

Response to the Law Commission and Scottish Law Commissions' third joint consultation paper of automated vehicles.

Author: *National Engineering Policy Centre* on behalf of the engineering profession

Date: March 2021

Contents

Introduction
Major concerns
Responses to selected consultation questions
Abbreviations

Introduction

This document is a response by the National Engineering Policy Centre (NEPC)¹ to the questions raised by the Law Commission and Scottish Law Commission (Referred to as the Law Commissions) in their document: *Automated Vehicles: [Consultation Paper 3 - A regulatory framework for automated Vehicles: A joint consultation paper](#)*.

We believe that engineers and technology developers need to work with the legal profession to manage this complex and rapidly evolving technology, and we welcome the opportunity to input to the Law Commission's review. This paper comments on only on those questions which were considered to affect the engineering profession.

Key messages

Our main messages are:

- It is important that new or revised regulation in the UK should not become a barrier for UK based developers that puts them at a disadvantage compared to other countries. However, regulations and regulators that are outcome-focused, risk-informed and aware of the engineering realities, can be an enabler of safe and ethical autonomous vehicle (AV) development.²

¹ National Engineering Policy Centre is a unified voice for 43 professional engineering organisations, representing 450,000 engineers, a partnership led by the Royal Academy of Engineering. We give policymakers a single route to advice from across the engineering profession. We inform and respond to policy issues of national importance, for the benefit of society

² National Engineering Policy Centre (2020) [Safety and ethics of autonomous systems: project overview](#)

- We agree strongly with the need for a wide review of product liability. The legal liabilities of all technical personnel involved with control systems are currently clear. Technical developments in autonomous systems will undermine the current basis for assigning responsibilities for their performance.
- Comparisons of the safety of automated and autonomous systems with human behaviour to set design requirements is an extremely complex problem. We suggest that the Law Commissions work closely with the engineering profession to ensure the regulations are implementable.
- Regulations will need to evolve with both the AV technology and the increasing sophistication of the verification techniques available.
- UK legislation should recognise that autonomous vehicle (AV) technology is under development for future international markets with commercial pressures only allowing small variations for national requirements.

Responses to selected consultation questions

Consultation Question 1 (Paragraph 4.114)

18.1 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?

NEPC Response

The consultation paper recognises the problem of terminology in Paragraph 4.6:

Different sources use different terminology. Although the SAE refer to an alert given by a Level 3 system as “a request to intervene”, this may understate its importance. The UN Regulation on Automated Lane Keeping refers to a “transition demand”³. This gives a clearer picture of the significance of the alert, and we have adopted the term “transition demand” in this paper.

Although we understand the reasons to define a new term “transition demand” for consistency within a document, this does not help from the perspective of the system designers. They must interpret whichever term is used and write quantitative requirements that can be tested. It must also be recognised that the SAE autonomy levels have drawbacks. They are widely quoted but are only one of at least eleven different definitions of

³ UN Regulation 157 on uniform provision concerning the approval of vehicles with regards to Automated lane Keeping System ECE/TRANS/WP.29/2020/81 (ALKS Regulation), para 2.2.

autonomy levels used in different applications⁴. This range of definitions is necessary in order to write testable, and verifiable requirements for products in a particular application field.

A key question for design engineers and their employers is the extent of their responsibilities when their product is used. This helps clarify who is considered responsible for the consequences of the systems actions. The transition time should mark the point at which responsibility is passed from the ADS to the driver and *vice versa*.

We agree with the idea behind your **proposal (1)** that a car is not self-driving when the driver has to monitor the environment.

Proposal (2) introduces complications as it leads to a period of time when the car expects the driver to react, but they have a reaction time of seconds or tens of seconds to make a safe response. The car's motion will continue during this time. Where does the responsibility for its action lie? The consultation document, in paragraph 4.49 states that an automated (as against self-driving) car supports an outcome of:

(c) A safe, predictable transition phase, which includes sufficient lead time for the driver to complete a safe process to take dynamic control

The responsibility for the car's behaviour during this time remains with the ADSE, as such the responsibility lies with the designer. There is a need to better define what is meant by sufficient time and the conditions for transfer to occur. The hand-over should only occur once the system believes the driver is capable of safely taking over control of the vehicle, in this context capable needs to be further specified. An ethical black box model that uses in vehicle sensing could potentially help define the status of the driver during transition requests (e.g., is the driver sleeping, sick, unconscious?).

In a scenario where the car starts to decelerate whilst continuing in its road lane, but the competent driver reacts as quickly as they can based on their view that the safest action is to change direction, or even accelerate, who has responsibility for the consequences of the next events?

It is crucial at the stage of initial certification of any autonomous system, to not only assess its capabilities in autonomous mode, but also how it will interact with the human operator, the role for a standard interface should be considered. There also must be clarity and transparency as to what features can be customised, disabled or overridden by users. The implications for inclusion must also be considered as their ability to react may pose a greater risk with some users⁵ and exclude other users entirely.

As the term 'safe enough' in **proposal (3)** is better defined this should be supported with the validation criteria required to show this threshold has been met.

Consultation Question 3 (Paragraph 5.118)

18.3 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?

⁴ Gillespie, Tony, *Systems Engineering for Autonomous Systems*, Scitech 2019, Appendix A3 Definitions of Autonomy and Autonomy Levels

⁵ Li S, Blythe P, Guo W, Namdeo A. [Investigation of older drivers' requirements of the human-machine interaction in highly automated vehicles](https://doi.org/10.1016/j.trf.2019.02.009). *Transportation Research Part F: Traffic Psychology and Behaviour* 2019, **62**, 546-563. DOI: <https://doi.org/10.1016/j.trf.2019.02.009>

NEPC Response

A decision that a vehicle can “safely drive itself” has the consequence that its design must be reviewed against the relevant safety case. Consideration must be given to how this is maintained throughout the lifespan of an AV. If the design incorporates previous hardware and software components, there will need to be consideration of the division of liabilities between the original designers and the regulator’s technical assessors.

Consultation Question 4 (Paragraph 5.119)

18.4 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.

Consultation Question 5 (Paragraph 5.120)

18.5 We welcome observations on how automated vehicles can be made as safe as reasonably practicable.

NEPC Response to Questions 4 and 5

Defining “safe” as a basis for assessing an automated design is problematic for engineering design as it must be verifiable in a way that is acceptable both technically and legally. Similar problems arise when defining the characteristics of the three humans given in Question 4 a, b and c.

We agree with paragraph 5.5 that the assessment of an AV’s safety should be based on a balance of:

1. as safe as reasonably practicable;
2. as safe as a competent and careful human driver;
3. does not cause a fault accident;
4. and a positive risk balance (so that, overall, AVs are safer than the average human driver).

but disagree with Question 4 as it does not include consideration of what is reasonably practicable.

As Low As Reasonably Practicable (ALARP) is good engineering practice used as a basis of assessing a design at all stages of its life cycle. Every new design must start with precise and quantified requirements. As the report recognises, the challenge for the engineering profession is quantifying these qualitative requirements. An ALARP approach based on a risk assessment can provide this assessment. The ALARP principle is likely to include an obligation for the system to identify complex or unusual circumstances to the operator to enable control to be handed back. The risk assessment should be reviewed by the regulatory authority at an early stage. As the design evolves, other criteria can be incorporated.

While ALARP can be a powerful tool this principle can be interpreted differently amongst regulators, engineers, and across sectors. Additionally, what is “reasonably practicable” in terms of safety analysis is likely to evolve with new generations of autonomous vehicles. How ALARP should be interpreted for an ADS should be clearly defined, working in collaboration with developers.

The Globally At Least As Good (GAMAB or GAME) approach should also be considered as it requires that all new guided transport systems must provide a level of risk at least as good

as the one offered by any equivalent existing system. This is the approach being taken by the CAA in CAP 722 for Unmanned Aircraft Systems.

For these assessments it will be important to consider that the mistakes made by an AV will be different to those made by a human driver so comparison to a hypothetical reasonable human may prove challenging.

The Law Commissions may wish to raise this issue with the Civil Aviation Authority (CAA) as they had comparable problems when comparing Unmanned Air Vehicle (UAV) collision avoidance requirements with the actual performance of human pilots. We recognise the specific challenges are different but believe there will be opportunities to share learning.

Consultation Question 6 (Paragraph 5.121)

18.6 We welcome practical suggestions for how AV regulators can fulfil their public sector equality duty.

NEPC Response to Question 6

The problem is broader than automated vehicles, it is a subset of the wider issues of the ethics of Artificial Intelligence (AI) and its application to autonomous systems. There are national and international initiatives addressing these, but they have not yet reached agreed approaches. In particular the British Standards Institution BS8611, Guide to the ethical design and application of robots and robotic systems, should be central to ethical assessments.

Consultation Question 16 (Paragraph 8.83)

18.16 We seek views on whether the regulator that classifies vehicles as self-driving should have power to allow their deployment in limited numbers, so as to gather further data on their safety in real world conditions.

NEPC Response to Question 16

We consider that methods to verify new or changed vehicles in real world conditions are essential; these should go beyond safety. Such verifications must be carried out in a regulated manner in order to ensure safety of the vehicle, pedestrians and other road users, and credibility of the results for later assessment by testers and regulators. The regulatory body for these tests could, but not necessarily, be the one suggested here.

The data captured in real world testing should be collected for clearly stated purposes and standardised to make it accessible to those who could use it to improve their software systems, while preserving intellectual property. Regulations should be put in place for obliging companies to share data on incidents, near-miss and other aspects of AVs deriving from road tests. Accident/incident investigation is common practice in the other transport modes and provides an important neutral information sharing function that enables lessons to be learned across the sector.

Consultation Question 17 (Paragraph 10.82)

18.17 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?"

NEPC Response to Question 17

Extensive testing should be a requirement for achieving any suitable certification. Transparency and data sharing between the international stakeholders should also be encouraged to aid the understanding of the potential risks. However, data ownership and IP matters will need to be managed accordingly.

Consultation Question 18 (Paragraph 10.83)

18.18 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?

NEPC Response to Question 18

We agree that the regulator should have these powers.

The Law Commissions should consider what constitutes necessary data and information and how it is collected. As pointed out in the paper, the UN is currently working on EDR and Data Storage System for Autonomous Driving (DSSAD). However, EDR and DSSAD lack location data, which is necessary for accident reconstruction and legal investigation, but problematic for privacy reasons.

Data may be available from the ADS and ADSE, but without regulations this will be under the control of the manufacturer or ADSE. Strong consideration should be given to mandating an EDR similar to an aircraft or railway “black box”, that requires explainability. The current proposals of EDR and DSSAD should be reviewed to test the legal usefulness of datasets derived and specify the requirements for underlying standards for data that is collected within a “black box”.

Note also that when a map forms part of the AV’s guidance system it has safety and integrity requirements. This implies that map sources must be certified as reliable, with publicly available accuracies and shortcomings.

The regulator must also consider the integrity of real-time updates to on-board information such as road works. A self-driving car will also need a high level of certainty that it is receiving all relevant information for the journey. Lower integrity levels may be acceptable for automated cars, but the driver will need to understand this and their responsibilities to interpret that information.

Data collection on the configuration of software, its internal state and communications between components may also prove important.

Consultation Question 19 (Paragraph 10.84)

18.19 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.)

NEPC Response to Question 19

We make the following comments on the issues in this question:

(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?

No, unless compelling reasons are given by the ADSE. For example, these could be for controlled tests with a safety case and risk assessment. The justification for our 'no' response is that the original type-approval authority will have, or have access to, data that the UK authority may not. A well-known example is the loss of the Ariane 3 launcher in 1996⁶ when software that was safe in a 16 bit processor was reused in a 64 bit processor and no longer safe.

It is unlikely that cars with UK-only software will remain in the UK, so they will need to operate safely and legitimately in other regulatory regimes.

(2) Should the scheme should also deal with cybersecurity?

Yes, the scheme should not go ahead without consideration of cyber security as there are a range of cyber attacks that need to be assessed and mitigated for. It is highly likely that automated cars will have at least one external datalink which presents a cyber security risk.

(3) Are other powers needed? (Note that data is discussed in Chapter 17.)

The regulator must have powers to approve data used as part of the ADS' guidance system. The most obvious example is maps, a human can interpret the display based on experience and observation of their environment to resolve any ambiguities; an ADS which expects a map of a minimum quality may not correctly interpret a lower quality map. Road-condition updates or police instructions are other examples of data which will require on-board authorisation before being acted on.

The regulator must be able to inspect and approve the mechanisms for modifying embedded software during use. In particular, the regulator must be assured that any dynamic changes in software behaviour have been assessed to be safe.

Consultation Question 20 (Paragraph 10.100)

18.20 Should the authority administering the scheme to assure safety while automated vehicles are in use be kept separate from type approval authorities (as is already the case)? Alternatively, should both functions be combined in a single body?

NEPC Response to Question 20

Our strong opinion is that the safety scheme administrators and type-approval authorities should be kept separate to ensure that safety considerations are not compromised by the pressures often seen in type approval.

⁶ Ariane 501 Inquiry Board Report. Available at: <http://esamultimedia.esa.int/docs/esa-x-1819eng.pdf>

Consultation Question 36 (Paragraph 12.95)

18.36 We provisionally propose that the legislation should include a regulation-making power to clarify those roadworthiness failings which are (and those which are not) the responsibility of the user-in-charge.

Do you agree?

NEPC Response to Question 36

We agree strongly. Clarity for the responsibilities for roadworthiness will ensure that engineers and their management can identify their roles and include meeting them as part of their organisational processes.

Consultation Question 38 (Paragraph 13.86)

18.39 We provisionally propose that:

(4) the regulation of self-driving vehicles should distinguish between an Automated Driving System Entity (which vouches for the design of the system) and an operator (responsible for the operation of individual vehicles);

(5) all vehicles authorised for use on roads or other public places with no user-in-charge should either:

(a) be operated by a licensed operator; or

(b) be covered by a contract with a licensed operator for supervision and maintenance services;

(6) it should be a criminal offence to use a NUIC vehicle on a road or other public place unless it is operated by a licensed operator or is covered by a contract with a licensed operator for supervision and maintenance services.

Do you agree?

NEPC Response to Question 38

We agree in principle with this proposal but consider that regulations will need to evolve considerably as the ADS technology and the sophistication of the verification mechanisms evolve.

Consultation Question 44 (Paragraph 14.107)

18.46 We provisionally propose that:

(1) it should be a criminal offence for an ADSE to omit safety-relevant information or include misleading information when putting a vehicle forward for classification as self-driving or responding to information requests from the regulator;

(2) the offence should apply to senior managers (where it was attributable to the manager's consent, connivance or neglect);

(3) the offence should not apply to more junior employees;

(4) the offence should carry a higher sentence if it is associated with a death or serious injury;

(5) the offence should be prosecuted in England and Wales by either the regulator or the Crown Prosecution Service and in Scotland by the Procurator Fiscal.

Do you agree?

Consultation Question 45 (Paragraph 14.108)

18.47 We seek views on the following proposed offences.

(Then a set of detailed offences)

NEPC Response to Questions 44 and 45

We assume that professional engineers will follow their relevant Code of Conduct which includes obeying the law, with provisions for whistle-blowing.

Consultation Question 46 (Paragraph 14.109)

18.48 We welcome views on whether an ADSE should be under a duty to present information in a clear and accessible form, in which safety-critical information is indexed and signposted.

NEPC Response to Question 46

We strongly agree that transparency is key. It is good practice and is a standard contract requirement in many, if not all fields of engineering.

Consultation Question 52 (Paragraph 16.24)

18.54 We provisionally propose that the way the Automated and Electric Vehicles Act 2018 deals with contributory negligence and causation is:

- (1) adequate at this stage; and
- (2) should be reviewed by the UK Government in the light of practical experience.

Do you agree?

NEPC Response to Question 52

We do not wish to comment on the operation of the act to date. Should there be a review, we suggest that this should include:

- The responsibilities and liabilities through the supply chain.
- The responsibilities of designers and their organisations.
- The legal status of highly-automated vehicles with many autonomous features and may be capable of self-driving in many circumstances.
- The suite of verification techniques and their efficacy

Consultation Question 53 (Paragraph 16.32)

18.55 We provisionally propose that measures should be put in place to compensate the victims of accidents caused by uninsured AVs.

Do you agree?

NEPC Response to Question 53

We do not wish to agree or disagree. How the AV could be connected to the DVLA database and restrict its use, using its ADAS, could be explored as a technical mitigation with consideration of public acceptability.

The role for non-fault model such as New Zealand's No-Fault Accident Compensation Scheme could be explored to overcome difficulties in attribution of "defects" and "faults" in collisions involving complex autonomous systems to ensure just settlements.

Consultation Question 54 (Paragraph 16.47)

18.56 We provisionally propose that:

- (1) product liability law should be reviewed to take account of the challenges of emerging technologies;
- (2) any review should cover product liability as a whole, rather than be confined to automated vehicles; it should not, therefore, form part of this project on automated vehicles.

Do you agree?

NEPC Response Question 54

We agree strongly with a wide review of product liability. It must cover the responsibilities of all organisations and employers specifying, designing and using autonomous systems and other emerging technologies. Although it may be possible to find 'local' solutions to ADS problems, similar issues will arise for every autonomous system that has close interactions with humans.

Autonomous systems are becoming increasingly prevalent and these often respond to inputs in a way that is not necessarily predictable to the user. This contrasts with more traditional deterministic systems which will reliably give the same response to the same inputs and hence is predictable to its user and other entities.

Every autonomous system's behaviour depends on the design and verification of its original algorithms, but these behaviours may change if it uses machine learning methods. Achieving a human understanding of why a particular decision was made by an autonomous system is an important ongoing area of research. There are numerous examples of learning systems being fooled by simple changes to their input information, for this scenario is the original designer responsible for flawed reasoning in circumstances which are not identical to the algorithms' original tests?

We are concerned about liabilities for the behaviour of all non-deterministic processes used in control systems and the division between designer, supplier, maintainer and user. Boundaries need to be established based on legal and technical considerations. Consider Figures 2.1 and 13.1 in the Law Commissions' report; all ADS behaviours, AV control systems and transition facilitation decisions are set by designs based on engineering specifications. Obtaining initial regulatory approval is the responsibility of employees in the ADSE. However for maintenance, a Fleet Operator responsibility will include software updates, some of which will change ADS behaviour. Are the original designers responsible for making their software compatible with all future updates? Will the regulator-approved tests on limiting behaviours need to be repeated whenever new software or data from a new supplier is installed? What are the responsibilities of individual engineers either as a designer or as a technical manager authorising the company processes to deliver a safe product upgrade? Which company has final design authority for an update from a new supplier to a subsystem from an OEM that either has closed down or changed market?

These issues apply to most autonomous systems and are sufficiently complex both technically and legally to justify detailed discussions with both professions.

Consultation Question 58 (Paragraph 17.95)

18.60 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?

NEPC Response to Question 58

We agree with this as far as it goes, and the procedure concerning recording, storing, processing, accessing and protecting data should be standardised and collected with a clear purpose. However, we advise that the word 'accessed' is insufficient as it may be interpreted as simply a technical description of the data and communication standards used. The provenance of the accessed data needs to be considered as part of this. Inadvertent or deliberate use of data from uncertain sources for ADS decisions has a high probability of producing unreasonable behaviour. There must be a secure method of verifying that incoming information is from a reliable source. Consider the example of traffic information or police requests for a vehicle to stop; these must have valid provenance for legitimate action by the ADS. The requirement for valid provenance is recognised in international law for weapon targeting where all data used as a basis for weapon release must have known provenance.

The Law Commissions and regulators must recognise the international nature of the AV research, development, and manufacturing industries. Intellectual property is a valuable commodity, with commercial considerations causing companies to refuse to give adequate detail for testing compliance with national regulations. Unwillingness to conform to the standards may pose challenges to certification of the AV safety.

The Law Commission may wish to consider the role for a concept similar to that of critical functions for Lethal Autonomous Weapon Systems (LAWS). This was introduced by the International Committee of the Red Cross (ICRC) to overcome problems with giving one autonomy level to a system when, in practice, different parts of the system are at different autonomy levels. It makes it easier to look at regulations for specific functions that form part of the authorised decision chain.

List of abbreviations

ADAS: Advanced Driver-Assistance Systems
ADS: Automated Driving System.
ADSE: Automated Driving System Entity.
ALARP: as low as reasonably practicable.
AV: automated vehicle.
BSI: British Standards Institution.
CAA: Civil Aviation Authority.
EC: Engineering Council
EDR: Event Data Recorder
LAWS: Lethal Autonomous Weapons
NEPC: National Engineering Policy Centre
OEM: Original Equipment Manufacturer.
RAEng: Royal Academy of Engineering.
UAV: Unmanned Air Vehicle.
UN: United Nations