Deloitte.

Automotive Software Quality

What do OEM's
have to consider for the future?

The automotive industry is undergoing a profound change. Manufacturers, industry associations and policy makers must react as quickly as possible to technical and social megatrends and adapt to changing legal and economic conditions. For the first time, software is playing a decisive role in the competitiveness of car manufacturers.

From a global perspective, there is no alternative to the development of autonomous cars.

The development of highly automated vehicles for road traffic requires enormous investment. The global R&D expenditures of the German automotive industry are growing at a significant double-digit rate each year and passed the 39 billion euro mark in 2015 – further increases are to be expected due to impending challenges in the next few years. For this investment to be profitable, the market must both accept and demand highly automated vehicles. To ensure market success, two factors are vital:

- Demand needs to be created, for example by offering solutions providing better comfort, increasing time gains and improving safety. Future consumers will consider prestige and technological leadership to be less important than mobility and environmental aspects.

- Apart from promoting the benefits of automated vehicles, building sustainable trust in the new technology is a key factor in achieving long-term success. Highly developed and creative technology, on its own, will only result in short-term demand. Preceding technological hype will result in negative market reactions and disappointment, if the quality and reliability of the technology cannot be guaranteed. A lack of quality in the case of highly automated vehicles is not only annoying – it is dangerous. The biggest challenge to deal with is the fact that someone who does not have their hands on the steering wheel tends to feel vulnerable and assesses risks to be very high. Instances such as the deadly accident of a Tesla vehicle in the summer of 2016 – which drove into a cruising truck, after the activated autopilot mistook the truck's white side-wall for free space – might have strengthened this perception.

A recent study by Deloitte[1] illustrates the current perception of automated cars:

Only in China and India do more than half of the respondents accept highly automated cars (semi-autonomous and autonomous driving). In traditional car manufacturing countries such as the US, Japan, South Korea, and Germany, the acceptance is significantly below 50%. Germany ranks last with an acceptance of less than 25%. The good news is that, across all countries surveyed, the interest in semi-autonomous and autonomous driving is highest among the younger generations (generations Y and Z). The main reason for this surprisingly low acceptance is the consumers' feeling of insecurity in relation to highly automated cars. The number of respondents expressing such fears varies between 62% (China) and 81% (South Korea). Germany has an average fear rate of approximately 72%. Potential customers become somewhat more confident if, for a certain period of time, highly

[1] What's ahead for fully autonomous driving - Consumer opinions on advanced vehicle technology - Perspectives from Deloitte's Global Automotive Consumer Study (22,000 respondents from 17 countries).

Increasing requirements with regard to performance, compatibility, and maintenance of IT components force increased standardization.

automated vehicles can demonstrate that they are safe. Under these circumstances, 47% (Germany) to 81% (China) of all respondents would agree to using such vehicles.

Compared to conventional cars, it is obvious that higher safety and greater comfort is insufficient to lead highly automated cars to market success. Manufacturers need to find ways to build and maintain confidence in this technology. If traditional manufacturers cannot cope with this requirement, new companies are ready to take over their role.

From a global perspective, there is no alternative to the development of autonomous cars: they have the potential to significantly change car traffic, especially in urban areas. The space available for traffic and parking will become increasingly scarce and expensive. In addition, the costs of individual car ownership are rising. Alternative ownership forms of personal mobility, such as publicly available shared vehicles, offer an improvement in terms of costs, convenience, and safety. Autonomous cars are better suited to this purpose than individual vehicles.

The market is changing in four main areas:

- A current focus is on the introduction of emission-free vehicles, including their charging infrastructure, enabling high performance and long range. Affordability is crucial to making the transition from fossil to electrical energy attractive.
- Assistance systems are growing in importance, culminating in autonomous driving. For this reason, vehicles must communicate with each other, as well as with infrastructure components surrounding them.
- In the end, vehicles will become more and more digital, enabling their users to communicate, work, or enjoy multimedia entertainment while driving.
- The increase in autonomous driving functions, combined with the possibility of individualizing cars driven by software, leads to the great attractiveness of "shared cars". Specialized mobility providers will keep their fleet of cars permanently available, which creates an interesting transportation alternative to rental companies, especially for short distances in urban areas. These mobility providers will use, on a wide scale, exclusive parking lots for their fleet, making the search for scarce and expensive parking spaces unnecessary.

In all these domains, data and software are used to communicate and process central functions. Stakeholders comprise OEMs (development, production, quality assurance, and IT departmentsC), IT service providers (cloud services and telecommunication), legislators, and standardization bodies. All stakeholders will have to answer four questions regarding the role of software in a vehicle:

1. How will the quality of software-driven functions in cars be defined and ensured?
2. How can car manufacturers protect their brands from damage and themselves from suffering the legal consequences of quality issues? And what role does software development play in this regard?
3. What challenges arise for OEMs from the security and data protection requirements of networking vehicles and connected infrastructure (such as cybersecurity requirements)? How can manufacturers meet them?
4. Is there a need for additional legal regulations (such as further type approval requirements/audits) to account for the changes in the vehicle as well as the overall traffic?

In this paper, we draw on experiences gained from past and present projects in the automotive sector.

1. How will the quality of software-driven functions in cars be defined and ensured?

There is still a lot of work to be done: neither comprehensive nor generally applicable regulatory standards exist that could be set as requirements for type approvals. Nor is there a software (!) quality assurance measure (certification processes) available to car manufacturers. Current development guidelines (e.g., ISO 26262) or audit standards such as Automotive Spice, CMMI and Misra ensure a well-structured and reliable process. They are based on the assumption that a good process will lead to a good result. However, checks, as appropriate for the complexity and functional scope of the software controlling the vehicles, are not part of these standards. Such checks are only conducted in exceptional cases.

Current tests are based on risk scenarios and test procedures. These differ for each OEM and supplier. ISO 26262 correctly requires that tests have a different precision and intensity, depending on the risk assessment for the functions and modules developed. Yet testing depends on evaluations made by individuals or processes established in a company. Testing can also be heavily influenced by time pressure relating to the SOP (Start of Production). At present, no general and mandatory set of risk and test scenarios exists.

Developing such a set of risk test scenarios would be expensive and time-consuming for OEMs. As an alternative, the legislator could provide relief by defining minimum requirements for safety and reliability, which could be implemented through car type approvals. However, a German attempt at going it alone would be neither efficient nor permissible. Instead, the requirements of German law must be coordinated at the European level and agreed upon at the UN and G7 levels.

Examples already exist in the aviation industry, and also in the medical apparatus industry.

Increasing requirements with regard to performance, compatibility, and maintenance of IT components force increased standardization. This puts the focus of vehicle safety increasingly on cybersecurity, making it an integral part of software quality. This is not like current vehicles, which are somewhat protected from massive hacker attacks or computer virus attacks through their proprietary, individual architectures.

Standardization of vehicle architecture will change this. Therefore, measures to secure rolling data centers and online backbones (cloud services) are crucial and have to become part of future risk scenarios and test requirements. The German, American, and Japanese governments have all issued corresponding instructions and guidelines.

Software will mainly influence the future in automotive development.

Automotive manufacturers and their suppliers strive for the highest quality. This notion is reflected in the reliability and longevity of modern cars, while performance and functionality are continuously improved. Rusty car bodies, frequent tire punctures, permanent refilling of engine oil etc. are predominantly problems of the past. These problems have one thing in common: they all concern hardware failures. Yet developing software will mainly influence future development in automotive development and software requires new quality mechanisms.

A number of reasons play a role in this:

Dynamics
While the car body and engine parts do not change over their respective life cycles, software is highly dynamic. The reason is the need for ever-evolving new functions and mandatory updates to correct mistakes and mitigate risks (especially concerning the potential risks of cyberattacks).

Life Cycle
The life cycles of software and hardware differ fundamentally from each other in nearly all phases, from development to production, exploitation, and resale or scrapping. Some examples to highlight the need for a differentiated approach: terms of use of software (licensing), usage transition of installed additional car features, transmission of privacy policies when cars are used by different users, data erasure in case of resale or at the end of use, and ensuring the long-term compatibility of formats for data exchange.

Complexity

Software is not just one component of the vehicle, it is one of a number of components (ECUs), which fulfill different tasks. Even the tires, shock absorbers, and wishbones of new vehicles have sensors which generate data and statuses – transmed through either the wiring or integrated software modules. In any case, the many sensors, actuators, and control units create a lot of data traffic, which must be sent, received, understood and interpreted. Information from outside the vehicle is increasingly adding to this volume of data, e.g., navigation systems (including telematics services). In future, short-term radio communications between vehicles (car to car) or between a vehicle and external components (car to infrastructure) may add to the external communication. The quantity of data and the different processing mechanisms are growing increasingly complex, always creating new challenges. This development is not comparable to the development of hardware.

Test methods

The functionality of a vehicle's hardware is finite, even considering every hardware interaction, and can be examined after a stringent quality assurance of single components. Various testing methods in virtual and real surroundings, such as test benches, test tracks or the street, have been developed. By contrast, software is too complex for comprehensive testing of all components. There are simply too many functions, hence software should never be seen as being without errors. Test procedures are aimed at covering specific risks. Test methods such as HIL, SIL, or VIL[2] aim to achieve the highest possible coverage. It is important that the covered risk scenarios and corresponding tests have already been developed during the conceptual phase of the software (security by design). A retroactive roll-back of the functions developed is bound to lead to errors and quality gaps. The more centralized the vehicle architecture is, the better tests can be prepared and carried out. Decentralized modules must be tested completely, according to their functional scope, before being included in an integration test.

[2] Hardware in the Loop, Software in the Loop, Vehicle in the Loop.

Supply Chain

An integrated approach to software development and coordinated testing is currently prevented by the complexity of the supply chain structure, typical for the sector. Most software in cars is supplied by third-party providers. Development and testing procedures, and also the source code, are often inaccessible to car manufacturers.

OEMs require suppliers to use the above-mentioned procedures for quality assurance (Spice, CMMI, Misra etc.), in the form of contractual guarantees and spot tests. However, an examination of the content, the proof of successful testing, or spot checking of source code are seldom performed.

Cross-linking of components

In car manufacturing companies, the departments responsible for vehicle and data security do not necessarily work together systematically – or even understand each other sufficiently. In addition to that: in the near future, cars will be part of a high-performance network, which will also include platform technologies and components from third-party providers. Future security concepts will have to take this high degree of cross-linking into account. Today, this is not yet done sufficiently.

IT competence development

The classic car manufacturers are still not positioned and well enough equipped to comprehensively ensure the application of secure IT-relevant criteria – mainly data integrity, reliability, and availability of the software. OEMs need to develop these competences and establish relevant testing procedures. It is imperative to create a database of all imaginable risk scenarios and to update it constantly, as soon as new risks emerge, as in the aviation and medical technology industries. Extended security and practical tests will be mandatory for future type approvals of partially or completely autonomous vehicles. Car manufacturers should prepare themselves adequately.

Today's luxury cars have more than 100 million lines of source code, encompassing control and steering, assistance, and multimedia functionalities from a variety of suppliers.

2. How can car manufacturers protect their brands from damage and themselves from suffering the legal consequences of quality issues? And what role does software development play in this respect?

Drivers of highly automated vehicles want to be safe; quality requirements for software must take this into account. Should an accident happen which is not caused by drivers, liability may become an issue. If drivers were to be liable for a software problem not known to them, the car would not find acceptance. Every software decision must therefore be documented, because correct decisions can also cause an accident, e.g., the alternative may lead to worse effects. An example: a vehicle hits another vehicle to avoid a person on the street.

The following discussion concerns one central question: can customers trust OEMs and their products? Two important software and data privacy aspects have to be considered:

Black Box vs. Open Systems

OEMs face major challenges to ensure and maintain a comprehensive promise of quality and to document automated decisions of vehicles, since the built-in software is produced predominantly by parts and component suppliers (including global players as well as small innovative development companies). These companies are protected by intellectual property rights laws. For this reason, the source code is rarely disclosed and is like a black box in most cases. Consequently, quality risks are hidden, and it is difficult to assess

how software decisions are taken. Car manufacturers will have to take these issues into account when designing and stipulating contracts with their suppliers. Ultimately, this will have far-reaching consequences for testing, reviewing, and auditing processes.

Retaining Consumer Trust

Compared to big IT companies, today's car manufacturers enjoy considerably greater consumer trust with regard to product quality and the administration of data. Currently both hardware and software are provided from a single source, i.e., the manufacturer. The automobile OEM's claims to high quality are known and have led to high quality and extremely reliable vehicles on our streets. It is critical for the manufacturer's success to extend this claim of high quality to the development and maintenance of software. This helps OEMs to retain the high level of trust over big IT groups or emerging newcomers in the mobility playground.

Customers trust OEMs in respect of their personal data. The past has shown OEMs to be trustworthy in the administration of personal data, by contrast to companies such as Microsoft, Google, Apple etc. There has scarcely been a scandal shocking the automotive industry so far. Notwithstanding this, the intensive use of data by OEMs is still in its infancy. However, software applications for communications and media usage are on the rise and will grow in importance, especially for autonomous vehicles. In order to achieve an individual and integrated functionality, similar to our smartphone experience, a plethora of data has to be exchanged and crosslinked. The ubiquitous challenge in this context will be the appropriate balance between the minimal use of personal data and the perfect costumer experience – including a high level of data protection. This data protection has to apply to applications from third party suppliers, potential marketplaces for applications sales, and to any digital backbones used by the vehicle.

As a solution, an independent "trust center" could be implemented for the administration of vehicle-related data. This would ensure compliance with data privacy and security principles, by providing service providers with processed data, in conformity with the law. The trust center would epitomize a trustworthy third party and act as a facilitator between the data owner and the potential data user. This trust center would assess data inquiries and only answer those complying with data privacy regulations.

Today's luxury cars have more than 100 million lines of source code, encompassing control and steering, assistance, and multimedia functionalities from a variety of suppliers. In order to handle this complexity, to further enhance the speed of development cycles, and to facilitate fast online updates, new methods of development and forms of collaboration throughout the entire supply chain are essential. In the following, the most eminent features of this topic will be discussed.

Only an open system architecture can be fully assessed and enhanced

Nowadays, software features in cars are developed in line with ISO 26262. Car manufacturers and suppliers rarely cooperate in this process, even though it is of pivotal importance for a continuous process of software enhancement and development. Car modules including software provided and delivered by suppliers are still treated as black boxes.

Applying traditional and established automotive supply chain processes to software will eventually lead to a deadlock. Current process designs cannot provide the required speed of development, security/ integrity and transparency since the all-embracing product overview is not provided. As a result, the quality of software is ultimately compromised. Although most vehicles differ in their communication networks, the major part of information is transferred via the CAN-Bus-Architecture and distributed electronic control units (ECU). An open system architecture, presumably based on a well-established and high-performance operating system, e.g., Linux, will ultimately replace the proprietary architecture of today's cars. Developments are moving towards a much stronger centralization of the IT architecture in the vehicle by means of which certain functionalities or apps are deployed on a standardized operating system.. Access to the hardware will be limited to the operating system, much like modern IT architectures.

In the medium and long run, such architectures will facilitate easy and fast maintenance and the enhancement of functions. Moreover, development processes can focus on the main functions within certain standards. In addition, tests, documentation, and collaboration throughout the entire supply chain will be facilitated. In this context, the software development association AUTOSAR[3] is performing substantial pioneer work by designing an industry standard for system software in vehicles.

A number of manufacturers have already announced that they will disclose their architectures. This is based on the OEM's desire to defend themselves against powerful new competitors, who could enter the market through cross-sector cooperation. Prime suspects are companies that already produce operating systems/ have experience in the data business, e.g. Apple, Microsoft, Google etc. However, for such publicly announced initiatives, the affected manufacturer and manufacturing groups in the automotive industry lack the following:

1. The intellectual property of the components which are produced throughout the automotive value chain. Therefore, only parts of an (operating) system can be opened without violating the intellectual property rights of others.
2. Agile and nonetheless reliable methods of software development, which could compete with the procedures developed by IT and internet giants over several decades.

It is therefore not surprising that a company which is quite negligible in terms of its market share has mixed up the whole automotive industry and is setting trends in terms of technology: unlike conventional manufacturers and their relatively inflexible structures, Tesla has had the opportunity to build a company on a green field site and to align it with upcoming technological challenges.

One focal point is the rapid and reliable development of software which provides basic functionality and data security and can be enhanced by constant updates, as do competitors from the IT and internet environment. Like operating systems for computers and mobile phones, the user (here: the driver) provides the relevant data for improvements. In general, this does not happen actively but via protocols which are automatically transmitted from the operating system of the vehicle. It therefore makes sense that Tesla owns essential parts of the intellectual property and uses agile development methods. It is not for no reason that some of the big conventional vehicle manufacturers consider Tesla as a major competitor. They know why.

Without any doubt, the large OEMs around the world are (still) able to build superior cars. However, traditional car manufacturers still measure quality based on traditional parameters, e.g. gap dimensions. Furthermore, the construction of a vehicle is fully completed before market introduction. Thus OEMs try to avoid any further adjustments. By contrast, Tesla has ensured its software quality by issuing 200 online updates over the past year. This keeps the functionality of Tesla's vehicles up-to-date, even enabling later enhancements. Updates are partly optional for vehicle owners, thus, the business of the future is already reality. Conventional OEMs mainly interpret product care as the development of the next vehicle generation, e.g. a facelift to a model series. Tesla continues to take care for its products, even if they are already on the market. This approach has been mainly known from IT products and TC terminal devices. This does not mean that Tesla has chosen the best path, just a different one. Using drivers and their vehicles as beta testers can occasionally lead to dangerous situations. The combination of the advantages of both alternatives are the way for the future: on the one hand extensive quality requirements and the desire to introduce matured functionality into the market, on the other, agile methods of development and sophisticated approaches to incremental tests, online update ability and a permanent improvement claim.

[3] AUTomotive Open System ARchitecture

Initial attempts by OEMs to build up small, flexible, legally independent business units with essential development responsibilities, are a step in the right direction. However, OEMs still primarily rely on existing structures for the implementation. Ultimately, all innovative ideas are in danger of coming to a halt at this point. In the medium term, there is thus no alternative but to develop a new organization for themselves and their supply chains.

3. What challenges arise for OEMs from the security and data protection requirements of networked vehicles and connected infrastructure (such as cybersecurity requirements)? How can manufacturers meet these?

Cars are becoming increasingly interconnected, internally as well as with the internet. However, nowadays they are less effectively protected than office computers, mobile phones, and tablets. To change that, the whole quality and safety process must be adapted according to ISO 26262. The industry needs cyber-specific risk scenarios, which need to be implemented in software development as well as in the component manufacturing process.

Maintenance platforms for the online access of a manufacturer and its workshops are a mandatory component of those scenarios and therefore part of comprehensive security governance, aiming to make the vehicles resistant to cyberattacks.

In this respect, ISO 21434, a new standard currently being developed for automotive cybersecurity, could become useful: however, the outlined principles of this standard must be implemented and – quite importantly! – monitored in the research and development processes of the whole supply chain. As both the ISO Standard and type approval are simultaneously evolving, it is currently not yet assured that the future requirements for type approval, including possible additional tests of technical services, fully correspond to the ISO 21434 standard. It is only certain that regulatory requirements will focus on far more than cybersecurity. The quality of the software used in vehicles, as well as the protection of personal data, will play a major role and will need to be included in the risk and test scenarios of both manufacturers and their suppliers.

Online updates of vehicle software without a workshop visit are indispensable from a safety and security point of view.

Remote maintenance and online-updates

Online updates of vehicle software without a workshop visit are indispensable from a safety and security point of view.

However, all functions facilitating online or over-the-air updates need to be designed in such a way that spontaneous and unforeseen unavailability of the car or the owner's rejection of internet access will not lead to serious errors. How should a manufacturer or workshop react when it notices a critical safety error occurring in the car, but the car owner does not respond? Some manufacturers already have the possibility of shutting down the vehicle online. In this case, the question arises of whether such a reaction will be acceptable or even obligatory from a legal perspective in the future?

The possibility of online updates is an essential requirement for the above-mentioned software development methods, which focus on a faster, more agile process. Furthermore, online updates also enable the actualization and (fee-based) extension of the vehicle's functionality. The requirements on the updates in terms of quality and security are thereby on the same level as the initial core software. Interfaces for online updates, as well as the underlying backbones of global cloud-systems, are a relatively new field for OEMs. The strict requirements of those systems with respect to security and data protection can also be ensured with the help of trusted third parties.

Safety-relevant or not?

All electronic components have to be classified as to whether and to what extent they influence vehicle safety. In principle, ISO 26262 prescribes similar requirements, specifically the classification of each component to an "Automotive Safety Integrity Level" (ASIL). The criteria of this classification and the corresponding process must be obligatory across sectors. Multimedia and business applications can be considered uncritical for safety and can therefore be opened to third parties via an API (programming interface). All systems with an impact on driving behavior must be separated.

This means: every vehicle will consist of two system platforms. Regardless of this, an interface is needed for applications which require access to both platforms. For example, a tour guide (not a safety-relevant component) uses data from the navigation system, which is highly important for operational safety, especially that of autonomous vehicles.

Controlled changes in this area influence safety and security on one hand and the efficiency and agility of software development on the other. Another important competitive factor is the possibility of integrating third parties securely and can thus have a major impact on comfort, performance, and the features of the car.

Increased competition through lower market entry barriers

Car manufacturers will no longer only compete with peers but also with IT and internet companies. The market entry barriers in the automotive sector are being lowered, mainly due to the rise of electric mobility. The expertise of classic car manufacturers and suppliers is the extremely complex drivetrain, including the engine, clutch, gears, differential, drive shaft, and wheel, as well as electronical components such as ABS and ESP. However, if every wheel has its own electric motor, the software takes over the majority of the functions of the drivetrain.

In the long run, the market will break down into a hardware, a software, and a service-market. In line with conventional data processing and mobile devices industries, the hardware market will be characterized by low margins and – at least initially – by overcapacities. By contrast, noticeable margins and the essential business lie in the software and service industries. This enables new competitors with core competencies far away from the design and construction of vehicles to gain market access. Apart from well-known companies such as Apple, Microsof, and Google, service companies such as Uber and Lyft will develop and exploit new business models. Some OEMs are already trying to position themselves in the service sector, however they have severe shortfalls regarding agile and rapid software development and their supply chain. In these areas, Apple, Google, and Microsoft have a clear competitive advantage over conventional vehicle manufacturers. OEMs can only compete by abandoning old habits and entering comprehensive vertical and horizontal cooperation (e.g., the map service HERE). The failure to adapt will result in falling far behind, from which a recovery may be impossible.

In the long run, the market will break down into a hardware, a software, and a service-market.

4. Is there a need for additional legal regulations (such as further type approval requirements/ audits) to account for the changes in the vehicle as well as overall traffic?

Regulation prevents reasonable economic behavior and slows down innovation – this doctrine is not always true. The situation of the automotive industry is extremely complex because of dynamically emerging actors, disruptive technological changes, and the general importance of the automotive industry due to its sheer size. Regulatory action, following a certain vision and claim of intuition could pool forces, initiate or strengthen developments, and thus promote innovation.

It is mandatory to regulate some issues because an ethically correct decision is more important than the technical or economic interests of OEMs. A major contribution is made by the ethics committee of the German Department of Transportation which is composed of legal, societal, ethical, technical, and economic experts. This commission and other working groups in the Ministries are trying to answer fundamental questions concerning autonomous driving. Some examples are:

- Which driving situations can be decided autonomously, which cannot?
- Should safety and security standards be stipulated by law to prevent the level of safety being dependent on the price of the car and thus on the buyer's income?
- To what extent do insurance companies have to accept liability for autonomous driving?
- Who owns the data (Big Data) generated by autonomous cars?
- What should be paramount: data protection or storage of data for an extended period of time? This is important to determine guilt in the case of accidents or for the ever more important communication between car and infrastructure.

These questions are not merely of an ethical nature. They have a huge impact on the competitive situation. Since software and data will become more important than the production of vehicles in the long run, OEMs face a major challenge. On the one hand they need to develop a software system which controls the individual vehicle units directly, on the other to develop the operating system for overarching coordination. This software must not only be accepted by the market but must also be able to compete with new actors from the IT industry.

Further regulation will be introduced, since it can no longer be ignored that software controls the vehicle in an increasing number of situations, e.g. the regulation of the compressive forces for electrically operated windows to prevent injuries from trapping your hands. Failure to comply with such regulations will not only affect the hands caught. Certain requirements cannot be left to the competition of price and cost in the market. Regulation needs to set and enforce standards. It can thus provide a basic security which manufacturers are forced to comply with.

The biggest lever for the regulator is type approval. As vehicle traffic has already assumed global dimensions, it not possible for any country to find a solution independently. All measures need to be coordinated at the EU, G7 and UN levels (Vienna Convention on road traffic). It is in the interests of the population and the automotive industry that high safety standards be set. This has two main reasons: first of all, German OEMs could lose their good reputation for safety and quality. Secondly, for semi-autonomous and autonomous vehicles to successfully navigate in German's dense traffic, these cars will have to comply with high standards. This might ultimately lead to a competitive advantage on global markets.

Mandatory standard for system software

A joint effort by OEMs may increase the likelihood of success, but such attempts are unlikely to happen without regulating the terms of competition. Currently, competition is too strong and the legitimate fear of antitrust sanctions too great. The creation of safety and security standards, either through laws or by existing standardization organizations such as ISO or SAE, would be very likely to have a favorable effect. An operating system developed centrally for a majority of OEMs would only need a single set of updates if new security risks should emerge. Interfaces and the certification relevant for type approvals would only have to be defined and issued once. This could ultimately lead to a greater focus on quality and reliability due to less competition and less time pressure.

Data privacy

Equally, the security of personal data will not be possible without regulation. On the one hand there is the risk that strong European data privacy rules will block innovations in car communications ("car to car" and "car to x"), vital for autonomous traffic. On the other, strict, comprehensible data privacy is essential for establishing the consumer trust necessary for technological upheavals (such as the one currently occurring in the automotive industry). There are therefore good prospects that sensible regulations will promote the development of modern vehicles and a forward-thinking transport infrastructure, at least in Europe.

A significant contribution can also be made via the conception and development of software and interfaces in vehicles. "Privacy by design" is the key term in this context. Most functions that require data, such as autonomous driving or additional user services, can be achieved without the transfer of personal data. This is at least the case if it is already considered and implemented at the conceptual stage. For all other applications, it is necessary to have either the user's consent (known from smartphones) or a law superior to data privacy (e.g. a black box to record driving movements).

The initiative should originate from the OEMs and could be promoted and secured with the help of external third parties, i.e., trustees for the lawful usage and administration of data. Without such initiatives, the legislator will set the legal framework. This might be stricter than the stakeholders of the automotive industry would wish for.

At the moment there are many parallel developments in the automotive industry, from which questions arise regarding the future balance of this globally important economic sector. New actors will enter the market, while traditional players could disappear. Disruptive technologies are a catalyst for such developments. It is important not to forget the customer in this technological race because even these data centers on wheels need to be bought and used by somebody.

Important issues are and will remain: car reliability, security, quality, and the manufacturer's benefit promise, which must be in a well-balanced ratio between acquisition and maintenance costs. Various customer groups will evaluate these factors differently.

One thing is for sure: these issues will remain exciting.

Safety and Security – what is the difference?

At first glance, both terms refer to the same idea – but their meaning differs in the context of the automotive industry.

Safety describes the effort to prevent mistakes in the core functions of a vehicle or, in a worst case, to protect the occupants and other persons involved from harm. Components such as brakes, steering, airbags, and the crumple zone of a car, but also electronic assistants such as ESP or ABS are critical to safety.

Security, on the other hand, means the security of software systems against malfunctions and external attacks. Software in cars has various roles: engine control, external communications, but also car safety and security.

Contacts

Andreas Herzig
Partner Risk Advisory
Tel: +49 (0)711 16554 7160
aherzig@deloitte.de

Peter Wirnsperger
Partner Risk Advisory
Tel: +49 (0)40 32080 4675
pwirnsperger@deloitte.de

Ingo Dassow
Director Risk Advisory
Tel: +49 (0)30 25468 451
idassow@deloitte.de

Deloitte.

Issued 8/2017