SMMT
DRIVING THE
MOTOR INDUSTRY

Connected and Autonomous Vehicles

Position Paper

THE SOCIETY OF
MOTOR MANUFACTURERS
AND TRADERS LIMITED

February 2017

Disclaimer
This publication contains general information and although SMMT has endeavoured to ensure that the content was accurate and up-to-date at the point of publication, no representation or warranty, express or implied, was made as to its accuracy or completeness and therefore the information in this publication should not be relied upon. Readers should always seek appropriate advice from a suitably qualified expert before taking, or refraining from taking, any action. The contents of this publication should not be construed as advice or guidance, and SMMT disclaims liability for any loss, howsoever caused, arising directly or indirectly from reliance on the information in this publication.

CONTENTS

LIST OF ACRONYMS

2/3/4/5G	generations of mobile telecommunications technology
3GPP	3rd Generation Partnership Project
AAM	Alliance of Automobile Manufacturers (US)
ACC	adaptive cruise control
ACEA	European Automobile Manufacturers' Association
ACSF	automatically commanded steering function (as part of UN Reg. 79 on Steering Equipment)
AEB	autonomous emergency braking
AGA	Association of Global Automakers (US)
B2B	business-to-business
bCall	breakdown call
CAV	connected and autonomous vehicle
C-CAV	Centre for Connected and Autonomous Vehicles
C-ITS	Cooperative Intelligent Transport Systems
CLEPA	European Association of Automotive Suppliers
ConVeX	Connected Vehicle to Everything of Tomorrow consortium
C-V2X	cellular vehicle-to-everything (usually implying V2V and V2I)
DCMS	Department for Culture, Media and Sport
DSRC	Dedicated Short-Range Communication
DSSA	Data Storage System for Automatically Commanded Steering Function
DVLA	Driver and Vehicle Licensing Agency
DVSA	Driver and Vehicle Standards Agency
eCall	emergency call
ECU	electronic control unit
ExVe	Extended Vehicle concept
FIGIEFA	International Federation of Automotive Aftermarket Distributors
GATEway	Greenwich Automated Transport Environment project
IP	intellectual property
ISO	International Organization for Standardization
ITS-G5	European standard for vehicular communication on IEEE 802.11p
LKA	lane keeping assistant
LTE	Long-Term Evolution
MI5	Military Intelligence, Section 5 (UK's domestic security service)
MOT	Ministry of Transport test
NIC	National Infrastructure Commission
OICA	International Organization of Motor Vehicle Manufacturers
OTP	Open Telematics Platform
PAVE	People in Autonomous Vehicles in Urban Environments consortium
R&D	research and development
RCP	remote control parking
SAE	Society of Automotive Engineers
UK CITEUK	Connected Intelligent Transport Environment project
UNECE	United Nations Economic Commission for Europe
V2C	vehicle-to-cloud
V2I	vehicle-to-infrastructure
V2V	vehicle-to-vehicle
V2X	vehicle-to-everything
VIN	vehicle identification number
WAVE	Wireless Access in Vehicular Environments (IEEE 802.11p)
WP.29	Working Party 29 (UNECE)

EXECUTIVE SUMMARY

INTRODUCTION AND BACKGROUND

Definitions

A **connected vehicle** is a vehicle with technology that enables it to communicate and exchange information wirelessly with other vehicles, infrastructure, other devices outside the vehicle and external networks. An **autonomous vehicle** is a vehicle that is, in the broadest sense, capable of driving itself without human intervention. This paper adopts the International Organization of Motor Vehicle Manufacturers' (OICA) definition of levels of automation, which is based on the Society of Automotive Engineers' (SAE) International Standard J3016 (see Figure 1 on p.17).

While series production of autonomous vehicles is still some years away, there has been an increase in **assistance systems and partial automation** (SAE Levels 1 and 2) introduced over the years to support the driver, who continues to perform and takes responsibility for the dynamic driving task. At SAE Level 3, i.e. **conditional automation**, the driver remains "in the loop" such that the driver is receptive to system-issued requests to intervene and ready to take back full control from the system. By extension, we define autonomous vehicles as technology that falls within SAE Level 4 (**high automation**) and Level 5 (**full automation**), where the driver is "out of the loop". The system is capable of performing all the functions at previous levels but without any expectation that the driver will respond to a request to intervene and take back control.

Vehicles with some levels of automation do not necessarily need to be connected, and vice versa, although the two technologies can be complementary. Technology convergence, however, will result in intelligent vehicles that are both connected and autonomous, hence **connected and autonomous vehicles** (CAVs).

Potential benefits and expected deployment

The expected economic and social benefits of CAVs to the UK are:

- £51 billion per year to the UK economy by 2030;
- 320,000 new jobs created, 25,000 of which are in automotive manufacturing by 2030;
- 2,500 lives saved and 25,000 serious accidents prevented between 2014 and 2030;
- Cleaner mobility and reduced emissions;
- Improved traffic flow and efficiency and reduced fuel consumption;
- Giving the aged and infirmed access to mobility; and
- Increased productivity.

Some vehicle manufacturers and new entrants from the technology sector choose to bypass incremental innovation along the SAE levels, particularly Level 3, and introduce autonomous vehicles outright for either specific segments of the market (e.g. autonomous taxis) or series production aimed at the wider market (e.g. Level 4 capable cars for private ownership). Other vehicle manufacturers, however, are developing autonomous driving technologies based on incremental escalation along the SAE levels, i.e. from increasing levels of driver assistance and automation to ultimately fully autonomous driving.

DATA PROTECTION, SECURITY, SAFETY AND INNOVATION

Types of vehicle generated data

This paper is concerned with data that originate in the vehicle, such as vehicle speed, fill and consumption levels, battery status, ambient temperature, vehicle location, engine injection behaviour and fuel pump performance. Vehicle data is mostly generated within the vehicle control units and is related to **technical performance** or **vehicle operation**. Vehicle generated data excludes data imported by vehicle users (e.g. mobile phone) and data received from external sources (e.g. third party apps, infrastructure data).

The relevance of vehicle operating data in terms of data protection and privacy depends on the extent to which they can be combined with other data, such as the vehicle identification number (VIN), that may result in the identification of an individual.

Various stakeholders are increasingly interested in accessing and using the growing amount of vehicle generated data. A comprehensive and broadly accepted understanding of the types of vehicle generated data, their potential applications, intellectual property (IP) implications and data protection relevance is therefore a prerequisite for informed debate. Vehicle generated data can be divided into three distinct types (see Table 2 on p.23):

- **Type 1: Non-brand differentiated data**
    - Data that is not differentiated by vehicle manufacturers; not considered IP sensitive.
    - No data protection relevance as long as it is not tied to the VIN or any personal identifier.

    1A: Data in the public interest that is contributed for improvement of traffic management and safety
    - Anonymised data is shared between contributing parties to enable improvements in traffic management and safety.
    - Examples: activation of hazard warning light, position of active emergency vehicles, road conditions, roadblocks and traffic flow data.
    - Data sharing should be based on reciprocal agreements.

    1B: Defined datasets across participating vehicle manufacturers for potential third-party commercial services
    - Anonymised data is made available based on individual agreements.
    - Examples: ambient temperature, average speed and on-street parking.

- **Type 2: Brand differentiated data**
    - Data that is differentiated by vehicle manufacturers; considered IP sensitive.
    - Strictly of a technical and/or operating nature.
    - No data protection relevance insofar as it is not tied to the VIN or any personal identifier.

    2A: Data with vehicle manufacturer-specific IP relevance
    - Anonymised data that is used for brand-specific applications and support services for the vehicle.
    - Examples: lane marking perception, proprietary sensor data, engine operating map and gearbox operating map.
    - Intellectual property shared only between vehicle manufacturers and designated partners based on B2B agreement.

2B: Data for component analysis and product improvement

- Anonymised data that is used to fulfil component analysis and product improvement related to the vehicle, having regards notably to manufacturer's obligations under product liability.
- Examples: actuator data, engine injection behaviour, fuel pump performance, automatic transmission shifting behaviour, fault memory data, battery performance and stability control data.
- Data is shared only between vehicle manufacturers and relevant component development partners and/or suppliers, based on B2B agreement, for product improvement purposes.

- **Type 3: Personal data**
  - Data that supports services requiring user or vehicle identification.
  - Data handling must meet strict data and privacy protection requirements.
  - Examples: vehicle location, movement profile, average speed, acceleration, fuel and consumption levels, where these are combined with the VIN or some personal identifiers; navigation destinations, the user's address book, personalised access to third-party services, infotainment settings, personalised in-car settings, and user's health and wellbeing data.
  - Right of access to personal data, taking into account the customer's privacy rights, is granted only to parties authorised to process data by law, contract and customer consent.

Type 1 and Type 2 data can easily become Type 3, i.e. personal, data the moment it is tied to a personal identifier, such as but not limited to the VIN.

Another type of data that is relevant to autonomous driving, but falls outside the framework set out in Table 2, is pre- and post-crash data. This type of data is stored in a Data Storage System for Automatically Commanded Steering Function (DSSA), which acts as an event data recorder for automated driving at SAE Level 3 and above. The DSSA also logs limited data, for a limited period of time, even when there is no critical event (e.g. a crash) when automated driving mode is engaged. Such data may be useful evidence to prove who is in control of the vehicle in the event of traffic violations. The DSSA must be regulated internationally to avoid a patchwork of national legislations.

Protection of personal data

SMMT members throughout the entire automotive value chain already provide high levels of data protection in full compliance with existing data protection and privacy laws and regulations. Customers are also provided with options regarding the processing and use of their personal data. No personal data is transferred to third parties without the consent of the customer, who retains the right to activate or deactivate services and transmission of data. Where consent has been given, data is processed accordingly to purposes, in a proportionate manner and not retained for longer than necessary.

Many vehicle manufacturers are signatories to the following *ACEA Principles of Data Protection in Relation to Connected Vehicles and Services*:

- We are transparent
- We give customers choice
- We always take data protection into account
- We maintain data security
- We process personal data in a proportionate manner

Where vehicle manufacturers do not control personal data processed by unaffiliated third parties that provide applications or services through the communication interfaces in the vehicle, these providers are encouraged to apply the same principles. However, vehicle manufacturers cannot be held responsible where there is a breach of privacy or loss of personal data as a result of deficiencies in non-manufacturer approved third party tethered or retrofitted devices in vehicles (e.g. dongles).

Data handling relationships and obligations in the context of fleets

Unless vehicle manufacturers have entered into a specific legal agreement with each of the registered keepers, otherwise known as the vehicle owners in the context of fleet operators, and/or have a contractual obligation to do so,

- vehicle user data, i.e. personal data, is only ever used or shared with the express and prior consent of the vehicle user, not the registered keeper;
- the primary user of a connected vehicle, i.e. the individual registering for the connected vehicle services and agreeing to the terms and conditions associated with these, must be put at the heart of any data consent process; and
- vehicle manufacturers do not by default have an obligation to provide vehicle data to registered keepers.

The onus is on either the primary user or the registered keeper, depending on their contractual agreement, to perform or request for a factory reset of personalised connected services before the vehicle is passed on to a new primary user.

Access to vehicle generated data

The connected vehicle is not a “smartphone on wheels” – the vehicle requires much higher standards in security, safety and privacy. Unrestricted direct access to vehicle generated data via an open in-vehicle interface runs the risk of compromising security, safety and privacy, as it provides an open door to unauthorised access to the vehicle’s security electronics from external sources. The integrity of vehicle systems cannot be guaranteed by vehicle manufacturers when vehicles are compromised as a result of the use of applications, services or devices (e.g. dongles) developed by third parties to directly access vehicle generated data via an open in-vehicle interface.

Overly restrictive access to vehicle generated data may stifle innovation and fair competition and hinder value creation. Access to vehicle generated data must therefore be guaranteed to be fully non-discriminatory with regard to pricing, amount and type of data made available, timeliness of data transfer and other relevant quality criteria agreed by contracting parties. It must allow for consumer choice, innovation and fair competition without the abuse of market power and the establishment of digital market monopolies.

SMMT believes that access to vehicle generated data must uphold the principles of security, safety and privacy without stifling innovation and fair competition. SMMT also supports the guiding principles on granting access to in-vehicle data and resources set out in the *European Commission C-ITS Platform Project final report*:

- Consent as data provision condition
- Fair and undistorted competition
- Data privacy and data protection
- Tamperproof access and liability
- Data economy

The European Automobile Manufacturers' Association (ACEA) and the European Association of Automotive Suppliers (CLEPA) have proposed the Extended Vehicle (ExVe) approach, whereby vehicle generated data will be relayed to a back-end server maintained by the manufacturer. The data could then be directly transferred from the manufacturer's secure back-end interface to third parties for the provision of services. Alternatively, any market participant may also set up a neutral server to gather data from one or more manufacturers' back-end servers to be provided to third parties.

The Coalition for Interoperable Data Access, which includes the International Federation of Automotive Aftermarket Distributors (FIGIEFA), stresses the need to allow for consumer choice at the point of pre-repair and in installing or using alternative, i.e. third party, apps. The Coalition calls for an interoperable, standardised and secure in-vehicle Open Telematics Platform (OTP), from which all relevant vehicle generated data should be accessible to third parties free of charge, in an unmonitored and non-discriminatory way via the on-board diagnostics.

Discussions and initiatives to find a common solution are underway at the European level.

VEHICLE CYBER SECURITY

SMMT members implement appropriate technical and organisational measures for protecting the integrity of the vehicle and its systems. High levels of technical safety, including suitable cryptography, layering, separation and identity authentication, are continuously refined for the software, firmware and hardware architectures of the vehicle as well as remote access to the vehicle via telecommunications networks.

SMMT considers guidelines to be the most appropriate measure at this stage; common guidelines at the processes level during the design and development of vehicle systems are necessary as part of the security-by-design principle. Manufacturers should be allowed the freedom to implement additional proprietary technical security solutions in addition to adhering to these process guidelines.

SMMT supports the development of a set of guidelines for ensuring vehicle cyber security currently being developed under the auspices of the WP.29 at the UNECE, specifically:

- Verifiable security measures based on existing security standards;
- Integrity protection measures;
- Appropriate measures to manage used cryptographic keys;
- Protection of the integrity of internal communications between controllers; and
- Strong mutual authentication and secure communication for remote access for online services.

These guidelines should be expanded to include high-level principles on board-level governance, the supply chain, product aftercare and incident response, personnel, procurement, and data storage and transmission.

Government support and investment therefore must not only focus on the security of vehicles but also on the cyber resilience of the entire connected mobility network.

CONNECTIVITY AND INFRASTRUCTURE

Digital infrastructure: ubiquitous connectivity as a priority

Communication involving connected vehicles can be divided into three main types based on the nature of the information exchanged: tactical (ad-hoc), strategic and infotainment. Although an autonomous vehicle does not necessarily need connectivity, vehicle-to-everything (V2X) communication complements autonomy and provides redundancy for safety-critical functions, particularly in non-line-of-sight situations and extreme weather conditions.

Four key challenges related to connectivity will shape the speed and breadth of connected vehicles deployment in the UK: **coverage, reliability, bandwidth and capacity**. Ubiquitous coverage is the automotive industry's top priority, regardless of the choice of technology, which in the current context is mainly a tussle between cellular and ITS-G5 (also known as 802.11p, WAVE or DSRC).

Many connected vehicle services available today, including certain geolocation services, navigation, WiFi hotspot, eCall, bCall and telematics, can be deployed with existing 3G and LTE 4G (or LTE-V) cellular spectrum. However, patchy and inadequate coverage in extra-urban environment and the road network, as well as unreliable signal strength, will hold the UK back as a market for deployment of connected vehicles. Some vehicle manufacturers have already stated in public that the UK is not among their top three markets of choice when launching new connected vehicle functionalities owing to poor coverage. Currently almost 4,600 miles (2%) of UK roads have no 2G coverage from any network provider, whereas only 43,000 miles (18%) and 119,000 miles (48%) have full 4G and 3G coverage respectively.

SMMT recommends:

- The Government's Centre for Connected and Autonomous Vehicles (C-CAV) should consider drawing up a plan in conjunction with the Department for Culture, Media and Sports (DCMS) to put in place the digital infrastructure needed to provide ubiquitous connectivity across the entire UK road network.

- The Government should consider, as part of its forthcoming 5G Strategy, mandating mobile network operators to extend coverage to less densely populated areas and specifically the entire UK road network as a condition for 5G licences auction. Alternatively, the Government may wish to study the feasibility of and consider introducing in-country roaming across mobile networks.

- There ought to be network neutrality, in that data transmission for safety-critical services must be prioritised ahead of other services, with each category ascribed a defined quality of service.

Strategic plan for 5G roll-out

The automotive industry welcomes the potential that 5G can deliver for high-bandwidth and low latency services, particularly in-vehicle content streaming. Vehicle manufacturers need to plan for the changes required of vehicle technology, systems and architecture way ahead of anticipated 5G roll-out in 2020. The Government's 5G Strategy should therefore provide some clarity on the UK 5G roadmap, deployment strategy and roll-out phases across industry verticals.

Certain stakeholders consider ITS-G5, which uses the 5.9 GHz frequency band, as a viable technology for short-range communication. However, some vehicle manufacturers have already decided on a future solely with cellular (LTE and 5G), while an increasing number of other manufacturers too are now seriously considering if cellular could in the longer term be the most cost-effective option that facilitates both long- and short-range communication. What is clear, though, is that ITS-G5 and C-V2X cannot coexist on the same frequency channel due to differences between the wireless systems. The automotive industry therefore supports investigations into using C-V2X (on LTE in the first instance and thereafter 5G new radio) at a carrier frequency between 3.4-3.8 GHz.

The Government should ensure that connected vehicle trials and connected corridor projects must not only actively experiment with ITS-G5 using the 5.9 GHz band, but also include LTE and 5G using the 3.4-3.8 GHz band. Ultimately, however, European-wide harmonisation and commonality in terms of communications technology is desirable. This ensures interoperability across markets and avoids cost inefficiencies.

SMMT welcomes the Government's recent Autumn Statement announcement of £740 million through the National Productivity Investment Fund targeted at supporting the market to roll out full-fibre connections and future 5G communications, including supporting 5G trials. The Government must now go further by using its convening power to set up, or support the setting up of, a national initiative to coordinate 5G trial and demonstration projects involving multiple industry verticals including automotive.

Physical infrastructure

Proper maintenance of existing informational infrastructure, including signage and gantries, is essential given a mixed-fleet environment before the motorparc gradually becomes fully connected. The Government must also ensure our national road infrastructure is maintained to a high quality to enable the deployment of SAE Level 3 driver assistance systems and Levels 4 and 5 autonomous driving. Technology at these levels relies considerably on cameras, working in tandem with radar, Lidar and other sensors. Clear road markings are therefore a priority on not just the Strategic Road Network but also the wider road network.

REGULATORY LANDSCAPE

General approach to regulation

SMMT agrees with the concept and rationale of a rolling programme of regulatory reform that the Government launched in the summer of 2016, with the aim of preparing the UK market for deployment of advanced driver assistance systems and autonomous driving technologies. However, the Government must exercise prudence and care in reforming regulation. In particular, SMMT wishes to stress that:

- New regulation must only be introduced where it is absolutely necessary, where existing regulations are inadequate, and where industry mechanisms and market forces are not capable of providing effective solutions.

- Changes to the regulatory framework must support and encourage the development and uptake of CAV technologies; they must achieve the intended outcomes rather than precipitate unintended adverse market consequences.

- The Government must work closely with SMMT and the automotive industry to ensure that the regulatory framework keeps pace with technology advancement, the effectiveness of each wave of regulatory reform is assessed and the most appropriate technologies are being reviewed. The pace of regulatory reform needs to be more rapid to react to technology roll-out.

- The Government must ensure that, when undertaking any regulatory reform, its approach is technology neutral. It must ensure that any changes do not unintentionally prejudice or promote particular technologies or the approach taken by particular manufacturers.

Harmonisation and interoperability

Harmonised international and European regulatory frameworks are necessary for legal certainty with regard to deployment and cross-border interoperability, while also providing manufacturers with the confidence that they need in order to invest. SMMT supports the joint strategy set out in the Amsterdam Declaration of April 2016, which emphasises the importance of coherent international, European and national regulatory frameworks.

In view of the decision of the UK to leave the European Union, the Government must ensure that regulatory divergence does not develop and that consistency with EU regulation and standards is maintained. This is essential if the UK is to be vehicle manufacturers' location of choice for the development, testing and deployment of CAVs. At the international level, the adaptation of relevant UN regulations to satisfy the requirements and enable the deployment of automated functions and autonomous driving must also be expedited.

An international regulatory framework is also required for the introduction and deployment of a Data Storage System for ACSF (DSSA), which acts as an event data recorder for automated driving, as a necessary supporting technology in all vehicles with SAE Level 3 and above capability. SMMT believes this must be addressed at the UNECE level in order to achieve international harmonisation, as well as to avoid a patchwork of national legislations that will only serve to hamper the deployment of autonomous vehicles.

Insurance and liability

SMMT is in **conditional agreement** with the Government's proposal that **compulsory motor vehicle insurance will be extended to create a single insurer model to protect victims where the autonomous vehicle causes a crash in automated mode**. The victim will have a direct right against the motor insurer and the insurer in turn will have a right of recovery against the responsible party to the extent there is a liability under existing laws, including under product liability laws. The Government also takes the view that it is not a proportionate response at this stage to make any changes to product liability law to facilitate the arrival of what will initially be a small number of autonomous vehicles.

SMMT's support is predicated on four important conditions:

- The proposal and its implementation **must not effectively pre-empt, or give the impression of pre-empting, the determination of fault**.

- The proposal and its implementation **must not result in unintentionally hampering consumer uptake of these vehicles through actual or perceived higher insurance premiums or the misconception that these vehicles are unsafe**.

- **A DSSA, which acts as an event data recorder for automated driving, must be made compulsory for all autonomous vehicles through international regulation**.

- There must still be **sufficient flexibility in the market for different motor insurance models** for autonomous vehicles to be offered.

Insofar as limits to liability are concerned, two additional points must be considered:

- Where the registered keeper or primary user attempts to circumvent, or fails to properly and reasonably maintain, the autonomous vehicle technology, the registered keeper or primary user whose "contributory negligence" results in an accident will have to accept responsibility and liability. However, the Government should carefully define what amounts to reasonably maintaining such technology and ensuring it is in safe working condition.

- The state-of-the-art defence principle should apply in determining limits to liability, as at the time the product was in the manufacturer's control the state of scientific and technical knowledge is such that the manufacturer could not have been expected to discover a defect. However, state-of-the-art itself is quickly becoming a moving target as software updates become more frequent.

Review of specific regulations

SMMT believes that the text of the Highway Code should be amended to account for vehicle automation capability. These specific rules should be clarified, updated or amended:

- Rule 150 (related to use of driver assistance systems and distraction) should be updated to better explain motorway assistant and remote control parking technologies.

- Rule 160 (related to driving with both hands on the wheel) should be amended to accommodate remote control parking and remote control drive, where it must be made clear the driver is still in control.

- Rule 126 (which recommends a two-second gap between vehicles) should be relaxed to enable basic platooning, involving trucks and heavy goods vehicles in the first instance, once the technology is proven to be safe.

In addition, the following Construction and Use Regulations should be clarified to enable remote control parking:

- Regulation 104 (the driver should be in a position to be able to control the vehicle)

- Regulation 107 (switching off the engine when the vehicle is not attended)
- Regulation110 (not using hand-held mobile phones while driving)

However, as long as drivers are still “in the loop”, they are still prohibited from using a hand-held mobile phone while performing ordinary driving tasks (Regulation 110).

The Driver and Vehicle Licensing Agency (DVLA) and Driver and Vehicle Standards Agency (DVSA) must start examining the potential implications on, and the possible repurposing of, driver training, licensing, the driving test and the MOT test in preparation for the deployment of vehicles with increasing levels of automation, culminating with fully autonomous vehicles.

MAKING THE UK A GLOBAL CENTRE OF EXCELLENCE

National strategy

The automotive industry has welcomed the creation of the Centre of Connected and Autonomous Vehicles (C-CAV) which acts as a vital focal point for all of the Government's work in relation to CAVs. We also commend the Government for backing CAV technology research, development and testing through project funding. The Government’s rolling programme of regulatory reform is another step in the right direction, as is its continuing engagement with the industry.

C-CAV must now go one step further by developing a clear and joined-up national strategy for making the UK a global centre of excellence in relation to CAVs based on a thorough understanding of UK strengths and competencies. This must be done by working closely with the automotive industry through SMMT and the Automotive Council and by building on the significant strengths that already exist in not just the automotive industry but also adjacent industries such as technology (software, artificial intelligence), cyber security, telecoms and insurance.

A national strategy should:

- Articulate in very clear terms how the UK should leverage on the outcomes of the publicly funded CAV projects and testbed ecosystem;

- Focus on funding a small number of ambitious game-changing projects rather than spreading public funds more thinly over a larger number of less impactful, albeit interesting, projects;

- Set out how the Government plans to create the conditions (e.g. national infrastructure, R&D capabilities, skills and finance opportunities) that will make the UK attractive for CAV investment;

- Prioritise developing a pipeline of highly skilled engineering talent from non-traditional automotive engineering backgrounds (e.g. electrical and software engineering, machine learning and artificial intelligence, data science and human factors) to deliver future CAV technologies; and

- Consider setting up a neutral national data aggregation platform for sharing anonymised data for the improvement of traffic management and safety.

Forging public acceptance

Soft barriers related to public acceptance and trust may hold back the widespread deployment of CAVs. Consumer education and a strategic plan for integrated communications that take the public on a journey from the lower levels of vehicle automation through to fully autonomous driving are pivotal for gaining consumer buy-in and for increasing public confidence.

SMMT calls for the Government to set up for CAVs the equivalent of the Go Ultra Low campaign for ultra low emission vehicles. This should be a consumer-targeted campaign that is jointly funded by the Government and participating vehicle manufacturers, and that seeks to provide the public with a one-stop-shop resource for information and potential purchase decision. Planning and preparation for such initiative should commence now, geared towards launch in conjunction with the introduction of the first Level 4 capable vehicle in the UK market.

1. INTRODUCTION AND BACKGROUND

1.1 Definitions

From what was purely a mechanical invention, the automobile has evolved to become a highly sophisticated machine replete with digital technologies. *Connected* and *autonomous driving* technologies are continuing to revolutionise vehicles and fundamentally changing the driving experience. It is expected to also change the way we "consume" mobility in the future.

A **connected vehicle** is a vehicle with technology that enables it to communicate and exchange information wirelessly with other vehicles, infrastructure, other devices outside the vehicle and external networks. Connected vehicles have the potential to increase convenience and comfort for drivers and passengers, improve personalisation and delivery of services, and contribute towards achieving social objectives such as enhancing road safety, reducing fuel consumption and emissions, facilitating parking, and improving traffic management and efficiency.

An **autonomous vehicle** is a vehicle that is, in the broadest sense, capable of driving itself without human intervention. This paper adopts the International Organization of Motor Vehicle Manufacturers' (OICA) definition of levels of automation,[1] which is based on the Society of Automotive Engineers' (SAE) International Standard J3016[2] (Figure 1). A recent update to SAE J3016 that provides more granular technical description is available in Appendix A.

While series production of autonomous vehicles is still some years away, there has been an increase in **assistance systems and partial automation** (SAE Levels 1 and 2) introduced over the years to support the driver, who continues to perform and takes responsibility for the dynamic driving task. These include lane departure warning, collision warning, blind spot monitoring, adaptive cruise control (ACC), lane keeping assistant (LKA), parking assistant, autonomous emergency braking (AEB) and remote control parking (RCP). See Appendix B for a glossary of these features. The driver is still ultimately responsible for the dynamic driving task.

At SAE Level 3, i.e. **conditional automation**, the driver remains "in the loop" such that the driver is receptive to system-issued requests to intervene and ready to take back full control from the system as necessary and acknowledge any vehicle warnings issued by vehicle systems that do not necessarily issue a transition demand (e.g. fuel tank depletion, faulty headlamp). The difference, however, is that the driver does not need to monitor the dynamic driving task nor the driving environment at all times, as this is performed by the system when it is engaged.

By extension, we define autonomous vehicles as technology that falls within SAE Levels 4 and 5, where the driver is "out of the loop", i.e. the driver is no longer needed during the specific use cases (Level 4) or in full end-to-end journeys (Level 5). The system is capable of performing all the functions at previous levels but without any expectation that the driver will respond to a request to intervene and take back control of the dynamic driving task. The difference between these two levels is in the scope of its use. At Level 4, i.e. **high automation**, the system's capability is restricted to defined use cases, or operational design domains, such as urban automated driving. At Level 5, i.e. **full automation**, the

[1] The International Organization of Motor Vehicle Manufacturers' definition, accessible at https://www2.unece.org/wiki/download/attachments/25886757/(ITS-AD_04-14)%20OICA_TF_AD_Presentation_ITS_AD_Meeting_2015_06_15.pdf?api=v2.

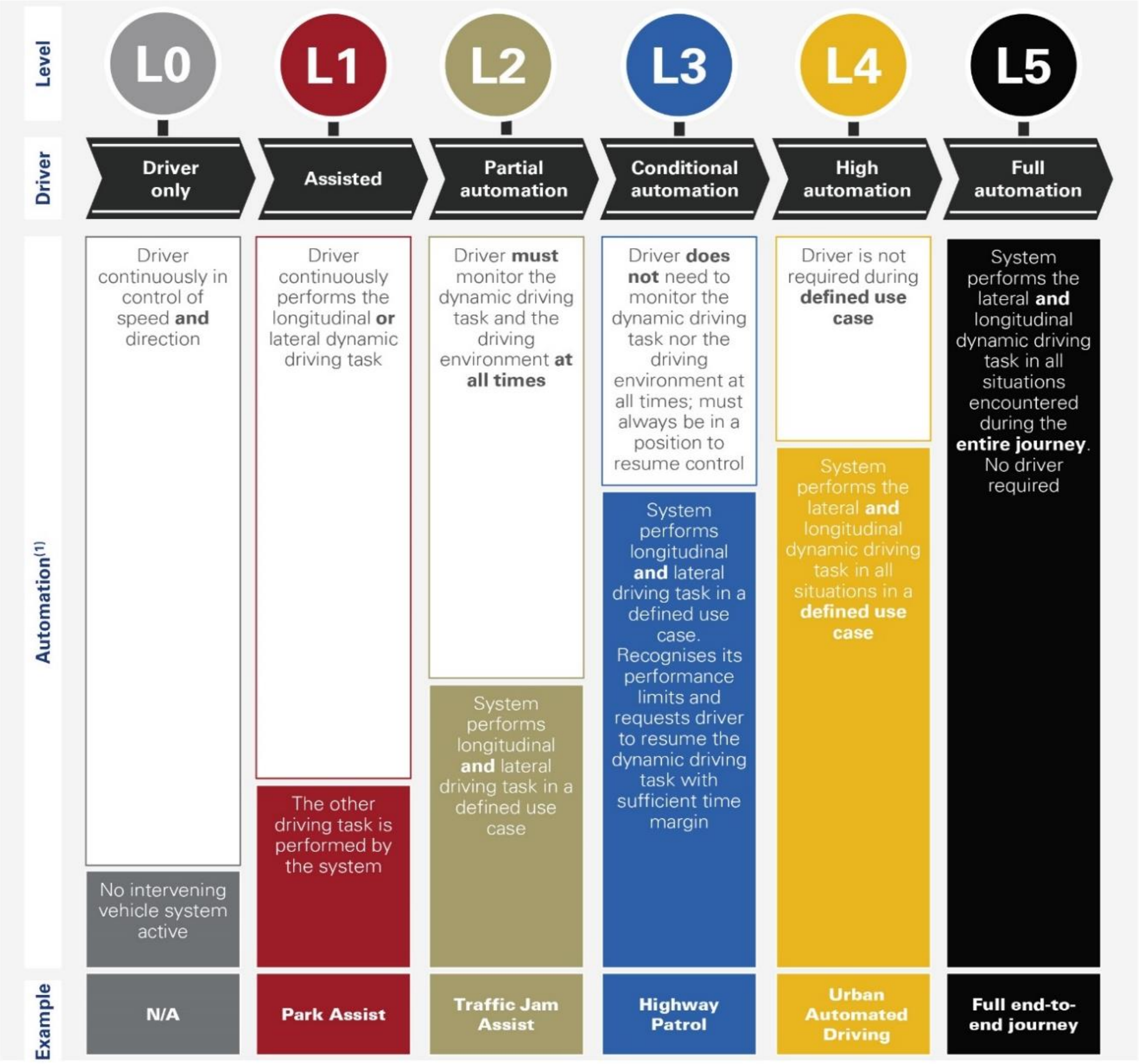
[2] The Society of Automotive Engineers' definitions published under International Standard J3016, accessible at http://www.sae.org/misc/pdfs/automated_driving.pdf.

system is capable of performing under any use case. In other words, it is capable of self-driving to deliver full end-to-end journeys.

Vehicles with some levels of automation do not necessarily need to be connected, as they are able to discern the environment and perform certain functions without necessarily being connected to a network, other vehicle or infrastructure. On the other hand, connected vehicles already on the market today do not necessarily have automated capabilities. The two technologies, however, can be complementary, particularly in situations where Level 3 and above automation may be enhanced by connectivity to receive warnings of objects that are out of the line of sight (e.g. at blind junctions) and to receive information regarding distant environments (e.g. traffic disruption five miles ahead).

As technology advances, there will be future convergence of both connected and autonomous driving technologies, resulting in intelligent vehicles that are both connected and autonomous. We refer to these as **connected and autonomous vehicles** (CAVs).

Figure 1: Levels of automation.



Level	L0	L1	L2	L3	L4	L5
Driver	Driver only	Assisted	Partial automation	Conditional automation	High automation	Full automation
Automation[1]	Driver continuously in control of speed **and** direction	Driver continuously performs the longitudinal **or** lateral dynamic driving task	Driver **must** monitor the dynamic driving task and the driving environment **at all times**	Driver **does not** need to monitor the dynamic driving task nor the driving environment at all times; must always be in a position to resume control	Driver is not required during **defined use case**	System performs the lateral **and** longitudinal dynamic driving task in all situations encountered during the **entire journey**. No driver required
	No intervening vehicle system active	The other driving task is performed by the system	System performs longitudinal **and** lateral driving task in a defined use case	System performs longitudinal **and** lateral driving task in a defined use case. Recognises its performance limits and requests driver to resume the dynamic driving task with sufficient time margin	System performs the lateral **and** longitudinal dynamic driving task in all situations in a **defined use case**	
Example	N/A	Park Assist	Traffic Jam Assist	Highway Patrol	Urban Automated Driving	Full end-to-end journey

Source: OICA's Levels of Automated Driving, based on SAE J3016. See Appendix A for a recently updated SAE J3016 with technical description.

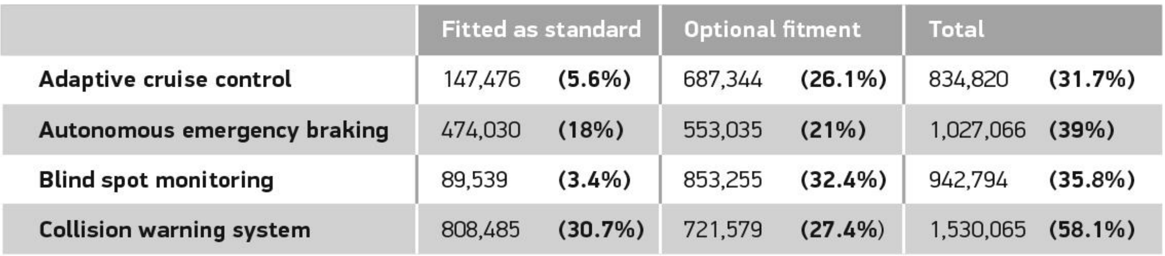
1.2 Potential benefits and expected deployment

The overall economic benefits of CAVs to the UK are expected to be in the region of £51 billion per year by 2030, of which £16 billion accrue to adjacent industries such as telecoms, technology, digital services and freight. It is also expected that up to 320,000 new jobs will be created, 25,000 of which are in automotive manufacturing, in the same period. Given that 94% of traffic accidents occur due to human error, significant social benefits are expected to be realised in increased safety that comes with automation, which could see 2,500 lives saved and 25,000 serious accidents prevented in the UK between 2014 and 2030.[3] Low-speed AEB technology, for example, has led to a 38% reduction in real world rear-end crashes.[4]

CAVs are also expected to contribute to cleaner mobility and increased productivity as they are capable of platooning and travelling at optimised speeds and headway gaps, thereby improving traffic flow and efficiency while reducing fuel consumption and emissions. For example, a government-commissioned study suggests a 12% improvement in delays and a 21% improvement in journey time reliability on urban roads in peak traffic periods even with low numbers of autonomous vehicles on the roads.[5] Another study shows that intelligent transport systems can potentially reduce CO_2 emissions by up to 20% by connecting vehicles with each other and with infrastructure.[6] Autonomous vehicles are also capable of giving the aged and infirmed who are not able to drive access to mobility.

However, the promise of these benefits and recent progress and press coverage may have given the public an impression that it will soon be technically feasible to introduce autonomous vehicles on UK roads. At the time of writing, vehicles on the market are only as advanced as SAE Level 2. SMMT new car registration figures show there is now a sizeable proportion of new cars in the UK fitted with driver assistance systems as either standard or optional (Table 1).

Table 1: Driver assistance systems in new cars registered in the UK, 2015.



	Fitted as standard		Optional fitment		Total	
Adaptive cruise control	147,476	**(5.6%)**	687,344	**(26.1%)**	834,820	**(31.7%)**
Autonomous emergency braking	474,030	**(18%)**	553,035	**(21%)**	1,027,066	**(39%)**
Blind spot monitoring	89,539	**(3.4%)**	853,255	**(32.4%)**	942,794	**(35.8%)**
Collision warning system	808,485	**(30.7%)**	721,579	**(27.4%)**	1,530,065	**(58.1%)**

Source: JATO Dynamics analysis of SMMT new car registration data 2015.

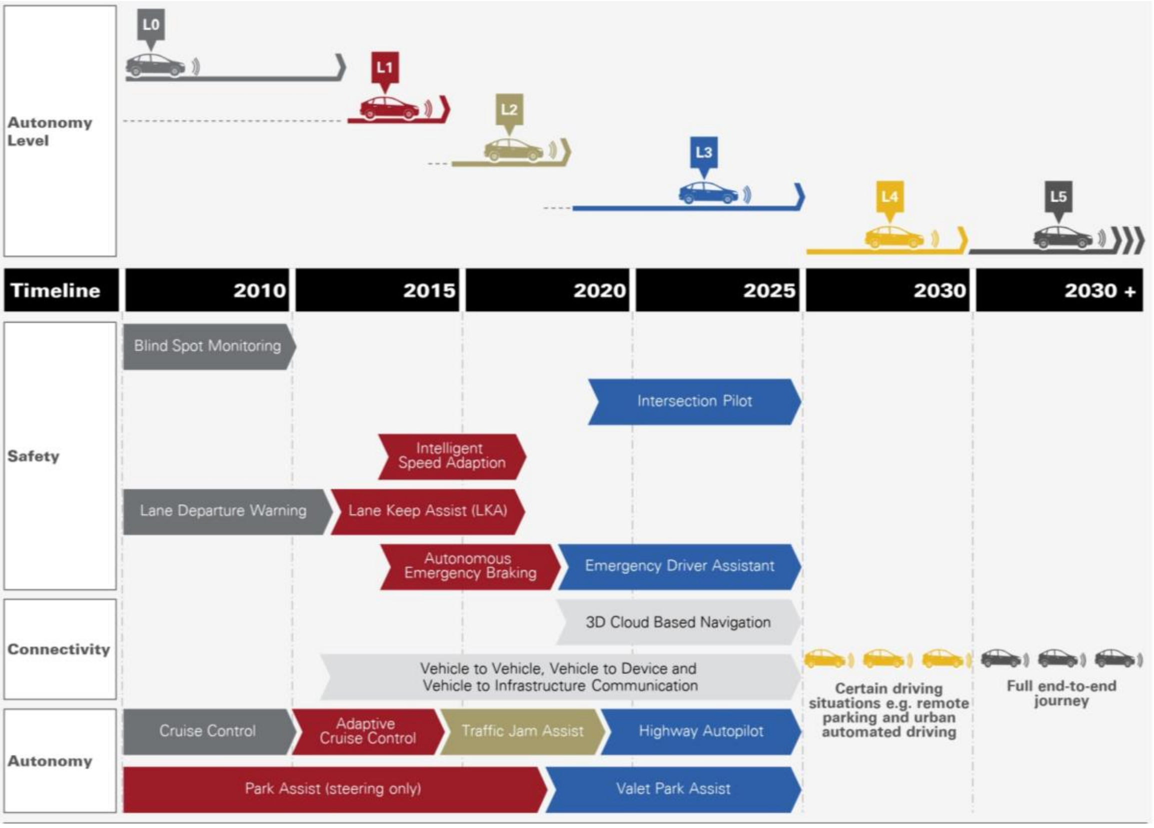
Some vehicle manufacturers and new entrants from the technology sector choose to bypass incremental innovation along the SAE levels, particularly Level 3, and introduce autonomous vehicles outright for either specific segments of the market (e.g. autonomous taxis) or series production aimed at the wider market (e.g. Level 4 capable cars for private ownership). Other vehicle manufacturers, however, are developing autonomous driving technologies based on incremental escalation along the

[3] KPMG (2015), Connected and Autonomous Vehicles: The UK Economic Opportunity.
[4] Fildes, B. et al. (2015), “Effectiveness of low speed autonomous emergency braking in real-world rear-end crashes”, Accident Analysis & Prevention, 81: 24-9.
[5] Atkins (2016), Research on the Impacts of Connected and Autonomous Vehicles (CAVs) on Traffic Flow.
[6] ERTICO (2015), Study of Intelligent Transport Systems for Reducing CO_2 Emissions for Passenger Cars.

SAE levels, i.e. from increasing levels of driver assistance and automation to ultimately fully autonomous driving.

A roadmap commissioned by SMMT suggests that production models of autonomous vehicles are expected to become widely available from 2025 (Figure 2), but will still account for less than 10% of the UK motorparc by 2030 (Figure 3). By contrast, we are more likely to see the rise in uptake of connected vehicles earlier than autonomous vehicles. By the end of this decade, connected vehicles are expected to make up a fifth of the UK motorparc and become the majority by 2025-26 (Figure 3).

Figure 2: Connected and autonomous vehicles technology roadmap.

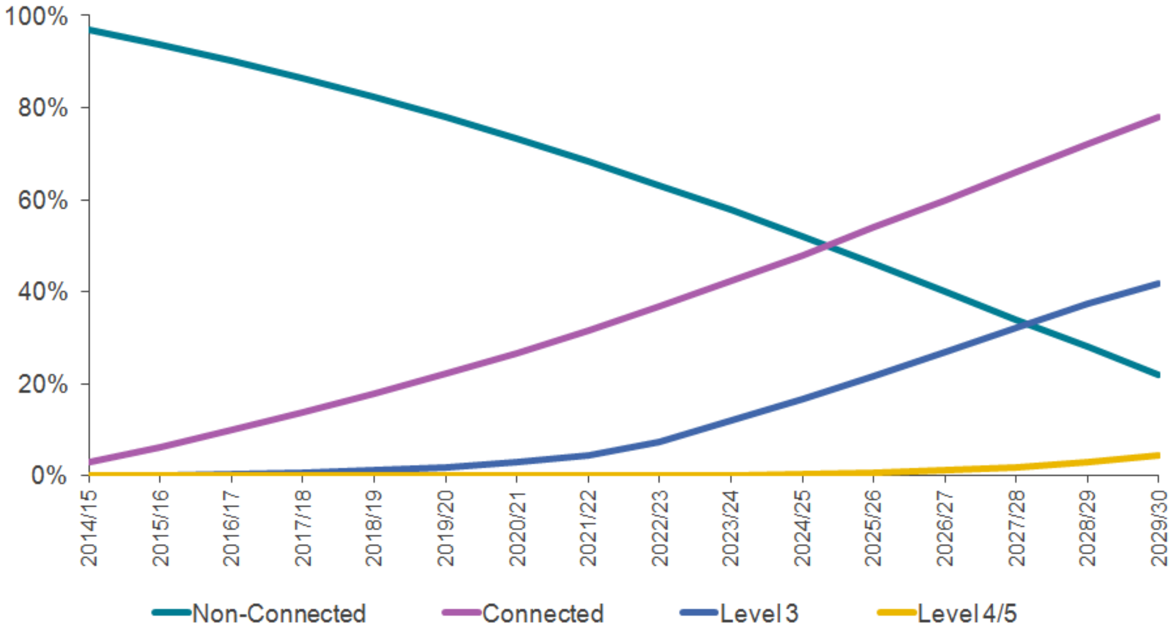

Autonomy Level
L0
L1
L2
L3
L4
L5
Timeline
2010
2015
2020
2025
2030
2030 +
Safety
Blind Spot Monitoring
Intersection Pilot
Intelligent Speed Adaption
Lane Departure Warning
Lane Keep Assist (LKA)
Autonomous Emergency Braking
Emergency Driver Assistant
Connectivity
3D Cloud Based Navigation
Vehicle to Vehicle, Vehicle to Device and Vehicle to Infrastructure Communication
Certain driving situations e.g. remote parking and urban automated driving
Full end-to-end journey
Autonomy
Cruise Control
Adaptive Cruise Control
Traffic Jam Assist
Highway Autopilot
Park Assist (steering only)
Valet Park Assist

Source: KPMG (2015), Connected and Autonomous Vehicles: The UK Economic Opportunity.

The automotive industry shares the Government's ambition to make the UK a leading location in the world for the development, testing and deployment of CAVs. However, the automotive industry cannot do this alone; the CAV ecosystem is one that essentially involves a wide range of key players. SMMT believes that to unlock the full economic, social and environmental potential of CAVs, close collaboration among the automotive industry, the Government and key adjacent industries such as technology, telecoms, insurance and infrastructure is both necessary and pivotal.

Because CAVs involve the integration of various technologies that originate from other industries and create potential economic value that is of interest to various stakeholders, a number of key issues and challenges that are relatively new to the automotive industry have emerged. This paper examines these issues and challenges, and sets out SMMT's position on data, vehicle cyber security, connectivity and infrastructure, the regulatory landscape and the UK's quest for global leadership.

Figure 3: Technology take-up as a percentage of total UK vehicle fleet.



Source: KPMG (2015), Connected and Autonomous Vehicles: The UK Economic Opportunity.

2. DATA PROTECTION, SECURITY, SAFETY AND INNOVATION

2.1 Types of vehicle generated data

This paper is concerned with data that originate in the vehicle, such as vehicle speed, fill and consumption levels, battery status, ambient temperature, vehicle location, engine injection behaviour and fuel pump performance. Vehicle generated data provides the basis for connectivity and a host of resulting services, including traffic management, infotainment, telematics and predictive diagnosis of vehicle or component condition. Vehicle generated data excludes data imported by vehicle users (e.g. mobile phone) and data received from external sources (e.g. third party apps, infrastructure data).

Vehicle data is mostly generated within the vehicle control units and is related to **technical performance** or **vehicle operation**. Such data records the system status for certain critical events (e.g. component malfunction, airbag deployment, stability control) as well as relevant information for vehicle functions (e.g. number of revolutions, acceleration, speed, ambient temperature, fuel levels, brake pad wear). Vehicle operating data is mostly volatile, as it is dependent on vehicle manufacturer, vehicle type, components, fitments and driving behaviour. Some operating data is recorded and stored for quality assurance purposes and the fulfilment of statutory product monitoring obligations.

However, some vehicle data may be relevant for data and privacy protection. The relevance of vehicle operating data in terms of data protection and privacy depends on the extent to which they can be combined with other data, such as the vehicle identification number (VIN), that may result in the identification of an individual. Similarly, to the extent that it can be tied to a personal identifier, data originating from the embedded connected vehicle system, such as navigation destinations, the user’s address book, personalised access to services and infotainment settings, may be considered personal data.

Various stakeholders are increasingly interested in accessing and using the growing amount of vehicle generated data. Repair and maintenance services, insurers, fleet operators, road infrastructure operators, traffic management authorities, entertainment and travel service providers, social networks, and even advertisers are all interested in accessing vehicle generated data for commercial purposes. Vehicle generated data may have potentially useful applications, such as to contact emergency services in the event of an accident, to predict when the vehicle is likely to require maintenance or repair in order to avoid a breakdown, to enable usage-based insurance, to provide personalised infotainment services, to provide relevant real-time localised information, to automatically pay for parking or tolls, and to advise the driver on route planning or diversion.

In the meantime, regulatory initiatives are under way in various jurisdictions as well as at the international level to regulate data sharing and protection, particularly in relation to personal data, for instance the EU General Data Protection Regulation that will come into effect from 25 May 2018. The European Commission, mandated by the eCall legislation, will assess the need for an interoperable, standardised, secure and open-access platform for accessing vehicle data by June 2017.

A comprehensive and broadly accepted understanding of the types of vehicle generated data, their potential applications, intellectual property (IP) implications and data protection relevance is therefore a prerequisite for informed debate. Vehicle generated data can be divided into three distinct types, namely non-brand differentiated, brand differentiated and personal data, as set out in Table 2.

- **Type 1: Non-brand differentiated data**
  Data that is not differentiated by vehicle manufacturers, and is therefore not considered IP sensitive. Such data has no data protection relevance as long as it is not tied to the VIN or any personal identifier.

  1A: Data in the public interest that is contributed for improvement of traffic management and safety
  Anonymised data is shared between contributing parties (e.g. between vehicle manufacturers and public authorities) to enable improvements in traffic management and safety. Examples include activation of hazard warning light, position of active emergency vehicles, road conditions, roadblocks and traffic flow data. However, data sharing should be based on reciprocal agreements so that contributing parties are entitled to use the shared data. A public authority-held neutral platform for data aggregation may be a conduit for the sharing of this type of data.

  1B: Defined datasets across participating vehicle manufacturers for potential third-party commercial services
  Anonymised data is made available based on individual agreements (e.g. between vehicle manufacturers and app developers). Examples include ambient temperature, average speed and on-street parking.

- **Type 2: Brand differentiated data**
  Data that is differentiated by vehicle manufacturers, and is therefore considered IP sensitive. Such data is strictly of a technical and/or operating nature, and has no data protection relevance insofar as it is not tied to the VIN or any personal identifier.

  2A: Data with vehicle manufacturer-specific IP relevance
  Anonymised data that is differentiated according to a vehicle manufacturer’s IP and is used for brand-specific applications and support services for the vehicle. Examples include lane marking perception, proprietary sensor data, engine operating map and gearbox operating map. As it constitutes intellectual property, such data is shared only between vehicle manufacturers and designated partners, which may include subsidiaries and/or dealers, based on B2B agreement.

  2B: Data for component analysis and product improvement
  Anonymised data that is differentiated according to a vehicle manufacturer’s IP and is used to fulfil component analysis and product improvement related to the vehicle, having regards notably to manufacturer’s obligations under product liability. Examples include actuator data, engine injection behaviour, fuel pump performance, automatic transmission shifting behaviour, fault memory data, battery performance and stability control data. Data is shared only between vehicle manufacturers and relevant component development partners and/or suppliers, based on B2B agreement, for product improvement purposes.

Table 2: Types of vehicle generated data.

Type of data	Type 1: Non-brand differentiated data		Type 2: Brand differentiated data		Type 3: Personal data
Description of datasets	1A: Data in the public interest that is contributed for improvement of traffic management and safety	1B: Defined datasets across participating vehicle manufacturers for potential third-party commercial services	2A: Data with vehicle manufacturer-specific IP relevance	2B: Data for component analysis and product improvement	3: Data that supports services requiring user or vehicle identification, or the use of personal data including but not limited to the VIN
Examples	Local hazard warning/activation of hazard warning light, accident position, position of active emergency vehicles, roadblocks, icy roads, potholes, average speed/traffic flow, ambient temperature	Ambient temperature, average speed, road sign recognition, on-street parking	Engine operating map, gearbox operating map, lane marking perception, proprietary sensor data, software algorithms	Actuator data, engine injection behaviour, fuel pump performance, automatic transmission shifting behaviour, fault memory data, battery performance, stability control data, battery status, brake pad wear	Vehicle location, movement profile, average speed, acceleration, fuel and consumption levels (along with VIN); navigation destinations, address book, personalised access to third-party services, infotainment settings, personalised in-car settings (e.g. seat), health and wellbeing data
Potential data processors	Public authorities (e.g. Highways England, local authorities)	Commercial or non-commercial third parties (e.g. app developers, aftermarket)	Vehicle manufacturer, partner(s) on vehicle manufacturer's behalf (e.g. dealers, subsidiaries)	Vehicle manufacturer, supplier(s), partner(s) on vehicle manufacturer's behalf	Only parties authorised to process data by law, contract and consent (e.g. insurers, app developers)
IP relevance	None	None	Vehicle manufacturer	Vehicle manufacturer and its supplier(s)	Some accruing to vehicle manufacturer but mostly none
Anonymity	Anonymised	Anonymised	Anonymised	Anonymised	User identified
Personal data protection relevance	None	None	None	None	Medium to high
Data provision	There must be no discrimination with regard to pricing, amount and type of data made available, timeliness of data transfer and other relevant quality criteria				
Data-sharing agreement	Individual reciprocal agreements with vehicle manufacturers	Individual agreements with customers and third-party market participants			

- **Type 3: Personal data**
  Data that supports services requiring user or vehicle identification, or the use of personal data including but not limited to the VIN. Such data may have partial IP significance to vehicle manufacturers, but more importantly its handling must meet strict data and privacy protection requirements.

  Examples include vehicle location, movement profile, average speed, acceleration, fuel and consumption levels, where these are combined with the VIN or some personal identifiers. Other personalised data include navigation destinations, the user's address book, personalised access to third-party services, infotainment settings, personalised in-car settings (e.g. seat, cockpit, interior ambience) and the user's health and wellbeing data (e.g. heart rate sensors embedded in the seatbelt). Right of access to personal data, taking into account the customer's privacy rights, is granted only to parties authorised to process data by law, contract and customer consent.

By implication, Type 1 and Type 2 data can easily become Type 3, i.e. personal, data the moment it is tied to a personal identifier, such as but not limited to the VIN. This is in line with the European Commission's recently published strategy on Cooperative ITS (C-ITS), which states that data broadcast by C-ITS from vehicles will, in principle, qualify as personal data as it will relate to an identified or identifiable natural person.[7] In practice, however, public or local traffic management authorities are not interested in identifying the individual but are more keen to understand traffic patterns and potential disruption by analysing large anonymised datasets (i.e. Type 1A). On the other hand, it may be relevant for vehicle manufacturers to identify the registered keeper of the vehicle whose fuel pump is showing signs of a fault or an imminent breakdown (i.e. Type 2B) so as to alert the registered keeper to take the necessary action, in which case existing data protection regulations apply.

Another type of data that is relevant to autonomous driving, but falls outside the framework set out in Table 2, is pre- and post-crash data. This type of data is of interest to various parties, particularly vehicle manufacturers, insurers, accident investigation authorities and potentially even the courts of law. It is stored in a Data Storage System for Automatically Commanded Steering Function (DSSA), which acts as an event data recorder for automated driving at SAE Level 3 and above. The information logged will include the operating mode of the vehicle. The DSSA must be regulated internationally at the United Nations Economic Commission for Europe (UNECE) to avoid a patchwork of national legislations. Discussion on this can be found in section 5.2.

The DSSA also logs limited data, for a limited period of time, even when there is no critical event (e.g. a crash) when automated driving mode is engaged. Such data may be useful evidence to prove who is in control of the vehicle in the event of traffic violations.

2.2 Protection of personal data

Effective data protection is essential if consumers are to have confidence in connected vehicles. The foundation for the responsible handling of personal data is upholding transparency and self-determination for the customer. SMMT members throughout the entire automotive value chain already provide high levels of data protection in full compliance with existing data protection and privacy laws

[7] European Commission (2016), "A European strategy on Cooperative Intelligent Transport Systems, a milestone towards, cooperative, connected and automated mobility", COM(2016) 766 final, released on 30 November.

and regulations. Customers are also provided with options regarding the processing and use of their personal data.

Data transfer to vehicle manufacturers, services providers, or other third parties, occurs only in limited and specifically defined cases, exclusively for the fulfilment of services used by the customer. This is strictly predicated on customer consent. No personal data is transferred to third parties without the consent of the customer, who retains the right to activate or deactivate services and transmission of data. Where consent has been given, data is processed accordingly to purposes, in a proportionate manner and not retained for longer than necessary. Moreover, customers will be able to deactivate their connected services, or part thereof, except where data must be processed to comply with legal, statutory or contractual requirements (e.g. eCall, with fleet operators).

Many vehicle manufacturers are signatories to the following *ACEA Principles of Data Protection in Relation to Connected Vehicles and Services*:

- *We are transparent* principle: Manufacturers commit to informing customers in a clear, meaningful and easily accessible manner the personal data, or categories of personal data, that is processed; the purposes for which the data is used; the third party, or categories of third parties, with whom the data may be shared; and the identity of the company or group of companies that governs the data processing. Customers will likewise be informed of any changes to manufacturers' privacy policies.

- *We give customers choice* principle: Manufacturers commit to giving customers the choice, where possible, of whether to share personal data; obtaining customer consent for sharing the data with third parties; and allowing customers to de-activate the geolocation functionality of the vehicle. The only exception to the latter is where geolocation data is needed for compliance with contractual or legal obligations, for example eCall.

- *We always take data protection into account* principle: Manufacturers commit to maintaining high levels of data protection when designing and developing new products, services and processes, including, if necessary, carrying out data protection impact assessments. This is in compliance with the EU General Data Protection Regulation principle of "privacy by design".

- *We maintain data security* principle: Manufacturers commit to implementing appropriate technical and organisational measures to protect customers' data against accidental or unlawful destruction, loss, alteration or disclosure.

- *We process personal data in a proportionate manner* principle: Manufacturers commit to processing only personal data that are relevant and retaining the data for only as long as it is necessary to fulfil the purposes for which it is collected. Manufacturers also anonymise and de-identify personal data where appropriate, as these are considered important mechanisms for protecting personal data.

The provision of connected services is sometimes delivered in partnership with companies from adjacent industries. Customers are informed of the identity of any third party service providers and, where appropriate, contracting partners. Where these services are provided, they are the responsibility of the provider and are subject to the provider's terms and conditions of use; vehicle manufacturers cannot be held responsible for these services offered in the vehicle. Customers should be able to decide the extent to which they wish to use the services of third parties. Where data processing is outsourced, contractual safeguards are put in place to protect personal data. Where vehicle manufacturers do not control personal data processed by unaffiliated third parties that provide applications or services through the communication interfaces in the vehicle, these providers are encouraged to apply the same principles.

However, vehicle manufacturers cannot be held responsible where there is a breach of privacy or loss of personal data as a result of deficiencies in non-manufacturer approved third party tethered or retrofitted devices in vehicles (e.g. dongles).

2.3 Data handling relationships and obligations in the context of fleets

In line with the *ACEA Principles of Data Protection in Relation to Connected Vehicles and Services* above, vehicle user data, i.e. personal data, is only ever used or shared with the express and prior consent of the vehicle user, not the registered keeper, otherwise known as the vehicle owner in the context of fleet operators. This is *unless* vehicle manufacturers have entered into a specific legal agreement with each of the registered keepers and/or have a contractual obligation to do so.

A connected vehicle could be used by numerous individuals while belonging to a single registered keeper. Although consent underpins the handling of all personal data, there is a risk that poorly considered consent procedures, for example requiring every driver to consent to data collection every time a connected vehicle is used, will be onerous and ultimately an annoyance that discourages people from using connected vehicles.

The primary user of a connected vehicle, i.e. the individual registering for the connected vehicle services and agreeing to the terms and conditions associated with these, must therefore be put at the heart of any data consent process. This means that consent is given only once by the primary user, at the time of registering for using connected services, and any data collection and/or handling when the vehicle is used by other users, falls under the terms the primary user signed with the manufacturer, *except* in cases where the manufacturer has entered into a specific legal agreement with the registered keeper who is not the primary user. Another exception is where more advanced on-board systems in certain vehicles allow for the setting and identification of multiple personal profiles, thereby allowing each user to activate his or her own profile – thus effectively becoming a primary user – when using the vehicle.

In the case of rental or company fleets, the onus is on either the primary user or the registered keeper, depending on their contractual agreement, to perform or request for a factory reset of personalised connected services before the vehicle is passed on to a new primary user. Unless an express request is made, the vehicle manufacturer should not be reasonably expected to know if there is a change of primary user.

Vehicle manufacturers do not by default have an obligation to provide vehicle data to registered keepers, *unless* they have entered into a specific legal agreement or are bound by contractual obligation to do so. Vehicle data refers to those that fall within Type 1B and Type 2 in Table 2.

2.4 Access to vehicle generated data

The secure exchange of vehicle generated data is fundamental for value creation within automotive and adjacent industries. However, the connected vehicle is not a “smartphone on wheels” – the vehicle requires much higher standards in security, safety and privacy. Protecting the integrity, confidentiality and availability of vehicle functionalities, electronic control units (ECUs) and data against cyber attacks and system manipulation is paramount to guaranteeing predictable vehicle behaviour and avoiding safety risks that may result in road casualties and severe traffic disruption.

On the one hand, unrestricted direct access to vehicle generated data via an open in-vehicle interface runs the risk of compromising security, safety and privacy, as it provides an open door to unauthorised access to the vehicle's security electronics from external sources. Every new external data interface increases the potential attack surface and entry points. This could also lead to secondary risks via networking, for example enabling vehicle theft by remote door unlocking and creating opportunities for fraud through mileage manipulation. Additional safety risks in the form of driver distraction could arise if third parties are granted unfettered access to the vehicle's on-board systems, such that user interfaces and function displays may be altered without adequate human-machine interface design considerations.

Furthermore, the integrity of vehicle systems cannot be guaranteed by vehicle manufacturers when vehicles are compromised as a result of the use of applications, services or devices (e.g. dongles) developed by third parties to directly access vehicle generated data via an open in-vehicle interface. It is neither feasible nor reasonable for vehicle manufacturers to test, validate and approve all third party applications, devices and services available on the market.

On the other hand, overly restrictive access to vehicle generated data may stifle innovation and fair competition and hinder value creation. Access to vehicle generated data must therefore be guaranteed to be fully non-discriminatory with regard to pricing, amount and type of data made available, timeliness of data transfer and other relevant quality criteria agreed by contracting parties. It must allow for consumer choice, innovation and fair competition without the abuse of market power and the establishment of digital market monopolies.

In view of these considerations, SMMT believes that access to vehicle generated data must uphold the principles of security, safety and privacy without stifling innovation and fair competition. SMMT also supports the guiding principles on granting access to in-vehicle data and resources set out in the *European Commission C-ITS Platform Project final report*:

- *Consent as data provision condition*: The data subject (owner of the vehicle and/or through the use of the vehicle or nomadic devices) decides if data can be provided and to whom, including the concrete purpose for the use of the data (and hence for the identified service). There is always an opt-out option for end customers and data subjects. This is without prejudice to requirements of regulatory applications.

- *Fair and undistorted competition*: Subject to prior consent of the data subject, all service providers should be in an equal, fair, reasonable and non-discriminatory position to offer services to the data subject.

- *Data privacy and data protection*: There is a need for the data subject to have its vehicle and movement data protected for privacy reasons, and in the case of companies, for competition and/or security reasons.

- *Tamperproof access and liability*: Services making use of in-vehicle data and resources should not endanger the proper safe and secure functioning of the vehicles. In addition, the access to vehicle data and resources shall not impact the liability of vehicle manufacturers regarding the use of the vehicle.

- *Data economy*: With the caveat that data protection provisions or specific technology prescriptions are respected, standardised access favours interoperability between different applications, notably regulatory key applications, and facilitates the common use of same vehicle data and resources.

At the European level, the European Automobile Manufacturers' Association (ACEA) and the European Association of Automotive Suppliers (CLEPA) have joined forces to find a solution for secure and safe access to vehicle generated data by third parties.[8] With vehicle manufacturers' express promise to be willing to share relevant vehicle data with third parties, ACEA and CLEPA have proposed a way forward whereby vehicle generated data will be relayed to a back-end server maintained by the manufacturer. The data could then be directly transferred from the manufacturer's secure back-end interface to third parties for the provision of services. Alternatively, any market participant may also set up a neutral server to gather data from one or more manufacturers' back-end servers to be provided to third parties. Manufacturers, however, will not be responsible for operating or financing the neutral server. This proposed architecture, also known as the Extended Vehicle (ExVe), is based on ISO 2007x standards. Liability therefore resides with vehicle manufacturers, who are responsible for the safe and secure transmission of vehicle generated data.

The Coalition for Interoperable Data Access, which includes the International Federation of Automotive Aftermarket Distributors (FIGIEFA), believes it is in the interest of fair competition and innovation that consumers and independent operators have the possibility to select the provider of their choice for added value and repair and maintenance services.[9] Recognising the need to allow for consumer choice at the point of pre-repair and in installing or using alternative, i.e. third party, apps is deemed fundamental to fair competition. For that matter, FIGIEFA and the independent aftermarket call for an interoperable, standardised and secure in-vehicle Open Telematics Platform (OTP), from which all relevant vehicle generated data should be accessible to third parties. This proposal is based in part on the European Commission's EUR 5/6 regulation that seeks to ensure independent operators have direct access to in-vehicle data, free of charge, in an unmonitored and non-discriminatory way via the on-board diagnostics.

Discussions and initiatives to find a common solution are underway at the European level. At the time of writing, ACEA and CLEPA seek to develop a proof-of-concept for their proposal through several key use cases and to better define the concept and attributes of a neutral server that gathers data from the vehicle manufacturer's back-end server. Given security is a key concern in the debate, FIGIEFA meanwhile seeks to appoint experts to assess the security attributes of both the ExVe and the OTP.

[8] See press release accessible at http://www.acea.be/press-releases/article/automotive-industry-joins-forces-on-access-to-vehicle-data. See also ACEA (2016), Position Paper: Access to vehicle data for third-party services.
[9] See press release accessible at http://www.leaseurope.org/uploads/documents/press-releases/pr161212-Coalition%20for%20Interoperable%20Data%20Access.pdf.

3. VEHICLE CYBER SECURITY

The increasing connectivity of digital devices including vehicles presents new challenges in relation to cyber security. Failure to ensure the security of a growing network of CAVs may not only undermine public confidence in the technology but could also present genuine risks to public safety.

SMMT members implement appropriate technical and organisational measures for protecting the integrity of the vehicle and its systems. High levels of technical safety, including suitable cryptography, layering, separation and identity authentication, are continuously refined for the software, firmware and hardware architectures of the vehicle as well as remote access to the vehicle via telecommunications networks. It is in the best interest of not only automotive but also adjacent sectors to ensure that robust standards, processes and systems are put in place that will guarantee the highest possible level of cyber security.

Notwithstanding current and future technical solutions, common guidelines at the processes level during the design and development of vehicle systems are necessary as part of the security-by-design principle. While the *ISO 26262 Functional Safety Standard for Electrical and Electronic Systems* serves a specific purpose, a set of basic principles for protection against unauthorised access to vehicle systems is needed. Existing examples include the *SAE J3061 Cyber Security Guidebook for Cyber-Physical Vehicle Systems* and the *AAM-AGA's Framework for Automotive Cyber Security Best Practices*.

SMMT considers guidelines to be the most appropriate measure at this stage, given the pace of development in this area. These guidelines should however be outcome- rather than output-based. Manufacturers should be allowed the freedom to implement additional proprietary technical security solutions in addition to adhering to these process guidelines. In the light of this, SMMT supports the development of a set of guidelines for ensuring vehicle cyber security currently being developed under the auspices of the WP.29 at the UNECE. Specifically,

- The protection of CAVs requires verifiable security measures based on existing security standards (e.g. ISO 27000 series, ISO 15408, ISO 29101);
- CAVs must be equipped with integrity protection measures (e.g. security software updates);
- Vehicle manufacturers and their suppliers must have appropriate measures in place to manage used cryptographic keys;
- The integrity of internal communications between controllers within CAVs must be protected (e.g. by authentication); and
- Online services for remote access into CAVs must have strong mutual authentication and secure communication between involved entities.

These guidelines should be expanded to include high-level principles on board-level governance, the supply chain, product aftercare and incident response, personnel, procurement, and data storage and transmission.

SMMT actively encourages the entire UK automotive industry to view cyber security as a pre-competitive issue and therefore participate in the Automotive Information Exchange run by the MI5's Centre for the Protection of National Infrastructure and in the Cyber-Security Information Sharing Partnership online platform that is now part of the National Cyber Security Centre. Both initiatives allow the industry and government to share intelligence on cyber threats and vulnerabilities in a secure and dynamic environment while operating within a framework that protects the confidentiality of shared information and the informant.

Although vehicle cyber security is an important issue in its own right, CAVs ultimately are but one component of a future interconnected national intelligent mobility network, which, when considered in the light of its scale and implications, is effectively part of critical national infrastructure. The attack surface and “back doors” will inevitably increase the more joined up our national multi-modal mobility services are. Government support and investment therefore must not only focus on the security of vehicles but also on the cyber resilience of the entire connected mobility network. Security-by-design must extend to much wider than just automotive.

4. CONNECTIVITY AND INFRASTRUCTURE

4.1 Digital infrastructure: ubiquitous connectivity as a priority

Communication involving connected vehicles can be divided into three main types based on the nature of the information exchanged: tactical (ad-hoc), strategic and infotainment.

- *Tactical, or ad-hoc*, communication is typically short range, mainly involves vehicle-to-vehicle (V2V) although in some cases also vehicle-to-infrastructure (V2I), and is exchanged for only a short period of time. An example of this is when a vehicle "informs" another that it is about to pull out of a blind junction. Safety is a key concern of tactical communication.

- *Strategic* communication is typically longer range, mainly involves vehicle-to-cloud (V2C) although in some cases also V2I, and is exchanged ahead of time to transmit useful information to the driver. An example of this is when traffic management authorities transmit messages regarding an incident (hence disruption or congestion) or an icy stretch of the road five or ten miles ahead. Journey planning, or alteration, is the usual concern of strategic communication.

- *Infotainment* examples include WiFi hotspot, weather information and music streaming. Convenience and comfort are among the key value propositions of infotainment.

Currently many vehicles are already connected to a range of convenience and infotainment services, while eCall, which introduces a safety element into vehicle connectivity, will be mandatory in all new cars type approved within the EU from April 2018. Although an autonomous vehicle, aided by its own sensing capabilities, high-precision maps and artificial intelligence, should be self-sufficient and able to function without connectivity, its sensors are limited to line-of-sight data collection. Sensor fusion with connectivity, i.e. vehicle-to-everything (V2X), can complement those capabilities and provide 360-degree non-line-of-sight awareness, thus extending the vehicle's ability to "see and hear" further down the road, at blind junctions, or in extreme weather conditions.

For example, the complementarity of connectivity, or indeed the redundancy that it provides, may be useful in situations where extreme weather conditions render the camera unusable, while for some reasons the radar and Lidar simultaneously fail. In such cases, an autonomous vehicle may still be able to make some safety-critical tactical decisions with the aid of V2V and V2I data.

Regardless of the type of communication, improving the UK's digital infrastructure in general is an essential prerequisite for the uptake of connected vehicles. Four key challenges related to connectivity will shape the speed and breadth of connected vehicles deployment in the UK: **coverage, reliability, bandwidth and capacity**. Ubiquitous coverage is the automotive industry's top priority, regardless of the choice of technology, which in the current context is mainly a tussle between cellular and ITS-G5 (also known as 802.11p, WAVE or DSRC). The former technology readily enables longer-range communication (strategic and infotainment), but R&D and field tests are now being carried out to establish its suitability for short-range communication (tactical/ad-hoc) as well. The latter is exclusively for short-range communication.

Many connected vehicle services available today, including certain geolocation services, navigation, WiFi hotspot, eCall, bCall and telematics, can be deployed with existing 3G and LTE 4G (or LTE-V) cellular spectrum. However, cellular coverage tends to be concentrated in highly populated areas for obvious commercial reasons. Patchy and inadequate coverage in extra-urban environment and unreliable signal strength will hold the UK back as a market for deployment of connected vehicles. Some vehicle manufacturers have already stated in public that the UK is not among their top three markets of choice when launching new connected vehicle functionalities owing to poor coverage.

Currently almost 4,600 miles (2%) of UK roads have no 2G coverage from any network provider, whereas only 43,000 miles (18%) and 119,000 miles (48%) have full 4G and 3G coverage respectively (Table 3). The National Infrastructure Commission's (NIC) recent report reveals that, even just in terms of voice coverage (2G), some 17% of A and B roads are in complete not-spots and an additional 42% have only partial coverage.[10]

Table 3: Mobile network coverage on the UK road network.

	Miles (%) of road in Britain with…		
	Full network coverage	Partial network coverage	No network coverage
2G	211,753 (86%)	28,975 (12%)	4,561 (2%)
3G	119,057 (48%)	111,679 (45%)	14,554 (6%)
4G	43,070 (18%)	65,950 (27%)	136,271 (56%)

Note: percentages might not add up to 100% because of rounding. Partial network coverage means that at least one of the four network providers – Vodafone, O2, EE, Three – will offer a signal.

Source: RAC Foundation analysis using Ofcom data, 2015.

The NIC report recommends that our motorways must have roadside networks fit for the future and that such infrastructure should be in place by 2025 based primarily on the fact that motorways, although comprising just over 1% of the total length of the entire UK road network, carry 21% of all vehicle traffic. This is unlikely to be good enough for the UK to realise its ambition to become a leading market for the deployment of connected vehicles. The simple fact that there is still a sizeable 79% of vehicle traffic on the remainder of the UK road network is a credible enough argument for better coverage beyond just motorways. Furthermore, while large sections of the motorways benefit from Highways England's optical fibre network that enables ITS-G5, the rest of the UK road network relies heavily on cellular coverage. Ubiquitous cellular coverage is essential for fully realising the safety-related benefits of connected vehicles, for example eCall.

If the UK is to be the leading market for deployment of connected vehicles and V2X services in the first instance and CAVs thereafter, the Government must devise a strategy to ensure signal coverage, irrespective of the choice of technology, does not become a key stumbling block. As a first step, the Government's Centre for Connected and Autonomous Vehicles (C-CAV) should consider drawing up a plan in conjunction with the Department for Culture, Media and Sports (DCMS) to put in place the digital infrastructure needed to support connected vehicles by ensuring there is ubiquitous connectivity across the entire UK road network.

[10] National Infrastructure Commission (2016), Connected Future.

Secondly, the Government should consider, as part of its forthcoming 5G Strategy, mandating mobile network operators to extend coverage to less densely populated areas and specifically the entire UK road network as a condition for 5G licences auction. Otherwise, if roll-out is completely market-led, mobile network operators are likely to commission infrastructure in densely populated urban areas to maximise the potential for commercial returns. This will still leave large sections of the UK road network with limited or no 5G coverage, as is the current situation with 3G and 4G. The deployment of new masts, or other infrastructure to provide ubiquitous coverage on the UK road network, should therefore be coordinated to ensure optimisation of location (e.g. serving both automotive and rail) and private investment. Alternatively, the Government may wish to study the feasibility of and consider introducing in-country roaming across mobile networks.

Thirdly, there ought to be network neutrality, in that data transmission for safety-critical services must be prioritised ahead of other services, with each category ascribed a defined quality of service.

4.2 Strategic plan for 5G roll-out

The DCMS's Future Communications Challenge Group, of which SMMT is a member, has identified 5G to be an area where the UK is in pole position to exploit for global deployment leadership and economic advantage. The automotive industry welcomes the potential that 5G can deliver for high-bandwidth (1000x greater than LTE per unit area) and low latency (<1ms end-to-end) services, particularly in-vehicle content streaming. However, technology investment is costly and the automotive industry wants to ensure that it does not incur huge sunk costs in technology that is either redundant or not fit for purpose several years after deployment. Vehicle manufacturers need to plan for the changes required of vehicle technology, systems and architecture way ahead of anticipated 5G roll-out in 2020.[11]

The Government's 5G Strategy should therefore provide some clarity on the UK 5G roadmap, deployment strategy and roll-out phases across industry verticals. Such clarity is important to vehicle manufacturers in making investment and CAV deployment decisions. This is particularly important as a continuing lack of clarity regarding the roll-out of 5G may result in some within the automotive industry viewing ITS-G5 as an alternative technology. The CAR2CAR Communication Consortium favours the adoption of ITS-G5 for V2V and V2I communication. Deployment of ITS-G5 infrastructure, which uses the 5.9 GHz frequency band, has already started in several cities and between cities in Europe. For example, the European C-ITS corridor project has created smart infrastructure using ITS-G5 from Rotterdam to Vienna. The technology is also being used for trials in several projects in the UK, including the A2/M2 London-Dover Connected Corridor and UK CITE in the Midlands.

The automotive and telecoms industries, meanwhile, are also exploring V2X communication using cellular. The recently established Connected Vehicle to Everything of Tomorrow (ConVeX) consortium, for example, will carry out the first announced Cellular-V2X (C-V2X) trial based on the 3GPP Release 14. Some vehicle manufacturers have already decided on a future solely with cellular, while an increasing number of other manufacturers too are now seriously considering if cellular could in the longer term be the most cost-effective option that facilitates both long- and short-range communication. The progress of the ConVeX consortium, as well as the 5G Automotive Association, is therefore of great interest and importance to the automotive industry.

[11] Romano, G. (2016), 3GPP RAN Progress on 5G, accessible at http://www.3gpp.org/ftp/Information/presentations/presentations_2016/3GPP%20RAN%20Progress%20on%205G%20-%20NetFutures.pdf.

However, the automotive industry takes the view that ITS-G5 and C-V2X cannot coexist on the same frequency channel due to differences between the wireless systems, and therefore supports investigations into using C-V2X (on LTE in the first instance and thereafter 5G new radio) at a carrier frequency between 3.4-3.8 GHz. The 3.4-3.8 GHz band is a good compromise between high and low carrier frequencies with regard to propagation characteristics and antenna size. Coexistence on 5.9 GHz implies the band needs to be divided between the two technologies, resulting in neither technology being able to carry all traffic safety applications as the divided frequency band will not be sufficient for either technology. As explained above, connectivity complements autonomous driving, not least in providing redundancy for safety-critical functions. If ITS-G5 and C-V2X would both operate at 5.9 GHz, the redundancy would diminish because signals from the two systems would undergo the same channel impairments, i.e. they will most likely fail at the same time. Separating the two technologies on different carrier frequencies adds true redundancy and the overall system is likely to be more robust against jamming.

So as to ensure that a technology neutral approach is taken to finding the optimum and most cost-effective way of connecting the UK's road network while keeping an eye on the developments in the aforementioned consortia, the Government should ensure that connected vehicle trials and connected corridor projects must not only actively experiment with ITS-G5 using the 5.9 GHz band, but also include LTE and 5G using the 3.4-3.8 GHz band. The UK will not be playing to its full strengths if we fail to make use of Europe's first and largest 5G R&D facility at the 5G Innovation Centre, University of Surrey.

Ultimately, however, European-wide harmonisation and commonality in terms of communications technology is desirable. This ensures interoperability across markets and avoids the escalation of costs as a consequence of deploying multiple alternative technologies.

Given that 5G is expected to enable the Internet of Things in the broadest sense, the most meaningful innovations can only be spawned and new economic value created if a number of industry verticals – for example, automotive, telecoms, retail, financial services, consumer electronics and energy – are brought together from the outset with the aid of government funding to co-create and trial new connected services. SMMT welcomes the Government's recent Autumn Statement announcement of £740 million through the National Productivity Investment Fund targeted at supporting the market to roll out full-fibre connections and future 5G communications, including supporting 5G trials.

The Government must now go further by using its convening power to set up, or support the setting up of, a national initiative to coordinate 5G trial and demonstration projects involving multiple industry verticals including automotive. The initiative must have the power and ability to look for solutions within the government machinery to overcome any potential stumbling blocks, such as data protection, cyber security and IP rights. The automotive industry will benefit from understanding the type of connected services that can be realistically, safely and profitably deployed in conjunction with other industry verticals.

4.3 Physical infrastructure

Developing and maintaining high-quality physical infrastructure is as critical as installing the necessary digital infrastructure to enable the deployment of CAVs. While there may be the possibility of doing away with signage and gantries on the road network in the longer term when dynamic information such as speed limits and temporal restricted access can be transmitted directly to connected vehicles' on-board system (V2I), this is predicated on ubiquitous connectivity on UK roads and a significant majority of, if not the entire, motorparc being connected vehicles. Given the current renewal rate of the UK motorparc, i.e. 12-15 years, this is unlikely to happen in the near-to-medium term. In the interim, proper maintenance of existing informational infrastructure is essential for a mixed-fleet environment.

However, what is more important is that the Government ensures our national road infrastructure is maintained to a high quality to enable the deployment of SAE Level 3 driver assistance systems and Levels 4 and 5 autonomous driving. Technology at these levels relies considerably on cameras, working in tandem with radar, Lidar and other sensors. Clear road markings are therefore a priority on not just the Strategic Road Network, which falls within Highways England’s remit, but also the wider road network, which is the responsibility of local authorities.

5. REGULATORY LANDSCAPE

5.1 General approach to regulation

To date the Government has taken a generally “light-touch” approach to regulation in relation to autonomous vehicle testing. For example, the publication of *The Pathway to Driverless Cars: A Code of Practice for Testing* in July 2015 has paved the way for testing to be carried out legally anywhere in the UK as long as it abides by the Code of Practice. This has been welcomed by the automotive industry and helped position the UK as a leading location for the development and testing of autonomous vehicles.

In the summer of 2016 the Government launched a rolling programme of regulatory reform aimed at preparing the UK market for deployment of advanced driver assistance systems and autonomous driving technologies. Vehicles with SAE Level 2 capabilities are already available, whereas Level 3 capable vehicles will arrive on the market in 2017. Although the environment for the *testing* of autonomous driving technologies is favourable in the UK, it is paramount that the Government ensures the UK is well placed to become a leading market for the safe *deployment* of vehicles equipped with Level 3 and above technologies.

SMMT therefore agrees with the concept and rationale of a rolling programme of regulatory reform. A fit-for-purpose and up-to-date regulatory framework serves as guidance for the automotive industry and sets reasonable expectations for the public and other stakeholders who will use, or may be affected by the use of advanced driver assistance systems and autonomous driving technologies. With rapid technological progress – not least in computing power, processor speed and artificial intelligence – regular adjustments to the regulatory framework will help ensure that the law remains fit for purpose while not curtailing the flexibility vehicle manufacturers need in developing technology. It is also hard to accurately anticipate how the public will respond to new technologies. Step-by-step adjustments to the regulatory framework which draw upon an accurate understanding of public acceptance and use of new technologies will help ensure that regulation remains relevant and effective.

However, the Government must exercise prudence and care in reforming regulation. In particular, SMMT wishes to stress that:

- New regulation must only be introduced where it is absolutely necessary, where existing regulations do not adequately cover the deployment and use of new technologies and functionalities, and where industry mechanisms and market forces are not capable of providing effective solutions.

- Changes to the regulatory framework must support and encourage the development of CAV technologies and the aspirations of both the consumer base and vehicle manufacturers; they must achieve the intended outcomes rather than precipitate unintended adverse market consequences. This is important for ensuring the UK market for vehicle sales and the conditions for the development of automotive technology remain world-leading and innovative.

- In assessing when these periodic reviews should take place and what near-to-market technologies they should cover at each review, the Government must work closely with SMMT and the automotive industry to ensure that the regulatory framework keeps pace with the rapid development of advanced vehicle technology, the effectiveness of each wave of regulatory reform is assessed and the most appropriate technologies are being reviewed. The pace of regulatory reform needs to be more rapid to react to technology roll-out. Changes to the Highway Code must be expedited to realise the potential of these technologies and to allow people to complete other tasks in the vehicle when SAE Level 3 or above is engaged.

- The Government must ensure that, when undertaking any regulatory reform, its approach is technology neutral. It must ensure that any changes do not unintentionally prejudice or promote particular technologies or the approach taken by particular manufacturers. For example, while minimum safety, security and performance requirements may be mandated, they must allow for different implementation routes and should not restrict vehicle manufacturers' individual deployment strategy. Continuing to work closely with SMMT and vehicle manufacturers will help mitigate this risk.

5.2 Harmonisation and interoperability

Harmonised international and European regulatory frameworks are necessary for legal certainty with regard to deployment and cross-border interoperability, while also providing manufacturers with the confidence that they need in order to invest. SMMT supports the joint strategy set out in the Amsterdam Declaration of April 2016, which emphasises the importance of coherent international, European and national regulatory frameworks. In view of the decision of the UK to leave the European Union, the Government must ensure that regulatory divergence does not develop and that consistency with EU regulation and standards is maintained. This is essential if the UK is to be vehicle manufacturers' location of choice for the development, testing and deployment of CAVs.

At the international level, the adaptation of relevant UN regulations to satisfy the requirements and enable the deployment of automated functions and autonomous driving must also be expedited. The clearest current example is the UN Regulation 79 on Steering Equipment, where the existing speed limit of 10 kmph for automatically commanded steering function (ACSF) for lateral manoeuvres should be repealed. The Government must also work collaboratively with international bodies and seek to set the pace of international regulatory reforms so as to ensure that they align with the UK's timetable for regulatory reviews and keep pace with UK reforms. Some SMMT vehicle manufacturer members have voiced dissatisfaction with the current pace of progress within the UNECE's Informal Working Group on ACSF.

An international regulatory framework is also required for the introduction and deployment of a Data Storage System for ACSF (DSSA), which acts as an event data recorder for automated driving, as a necessary supporting technology in all vehicles with SAE Level 3 and above capability. The device, while fully complying with data protection laws, is crucial for reconstructing the immediate events leading up to an accident involving vehicles with SAE Level 3 and above capability, thus assisting manufacturers, the authorities and insurers in determining the responsible and liable party, or parties. The information logged will include the operating mode of the vehicle. With protection of innocent victims of an accident and compliance with traffic regulations at its heart, we believe this will be a step in the right direction in building public acceptance of autonomous systems. The DSSA also logs limited data, for a limited period of time, even when there is no critical event (e.g. a crash) when automated driving mode is engaged. Such data may be useful evidence to prove who is in control of the vehicle in the event of traffic violations. SMMT believes the DSSA must be regulated at the UNECE level in order to achieve international harmonisation, as well as to avoid a patchwork of national legislations that will only serve to hamper the deployment of autonomous vehicles.

5.3 Insurance and liability

In the summer of 2016 the Government also proposed to extend compulsory motor insurance “to include product liability” for SAE Level 4 and 5 autonomous vehicles, when the driver “out of the loop”.[12] Following a public consultation, the Government has now amended its proposal such that **compulsory motor vehicle insurance will be extended to create a single insurer model to protect victims where the autonomous vehicle causes a crash in automated mode**. The victim will have a direct right against the motor insurer and the insurer in turn will have a right of recovery against the responsible party **to the extent there is a liability under existing laws, including under product liability laws**. The Government also takes the view that it is not a proportionate response at this stage to make any changes to product liability law to facilitate the arrival of what will initially be a small number of autonomous vehicles in proportion to the entire UK motorparc.[13]

The main reasons for the Government’s proposal are to assure the public that appropriate motor insurance cover is available for autonomous vehicles and that an appropriate insurance legal framework is in place by the time these vehicles enter the UK market, thereby encouraging the uptake of these vehicles.

SMMT is in **conditional agreement** with the Government’s proposal. Giving consumers the peace of mind and confidence to purchase these vehicles when they become available is critical to the growth of the market for this new technology. However, the support for this proposal is predicated on four important conditions:

- The proposal and its implementation **must not effectively pre-empt, or give the impression of pre-empting, the determination of fault**. It must not be assumed that any crash involving an autonomous vehicle operating in automated mode is necessarily the fault of the vehicle’s system, i.e. system malfunction or product defect.

- The proposal and its implementation **must not result in unintentionally hampering consumer uptake of these vehicles through actual or perceived higher insurance premiums or the misconception that these vehicles are unsafe**. With the promise of significantly enhanced safety resulting from the introduction of more autonomous technology in vehicles, the public rightly expect, ceteris paribus, insurance premiums to fall in response to a clear reduction in risks. However, if the public believe that these savings will be lost or substantially reduced as a result of extension of cover the motivation to adopt this new technology may be dented. Similarly, public adoption of new technologies is sensitive to the signals and messages consumers decode from government policy. There is a risk the very need for this new proposal itself, rather than vehicle manufacturers’ product liability, conveys to the public as though the industry itself is not fully confident of the safety of autonomous vehicles.

- **A DSSA, which acts as an event data recorder for automated driving, must be made compulsory for all autonomous vehicles through international regulation**. It will be more challenging for parties involved in an autonomous vehicle collision to prove who is at fault as compared with collisions involving only conventional vehicles. Data collected in a DSSA will be

[12] Centre for Connected and Autonomous Vehicles (2016), Pathway to Driverless Cars: Proposals to support advanced driver assistance systems and automated vehicle technologies.
[13] Centre for Connected and Autonomous Vehicles (2016), Pathway to Driverless Cars: Consultation on proposals to support advanced driver assistance systems and automated vehicles – Government response.

crucial for objectively determining liability. Data handling, processing and sharing activities will need to be reviewed, especially if they pertain to personal data, in order to align with data protection and/or privacy compliance requirements. For instance, UNECE regulation will need to address access to DSSA data and the purposes for which it can be processed.

- There must still be **sufficient flexibility in the market for different motor insurance models** for autonomous vehicles to be offered. For example, vehicle manufacturers should be free to offer to take full liability should an accident occur while a vehicle is in fully autonomous mode, i.e. the driver, or user, is completely “out of the loop”. While the industry understands this is a possible offering within the overall context of compulsory motor insurance that covers product liability, there is concern the public, already inundated with new concepts and multiple offerings, may not necessarily share the same understanding from the outset.

Insofar as limits to liability are concerned, two additional points must be considered:

- Where the registered keeper or primary user attempts to circumvent, or fails to properly and reasonably maintain, the autonomous vehicle technology, the registered keeper or primary user whose “contributory negligence” results in an accident will have to accept responsibility and liability. The registered keeper or primary user, however, has to be clearly instructed on the intended use of the technology and the consequences of bypassing, tampering with, neglecting or failing to reasonably maintain the technology. The Government should carefully define what amounts to reasonably maintaining such technology and ensuring it is in safe working condition. For example, this calls into question whether failure to enable a software update when prompted to do so the first time amounts to contributory negligence. The lack of clarity on the expected behaviours or responsibilities on the part of the registered keeper or primary user may discourage the ownership of autonomous vehicles.

- The state-of-the-art defence principle should apply in determining limits to liability, as at the time the product was in the manufacturer's control the state of scientific and technical knowledge is such that the manufacturer could not have been expected to discover a defect. This principle, which to an extent provides legal clarity and reliability, is widely adopted in other industries, has proven to work well in the past and is a major anchor of product liability. The industry’s concern, however, revolves around how software updates will be handled under a state-of-the-art regime. While vehicle manufacturers have to meet state-of-the-art criteria for the whole vehicle when introducing it to the market, software developments are constantly and fast evolving. What is deemed state-of-the-art for software today may no longer be state-of-the-art tomorrow, particularly with the potentially infinite number of unknown unknowns in the future. State-of-the-art itself therefore becomes a moving target as software updates become more frequent.

5.4 Review of specific regulations

SMMT believes that the text of the Highway Code should be amended to account for vehicle automation capability. For instance, updating Rule 150 (related to use of driver assistance systems and distraction) to better explain motorway assistant and remote control parking technologies, both of which involve the driver “in the loop”, and how they are used appropriately is warranted. The text in Rule 160 (related to driving with both hands on the wheel) needs to be amended to accommodate remote control parking and remote control drive, where it must be made clear the driver is still in control, although control is exercised not via the steering wheel but by using a hand-held, or actuation, device outside the vehicle.

Rule 126 (which recommends a two-second gap between vehicles) should be relaxed to enable basic platooning, which is most likely to be deployed on trucks and heavy goods vehicles in the first instance, once the technology is proven to be safe. As adaptive cruise control, motorway assistant and autonomous emergency braking become increasingly common features in new vehicles, these technologies working in tandem are capable of reducing the “thinking distance”, if not eliminating it altogether. Using the most technically advanced systems, it is possible to drive with a headway gap of 10 metres, or 0.5 second, instead of 50 metres, or 2.0 seconds. For instance, trucks travelling in suitable conditions at a set speed of 50mph may be able to operate with a headway gap of 6-22 metres, or 0.3-1.0 second.

In addition, SMMT believes Regulations 104 (the driver should be in a position to be able to control the vehicle), 107 (switching off the engine when the vehicle is not attended) and 110 (not using hand-held mobile phones while driving) of the Construction and Use Regulations should be clarified to enable remote control parking. However, as long as drivers are still “in the loop”, they are still prohibited from using a hand-held mobile phone while performing ordinary driving tasks (Regulation 110).

Looking further ahead, the Government, through Driver and Vehicle Licensing Agency (DVLA) and Driver and Vehicle Standards Agency (DVSA), must start examining the potential implications on, and the possible repurposing of, driver training, licensing, the driving test and the MOT test in preparation for the deployment of vehicles with increasing levels of automation, culminating with fully autonomous vehicles.

6. MAKING THE UK A GLOBAL CENTRE OF EXCELLENCE

6.1 National strategy

While it is not expected of the Government to actively participate in making markets, the Government can and should play an influential role in creating the right facilitating conditions for the market to grow and thrive. Towards this end, the automotive industry has welcomed the creation of the Centre of Connected and Autonomous Vehicles (C-CAV) which acts as a vital focal point for all of the Government's work in relation to CAVs. The industry remains supportive of the role and work of C-CAV.

We commend the Government for backing CAV technology research, development and testing through various measures. In addition to the publication of the Code of Practice for testing, the Government has made available £19 million of funding for three self-driving car trials in four locations (Milton Keynes, Coventry, Greenwich and Bristol), £100 million over five years for competition-led collaborative research and development projects, and another £100 million to develop a testbed ecosystem for CAVs. The Government’s rolling programme of regulatory reform to prepare the UK for the deployment of advanced driver assistance systems and autonomous driving technologies is another step in the right direction, as is its continuing engagement with the industry.

However, the UK is not the only country seeking competitive advantage and a leadership position in CAVs. The significant economic and social benefits that could come with the development and deployment of CAVs have led to many countries seeking to position themselves as frontrunners and world leaders. The German Government published its CAV strategy in September 2015, which sets out a clear ambition to remain the leading solution provider, to become the leading market for deployment and to introduce regular operations of CAVs.

The Government must decide whether the UK should seek to become the frontrunner on every single aspect of development, testing and deployment of CAVs, or to focus on specific areas. It is therefore imperative for C-CAV to now go one step further by developing a clear and joined-up national strategy for making the UK a global centre of excellence in relation to CAVs based on a thorough understanding of UK strengths and competencies. This must be done by working closely with the automotive industry through SMMT and the Automotive Council and by building on the significant strengths that already exist in not just the automotive industry but also adjacent industries such as technology (software, artificial intelligence), cyber security, telecoms and insurance.

A national strategy should include a clear articulation of how the UK should leverage on the outcomes of the publicly funded CAV projects and the creation of a unique CAV testbed ecosystem that integrates physical (i.e. proving ground and real world on-the-road) testing and virtual testing and validation capabilities. The strategy should focus on funding a small number of ambitious game-changing projects rather than spreading public funds more thinly over a larger number of less impactful, albeit interesting, projects. Step-change projects must also be able to create a critical mass of expertise around existing automotive centres of excellence involving industrial and academic research, design and development, manufacturing, and testing and validation.

The strategy, however, must not focus on just programme or project funding, but also set out how the Government plans to create the conditions that will make the UK attractive for CAV investment. These conditions include our national infrastructure, R&D capabilities, skills and finance opportunities. There are significant opportunities to encourage or expand inward investment into the UK by foreign companies seeking to partner with UK-based automotive and technology companies and to participate in collaborative research with academia and industry partners. Getting the strategy right is crucial for attracting investment that will drive productivity and economic gains.

CAV technologies are to a large extent a departure from traditional areas of automotive technology and innovation such as powertrains, drivetrains, chassis and materials. The Government must prioritise developing a pipeline of highly skilled engineering talent from non-traditional automotive engineering backgrounds – for example, electrical and software engineering, machine learning and artificial intelligence, data science and human factors – to deliver future CAV technologies. There is a general acknowledgement that while there is currently a pool of talent in the above areas, the vast majority of these engineers are found in the technology sector (e.g. computer software, gaming, apps, fintech, consumer electronics). The near-term challenge is to attract these engineers into automotive by demonstrating the value and relevance of their skills to CAV technologies. In the wider context and the longer-term, the Government must link its skills strategy and education system to the demands of industry. It is important to develop a culture that sees education as a means to an end, not an end in itself.

The Government may also wish to consider setting up a neutral national data aggregation platform for sharing anonymised data for the improvement of traffic management and safety (Type 1A in Table 2). Such platform may later be integrated with multi-modal journey information pulled in from public transit, rail, maritime and aviation.

6.2 Forging public acceptance

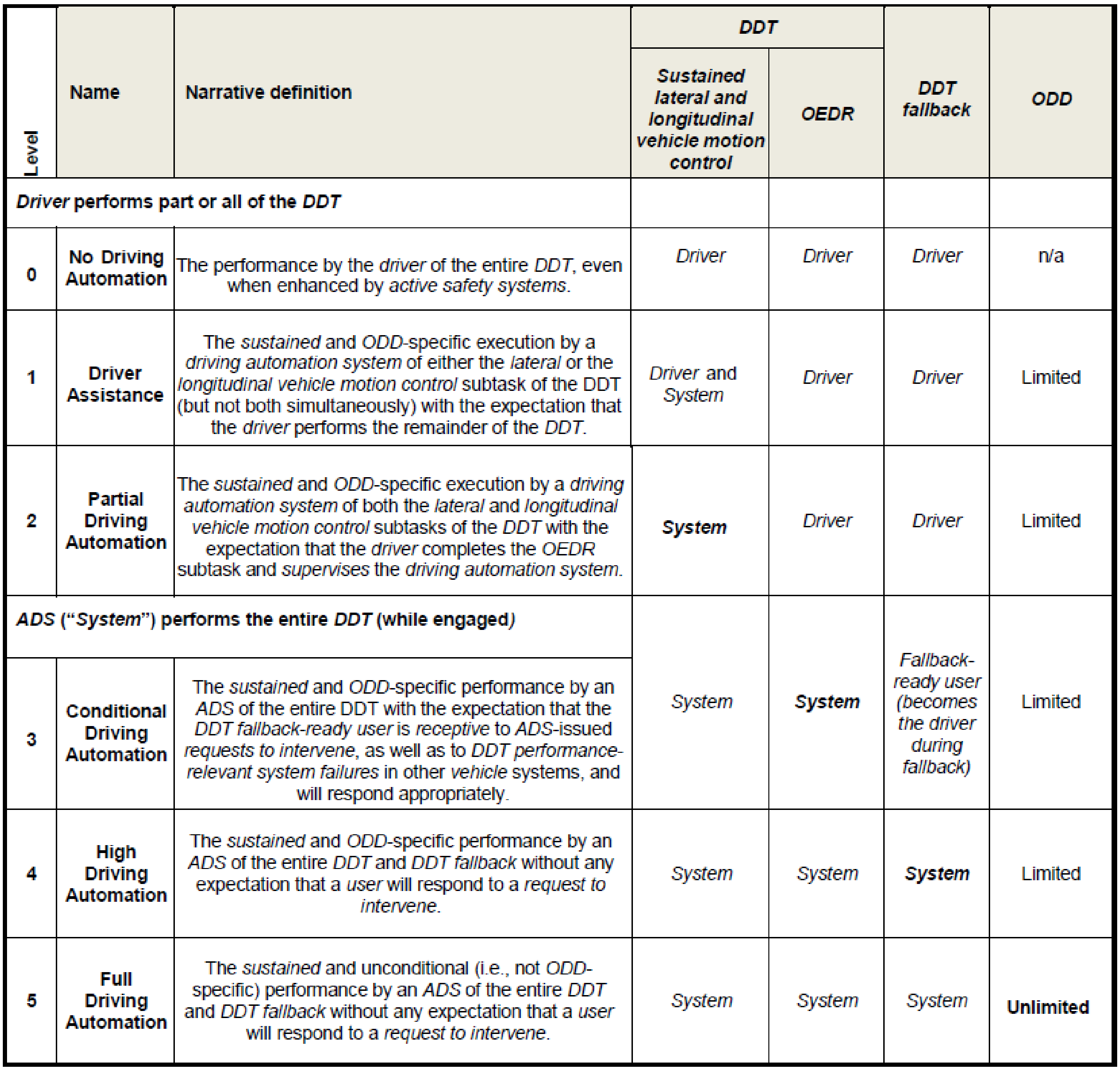
In order to make the UK a global centre of excellence for CAVs, not just hard regulatory and technological barriers must be overcome, but also soft barriers related to public acceptance and trust that may hold back the widespread deployment of CAVs. Existing CAV collaborative R&D projects and feasibility studies such as UK Autodrive, GATEway, UK CITE and PAVE have included a behavioural component that seeks to study how the public interact with autonomous vehicles and the level of public acceptance given different scenarios.

Consumer education and a strategic plan for integrated communications that take the public on a journey from the lower levels of vehicle automation through to fully autonomous driving are pivotal for gaining consumer buy-in and for increasing public confidence.

SMMT calls for the Government to set up for CAVs the equivalent of the Go Ultra Low campaign for ultra low emission vehicles. Replicating the successful Go Ultra Low model, this should be a consumer-targeted campaign that is jointly funded by the Government and participating vehicle manufacturers, and that seeks to provide the public with a one-stop-shop resource for information and potential purchase decision. Planning and preparation for such initiative should commence now and be gradually escalated as government and industry work together to better align regulatory, technology and product deployment roadmaps. The initiative should be launched in conjunction with the introduction of the first Level 4 capable vehicle in the UK market.

APPENDIX A: SAE J3016 LEVELS OF DRIVING AUTOMATION

The following summary of SAE J3016 levels of driving automation is an updated version published in September 2016, superseding the previous version published in January 2014. While the update has not materially changed the taxonomy, it provides more granular technical description.



Level	Name	Narrative definition	*DDT*		*DDT fallback*	*ODD*
			Sustained lateral and longitudinal vehicle motion control	*OEDR*		
Driver* performs part or all of the *DDT						
0	**No Driving Automation**	The performance by the *driver* of the entire *DDT*, even when enhanced by *active safety systems*.	*Driver*	*Driver*	*Driver*	n/a
1	**Driver Assistance**	The *sustained* and *ODD*-specific execution by a *driving automation system* of either the *lateral* or the *longitudinal vehicle motion control* subtask of the DDT (but not both simultaneously) with the expectation that the *driver* performs the remainder of the *DDT*.	*Driver* and *System*	*Driver*	*Driver*	Limited
2	**Partial Driving Automation**	The *sustained* and *ODD*-specific execution by a *driving automation system* of both the *lateral* and *longitudinal vehicle motion control* subtasks of the *DDT* with the expectation that the *driver* completes the *OEDR* subtask and *supervises* the *driving automation system*.	***System***	*Driver*	*Driver*	Limited
ADS* (“*System*”) performs the entire *DDT* (while engaged*)						
3	**Conditional Driving Automation**	The *sustained* and *ODD*-specific performance by an *ADS* of the entire DDT with the expectation that the *DDT fallback-ready user* is *receptive* to *ADS*-issued *requests to intervene*, as well as to *DDT performance-relevant system failures* in other *vehicle* systems, and will respond appropriately.	*System*	***System***	*Fallback-ready user (becomes the driver during fallback)*	Limited
4	**High Driving Automation**	The *sustained* and *ODD*-specific performance by an *ADS* of the entire *DDT* and *DDT fallback* without any expectation that a *user* will respond to a *request to intervene*.	*System*	*System*	***System***	Limited
5	**Full Driving Automation**	The *sustained* and unconditional (i.e., not *ODD*-specific) performance by an *ADS* of the entire *DDT* and *DDT fallback* without any expectation that a *user* will respond to a *request to intervene*.	*System*	*System*	*System*	**Unlimited**

Source: SAE J3016 Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles, accessible at http://standards.sae.org/j3016_201609/.

Glossary of SAE J3016 technical terms:[14]

- **ADS (Automated Driving System)**: The hardware and software that are collectively capable of performing the entire Dynamic Driving Task on a sustained basis, regardless of whether it is limited to a specific Operational Design Domain. This term is used specifically to describe a Level 3, 4 or 5 driving automation system.

- **DDT (Dynamic Driving Task)**: All of the real-time operational and tactical functions required to operate a vehicle in on-road traffic. These exclude the strategic functions such as trip scheduling and selection of destinations and waypoints. However, these include, without limitation, lateral vehicle motion control via steering; longitudinal vehicle motion control via acceleration and deceleration; monitoring the driving environment via object and event detection, recognition, classification, and response preparation and execution; manoeuvre planning; and enhancing conspicuousness via lighting, signalling and gesturing. Dynamic Driving Task fallback is the response by the user or by an Automated Driving System to either perform the Dynamic Driving Task or achieve a minimal risk condition after occurrence of a Dynamic Driving Task performance-relevant system failure or upon Operational Design Domain exit.

- **ODD (Operational Design Domain)**: The specific conditions under which a given driving automation system, or feature thereof, is designed to function, including but not limited to driving modes. These may include geographic, roadway, environmental, traffic, speed and/or temporal limitations.

- **OEDR (Object and Event Detection and Response)**: The subtasks of the Dynamic Driving Task that include monitoring the driving environment (detecting, recognising and classifying objects and events, and preparing to respond as needed) and executing an appropriate response to such objects and events as needed to complete the Dynamic Driving Task and/or Dynamic Driving Task fallback.

[14] SAE J3016 Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles, accessible at http://standards.sae.org/j3016_201609/.

APPENDIX B: GLOSSARY OF SELECTED SAE LEVEL 1 AND 2 FEATURES

Adaptive cruise control
Technology that dynamically adjusts a vehicle's speed to maintain a safe distance from the vehicle in front.

Autonomous emergency braking
Safety technology that takes into account the traffic conditions, objects or obstacles ahead and will automatically apply the brakes if the driver fails to respond to the conditions, objects or obstacles.

Blind spot monitoring and collision warning
Technology that detects objects in the driver's blind spot and informs and/or warns of a potential collision when the driver intends to change lanes.

Lane departure warning
A system that evaluates the lane markings with the aid of a video camera that detects the course of the lane, and warns the driver if the vehicle leaves the lane unintentionally.

Lane keeping assistant
A package of technologies that prevents the vehicle from drifting out of its lane by controlling the steering of the vehicle.

Parking assistant
In certain parking scenarios the system assumes lateral control. The driver activates the parking assistant, which then performs the task of steering. The driver applies the brakes only at the end of the parking manoeuvre.

Remote control drive
A feature that allows the driver to manoeuvre the vehicle from outside the vehicle at low speed, for example off-road rock crawling. Steering, speed and braking can be controlled using a mobile device outside the car.

Remote control parking
A feature that allows the driver to get out of the vehicle before the vehicle is manoeuvred into a parking space, and then to use the display key, or a specific device, to manoeuvre the vehicle into the space. The same applies to manoeuvring the vehicle out of a parking space.

Traffic jam assistant
In congested traffic, the vehicle drives within its own lane and keeps its distance from the vehicle in front.

SMMT
DRIVING THE
MOTOR INDUSTRY

Konstanze Scharring
Director of Policy
kscharring@smmt.co.uk

Sydney Nash
Senior Policy Manager
snash@smmt.co.uk

David Wong
Technology and Innovation Manager
dwong@smmt.co.uk

The Society of Motor Manufacturers and Traders Limited
71 Great Peter Street, London SW1P 2BN, United Kingdom
www.smmt.co.uk