AG/GE8897/ACE Geneva, 15 May 2023

UPDATED IRU POSITION ON AUTONOMOUS VEHICLES

IRU Position adopted at the IRU General Assembly on 12 May 2023.

IRU Position on the implementation of autonomous vehicles.

I. IRU POSITION

- The road transport industry embraces innovation and is in favour of a transition which allows for the **s**afe, **s**ecure, and **s**ustainable operation of autonomous vehicles (AVs). The industry is fully aware that higher levels of automation will not address the current shortage of drivers.
- The **development of technology** in the road transport sector will affect all operators, from goods transport and logistics to individual and collective passenger mobility.
- Transport operators or **drivers** should not be legally liable for any system failure, incidents, or accidents when a vehicle is operating autonomously.
- National and global legislation relating to **legal liability** should be revised to consider the use of vehicles with different driving automation systems according to the Society of Automotive Engineers (SAE).
- The use of automated vehicles should be included in training schemes **for transport operators and professional drivers**.
- **Data** collection sharing and **data** storage by authorities should not be allowed without the adoption of specific measures aimed at protecting the privacy of drivers and operators.
- The ownership of **data** related to transport operations should remain with operators.
- Regulatory measures should be in place to protect connected and autonomous vehicles against **cyberattacks**. Special cybersecurity provisions should be established for commercial freight vehicles and for collective passenger transport.
- Transport operators should be consulted and made aware of any new additions and/or changes to the functionalities and behaviour of automated vehicles with every **software update**.
- Governments need to facilitate the successful integration of AVs into the **existing road** network. The coexistence of autonomous vehicles and other road users must always be considered.
- Back-up solutions should be ready if systems fail.

II. ANALYSIS

Connected and automated vehicles can help to increase traffic safety, reduce vehicle greenhouse gas emissions, and alleviate traffic congestion. These benefits, however, will only become clear once connected and autonomous vehicles are rolled out on a large scale.

The introduction of autonomous vehicles will improve transport efficiency for operators and will provide further carbon reduction potential.

In 2018, IRU published its Position Paper on managing the transition to autonomous vehicles. The road transport industry embraces innovation and is in favour of a transition which allows for the **s**afe, **s**ecure and **s**ustainable (the 3 "s" strategy) operation of autonomous vehicles.

The use case approach should be taken in the implementation of automated vehicles. The first applications to be considered can be specific long-distance routes, followed by inter-city applications, and, finally, city applications for door-to-door distribution and passenger transport.

a) Drivers

- Drivers' liability

Connected and automated driving will have an impact on the liability of transport operators. According to Article 8 (5) of the United Nations Convention on Road Traffic (1968), "every driver shall at all times be able to control his vehicle or to guide his animals". This means that the driver may remain responsible and liable for operating the vehicle, even when that vehicle operates in full autonomy without the possibility for the driver to intervene in case of an issue. This raises questions concerning the current level of driver liability and has the potential to shift more of the legal burden to other parties, such as vehicle and component manufacturers.

Considering the current unclear legal framework, the following assumptions can be made:

– For SAE driving automation levels 0–2, the driver should not perform secondary tasks that will prevent them from taking control of the vehicle immediately when required. Considering that the driver remains in charge of any dynamic driving task (DDT), the liability remains with them.

– For SAE driving automation level 3, the driver should remain sufficiently vigilant as to acknowledge the need for a transition as well as any vehicle warnings or mechanical failures. Assigning liability to either the driver or the system remains unclear.

– For SAE driving automation levels 4 and 5, the driver has handed control to the vehicle and bears no responsibility. The liability is with the vehicle manufacturer.

- Driver training

Training schemes should include flexible modules on new technologies to make drivers aware of the use and functions of such technology. The driving automation levels defined by SAE should become common knowledge among drivers and the wider transport community in the coming years. Steps to develop specific training courses on advanced vehicle and automated systems should be considered. Training should emphasise the potential benefits that advanced automated systems offer through their ability to support different driving tasks. It should also include information on the efficiency benefits and increased sustainability of transport operations that result from using automated driving systems.

The impact of connected and automated vehicles on social and road safety legislation will be significant. However, higher levels of automation will not address the current shortage of drivers, but it could make the job more attractive and encourage young people to join the profession.

b) Data (cybersecurity and software updates)

Considering the specificities of the commercial road transport sector, the ownership of data related to transport operations should remain with transport operators. This will ensure that, in the case of an accident, transport operators are in the best position to cooperate with other parties, such as road authorities. Clear provisions should be introduced that address the degree of liability of transport operators and contain definitions by use case.

The safety and security of users, both commercial transport operators and drivers, should always come first when addressing specific safety, cybersecurity, and privacy aspects, especially when they relate to potential on-board access to vehicle data. We recognise that vehicles generate a large amount of data that is not standardised but formatted differently depending on the manufacturer. As a result, neither the user, the manufacturer, nor third parties can make the best use of the data. Therefore, interoperability and standardisation are necessary so users can choose any third-party service provider of their choice.

As vehicles become increasingly connected and automated, the risk of cyberattacks increases. In the event of a connected and automated vehicle being hacked by a third party, it is uncertain which party would bear responsibility and, ultimately, be liable. Concerted efforts must therefore be made to minimise the risk of cyberattacks on connected and automated vehicles, ensure data security, and uphold privacy legislation.

c) Infrastructure readiness

Competent national authorities are increasingly promoting the real-life testing and operation of autonomous vehicles. Vehicle manufacturers are investing heavily in vehicle automation. Indeed, self-driving vehicles already operate in controlled environments, such as dedicated lanes in cities and ports. Pilot projects are underway in advanced economies with self-driving commercial vehicles, such as trucks, buses and taxis. Other mobility sub-sectors, such as metros, have already accumulated a substantial amount of experience and know-how in running automated operations. According to scientific studies and information from vehicle manufacturers, the number of driverless commercial vehicles will increase considerably over the next 10–20 years, becoming a permanent feature on our roads.

Governments should promote the option of creating regulatory sandboxes to develop effective regulation that promotes innovation and digitalisation through supervised testing of the functionality of autonomous vehicles.

The foreseen step-by-step introduction of autonomous vehicles in traffic will face a transition period where the coexistence of conventional and highly automated vehicles will have to be managed to ensure an uninterrupted level of safety and efficiency. Road infrastructure will play a major role in managing this transition period in terms of:

- new methods of traffic flow modelling following the introduction of autonomous vehicles.
- the design, upgraded and adaptation of “hybrid” infrastructure [able to support the coexistence of fully or partially automated (connected or autonomous) and conventional vehicles.
- new forms of visual and electronic signalling and optical guidance to ensure readability by both autonomous and conventional vehicles, and enable automated driving in adverse weather conditions.
- ways to enlarge the electronic road horizon of autonomous vehicles by ensuring timely reaction to hazards ahead (via real-time warnings and information, traffic management plans, up-to-date digital maps, etc.).
- new safety performance criteria for road infrastructure, with the goal to set the basis for the timely deployment of an automation-appropriate infrastructure network.

- the successful integration of AVs into the existing road network, facilitated by governments, as the coexistence of AVs with others road users must always be considered.

* * * * *