Autonomous Vehicles

What insurers think now, want next and why

Introduction

In March last year, a driver of a partially automated vehicle was killed after the vehicle collided with a concrete lane divider in California. The driver of the car was expected to have their hands on the wheel and eyes on the road as a contingency measure but, according to in-vehicle data, failed to respond to several visual and one audible warning before the fatal accident occurred.

As the use of automated vehicles (as defined by the Law Commission) grows and incidents involving vehicles with some automated functions make the headlines, addressing the legislative structure that will govern their use becomes increasingly important. IUA members set out their views on the issue when responding to a consultation exercise initiated by the Law Commission of England and Wales and the Scottish Law Commission.

There were two clear messages:

i) users of vehicles other than those capable of high or full automation must be engaged in the driving task at all times and (ii) access to in-vehicle data will facilitate and underpin the use of automated vehicles.

New terms and concepts

The Law Commission's Consultation provided some clarity amidst a sea of new terms, steering clear of 'driverless car' and replacing it with 'automated vehicle', defined as 'a road-based vehicle capable of operating in an automated mode'.

These vehicles have been categorised into six levels by the Society of Automotive Engineers (SAE), extending from Level 0 'no automation' to Level 5 'full automation'. The Law Commission consultation looked at the highest three levels of automation (3, 4 and 5) that do not need human drivers for at least part of a journey, rather than addressing driver assistance systems that we see in use on UK roads today.

Level 3 and 4 automated vehicles – the road to full automation

In the short-term, the focus remains on Level 3 and Level 4 vehicles that will begin to make their way on to our roads in the next few years. A Level 3 vehicle is capable of generally performing all of the driving tasks, but a human 'fallback-ready user' must be receptive to a handover request in the event of a system failure; the user would otherwise not be expected to monitor the driving environment. This category of vehicle is due to be the first to reach UK roads and, in the view of IUA members, presents a potential threat to the widespread future use of automated driving technology in the UK is some core issues relating to the technology are not addressed. In particular, it is the strong recommendation of the IUA that it would not only be unreasonable, but potentially dangerous to expect that a 'fallback-ready user' who is not monitoring the driving environment will be capable of taking immediate control of the vehicle in an emergency situation.

According to a United Nations Economic Commission for Europe (UNECE) Resolution, a Level 4 Vehicle is one equipped with an automated driving system that operates within a specific operational design domain for some or all of the journey, crucially without the need for human intervention as a fall-back to ensure road safety. These operational design domains will likely initially be within city centres or on motorways. The user applicable to Level 4 vehicles is termed by the Law Commission as a 'user-in-charge' and their main role would be to operate the vehicle upon exiting the system's operational design domain. They would also have certain other positive obligations in respect of vehicle maintenance and insurance. The user-in-charge would not be a driver but must be qualified and remain fit to drive whilst the vehicle is driving itself and would not be responsible for monitoring the driving environment, having the option to undertake secondary activities whilst the automated driving system is engaged.

The Law Commission asked whether a user-in-charge who has taken control of a vehicle to mitigate an imminent accident should be liable for their actions if they fail to prevent the accident. IUA members have firmly agreed that were it to be established that the system had failed and was therefore about to cause an accident, any mitigating actions on behalf of the user-in-charge would not remove the blame from the automated driving system. It will be imperative that full and thorough data surrounding an accident, including system errors or defects present, are made available to insurers upon request in order to establish negligence. In its consultation response, the IUA suggested that consideration should be given to how the burden of proof would operate in circumstances where it is unclear from the in-vehicle data, and any other available evidence, whether an accident was imminent and was not identified by the automated system.

The threat of misconceptions before full automation

The final category of vehicle considered within the consultation, 'Level 5', perhaps will present the fewest concerns for insurers. This category of vehicle will be capable of carrying out all of the driving functions of a human driver in all situations and conditions. As with any other level of automation, it is the recommendation of the IUA that these vehicles are programmed to drive defensively. This would include, for example, reducing speed when required by law to do so due to weather conditions, when passing stationary buses and near schools, care homes or hospitals.

When reviewing the issue of SAE levels more broadly, IUA members have expressed strong concerns that misconceptions around the capabilities of an automated vehicle present a fundamental risk area. If a user of an automated vehicle perceives that a vehicle is capable of more than it is, this increases the probability of that individual wrongly disengaging from the driving task. The issue is further exacerbated by the fact that any individual utilising Level 3 technology for a significant period without being required to intervene, would likely gain a false sense of security, ultimately leading to misuse of the technology. Likewise, poor education around user types could lead to a 'fallback-ready user' wrongly considering themselves as a 'user in charge' and therefore being able to disengage entirely from the driving process. There is a fundamental need for absolute clarity regarding the terms 'fallback-ready user' and 'user in charge', given that such terms will define how users of automated vehicles perceive their responsibilities. Careful thought must be given to how the responsibilities of different types of user and capabilities of automated vehicles are publicised.

The fundamental importance of in-vehicle data

Underpinning the use of any automated vehicle is the availability of data around how that vehicle has operated and the level of intervention from a user within the vehicle. A key theme that has been reinforced by IUA members for several years is that it is of the utmost importance that an agreement with insurers is reached to ensure that in-vehicle data is provided to them in a usable format, following an incident, to ensure that consumers receive rapid and appropriate redress. The IUA response recommended that the Law Commission explore the possibility of a statutory requirement to collect, hold and transfer data, such as the following:

- time and location of event;
- status of automated driving system (engaged or unengaged);
- details of actions taken by 'user-in-charge' or 'fallback-ready user';
- details of any recent handovers;
- speed of vehicle prior to and at collision; and
- camera footage.

Without data clearly displaying whether a vehicle was in automated mode or being controlled by a user, liability disputes occurring between insurers and users following a collision will become commonplace. The data may include dash-cam style footage and could be used to protect innocent users who took control of an automated vehicle when an accident was imminent, but failed to prevent that accident. Whether an accident occurred or otherwise, it is envisioned that automated driving systems will self-report, automatically transferring data to manufacturers where a defect is present or an update is required. Additionally, data around the operation of automated vehicles can support publicity campaigns around their operation and effectiveness.

Insurers would also welcome access to in-vehicle data from the 'normal' operation of an automated vehicle. Such information could include reporting of any defects within a particular system or type of vehicle, the proportion of time specific vehicles or types of vehicle are in automated mode and the number of times a user was asked to take control of a vehicle. Data could allow broader analysis of hot spots for accidents, highlighting areas that Automated Vehicles have encountered issues dealing with, or specific types of obstacles, and potentially warning other vehicles. This information will likely prove paramount in supporting insurers understanding of this technology and pricing approaches taken.

A growing cyber threat

Whilst it is likely that the safety benefits of automated vehicles will be widely publicised and in time accident rates will fall, the changing threat landscape means that automated vehicles may also be vulnerable, presenting a systemic exposure for the (re)insurance market. Vehicles may become targets of malicious cyber-attacks seeking to take control of a vehicle or disrupt its normal operation. Such incidents would not be limited to when the vehicles are in use and could take place during the product development stage or via an over-the-air update. Additionally, a non-malicious cyber risk is present, as connected vehicles will depend on critical infrastructure and third party service providers, including GPS, power supply, communications networks and live data feeds. This reliance means that, in the event of a sever interruption; a single point of failure could bring a fleet of vehicles to a halt.

IUA members have discussed the potential for automated vehicles to have a lock-down function that could be engaged in the event of a suspected cyber attack. Such a function could be activated remotely or from within the vehicle itself and would lead to the vehicle, or a fleet of vehicles being targeted, to engage minimum functions that could enable it to reach a safe stop. It has been questioned whether building this ability across a fleet may bring as many cyber vulnerabilities as it seeks to counter.

New opportunities arising from new risks

In spite of the risks posed to automated vehicles, the London insurance market sees the development of automated vehicles as an opportunity, not only in providing (re)insurance for the testing of such vehicles, but in covering manufacturers against liabilities incurred during product development, maintenance and ultimately vehicle use. According to a member survey conducted by the IUA's Developing Technology Monitoring Group in October 2018, a number of firms are already providing insurance products for automated vehicles in the UK, Europe and North America. These products cover various aspects of the technology, including commercial and personal use, as well as manufacturing, and a quarter of companies surveyed are providing a product covering the testing of automated vehicles.

The ability for insurers to continue to develop products in this area will be facilitated by the introduction of the Automated and Electric Vehicles Act 2018. In a response to a Department for Transport consultation in 2015, prior to the finalisation of the Automated and Electric Vehicles Act 2018, the IUA supported government plans to make the motor insurer responsible, in the first instance, for the payment of a claim where the cause of an accident was an automated vehicle. This was and continues to be seen as the simplest way of accommodating automated vehicles within the insurance framework, incurring the least amount of change to current practices, whilst ensuring that victims of collisions are indemnified without undue delay. However, with any piece of new legislation and particularly one concerning a developing technology, the IUA has recommended ongoing review of the legislation. As information relating to incidents involving automated vehicles emerges, their use grows and potential vulnerabilities and risk areas emerge, it is imperative to ensure that any relevant legislation remains appropriate.

As long as the motor insurer remains liable in the first instance, the IUA has recommended that consideration be given to whether or not there should be minimum product liability limits purchased by manufacturers, to avoid potential coverage gaps where the limits within a motor policy exceed those of a product liability policy of a manufacturer. Further thought is required to ensure that manufacturers are adequately capitalised and potentially insured to pay for liabilities that they may incur throughout their business process.

Conclusion

IUA members have offered some stark warnings to the Law Commission regarding the technology. Clear messaging around the various levels of automation and the responsibilities of users of the technology must be at the forefront of the Government's thinking. Another important focus will be the types of in-vehicle data that insurers will need and how such will be transferred to them in a usable format. It is clear that insurance products will continue to evolve in this new landscape, with (re)insurers preparing to meet a shift in demand from motor to product liability policies. Addressing the questions raised in this article will not only limit the number of accidents caused by automated vehicles, but will also support insurers as they seek to develop products that will allow the UK economy to fully unlock the benefits of this emerging technology.

9th April 2019