Regulatory issues in IOT and focus on autonomous driving

Legal and regulatory issues

Sample regulations - an international overview - road safety, data privacy, cyber-security, and interoperability across borders in the European Union
Summary

- Why regulators should discuss such a far-fetched topic as autonomous vehicles (AV)?
- Key Regulatory issues in IOT and focus on autonomous driving
- Legal and regulatory issues
- Sample regulations - an international overview - road safety, data privacy, cyber-security, and interoperability across borders
Why AV (autonomous vehicles) ?

• Automotive and smart metering are the top ongoing areas of growth for IoT
• The future is already here, even if it is not evenly distributed (William Gibson)
• Most AV experiments starts in deserts...
• Regulatory challenges + electronic communications + mobility transformations (smart roads/cities + AV)
IOT vs Automotive (prioritized)

**IOT:**
- Identification/profiling
- Battery life
- Data protection
- Efficiency in spectrum and numbering management
- ...
- ...
- Security not by design (data breach, mission critical fault)

**AV:**
- Safety
- Safety
- Safety
- Etc...(but also lots of mission-critical data traffic conveyed over electronic communications networks, personal data to be stored, competition in services based on data)
Legal issues in automotive

Liability/Insurance

Liability - who’s responsible for accidents (NB 94% accidents due to human errors in ordinary cars)

Insurance - In the short term, insurance will likely continue to cover drivers as the primary holders of fault, but as drivers gradually cede control of their vehicles to software, manufacturers will assume greater responsibility under strict liability theories for faults in their transportation products.

Algorithms

For claims of manufacturing defects in the physical components of the car, this area of liability laws is unlikely to see substantial change: manufacturers will continue to be liable for defects in the physical construction of their vehicles, such as flawed raw materials or erroneous assembly.

For claims of malfunction in the software algorithm controlling the car, manufacturing defect claims will be more difficult to prove: courts do not apply manufacturing defect doctrine to software because nothing is actually manufactured.

Lessons for IOT?:

In the category “design defects”, a plaintiff must prove that the design of the vehicle or algorithm was itself defective.

Courts will either perform a consumer expectations test or a cost-benefit analysis. The consumer expectations test weighs the consumer’s reasonable expectation as to the safety of his vehicle.

The introduction of autonomous vehicle technology will further complicate the application of this test, as some consumers will have unrealistic expectations of their autonomous vehicle’s capabilities.

Under a cost-benefit analysis, however, courts will balance the societal benefits of introducing autonomous vehicle technology against the cost to manufacturers of developing and installing safer technology. It will not be difficult for a manufacturer to meet this burden, as a reduction in accident rates of even a few percentage points would result in hundreds of lives and billions of dollars saved.
Regulatory challenges for NRAs

General

• Evolution of international treaties (ECE) and standards
• Mobility transformation
• Two-sided markets («platforming transport systems»)
• Jurisdiction

Specific

• Spectrum
• Numbering
• Authentication / identification
• Privacy / Data protection
• New electronic communications services (= transport services, like UBER POP according to the ECJ)
The Court declares that an intermediation service the purpose of which is to connect, by means of a smartphone application and for remuneration, non-professional drivers using their own vehicle with persons who wish to make urban journeys, must be regarded as being inherently linked to a transport service and, accordingly, must be classified as ‘a service in the field of transport’ within the meaning of EU law.

Consequently, such a service must be excluded from the scope of the freedom to provide services in general as well as the directive on services in the internal market and the directive on electronic commerce.
Firebird II (1956), GM

Already based on smart road concept (signals to drive the car home...)

The Defense Advanced Research Projects Agency (DARPA) launched a competition to develop a self-driving car in order to mitigate the risk of roadside bombings resulting in a loss of life (after 9/11).

The first competition was held on March 13, 2004 in the Mojave Desert region of the United States. The 150 miles (240 km) route followed Interstate 15. None of the robot vehicles finished the route.

The vehicle of Carnegie Mellon University's Red Team traveled the farthest distance, completing 11.78 km (7.32 mi) of the course.

In 2005, 5 vehicles completed the 212 km course.
Today

• Self-driving cars are cars that do not require the driving of the natural person, as they can independently circulate on the road through a sophisticated mechanization. They are divided into several levels - from one to five - depending on the increasing complexity of the autonomy that they can achieve on the road and the effective help that must eventually be given by the natural person driver. When can we talk about autonomous driving?
AV levels

Figure: Different levels of automation (source: Society of Automotive Engineers-SAE)

Driver role

LEVEL 0
Driver only

LEVEL 1
Assisted

LEVEL 2
Conditional automation

LEVEL 3
High automation

LEVEL 4
System can cope with all situations automatically in a defined use case

LEVEL 5
Full automation
System can cope with all situations automatically during the entire journey. No driver required.

MONITORED DRIVING

Driver is continuously exercising longitudinal OR lateral control

Driver has to monitor the system at all times; must always be in a position to resume control

NON-MONITORED DRIVING

Driver is not required during defined use

Vehicle role

Eyes on Hands on

Eyes off Hands off

 Already on the market 2020-2030
Level 1 already widely spread

• The adoption of autonomous vehicles will likely sharply reduce accident rates because human error accounts for 90% or more of vehicle accidents. To address this, Level 1 technologies are hitting the market in increasing numbers: Nissan recently announced plans to equip many of its most popular vehicles with automatic emergency braking starting in 2018. The industry predicts that adoption of Level 1 autonomous vehicle technologies alone will profoundly reduce the occurrence of accidents.
AV and connected cars metadata and identifiers

Identifiers - fitness wearable

Identifiers - connected car
More than 80 ECUs (electronic control unit)
Automakers redesign around data/digital

- Automotive companies need to think regional if not global in order to survive; they also have an interest in a data economy based on the cloud technology platform.

- However, they may not be able to manage these processes. To give a concrete example, the traffic data of vehicles belonging to rental companies, generated by their customers, may not be managed directly by these companies but by the companies that physically acquire the data and know how to process it (for example Google with Maps).

- We will soon see that this is a crucial point in the European discussion on cooperative intelligent transport systems (C-ITS).
And the beat goes on....
Controversial results from WEF study:

- Shared AVs will reduce the number of vehicles on the streets and reduce overall travel times across the city. Findings showed that the number of vehicles on the road will decrease by 15% while the total number of miles travelled will increase by 16%. However, travel time will improve by just 4% on average.

- Introducing shared AVs will worsen congestion in the downtown area, mostly because these vehicles will be chosen as substitutes for short public transportation trips. Travel time will increase by 5.5% in downtown Boston. In Allston, a neighbourhood outside the city’s core, mobility-on-demand will mainly replace the use of personal cars rather than mass transit, and travel time will decrease by 12.1%.

- With the new modal mix, Boston will require roughly half as many parking spots, including those on streets and in parking structures. AVs present an opportunity to rethink the overall design of the city’s streets.
The ITS Automotive Networking Landscape

ITS Services and Applications
- Safety Services
- Commercial Services
- Convenient/Comfort Services

Communication Platform
- V2V
- V2I
- V2x (V2R, V2CA, V2D)

Platform Characteristics across V2V, V2I, V2x
(Why it is different and more challenging from traditional network platform?)

Security and Privacy Framework

Threat Models and Risk Assessment (What are the risks and impact if security and privacy of a specific ITS Service is compromised?)

Assurance Levels (Defined criticality levels)

Security and Privacy Requirements (What needs to be done?)
- ITS Service specific Requirements
- General Security and Privacy Principles (e.g. SeVeCom, V2I, No Security)

Security Architecture (Solution Decision Blueprint)

Architecture Components
- Identity
- Security
- Privacy
- and more...

Component Relationships (How do Architecture Components compose the overall architecture?)

Technical Solutions (incl. research contributions)

Security Testing Methods

- PKI (1605, X.509, Anonymous)
- Protocols (V-HIP, V-OTLS, SAE J2735)
- Encryption (ECDSA, RSA, ECIES, IEEE)

ILLUSTRATIVE
IEEE 1609.2 – Practical Internet of Things Security (Brian Russell)

The US Dept Transportation (USDOT), and academia have been developing CV technology for many years and it will make its commercial debut in the 2017 Cadillac. In a few years, it is likely that most new US vehicles will be outfitted with the technology. The **dedicated short range communications (DSRC)** wireless protocol (based on IEEE 802.11p) is limited to a narrow set of channels in the 5 GHz frequency band. To accommodate so many vehicles and maintain security, it was necessary to 1) secure the communications using cryptography (to reduce malicious spoofing or eavesdropping attacks) and 2) minimize the security overhead within connected vehicle BSM transmissions. The industry resolved to use a new, slimmer and sleeker digital certificate design.

The 1609.2 certificate format is advantageous in that it is approximately half the size of a typical X.509 certificate while still using **strong, elliptic curve cryptographic algorithms** (ECDSA and ECDH). The certificate is also useful for general machine-to-machine communication through its unique attributes, including explicit application identifier (SSID) and credential holder permission (SSP) fields. These attributes can allow IoT applications to make explicit access control decisions without having to internally or externally query for the credential holder’s permissions. **They’re embedded right in the certificate during the secure, integrated bootstrapping and enrollment process with the PKI.** The reduced size of these credentials also makes them attractive for other, bandwidth-constrained wireless protocols.

<table>
<thead>
<tr>
<th>Networked Car</th>
<th>Access Point</th>
<th>Certificate Authority (CA)</th>
<th>WAVES (Networks)</th>
<th>Network Operations Center (NOC)</th>
<th>WAVES Service Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vehicle Applications</td>
<td>DSSM Manager (1609.5 Networking)</td>
<td>Certificate Authority (1609)</td>
<td>Radio Handler (1609.3 Networking)</td>
<td>Identity Store (LDAP)</td>
<td>Registration &amp; Identity Proofing</td>
</tr>
<tr>
<td>1609.2 Security Services</td>
<td>1609.2 Certificate Manager</td>
<td>1609.2 Certificate Manager</td>
<td>1609.2 Security Services</td>
<td>Transaction Service Manager</td>
<td>1609.2 Security Services</td>
</tr>
</tbody>
</table>

ENOC

**Identity Repository (LDAP)**
Key trend: New regulations emerging to regulate the testing and deployment of autonomous and connected cars

The European Commission
Intelligent Transportation Systems (ITS), Action Plan in 2008 for the development of harmonised standards for implementing ITS and,
in 2009, submitting a request (Mandate M/453) to the European standardisation organisations regarding cooperative systems.
The 2009 Mandate led to the development of the ‘Release 1 specifications’ by the European Committee for Standardisation (CEN) and the European Telecommunications Standards Institute (ETSI), which were adopted in 2014.

Among other things, these specifications provide guidelines for radio frequencies and messaging formats to be used, enabling vehicles made by different manufacturers to communicate with each other and with the road infrastructure systems. CEN and ETSI are currently working on ‘Release 2 specifications’ to address more complex use cases.

An amendment to the UN Convention on Road Traffic, which came into force on 23 March 2016, allows control of the vehicle to be transferred to the car in real world usage, provided that these systems can be overridden or disabled by the driver.
- 2016 - The German transport minister has proposed a bill to provide a legal framework for the use of autonomous vehicles, aiming to put fully autonomous vehicles on an equal legal footing to human drivers.
- The French government has recently given approval for autonomous vehicles to be tested on public roads in the country without special permits or restrictions

Guidelines: the regulatory focus for a long time has been on enabling testing of autonomous vehicles and providing guidelines for the development of autonomous vehicles.

Both are positive steps, however, there is a risk that without clear legislation stakeholders may opt not to follow the guidelines, leading to a discordant development of ITS.
Key trend: Autonomous vehicles give rise to new liability issues

- Car owners (or, in certain situations in civil law countries, the driver) are in the first instance liable for losses arising from accidents caused by their vehicles.
- Consequently, car owners are required to have, at a minimum, third party liability insurance. Where an accident is as a result of a fault or defect in the car, car owners/drivers may then look to others (e.g., the manufacturer of the car or any component part) for recovery of any losses.
- In 2016, a man was killed when his Tesla’s Autopilot system failed to recognise a truck turning in front of his car.
- Tesla said that the Autopilot system is not meant as a substitute for the driver maintaining control of their vehicle. However, it has been reported that the man’s family have hired lawyers with expertise in product defect litigation to represent them. Recently, an investigation by the U.S. federal government cleared the Autopilot system of any fault in the incident and even praised the system’s design for its impact on lowering the number of traffic incidents involving Tesla vehicles.
- The report did, however, note that Tesla could have been more specific about the limitations of its autonomous driving features, and so it will be interesting to see how liability is apportioned in the future, when cars are advertised as, and drivers expect them to be, fully autonomous.
- The name “autopilot” was then changed to “assisted drive mode”
Liability issues (2)

- Attributing liability: in the absence of specific legislation, car owners will remain liable in the first instance for incidents caused by their autonomous vehicles. However, if an accident occurs in an autonomous vehicle as a result of an error or shortcoming in the systems as opposed to resulting from carelessness on the part of the owner, in some cases it might be considered unjust to attribute the incidents to the car owner or driver.

- A number of complicated liability questions arise in relation to car incidents involving autonomous vehicles.

  - For example, what if the vehicle had made a choice that the driver would never have chosen: should the driver be responsible? Who should be responsible for incidents caused by defects in the software interface between two cars or between a car and the road? The car manufacturer? The manufacturer of the software that failed to prevent the accident? Who should be held liable in the case of a cyber-attack on cars? Should the software manufacturer be strictly liable for defective software security that allowed third parties to hack into the car? Or should the owner be liable if, for example, they had failed to download software security updates? Should network providers be held liable if accidents are a result of a defect in connectivity causing the incidents?

  - The US Government’s response to a recent consultation on self-driving vehicles stated that they will establish a single-insurer model whereby the driver is covered both when they are operating the vehicle, and when they have activated self-driving features. Where the manufacturer is found liable, the insurer will be able to recover against the manufacturer in accordance with existing common law and product liability law.

  - Legislators across EU member states have proved eager to support the implementation of ITS.

  - However, neither national nor EU legislators have yet started to address the many and varied liability issues that arise in relation to ITS. Stakeholders should encourage discussions on and the adoption of legislation in relation to these liability issues.

- As a means of limiting manufacturer liability, stakeholders should consider developing ITS technology that can be programmed to incorporate override options (such as manual driving or route change options) and owner’s beliefs and preferences (such as how the owner would react if obstacles suddenly appear in the car’s path).

- Allowing car owners and drivers to retain some control and interaction would also mean they retain a level of responsibility (which could make it more straightforward to point to their contributory negligence in the event of an incident).
Big data and data analytics are driving new in-car technology, services and monetisation opportunities

• The addition of the connected car to these networks will create new opportunities to collect data that can be used for analytics purposes. Data analytics leverage big data to create value in a variety of different ways, such as to: - collect more accurate and detailed vehicle performance data, which could enable development of more efficient, safer or more advanced vehicles;

• - create highly specific segmentations of customers and tailor marketing of new vehicles, new in-vehicle technology (eg traffic routing, autonomous parking), better services (eg maintenance services) to meet customer needs and in-car monetisation opportunities (eg advertising of shops on route/at destination); and - improve strategic decision making in the business, which should ultimately deliver increased profitability.

• Data minimization is also a requirement under the EU GDPR that companies will think in advance about the potential opportunities to use data collected by cars for new purposes, so data protection safeguards can be incorporated from day one, a principle known as “Privacy by Design”.

• - Storing and processing data under EU law: cross-border data transfers of personal data out of the EEA are restricted. A compliance framework must be put in place to enable data to be shared across a group of companies or partners on a cross-border basis, to enable efficient and lawful use of data in conjunction with partners. It will generally not be possible to rely simply on consents set out in terms and conditions.

• It is also necessary to make strategic decisions as to where to store and process data collected from cars. - Good data governance: the UK government’s recent report on autonomous and connected vehicles highlights the importance of good data governance. Data relating to an individual’s vehicle in terms of speed, performance and location could be used for public benefit if a connected vehicle system is to operate as a whole.
Cyber security - the threats to connected car data and services, and cars themselves, evolve

- Manufacturers will hold significant quantities of commercially valuable information. Failings in data security may damage relationships with key stakeholders and partners, and damage its reputation. Of the many reasons for this: Automotive manufacturers work with an extensive network of third parties, from service providers to partners and collaborators, as well as authorities, and share significant amounts of commercially sensitive and sometimes personal information with each of them.

- Automotive manufacturers often deal, directly or indirectly, with individual consumers. They engage with consumers using new technologies, from mobile devices to social networks. Automotive manufacturers are engaged heavily in research and development and the lifecycle of product development, during which information provides a competitive edge, for a relatively long time. The risk of data leakage is therefore high.

- Regulatory frameworks require automotive manufacturers to collect and retain significant amounts of data. The data obtained by companies can also give rise to specific regulatory obligations to share data (e.g. safety data). These regulatory requirements can sometimes conflict with each other or with commercial interests.

- The connection of the car to the internet, and the increasing use of electronic devices within cars, opens up the potential for the car itself, as part of the “Internet of Things”, to be the target of cyber-attacks. Connected cars, and their supporting infrastructure, will inevitably hold personal data about car users, such as location data, which may be of interest to cyber-attackers.

- Any network of connected devices is vulnerable to attack through any of the devices in the network. Each device is a potential entry point for cyber attackers. This is of particular concerns where connected cars are attacked, given the potential physical harm.

- Cyber-attacks: automotive companies may find that data collected from connected cars, and the cars themselves, are prime targets for hackers, and other cyber threat actors such as criminals seeking information to sell to competitors for potential commercial gain or attempting to compromise vehicle systems to extract ransoms or cause physical harm. The growing phenomenon of increasingly sophisticated cyber-attacks is a current focus for law enforcement, regulators, law makers and businesses alike.

- Regulators and policymakers in the EU are increasingly sensitive to the possibility that outsourcing and cloud computing solutions can increase the risk of foreign (particularly, U.S.) authorities gaining access to data. Suppliers of services are a frequent target for regulatory requests for data. Microsoft has reported that it received almost 110,000 law enforcement requests between January 2015 and June 2016. It recently won a court battle in which it challenged a controversial NY court ruling which would require it to hand over data about EU customers which is held on servers in Ireland.
Cars as socially networked devices

- The current generation of connected cars already incorporates a number of social media apps. For example, BMW’s ConnectedDrive system has Facebook, Twitter and a Wiki Local app (which acts like an in-car travel guide), Mercedes-Benz’s mbrace system uses Yelp to help find restaurants and Audi Connect lets drivers not only find parking at their destination, but also reserve and pay for a space. The Audi Picture Navigation app allows users to use the location metadata embedded in a photo sent from a contact to plot a destination on the car’s navigation system.

- In addition to the systems offered by car manufacturers, Apple’s CarPlay and Google’s Android Auto integrate car users’ mobile devices with the car’s digital systems, allowing use of the dashboard monitor as an interface for car users to operate their mobile devices. These systems are designed with safer driving and in-car technology use in mind. Both systems incorporate voice-recognition and text-to-speech response technology allowing for almost entirely hands-free use.

- Other vehicle based social applications include Waze, a free to use community-based traffic and navigation app acquired by Google in 2013 for almost USD 1bn. Waze allows users to share real-time traffic and road info both passively as they drive, and actively by sharing reports on accidents, police activity, or other hazards on the road. In addition, there are volunteers in communities who act as local map editors.
C-ITS Services in EU: ad hoc or existing networks?

• More rapid deployment results in faster break-even due to ‘network’ effects: Increasing the rollout rate of C-ITS services and supporting infrastructure results in higher initial costs, but a more rapid break-even and better overall benefits. This due to the ‘network’ effects of larger numbers of equipped vehicles and infrastructure resulting in a much more rapid accrual of benefits in early deployment years – clearly demonstrating the benefits of targeting a more rapid rollout. Using cellular networks to provide V2I services can have immediate benefits:

• Using the cellular network to provide V2I services rather than dedicated roadside infrastructure allows a very high infrastructure penetration to be achieved across all roads from day 1. This results in a significantly faster ramp-up of benefits in the early years of deployment, with cashflow breakeven occurring earlier and annual net benefits in 2030 increasing by over €5bn to €17.3bn, with the BCR increasing to 7.4 from 6.1 between the central and cellular scenarios.

• Whilst many uncertainties remain around the possibility of using cellular networks in this way (including latency times for safety-based services, lack of understanding of future business models or roaming issues, costs, effect on individual service impacts, etc.), there is a clear argument for carrying out further work on this topic with the aim of clarifying uncertainties and supporting accelerated deployment of C-ITS services in Europe, with the associated improved benefits that this could bring.

• A small number of cost/benefit categories dominate the overall cost-effectiveness: Two cost items make up over 96% of total costs estimated: the costs of the hardware required to support the deployment of C-ITS services to vehicles make up c. 86% of total cumulative costs to 2030 in the central scenario, followed by aftermarket devices which make up c. 10% of total cumulative costs to 2030. Three elements make up c. 99% of total cumulative benefits estimated: the biggest contributor is reduced travel times/increased efficiency (66% of cumulative benefits to 2030 in the central scenario), followed by reduced accident rates (22%) and fuel consumption savings (11%).
Map building (Here)

How the service works:

Building the foundation

The base map is the foundation of HERE HD Live Map. Captured via a highly precise industrial process using our HERE True vehicles equipped with LIDAR, collecting 2TB of data everyday - with accuracy down to centimeters.

Ingestion via the crowd

Using crowdsourced vehicle sensor data we collect drive paths, lane markings, road edges, road signs, pavement markings and more. Combined with multiple data sources like satellite imagery helps us maintain a fresh HERE HD Live Map.

Map learning in the cloud

Vehicles differ in size, sensor set-up and drive path. These variations result in many observations of the same roadside objects. The machine (map) learning of HERE aggregates this varying sensor data to determine the precise location of road-side artifacts.

Updating the map

Once a feature is created and added to our map database we publish it to our HD Live Map and send the necessary tiles back to the vehicles, providing an accurate and real-time representation of the road network.
Sample regulations
Focus is on type approval standards and regulatory laws.

Type Approval Framework

The fundamental requirement for automated cars is that their use on public roads is permitted by law. To this end, production vehicles that are sold in EU member states require EC type approval, which is issued on the basis of Directive 2007/46/EC. This Directive contains no technical requirements. In appendix IV, it states that the majority of ECE Regulations are applicable. These regulations are formulated in accordance with the 1958 ECE Agreement—an international treaty that aims to standardise the technical requirements for vehicles and auto parts across borders. An individual ECE Regulation exists for virtually every component of a vehicle, containing the relevant technical requirements.

Problems With ECE Regulations

ECE Regulation 79, which contains requirements for the steering configuration, is problematic for automated cars. An “Advanced Driver Assistance Steering System” is only allowed to control the steering as long as the driver remains in primary control of the vehicle at all times, according to paragraph 2.3.4. In addition, such systems “shall be designed such that the driver may, at any time and by deliberate action, override the function” (paragraph 5.1.6.).
In the future ECE Regulation no. 79 will differentiate the five types of automatically commanded steering function (ACSF), each of which will need to adhere to specific requirements.

- Category A will include automatic parking systems, which are legal under current regulations and may operate at a maximum speed of 12 km/h.
- Category B is an automated steering function that is initiated or activated by the driver to keep the vehicle in a lane by influencing its movement.
- Category C includes systems that extend the functionality covered by Category B. It includes systems that can perform a single manoeuvre (e.g. lane change) when activated by the driver.
- Category D systems would include a function that can indicate and execute it only after the driver’s confirmation.
- Category E covers functions initiated or activated by the driver and can continuously determine manoeuvres (e.g. lane change) and complete them for extended periods without additional intervention from the driver.
Discussions in Germany have until recently primarily focused on highly and fully automated vehicles, which, according to the German Federal Highway Research Institute (BASt), will enable the driver to pursue other activities for sections of the journey.

These degrees of automation form the basis for the work of the “Roundtable of Automated Driving” (Runder Tisch Automatisiertes Fahren), an expert group created by the Ministry of Transport; they have also been incorporated in the Federal Government’s strategy for automated and connected driving (Strategie automatisiertes und vernetztes Fahren).

However, highly and fully automated vehicles were regrettably called into question by the Ministry of Justice at the end of 2015. It appears that the relevant authorities prefer drivers to maintain constant control and reject changes to the law that would explicitly allow them to pursue other activities while driving.
On the road to automated mobility: An EU strategy for mobility of the future
Level 3-4

- Passenger cars and trucks able to autonomously handle specific situations on the motorway (automation levels 3 and 4) are expected to be available by 2020 (in particular highway chauffeur for cars and trucks, truck platooning convoys). Cars and trucks able to handle some low speed situations could be in cities by 2020, such as rubbish trucks (working together with human employees) or valet parking (cars self-driving to a parking space).

- The capabilities of vehicles will then be further developed to satisfy increasingly complex situations (e.g. longer operating time or longer range with no driver input). Public transport, vehicles able to cope with a limited number of driving situations at low speed (automation level 4) are expected to be available by 2020 (in particular urban shuttles for dedicated trips, small delivery or mobility vehicles).

- These will most likely still require human supervision and/or operate on a very short range. The number of situations that these vehicles will be able to handle will then increase with time (e.g. a longer operating time or longer range with no human supervision, higher speed).
Approval milestone

European Parliament
2014-2019

TEXTS ADOPTED

P8_TA(2018)0179
Approval and market surveillance of motor vehicles and their trailers, and of systems, components and separate technical units intended for such vehicles

Quotes from the EC Communication

• Even though automated vehicles do not necessarily need to be connected and connected vehicles do not require automation, it is expected that in the medium term connectivity will be a major enabler for driverless vehicles. Therefore, the Commission will follow an integrated approach between automation and connectivity in vehicles. When vehicles become increasingly connected and automated, they will be able to coordinate their manoeuvres, using active infrastructure support and enabling truly smart traffic management for the smoothest and safest traffic flows.

• Many vehicles are already connected with cellular technologies and all new cars are expected to be connected to the internet by 2022. This connectivity enables access to information on traffic conditions ahead (e.g. accidents, roadworks, environmental conditions), but will also allow large scale fleet data to be gathered by public authorities, such as anonymised real-life average fuel/energy consumption or real-time traffic conditions.

• As of 2019, some new vehicles series will also be equipped with short-range Wi-Fi-based communication devices. These technologies enable safety-related services requiring very low latency. They will also allow automated vehicles to coordinate their manoeuvres in complex traffic situations. As of 2020, emerging 5G technology will considerably broaden the communication mix, providing more complex and improved services.
• EU vehicle approval framework legislation, modernised in 2018, ensures a real internal market for vehicles - Member States cannot adopt national rules that contradict EU vehicle legislation - and a special procedure is foreseen for new technologies.

• The EU vehicle approval framework serves as a model for international harmonisation with our international partners (e.g. Japan, Russia and China). The United States is also planning to implement similar principles (see text box).

• In addition, EU data protection rules are increasingly recognised at international level as setting out some of the highest standards of data protection in the world and are shaping the digital revolution in line with European values. But new regulatory changes will have to follow in order to build a harmonised, complete and future-proof framework for automation.
Large scale testing (EC Comm)

- Many initiatives are already underway in the Member States (e.g. Germany, France, United Kingdom, Sweden and Netherlands), especially for large scale testing, which is also supported by the Commission. There is however a need to better coordinate these initiatives.

- In the Declaration of Amsterdam, Member States called upon the Commission to develop a shared European strategy on automated and connected driving, to review, and where necessary, adapt the EU regulatory framework, to develop a coordinated approach towards research and innovation and to deploy interoperable Cooperative Intelligent Transport Systems.
The Commission has already taken actions to promote the deployment of connectivity infrastructure and services in the support of automated vehicles with the adoption of strategies for the 5th generation of communication networks ("5G") and the space strategy.

The Commission has also recently proposed an initiative on artificial intelligence that will support driverless vehicles. The Commission has prepared the ground for a shared strategy on driverless mobility with an extensive stakeholder and Member State consultation process, in particular through the GEAR 2030 high level group which adopted recommendations on automated and connected vehicles on 18 October 2017.

Those recommendations built on earlier work to deploy Cooperative Intelligent Transport Systems and to bring together the telecom industry and the automotive industry.
CAM - Connected and Automated Mobility

• The development and large-scale deployment of Connected and Automated Mobility (CAM) provides a unique opportunity to make our mobility system safer, cleaner, more efficient and more user-friendly.

• CAM refers to autonomous/connected vehicles or self-driving cars (vehicles that can guide themselves without human intervention).

• Member States, industry and the European Commission collaborate to achieve the EU's ambitious vision for connected and automated mobility in a Digital Single Market, taking into consideration public authorities, citizens, cities and industry interests.

• With the evolution of digital technologies, such as robotics, internet of things, artificial intelligence, high-performance computers and powerful communication networks, vehicles in general, and cars in particular, are quickly changing. Therefore policies and legislation relating to digital technology, including cybersecurity, liability, data use, privacy and radio spectrum/connectivity are of increasing relevance to the transport sector. These aspects need coordination at the European level in order to ensure that a vehicle may remain connected when crossing borders.
The European Commission supports the introduction and deployment of CAM on various levels:

- Policy initiatives: developing policies, communications, roadmaps, strategies in close collaboration with stakeholders. DG CONNECT's role is to bring together stakeholders and countries to foster exchanges of experience, ideas and proposals;
- Development of standards at the European level;
- Co-funding of research & innovation projects (H2020), support actions and of infrastructure pilots;
- Legislation at the European level when needed;
- Cross-border corridors

The 29 signatory countries of a Letter of Intent signed at Digital Day 2017 agreed to designate digital cross-border corridors, where vehicles can physically move across borders and where the cross-border road safety, data access, data quality and liability, connectivity and digital technologies can be tested and demonstrated.

The European Commission's ambition is to focus on these corridors in future EU automated driving projects in the area of digital policies, with links to cybersecurity, privacy, 5G, internet of things, data economy, free flow of data, etc.
C-ITS + GEAR

• Other relevant initiatives:
  • The Cooperative Intelligent Transport Systems (C-ITS) is a system allowing the exchange of information between vehicles, and between vehicles and the road infrastructure. Road authorities/operators are working closely together on the C-ROADS Platform, which allows to harmonise the deployment of C-ITS activities across Europe. The goal is to achieve the deployment of interoperable cross-border C-ITS services for road users.

  • The Commission launched the High Level Group GEAR 2030 in January 2016, in an effort to ensure a coherent EU policy on vehicles. The group gathered several Commissioners, Member States and stakeholders representing the automotive, telecoms, IT and insurance industries. The group made recommendations to ensure that the relevant policy, legal and public support framework is in place for the roll-out of highly automated and connected vehicles by 2030.
In the context of the round table on Connected and Automated Driving (CAD), the industry has initiated the following cooperation initiatives:

- **European Automotive - Telecom Alliance (EATA)**
  - The Commission initiated a number of High Level Round Table discussions to strengthen the digital dimension of CAM. These discussions have brought together the industrial players from the digital and automotive sectors to develop joint road maps and establish cross-border deployment actions. Among the main achievements of the Round Table is the creation of the "European Automotive - Telecom Alliance" (EATA) to promote the wider deployment of connected & automated driving (read the announcement).

- **The first target of the Alliance is to implement the pre-deployment project for testing CAM in a real setting.**

- **5G Automotive Alliance**
  - In parallel, the industry joined up to create the 5G Automotive Alliance (5GAA) to specifically promote 5G in the automotive sector. A Memorandum of Understanding amongst EATA and 5GAA was signed at the Mobile World Congress (February 2017).

- **CAR2CAR Consortium**
  - The CAR2CAR consortium focuses on wireless vehicle-to-vehicle (V2V) communication applications based on ITS-G5 and concentrates all efforts on creating standards ensuring the interoperability of cooperative systems spanning all vehicles classes, across borders and brands. The Consortium works in close cooperation with the European and international standardisation organisations like the European Telecommunications Standards Institute (ETSI) and European Committee for Standardisation (CEN).