CertiCAV CP3 Responses

From the CertiCAV team at Connected Places Catapult

31st March 2021

#	Question / Answer
1	We provisionally propose that: (1) a vehicle should not be classified as self-driving if, with the ADS engaged, the user-in-charge needs to monitor the driving environment, the vehicle or the way it drives; (2) it is nevertheless compatible with self-driving to require the user-in-charge to respond to a clear and timely transition demand which: (a) cuts out any non-driving related screen use; (b) provides clear visual, audio and haptic signals; and (c) gives sufficient time to gain situational awareness. (3) to be classified as self-driving, the vehicle must be safe enough even if the human user does not intervene in response to any event except a clear and timely transition demand. Do you agree?
	We agree with points (1) and (2), and provisionally agree with (3). We note that, using the Koopman/Edge Case Research "automation modes", self-driving vehicles must be capable of either automated or autonomous mode operation. For point (2), the problematic area is likely to be what counts as sufficient time to gain situational awareness.
3	We provisionally propose that the decision whether a vehicle is sufficiently safe to "safely drive itself" should be made by the Secretary of State, as informed by advice from a specialist regulator. Do you agree?
	We did not consider legislature mechanism. However, in general we think that the approval of HAVs (Highly Automated Vehicles) should be based on clear technical requirements that are known to the ADSE in advance.
4	We welcome observations on which of the following standards is most appropriate when assessing the safety of automated vehicles: (a) as safe as a competent and careful human driver; (b) as safe as a human driver who does not cause a fault accident; (c) overall, safer than the average human driver.
	We agree that c) is unlikely to be sufficient on its own, but may have a role in combination with either a) or b). A vehicle which is less safe than the average human driver (in the same operating environment) seems unlikely to be acceptable to the public. Suggest that b) is desirable but some compromise may be necessary to make it technically achievable. For example basing the definition of 'at-fault' on a machine-verifiable technical standard rather than existing law. Additionally, while there is a mixed fleet of human drivers and AV, we wonder if adherence to this specification by itself would result in acceptable safety levels.

	We agree that option a) represents a very high bar for AV's, and yet at the same time a direct comparison to human performance risks limiting the ultimate safety of AV's to that of human drivers. We suspect applying statistical acceptance criteria for metrics may be a way forward, in combination with other methods as suggested above.
5	We welcome observations on how automated vehicles can be made as safe as reasonably practicable.
	We believe that to provide sufficient assurance requirements should be verifiable by formal methods, and therefore require components of conditions, limitations and certainty, and must reference formal performance indicators. These would have to go significantly beyond the example statements supplied in Qu4, which could support retrospective judgement of individual cases but are not 'standards' that can be applied to system assurance in the technical sense.
7	We provisionally propose that: (1) safety assessment should use a variety of techniques; (2) manufacturers/developers should submit a safety case to regulators showing why they believe that the automated driving system is safe; (3) regulators should: (a) provide guidelines for what is in the safety case; (b) audit the safety case; (c) prepare guidance for manufacturers and developers on preferred standards; and (d) carry out at least some independent tests. Do you agree?
	(1) - Yes (2) It is important to consistently stress the need for safety case to be a structured and systematic argumentation that demonstrates that requirements are met, backed up by evidence. Otherwise the use and effectiveness of safety case could be eroded. (3) (a) yes, and potentially regulations, and principles/objectives applied. (c) "preferred standards" might be too prescriptive until AD development and assurance is sufficiently covered by widely-accepted standards.
8	We seek views on whether an approval authority that intends to use a scenario database as part of the testing procedure should consult road user groups on the range of scenarios to be included.
	Depends on the objectives of the scenario testing. The goal should be to ensure that the vehicle will perform safely amongst all types of road users, and we support the principle of road user groups having a role in identifying scenarios. This should be supplemented by other means of scenario generation (e.g. on-road data gathering). It is not clear to us whether road user groups should be involved in determining which scenarios are actually selected for independent testing. A key role of this testing could be to validate the safety case produced by the ADSE, in which case scenario selection should be designed to identify possible weaknesses in the manufacturer's safety argument as efficiently as possible (bearing in mind that it is not possible to test everything). This might mean omitting from the test some scenarios which user groups reasonably see as important. For example, if the manufacturer provides a strong, evidenced argument that two groups of road users will be treated identically by the system, testing two versions of the same scenarios with different road users would be inefficient.

9	We provisionally propose that: (1) unauthorised automated driving systems should be prohibited; and (2) this should be subject to an exemption procedure by which the Secretary of State may authorise unauthorised systems to be used in tests and trials. Do you agree?
	Yes, provided it is introduced alongside defined and controlled governance of use of unauthorised vehicles in relation to vehicle testing.
10	We provisionally propose that: (1) the Government should establish a domestic scheme to approve automated driving systems (ADSs) for use on roads in Great Britain (a "national ADS approval scheme"); (2) manufacturers should have a free choice to apply for approval under either the UNECE system of international type approvals or through the national scheme; (3) developers should be able to submit an ADS for national approval, even if they are not responsible for manufacturing the whole vehicle. Do you agree?
	We disagree with points (1) and (3), because we see a close coupling between and ADS and the vehicle it is installed on (the HAV). While the majority of the software and hardware that comprise an ADS may be portable between vehicles, most safety outcomes are dependent on vehicle-specific attributes (such as sensor mounting points which affect field-of-view and propensity to gather debris on the sensors, braking capability, controller/actuator calibration, vehicle dimensions, etc). We agree that developers should be able to submit a HAV for approval even if they do not manufacture the whole vehicle. However, it may be preferrable if they took responsibility for the whole vehicle. The installation of an ADS is likely to affect many of the existing safety systems, and overall engineering, of the vehicle. For example, are the ADS actuators as reliable as the mechanical systems they replace? Do sensors affect the aerodynamics and cause handling issues? Do ADSE sensors block the view of OEM sensors? Does the ADS installation disable any existing electronic systems? Does installation of ADS cabling require drilling into the chassis? Do sensor mounting points cause additional stress on the bodyshell? Are there any (additional) risks from a roll-over event due to components mounted on the roof?
11	We provisionally propose that: (1) an ADS approval scheme should be established through regulation under the Road Traffic Act 1988, without further legislative reform; (2) an ADS should be defined as a combination of software, hardware and sensors, which can be installed in a "type" of vehicle; (3) when an ADS is approved, the approval should be accompanied by specifications for: (a) the type of vehicle in which it can be installed; and (b) how the ADS is installed within the vehicle; (4) where an ADS is installed in a pre-registered vehicle, an example vehicle should be submitted to the regulator for approval of the installation. Do you agree?

	We mainly disagree with this, for the reasons provided in our response to Qu10. We can see there would be benefits for both developers and regulators if evidence from approval of a HAV could be re-used for a different have fitted with the same ADS. But how this would work would have to be considered carefully.
13	We provisionally propose that: (1) once an ADS has received type approval at either international or domestic level, an Automated Driving System Entity (ADSE) would need to submit the vehicle to the UK safety regulator for categorisation as able to safely drive itself; (2) the safety regulator should make a recommendation to the Secretary of State for how the vehicle should be classified; (3) it should be open to the safety regulator to recommend that an ADS-enabled vehicle is classified in one of three ways: as not self-driving but driver assistance; as self-driving only with a user-in-charge; or as self-driving without a user-in-charge; (4) the safety regulator should only recommend classification as self-driving (either with or without a user-in-charge) if it is satisfied that: (a) an ADSE is registered as taking responsibility for the system; (b) the ADSE was closely involved in assessing safety and creating the safety case; and (c) the ADSE has sufficient funds accessible to the regulator to respond to improvement notices, to pay fines and to organise a recall. Do you agree?
	We disagree, as each mode of operation (self-driving categorisation) implies different requirements for vehicle design and functionality. Vehicles are unlikely to be suitable for a particular mode of operation unless they were designed for it. This means it is not possible to fully separate the two stages of approval. For example: An ADS designed for driver assistance only should make the user aware of its limitations. This should not be limited to marketing material but could also include (for example) restrictions on in-vehicle screen use and a system to monitor driver attentiveness. This would not be appropriate for the other two operation modes. Hypothetically, if the Secretary of State were to approve a HAV only for driver assistance when it had been designed and type-approved for automated mode driving, it would be unlikely to have the driver monitoring systems in place to ensure the attentiveness of the UIC. As far as safety is concerned, a better option could be to withhold approval completely. An ADS for UIC operation must be designed in such a way that it can safely be operated by an ordinary member of the public with minimal training. This might mean less acceptance of systems which need specialist maintenance or monitoring than for a NUIC vehicle. An ADS for NUIC operation must be capable of handling all situations without creating a transition demand, but could rely on the presence of a fleet operator or external monitoring systems.
17	We provisionally propose that legislation should establish a scheme to assure the safety of automated driving systems following deployment, giving scheme regulators enhanced responsibilities and powers. Do you agree?

	Yes. Especially for the first few generations of automated vehicle, while pre-deployment testing processes are still being refined, there is a very real possibility of vehicles being approved which are shown to be unsafe after deployment. It is important that there are mechanisms to require improvements, withdraw approvals and update standards for future approvals based on operational experience.
18	We provisionally propose that the enhanced scheme should give regulators the following responsibilities and powers: (1) scheme regulators should be responsible for comparing the safety of automated and conventional vehicles using a range of measures; (2) to do this the regulator should have power to collect information on: (a) leading measures (instances of bad driving which could have led to harm) and (b) lagging measures (outcomes which led to actual harm); (3) regulators should have power to require an ADSE: (a) to update software where an update is needed to ensure safety and continued compliance with the law; (b) to keep maps up-to-date, where an AV relies on maps to ensure safety and compliance with the law; (c) to communicate information about an ADS to users in a clear and effective way, including where necessary through training. Do you agree?
	We agree. Regulators should have powers to ensure that vehicles are meeting the expected standards in real operations. Pre-deployment testing can be thought of as an initial check that the standards are likely to be met, but this cannot be guaranteed until real operational experience is gained. Note that 3(c) may have some implications for consumer protection - should a manufacturer be able to require second-hand car buyers to take a (paid for) training course, for example? This regulatory approach relies on consumer training to ensure safety for a potentially large number of AD systems, each with different ODDs and HMI. An alternative option could be to define a smaller set of allowable ODDs/features for HAVs (as has effectively be done for ALKS).
19	We welcome views on the following issues: (1) Should scheme regulators be empowered to approve software updates that apply only within the UK, without requiring the manufacturer to return to the original type approval authority? (2) Should the scheme should also deal with cybersecurity? (3) Are other powers needed? (Note that data is discussed in Chapter 17.)
	We agree that, regardless of the national/international considerations, it is essential to manage change control for HAVs. We note for points (1) that there is potentially a grey area between 'software' and 'maps' that covers other data used by the ADS in performing the DDT. For example, an ADS might store the rules-of-the-road as a configuration file, and a change to the rules-of-the-road may not need any code changes. They could potentially argue that this was neither a map or a software update (and escape any regulatory assurance requirements). On the other hand, the rules-of-the-road could be coded tightly into the core ADS algorithms. In that case, updating the rules-of-the-road would be very likely to have an effect on ADS behaviour in all countries, and not just the one where the rules changed.

21	What formal mechanisms could be used to ensure that the regulator administering the scheme is open to external views (such as duties to consult or an advisory committee)?
	We believe that an independent investigation body could contribute to this (see also response to question 25). In the aviation, marine and rail industries these bodies have specialist expertise to investigate accidents and publish detailed, public-facing reports. They can address their recommendations to any organisation in the industry, including the regulator. The large number of road vehicles means this approach might not apply directly, but such a body could still have a role in investigating the most serious accidents or a random sample.
23	We provisionally propose that the regulator which assures the safety of AVs in-use should have powers to impose the following sanctions on ADSEs: (1) informal and formal warnings; (2) fines; (3) redress orders; (4) compliance orders; (5) suspension of authorisation; (6) withdrawal of authorisation; and (7) recommendation of attendance at a restorative conference. Do you agree?
	Agree that all of these options should be available. Suggest that the regulator should be able to (at least) require improvements or suspend authorisation wherever an ADS is believed to be operating outside of the agreed requirements, even if there is no suggestion of malice or neglect (i.e. the sanction is for the protection of the public, not as a punishment). We feel that there are many potential options for balancing independence and powers to apply sanctions between the pre-deployment regulator, the in-use regulator, and the collision investigation body.
25	We provisionally propose that a specialist collision investigation unit should be established: (1) to analyse data on collisions involving automated vehicles; (2) to investigate the most serious, complex or high-profile collisions; and (3) to make recommendations to improve safety without allocating blame. Do you agree?

	Yes. We note that AVs will operate in a mixed environment, amongst vehicles controlled by humans and on roads designed and maintained by local traffic authorities. An investigation body may need to make recommendations to any stakeholder in this system. We agree that the police have significant experience and expertise in attending to and investigating collisions involving human-driven vehicles. This will continue to be vital to investigating potential HAV incidents, and understanding what happened in them (although the "what" will be potentially be simpler given the potential of HAVs to record data). However, understanding **why** a collision involving a HAV occurred will require an additional skillset covering AI, robotics, and error finding in complex software systems. Therefore we suggest that a specialist body is needed, but it should work very closely with police traffic investigation units. Additionally, this body should have a responsibility to feed findings back to the pre-deployment and in-use regulators (and they should have a responsibility to act on recommendations).
27	We welcome views on: (1) the issues the forum should consider; (2) the composition of the forum; and (3) its processes for public engagement.
	We suggest there are two key parts to this work: defining what the rules mean, and defining when it might be acceptable to not comply with them. Aim should be to reach a consensus on the meaning of as many rules as possible. Forum should separately aim to set out principles for when non-compliance may be tolerated. Another consideration is that this is an international problem (and the differences in traffic regulations between countries are relatively insignificant compared to the challenge of implementing them for HAVs). Therefore, any forum should establish links with the international community working on this problem. We also believe that there may be a role for a set of rules less directly based on the current ones. This could be a formal, logical specification with the goal of ensuring that automated vehicles from different manufacturers will not collide with each other. This might look more like (for example) Mobileye's RSS concept than the current highway code.
29	We provisionally propose that following the end of the transition demand period: (1) the user-in-charge should re-acquire the legal obligations of a driver, whether or not they have taken control of the vehicle; and (2) if, following a failure to respond to a transition demand, the vehicle stops in a manner which constitutes a criminal offence, the user-in-charge should be considered a driver and should therefore be liable for that offence. Do you agree?

	We are concerned that this is highly dependent on the time allowed for the UIC to gain situational awareness, and the degree of distraction they had prior to the transition demand. The "end of the transition demand period" may not give them time to assess and respond to the critical situation that triggered the demand. Would this requirement mean that UIC vehicles must have a driver monitoring system (DMS)? If so, what should the ADS do when the UIC is unresponsive – execute an MRM (and make the UIC liable for the consequences)? If the vehicle does not have a DMS, there is a significant burden on the UIC to remain alert and awake, despite having no task to perform or monitor, and no electronic systems to ensure they remain awake and alert.
33	We seek views on whether the new proposed offence of being carried without a user-in-charge should only apply if the person: (1) knew that the vehicle did not have a user-in-charge; and (2) knew or ought to have known that a user-in-charge was required
	We wonder if this complex topic could be resolved at a technical level instead. For example, regulations could require that a UIC HAV must detect an alert human occupying the driver's seat before commencing a journey.
34	We provisionally propose that a user-in-charge who takes over control of the vehicle: (1) should be considered a driver; but (2) should have a specific defence to a criminal offence if, given the actions of the ADS, a competent and careful driver could not have avoided the offence. Do you agree? If not, we welcome views on alternative legal tests.
	We tentatively disagree with this (see also response to Qu29). This could result in the UIC being held at fault in cases where their driving was poor as a result of a rushed handover. For example, if a driver looks up from a secondary activity to see an immediate risk of collision, they are likely to try to take over without having had time to re-engage with the driving task. In this situation, their best efforts to avoid a crash may fall below the standard of a driver who is already fully engaged. Criminalising this behaviour is unlikely to be an effective deterrent and may not improve safety.
37	We provisionally propose that: (1) where an individual is exercising lateral and longitudinal control (steering and braking) over a vehicle remotely, that should not be regarded as a form of "self-driving"; and (2) where lateral and longitudinal control are exercised by an ADS, all other forms of remote operation should be regulated as "self-driving". Do you agree? We welcome views on whether the current definition of when a vehicle "drives itself" under the Automated and Electric Vehicles Act 2018 should be amended to deal with some forms of remote operation which may involve a degree of "monitoring".
	Our comments are that this is a complex area. Is the intention that a UIC vehicle must always have driver controls, and a NUIC vehicle must never have driver controls? Remote operators and privately-owned NUICs could potentially render the converse true.
39	We welcome views on whether NUIC operators should be required to demonstrate professional competence through a safety management system, as set out in a safety case.

	Agree with the principle of organisational, rather than individual, competence. The skills required may be too diverse to expect one individual to be competent in all aspects of operation. However the safety management system should define individual roles with clear responsibilities and competence requirements.
40	We provisionally propose that, irrespective of the nature of the vehicle, a licensed operator should be under a duty to: (1) supervise the vehicle; (2) maintain the vehicle; (3) insure the vehicle; (4) install safety-critical updates and maintain cybersecurity; and (5) report accidents and untoward events (as defined by the regulator). Do you agree?
	We feel this requires clarification. We note that vehicles with NUIC capability may also be capable of other modes of operation, including manual (e.g. a self-delivering hire car). It should be carefully considered whether these responsibilities depend on the vehicle's capability, operator (e.g. LFO) or mode of operation.
41	We provisionally propose that legislation should include a regulation-making power by which some or all of these duties could be transferred to the registered keeper or owner, if it was shown that it was appropriate to do so. Do you agree?
	We note that the service should be accessible, but potentially every vehicle operated by the HARPS need not be.
45	We seek views on the following proposed offences. Offence A: non-disclosure and misleading information in the safety case Offence B: non-disclosure and misleading information in responding to requests Offence C: offences by senior management Offence D: aggravated offences in the event of death or serious injury following non-disclosure or provision of misleading information to the AV safety regulator
	We note that, for Offence B, the regulator could demand information that is highly commercially sensitive. The ADSE should have assurances that this information will only be demanded when necessary, and it will be managed appropriately. For Offence C, we agree but feel that “senior management” should refer to only the highest level of management within an organisation (a handful of individuals).
53	We provisionally propose that measures should be put in place to compensate the victims of accidents caused by uninsured AVs. Do you agree?
	We wonder if there is a technical solution possible here, for example a public authority could maintain a database of all HAVs that are insured. Then an approval requirement for an ADS would be that it connect to this database to confirm it is insured before commencing any journey.

55	We provisionally propose that: (1) for a vehicle to be classified as self-driving, it needs to record the location as well as the time at which the ADS is activated and deactivated; (2) the Government should work within the UNECE to ensure data storage systems for automated driving record these data; and (3) any national system to approve an ADS should require these data to be collected, subject to safeguards. Do you agree?
	We agree with this, and suspect that even for police traffic investigations, it may be necessary to know the location of the vehicle to confirm it was the vehicle involved in the collision. It also seems likely that collision investigations may require data to be recorded over and above the timestamp, location, and ADS activation status.
58	We provisionally propose that: (1) when an ADSE applies for categorisation of its vehicle types as self-driving, it should present the regulator with details on how data will be recorded, stored, accessed and protected; (2) the regulator should only categorise a system as self-driving if it is satisfied that that the ADSE has systems to abide by its obligations under the GDPR. Do you agree?
	Yes, we fully agree with these proposals.