grape up®

Software-defined vehicle:

How AI and Cloud Computing Set the Course of Change in the Automotive Industry in the Months to Follow

Table of contents

Foreword 3

Where are we now

1. 8 Examples of How AI Drives the Automotive Industry 4

Where are we going

2. What Trends Will Set the Course of Change in the Automotive Industry for next months 15

Where will we be tomorrow

3. Machine Learning at the Edge – Federated Learning in the Automotive Industry 24
4. The Next Step for Digital Twin – Virtual World 31

Summary 34

— Meet the authors
— About Grape Up
— How working with Grape Up can help you innovate

Foreword

If you listen to CARIAD, Stellantis, Tesla, Audi, and others, you will learn that each and every one of these companies believes that the future of the automotive industry is software-centric. As the name says, if you want to achieve that, you have to learn how to build software and this may be a bumpy road for most of the OEM's. How to align a legacy, waterfall approach of building cars with the lean, agile software development paradigms, or modern, disruptive cloud and AI technologies? CARIAD already seems to know, Stellantis says they have a plan, Porsche is at full speed, and Tesla was born that way.

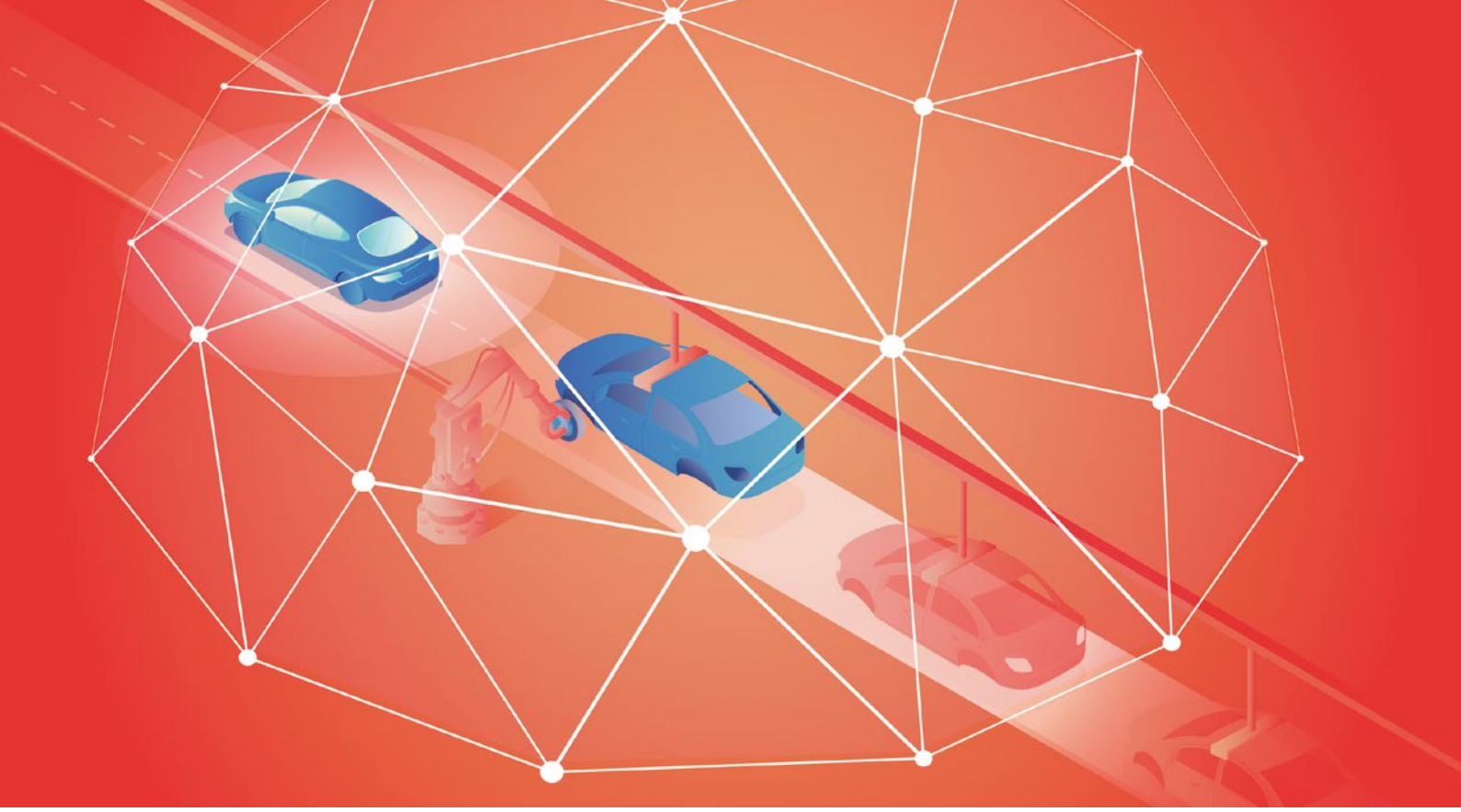
In this whitepaper, we look at the realities of the market, how the automotive industry is transforming, and highlight specific technologies that will soon be setting the course of change.

- **In part one** you will find 8 real-life examples of how AI can be used in the automotive industry. Each of them is supported by a true use case of a well-known OEM or software company that already managed to implement such solutions.
- **In part two**, we identify a number of key trends that will impact the entire automotive ecosystem and are more than likely to dominate the discourse and major implementations over the next several months.
- **Last but not least**, the third part consists of 2 technologies that are still to come, but whose implementation will take AI and cloud solutions to a whole new level, and thus will certainly accelerate the spread of software-defined-vehicles. We are talking about the federated learning method and the virtual world concept, which is touted as the successor to the digital twin solutions.

Enjoy your reading

Marcin Wiśniewski
(Head of Business Development - Automotive Industry)

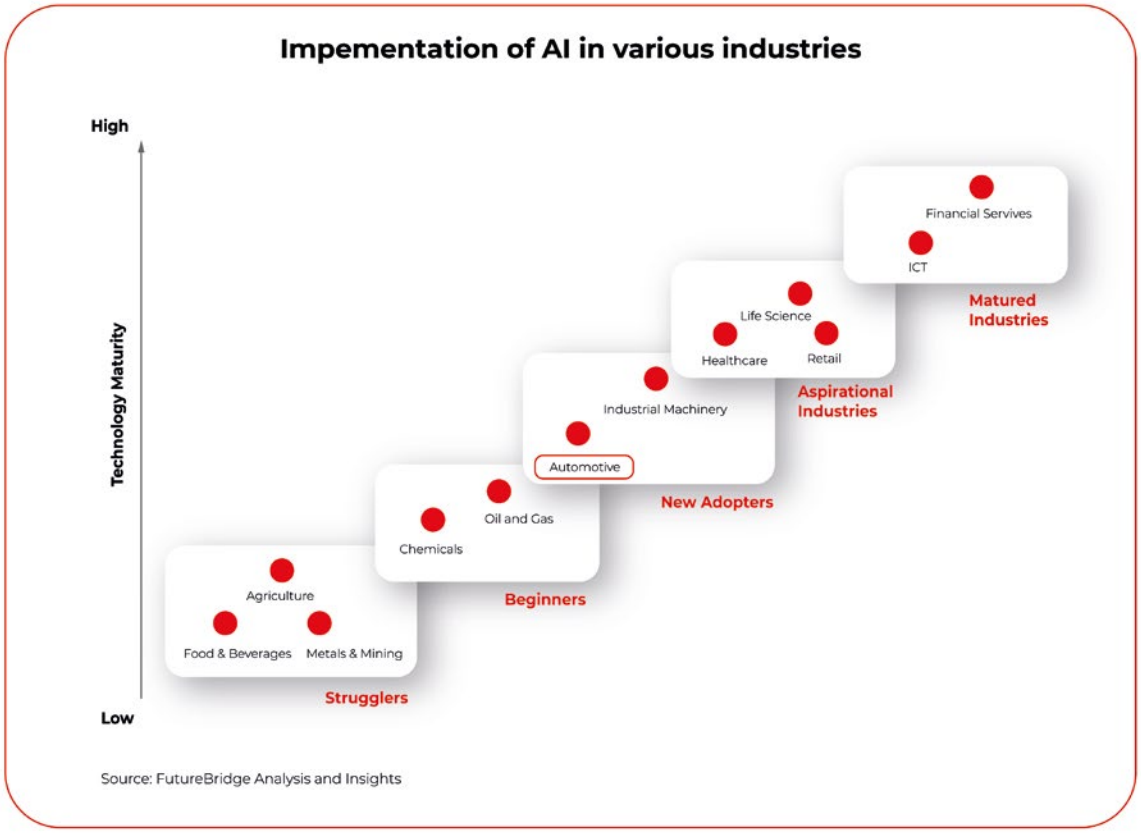
Adam Kozłowski
(Head of Automotive R&D)



8 Examples of How AI Drives the Automotive Industry

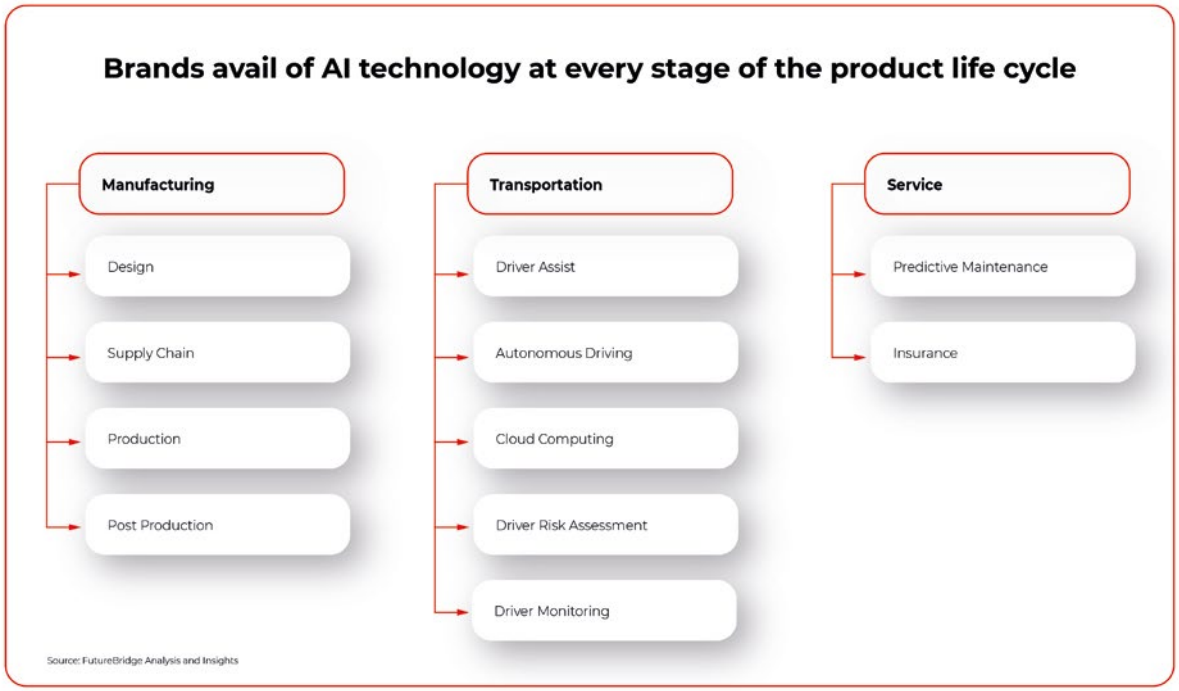
Just a few years ago, artificial intelligence stirred our imagination via the voice of Arnold Schwarzenegger from "Terminator" or agent Smith from "The Matrix". It wasn't long before the rebellious robots' film dialogue replaced the actual chats we have with Siri or Alexa over our morning cup of coffee. Nowadays, artificial intelligence is more and more boldly entering new areas of our lives. The automotive industry is one of those that are predicted to speed up in the coming years. By 2030, 95-98% of new vehicles are likely to use this technology.

Looking at the application of AI in various industries, we can name five stages of implementation of such solutions. Today, companies from the Communication Technology (ICT) and Financial Services ("Matured Industries") sectors are taking the lead. Healthcare, Retail, Life Science ("Aspirational Industries") are following closely behind. Food & Beverages and Agriculture ("Strugglers") and companies from the Chemicals and Oil and Gas sectors ("Beginners") are bringing up the rear. The middle of the bunch is the domain of Automotive and, partly related to it, Industrial Machinery.



Although these days we choose a car mainly for its engine or design, it is estimated that over the next ten years, its software will be an equally significant factor that will impact our purchasing decision.

AI will not only change the way we use our vehicles, but also how we select, design, and manufacture them. Even now, leading brands avail of this type of technology at every stage of the product life cycle – from production through use, to maintenance and aftermarket. Let's have a closer look at the benefits a vehicle manufacturing company can get when implementing AI in its operations.



Manufacturing – how AI improves production?

An average passenger car consists of around 30,000 separate parts, which interestingly enough, are usually ordered from various manufacturers in different regions of the world. If, on top of that, we add a complicated manufacturing process, increasingly difficult access to skilled workers and market dependencies, it becomes clear that potential delays or problems in the supply chain result in companies losing millions. Artificial intelligence can predict these complex interactions, automate processes, and prevent possible failures and mishaps.

1. You will be able to work out complex operations and streamline supply chains

— Artificial intelligence complements Audi's supply chain monitoring. When awarding contracts, it is verified that the partners meet the requirements set out in the company's internal quality code. In 2020, over 13,000 suppliers provided the Volkswagen Group with a self-assessment of their own sustainability performance. Audi only works with companies that successfully pass this audit.

2. More efficient production due to intelligent co-robots working with people

For years, companies from the automotive industry have been trying to find ways to enhance work on the production line and increase efficiency in areas where people would get tired easily or be exposed to danger. Industrial robots have been present in car factories for a long time, but only artificial intelligence has allowed us to introduce a new generation of devices and their work in direct contact with people. AI-controlled co-bots move materials, perform tests, and package products making production much more effective.

- **Hyundai Vest Exoskeleton** (H-VEX) became a part of Kia Motors' manufacturing process in 2018. It provides wearable robots for assembly lines. AI in this example helps in the overall production while sensing the work of human employees and adjusting their motions to help them avoid injuries.
- **AVGs** (Automated Guided Vehicles) can move materials around plants by themselves. They can identify objects in their path and adjust their route. In 2018, an OTTO Motors device carried a load of 750 kilograms in this way!

3. Quality control acquires a completely new quality

The power of artificial intelligence lies not only in analyzing huge amounts of data but also in the ability to learn and draw conclusions. This fact can be used by finding weak points in production, controlling the quality of car bodies, metal or painted surfaces, and also by monitoring machine overload and predicting possible failures. In this way, companies can prevent defective products from leaving the factories and avoid possible production downtime.

- **Audi** uses computer vision to find small cracks in the sheet metal in the vehicles. Thus, even at the production stage, it reduces the risk of damaged parts leaving the factory.
- **Porsche** has developed “Sounce”, a digital assistant, using deep learning methods. AI is capable of reliably and accurately detecting noise, for example during endurance tests. This solution, in particular, takes the burden off development engineers who so far had to be present during such tests. Acoustic testing based on Artificial Intelligence (AI) increases quality and reduces production costs.

4. AI will configure your dream vehicle

In a competitive and excessively abundant market, selling vehicles is very difficult. Brands are constantly competing in services and technologies that are to provide buyers with new experiences and facilitate the purchasing process. Manufacturers use artificial intelligence services not only at the stage of prototyping and modeling vehicles, but also at the end of the manufacturing process, when the vehicle is eventually sold. A well-designed configurator based on AI algorithms is often the final argument, by which the customer is convinced to buy their dream vehicle. Especially when we are talking about luxury cars.

- **The Porsche Car Configurator** is nothing more than a recommendation engine powered by artificial intelligence. The luxury car manufacturer created it to allow customers to choose a vehicle from billions of possible options. The configurator works using several million data and over 270 machine learning modules. Effect? The customer chooses the vehicle of their dreams based on customized recommendations.

Transportation – how AI facilitates driving vehicles

A dangerous situation on the road, vehicle in the blind spot, power steering on a slippery surface. All those situations can be supported by artificial intelligence, which will calculate the appropriate driving parameters or correct the way the driver behaves on the road. Instead of making automatic decisions – which are often emotion-imbued or lack experience – brands increasingly hand them over to machines, thus reducing the number of accidents and protecting people's lives.

5. Artificial intelligence will provide assistance in an emergency

- **Verizon Connect** solutions for fleet management allow you to send speed prompts to your drivers as soon as your vehicle's wipers are turned on. This lets the driver know that they have to slow down due to adverse road conditions such as rain or snow. And the intelligent video recorder will help you understand the context of the accident – for instance, by informing you that the driver accelerated rapidly before the collision.

6. Driver monitoring and risk assessment increase driving safety and comfort

Car journeys may be exhausting. But not for artificial intelligence. The biggest brands are increasingly equipping vehicles with solutions aimed at monitoring fatigue and driver reaction time. By combining intelligent software with appropriate sensors, the manufacturer can fit the car with features that will significantly reduce the number of accidents on the road and discomfort from driving in difficult conditions.

- **Tesla** monitors the driver's eyes, thus checking the driver's level of fatigue and preventing them from falling asleep behind the wheel. It's mainly used for the Autopilot system to prevent drivers from taking short naps during travel.
- **The BMW 3 Series** is equipped with a personal assistant, the purpose of which is to improve driving safety and comfort. Are you tired of the journey? Ask for the "the vitalization program" that will brighten the interior, lower the temperature or select the right music. Are you cold? All you have to do is say the phrase "I'm cold" and the seats will be heated to the optimal temperature.

Maintenance – how AI helps you take care of your car

Carsthatwearedrivingtodayarealreadyprettysmart. They can alert you whenever something needs your attention and they can pretty precisely say what they actually need – oil, checking the engine, lights etc. The Connected Car era however equipped with the possibilities given by AI brings a whole lot more – predictive maintenance. In this case AI monitors all the sensors within the car and is set to detect any potential problems even before they occur.

AI can easily spot any changes, which may indicate failure, long before it could affect the vehicle's performance. To go even further with this idea, thanks to the Over-The-Air Update feature, after finding a bug that can be easily fixed by a system patch, such a solution can be sent to the car Over-The-Air directly by the manufacturer without the need for the customer to visit the dealership.

7. Predictive Maintenance prevents malfunctions before they even appear

— **Predi** (an AI software company from California) has created an intelligent platform that uses the service order history and data from the Internet of Things to prevent breakdowns and deal with new possible ones faster.

8. Insure your car directly from the cockpit

Driving a car is not only about operating costs and repairs, but also insurance that each of us is required to purchase. In this respect, AI can be useful not only for insurance companies, but also for drivers themselves. Thanks to the appropriate software, we will remember about expiring insurance or even buy it directly from the comfort of our car, without having to visit the insurer's website or a stationary point.

- The German company **ACTINEO**, specializing in personal injury insurance, processes and digitizes 120,000. claims annually. Their ACTINEO Cockpit service is a digital manager that allows for the comprehensive management of this type of cases, control of billing costs, etc
- In collaboration with Ford, **Arity** provides insurers – with the driver's consent, of course – data on the driving style of the vehicle owner. In return for sharing this information, the driver is offered personalized insurance that matches his driving style. The platform's calculations are based on "more than 440 billion miles of historical driving data from more than 23 million active telematics connections and more than eight years of data directly from cars (source: Green Car Congress).

When will AI take over the automotive industry?

In 2015, it is estimated that only 5-10% of cars had some form of AI installed. The last five years have brought the dissemination of solutions such as parking assistance, driver assistance and cruise control. However, the real boom is likely to occur within the next 8-10 years.

From now on, artificial intelligence in the automotive industry will no longer be a novelty or wealthy buyers' whims. The spread of the Internet of Things, consumer preferences and finding ways of saving money in the manufacturing process will simply force manufacturers to do this – not only in the vehicle cockpits, but also on the production and service lines.

In the next section, we examine five key changes that have already been initiated in the market and which, together with the increasing use of AI, will shape the direction in which software-defined vehicles will develop. These are changes not only in terms of technology, but also legislation, nature conservation or the way we increasingly use transport (socio-cultural changes).

A modern car packed with technology, several hundred thousand pieces of information and operating at the junction of various ecosystems must be developed and considered in such a broad context. It ceased to be solely a vehicle a long time ago. Just like mobile devices, it is transforming before our eyes into a multidisciplinary machine that also provides entertainment, influences our behavior and the way we spend our leisure time.

What Trends Will Set the Course of Change in the Automotive Industry for next months

Buzzword of the next months: OTA or EV? Both!

If you are a car geek and digitalization fan, you probably know what were the hottest car premieres in 2021. But do you know what all these cars have in common?

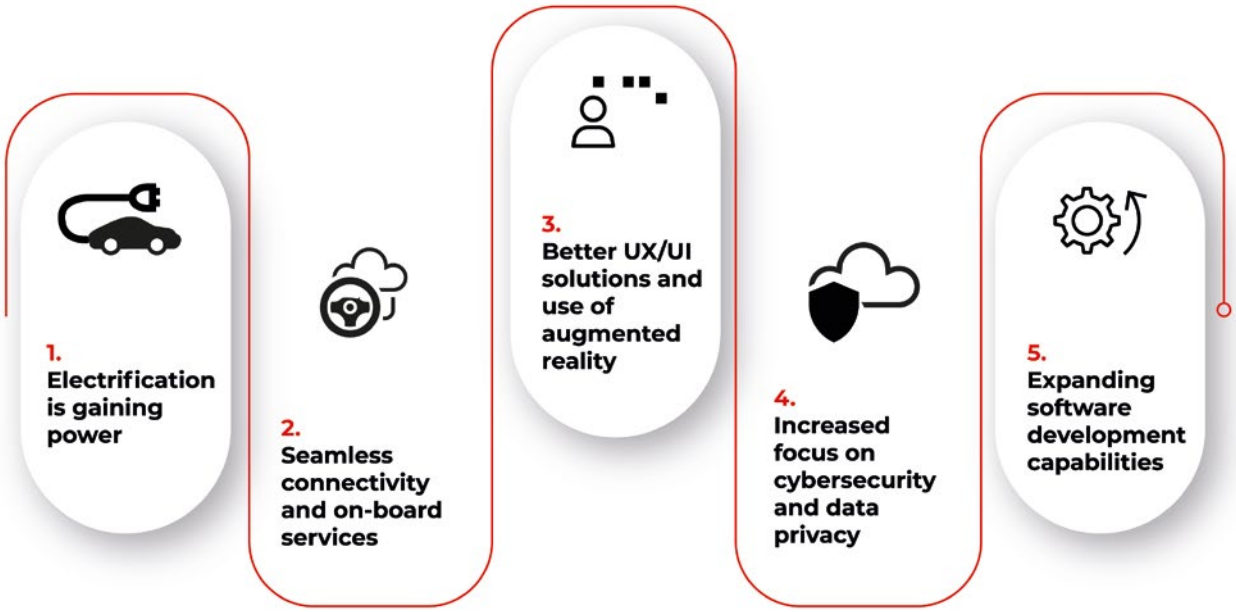
- **Audi e-Tron GT**
- **Ford Mustang Mach-E**
- **Mercedes EQS**
- **BMW iX**
- **Rivian R1T**
- **Lucid Air**

All of them are electric – because electricity is here to stay! They are all smartphones on wheels because software is the new V8! And all of them take advantage of the hottest trend in connectivity: OTA (over-the-air updates), which means the possibility of adding new features through updates without visiting the dealership. Straight from the cloud. It, at the same time, builds a highway for the creation of new revenue streams and a completely new level of customer care provided by vehicle manufacturers.

It means all the predictions and all the trends we have seen in recent years are here to stay, but now all OEMs are on board, and the trends will play a much more significant role.

Let's take a look at those that we think are worth highlighting as the automotive trends for next months and above.

What should we look at over the next months?



Change 1: Electrification is gaining power

There is no escape from electricity – mainly due to the challenges facing zero emissions. 2021 ended as the year with the highest sales of these vehicles (EV and PHEV combined), reaching 6.4 million units worldwide [EV Volumes]. This is a 98% increase compared to the previous year. It is likely that the EV sector will face changes in the next 10 years, comparable to what happened in the internal combustion engine vehicles during the first 100 years of development! What influences (and will continue to influence) the increasing consumer interest in electrics? There are numerous factors. Let's list the most significant ones.

The spread of other EVs

Urban scooters, bicycles, and electric mopeds are no longer a surprise and are increasingly becoming the dominant mode of transport in congested city centers. With the spread of the shared mobility trend, which makes it easy to rent out vehicles for a flexible period of time, consumers are gaining confidence in them and begin to notice the advantages of this solution, which is reflected in their future purchasing decisions when it comes to new cars.

New legislation on EVs

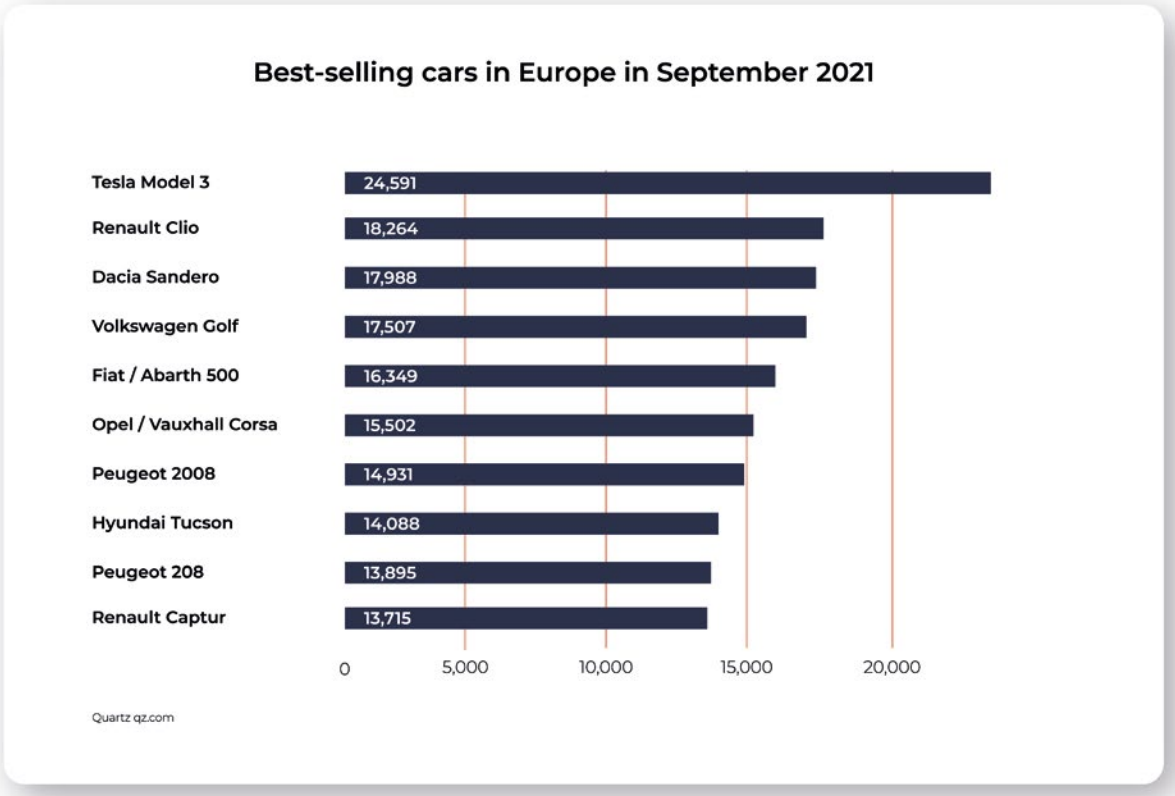
The UK, France, Norway, and Germany are implementing laws to ban the sale of new petrol cars by 2025. California wants to reach this goal in 2035 and replace its entire fleet of diesel buses with electric ones as early as 2029. Changes in legislation inevitably trigger changes in vehicle production and affect other sectors. For instance, the construction industry, which will be obliged to equip buildings with sockets and an electrical grid that will allow the charging of electrics in their own homes, which is already done in the USA.

Increased range of EV

The range of electric vehicles has always been a challenge compared to petrol

vehicles. The problem was not just the short life of the battery itself, but also the limited network of available chargers. With the development of new technologies for extracting minerals necessary for making batteries and ways of power storage, these factors will gradually become marginalized.

— **Tesla** announces it is phasing out the use of cobalt in its batteries to produce a $25,000 electric vehicle in three years – although it is already leading the way in new car sales in Europe.
— **Lilac Solutions**, a company supported by Bill Gates' Breakthrough Energy Ventures, is implementing technology that allows lithium to be extracted without draining groundwater.
— Alternatives to lithium-ion battery technology are emerging, such as the solid-state batteries being developed by **Toyota**.



— There are also growing claims that it is not batteries but **supercapacitors** that will power electric vehicles. Instead of storing energy in chemical form, like a battery, they hold it in an electric field. This makes them more durable and ensures a longer life cycle.
— In 2019, there were 175,000 public EV chargers in Europe. By 2025, it is estimated that this number will reach 1.3 million, and in **2030 it will already be 2.9 million** [EV volumes]. With the development of connected car technology, this will enable more charging points to be found efficiently and without hassle, and will substantially extend the possibility of a seamless journey.

Change 2: Seamless connectivity and on-board services

OK, 5G is the thing! In China all their biggest cities already have 5G coverage, now the USA and Europe must and will follow. 5G takes internet connectivity to another level. This is and will be a complete game-changer in several areas:

V2X for building a mesh of connected vehicles, road infrastructure and third party devices. Autonomous driving applications with hybrid cloud and edge systems, requiring very low latency. Real-time telematics for tracking the status and location of vehicles almost in real-time, which will make driving safer and more comfortable, save time, reduce vehicle operating costs or allow the purchase of an insurance policy tailored to the driver's driving style.

Change 3: Better UX/UI solutions and use of augmented reality

Cockpits of modern vehicles are filled with screens. Pushing all controls, buttons, and knobs to touchscreens decreases production costs and makes the vehicle look more premium. At the same time, customers report that the vehicle interfaces are increasingly harder to operate. Also, the old, slow, or stuttering infotainment makes the whole look & feel of the vehicle worse.

This forces manufacturers to put more effort into the UI/UX design, as well as improving other, safer ways to interact with vehicles. A great example of this are solutions already familiar to consumers in other market sectors – voice assistants and gesture recognition, as well as the most developing technology in this field, i.e. augmented reality.

The latter is increasingly used in vehicles in the form of a Heads-Up Display on the windshield. The following applications can be listed in the vehicles entering the market:

1. Intelligent Terrain Mapping – which assists the driver whilst driving by displaying directions, a road map and information about upcoming landmarks.
2. Automated Parking Assistance – which, by means of additional lines and indicators on the camera, can make parking or difficult maneuvers easier.
3. Augmented Marketing – combining AG with sales and entertainment – not only in the form of offers displayed on the windshield, but also in the course of selling vehicles and advertising them, when you can feel the driving experience without having direct contact with the vehicle.
4. Intuitive Road Safety – warning of dangerous driving, pedestrians in lanes, or drivers drifting into the other lane.

Change 4: Increased focus on cybersecurity and data privacy

The connected car operates in a V2X ecosystem consisting of data networks, road infrastructure, other vehicles, and third-party applications. In such an environment, the threat level of cyberattacks is at a very high level. Hence, in the coming years, those involved in the automotive industry must make the utmost efforts to protect not only consumers' sensitive data but also their lives and health.

That cyber attacks will occur is more than certain. The industry's task is to adapt current technology and regulations so that potential threats are minimized at the point a vehicle leaves the factory.

Cyber security should be at the heart of every SVD vehicle leaving the factory. Especially since we're not just talking about the sensors that will be programmed but entire production chains, which can also become potential targets for attack.

In order to prevent such activities, as of 2018, more than 80 organizations from around the world, have created the ISO/SAE 21434: "Road vehicles – Cybersecurity engineering" standard, which encompasses a set of guidelines for securing vehicle design, manufacturing, maintenance and decommissioning processes. These guidelines define cybersecurity processes for different phases of vehicle development, specifically:

- addressing and mitigating process vulnerabilities;
- identifying unsecured ECU (engine control unit) connection protocols;
- and unsecure aftermarket products and services.

The software industry, however, which supplies software to OEMs, must be prepared for the European Commission's regulations on AI-related rules. The

regulations are expected to cover:

- the potential risks that artificial intelligence applications can create;
- requirements for AI systems for high-risk applications;
- specific responsibilities of artificial intelligence users and high-risk application providers;
- proposals for compliance evaluation before marketing the AI system;
- governance structure for AI applications at European and national level.

In the interim period, the regulation may be effective in the second half of 2022. The second half of 2024 is the earliest period of application of the regulation to AI application operators.

Change 5: Expanding software development capabilities

The transition from a vehicle company to a company dealing with software on four wheels is a complex and challenging process. Such a transformation inevitably awaits all automotive companies in the coming years. It is worth noting a few factors that are critical to the success of this endeavor.

Companies need to build their internal software development structures, become attractive employers for software engineers and gain great partnerships in the software development world. Increased focus on reliable internet connectivity for all produced vehicles, as well as cloud connected car systems.

Work on regulatory compliance in terms of GDPR, data collected from vehicles and cybersecurity. Constant growth of software development teams and departments, as well as new partnerships regarding software, cloud and AI.

Change – the only certain thing in the automotive industry

Changes related to the reduction of CO2, the development of the Internet of Things, or automation will affect most industries in the coming years. However, the automotive sector, where technological, social, ecological, and consumer trends meet, may become a litmus test for the upcoming developments.

Just as new technologies took the telecommunications or smart building industry by storm a few years ago, they will now begin to change the way we use vehicles. Can we set a date when we can say with a high degree of certainty: this year will be the year of the connected car? Unlikely. Just as the marketing specs failed, who claimed each year: that this year will definitely be the year of mobile.

These changes grow exponentially, remaining unnoticed for a long time, but suddenly we realize that they are already with us. The two technologies presented further in this publication could be a case in point. One of them relates to the more rapid development of artificial intelligence, the other will enable the development of cloud solutions to a size that today remains only in the realm of consideration. Learn about the federated learning method and the virtual world concept, which could prove to be a real game-changer for the automotive industry.

Machine Learning at the Edge – Federated Learning in the Automotive Industry

Machine Learning combined with edge computing gains a lot of interest in industries leveraging AI at scale – healthcare, automotive, or insurance. The proliferation of use cases such as autonomous driving or augmented reality, requiring low latency, real-time response to operating correctly, made distributed data processing a tempting solution. Computation offloading to edge IoT devices makes the distributed cloud systems smaller – and in this case, smaller is cheaper. That's the first most obvious benefit of moving machine learning from the cloud to edge devices.

How can federated learning be used in the automotive industry?

Using the automotive industry as an example, modern cars already contain the edge device with processors capable of making complex computations. All ADAS (Advanced Driver Assistance Systems) and autonomous driving calculations happen on-board and require rather significant compute power. Detecting obstacles, road lanes, other vehicles, or road signs happens right now using onboard vehicle systems. That's why collaboration with companies like Nvidia becomes crucial for OEMs, as the need for better onboard SoCs does not stop.

Even though the prediction happens in the vehicle, the model is trained and prepared using regular, complex, and costly training systems built on-premises or in the cloud. The training data grows bigger and bigger making the training process computationally expensive, slower, and requiring significant storage, especially if incremental learning is not used. The updated model may take time to be passed to the vehicle, and storing the user driving patterns, or even images from the onboard camera, requires both user consent and adherence to local law regulations. The possible solution for that problem is using a local dataset from each vehicle as small, distributed training sets and training the model in the form of "federated learning", where the local model is trained using smaller data batches and then aggregated into a singular global model. This is both more computational and memory efficient.

What are the benefits of federated learning?

One of the important concepts highly associated with machine learning at edge is building Federated Learning on top of edge ML. The combination of federated learning and edge computing gives important, measurable advantages:

- **Reduced training time** – edge devices calculate simultaneously which improves velocity compared to a monolithic system.
- **Reduced inference time** – compared to the cloud, at the edge inference results are calculated immediately.
- **Collaborative learning** – instead of single, huge training dataset learning happens simultaneously using smaller datasets – which makes it both easier and more accurate enabling bigger training sets.
- **Always up-to-date model in vehicle** – the new model is propagated to the vehicle after validation which makes the learning process of the network automatic.
- **Exceptional privacy** – the omnipresent problem of secure channels for passing sensitive user data, anonymization, and storing personal user data for training purposes is now gone. The learning happens on local data in the edge device, and the data never leaves the vehicle. The weights which are being shared cannot be used to identify the user or even his driving patterns.
- **Lack of a single point of failure** – the data loss of the training set is not a threat.

Benefits from these concepts contain both cost savings and accuracy improved, visible as an overall better user experience when using the vehicle systems. As autonomous driving and ADAS systems are critical, better model accuracy is also directly associated with better security. For example, if the system can identify pedestrians on the road in front of vehicles with accuracy higher by 10%, it can mean that an additional 10% of collisions with pedestrians can be avoided. That is a measurable and important difference.

Of course, the solution does not come only with benefits. There are certain risks that have to be taken into account when deciding to transition to federated learning. The main one is that compared to the regular training mechanisms, federated learning is based on heterogeneous training data – disconnected datasets stored on edge devices. This means the global model accuracy is hard to control, as the global model is derived based on local models and changes dynamically.

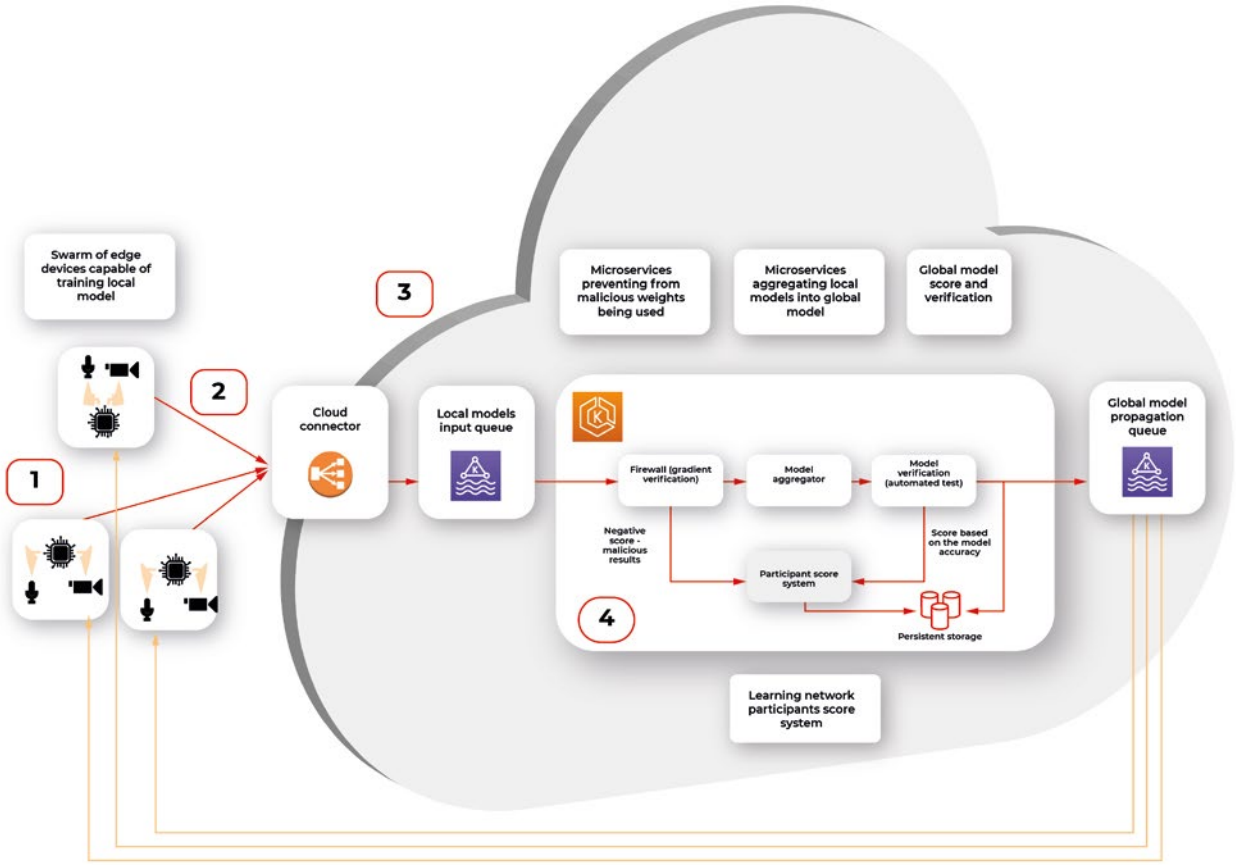
This can be solved by building a hybrid solution, where part of the model is built using safe, predefined data, and it is gradually enhanced by federated learning. This brings both worlds closer together – amounts of data impossible to handle by a singular training system and stable model based on a verified training set.

Architectural overview

To build this kind of system, we need to start with the overall architecture. Key assumptions are that the infrastructure is capable of running distributed, microservices-based systems and has queueing and load balancing capabilities.

Edge devices have some kind of storage, sensors, and SoC with CPU, and GPU capable of training the ML model.

Let's split it into multiple subsystems and consider them one by one:



1. Swarm of connected vehicle edge devices, each one with connected sensors and ability to recalculate model gradient (weights.)
2. Connection medium, in this case fast, 5G network available in the car
3. Cloud connector, being a secure, globally available public API where each of the vehicle IoT edge devices connect to.
4. Kubernetes cluster with federated learning system split into multiple scalable microservices:

   a) Gradient verification / Firewall – system rejecting the gradient that looks counterfeit – either manipulated by 3rd party or being based on fictional data.
   b) Model aggregator – system merging the new weights into the existing model and creating an updated model.
   c) Result verification automated test system – system verifying the new model on a predefined dataset with known predictions to score the model compared to the original.
   d) Propagating queue connected to (S)OTA – automatic or triggered by user propagation of updated model in the form of an over-the-air update to the vehicle.

A firewall?

The firewall here, inside the system, is not a mistake. It is not guarding the network against attacks. It is guarding the model against being altered by cyber attacks. Security is a very important aspect of AI, especially when the model can be altered by unverified data from the outside. There are multiple known attack vectors:

- **Byzantine attack** – regarding the situation, when some of the edge devices are compromised and uploading wrong weights. In our case, it is unlikely for the attacker to be omniscient (to know the data of all participants), so the uploaded weights are either randomized but plausible, like generated Gaussian noise, or flip-bit of result calculation. The goal is to make the model unpredictable.
- **Model Poisoning** – this attack is similar to the byzantine attack, but the goal is to inject the malicious model, which as a result alters the global model to misclassify objects. The dangerous example of such an attack is by injecting multiple fake vehicles into a model, which incorrectly identifies the trees as “stop” road signs. As a result, an autonomous car would not be able to operate correctly and stop near all trees as it would be a cross-section.
- **Data Poisoning** – this attack is the hardest to avoid and easiest to execute, as it does not require a vehicle to be compromised. The sensor, for example, camera, is fed with a fake picture, which contains minor, but present changes – for example, a set of bright green pixels, like on the picture:

This can be a printed picture or even a sticker on a regular road sign. If the network learns to treat those four pixels as a “stop” sign. This can be painted, for example, on another vehicle and cause havoc on the road when an autonomous car encounters this pattern.

As we can see, those attacks are specific to distributed learning systems or machine learning in general. Taking this into account is critical, as the malicious model may be impossible to identify by looking at the weights or even prediction results if the way of attack was not determined. There are multiple countermeasures that can be used to mitigate those attacks. Median or distance to the global model can be calculated and quickly identify rogue data. The other defense is to check the score of the global model after merging and revert the change if the score is significantly worse.

In both cases, the notification about the situation should be notified, both to operators as a metric and to a service that gives scores to the vehicle edge devices. If the device gets repeatedly flagged as wrong-doing, it should be kicked out of the network, and investigation is required to figure out if this is a cyberattack and who is the attacker.

Model aggregation and test

As we know, taking care of the cybersecurity threats specific to our use case, now the important step is merging the new weights with the global model.

There is no one best function or algorithm that can be used to aggregate the local models into global models by merging the individual results (weights). In general, very often average, or weighted average gives sufficient results to start with.

The Aggregation step is not final. The versioned model is then tested in the next step using the predefined data with automated verification. This is a crucial part of the system, preventing the most obvious faults – like the lane assist system stopping to recognize roadside lines. If the model passes the test with a score at least as good as the current model (or predefined value), it's being saved.

Over-the-air propagation

The last step of the pipeline is enqueueing the updated model to be propagated back to vehicles. This can be either an automatic process as in continuous deployment directly to the car or may require a manual trigger if the system requires additional manual tests on the road.

A safe way of distributing the update is using the container image. The same image may be used for tests and then run in vehicles greatly reducing the chance of deploying failing updates. With this process, rollback is also simple as long as the device is able to store the previous version of the model.

The results

Moving from legacy, monolithic training method to federated learning gives promising results in both reduced overall system cost and improved accuracy. With quick expansion of 5G low-latency network and IoT edge devices into vehicles, this kind of system can move from theoretical discussions, scientific labs, and proofs of concepts to fully capable and robust production systems. The key part of building such a system is to consider the cybersecurity threats and crucial metrics like global model accuracy from the start.

The Next Step for Digital Twin – Virtual World

Digital Twin is a widely spread concept of creating a virtual representation of object state. The object may be small, like a raindrop, or huge as a factory. The goal is to simplify the operations on the object by creating a set of plain interfaces and limiting the amount of stored information. With a simple interface, the object can be easily manipulated and observed, while the state of its physical reflection is adjusted accordingly.

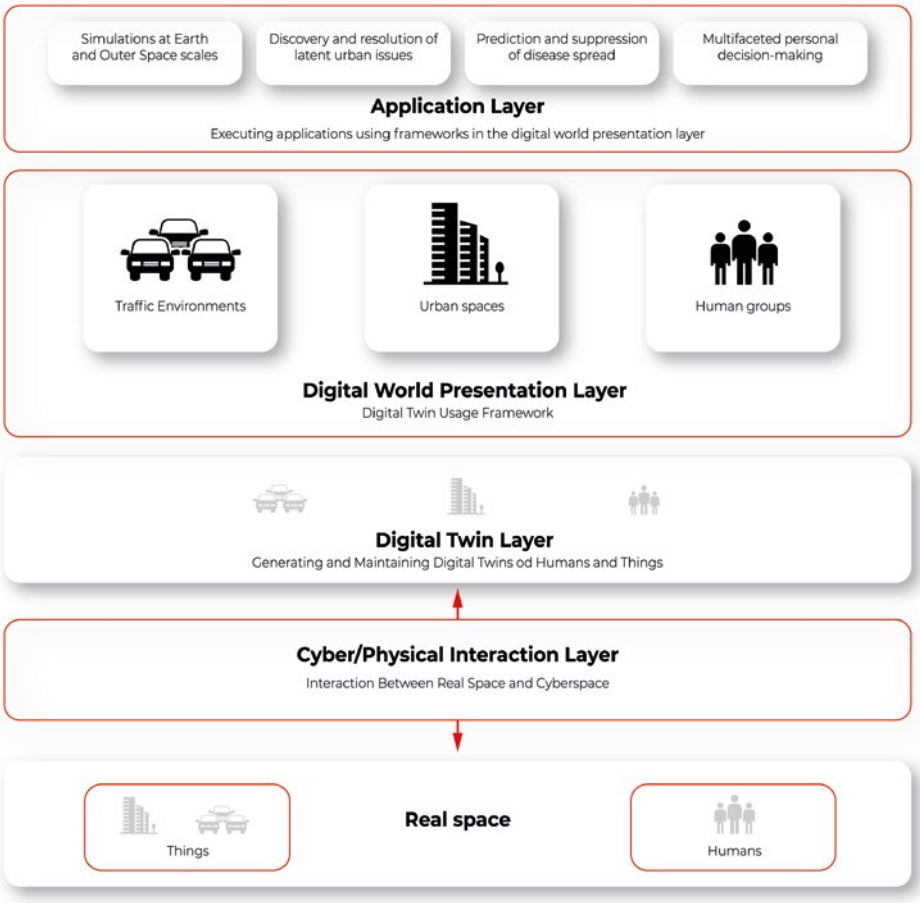
In the automotive and aerospace industries, this is a common approach to use virtual objects representation to design, develop, test, manufacture, and operate both parts of a vehicle, like an engine, drivetrain, chassis/fuselage, or a full vehicle – a whole car, motorcycle, truck or aircraft. Virtual representations are easier to experiment with, especially on a bigger scale, and to operate – especially in situations when connectivity between a vehicle and the cloud is not stable ability to query the state anyway is vital to provide a smooth user experience.

It's not always critical to replicate the object with all details. For some use cases, like airflow modeling for calculating drag force, mainly exterior parts are important. For computer vision AI simulation, on the other hand, user checking if the doors and windows are locked only requires a boolean true/false state. And to simulate the combustion process in the engine, even the vehicle type is not important.

Today, artificial intelligence takes a significant role in a lot of car systems, to name a few: driver assistance, fatigue check, predictive maintenance, emergency braking, and collision avoidance, speed limit recognition, and prediction. Most of those systems do not live in a void – to operate correctly they require information about the surrounding world gathered through V2X connections, cameras, radars, lidars, GPS position, thermometers, or ABS/ESP sensors.

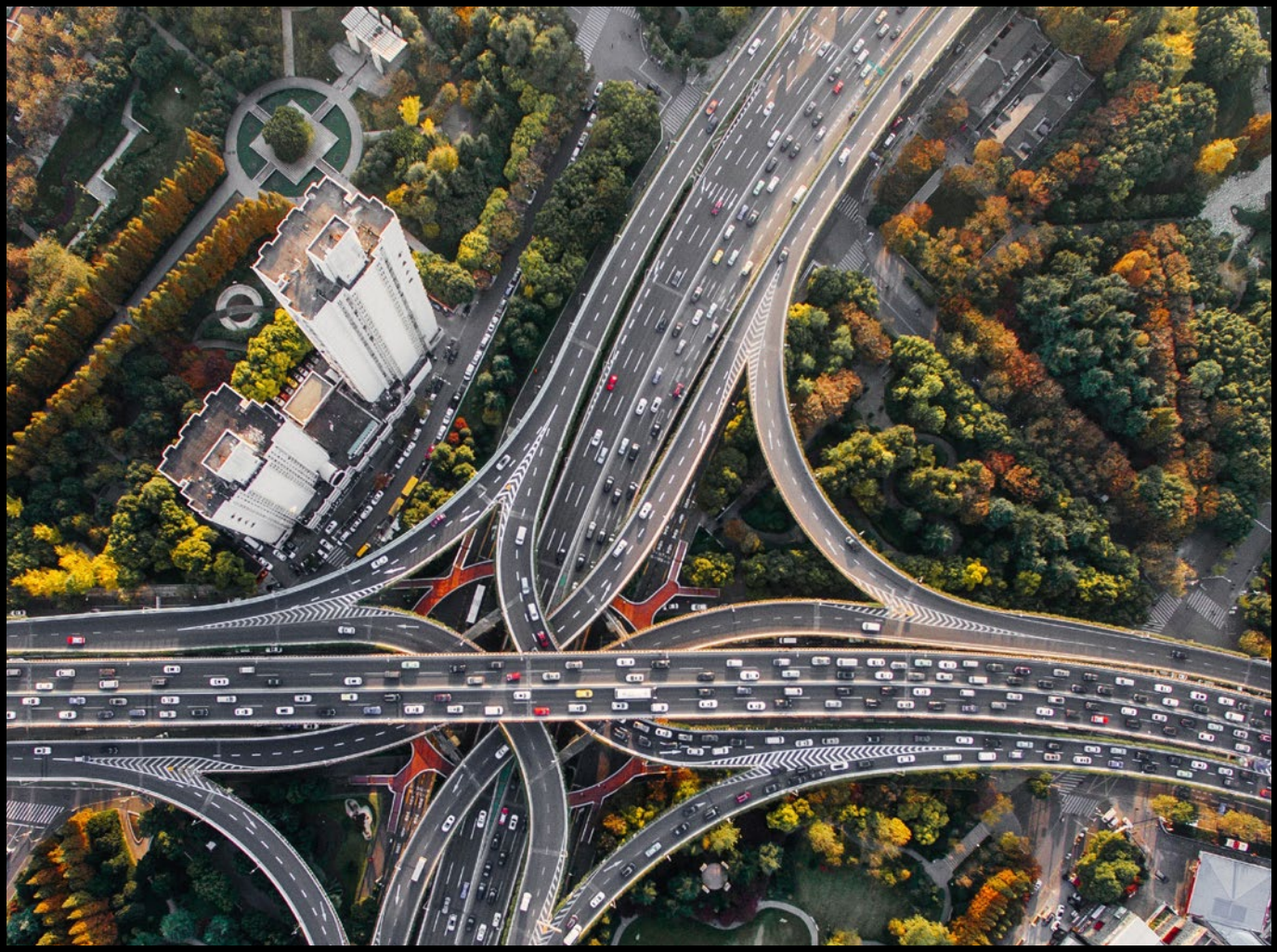
Let's take Adaptive Cruise Control (ACC). The vehicle is kept in lane using computer vision and a front-facing camera. The distance to surrounding vehicles and obstacles is calculated using both a camera and a radar/lidar. Position on the map is gathered using GPS, and the speed limit is jointly calculated using the navigation system, road sign recognition, and distance to the vehicle ahead. This is an example of a complex system, which is hard to test – all parts of it have to be simulated separately, for example, by injecting a fake GPS path. Visualizing this kind of test system is complicated, and it's hard to use data gathered from the car to reproduce the failure scenarios.

Here the Virtual World comes to help. The virtual world is an extension of the vehicle shadow concept where the multiple types of digital twins coexist in the same environment knowing their presence and interfaces. The system is composed of digital representation of physical assets whenever possible – including elements recognized via computer vision. Vehicles, road infrastructure, positioning systems, or even pedestrians are part of the virtual world. All vehicles are part of the same environment meaning they can share the data regarding the position of other traffic participants.



- Such a system provides multiple benefits: Improved accuracy of assistance systems, as the recognized infrastructure and traffic participants can come from other vehicles, and their position can be estimated even when they are still outside the range of sensors.
- Easier, more robust communication between infrastructure, vehicles, pedestrians, and cloud APIs as everything remains in the same digital system.
- Possibility to fully reproduce conditions of system failure as the state history of not just the vehicle, but all of its surrounding remains in cloud and can be used to recreate and visualize the area.
- Ability to enhance existing systems leveraging data from the greater area – for example, immediately notifying about an obstacle on the road in 500 meters and suggestion to reduce speed.
- The extensive information set can be used to build new AI/ML applications, like real-time weather information (rain sensor) can be built to close sunroofs of vehicles parked in the area.
- The same system can be used to better simulate its behavior, even using data from real vehicles.
- Common interfaces allow for quicker implementation.

Obviously, there are also challenges – the amount of data to be stored is huge, so it should be heavily optimized, and storage has to be highly scalable. There is also an impact of the connection between the car and the cloud. Overall, the advantages overweight the disadvantages, and the Virtual World will be a common pattern in the next years with the growing implementation of software-defined vehicles and machine learning applications requiring more and more data to improve its operations.



Summary

We live in a world where AI and cloud computing have already become commonplace and everyone benefits from them. Companies working at the intersection of the automotive industry should not let this moment slip by.

What seemed like a distant future just yesterday, now has become common practice. The 5G network, the growth of the Internet of Things, electrification, and new methods of machine learning mean that purchasing insurance straight from the car cockpit or uploading a new vehicle feature from an app has become an everyday activity.

To effectively develop software-defined vehicles, ensure the safety of users and at the same time open up new revenue streams for manufacturers, you need a dependable partner who understands the potential of AI. It must be someone who knows how to use its power to create the car of the future, someone that keeps abreast of changes and will provide technological support at every stage of the vehicle life cycle - from its design, through production, use and software upgrades.

Meet the authors

Adam Kozłowski

Solution Architect and Head of Automotive R&D at Grape Up

Adam had worked as a C/C++ and JavaScript Developer before he started his journey to the Cloud and Machine Learning world. Adam is an active advocate of Kubernetes and open-source cloud-native solutions. He is a huge fan of RnD initiatives, rapid prototyping, MLOps, and building great software products enhanced by ML algorithms. Throughout his career, Adam has been working with established enterprises like Rijkswaterstaat, Porsche, or Allstate to build their mission-critical systems. Currently responsible for consulting automotive projects, specializing in Cloud and MLOps solutions for the automotive industry.

Marcin Wiśniewski

Head of Business Development - Automotive Industry at Grape Up

Marcin works at Grape Up as a Head of Business Development. He collaborates closely with customers on identifying their needs and connecting them with experts helping in leveraging AI and cloud-native technologies to deliver software that ensures competitive advantage and business growth. He is an agile software development evangelist & a DevOps culture advocate.

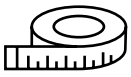
About Grape Up

Grape Up provides automotive software development and consulting services for vehicle manufacturers, mobility providers, and Tier1 suppliers. By delivering end-to-end services for building Software-Defined Vehicles, Grape Up enables the most innovative companies to create the software-centric future of the automotive industry.

Fueling the software-driven transformation in the automotive industry, we help the leading vehicle manufacturers and mobility providers execute the CASE strategy, focusing on Connected Cars and Shared Mobility.

Together, we constitute value-aligned partnerships based on constant feedback, ownership, and willingness to innovate. Developing software for automotive companies, we leverage the Agile Software Production Lifecycle, cloud-native technologies, and Data Science.

How working with Grape Up can help you innovate



You gain a system or a software product **tailored for your specific needs.**

You possess **full ownership** of the Intellectual Property.

Your team collaborates with experts in open-source technologies, and your enterprise avoids falling into the vendor lock-in trap.

We provide over 16 years of experience in building fast and reliable enterprise solutions based on Cloud and AI technologies.

Grape Up internal RnD department works with the most innovative ideas and empowers you to leverage groundbreaking technologies and cutting-edge solutions before your competitors.

Our experts actively contribute to the development of crucial technologies. Working with Grape Up, you can utilize expertise gathered through innovative R&D projects, solutions built jointly with industry leaders, and insights collected during the most influential software-related conferences.

We build our expertise by developing R&D and innovative projects for the leading automotive and insurance enterprises

Porsche Automotive Cloud

Grape Up helped Porsche AG to create a robust, scalable IoT system that can handle thousands to millions of cars from VAG and connect them to one unified platform.

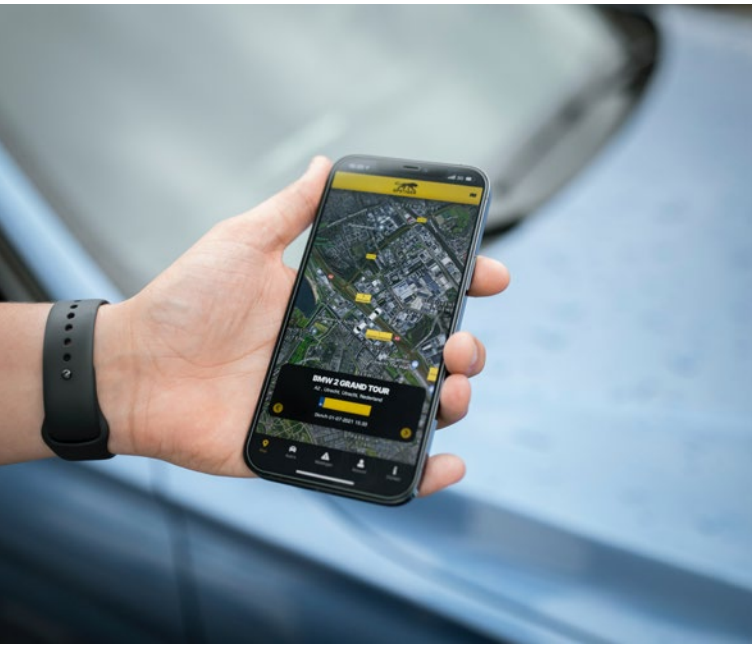
The collaboration enabled Porsche to determine technologies and concepts allowing the company to develop new services faster in the cloud and create an environment connecting users, vehicles, and third-party software - all to provide an exceptional customer experience.

AI and ML Deployment Platform

AI Deployment Platform handles a vast number of AI/ML projects for one of our partners – Sports Car Manufacturer. It is used for streamlining the process of creating, testing, and deploying to production Artificial Intelligence and Machine Learning models for Data Science teams.

Grape Up role in this project was to design reliable and extensible architecture, capable of handling hundreds of client accounts for the platform, as well as pick the best tools for the task.
The platform is hosted in the AWS cloud taking benefits from high performance across multiple regions around the globe.

Touchless and Telematics for The Leading Rental Car Company



Grape Up created an application allowing for renting cars providing the contact-less experience. Using a mobile phone, customers can make a car reservation, check its status, pay for it, locate the car as well as control basic functionalities of the car such as opening and closing the doors.

For the same customer, Grape Up designed and implemented the real-time data streaming platform which includes data such as rental rates and telematics. Along with that, Grape Up is also developing a Stolen Vehicles Recovery application.

grape up®

Do you need support from experts who specialize in cloud and internet of things solutions for the automotive industry?

Do not hesitate to contact us. We will be happy to share our expertise and experience to help you build a data monetization model, starting from your customers' actual needs.

Adam Kozłowski

Head of Automotive R&D

adam.kozlowski@grapeup.com

Marcin Wiśniewski

Head of Business Development - Automotive Industry

marcin.wisniewski@grapeup.com
+48 530 250 478