The Future of Mobility is here

Navigating a regulatory blueprint for type approval of Level 4 Autonomous Driving

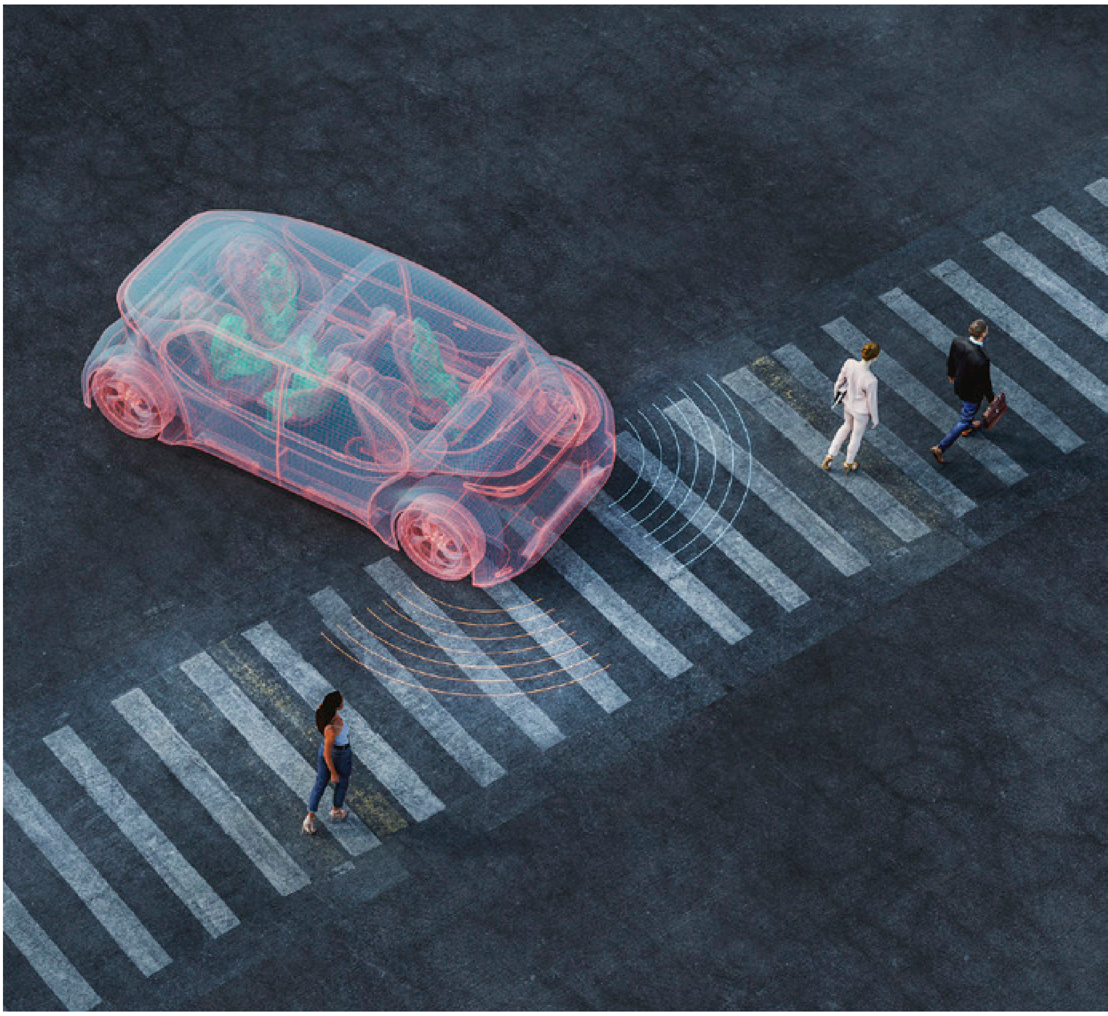


Table Of Contents

Introduction

A new era of human mobility has begun and what seemed only very recently to be part of a distant future is now rapidly becoming a reality: Fully Autonomous Driving within an Operational Design Domain allows vehicles to drive without the need of their driver's attention.

Technological breakthroughs in Artificial Intelligence (AI), sensors, and connectivity induced a worldwide race for the first approvable fully Autonomous Driving system. These innovations continue to disrupt the mobility industry and have brought the autonomous revolution in noticeable reach. In a matter of months, the first highly automated vehicles could come to German public roads and change the way we travel and commute.

High quality standards and well-founded regulations are indispensable enablers for these developments. Concerns prompted by risks associated with autonomously operating vehicles must be overcome by ensuring their safety and reliability. The notion that a machine can make independent decisions with potentially detrimental effects on the well-being of humans is frightening for many people. A fit-for-purpose approval process is thus crucial to meet these safety concerns and enable a rapid market penetration of autonomous vehicles. Only by putting trust into the center of the development, regulation, and operation of Autonomous Driving systems from the get-go, the uneasiness of stepping into a driverless vehicle can be successfully addressed.

Lawmakers in Germany recognised this need early on and created an unprecedented legislative framework. The Autonomous Driving Act and the recently published Autonomous Vehicle Approval and Operation Ordinance (AFGBV) allow the approval and operation of autonomous vehicles (SAE Level 4) on public roads. Germany has become a global front-runner in regulation but meeting all relevant requirements of the AFGBV remains a significant challenge for suppliers, manufacturers, and operators of Autonomous Driving systems. Furthermore, other emerging standards and regulations addressing idiosyncratic risks of new technologies like AI add complexity to the task of receiving type approval for autonomous vehicles.

Given that the regulatory landscape is highly dynamic and complex, practical organisational approaches are required in order to comply with all relevant legal obligations. This whitepaper, therefore, provides practical insights on how to meet existing and arising obligations through adaptive governance and compliance systems. Compliance and anticipation of regulations and standards will create a competitive advantage and demonstrate the ability to develop trustworthy autonomous systems.

Part 1

Profound change brings new opportunities

Mobility trends

Human mobility is facing a major technology-driven change.[1] With unseen acceleration, we're heading towards a new normal in which our notion of mobility will be transformed significantly. Broad societal demand for safer, more convenient, and environmentally friendly mobility is met by advancements in technology – notably in areas of batteries, sensors, connectivity, the Internet of Things (IoT), Artificial Intelligence (AI), and cloud computing. Moreover, lawmakers and regulators are aiming at accelerating and shaping the transformation of mobility while a standardized approach on how to address novel regulatory requirements in practice is missing.

The European regulation initiative puts a focus on trust and sustainability by promoting a shift towards electric mobility and by setting high-quality standards for the development and operation of Automated Driving systems as well as its underlying technologies.

This fast evolution of consumer demands, technology improvements and regulatory guidance opens the market for novel entrants and service offerings.

In the new mobility ecosystem, innovative car manufacturers and digital service providers are challenging established OEMs, suppliers and transport operators in four main areas (see Figure 1).

1 Strategy& – Digital Auto Report Volume 2 – 2021

Figure 1: The four trends shaping tomorrow's mobility

01 Connected Mobility

Enhanced connectivity, new multimedia systems and integrated electronic features ranging from sensors and cameras to seat heating have transformed the modern car into a platform with entirely new, often subscription-based business models. With the availability of an ever increasing and diverse digital service portfolio including functions-on-demand, cars' software systems have become a top priority for OEMs, suppliers and digital service providers alike.

02 Electric vehicles

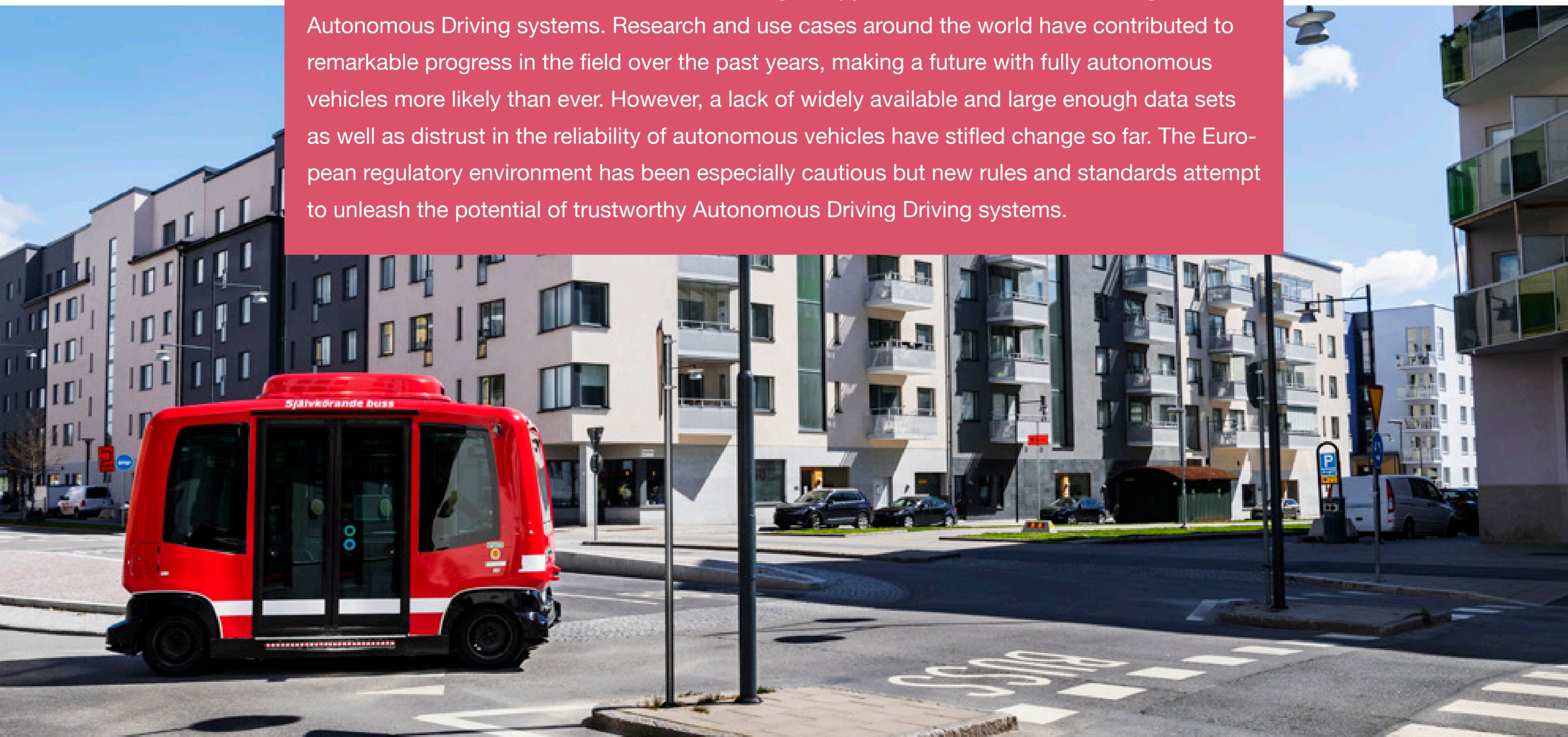
Advances in battery technology and the efficiency of electric motors enabled a more environmentally friendly and operationally cheaper mode of transportation. Public incentives and growing model choice has boosted the maturity of electric mobility and increased its attractiveness for the mass market. Further improvements in battery technology and establishing a reliable and widespread infrastructure remain challenges for making electric vehicles more competitive and reducing their CO_2 footprint.

03 Smart Mobility

Improved availability of data and better connectivity have enabled the rise of a transportation ecosystem which focuses on moving people and goods sustainably and efficiently. Shared mobility constitutes a sub-segment and an important value pool focusing on people transport with passenger vehicles. In this regard, particularly urban centers are attractive markets for new mobility initiatives. However, consumer preferences have shown that private modes are still the dominant component of mobility.

04 Autonomous Driving

A combination of sensors such as radars, lidar and cameras, progressively more abundant data and intelligent applications facilitated the emergence of Autonomous Driving systems. Research and use cases around the world have contributed to remarkable progress in the field over the past years, making a future with fully autonomous vehicles more likely than ever. However, a lack of widely available and large enough data sets as well as distrust in the reliability of autonomous vehicles have stifled change so far. The European regulatory environment has been especially cautious but new rules and standards attempt to unleash the potential of trustworthy Autonomous Driving Driving systems.



Especially developments in the field of Autonomous Driving promise to radically change our mobility and provide a wide range of opportunities for manufacturers, operators and users.

Levels of automation

> “Driverless vehicles will change our lives, just as steam trains and motor cars did before them.”
>
> (European Commission)[2]

The automotive industry has introduced outstanding advanced safety systems and driver assistance technologies in recent years, with different levels of automation emerging. To ensure that the industry, governments, and the public speak with a consistent differentiation, the international Society of Automotive Engineers (SAE) defined a common language in its standard (J3016) titled “Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems”.[3] In total, six different levels of automation are defined according to SAE (see Figure 2).

In May 2022, first cars with Level 3 Automated Driving systems went on sale in Germany[4] joining other first adopters around the world.[5] The dissemination of Level 3 certified systems will continue to advance and provide a solid starting point for the next level. In practice, however, Level 4 still faces significant challenges, which lawmakers will address through ordinances and regulations.

Beginning at level 4, the term Autonomous Driving (AD) is often used, as the vehicle is autonomously capable of conducting driving operations within its limited Operational Design Domain

Level 0:
No Automation
All driving operations (steering, accelerating, braking) are controlled by the driver.

Level 1:
Driver Assistance
Vehicle assists the driver either with lateral (steering) or longitudinal (accelerating, braking) vehicle motion control subtask.

Level 2:
Partial Automation
Vehicle assists the driver with lateral and longitudinal vehicle motion control subtask.

Level 3:
Conditional Automation
Vehicle can perceive the environment and perform the driving task autonomously under certain conditions. However, the driver must be ready for takeover at any time.

Level 4:
High Automation
Vehicle can perform the driving task autonomously under certain conditions. The driver must not be ready for takeover.

Level 5:
Full Automation
Vehicle can perform the driving task autonomously in any condition (in every geographical area, not limited to a maximum speed, etc.).

Figure 2: Levels of vehicle automation

2 European Commission – On the road toautomated mobility: An EU strategy for mobility of the future – 2018

3 SAE International – SAE J3016 – 2014

4 ETCS – Europe’s first cars with level 3 automated driving go on sale in Germany – 2022 [online]

5 NIKKEI – Honda launches world’s first level 3 self-driving car – 2021 [online]

(ODD) and without the need of a human driver. Instead, humans can either be just passengers in a remotely monitored vehicle with the ability to initiate an emergency stop or they take the role of safety operators who can take control in case of an alert by the system. However, in the absence of a timely response to an alert, a Level 4 Automated Driving system is also capable of automatically transferring into a safe state. Many milestones are still ahead on the road to a fully autonomous mobility (Level 5) but the tremendous opportunities that arise from the laws and regulations adopted over the past years will allow the technology to mature and to build trust throughout the society.

New opportunities in Autonomous Driving

Level 4 Automated Driving systems considerably augment the range of possible mobility use cases. In public transport, for example, a high level of autonomy enables buses to move without drivers on fixed routes all day round. A looming shortage of qualified bus drivers[6] is motivating municipalities to find alternative solutions for their mobility. Still, the complexity of traffic must be kept in mind. Especially during late and early hours as well as in extended commuting and rural areas around cities, remotely monitored but driverless vehicles can provide a feasible and cost-efficient solution. In logistics, use cases for Level 4 Automated Driving systems are immensely promising. The logistics industry suffers from shortages of truck drivers[7] and thereby possesses an equally compelling rationale to adopt autonomous vehicles. Furthermore, trucks play an important role in connecting major distribution centers and transportation hubs to various producers and consumers. In this context, many routes are well established and frequently used, making them attractive for the implementation of autonomously operating trucks. Not only are autonomous trucks able to replace truckers in these cases but they can also produce fleet-level benefits due to optimized driving behavior e.g. in larger formations of trucks and driving without interruption by breaks.[8]

Private mobility is also expected to benefit. Automated valet parking allows parking lots and garages to be operated more efficiently and reduces stressful or dangerous situations for customers. Business or holiday trips on frequently used routes or even daily commutes can be converted into valuable work, leisure, and resting time whilst the autonomous vehicle transfers the passengers quickly and safely to their destination. Autonomous taxis and autonomous car sharing have a chance of shaping the future of mobility in larger cities making car ownership obsolete whilst delivering a high level of individual mobility with great flexibility.[9]

The market volume for Autonomous Driving is increasing rapidly and enables new monetisation opportunities – making it worthwhile for companies to invest now.

By 2030 the worldwide demand for autonomous cars is estimated to exceed 3 million units and exhibits average growth rates in excess of 50 % per year until then.[10] In the same year, the overall market volume for Advanced-Driver-Assistance-Systems (ADAS) in the US, Europe, and China combined is expected to exceed 270 billion USD.[9] Additionally, demand for Autonomous Driving systems is already creating new and tangible market opportunities for soft- and hardware, sensor and camera technologies (e.g. Lidar), localization and mapping services, data (e.g. labeled imagery or videos from driving operations), mobility infrastructure (e.g. smart parking garages), simulation engines and consumer applications.

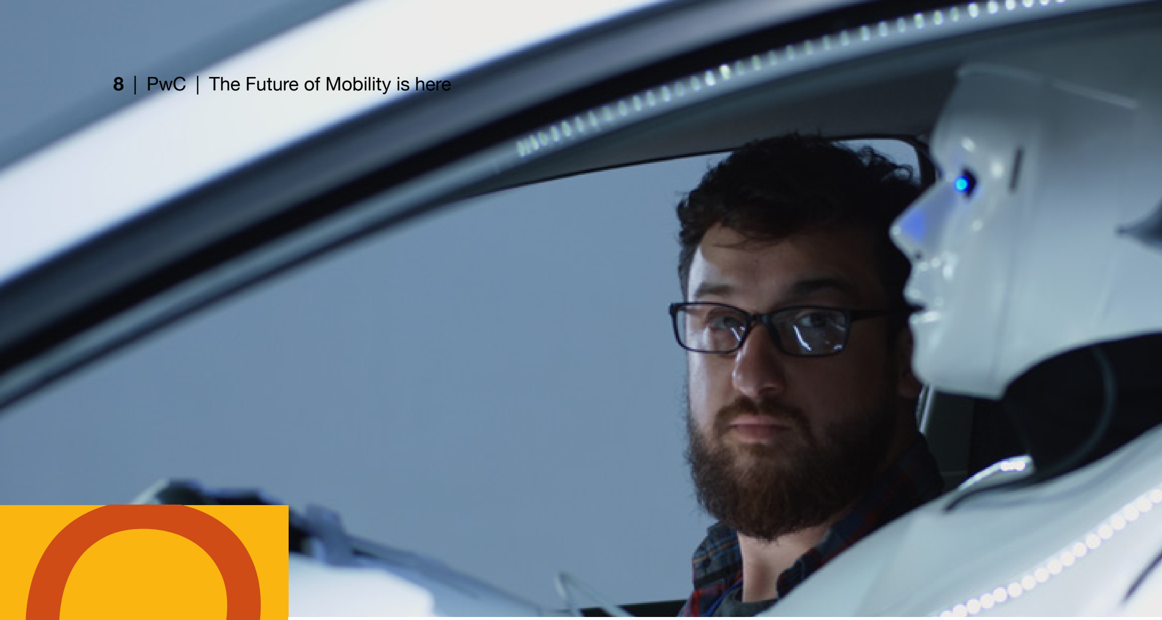
6 Verbände – Fachkräftemängel bremst Verkehrswende aus: Zehntausende Busfahrer:innen zusätzlich benötigt – 2022 [online]

7 Alexander Burstedde – LKW-Fahrer werden auch in Deutschland knapp – IW-Kurzbericht 80/2021

8 DVZ – Autonome E-Lkw: Die Nachrüstlösung kommt – 2022 [online]

9 Strategy& – Digital Auto Report – 2019

10 Grand View Research – Autonomous Vehicles Market Demand To Reach 3,195.5 Thousand Units By 2030 – 2022 [online]



2

Part 2

Digital Trust at the heart of autonomous mobility

To unleash the market potential and develop high-quality Autonomous Driving systems, gaining the trust of regulators and consumers is a prerequisite.

Recent surveys have shown that only between 14 % and 36 % of German consumers would use Autonomous Driving systems at their full capacity. Many are voicing safety concerns which are often validated by sensational media reports on accidents involving autonomous vehicles. In this regard, the ever-increasing complexity[10] of autonomous systems opens doors not only for new safety critical hazards but also for new security issues. The need for appropriate industry standards and regulations with clear requirements to guarantee safety and security is of utmost importance.

Risks associated with Autonomous Driving

Making vehicles autonomous with functionalities like collision avoidance or lane-keeping assistance brings increased software and hardware complexity. This is fueled by the need for using Artificial Intelligence (AI) technologies, for example, to perceive the environment and make smart decisions. The performance of such functionalities needs to be guaranteed at all times in order to ensure safety. On the other hand, those modules distributed across the vehicle need to communicate using an in-vehicle network, which renders vehicles highly vulnerable to various security attacks and privacy breaches.

In the automotive industry, safety as a discipline became well established in the last decades. Safety is defined according to ISO 26262 as the "absence of unreasonable risk" and addresses risks caused by intended functions, including foreseeable misuses e.g. systematic failures and random hardware failures. The most prominent hazard of autonomous vehicles lies within its perception layer; how the vehicle sensors perceive the environment. Uncertainties and potential risks could arise from many situations in this regard. For example, traffic accidents might occur due to a blocked visual field, which may be caused by parked cars or buildings in urban settings. Another risk exists when traffic participants like pedestrians or bikes are not recognised or if they are classified incorrectly. Similarly, the incorrect anticipation of autonomous driving decisions by other road users can have disastrous consequences. Therefore, assuring the safety of autonomous vehicles presents significant challenges to traditional software safety both in terms of risk analysis and mitigation in line with all relevant traffic scenarios.

Security, however, a fast-developing discipline not only in automotive, refers to the protection against malicious manipulation. It encompasses a new dimension of quality for vehicles that protects against external threats. Secure vehicles shall be resilient to remote attacks, able to detect emerging attacks and to react appropriately – ultimately ensuring the passengers safety. The increasing connectivity of vehicles allows remote attacks in which the attacker is not even within the vicinity of the vehicle. An experiment from 2015 already showed that a driving car can be manipulated remotely. Hackers managed to control the brakes, speed, air conditioning and radio of a distant car.[11] As autonomous vehicles are controlled by Artificial Intelligence models that can be digitally manipulated, further potential cyber risks arise. Moreover, since personal data is inevitably processed in autonomous vehicles, data protection requirements must also be considered to avoid data breaches. These include, in particular, privacy breaches of sensitive data such as routes driven or the detection of pedestrians combined with localization data. The urgency on manufacturers to address these safety and security risks as part of their go-to market concerns is pressing. Thus, integrating both disciplines at the outset of the development process and embracing a safety and security culture that aligns with current and future regulatory requirements is vital.

Regulations and Frameworks

To address the risks posed by autonomous vehicles and related technologies, legal obligations already exist.

Type Approval – Homologation & AFGBV

Vehicle homologation is a well-established system for approving motor vehicles and vehicle parts. It is based on the principle of reciprocity and reduces market barriers by standardizing vehicle-specific requirements. This standardisation of vehicle specific requirements reduces market barriers. Current homologation regulations in Germany come mainly from the United Nations Economic Commission for Europe (UNECE). As of now, 163 UNECE regulations set requirements for various components and vehicle systems. The scope ranges from brakes and electrical assistance systems to requirements for vehicle emissions. These regulations aim to ensure a minimum level of safety for all road vehicles admitted to road traffic.

> “Autonomous Driving will permanently change our mobility and offers enormous potential, for example in passenger transportation or in the last mile logistics. The fact that autonomous vehicles will be able to participate in normal road traffic in our country in the future is unique worldwide and was an enormous feat. But it is precisely with this detailed experience in developing the legal framework and its implementation that we can make a significant contribution to further work at the international level.”
>
> **Dr. Volker Wissing**
> **Federal Minister for Digital and Transport**

Since there were no regulations regarding Autonomous Driving in course of homologation, Germany was the first country to introduce an initiative at national level in July 2021. The Federal Ministry for Digital and Transport (BMDV) developed the “Act on Autonomous Driving” to supplement and amend the provisions of the Road Traffic Act. According to the renewed legislative framework, highly automated vehicles of Level 4 are permitted to operate in public traffic

11 Handelsblatt – Risiko vernetzte Autos: Wenn Hacker plötzlich Gas- und Bremspedal bedienen – 2019 [online]

if they have received approval from the relevant authorities. In a second step, the Autonomous Vehicle Approval and Operation Ordinance (AFGBV) entered into force on June 24, 2022, to complement the legislative framework. It concretizes the Act on Autonomous Driving with a focus on further requirements (see Figure 3).

The AFGBV introduces an extensive framework to enable Autonomous Driving on German roads containing organisational and regulatory aspects. It describes a process that not only applies for the type approval of autonomous vehicles but also for Autonomous Driving functions that can be subsequently activated. Most of the requirements of the AFGBV are consistent with existing approval structures, but there are some important additions. In particular, approval is tied to a previously permitted Operational Design Domain (ODD). Vehicle owners must thus fulfill further requirements and cooperate with the competent state authorities responsible for the intended ODD. Moreover, the AFGBV addresses a wider group of persons since the requirements not only affect the manufacturer and the vehicle owner, but also the technical supervisor – a natural person remotely supervising the vehicle in case of technical difficulties. In addition to these novelties, Annex I to III of the AFGBV sets out extensive system requirements for motor vehicles with Autonomous Driving functions. The requirements are divided into various subsections and deal with functional requirements, test and validation methods, digital data storage, human-machine interfaces, and information technology safety, for instance. It is important to note that the requirements of the AFGBV doesn't stop after a successful type approval. Since autonomous vehicles have never operated on public roads before, market monitoring requirements are laid out to ensure a sufficient degree of safety.

Setting uniform rules and standardizing procedures in the course of the AFGBV should facilitate go-to-market and speed of innovation and should not create new complexities. Considering the current state of development of Autonomous Driving technologies and the quality of the Artificial Intelligence and algorithms used, it is now of high importance to gather more experience and particularly data necessary to further develop this disruptive technology. The AFGBV allows mobility service providers to operate, test, and continuously improve the technologies under strict regulations and tight controls. This is necessary to move from simulation environments and test tracks to reality and make these technologies benefit society. Consequently, this ordinance represents a significant competitive advantage for the automotive industry and the development of Autonomous Driving in Germany.

Bundesministerium für Verkehr und digitale Infrastruktur

Verordnung
zur Genehmigung und zum Betrieb von Kraftfahrzeugen mit autonomer Fahrfunktion in festgelegten Betriebsbereichen

(Autonome-Fahrzeuge-Genehmigungs-und-Betriebs-Verordnung – AFGBV*)

The ordinance essentially governs:

Type approval
Procedural requirements for the granting of national type approvals for motor vehicles with Autonomous Driving functions.

Admission requirements
Approval of defined operating areas and registration of vehicles to road traffic.

Responsibilities
Requirements and obligations for persons involved in the operation of motor vehicles with Autonomous Driving functions.

System requirements
Technical requirements for the Autonomous Driving function, as well as testing requirements.

Figure 3: Overview of the supplementary requirements from the AFGBV

> "With the adoption of the legal ordinance, we achieve a milestone in the automotive and mobility industry"
>
> **Dr. Joachim Damasky, VDA Managing Director**

While Germany is playing a pioneering role in the regulation of autonomous vehicles, the European Union is following suit. In August 2022, the regulation (EU) 2022/1426 was published, which provides rules for the application of the general type of approval regulation (EU) 2019/2144 in the context of automated driving systems and fully automated vehicles. The new regulation establishes uniform procedures and technical specifications at the European level.

EU AI Act

Since autonomous vehicles must perform tasks that replace human-decision making, various AI components are used. For instance, AI technologies must recognise road signs and traffic lights and act appropriately. At the same time, they detect road conditions and routes along with the movements of other road users. The driving behavior needs to be adjusted accordingly. Any misinterpretation of AI technologies can lead to severe danger. Therefore, regulations that govern the handling of AI are imperative. In April 2021, the European Commission released a draft of a generally applicable EU AI Act to ensure trustworthy and human-centered AI. The Act establishes uniform guidelines for the development, commercialization, and application of AI-driven systems, products, and services within the EU. Thereby, it formalizes the high requirements of the EU's trustworthy AI concept, which demands that AI is legally, ethically, and technically sound while complying with human rights, and the rule of law.

The EU AI Act defines four levels of risk in using AI: minimal or no risk (risk level 1), limited risk (risk level 2), high risk (risk level 3), and unacceptable risk (risk level 4). At level 1, free use of AI is possible. At level 2, the use of AI must be labeled with the information that it is an AI-based system and the option to cancel the use. Critical infrastructures (e.g. transport) and safety components of products in the context of Autonomous Driving are likely to be classified as level 3 "high risk" and are therefore subject to obligations, like a high level of required robustness, security, and accuracy, before they can be put on the market. Applications of level 4 are generally not permitted. The regulations described above are primarily general and thus cover a broad area of safety and security. They provide a reliable framework within which mobility service providers can operate. However, other aspects need to be addressed, especially in the case of connected vehicles.

Cybersecurity & Software Updates

As a reaction to the rising threat of cyber-attacks on vehicles, the United Nations Economic Commission for Europe (UNECE) recently published the regulations UNECE R 155 and UNECE R 156 as part of the homologation framework. The first named regulation stipulates that manufacturing companies must implement fully functional and audited cyber security management systems (CSMS) to monitor and control the cyber security of their vehicle fleet until 2024. Via the use of these business-critical resilient CSMSs, it can be ensured that the entire value chain of digital ecosystems is protected. The second regulation, UNECE R 156, states that software updates altering vehicle functions which require approval (e.g. regarding exhaust or brake system) must be tested and submitted to the approval authority before release. Such functions may be particularly vulnerable targets from the perspective of an attacker; thus, it is not yet obvious how this will affect the delay between the discovery of a security vulnerability and the earliest possible delivery of a security update.

These regulatory initiatives show that manufactureres and suppliers need to make their cyber initiatives much more interconnected, embed cybersecurity into the core of the company's operations, and integrate cyber risk management into the company's risk management.

Part 3

How to navigate through the jungle of requirements

Manufacturers and operators of autonomous vehicles face a wide range of requirements that are not always easy to oversee in terms of efficient and effective routes for their implementation. These include procedural requirements concerning the approval process and evidence of safety, technical requirements regarding safe and secure functionalities, and data protection requirements.

Approval Procedure

A first step of the autonomous vehicle approval process along the AFGBV is to apply for a so-called testing permit, which allows the manufacturer to test a prototype vehicle on public roads under certain conditions. This is crucial to test the vehicle under realistic conditions, but also to gain additional real-world data which is needed in the development process and especially for Artificial Intelligence (AI) models. Among other prerequisites, the manufacturer must present a development concept and use an already approved conventional vehicle as the basis for the prototype.

After granting a testing permit, the autonomous vehicle is tested in real traffic as well as on test sites. Since unforeseen events can occur anytime while operating prototype vehicles in road traffic, the need for permanent monitoring and sufficient safeguards is high during that phase. To cover as many traffic scenarios as possible, simulation in a virtual environment can also be imminent and at the same time an opportunity to accelerate testing. The results obtained in simulations are validated by comparison with the results of real test drives. The testing permit thus is needed to ensure the overall safety evidence which is indispensable since trust in Autonomous Driving functions can only be established by proving an equal or higher level of safety compared to a human driver.

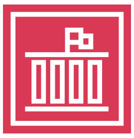
After completing the testing phase, the AFGBV specifies three further steps, as shown in the following figure:

1. 

Operating permit
An operating permit for motor vehicles with Autonmous Driving functions must be applied for at the Federal Motor Transport Authority.

2. 

Approval for defined operating range
Approval for the vehicle type within a defined operating range must be granted by the competent authority. To that, the area of operation must be described.

3. 

Road registration
The final step is the actual road registration of the vehicle with Autonomous Driving function by assigning an official license plate and issuing the vehicle documents.

Figure 4: Summarised three-step approval approach according to AFGBV

One step is to apply for type approval at the Federal Motor Authority. For a successful application, compliance with technical and organisational requirements specified in the AFGBV and its annexes is necessary among other prerequisites. Since few best practices are currently available for the approval of autonomous vehicles, this step must be carried out in close coordination with the Federal Motor Transport Authority. As an additional step, the Operational Design Domain (ODD) must be approved by the competent state authority. This must be initiated by the vehicle's holder with a comprehensive definition of the intended operating area. Only if both, type approval and the approval of the ODD are granted, and thus the safe operation of the autonomous vehicle within its operation area is ensured, the vehicle may be registered to road traffic according to AFGBV and Road Traffic Act.

Safety Requirements

A central requirement for manufacturers to comply with the AFGBV is the development of a safety concept, which evaluates the safety of the driving function. All potential hazards and operational risks the autonomous vehicle may encounter must be systematically identified, assessed, and if necessary mitigated by system improvements. The approach should correspond to the state-of-the-art, which can be fulfilled by complying with different automotive standards.

While such standards are not legally binding in principle, they can become mandatory if certain legal documents refer to them or require compliance. Regarding Autonomous Driving, this applies to the standards ISO 26262 'Road vehicles – Functional safety' and ISO/PAS 21448 'Road vehicles – Safety of the intended functionality' to which the AFGBV refers.

Compliance with ISO 26262 has been a basic requirement for the safety of vehicles for years and must also be ensured for newly constructed autonomous vehicles. ISO 26262 addresses the safety of electric and electronic components of the vehicle and aims at preventing malfunctioning or foreseeable misuse. To comply with the standard, the manufacturer must perform the following steps: A comprehensive item definition describing the vehicle's functional parts is followed by a hazard analysis and risk assessment (short: HARA) which identifies and quantifies potential upcoming risks. The quantification is made through a so-called Automotive Safety Integrity Level (short: ASIL) which is determined by the degrees of severity, controllability, and exposure of the hazardous situations. As a result, a list of high-level safety goals can be derived which are subsequently broken down to safety requirements and implemented on a technical level. The ISO 26262 development procedure ends with verification and validation steps to ensure a sufficient level of safety. Subsequently, further requirements regarding a release for production, operation, service, and decommissioning must be addressed. ISO 26262 thus covers the entire product life cycle.

Compliance with ISO/PAS 21448 shall guarantee that the proper operation of the vehicle is free of unreasonable risks, even in unknown traffic scenarios. Therefore, not only hazards caused by faulty behavior of humans or machines but also risks resulting from insufficient functionalities are prevented. The basic procedure described in the standard is as follows: After a precise specification of the vehicle's function and system architecture, a hazard analysis and risk assessment similar to the one in ISO 26262 is conducted to identify prior unknown risks related to the intended functionality. In the context of Autonomous Driving, this step results in a catalogue of testable traffic scenarios. Afterwards, a series of functional modifications is implemented to cope with the identified risks. The procedure is repeated iteratively until analyses show that the risk resulting from the technical architecture implementing the intended functionality is reasonably low. Ultimately, ISO/PAS 21448 is a necessary extension to ISO 26262 for addressing Autonomous Driving specific hazards. For example, insufficiently trained AI models for object detection and classification can lead to the misclassification of people without the presence of any malfunction in the system. Such hazard would therefore be outside the scope of ISO 26262 but inside the scope of ISO/PAS 21448.

For efficient compliance with both standards, an integral approach is needed, considering the complementary aspects of safety from the outset. Since the procedures overlap and very similar analysis techniques and methods are recommended to foster safety, synergy effects can be achieved by such an approach. Since the standards procedure can end in hundreds or thousands of requirements, a suitable requirements management tool becomes essential for traceability and transparency. Particularly useful in this regard are Application Lifecycle Management (ALM) tools, which ensure compliance by providing full traceability from requirements to test cases to test results.

Cybersecurity Requirements

The transformation of the automotive industry from classical engineering companies to suppliers of software-driven products, such as automated or autonomous vehicles, results in additional IT-related risks. Next to ensuring functional safety or the safety of the intended functionality, manufacturers now must also consider hazards potentially arising from digital threats. Therefore, especially connected vehicles must implement sufficient safeguards to ensure the cybersecurity of the vehicle operation.

The AFGBV explicitly states requirements to ensure a sufficient degree of cybersecurity.

In particular, the requirements of regulation UNECE R 155 "Cyber security and cyber security management system" must be fulfilled. The most important requirement of this regulation is to set up an extensive cybersecurity management system (CSMS), a systematic, risk-based approach to define procedures, governance, and responsibilities regarding cybersecurity-related aspects. The outlined framework should enable organisations to ensure cybersecurity holistically and to consider the influence of cybersecurity in each part of the company. Therefore, the CSMS must cover all phases of the vehicle's lifecycle from development over production to the post-production phase. In doing so, cybersecurity is considered from the very beginning in the manufacturer-supplier relationships throughout the supply chain. In practice, cybersecurity is usually implemented into the company's processes as follows: Each internal procedure and organisational department is scanned for possible cybersecurity-related risks, which are assessed for severity and if possible quantified. If the implemented systems are not able to mitigate the risk to an appropriate level, organisational changes are initiated to improve the handling of cyber-relevant issues.

For compliance with UNECE R 155, manufacturers may refer to the requirements of ISO/SAE 21434 "Road vehicles – Cybersecurity engineering". As an internationally recognised standard, ISO/SAE 21434 describes a framework for the development of cybersecurity-related products in the automotive industry. Compliance with this standard ensures revolutionary developments and provides detailed information on how to implement a comprehensive CSMS, which is helpful for the fulfillment of UNECE R 155 requirements.

Data Protection Requirements

With Autonomous Driving, various data protection aspects must be considered. Regarding the vehicle itself, the vehicle identification number (VIN) and the license plate represent personal data that can be directly assigned to an individual. If this data is linked with localization data and a time stamp, for example, movement profiles and individual behavior patterns can be derived, which poses a significant risk to the rights of the data subjects. On the other hand, the AFGBV requires autonomous vehicles to be equipped with modern sensor technology like cameras to detect objects and persons in the environment. These built-in cameras also inevitably record personal data in real traffic situations, in which the behavior of individuals can be observed.

To protect personal data, the AFGBV refers to the EU General Data Protection Regulation (GDPR), which imposes numerous requirements. To fulfill information obligations according to Article 13 GDPR, for example, manufacturers must attach visible information to vehicles that record their environment with cameras. This information includes the person responsible and the purpose of the processing, as well as the length of the data storage. Non-compliance with this requirement can result in fines reaching millions of euros, as the past has shown.[12] In particular, Articles 24, 25, 32, and 35 of the GDPR are referenced multiple times for the approval of autonomous vehicles which brings further obligations for manufacturers. According to Article 35, it becomes necessary to carry out a thorough data protection impact assessment before any processing takes place. Article 24 states that adequate organisational and technical measures must be implemented to protect the rights and freedoms of the natural persons affected by the processing. Therefore, the data controller must consider the specific use case and the potential risks for the rights of privacy and freedom of others. In addition, Article 25 requires data protection by design and default. Therefore, all measures must already be applied during the definition of the data processing as well as during the processing itself (data protection by design). Additional measures must be implemented to ensure that only necessary data is processed, and processing time and accessibility are limited to a minimum (data protection by default). Article 32 requires that the confidentiality, integrity, availability, and resilience of processing systems be ensured at all times. In general, it becomes important not to limit the scope to the recording of new data, but to include other aspects of data processing, e.g. transmission and storage, to ensure overall secure processing. Data protection and cybersecurity must therefore go hand in hand.

Compliance with GDPR requirements is not self-evident, and many questions must be addressed for data protection-compliant Autonomous Driving.

A possibility to circumvent the numerous and profound requirements is the complete anonymization of the data according to recital 26 GDPR. However, suitable technical solutions are required, and it must be assessed whether the modification of original data will lead to performance restrictions during subsequent processing. For example, AI models trained with anonymized image data can degrade significantly in performance when applied for object detection with non-anonymized data and vice versa. At worst, this may result in inadequate detection of persons with potentially harmful outcomes. Consequently, the intended camera and sensor concept must be aligned with the AI models from the very beginning to simultaneously ensure data protection and security.

Hardware Requirements

The increase in sophisticated software components needed for autonomous vehicles also leads to greater demands for hardware performance and energy efficiency.

Especially since a large amount of data is captured and must be processed in real time for safe environment perception, the demands for powerful processors are high. This is fueled

12 State Commissioner for Data Protection Lower Saxony – 1,1 Millionen Euro Bußgeld gegen Volkswagen – 2022 [online]

insofar as the data comes from a wide variety of sources such as radar, lidar, cameras, or GPS. Also, breakthroughs in the performance of machine learning models and the ability for some algorithms to successfully perform object and lane detection at high frequency require powerful system architectures, which are yet to be commoditised.

The qualification of hardware components used for safety-critical architectures in the automotive industry poses further requirements for manufacturers. Components used must follow specific industry standards for manufacturing and performance to ultimately support the vehicle's evidence of safety. ISO 26262, for example, specifies concrete fault metrics for hardware components, depending on the required automotive Safety Integrity Level (ASIL). Other specific standards referenced in ISO 26262, such as AEC-Q100 or AEC-Q200, state requirements for stress testing integrated circuits or passive components. As described, processors are subject to high-performance requirements which must be proven by appropriate analyses and tests depending on the ASIL. Such requirements also apply to individual sensors, depending on the chosen system design. In practice, redundancy in the system design of hardware components is therefore often required to increase safety. In other words, several sub-components are implemented for an identical task. While these sub-components differ in their configuration it is ensured that one component can still perform the task in case of failure of the other.

Since Autonomous Driving systems are developed in a collaboration between manufacturers and suppliers, extensive cooperation is vital for compliance with standards throughout the supply chain. It must be ensured that the hardware components are developed with the right properties and also produced without defects. Audits carried out by the manufacturer at the supplier's premises can increase safety in this respect, while suppliers can also be obliged to comply with the relevant standards by contractual agreements.

Testing Requirements

Ensuring the safety of autonomous vehicles differs from conventional vehicles. Due to the absence of a human driver, the Autonomous Driving function must be able to cope with all traffic situations on its own. Therefore, not only the performance of technical systems, but also the vehicle's ability to navigate safely through real-world traffic must be evaluated. Only by setting up a holistic safety argumentation process, manufacturers can provide adequate evidence that the Autonomous Driving function can safely handle all traffic scenarios in its Operational Design Domain (ODD). At this point, it becomes necessary to use scenario-based testing methods, which also enable the efficient simulation of innumerable traffic scenarios in parallel. In fact, using scenario-based testing is a central requirement manufacturers have to fulfill in order to comply with the AFGBV.

The big challenge in scenario-based testing is to define the nearly infinite number of possible real-world traffic scenarios.

One traffic scenario is thereby composed of different traffic scenes in time. Possible scenarios can be created in various ways, such as using historical traffic data or by systematic approaches deriving them from traffic laws and rules the vehicle has to comply with. Since altering the values of different variables in one scene (e.g. distances between vehicles, vehicle speed, weather conditions, etc.) can bring different scenarios, parameterizable simulation models should be used for testing to reduce effort. Due to limited resources, a subset of traffic scenarios must be chosen considering the requirements from standards and regulations and later tested without reducing the significance of the safety argumentation. The catalog of scenarios must cover all relevant traffic scenarios, while containing a reasonable amount of scenarios which is possible to test in an appropriate period. Providing evidence that the scenario catalogue is sufficiently complete is another prerequisite of the AFGBV. To achieve a wider coverage of real-world traffic scenarios, it can be helpful to use stochastic variation methods turning the abstract functional scenarios into different concrete scenarios.

A first attempt to implement a scenario-based testing procedure for automated vehicles (Level 3) has been developed within the PEGASUS project, which was promoted by the German Federal Ministry for Economic Affairs and Energy (BMWi). The goal was to create a framework for the overall safety argumentation of automated vehicles restricted to common highway driving scenarios. The approach of the PEGASUS project starts with the creation of suitable scenarios and the definition of requirements and criticality metrics used for testing afterwards. Different sources of knowledge from traffic data to laws and regulations have to be used for that purpose. Following the PEGASUS procedure, the gained scenarios are then refined into a shared data format and critical ones are chosen to be tested in simulations. By testing the vehicle within realistic simulation environments, it becomes possible to identify critical system behavior which is not yet known. This allows subsequently to consider a larger number of safety-critical issues within the development process and ultimately supports evidence for the safety argumentation process.

4

Part 4

Compliance as competitive differentiator in a dynamic regulatory environment

Addressing technological challenges with uniform regulations currently poses a bottleneck

Humans are able to drive different types of vehicles due to their sensory, cognitive, and motoric abilities. Vehicles must also inherit these abilities to perform the driving task autonomously. This requires new system architectures based on various hardware components as well as AI models that can handle cognitive tasks. However, such system architectures have not yet been tested over the long term. Besides ensuring proper interaction of individual hardware components, AI in particular constitutes a new source of potential risk, as shown in Part 2. Due to the various potential risks of the novel system architectures, standardized regulations are necessary to ensure the safety and security of the entire vehicle system.

As outlined before, first regulatory approaches already exist in this regard and existing standards are becoming mandatory for manufacturers of autonomous vehicles in Germany. However, standards such as ISO 26262 (functional safety), ISO/PAS 21448 (safety of the intended functionality) and ISO/SAE 21434 (cybersecurity) make little or no reference to these new risks. Also, the AFGBV does not include requirements specific to AI-powered systems of autonomous vehicles yet and currently relies on more general requirements. This inevitably leads to many uncertainties in the development of Autonomous Driving functions, as best practices are still lacking. Additional regulation and standardization are imperative to further gain guidance but does not impose too many restrictions to allow different technological approaches to emerge.

Lawmakers and standardisation bodies are already working on closing the gap through standards and regulations. As part of efforts by ISO, new standards for the safety of AI systems in the automotive context (e.g. ISO/AWI PAS 8800, ISO/IEC DTR 5469) and for the overall safety of Automated Driving systems (e.g. ISO/AWI TS 5083) are being developed. Also on a supranational level, the European Commission is working on improving its proposal for harmonised rules on Artificial Intelligence as described in Part 2. Due to the inherent risks of used AI models, autonomous vehicles are likely to be classified as high-risk systems under the upcoming EU AI Act. Requirements associated with this status cover measures like robustness and security, accuracy, monitoring systems, technical documentation, resource management as well as human oversight systems just to mention a few. Further requirements must be considered, for example, during homologation. In June 2022, an amendment to regulation UNECE R 157 concerning the Automated Lane Keeping Systems (ALKS) was adopted by the European Commission. While this regulation is applicable for Level 3 Automated Driving systems, regulations for Level 4 can be expected soon at UNECE level.

Technological challenges and uncertainty from emerging standards and regulations are not the only bottleneck for quicker and broader adoption of Autonomous Driving. The discrepancy between the speed of necessary conformity assessments and the desired pace of improvement of vehicle systems creates a significant tradeoff for manufacturers and assessment bodies alike. Currently, every modification of vehicles with already granted type approval requires the renewed approval of the Federal Motor Transport Authority. Additionally, as more and more companies desire type approvals for autonomous vehicles, larger capacities for thorough assessments are needed. Manufacturers and suppliers must therefore establish a process that allows successive type approvals by harmonising all safety and formal aspects throughout all phases of the product life cycle.

Due to the importance of its automotive industry, Germany needs to play a pioneering role in developing safe and reliable Autonomous Driving systems.

Harmonised regulation paired with standards sufficiently addressing novel risks, along with efficient approval systems administered by trusted third-parties is of chief importance for maintaining competitiveness. Harmonising the plethora of different upcoming requirements from standards and regulations will be a difficult task. Manufacturers and suppliers implementing Autonomous Driving systems thus will need reliable partners to make their way through the jungle of requirements and to successfully achieve compliance.

Flexible and anticipatory compliance as competitive differentiator

To tackle existing and emerging regulations and standards quickly and efficiently, all manufacturers of Autonomous Driving systems and their suppliers need to make adaptive governance and compliance milestones in their strategic roadmap. A comprehensive and flexible governance approach is needed to address the safety-related aspects of Autonomous Driving systems early on, thus guaranteeing long-term success throughout its entire lifecycle. Identifying and building the necessary components for fulfilling requirements laid out in standards and regulations is only one aspect of compliance. Policies, processes, and assessment results as well as changes and updates need to be adequately documented and provided to regulatory authorities or conformity assessment bodies upon reasoned request.

By staying ahead and preparing for compliance in anticipation of upcoming regulations and standards, companies can gain a competitive edge and demonstrate their ability to implement trustworthy Autonomous Driving systems.

The evolving nature of regulations and standards demands the implementation of a streamlined process for continuously meeting regulatory requirements and standards. Especially for all systems employing AI techniques, emerging standards and regulations add a new level of complexity to compliance management for implementers of Autonomous Driving systems.

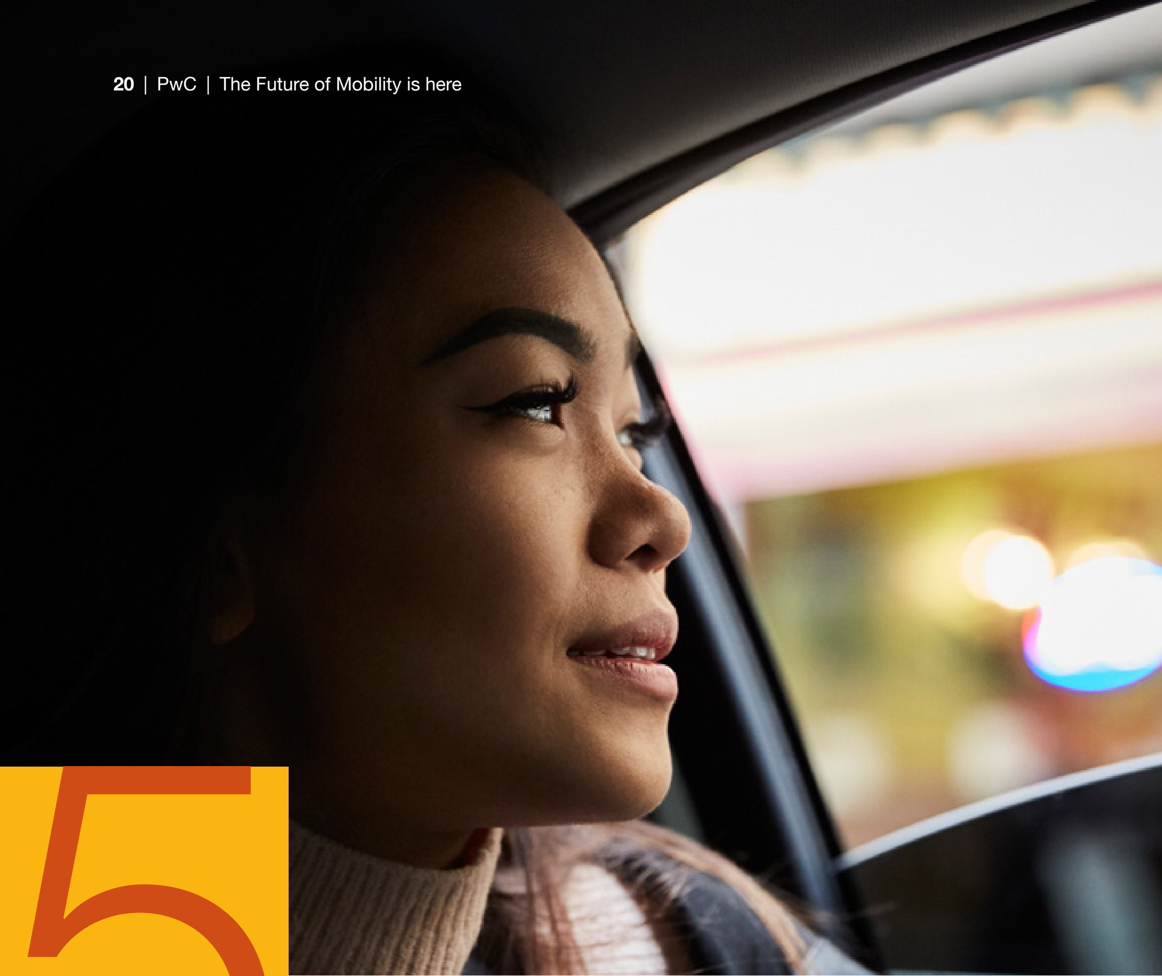
Without the know-how to establish a robust and flexible governance, compliance becomes a costly and time-consuming process.

The goal of compliance is to avoid financial or reputational damage to an organisation. However, compliance-related bottlenecks such as the necessary approvals for autonomous vehicles mentioned in the previous section impair a company's ability to achieve business objectives swiftly. Hence, having the competencies to anticipate and resolve roadblocks is crucial. Employing additional qualified personnel is expensive though. Smaller companies and especially start-ups often do not have sufficient resources to build their own compliance teams whilst large OEMs and tech companies face significantly fewer obstacles. In both cases, specialist advice and governance technologies contribute to saving time and expenses, provide structure to your governance and bring validated best-practice processes to an organisation more quickly.

An experienced partner will try to understand a business's compliance needs and build tailored solutions to match them. Depending on the role in the value chain and the extent of the company's operation, different designs serve the purpose of establishing compliance best. However, any holistic approach considers the relevant safety and security standards and identifies the core challenges that arise from the complex jungle of requirements. An elaboration of the applicable standards and regulations fulfillment approach including the identification of dynamic changes and innovations along the AFGBV into a workable and reusable format is a must.

A readiness check of existing governance processes establishes an understanding of the overall compliance efforts and serves the identification of necessary improvements. Based on this knowledge, concrete guidance and roadmaps can be created, covering all aspects from prioritization based on safety reasoning to the coordination of the relevant stakeholders.

With the clarity that milestones and objectives provide, companies can start to implement successful practical approaches for the development of governance structures, which ultimately receive the desired approvals and achieve trust in Autonomous Driving systems.



5

Part 5

Summary & Outlook

Our today's mobility is undergoing a profound transformation, as outlined in Part 1. In addition to the mobility trends Connected Mobility, Electric Vehicles and Smart Mobility, Autonomous Driving in particular has the potential to become a game changer. Especially in the transport sector, autonomous vehicles can enable new business models from which not only manufacturers and owners, but also society can benefit. Autonomous vehicle fleets can be used to enhance public transport services and, for example, to alleviate the shortage of long-distance drivers for the transport of goods. However, the market for autonomous vehicles is still in its infancy, with forecasts predicting an enormous market volume of trillions of dollars in the future. Those who manage to scale Autonomous Driving technologies fast enough, while overcoming several current challenges, can leverage this market potential. Several companies already recognised this opportunity, so the first type of approval is already around the corner.

As illustrated in Part 2, Digital Trust is crucial for market success in this regard, as new risks arise from the complex and sometimes opaque technologies required for Autonomous Driving functions like Artificial Intelligence (AI). These risks concern on the one hand the safety of the intended functionality, but also the security against unwanted and harmful external attacks. At this point, various legal regulations and frameworks must already be considered by manufacturers and suppliers to ensure a minimum level of safety. The German Autonomous Vehicle Approval and Operation Ordinance (AFGBV) in conjunction with the Act on Autonomous Driving is of particular relevance as it is the world's first legislative framework for this topic. Compliance with the numerous requirements of the AFGBV enables type approval and road registration of autonomous vehicles. However, just sticking to AFGBV requirements is insufficient and it is necessary to consider other regulations, for example regarding cybersecurity, or AI-specific regulations which are on the horizon like the EU AI Act.

The requirements needed to be considered from different sources are already diverse and not easy to oversee, as shown in part 3. Our experience shows that although the procedure for type approval and road registration is clearly specified, many questions arise concerning the compliance of technical requirements regarding safety and security due to a lack of best practices. Uncertainties also exist regarding the required test methods and scale. In addition, data protection issues must be clarified, since autonomous vehicles inevitably process personal data, especially utilising built-in cameras. At this point, manufacturers and suppliers must develop their individual approval approaches considering requirements of the AFGBV, GDPR and various safety standards. This includes the creation of a safety argumentation process with a comprehensive test concept. As we have noted, the Federal Motor Transport Authority and technical services involved in the type of approval process also have few established processes to date. Therefore, manufacturers and suppliers need to work closely with all relevant authorities while developing their individual approval approach. Moreover, it should be recognised that the development of autonomous vehicles is generally done in cooperation between manufacturers and suppliers, which vary in terms of value depth. To ensure the safety of the developed product, collaboration at an early stage is thus imperative. Ultimately, implementing a holistic and standardized process that harmonises all safety and formal aspects over the product lifecycle and throughout the supply chain allows us to take a frontrunner position and efficiently obtain type approvals for different kinds of autonomous vehicles. At the same time, (digital) trust will be established within their products which will be a strong competitive advantage.

Since the regulatory landscape is highly dynamic, the enablement of manufacturers to anticipate upcoming requirements properly is another critical success factor, as described in Part 4. In the field of Artificial Intelligence, in particular, further requirements can be expected including adapted and novel security standards. In this respect, we could observe that the implementation of an adaptive organisation-wide AI governance structure is highly valuable, especially due to the numerous technical and compliance peculiarities that come with the usage of AI. Only by creating transparency through a clear assignment of roles and responsibilities, and implementing structured processes, can companies realize complex AI projects in a time- and cost-efficient manner. With increasing experience in the approval of autonomous vehicles, updated and new legal obligations can also be expected in the near future. Adoption speed is thus critical to deal with the dynamics of changing and newly emerging requirements. Throughout the entire lifecycle of Autonomous Driving systems, good compliance management is needed to stay ahead and anticipate the implications of evolving regulations and changing standards. Organisations that establish holistic and adaptable compliance management addressing the specific challenges outlined in this whitepaper benefit from faster and less costly approvals, higher safety levels, and differentiation in the market by trust in the quality of their Autonomous Driving systems.

Professional support for your approval process

On the road to Autonomous Driving, there are still many challenges that are difficult to overcome alone. As a reliable partner, we help you to pass through the jungle of requirements and to design the approval process efficiently with a strategy that is holistic but individually tailored to your use case.

Contact

Hendrik Reese

Partner | Risk & Regulatory Consulting

Tel.: +49 151 14806264

hendrik.reese@pwc.com