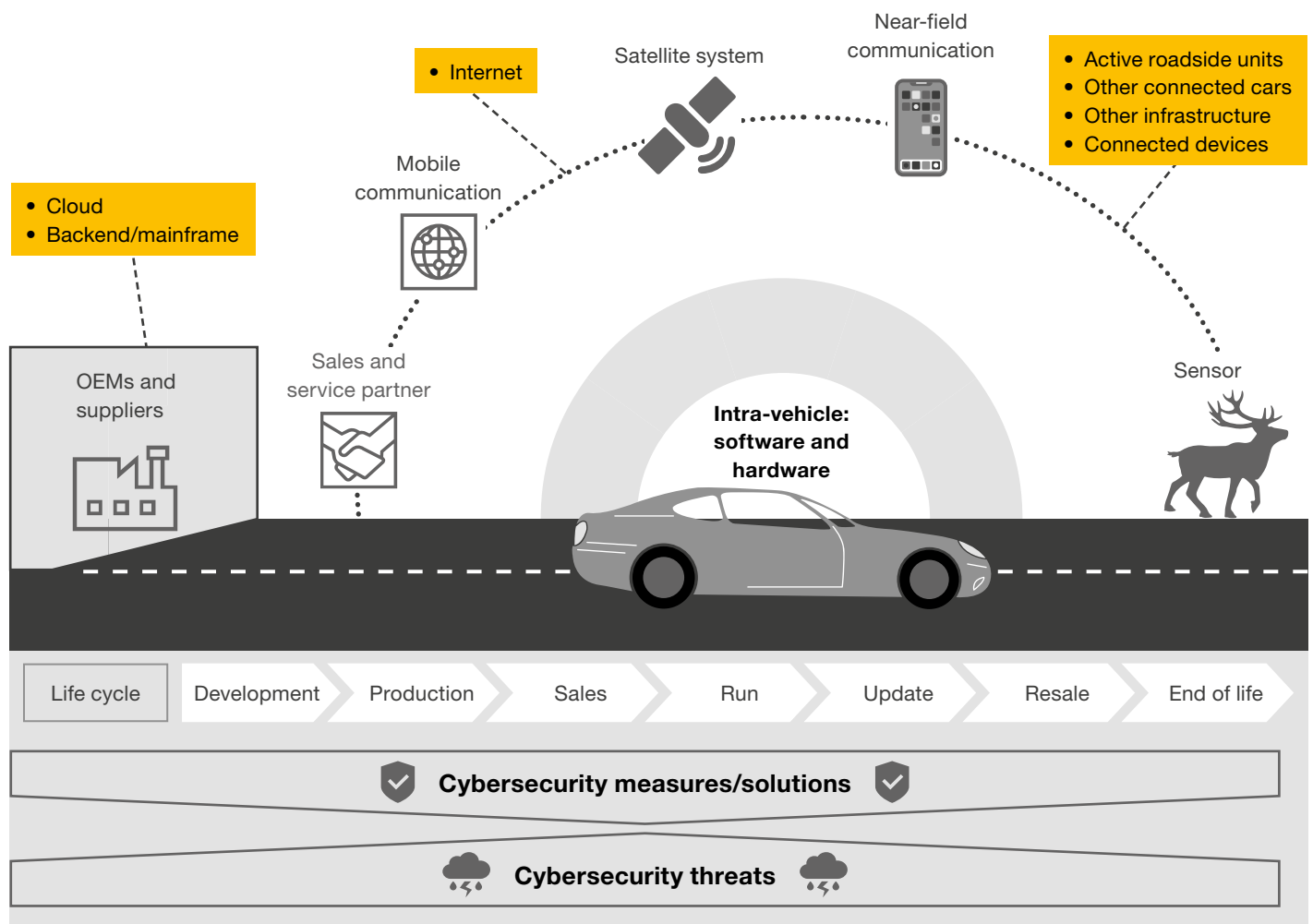
● All - - - OEMs - - - Suppliers ···· Market experts



The automotive ecosystem

This survey is based on our understanding of the automotive ecosystem. Of course, the vehicle itself is at the heart of this ecosystem – it consists of hardware and software and is closely connected to its environment. OEMs manufacture the vehicle using components from suppliers, and the vehicle is then sold to the customer directly or via a sales partner. This will involve wired connections to the vehicle that enable updates from the OEM and its sales or service partners. Vehicles are also connected to OEMs, suppliers and users via mobile internet, which allows them to exchange information or use services. Users and other attendees can also connect to a vehicle and its related services using near-field communication. And the vehicle also gathers information from non-connected or indirect traffic participants.

Fig. 1 Our understanding of the automotive ecosystem



B | Key takeaways

We spoke to experts from across the automotive industry who manage cybersecurity. What stood out from their responses? Here are the most revealing insights from their answers.

1.

Cybersecurity threats are growing for the automotive ecosystem – and there is an urgent need for better security

Our survey began by asking respondents about their perception of the cybersecurity challenges for the automotive ecosystem. The results revealed a difference of opinion between OEMs and suppliers. This illustrates the variety of opinions about vehicle-related cybersecurity management within the automotive sector, where this topic is relatively new – and the level of clarity and transparency is relatively low. But there was broad agreement on one point: cyberattacks on vehicles and the automotive ecosystem as a whole will increase dramatically (see Hypothesis no. 13).

When asked for their assessment of cybersecurity threats to the vehicle ecosystem, suppliers were generally more critical. Threats faced by OEMs were assessed more critically by the suppliers than the OEMs themselves. Similarly, threats faced by suppliers were assessed more critically by the OEMs than the suppliers (see Figure 2). This is a revealing sign of the lack of communication and transparency between OEMs and suppliers about cybersecurity threats.

At the same time, respondents mostly agreed that security management systems run by OEMs and suppliers need to grow even closer together to comply with regulations (see Hypothesis no. 3). OEMs and suppliers also expressed very similar opinions about the importance of cooperation along the value chain, although it seems that there are still some automotive suppliers who are not yet aware of the critical role they play in supporting CSMS for OEMs (see Hypothesis no. 11).

Respondents from OEMs and suppliers broadly agreed on which life cycle phases face the biggest threats (see Figure 2): the run phase, which includes the update phase, was considered the most vulnerable. This makes sense because this is the longest phase in the life cycle and the most difficult to control. It is also the phase where attackers have easiest access to vehicles, because they can buy a car and test potential attacks on it.

There was further agreement that the update phase is the most vulnerable to being compromised, i.e. by malware. This indicates that compromised updates are considered a likely path for malware to enter vehicles. On this point, it is important to note that not all updates are alike: remote updates affect vehicles en masse, while local software updates or physical misconfiguration target a single specific car. Both, however, can be very dangerous to the public, and may severely harm the manufacturer's reputation.

Hypothesis no. 13

Cyber-attacks on both vehicles and on the entire automotive ecosystem will increase dramatically.

Average agreement

+1.7

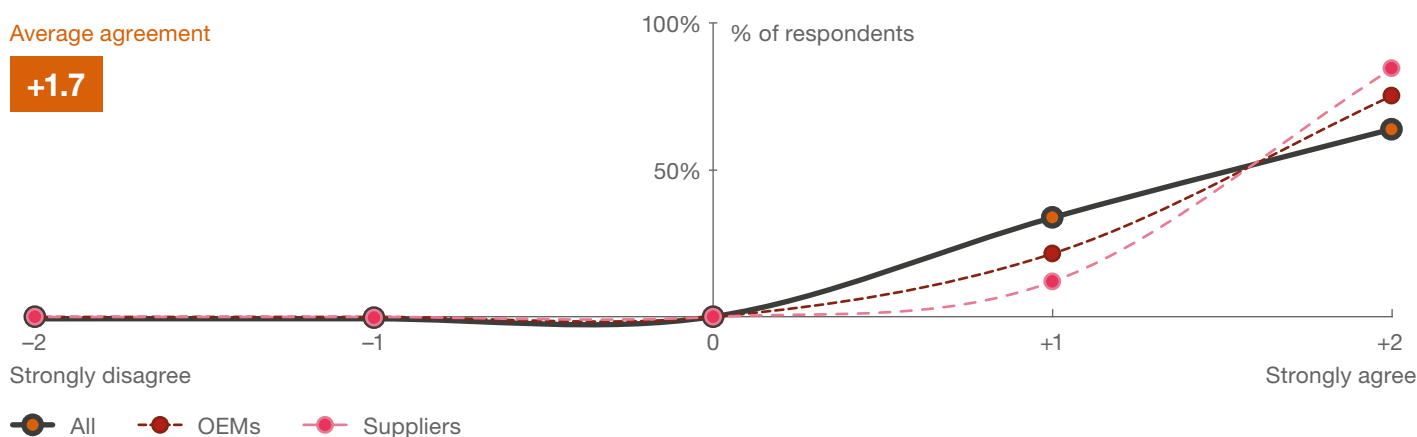
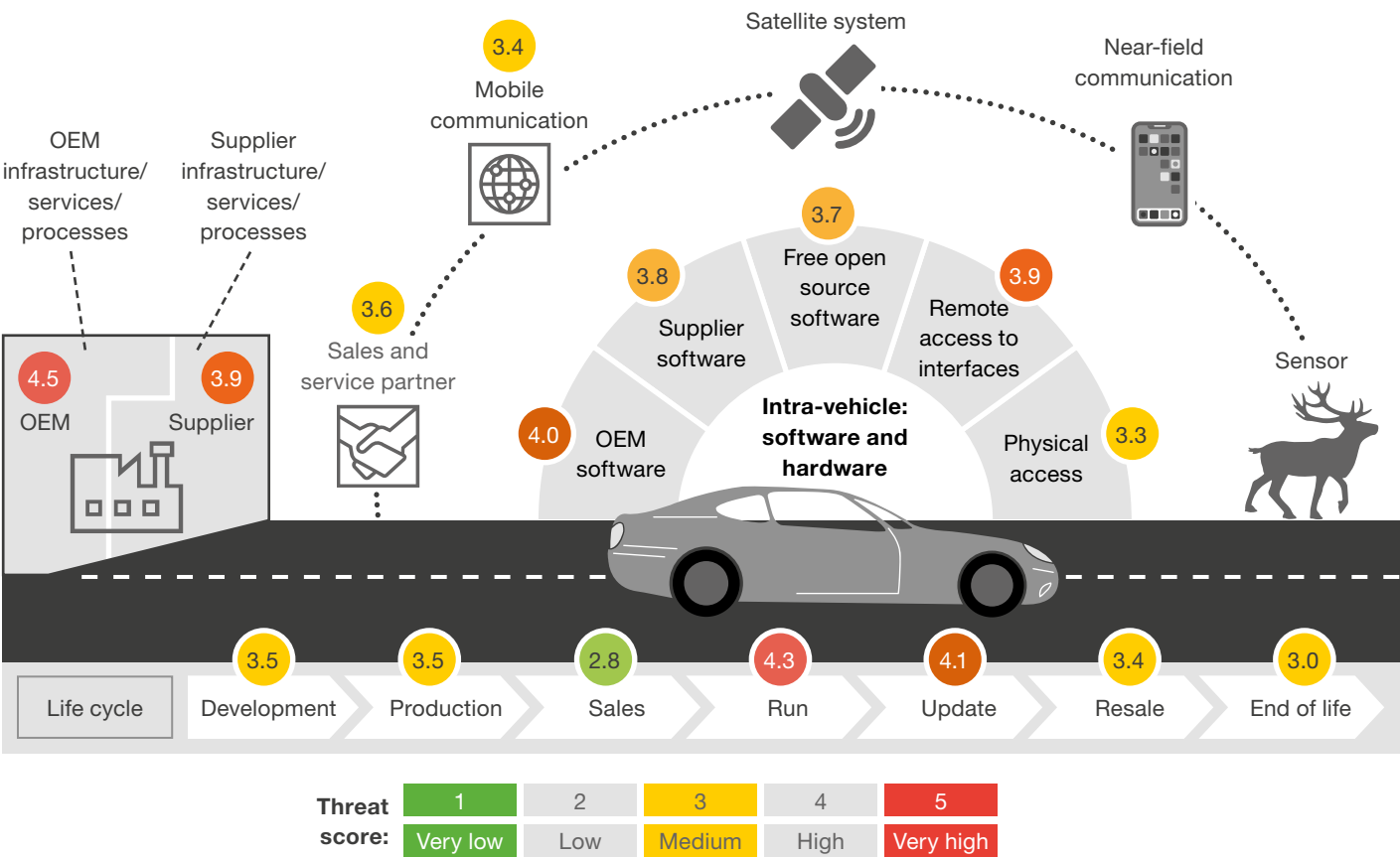


Fig. 2 What is your assessment of cybersecurity threats to your vehicle ecosystem?

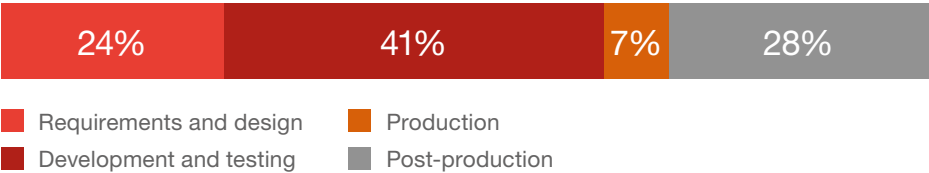


Which stage of the vehicle manufacturing process will identify the most security vulnerabilities? All respondents stated that the development and testing phase will be key to revealing weaknesses (see Figure 3). It is striking that interviewees estimated that around a third of vulnerabilities will be identified after production. This means respondents expect that one in every three vulnerabilities will not be identified during pre-production testing, despite the vast amounts of money and effort that automotive companies put into

testing. These threats are the most significant because they target cars during operation and use by the end customer. It is important to remember that the post-production phase can last for up to 20 years, so it is difficult to foresee what new vulnerabilities may arise in this time. However, stakeholders in the automotive

sector may be underestimating the challenge of keeping connected cars secure once they leave the showroom. In particular, this phase will open up new vectors for attack, ranging from dealerships through to other connected devices and external services.

Fig. 3 In which phase of vehicle development are most security vulnerabilities likely to be identified?



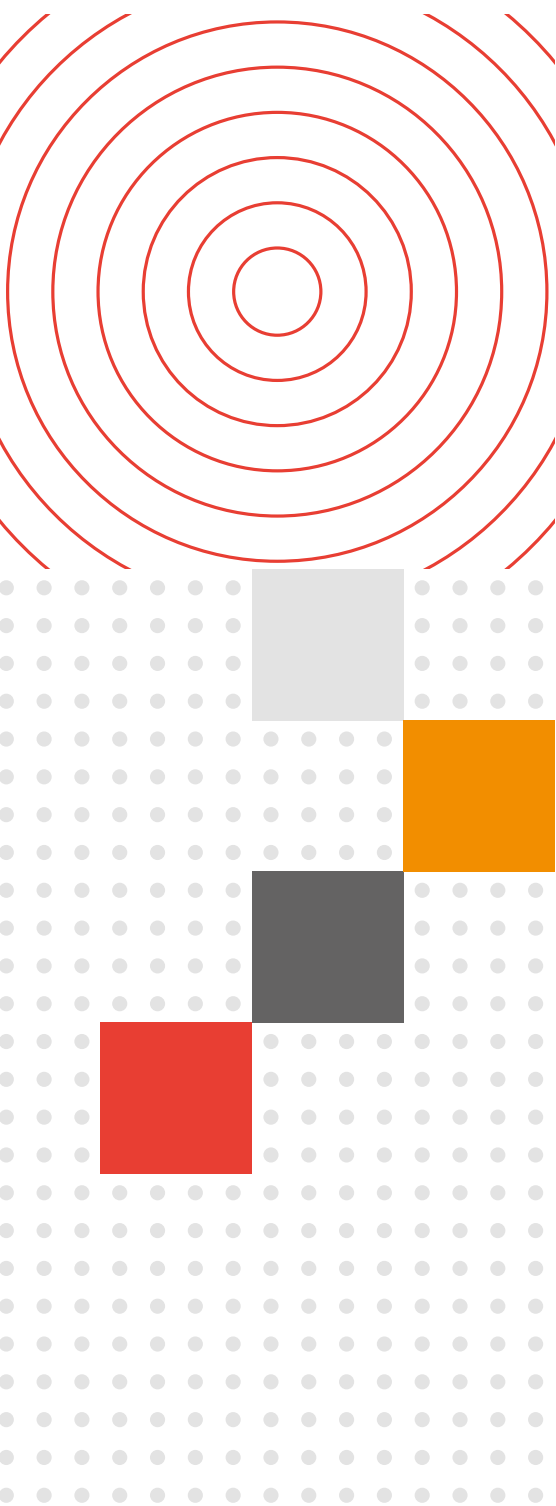
2.

Technology is evolving rapidly and regulation is not keeping up – even though it is business-critical

In view of the technological development of connected and autonomous driving, as well as the significance of the topic in society, consistent security requirements from regulators are long overdue. In line with this, almost all interviewees agreed that UNECE Regulation No. 155 (CSMS) is absolutely necessary as it will lead to more secure vehicles (see Hypothesis no. 8).

At the same time, OEMs are being faced with the threat of being unable to get new vehicle types approved in many markets without a CSMS. From July 2022, UNECE Regulation No. 155 will require OEMs to provide proof of an audited CSMS in order to register new vehicle types with national registration authorities in 56 countries worldwide. From July 2024, no new vehicles may be produced if a CSMS is not in place. Similar regulations are expected in non-UNECE countries.

The business-critical nature of CSMS is already showing: more than two fifths of interviewees said that CSMS requirements will result in delays in homologation of new vehicle types (see Hypothesis no. 6).



3.

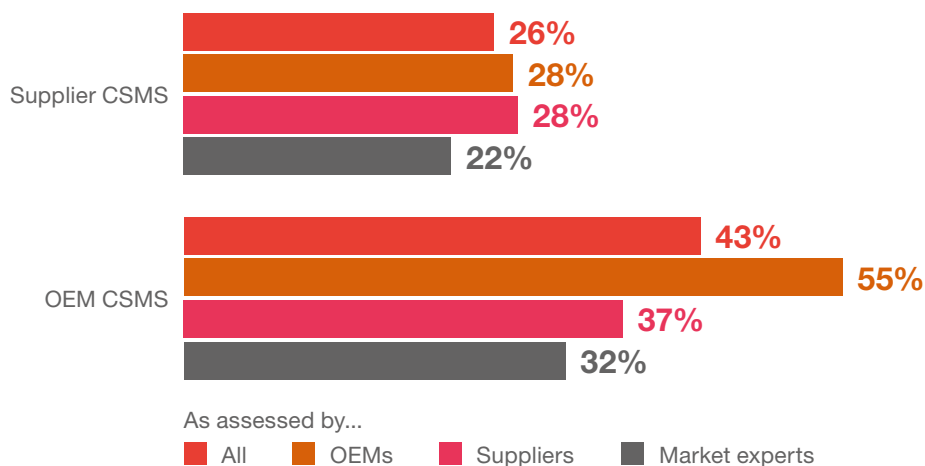
OEMs and suppliers have addressed CSMS, but most are only at the design stage and have a low level of maturity. They need to go further

All OEMs surveyed stated that they had implemented a CSMS. However, this statement mostly refers to designing a CSMS, because most respondents also stated that most CSMS are not yet operational. Around two thirds of participating OEMs have already had their CSMS design audited by an external auditor (see Figure 9). When participants were asked to rate the prevalence of audited CSMS among their global competitors, the rates were lower. Only two fifths of OEMs and one quarter of suppliers are estimated to have had their CSMS assessed (see Figure 4).

As described in the introduction, OEMs are passing the regulatory requirements on to their suppliers by including specifications and obligations in contracts. This approach is understandable given that OEMs have limited control over security – much of the technological implementation is dependent on their suppliers. Accordingly, the onus is on the suppliers to ensure that components they deliver to different OEMs or for different vehicle models are secure.

In this context, it is essential that OEMs are required to verify that their suppliers have complied with all relevant regulations and standards, as this forms the foundation of end-to-end cybersecurity for software and hardware components – and ultimately for the entire vehicle. However, apart from individual risk ratings, there is still no common measure of vehicle cybersecurity in the automotive industry.

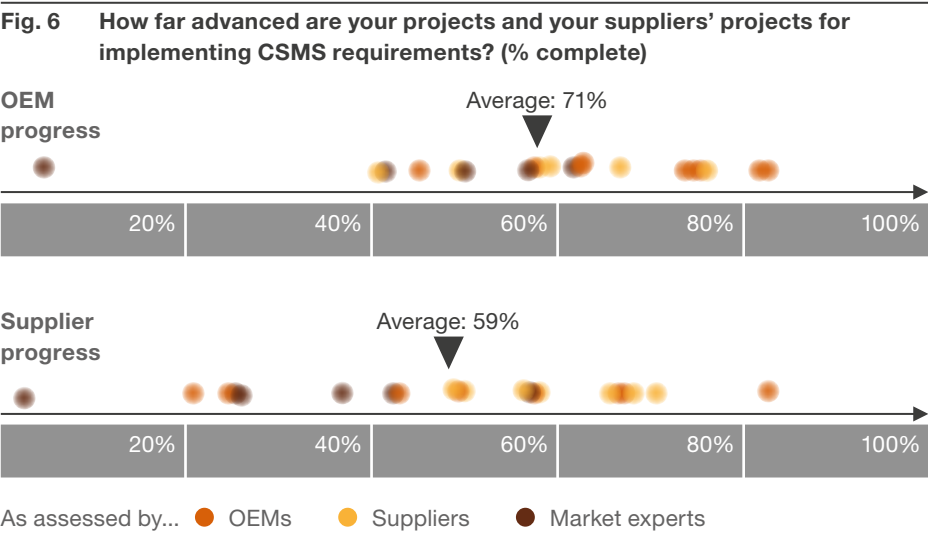
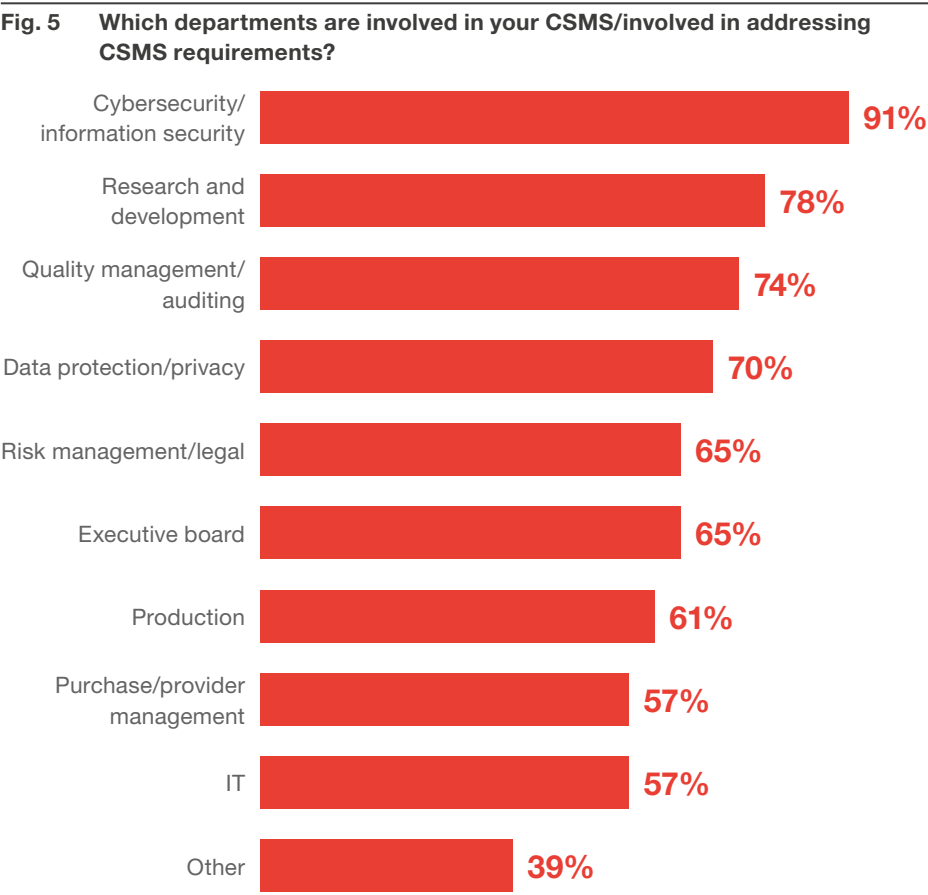
Fig. 4 Based on your experience, what proportion of OEMs and suppliers do you think have successfully assessed their CSMS?



Among the OEM representatives interviewed, 75% stated that they have already imposed CSMS-specific contractual requirements on their suppliers, and the same proportion of suppliers said that they have been required to meet CSMS-specific contractual requirements by OEMs. The remaining 25% may refer to situations where similar requirements were already in place but have not yet been updated to specifically consider CSMS.

We also asked which people or departments are actively involved in efforts to address CSMS. The results showed a higher level of involvement among OEMs than suppliers, across all areas of these companies (see Figure 5). This indicates that suppliers still take a rather selective view of CSMS, only considering them for certain services or products that they provide to OEMs. For OEMs, on the other hand, CSMS have become a larger part of their internal governance structures. The level of involvement from executive boards is also interesting in this context, as every major project requires support from senior management to succeed.

Which phase of implementation have these CSMS projects reached? It depends who you ask. OEMs, suppliers and market experts gave very different answers about the level of progress they believe has been made, with responses ranging from just 5% all the way to 100% complete. These results indicate the total lack of transparency on this topic in the automotive industry, with all respondents clearly struggling to assess what position the various ecosystem players are in (see Figure 6).

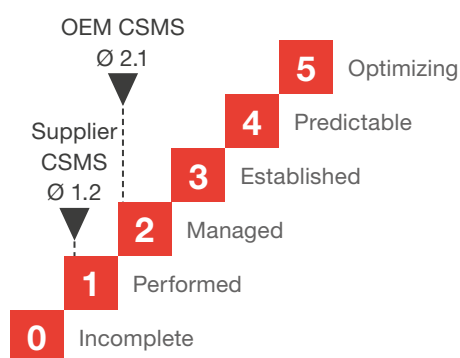


The answers to this question also suggest that market experts have different expectations to OEMs and suppliers. It's possible that OEMs and suppliers are only aiming to meet the minimum requirements for CSMS, whereas experts have more demanding expectations.

Respondents from within the industry did, however, make similar assessments of the maturity of OEMs. This could mean suppliers are already taking notice of the requirements imposed by OEMs. The fact that OEMs rated the progress of suppliers as less advanced than the suppliers assessed their own progress could mean that OEMs are not satisfied with the solutions they are receiving.

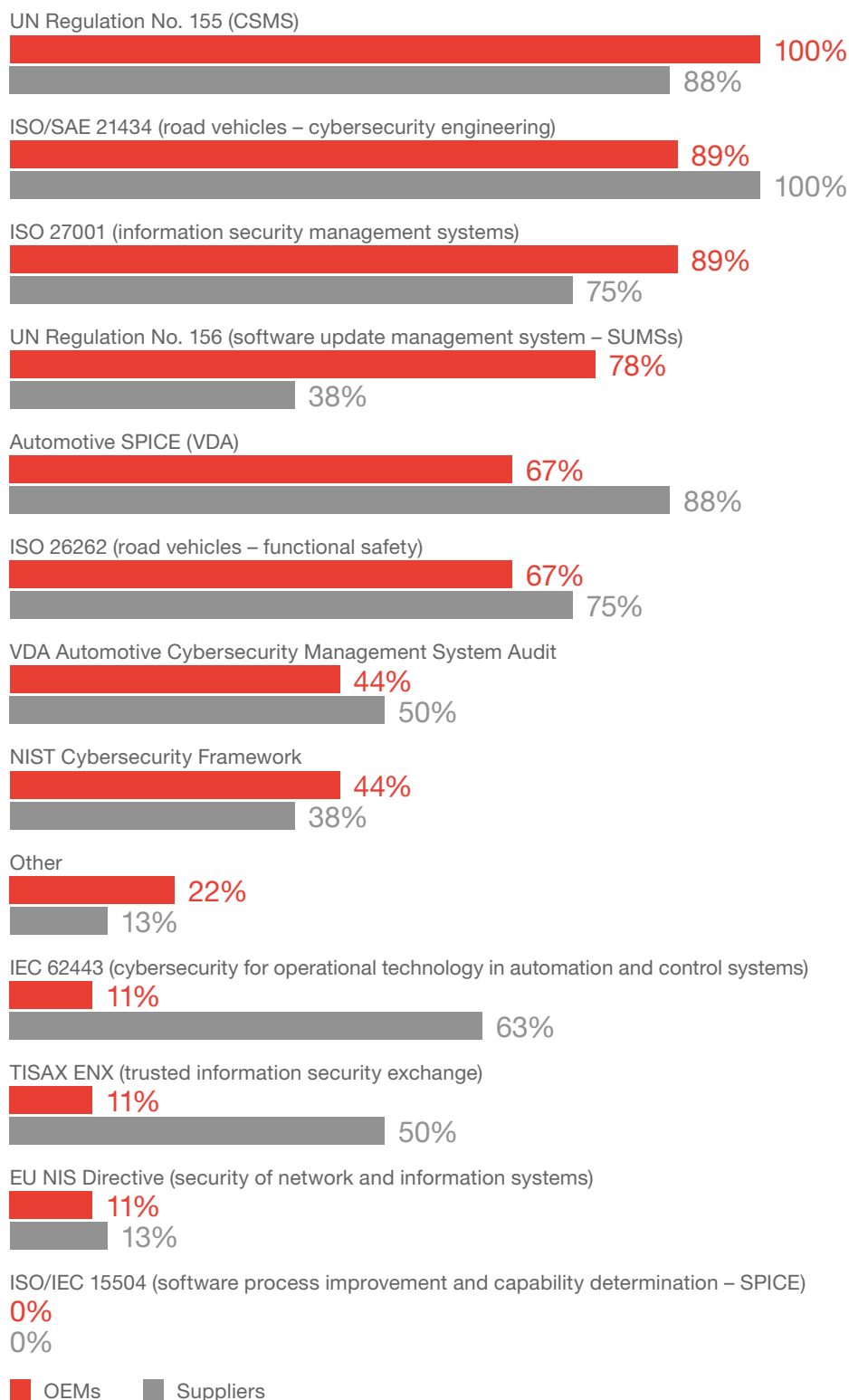
Approaches to CSMS also seem to be more advanced within OEMs than suppliers. However, respondents clearly share a perception that CSMS implementation is in its infancy (see Figure 7), and that there is still a significant amount of work to be done before connected vehicles can be operated en masse at the desired levels of efficiency and security.

Fig. 7 Based on your experience, what is the average maturity level of OEM CSMS?¹



¹ Maturity Level resp. VDA ISA 5.1

Fig. 8 Which standards/frameworks are relevant for your/a CSMS?



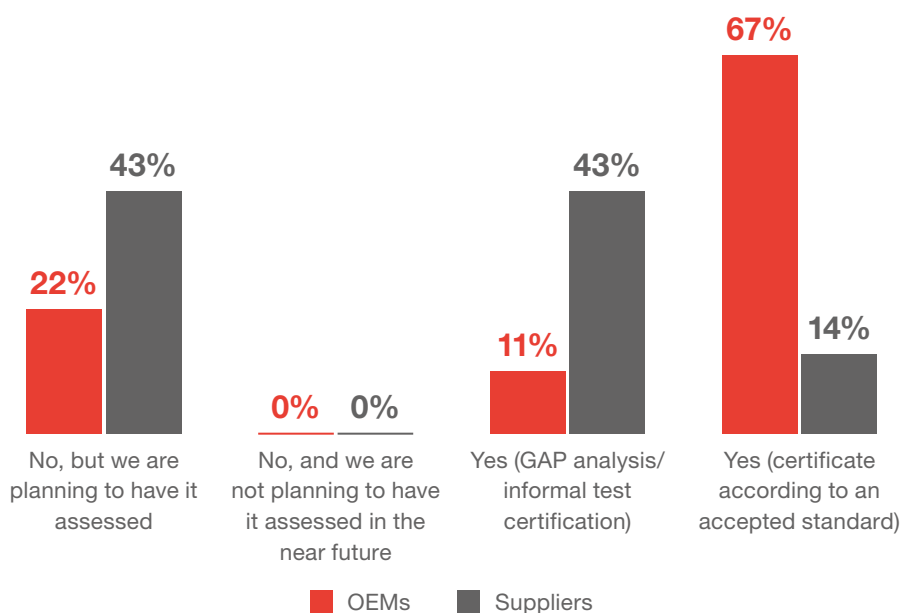
When it comes to CSMS maturity, suppliers lag behind OEMs. But even among suppliers, the picture is very heterogeneous. Some are doing better than average (especially Tier 1), others are not. For suppliers in particular, a CSMS is a major competitive advantage because they can prove to OEMs that they comply with security requirements. This competitive advantage may end up becoming an essential requirement for suppliers wanting to do business with OEMs as CSMS standards become more rigorous.

There is a lack of consensus on the standards and frameworks that respondents considered to be relevant for their CSMS. In a global market, OEMs and suppliers must each select

which security standards to use as a basis for their approach to CSMS – either on a regional or a global level. Because of this, our survey also attempted to get a clear picture of which standards or frameworks are emerging as the most important.

Certification offers a way of making potential issues visible in this context – and OEMs need certification in order to access the market. All of the respondents in our survey stated that they recognise the value of getting their CSMS assessed (see Figure 9). Most OEMs already have certification in line with UNECE Regulation No. 155. Suppliers are mostly relying on GAP analysis and informal test certification at present, but have clear plans for external certification in the future.

Fig. 9 Has your CSMS been assessed by an external auditor?





4.

There are obstacles on the way to better cybersecurity

If everybody agrees on the scale and seriousness of the cybersecurity threats facing automotive companies, why haven't these companies made more progress? To understand the reasons behind this, we asked respondents to list the biggest obstacles to making vehicles more secure. This was another rare point of consensus, with lack of skilled personnel and time pressure clearly emerging as the two key challenges, followed by inadequate specification of requirements (see Figure 10).

Fig. 10 What do you currently see as the biggest obstacles to making vehicles more secure?

1

Shortage of skilled staff/lack of know-how and training

2

Time pressure created by external or internal deadlines

3

Lack of interpretation and specifications of requirements

4

Complexity of supply chain

5

Lack of awareness among management

6

Lack of budget

7

Lack of backend infrastructure

8

Vehicle hardware components not available



There is also a need for action on the question of how cybersecurity is managed within companies. At present, automotive executives are not generally convinced of the need for fully integrated management systems. While all respondents stated that they have implemented CSMS to some degree, these systems are not yet integrated into a consolidated

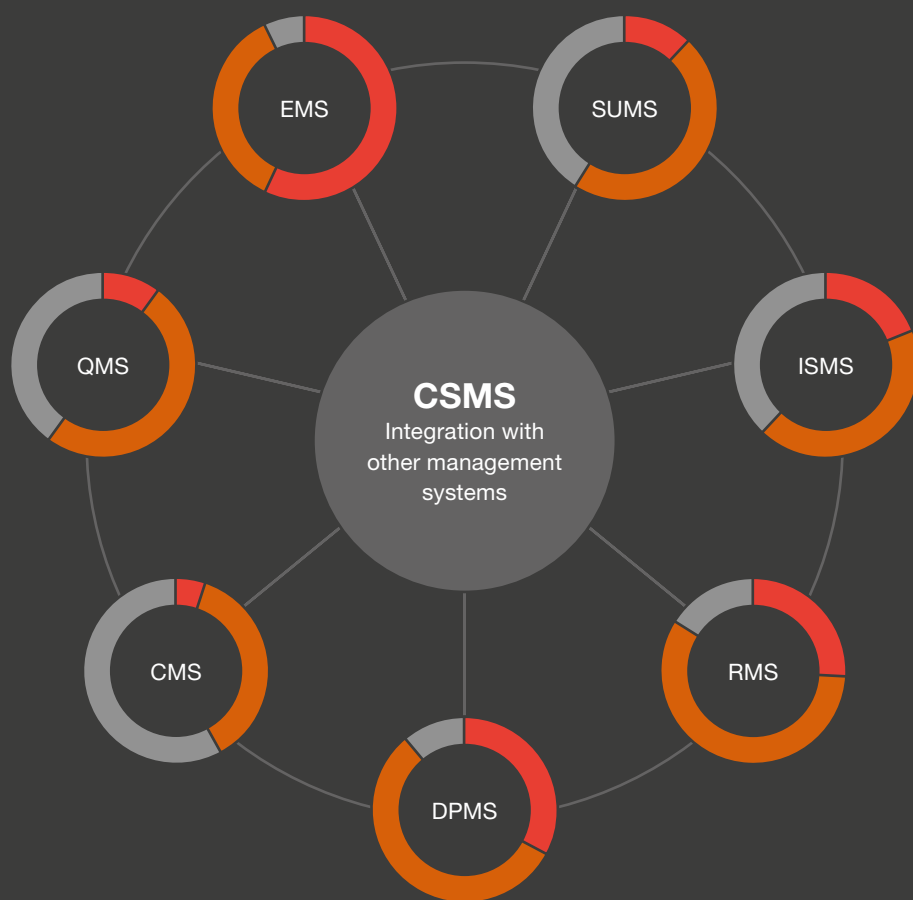
management approach (see Figure 11). Instead, most companies are only just beginning to connect their CSMS with other systems. Quality management systems (QMS) and product compliance systems are the most common places to start. Typically, OEMs have so far achieved slightly higher levels of integration than suppliers.

One of the questions in the survey concerned the issue of whether OEMs will limit their CSMS to the essentials and engage in very little integration with other management systems for reasons of certifiability and risk segmentation. The interviewees were unsure on this issue: one third agreed, one third disagreed, and the remaining third stayed neutral (see Hypothesis no. 4). This question exposed an element of disagreement compared to the broad agreement on the need for CSMS to grow closer together. Some respondents stated that OEMs might deliberately try to limit the scope of these systems. So how can management systems be integrated successfully?

However, real integration may not be the aim at present. The interviews suggested that most companies are aiming more to interlink their management systems, rather than achieve full integration. This would support the flexibility and auditability of the CSMS approach. At the same time, a purely compliance-driven approach is risky – because a clear business strategy should be the starting point for digital transformation.

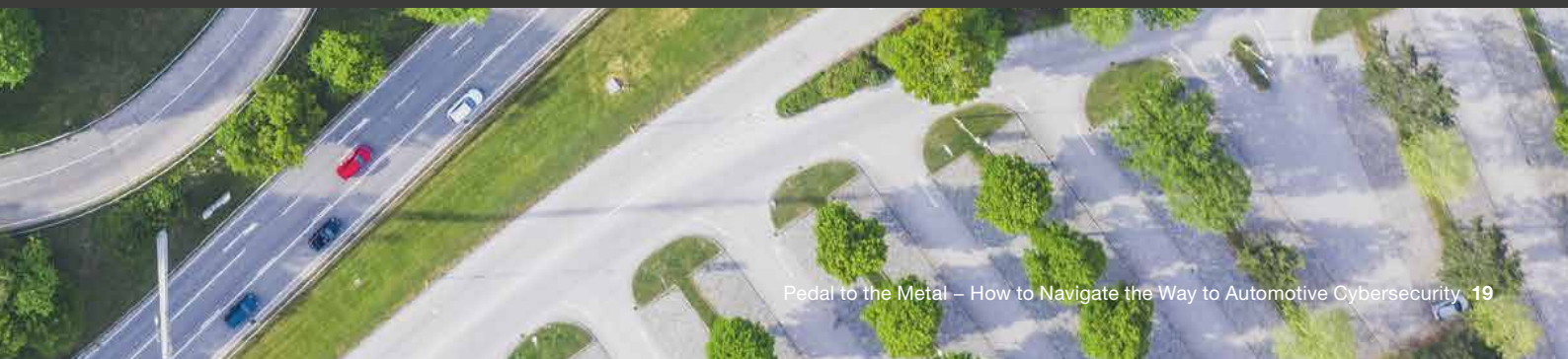
Looking at the supply chain, there is also ambiguity about whether OEMs provide their suppliers with comprehensive support to help them meet CSMS requirements (see Hypothesis no. 10). Most respondents believe that OEMs will insource some parts of the value chain again, while outsourcing will further increase in other parts (see Hypothesis no. 5). However, strong collaboration will remain important because automotive supply chains will stay highly interwoven.

Fig. 11 How strongly is your CSMS integrated with other management systems?



SUMS = Software update management system; ISMS = Information security management system; RMS = Risk management system; DPMS = Data protection management system; CMS = Product/compliance management system; QMS = Quality management system; EMS = Environmental management system

■ Not integrated ■ Partially integrated ■ Fully integrated



5.

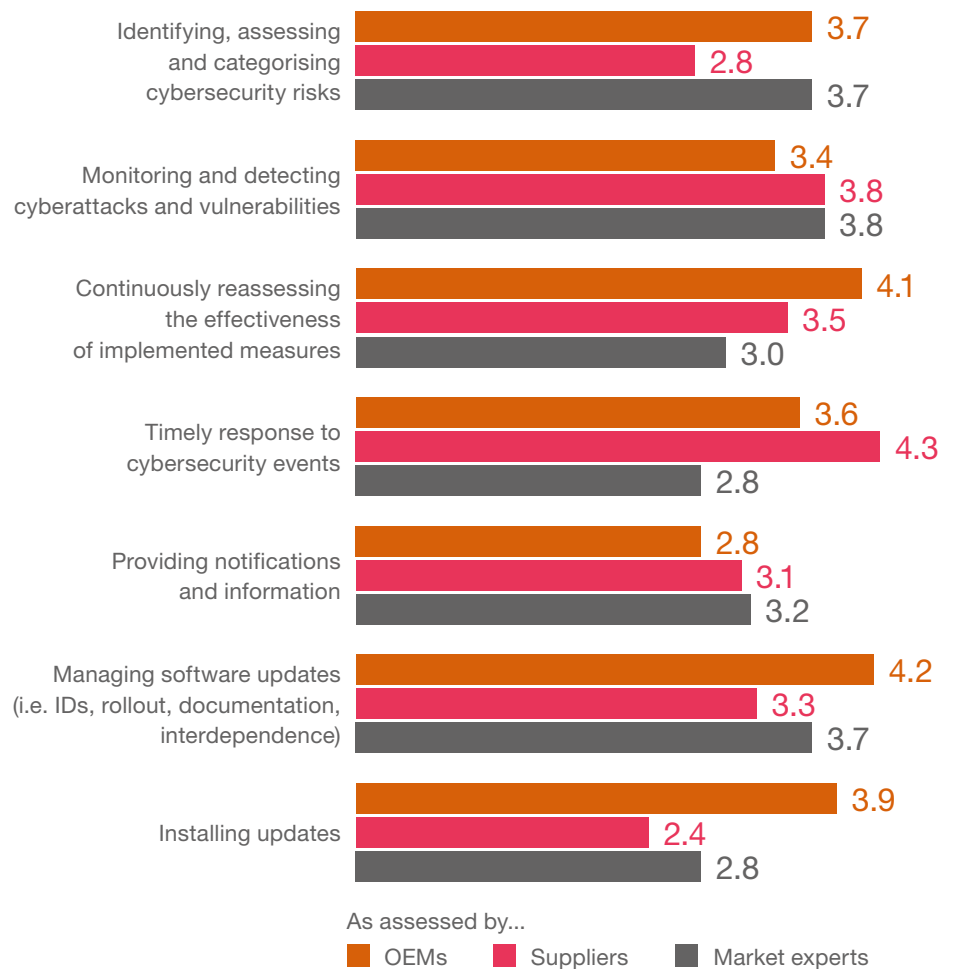
When it comes to implementation, the devil is in the details

While many respondents appear to have already implemented CSMS, several core CSMS processes are still considered difficult to implement. The results of our survey revealed contrasting perceptions of challenges related to implementing CSMS (see Figure 12). When asked which CSMS requirements are most difficult to address, the most common response from suppliers was “timely response to cybersecurity events”. OEMs, on the other hand, were most likely to answer “managing software updates (i.e. IDs, rollout, documentation, interdependence)”.

These responses show that OEMs and suppliers view CSMS from very different perspectives. OEMs are usually responsible for handling updates. This is a much smaller issue for suppliers because they are only responsible for providing a piece of software to update an electronic control unit (ECU) – but not for getting that update to the vehicle. This suggests that OEMs have not yet passed this obligation on to suppliers via contracts. As a result, OEMs and suppliers do not have a common perception of the challenges of implementing effective CSMS.

Fig. 12 Which CSMS requirements are most difficult to address?

1=very easy; 2=easy; 3=medium; 4=difficult; 5=very difficult



The efficiency of CSMS design will become apparent in operation, so it will also have a significant impact on the cost of cybersecurity for ongoing business. If CSMS designs that are currently being implemented cannot be operated as planned, these systems will represent the next compliance risk – non-compliance with the company’s own organisational requirements.

Human behaviour is another area of uncertainty. Some respondents stated that the focus should be on major efforts at the design stage to boost security, while others suggested that there’s not much that the industry can do if users fail to take responsibility (see Hypothesis no. 12) – by connecting vehicles to non-secure devices, using aftermarket parts from third parties or postponing software updates, for example.

6.

There are clear trends towards technological solutions that support CSMS

What exactly does the industry need to work on? Respondents gave us a list of technical developments that need to be addressed in order to advance CSMS in the automotive sector (see

Figure 13). Software architecture is key, and was listed by 96% of the interviewees. Usability, security, safety and maintenance are all determined by software. The modularity and scalability of vehicle software and computing power will be crucial, as these factors are essential for cost-effective production and operation of vehicles in the long term. Around three quarters of the interviewees also stated that technological development is needed for fleet monitoring and vehicle security operations centres (SOC).

Fig. 13 Which areas need the most technological development to properly meet CSMS requirements?

Top 5

1

Vehicle software architecture

2

Fleet monitoring/SOC

3

OEM and supplier backends

4

Vehicle technical architecture

5

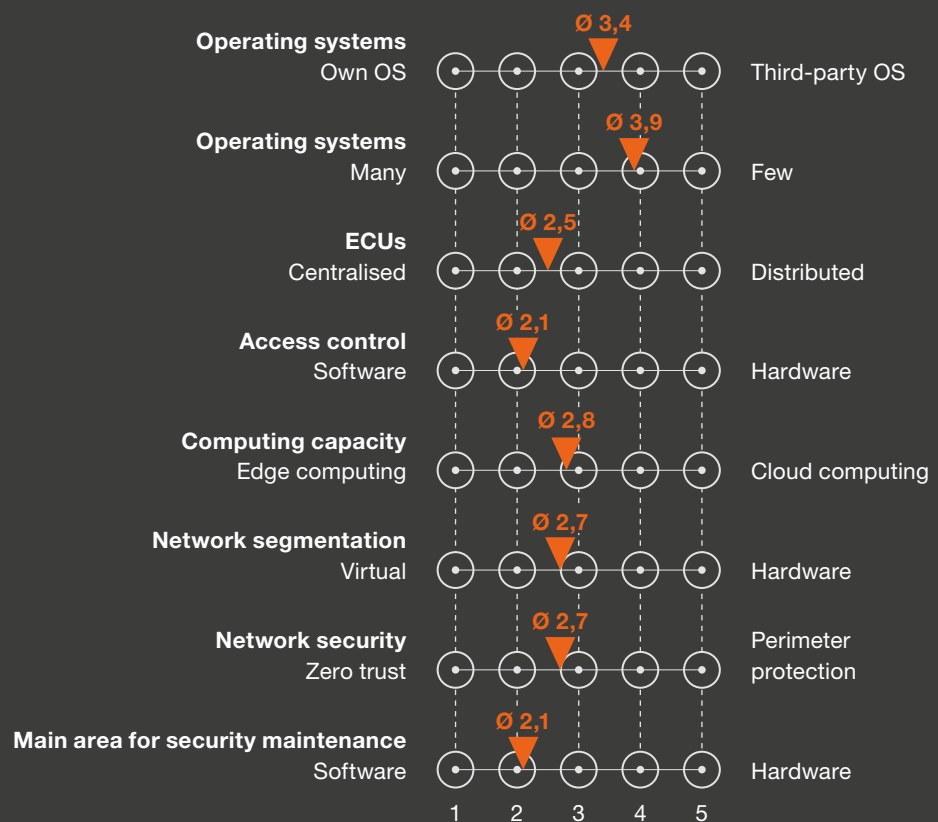
Mobile communications infrastructure

Respondents were then asked how the current evolution of cybersecurity will transform vehicle architecture in the future. Most answers kept away from the stronger ends of the opinion scale (see Figure 14), which suggests that there is still a significant variety of opinions about what the future holds and what long-term strategy companies will choose. The biggest difference between OEMs and suppliers was related to ECUs, with suppliers expressing the belief that the number of ECUs within a vehicle will decrease faster than OEMs feel is likely. Even though the number of ECUs is tending to decrease, the complexity of vehicle control systems is increasing. This places higher

requirements on software functions, which is why software is offering an increasingly large potential target for cyberattacks.

We also asked for opinions about the importance of functioning national infrastructure and a stable political and economic environment (see Hypothesis no. 7). There was clear agreement that autonomous and connected driving requires strong structures outside the automotive industry. This shows that security is not just up to OEMs and suppliers. Governments must also create the right conditions to enable secure driving in the future.

Fig. 14 Which vehicle architecture principles is the current evolution of cybersecurity likely to lead to?



7.

Implementing CSMS is difficult and needs a lot of resources

There were big differences in the timings for initial implementation of respondents' CSMS projects. In general, OEMs are further ahead and expect to finish sooner, which makes sense given that they are being directly targeted by regulations. However, suppliers are following up. This suggests that OEMs are successfully integrating new CSMS requirements into their supply chains. Perhaps most interestingly, the average project duration stated by respondents is 30 months. This shows that CSMS projects are difficult – and are almost certainly labour-intensive too (see

Figure 15). Taking a look at the list of the departments involved makes this fact even clearer (see Figure 5).

On the issue of how OEM investments in implementing CSMS will be allocated within the automotive ecosystem and vehicle life cycle, respondents said that 21% of investments will go into each of the development and run phases, with a further 20% going into each of the production and update phases (see Figure 16). Since the update phase is part of the run phase, this means that more than 40% of CSMS investments will go into operations. OEMs that now invest very specifically in standardised processes, automation and suitable tool support will save costs in the future run phase and thus gain a competitive advantage. This is a particularly important long-term consideration, given that vehicles may be on the road for up to 20 years.

Fig. 15 Start, end and duration of initial CSMS projects

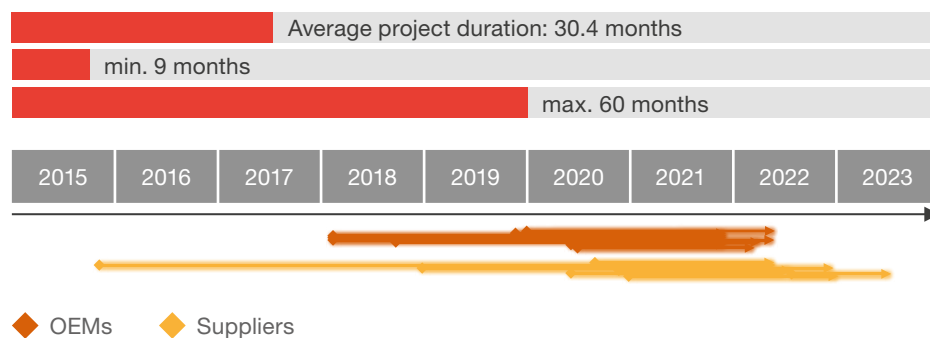
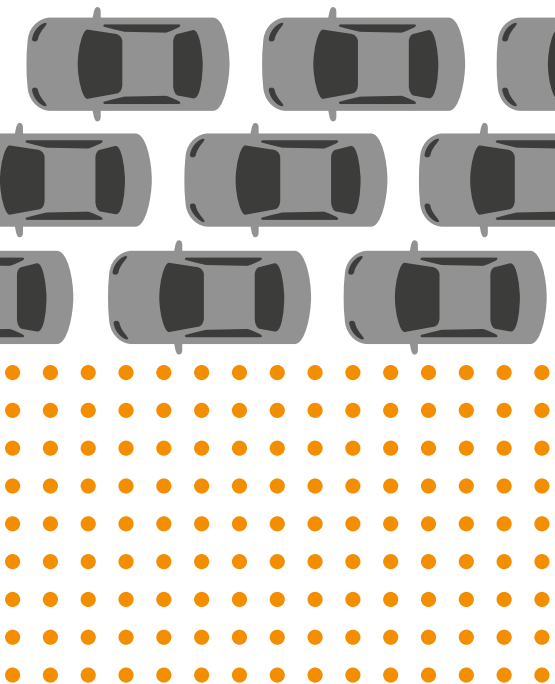
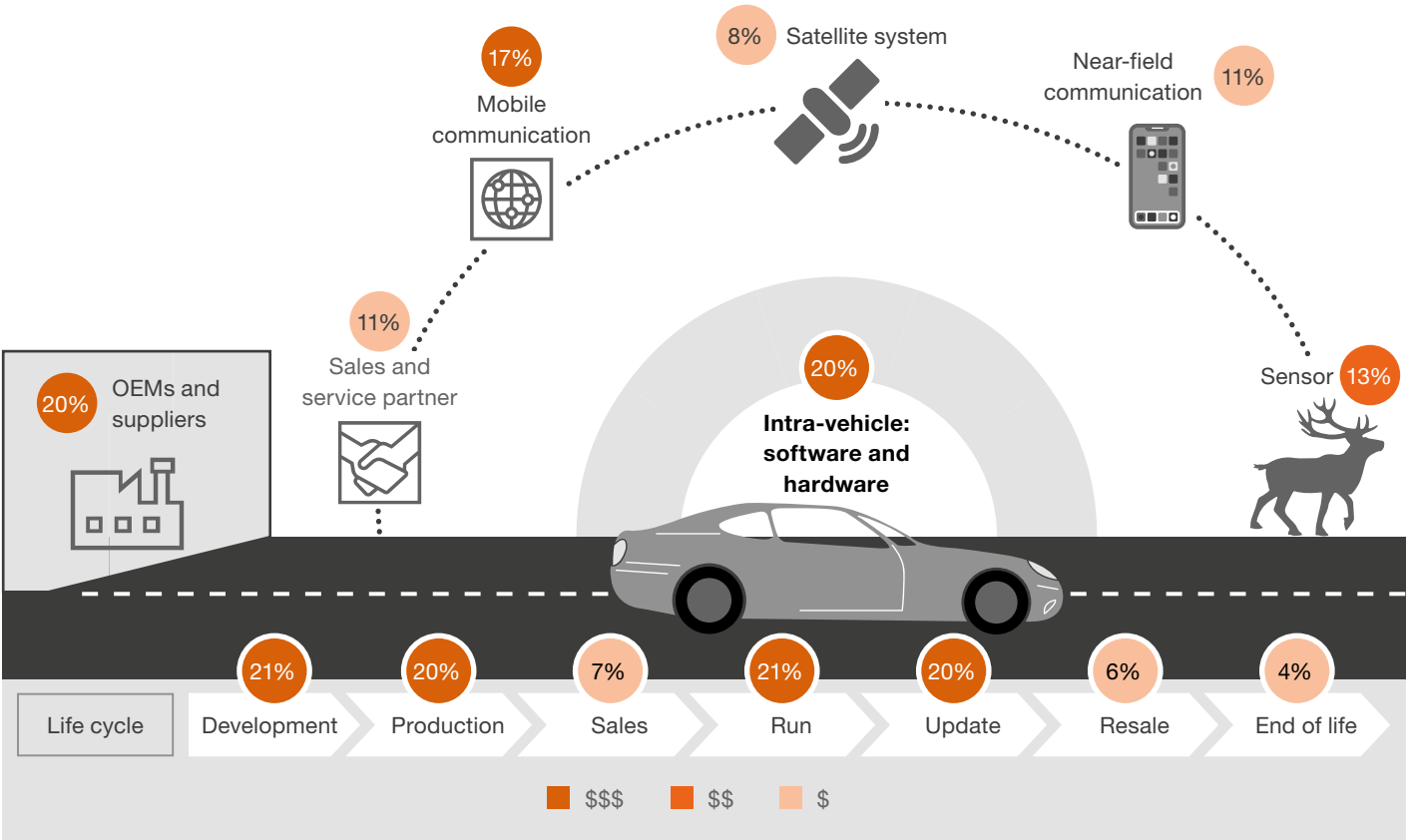


Fig. 16 How will OEM investments in implementing CSMS be allocated within the automotive ecosystem?



While CSMS projects require large amounts of resources, they are also essential for any manufacturer wanting to sell vehicles in the modern connected world. Market experts strongly believe that OEMs would have incurred the very high costs of meeting CSMS requirements even without being forced to do so by regulation, because only secure vehicles will succeed on the market in the long term. Opinions from suppliers on this statement were more divided (see Hypothesis no. 1).

These figures indicate that the automotive sector needs to invest in almost every part of the ecosystem. This also suggests that CSMS must be integrated with all phases of the vehicle life cycle, which will make CSMS into very complex, long-term projects. Any companies which haven't yet started their CSMS journey will have a lot of catching up to do.

8.

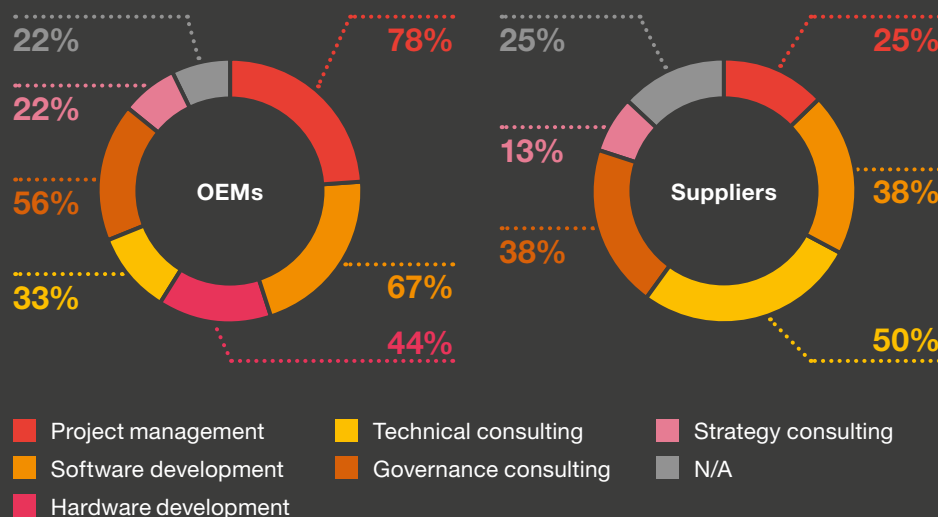
Effective CSMS can provide an exciting competitive advantage

The future of the automotive industry will open up incredible opportunities for companies that adapt quickly by embracing new technologies and getting ahead of the game on regulations. Most of the organisations surveyed stated that they are joining forces with external parties to accelerate their CSMS journey. Again, there are differences between OEMs and suppliers, with almost four fifths of OEMs using third-party project management office (PMO) support compared to just a quarter of suppliers. Use of third-party help for software development was also more common among OEMs (67%) than suppliers (38%).

The value of effective CSMS was a point of broad agreement for all interviewees. If the OEMs affected by the UNECE requirements are able to efficiently design and operate their CSMS, they will gain competitive advantages over others. Among OEMs, 89% agreed that high cybersecurity maturity will be a distinct competitive advantage for selling vehicles in the future (see Hypothesis no. 2), and two thirds agreed that connected and autonomous driving will greatly change previous market shares (see Hypothesis no. 9).

Existing cybersecurity capabilities are important USPs, especially in the current development phase. This is particularly true for suppliers, as they have not yet been directly affected by regulation. However, as global norms for CSMS mature and become standardised, this USP will increasingly become a fundamental requirement for doing business as an automotive supplier.

Fig. 17 In which area are you using the most third-party support for implementing your CSMS/CSMS requirements?



C | Outlook and conclusion

Innovation is inevitable

Technology in the automotive sector is evolving at an incredible rate. This is generating new and challenging threats for the industry and its customers, potentially costing companies huge sums of money – or even human lives when cars are on the road.

Vehicles and the environment they drive within will be heavily influenced by developments such as 5G (and beyond), improved sensors, optical image processing and quantum computing. Software will be key: modular and scalable software and computing power within vehicles will enable companies to produce and operate vehicles cost-effectively in the long term.

Responses need a boost

Governments and institutions are attempting to respond to these technological innovations by launching new and increasingly strict regulations and standards. So far, however, these efforts have been too vague to actually provide the protection that their authors want. It is up to the manufacturer to flesh it out and even gain a competitive advantage through smart and business strategy driven cybersecurity management.

Our survey has shown that OEMs are already taking action by developing CSMS designs and taking initial measures. This is a promising starting point, but the maturity and scope of these measures need to improve. Suppliers have made less progress than OEMs on their CSMS journeys, but both OEMs and suppliers need to advance their efforts to integrate CSMS with other systems for management, compliance and governance.

The road is long and winding

CSMS projects are clearly full of new challenges, while also requiring substantial amounts of time and money. It will be important for business leaders and senior managers to understand the importance of CSMS – and their potential to open up exciting competitive advantages for trailblazing companies. Interestingly, the respondents were almost unanimous in their agreement that UNECE Regulation No. 155 will lead to safer and more secure vehicles, despite the investments that it will make necessary. When all is said and done, safety and security is the key factor in this discussion.

Overall, the automotive industry is typified by a lack of consistency and transparency when it comes to

addressing cybersecurity threats related to connected vehicles. The industry has yet to establish an effective approach that brings together the various influences, including technological progress, regulation, competition and customer expectations. New market players may have a more streamlined backend and technological structure, but established players have a lot of experience in complying with new regulations. The interviews for this survey also revealed an almost total lack of focus on securing sales organisations, which is just one revealing sign that the full value chain is not even close to being covered. Creating uniform standards and a common set of requirements for CSMS would be extremely valuable in promoting progress in this area.

Contrasting CSMS facts	OEMs	Supplier
Progress of initial CSMS projects	71%	59%
Estimated CSMS maturity level (0–5)	Ø 2.1	Ø 1.2
Estimation of global competitors successfully assessed a CSMS	43%	26%





Recommendations

■ Anticipate regulations

Since the average CSMS project duration is 30 months, companies who have not already been on the road for a long time must be fast and check upcoming regulatory and contractual requirements in all relevant markets. OEMs should take a results-oriented approach and adhere closely to the assessment specifications of the national approval authorities.

■ Develop business strategy

Large and complex projects, even if they are necessary from a regulatory standpoint, should always follow the business transformation strategy.

■ Exploit synergies

In view of the strong cost and time pressure: To achieve synergies, companies should use structures of existing management systems to design and implement their CSMS. This includes

the use of standard processes and tools to avoid complexity and customization before common interpretations and market standards are established.

■ Increase maturity

The maturity of the CSMS needs to be increased. This includes the measurement and reporting of the maturity within the own company, but also with the business partners in the value chain. While the identification of risks works for many participants, it is important to make them controllable also from a management perspective.

■ Test for practicality

After designing a CSMS companies should conduct a dry run to validate whether their CSMS work effectively and resource-saving in operations.

■ Prioritize software

Software is Key: Specify clear requirements for the software architecture and place them in your own value chain to ensure the secure integration of OEM and supplier software.

It's time to put the pedal to the metal for CSMS

OEMs need to make strategic decisions about their positioning and product portfolios. UNECE Regulations No. 155 and 156 provide a good starting point, but still do not go far enough: more specific guideline is needed, covering all markets and taking all areas of law into account. At present, alternative regulations continue to exist for significant automotive markets – in some cases imposing different requirements. OEMs are therefore currently in a position that requires decisions about target regions and markets for products and ecosystems to be made at the development stage. Some companies may struggle when attempting to develop universal products. However, effective decision-making will generate a significant competitive advantage if sufficient scalability can be maintained.

Looking ahead, the ecosystem around road vehicles is set to undergo massive expansion. Customer expectations are rising, and increasingly attractive business opportunities are emerging for companies willing to embrace the potential to position vehicles as a place for other companies to sell their services – from TV streaming to remote working. An effective CSMS protects this valuable ecosystem and is therefore business-critical from several points of view.

A CSMS is and will continue to be a basic requirement for vehicles to be registered and produced in many markets worldwide. Violation of compliance requirements can lead to the revocation of operating licences for entire vehicle fleets, and to the threat of fines and major legal disputes.

Moreover, continuously operated cybersecurity has a significant impact on vehicle costs. A smart CSMS in combination with a modular and scalable software architecture will determine how cost-efficiently the ecosystem can be operated throughout its life cycle.

Finally, a CSMS not only protects people but also the basis for substantial future revenues and new data- and service-driven business models centred around the new living and working place: the car.

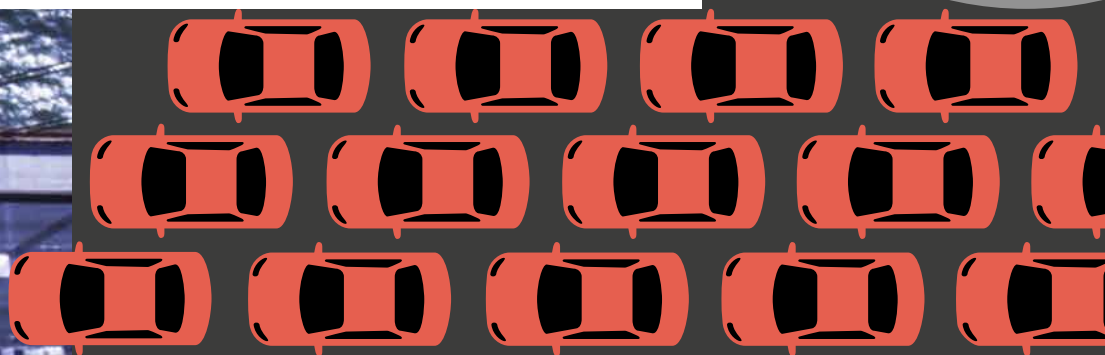
The course has been set. Any company hoping to enjoy success in this market must keep up with the pace of the automotive transformation.

Overall, there's a long and winding road ahead to achieve secure and efficient automotive ecosystems – and it will take teamwork, speed and navigation skill to reach that destination.



Survey methodology

PwC's Global Automotive Cyber Security Management System (CSMS) Survey involved semi-structured 60-minute interviews with 30 representatives from the automotive sector, mainly with roles in product security, R&D, quality assurance and information security. The interviews were conducted during March and April 2022, using a web-based questionnaire. 39% of respondents work for OEMs and 35% work for suppliers, while the remaining 26% are market experts. Most respondents are at management level (78%), with 13% at expert level and 9% at general staff level. They are based in 11 different countries: Austria, the Czech Republic, Finland, France, Germany, Italy, Japan, South Korea, Sweden, the UK and the USA. Data has been anonymised, and was rounded for use in graphics.



Contact us

PwC is a trusted partner for businesses in the automotive sector. We share our knowledge of major trends and help our clients prepare for upcoming bumps in the road. Our cross-functional teams quickly identify and implement innovative

and sustainable solutions to key challenges. And we combine our global perspective with knowledge of local legislation to guide our clients on their journeys towards meeting evolving customer demands.

Together, we will make sure your business is ready for the future – wherever the road takes us.



Harald Wimmer

Global Automotive Leader
Partner, PwC Germany
Tel: +49 221 2084-240
harald.wimmer@pwc.com



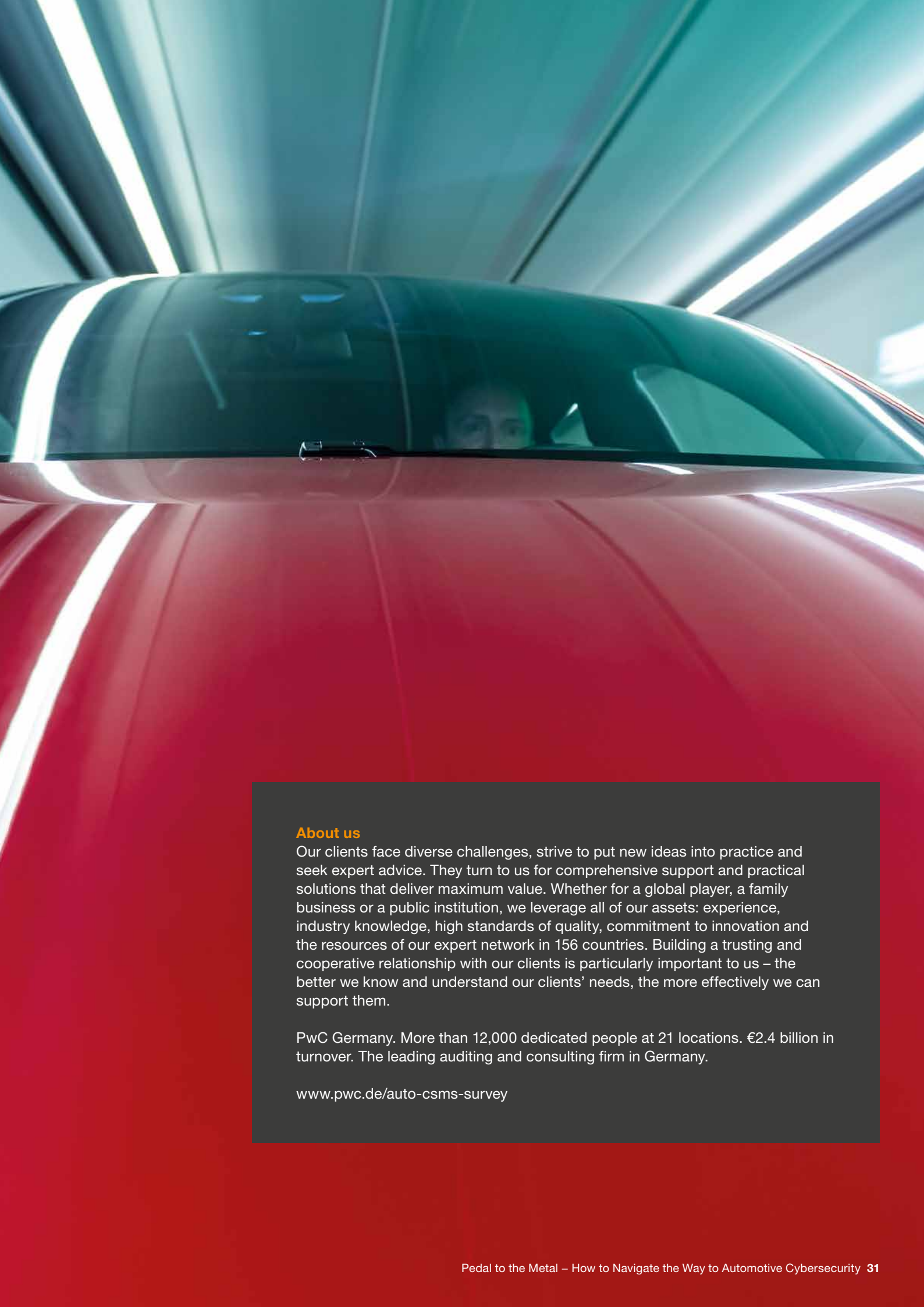
Joachim Mohs

Global Industrial Manufacturing
and Automotive, Cybersecurity
and Privacy Leader
Partner, PwC Germany
Tel: +49 040 6378-1838
joachim.mohs@pwc.com

Find out more and tell us what matters to you by visiting us at:

Global Automotive:
www.pwc.com/gx/en/industries/automotive.html

Global Cybersecurity:
<https://www.pwc.com/gx/cybersecurity>



About us

Our clients face diverse challenges, strive to put new ideas into practice and seek expert advice. They turn to us for comprehensive support and practical solutions that deliver maximum value. Whether for a global player, a family business or a public institution, we leverage all of our assets: experience, industry knowledge, high standards of quality, commitment to innovation and the resources of our expert network in 156 countries. Building a trusting and cooperative relationship with our clients is particularly important to us – the better we know and understand our clients' needs, the more effectively we can support them.

PwC Germany. More than 12,000 dedicated people at 21 locations. €2.4 billion in turnover. The leading auditing and consulting firm in Germany.

www.pwc.de/auto-csms-survey

