ARTICLE:

Autonomous vehicles – who will be liable for accidents?

By **Roger Kemp**

The attraction of autonomous vehicles

In the last five years, there has been increasing enthusiasm for autonomous (i.e. self-driving, or driving by software) vehicles. There are many benefits claimed for them: lower energy demand, better use of infrastructure, fewer accidents and mobility for all, including those who, for reasons of age or infirmity, are unable to drive. A report by consultants KPMG[1] concluded that the adoption of autonomous vehicles (AVs) could add more than £50 billion per annum to Britain's Gross Domestic Product by 2030. Connected AVs (i.e. autonomous vehicles that can communicate with each other and with the fixed infrastructure or both) are being researched or developed by major technology and car companies. The work is being supported by many governments, and has been reviewed by the UK House of Lords.[2] In November 2017 the UK Chancellor, Philip Hammond, told the BBC Today programme: 'It will happen, I can promise you. It is happening already ... It is going to revolutionise our lives, it is going to revolutionise the way we work.'[3]

A change from road transport based on vehicles under the control of identifiable on-board drivers to a situation where vehicles may be controlled by computer systems developed and managed by complex international industrial organisations is radical. This paper raises some of the issues of legal liability that might arise.

The paper does not discuss the wider political and social issues raised by the widespread introduction on autonomous vehicles. In passing, it can be noted that, for 100 years, the car has been 'sold' as a symbol of personal freedom; moving to a situation where every journey is managed and logged by an international corporation would be a dramatic shift. The paper also excludes issues of energy consumption, traffic congestion and effects on public transport. These are all important questions that will need to be debated before countries become irrevocably committed to AVs.

How is autonomous defined?

Internationally, very similar definitions are used for levels of autonomous operation:

Level	Name	Definition	Acceleration, braking and steering	Responsibility for safety
0	No automation	Full-time performance by human driver of all aspects of the driving task	Human driver	Human driver
1	Driver assistance	Automated assistance of either steering or acceleration/ deceleration with human driver performing all other tasks	Human driver with advice	Human driver
2	Partial automation	Automated steering and acceleration/ deceleration with the human driver performing all other actions	Supervised automation	Human driver
3	Conditional automation	Automation of all aspects of the driving task with the expectation that the human driver will respond appropriately to a request to intervene	Automation or human driver	System, unless it requests intervention
4	High automation	Automation of all aspects of driving tasks in a defined geographical area, with no requirement for a human driver to intervene	Fully automated	System
5	Full automation	Full-time automation of all aspects of driving tasks under any circumstances which could be accomplished by a human driver	Fully automated	System

Level 0 is the default situation today (Level 0 has no automatic capability – it provides indications, but there is no connection to anything that can control the speed or steering of a car); sensors can provide lane-departure warnings, electronic stability control, collision warnings, parking assistance, speed limit reminders, satellite navigation and many other advisory functions. Under close driver supervision, some of these sensors can be used to manage 'hands off' parallel parking or adaptive cruise control. This is classed as Level 1.

By integrating adaptive cruise control and lane departure warnings into the control system, a Level 2 system can manage steady state driving on a clearly defined route, such

[1] *Connected and Autonomous Vehicles – The UK Economic Opportunity* (March 2015, kpmg.co.uk).
[2] *Connected and Autonomous Vehicles: The future?*, House of Lords Science and Technology Select Committee, 2nd Report of Session 2016–17, HL Paper 115.
[3] Gwyn Topham, 'Philip Hammond pledges driverless cars by 2021 and warns people to retrain', *The Guardian*, 23 November 2017.

as a motorway, or inching forward in a traffic jam.[4]

In the next stage of automation, Level 3, the driver can leave driving to the vehicle software, but has to be ready to take over if or when it decides it cannot continue.

In Level 4 the system can manage driving in known conditions (such as in specified urban areas when there is no snow on the ground).

Finally, in Level 5, the vehicle can undertake end-to-end driving anywhere and under all conditions.

The benefits of AVs really only come into their own in Levels 4 and 5. In the lower levels, a competent driver has to be available in the vehicle at all times. Vehicles in these categories are therefore not suitable for providing mobility to the elderly or others who are not able and authorised to drive themselves.

Different evolutionary routes

If the end objective is the widespread adoption of self-driving cars, there are various routes to achieving this aim. Some developers, such as Waymo (with Google, part of the Alphabet Group), are concentrating on vehicles that incorporate a highly detailed three-dimensional map of the area of operation, accurate to a few centimetres. Each time a vehicle goes over a route, it can update its internal map and a fleet of similar vehicles can share their mapping knowledge.

Knowing, with great accuracy, the fixed environment in which they are operating, makes it easier for the vehicles to differentiate between the background and unexpected objects such as pedestrians or other vehicles. The limitation of this approach is that the AVs can only operate in a closely specified geographic area which has recently been mapped in fine detail. However, a major benefit, relevant to the subject of this paper, is that the vehicles rely only on their internal maps and there is no supply chain of providers of safety-critical mapping information or other data.

An alternative option being pursued by some car companies such as Tesla, is to design an AV that can scan the road ahead and plot a safe course, thus requiring only a basic internal map. This requires more sophisticated sensors and software but has the benefit that the vehicle is not constrained to a limited geographical area for which highly detailed and up-to-date mapping data are available. At least in theory, this type of AV could drive safely anywhere it had the equivalent of a satnav map and would be able to respond appropriately to diversions, road works and other disruptions.

Some of the claimed benefits of autonomous vehicles only become available when vehicles communicate with each other or with the fixed infrastructure. Convoys of cars, travelling with less than the Highway Code 'safe braking distance' between them are envisaged. This is claimed to be possible because following cars will receive information on what the lead car is intending to do, rather than waiting until its radar senses what the car in front is actually doing, as happens today with adaptive cruise control. Connected Autonomous Vehicles (CAVs) pose particular problems of responsibility and liability, discussed later in this paper. (It should be noted that connected vehicles can only achieve many of the benefits of AVs identified by the UK government, such as increasing motorway capacity.)

If some CAVs are planned to have vehicle-to-vehicle (V2V) communication, other plans are for vehicle-to-infrastructure (V2I) interactions. For many years, the rail industry has used junction optimisation software to schedule trains on conflicting movements through junctions to minimise the overall delay. A similar type of system could be installed at roundabouts or traffic lights used by CAVs. As with V2V communication, this raises complex issues of safety responsibility, which is why some car manufacturers are not keen on the idea.

Ownership models

For conventional cars, there have been international requirements appertaining to both the manufacturer and the driver for many years – the earliest being the *International Convention on Motor Traffic* concluded in Paris in October 1909. More recently, the United Nations Economic Commission for Europe (UNECE) has established conventions that require countries to adopt non-conflicting standards on such issues as certification of drivers, approval of motor vehicles and

[4] This was the situation for the Tesla Model S 70D car involved in an accident with an HGV in Florida on 7 May 2016. It was operating with 'traffic-aware cruise control' (TACC), which controlled its forward movement and 'Autosteer' which kept the vehicle within lane markings.

road signage. The most relevant is the 1968 Vienna Convention (as amended).[5] Article 8 states:

> 1. Every moving vehicle or combination of vehicles shall have a driver.
>
> 2. [not relevant – concerns animals]
>
> 3. Every driver shall possess the necessary physical and mental ability and be in a fit physical and mental condition to drive.
>
> 4. Every driver of a power-driven vehicle shall possess the knowledge and skill necessary for driving the vehicle; however, this requirement shall not be a bar to driving practice by learner drivers in conformity with domestic legislation.
>
> 5. Every driver shall at all times be able to control his vehicle or to guide his animals.

Annex 5 covers *Technical Conditions Concerning Motor Vehicles and Trailers.* This lists various requirements for vehicles including braking and lighting. The Convention is written on the basis that the vehicle has to meet defined standards and that safety, in operation, is the responsibility of the driver. AVs of Level 3 and below will have a driver compliant with Article 8. AVs of Levels 4 and 5 do not have a driver and thus there is a question over who carries the responsibility that would otherwise be the driver's.

Prototype running of AVs is being undertaken by the manufacturers of AV systems – generally large automotive or technology companies. They carry both the responsibilities of the manufacturer of the vehicles and also those of the driver, so it does not matter where the boundary between the two lies.

Responsibilities becomes less well defined if AVs are leased or sold, either to companies, such as delivery contractors or taxi firms, or to individuals. These companies or individuals then become the *operators* of the vehicles (a term used later in this paper). They (or their employees) cannot be classed as drivers but they do not have the competence of manufacturers to ensure the safety of the automated systems.

Ownership models for the future use of AVs are important. Without a driver, responsibility for safe operation must rest with an operator competent to discharge that responsibility. This may place limitations on the ability of companies or individuals to own or lease AVs. A road traffic system in which all vehicles are owned and/or operated by an oligopoly of large industrial groups (mainly based in the USA) would be very different to that we know today.

Who will drive the Queen?

In a recent book,[6] Christian Wolmar opens a discussion on the interoperability of AVs with other traffic by posing the question that forms the title of this section. It seems highly unlikely that presidential motorcades, royal transport, ministerial cars and other VIP transport will ever be controlled by software. To these can be added some emergency services, breakdown trucks, motorcycles and vehicles used for trades that are incompatible with fully automatic operation. Basically, there will never be a situation where all vehicles are autonomous – AVs will always have to be interoperable with other manually-controlled vehicles and non-motorised road users, such as pedestrians, cyclists, horse riders and, in rural areas, flocks of sheep.

Although some commentators talk about an eventual high take-up of AVs, this is unlikely to happen quickly. For automation that relies on a detailed internal map, AVs will initially be limited to particular cities. AVs that do not rely on detailed internal mapping will be able to expand their areas of operation more rapidly. Although some 'tech-friendly' authorities may introduce changes to road layouts, signage and other infrastructure to accommodate AVs, it is unrealistic to expect all local authorities to bring their infrastructure up to that standard before AVs are widespread. The significance of this is that AVs will have to be developed to be interoperable with conventional traffic on existing roads; one cannot expect drivers to adopt their behaviour to accommodate AVs or for all local authorities to guarantee elimination of road features AVs find difficult.

Level 5: the Florence test

Level 5 means autonomous under all circumstances and that includes cities such as Florence (Firenze). The central area of the city is pedestrianized. But when delivering clients to their hotels, taxis are expected to navigate past tour groups, pavement cafés, horse-drawn carriages, market traders, Segway scooters, in-

[5] United Nations Economic Commission for Europe (UNECE), *Convention on Road Traffic*, Vienna, November 1968.

[6] Christian Wolmar, *Driverless cars: on a road to nowhere* (London Publishing Partnership, 2018).

line skaters, queues for bars and cafés snaking across the road, and groups of teenagers sitting on the kerbs and chatting. Away from the centre, the roads are more clearly delineated, but AVs will still have to coexist with horse-drawn carriages and, at the end of the day, market traders going home, at 5 km/h, with their folded-up, electrically-propelled stalls.

In a Level 5 AV, the system carries out all driving functions under all conditions. While this may be reasonably straightforward in suburban California or newly-built urban areas such as Milton Keynes, one has to ask whether it is realistic in Florence or in rural Tuscany, the Hebrides or the Pyrenees. In winter, human drivers may have to navigate their vehicles through floods or on snow-covered roads with only minimal markings; many country roads have single-track sections where drivers observe unwritten conventions about who goes first or who reverses back to a passing place; drivers of cars boarding ferries are expected to respond to traffic lights, hand signals or verbal instructions.

To further complicate the situation, many sensors on present-day cars can be overcome by poor environmental conditions. Driving in winter, the front of a car can become covered by wet snow, leading to video cameras, proximity sensors and radar sensors reporting failure. On country roads, splattered mud can have a similar effect in any season. It would be over-optimistic to assume AVs would be immune to such problems.

If a significant benefit of a Level 5 vehicle is that it provides autonomous mobility to people who are young, old or disabled, it has to be able to cope with whatever road traffic conditions it encounters; there is no option to hand over control when conditions become difficult. Realistically therefore, it seems improbable that fully autonomous Level 5 vehicles will be operational internationally within the foreseeable future. Level 4 vehicles, probably with control systems using detailed internal mapping and limited to a specific geographical area, are more likely but still very challenging.

The progressive introduction of AVs could cause difficulties for some communities – particularly if the first applications are in taxi or home delivery services. For instance, would it be a denial of someone's legal rights if taxi firms refuse to accept their address because it is outside a computer-mapped area?

Design authorities and systems authorities

There are two types of entity that can be seen to have responsibilities for AV safety – design authorities and systems authorities. For almost any engineering artefact, one can identify a design authority – usually the company that made it. In the aviation industry, separate design authorities can be identified for the airframe (e.g. Airbus), the engine (e.g. Rolls Royce) and the landing gear (e.g. Safran). In most cases, the liability for an accident caused by a mechanical or electrical failure can readily be allocated to one of these bodies.

For road vehicles, the overall design authority is usually the manufacturer (such as Ford, JLR, or PSA). Where they have bought-in a complete subsystem, such as an engine management system on a subcontract, the subcontractor could be held liable for accidents caused by that subsystem.

Complicated projects, comprising several subsystems all provided by different bodies, cannot readily be described as being the responsibility of a single design authority. When Lines 3 and 4 of the Seoul Metro were built in the 1980s, the operating company placed separate contracts for the trains (a UK company), the signalling (a US company), the power supply (a different US company) and the telecommunications (another US company). They then appointed one of these to undertake the systems engineering to ensure that all the various parts of the project could work together safely. Each of the different work packages had a design authority, so Union Switch and Signal were the Design Authority for the signalling system but a different company, GEC Transportation Projects, was the System Authority responsible for ensuring that the signalling was compatible with the power supplies and traction systems.

A system authority, sometimes referred to as a system architect (SA), is needed when a system is undergoing change.[7] The change could be the development of new activity, such as building a network of international space stations. Alternatively,

[7] The word 'system' has many uses and definitions. In this paper, it is taken to mean the following: An organised structure that consists of interconnected and interdependent elements (often the responsibility of different organisations) built to achieve a defined objective. System elements can themselves be subsystems, each consisting of further sets of elements. Systems display emergent properties not seen in the individual elements.

it could involve an existing system being subjected to significant changes either to its objectives, the environment in which it operates or to the technology it uses.

Developers of computer software refer to a V-diagram for software testing.[8] A variation of this diagram can be used for defining the role of system architect:

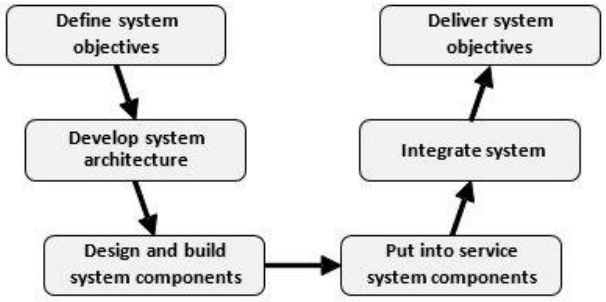

Figure 1: How a systems architect fits into project delivery

Starting at the top left, the objectives of the system are defined. For instance, to restructure the accident and emergency (A&E) services in a region these might include: emergency service response times, waiting times in hospital, death rates, ability to cope with an epidemic, patient confidentiality, cost and so on. The objectives are defined as desired outcomes, not how those outcomes are achieved.

The system architect (SA) body takes these objectives, analyses different options and produces a system architecture that will satisfy the outcomes. For the A&E example, the architect might analyse possible combinations of walk-in centres, computer-based diagnostics, regional hospitals, community nurses, mobile treatment centres and extended GP facilities. The SA's outputs are recommendations of what facilities are needed and how they would interact. The design authorities for these facilities use the SA's guidance when designing and building facilities. The right hand side of the diagram is about putting into service the various components of the system. At the top right the system objectives are delivered.

Development of an electrically-powered autonomous transport system may need both a systems authority and various design authorities. The latter group could include mapping contactors, highways authorities responsible for the road network and road signals, battery charging network contractors, vehicle builders and various control system suppliers. The systems authority would ensure that, when these groups are brought together, the end result is a functional and safe system.

In manually-driven cars, drivers are held responsible for operational failures. If they drive too fast and overturn on a bend, or drive too close and cannot stop when a car in front indicates to turn across the oncoming traffic, they are liable. It is not an adequate defence to say that the road authority should have imposed a speed restriction on the bend or the preceding driver should not have wanted to make (an entirely legal) manoeuvre.

The situation for an autonomous vehicle may be different. Some models of AV evolution assume safe operation will depend on accurate knowledge of the infrastructure, highly-detailed mapping and predictable operation of road signs and other indications, which places responsibilities on infrastructure managers which they may be unwilling to accept. For the present prototype AV trials, the major automotive and tech companies are acting as main contractors/operators who take responsibility for everything (and have made ex-gratia payments to those injured when things go wrong). This situation is unlikely to continue into full-scale, world-wide operations. While it may be technically straightforward, if resource-consuming, to maintain up-to-date maps at centimetre detail of the urban areas of Palo Alto, California or Phoenix, Arizona, it would be impracticable to maintain a similar standard of mapping of the network of minor roads in the north Pyrenees, on the Mull of Kintyre or of the many thousands of comparable locations in Europe, not least because many of the physical features near the roads are vegetation and are forever moving and changing.

Thus the model of each manufacturer maintaining independent and detailed mapping of all routes over which their AVs may operate, becomes unrealistic for continent-wide Level 5 automation. At this scale, either AVs would have to be developed to be fully self-contained and able to operate safely on any road, anywhere, or there would be a need for collaboration between vehicle infrastructure providers, mapping agencies and other parties leading to ambiguity about overall responsibility for vehicle safety.

Some types of AVs are likely to rely on communications links with the infrastructure. In

[8] Ian Sommerville, *Software Engineering* (10th edn, Pearson, 2015).

particular, CAVs (connected autonomous vehicles) could communicate with other vehicles – probably made by different companies – when running in convoys, and with 'smart' traffic signs. This implies that safe operation could depend on the correct functioning of data networks and the integrity of interfaces with road signalling and other vehicles. In this situation, an individual AV builder cannot be responsible for operation of the complete system and a systems authority will be needed.

Who could be a systems authority for Connected Autonomous Vehicles?

Making the assumption that connected autonomous vehicles (CAVs) are developed, as the UK government hopes, by 2040 there might be a dozen different manufacturers producing CAVs that operate across Europe. They would communicate with each other and with the fixed infrastructure and might take mapping data from a large number of different sources. Under these conditions, there would clearly be a need for a systems authority, but it is far from clear who or what this could be. One option, that might have been seriously considered 30 years ago, would be for national transport authorities – or even a department of the European Commission – to take this role, but that is unlikely in the present political climate.

An important aspect of a systems authority would be to manage the interfaces between the different participants. For a comparison, it is instructive to look at the way the World Wide Web Consortium (W3C) is managed. [Note: this is not the internet itself, which refers to the connectivity between computers and systems.] W3C is the systems architect for the world-wide web (www).[9] It is an international community with about 400 (mainly institutional) members where a full-time staff and the public work together to develop web standards. W3C sees its mission as 'to lead the Web to its full potential'. W3C is administered via a joint agreement among Host Institutions: Massachusetts Institute of Technology (MIT), the European Research Consortium for Informatics and Mathematics (ERCIM), Keio University in Minato, Tokyo and Beihang University (BUAA) in Beijing, China. The W3C staff (many of whom work physically at one of these institutions) are led by a Director and CEO. A small management team is responsible for resource allocation and strategic planning on behalf of the staff. Much of the work is done by the Advisory Committee, composed of one representative from each member, a Technical Architecture Group, which primarily seeks to document Web Architecture principles, and the chartered groups comprising Member representatives and invited experts, which produce most of W3C's requirements, such as interface specifications.

The Technical Architecture Group (TAG) undertakes the core systems architect role for W3C. The mission of the TAG is defined as stewardship of the Web architecture. There are three aspects to this mission:

> (i) to document and build consensus around principles of Web architecture and to interpret and clarify these principles when necessary;
>
> (ii) to resolve issues involving general Web architecture brought to the TAG; and
>
> (iii) to help coordinate cross-technology architecture developments inside and outside W3C.

The primary activity of the TAG is to develop Architectural Recommendations. An Architectural Recommendation is one whose primary purpose is to set out fundamental principles that should be adhered to by all Web components. The nature of a digital communications system is that addressing has to be perfectly correct. Anyone who has mistyped a web address will be well aware that the likely outcome is a complete failure of communication. It is essential in a complex technical environment that standards are precise and detailed. The W3C website contains thousands of pages setting out what is acceptable and what is not acceptable in terms of the interface with other web users, much of it in great technical detail.

The model adopted by W3C could cope with the complexity of the interface standards needed by CAVs, but W3C standards have never been applied to safety-critical systems. If a Web communication fails, the users probably curse, switch off, make a coffee, switch back on and try again. No-one will take legal action against the members of a committee for producing a set of specifications that, in certain unusual conditions, cause communication to be lost. However, the same degree of tolerance would not be shown if there is a failure of communications within a convoy of heavy trucks running at 100 km/h on a motorway. Faulty communication could result in a

[9] The section is based on information from the W3C website.

massive pile-up with many fatalities and injuries. In such an event, the public would expect a formal inquiry, with the prosecution of anyone found to be at fault. The state cannot be seen to provide the AV industry with a waiver of the law.

The railway industry has come to terms with the need for high-integrity systems engineering. Throughout most of the EU, trains operated by many different companies travel safely over infrastructure owned by various national organisations. The price of this interoperability and safety is a highly conservative and risk averse design and approval process. While convoy operation of CAVs is being considered as a way of operating road vehicles at much less than a braking distance apart, the railways have spent the last 30 years slowly working towards a moving-block system that would reduce train separation to a braking distance (plus a margin) as opposed to the more conservative fixed-block signalling systems that have been operated since early last century. Software for railway signalling systems is simple and built using high-integrity design techniques. It is orders of magnitude simpler than the software structures being developed in the AV industry.

As part of a review of the operation of the electrical supply system of Great Britain, a survey considered several systems architect models used by different industries.[10] None of the industries surveyed in this report has a systems architect or system authority model suitable for the continent-wide adoption of autonomous vehicles. The lack of a system authority will not slow the initial development being undertaken by single companies in restricted geographical locations, but a model that manages safety, enables continent-wide operation, discourages monopolies, encourages competition and ensures clear accountability has not yet been identified.

It is instructive to consider the attempt of the UK rail industry to establish a systems authority to cover the area of wheel-rail interfaces. On 17 October 2000, there was a major rail crash at Hatfield, Hertfordshire; four people were killed and 70 were injured. Initial investigations found that the rail fracturing had caused the accident, which lead to the train derailing. More detailed investigations determined the problem to be one of rolling-contact fatigue. A paper written several years prior to the accident had identified at least eight parameters that affect rolling contact fatigue – axle load, wheel diameter, wheel-rail contact profile, cant deficiency, flange lubrication, traction enhancers, rail material and heat treatment, rail installation, traction control system characteristics, operational timetable and primary suspension stiffness.[11]

Railtrack were held liable for the Hatfield accident because their inspection regime had not picked-up initial stages of cracking. To avoid similar incidents in future, the industry decided to establish a systems authority including experts from all the parties who had influence over the factors that could lead to this type of fatigue. This included rail manufacturers, train operators, rolling-stock suppliers and infrastructure maintainers.[12] None of these could solve the problem by themselves, but they could all contribute to a solution. However, establishing the committee was difficult and was eventually abandoned, as it was impossible for members to obtain professional liability insurance individually, and their employers were not prepared to carry the potential liability of having been party to a decision that could result in a major train crash.

This is significant issue for the development of CAVs. While AV development activities are restricted to trials operated by a single company large enough to carry any potential liability, there are no issues of divided responsibilities. However, a mature AV industry with several manufacturers producing vehicles that communicate between themselves, relying on a plethora of partners for the infrastructure, requires a degree of coordination that can only be provided by a systems authority of some sort, and it is difficult to see what grouping of organisations would take on that role.

Are maps safety-critical?

An autonomous vehicle views the world through a wide variety of sensors. It has radars that measure distance to the next car, cameras that take in colour images of the street, and its Lidar sensors send out laser pulses that gauge the surroundings. Unlike a human driver, who takes-in the environment during the journey and, at most, needs a map with the level

[10] IET Expert Group: Power Network Joint Vision, *Transforming the Electricity System: How other sectors have met the challenge of whole-system integratio*n (Institution of Engineering and Technology, October 2014).

[11] A. F. Bower and K. L. Johnson, 'Plastic flow and shakedown of rail surface in repeated wheel rail contact', *Wear*, Volume 144, Issues 1-2, 1991, 1 – 18.

[12] The author represented the rolling stock manufacturing sector on this group.

of detail of a road atlas, some current AVs need a three-dimensional representation of the environment around it that is updated continuously and is accurate down to a few centimetres.

During a day's driving, an AV with a built-in detailed map can collect more than a terabyte (1 TB) of data (roughly the total capacity of a laptop hard drive). With that much detailed information coming from the car's many sensors, a fleet of cars operating in a city would amass a massive amount of information that can be used to provide more accurate mapping so the fleet continually updates its three dimension (3D) 'map' of the city. This raises an interesting question about who is responsible for the accuracy of the map. In conventional mapping there is a sign-off where the relevant manager in the organisation confirms the map is acceptable, but who would accept responsibility for the accuracy of a map produced by a committee of vehicles being driven by software?

While this level of detailed mapping might be practicable for a Level 4 AV operating in a restricted area, it is difficult to see how it could be maintained for Level 5 vehicles operating over several countries, which is why some companies, like Tesla, have avoided this approach. However, they would still need a map for guidance. The European map data for a present-day navigation system is around 20 Gigabytes (GB), which takes half an hour to download from the internet and an hour to install.[13]

At present the largest AV developers have their own mapping systems. Alphabet's mapping competence is seen as a major advantage for Waymo, its AV subsidiary (Alphabet owns Google Maps, Google Earth, Google Street View and the navigation app Waze, which tracks real-time traffic). While operating in a single city, a unique mapping system is not a severe limitation, but the amount of data that would have to be transferred in a country-wide update makes it impracticable for unconstrained use.

The *Financial Times* reports that Brian McClendon, the former head of Google Maps, believes that eventually detailed maps will not be needed because the cars will be more intelligent.[14] This appears to be some way from the present strategy of Waymo, and moves the group closer to car manufacturers who are designing for a system in which safe operation is not dependent on map data.

[13] Data for a 2016 Volvo XC60.
[14] Leslie Hook, 'Driverless cars: mapping the trouble ahead', *Financial Times*, 21 February 2018.

Even if mapping data is not safety-critical in the sense that faulty data could directly cause a crash, it could still be important in overall system safety. The Bay Gateway, a link from the Heysham port to the M6 avoiding Lancaster, has been in the Lancashire transport plan since 1948. In March 2013 the Secretary of State for Transport granted approval for construction, which started the following year. It was open for traffic in September 2016 and was officially opened by the Lord Lieutenant on 2 March 2017. A Volvo satnav map, updated in June 2017, did not include the new road. It is interesting to surmise how this oversight occurred. A hypothetical methodology would be: Lancashire County Council takes the 'as built' map data from the contractor and informs Ordnance Survey, which includes the road on a master map; a data acquisition company (one in each country of the 28 covered by the satnav data?) takes the data and sends it to a mapping contractor which prepares the map updates for the car manufacturer which are then available for download from their website – at least six different organisations.

While an out-of-date map is merely an inconvenience when driving manually, what happens if an autonomous vehicle has an equally out-of-date map?

In the Bay Gateway project, the N-bound slip road at M6 J34 has been moved almost 1 km north, there is a new bridge across the River Lune, a dual carriageway parallel to the M6 for several hundred metres and several new roundabouts. Many of the existing roads have been changed significantly and road numbering has been altered. If an AV were navigating solely by the map, it would become lost. In this case, would it have the intelligence to abandon the map and read the road signs?

This train of thought leads to a number of questions in relation to liabilities:

1. Some existing AVs need highly detailed and accurate mapping, but when more intelligent vehicles could use more basic geographic data, would they still need an up-to-date map to navigate complicated road layouts safely?

2. If the lack of an up-to-date map causes a vehicle to become confused, does it just keep going along any old road and hope it will find its way later, or does it stop and ask for help? If so, from whom? And if several dozen vehicles (from the same supplier and/or with the same map software) all become confused

in the same place at much the same time and all take the same course of action, how would the resulting traffic jam be untangled and by whom?

3. Who is responsible for ensuring the map in a car is updated? Assuming it is a chain of bodies (as above) how many of them would be prepared to accept responsibility in the event of an accident (or, more likely, severe traffic congestion) caused by an out-of-date map or do they all discharge the responsibility via terms and conditions – if so, onto whom, and will the law permit the responsibility to be passed?

4. What criteria does an AV use to decide to abandon its internal map and navigate by road signs or dead reckoning? Does it have the intelligence to recognise when a road sign has been moved, either inadvertently or 'for a bit of a laugh'?

5. How often do maps need to be updated? If it is once a week and each of 10 million AVs downloads 'only' 20 GB/update, that is a lot of data. Which body is responsible for managing the network?

6. If an AV misses a map update (perhaps the operator leaves it in a garage while overseas for a month) is it still allowed on the roads? If an update agency ceases to exist or suffers a major computer failure (ransomware, loss of supply?), does that mean that all vehicles using that system are prohibited from travelling?

An alternative sometimes discussed is that a vehicle does not carry an up-to-date map in memory but downloads it in real time from the fixed infrastructure. This could bring other complications, one of the more significant of which is that the Highways Agency (or whoever is responsible for the road in question) might acquire legal responsibility for some types of accident or major congestion involving AVs. And failure of the local infrastructure, possibly due to a cyber-attack or a local failure of the electricity system, could potentially immobilise thousands of vehicles. At present, there does not seem to be a well-thought-out solution to, what is admittedly, a long-term problem.

Road signs

All vehicles are expected to comply with speed limits and road signs; most of these are permanent but many are temporary for road maintenance, floods or to cope with accidents. Human drivers observe fixed roadside signs, electronic signs, and other indications.

The 1968 UNEC *Convention on Road Signs and Signals* defined, in broad outline, the principles to be adopted internationally for road signs. Subsequently the Inland Transport Committee (ITC) of the Economic Commission for Europe organised another agreement to supplement the Vienna Convention (document E/ECE/812-E/ECE/TRANS/566) which provides greater detail.

Despite these standardisation efforts, there are many situations where a country introduces road signs that are not precisely defined in these treaties. For example, in France, a speed limit sign is not displayed at the start of a built-up area but an official sign indicating a town is taken as the start of the 50 km/h urban speed limit; Volvo's traffic sign information (TSI) system, which has a camera to read road signs, fails to recognise this information. This is one example, experienced by the author; there are likely to be many similar potential situations. For a manually-driven car this is not a problem, because the driver is responsible for understanding and complying with the speed limits and the dashboard indication is a 'reminder', but an AV could not rely on a system with that defect.

Some cars have a speed limit advisory system that is programmed into the satnav. In September 2017, a nearly new Mitsubishi people carrier (in which the author was a passenger) going through the roadworks on the M60, where large 40 mph temporary speed limit signs were prominently displayed, showed a speed limit of 70 mph on the dashboard display, oblivious of the temporary signage.

Even when a speed limit recognition system is effective on a plain road, it is often confused at junctions. Western Avenue in London is a large thoroughfare with a speed limit of 40 or 50 mph. Many of the residential side roads have 20 or 30 mph speed limits. A TSI system is easily confused if a lower limit sign is a few degrees out of alignment. A human driver travelling at 50 mph in a steady stream of traffic would ignore an unexpected indication. Whether an automatic system could do likewise is less certain and a sudden brake application in a dense, fast stream of traffic could have serious consequences. It

also conflicts with Article 17, s1 of the Vienna convention, which states that 'No driver of a vehicle shall brake abruptly unless it is necessary to do so for safety reasons'. This raises the issue of liability for inadequate signage. At present, a partially obscured speed limit sign can be used by a driver as a reason to avoid a speeding conviction, but there is no record of councils being held liable for an accident caused by a car driving too fast after passing an obscured or misplaced sign. It is the driver's responsibility to drive at a safe speed, irrespective of the speed limit. Would this still be the case if an AV were relying on signage?

Software complexity and validation

Software integrity can be ensured for relatively straightforward functions, such as railway signal interlocking, nuclear power control or aircraft fly-by-wire systems, by using rigorous (and expensive) formal design methods. The software on manually-driven cars can run to 100 million lines of code. Although some may by written using formal design methods, other software uses less rigorous techniques and the introduction of errors is unavoidable. AVs will be much more complicated. Realistically, the complete software on an AV will have thousands of faults – most, hopefully, not serious. (It could be hundreds of times more complicated than consumer products, such as Windows 10, and probably built by more than a dozen different organisations – all protecting their intellectual property.) Testing cannot be definitive: testing for all possible combinations of potential failure modes would take a large team many decades or even centuries. The most prevalent faults may be picked-up in tests, but there will be many others that only become obvious faced with a particular sequence of events. While the software in reactor control systems or railway signalling systems in each revision is fixed and the outcomes are deterministic, much AV software uses artificial intelligence (AI) where the car learns from its experience and, in effect, rewrites its own code. This cannot be validated by the same techniques as deterministic software. Establishing the safety integrity of AI systems is an active research area with an uncertain timescale.

Data on manually driven cars shows a safety performance of just over 1 fatality per billion km.[15]

Research published by the Rand Corporation concludes:[16]

> 'The results show that autonomous vehicles would have to be driven hundreds of millions of miles and sometimes hundreds of *billions* of miles [under realistic traffic conditions] to demonstrate their reliability in terms of fatalities and injuries. Under even aggressive testing assumptions, existing fleets would take tens and sometimes hundreds of years to drive these miles – an impossible proposition if the aim is to demonstrate their performance prior to releasing them on the roads.' (Italics in the original)

This leaves a difficult situation in terms of assuring the safety of some types of AVs and, particularly, CAVs. On one hand, the formal structured programming techniques that can give confidence that accidents are 'designed out' have never been used on a system as complicated as an AV. On the other hand, demonstrating safety by test running would be extremely expensive and could take decades, even with large test fleets.

Software updates

Anyone with a Windows computer will be aware of the screen message '*Working on updates. Don't turn off your computer. This will take a while*.' Similar updating processes will be essential for AVs. There have been situations when experience in the field has indicated a Windows update has had unforeseen effects, which Microsoft has issued another update to correct. For PC operating systems, a problem of this sort could have economic effects but is unlikely to have serious safety consequences as, in general, Windows computers are not used in safety-critical applications. The same is not true of aerospace, nuclear and rail applications where computers are used in real-time control systems and where a failure could have serious consequences.

A *Eurostar* cross-channel train uses a duplicated network of 38 computers for train management. Data transmitted includes power demand, train direction, raising and lowering the pantograph, operation of country-specific external steps, air conditioning settings, availability of water in the toilets, and dozens more functions. However, the safety-critical

[15] Professor Martyn Thomas, *Is Society Ready for Driverless cars?*, Lecture at Gresham College, 24 October 2017.

[16] Nidhi Kalra and Susan M. Paddock, *How Many Miles of Driving Would It Take to Demonstrate Autonomous Vehicle Reliability?* (The Rand Corporation, 2016), 10.

emergency braking demand was also transmitted by modulating pressure in a pneumatic pipe so, even if the electronics failed totally, it is still possible for the driver to apply the brakes.

During the development of the train, a 'Laborame' (Labo = laboratory, rame = train, in French) was set up in Alstom's Stafford Research Centre.[17] This hardware allowed the data network to be tested faster than real time and with thousands of potentially conflicting data messages and imposed fault conditions. The quality procedures were adapted from those used on Sizewell B nuclear power station and in military aerospace systems. They required that, every time a software module was updated, the module in question was subjected to a detailed test and then inserted into the *Laborame* for tests to ensure its compatibility with other functions. This made the development less rapid than might otherwise have been the case but much more reliable. The network went into service with far fewer faults than simpler systems on previous projects.

The *Eurostar* train management network was a very simple deterministic control system that did not include the safety-critical emergency brake function. In comparison, the systems on an AV will be perhaps 1,000 times more complex and many would be able to cause a fatal accident. Validating the original control systems will be a major exercise that will probably use software analysis, laboratory simulation (similar in principle to the *Laborame*) and extensive operational trials. The process will not be quick and will be expensive. It is likely that, only once the control system is fully validated and demonstrated to be safe, would European regulatory authorities be prepared to allow an AV to be used unsupervised on the road. For a connected autonomous vehicle (CAV) it is likely that the equivalent to the *Laborame* stage would have to include aspects of the fixed infrastructure, for V2I systems or of any alternative manufacturers' vehicles, for V2V applications.

This raises the question of updating. Users of Windows 10 will know that it receives updates at least once a month, with a major update once or twice a year. During the early years of AV operation, manufacturers will find many ways in which the control systems could be improved and will identify dozens of possible weaknesses or vulnerabilities. It is unlikely that the update intensity will be much less than for Windows. If a similar update procedure is used to other areas in the transport sector, each update will need to be fully validated, using much the same process as for the initial system. This would represent a major workload with significant cost and timescale implications.

What are the implications of a software update not being installed? If an AV operator leaves a vehicle in a garage for a couple of months without installing any updates, would it still be legal to operate? If not, would the regulatory system rely on human intervention to prevent its use or would there be some form of remote inhibit? The latter would provide a tempting feature for cyber-criminals as well as possibly leaving users stranded. And where would the liability rest, in the event of an accident that may have been caused by a failure to install an update?

There is an important question about who would be responsible for validating both the original software and the updates. In the UK civil nuclear industry, the Office of Nuclear Regulation (ONR) employs inspectors who can evaluate the safety case submissions made by firms operating on the 36 UK regulated sites. The safety cases include evidence of software validation and, where critical software is changed, the safety case has to be updated and revalidated. If the government decides to implement a similar methodology, one might see an Office for Autonomous Vehicle Regulation (OAVR). The workload would be considerably greater than for the ONR, which employs 500 staff, as the software is much more complicated and incorporates AI elements – almost unknown in existing safety-critical systems.

Accident Investigation

The complexity of AV control software and the difficulty of safety assurance presents a particular challenge for accident investigators. With manually-driven cars, many driving decisions rely on a driver's judgement. If a car emerges from a side turning into the path of a truck that is unable to stop in time, investigators may ask for evidence of the driver's intoxication level, eyesight and general health and, unless these identify an obvious reason, the accident is put down to unanalysable 'poor judgement'. AVs are different. 'Judgement' on whether to drive out of a side turning will be taken by a multitude of sensors and software packages. All of these can be analysed to see where the fault lies. An investigation that, for a manual car, would take an accident investigator a few

[17] At the time, the author was *Directeur du Project* of the consortium designing and building the *Eurostar* trains.

hours for an AV could be replaced by a forensic software analysis taking a large team many months.

If AVs become widely adopted, there could be dozens of accidents a day in which the vehicle or its associated infrastructure systems are potentially implicated. In how many administrations would it be acceptable for the regulatory authorities to say 'It seems the fatal accident was caused by a lack of judgement in the vehicle software, but we are not investigating further'?

The only way of determining what caused an accident in a software-controlled vehicle is to interrogate the software, post incident. This raises the questions of who can obtain access to the software, whether the evidence is destroyed by being accessed, and how trustworthy the evidence is. Mason and Stanfield[18] define the term 'trustworthiness' as describing

> 'that a thing deserves, or is entitled to, trust or confidence. There are two qualitative dimensions to the concept of trustworthiness: reliability and authenticity. Reliability is meant to demonstrate that the record is capable of standing for the facts to which it attests. Authenticity means the record is what it claims to be.'

The evidence necessary to investigate the reasons for an accident involving an AV could include video records, data streams from radar and lidar sensors, timed records of speed, acceleration, steering angle, power and brake demand and similar inputs to and outputs from the AV decision-making process. In addition, the accident investigator would also require records of how the control system was interpreting these data and what might be described as 'the thought process' within the vehicle. The first group of data is reasonably easy to define and, given the right software, to interpret. These data should be reliable if the recording process has been working effectively, if calibration records are available and if precautions have been taken to prevent overwriting of data. Authenticity can be proved if the records are appropriately date and location stamped and if the data store has been locked to prevent corruption. There may be grounds for regulators to insist that AVs carry a sealed 'flight recorder' like aircraft so these data can be analysed by someone external to the design organisation.

It is the second group of records that is more problematic. Video records from the first group of data may show unambiguously that an AV pulled out of a side turning into the path of a truck which then ran into it. They will not show why the AV performed this manoeuvre. There may be records of 'the thought process' but this is unlikely, unless the requirement to maintain such records is a contractual commitment of being allowed on the road. Even if the records exist, it is unlikely that many accident investigators would be able to make sense of them. If a power station system has a deterministic control function implemented in a few hundred lines of a language such as C++, many independent investigators would be able analyse how it worked and how it might have failed. An image analysis programme designed to extract the message 'approaching truck, direction XYZ, velocity V' from a video stream is much less easy to analyse. If the message about the approaching truck is supplemented by data streams from radars and lidars and analysed by an AI programme, it is unlikely that even the system designers would be able to ascertain exactly how the decision to cross the truck's path was taken.

Under most safety regulatory regimes, it would be unacceptable for important parts of an accident investigation to be undertaken by the party responsible for the system design, because of the conflict of interest, but it is not obvious how an AV equivalent of the Air Accidents Investigation Board (AAIB) would be able to find out what happened.

This brings us back to the question raised earlier:

> *Will it be acceptable for the regulatory authorities to say 'It seems the fatal accident was caused by a lack of judgement in the vehicle software, but we are not investigating further'?*

If this is not an acceptable response to an accident, what other options are there?

Cybercrime and cyberterrorism

A fleet of autonomous vehicles provides an attractive intellectual challenge for computer hackers and, more significantly, for cybercriminals: the possibility of affecting thousands of vehicles across the country, and thus spreading chaos, in which other crimes may be committed, would be particularly attractive. Any

[18] Stephen Mason and Allison Stanfield, 'Authenticating electronic evidence,' Chapter 7 in Stephen Mason and Daniel Seng, eds, *Electronic Evidence* (4th edition, Institute of Advanced Legal Studies for the SAS Humanities Digital Library, School of Advanced Study, University of London, 2017), 7.1.

system that requires regular wireless updates and where an external body has the power to disable a transport system remotely offers an open door for cybercrime.

Many traditional infrastructure systems, such as the electricity grid, have a supervisory control and data acquisition (*SCADA*) system to control equipment remote from the control room. Often these systems use proprietary data protocols and are not connected to the internet or other publicly accessible systems. Attacking them remotely is difficult.

By contrast, CAVs are expected to use standard internet communications and to be fully integrated into the data environment. The KPMG report mentioned earlier,[19] which seems to be the government's reference point for AV policy, estimates a 12 per cent increase in internet traffic due to AVs and says:

> 'Connected and autonomous vehicles will generate vast amounts of data if consumers choose to share it. This has the potential to open up a range of opportunities for consumer engagement and indeed monetisation for the data owner. This will become a source of competitive advantage for OEMs, technology companies and insurers as well as supporting automated traffic flow management.'

With that level of integration into commercial data networks, there will be few impenetrable barriers to a determined cybercriminal. Traditionally, car crime has been about stealing either complete vehicles or their contents. Because of the likely ownership models and the need for various levels of approval and certification to operate autonomously, it is unlikely that there will be a ready market for stolen AVs. However, if AVs develop as mail order couriers, criminals might find it profitable to hack into the data systems to divert the goods to other addresses. Alternatively, if there is a development in AV chauffeur services for young children from affluent families, more aggressive criminals might find AVs a potential source of profitable kidnaps.

It is cyberterrorism, rather than cybercrime, that is the greater cause for concern. The ability suddenly to disable only 5 per cent of the vehicles on Britain's motorways would cause serious disruption; the effects of a virus to cause suicidal acceleration would be far worse. Reprogramming a few thousand vehicles to head for Trafalgar Square could clog central London for days, and it seems there would be little to stop a terrorist using an AV to deliver an explosive device to its target. It is possible that the police or security services would ask for some electronic means of intercepting AVs to force them to stop in these circumstances but, this would also provide a 'backdoor' for criminals to access the vehicle control systems.

It is not clear which body could take overall responsibility for preventing AV-enabled cybercrime and cyberterrorism. Possibly the regulatory, approvals and licencing regime for AVs could require manufacturers to demonstrate strong barriers against cyberattack. For CAVs which rely on subsystems developed and operated by several parties, this may be a defining role for a systems authority. The defined role and technical competences of the AV regulator will be important.

How safe is safe enough?

People, not technical failures, cause a large proportion of accidents. Data from the railways, air transport, oil refineries and chemical works show that around half of all accidents are attributable, at least in part, to human factors. For road transport, research indicates that around 94 per cent of accidents can be attributed to human error.[20] If the analysis includes incidents that do not include injuries (such as body panels damaged by contact with trees, gateposts, walls and other fixed structures) the proportion could be higher.

However, this does not mean that eliminating human input will necessarily reduce the number or severity of accidents. In Level 3 and below, a competent, certified (and sober) driver has to be available at all times, ready to take over when the control system decides it cannot cope. This is likely to be at the times that are most challenging for drivers, such as through complex roadworks at night. If the driver of a Level 3 vehicle only accumulates driving experience under these circumstances, it is probable that the intervention will be more stressful and their accident rate will be far higher than for a more experienced driver in a manual

[19] *Connected and Autonomous Vehicles – The UK Economic Opportunity* (March 2015, kpmg.co.uk), 14.

[20] US Department of Transportation; National Traffic Highway Safety Administration: *Critical Reasons for Crashes Investigated in the National Motor Vehicle Crash Causation Survey* (DOT HS 812 115 A, February 2015).

car. If drivers are expected to intervene in an emergency or in unanticipated conditions, how will they gain and maintain the competence to do so? A complementary question is what the driving test should consist of for someone who has no experience of traditional driving but expects to be in charge of a Level 3 autonomous vehicle. If the driver of a Level 3 vehicle is required to intervene only after the vehicle has put itself in an untenable position, such as on the wrong side of a barrier in road works, does he carry the liability for anything that goes wrong in attempting to rectify the situation?

Reducing the number of road accidents is a desirable outcome. However there is a question whether the general public would be as forgiving of accidents caused by an automated vehicle as they are of 'human error' events. Most opinion-formers are also car drivers and, other than in cases of gross irresponsibility, tend to be forgiving of errors they might have committed themselves.

In the 1980s, when the initial London Docklands Light Railway[21] was being commissioned, an overenthusiastic junior engineer drove a train over the end of the Island Gardens elevated section. There was a huge furore, focusing on the fact that it was an automatic railway – the fact that the train was being driven manually and the auto-drive system was not operational was ignored. It soon became obvious that the safety standards expected by the press and public of an automatic system are far more stringent than those of a manual system. While figures of 1,732 road deaths and 22,137 serious injuries (2015 figures for the UK)[22] are broadly accepted by the public, it is doubtful that similar statistics be acceptable for AVs.

Regulating safety

Different transport modes have different safety regulatory regimes. UK railways have to comply with The Railways and Other Guided Transport Systems (Safety) Regulations 2006 (2006 No. 599) as amended; air travel in Europe has to comply with the European Aviation Safety Agency regulations, etc.

There is no obvious reason why the safety standards for AVs should be dramatically different to those for automatic railways or for industrial autonomous robot systems which, in the UK, are covered by the Health and Safety at Work Act. In the decade that the Health and Safety Executive was directly responsible for railway safety (from the Railways Act 1993 to the Railways Act 2005), the ALARP criterion (reducing risks to as low as reasonably practicable) was applied to individual subsystems of a train (which, incidentally, made the stabilisation and validation of any design very complicated, expensive and time-consuming). A similar philosophy has never been applied to manually-driven cars, but could be applied to automatic driving systems. The implications of a safety policy of this type on AVs would have a significant effect on their development. However, from a logical point of view, it would be justified as it is debatable whether the public (and the media) would be more forgiving of deaths caused by an automatic system on the roads, rather than an automatic system on the railways or in industry. It is difficult to make a consistent argument why road deaths should be treated more leniently than others.

Who is responsible?

The foregoing sections have raised several critical areas where the responsibility for safe operation of AVs could be ambiguous. The current phase of development where the only AVs running in any particular city are those constructed, maintained, operated and underwritten by one of the large US tech firms is unlikely to be representative of a future situation. If AVs are introduced widely in Europe, it is likely there will be several competing designs. If CAV technology takes off, as appears to be UK government policy, different makes of vehicles will have to work together and with infrastructure systems owned by a variety of private and public sector organisations.

It is inevitable that there will be accidents – whether more or fewer that with manually-driven cars cannot be ascertained with confidence until a large fleet of AVs has been in service for many years.

For accidents involving self-contained AVs, and for some accidents involving CAVs the cause will be readily attributable to particular component parts of an AV's anatomy and thus to a particular supplier or design authority. In other situations, particularly if V2V and V2I interconnectivity are developed, it will be less clear what happened and where responsibility lies. It could be due a fault within the CAV, with part of the roadside infrastructure or with external data coming from other parties. There are likely to be situations where all subsystems are working as

[21] The author was systems engineering manager of the main contractor.
[22] Department for Transport, *Reported road casualties in Great Britain: main results 2015* (June, 2016).

designed but, when brought together, they result in a 'system fault' for which none of the subsystem design authorities could be held responsible.

To manage the interactions between different parties involved in AV development requires an organisation that is the systems authority or systems architect. Bearing in mind the level of technical competence needed by such a body, the necessary independence from other participants and the potential liabilities if there is a systems fault (such as on a computer-linked consist of Heavy Goods Vehicles (HGVs) running at speed on a motorway), there may be few, if any, organisations that could (and would be prepared to) take on that role.

The complexity of AVs and of their software means that a detailed forensic analysis of an accident would require a large team of people who are fully conversant with that particular vehicle's operating software. Realistically, this will only be available in the manufacturer's design teams, and so an independent analysis of the causes of accidents, as is undertaken on conventional transport systems, is unlikely to be possible.

The introduction of fully autonomous (Levels 4 and 5) vehicles into the market-based road transport system will change drastically the liabilities of different bodies involved. Politicians and safety regulators will need to have a very clear view of responsibilities and liabilities before operation beyond tightly-controlled prototype fleets is contemplated.

Roger Kemp is a Professorial Fellow in the Engineering Department of Lancaster University, United Kingdom. Before joining the university in 2003, he was UK Technical and Safety Director of Alstom Transport. He is a Fellow of the Royal Academy of Engineering.