CAV safety and legal framework

As an ex-aerospace engineer and automotive engineer, I have some understanding of the systems involved in assuring safety in aircraft and automotive design. The implementation of failsafe and failure mode analysis and the calculation of risks. The legal liability and best practice to ensure that lessons are learnt and safety is continuously improved.

[redacted]

I would like to draw the Law commissions attention to recent events involving the Boeing 737 Max for which there is a congressional report outlining failures and changes to proposed to remedy these failures. I would say that this is particularly pertinent as the failure was due to autonomous control of the aircraft, the system design of these aircraft elements and their interaction with human factors.

Hardware safety, Software safety, Man-Machine interface.

The aerospace analogy is in some respects simplistic; a AV often occupies an urban space which is much more complex. It is already the case that more people die from being hit by cars than drivers or passengers. As such a greater regard needs to be taken for the external risks than the internal ones.

Analysis

Recent Boeing 737 history points to problems due to incomplete oversight.

UK only law

The foresight report recommended that standards be global as the costs of certification will be high and it is preferrable that only one process is required.

“The harmonisation of regulations and standards removes the complexity and cost to conform with varying local standards.” https://www.futureautonomous.org/

Social Impact

Proposed law issues

“causing death by dangerous driving. Instead, the issue would be a regulatory matter, to be resolved between the safety assurance regulator and the entity responsible.”

How?

The task for the safety assurance regulator would be near impossible.

Why would the entity responsible cooperate if it knows it was at fault. I note that Grenfell enquiry has had to give immunity in order to gain testimony, and now we can see clear culpability of some parties. This system of deregulation has served business over users, and I posit that Self driving is a much more complex environment. Millions of lines of code to understand if software was cause. Difficult to find cause post mortem, and then to attribute.

In regard to your questions;

Qu. 1

No (2) Some people can sleep and be very difficult to wake, even with noise and shaking.

This is fundamental and the data that you present really backs this up. Lack of attention leads to drowsiness. (2.19) I suggest that there is no safe middle ground. Further the lack of driving practice will degrade driver performance and could make them less able to drive safely.

Qu.2

Yes

Qu 3.

No.

IMO, the target is as H&S standard as safe as reasonably practicable. The Aviation industry has good practice in that the failure rate target for new aircraft is based on better than the last and an aim of zero. This is in no way a political decision and should be scientific. Probably a board of technical experts with a clear mandate to improve road safety for all users, without bias as you outlined. I worry that AVs will bias against pedestrians and cyclists are cars do now.

Qu. 4

The target is as H&S standard as safe as reasonably practicable. As stated above the target needs to move with time to be improving with technology and learning. Aviation law may help here, see also lessons from 737 Max.

Qu5. Aerospace safety system analysis. See 737 Max learning

Qu.6. Start by looking at road deaths. Pedestrians, cyclists and motorcyclists are at most risk. Please note that the higher energy of speed and mass add to the danger, such that heavier faster vehicles need greater scrutiny and better systems. The starship robots in MK weighing 20kg and going 8mph are very lightly regulated, if at all, with few incidents reported.

The non-human behaviour of starships robots is an issue. They do not drive like a human and can surprise other path users. This can be detrimental to the smooth flow. They are apt to stop in aukward places causing hazards.

Qu.7 This needs expanding. There are multiple disciplines here and numerical probabllity needs to be included see aerospace analyses.

Qu.8 Clearly. Cyclists are particularly vulnerable as they come in many shapes and sizes and are difficult for sensors and software to identify. In some respect the Automatic vehicle should need clear view around it in order to proceed as a bike appearing at the last minute from behind another object is a concerning scenario. Humans may anticipate cyclists based on seeing prior to being hidden etc. Strange un human driving style also needs to be considered. Sudden braking or swerving can cause accidents and this is an area that needs study.

Qu.9

(1) Yes, my Tesla Model 3 cruise control is not safe. It brakes due to shadows.
(2) No Secretary of state has no place in this complex safety arena.

Qu.10

(1) No. Emphatically unsafe suggestion. Completely bypassing a proven safety system is madness.
(2) No. There is more logic in supporting an international standard as manufacturers will then be willing to commit more resources to achieving approval in wider market.
(3) No. The system needs to be assured. It is difficult to assert responsibility when multiple parties are involved.

Qu.11

No. This is a safety system. A vehicle cannot be retrofitted with ADAS capability. The hardware and software need to be compatible. Please note that Uber switched off Volvo's AEB system as it added its own sensors. Volvo's sensors would not have prevented the accident in Tulsa, Arizona. To override the base cars logic is to remove a layer of safety that has been approved by regulators. This was an error that should not be repeated.

Qu. 13

No.

The approval by SoS is inappropriate. This is a technical area requiring specialist system knowledge. A SoS is unlikely to be adequately skilled to judge.

The safety regulator needs clear definition of responsibilities and powers before this system can be judged as safe. Further funds are not only requirement of an entity to be safe. They need to have competent professional experts. Aerospace industry and 737 Max have shown that human factors, organisation and clear responsibilities are vitally important factors.

Qu. 14

Well yes but this is far to open. Please see comments Qu 13. Further there are differences between a 40 tonne trucks travelling at 50 mph, a 20Kg robot moving 8mph on sidewalk. We will need categories as Car industry. Commercial vs passenger is likely, etc, etc. Also need clear responsibilities and powers.

Qu.15

Qu. 16

There may be merit in this type of approach with volunteer test users, who are not company representatives. I note Tesla is Beta testing its FSD system. This should be monitored by the regulation body. The number and diversity of users should be defined as a vaccine trial to provide maximum learning. Trials need to further accommodate geographic and seasonal variations. I note my Tesla doesn't like shadows, and brakes suddenly, which is unsafe and on the roads now.

Qu. 17

Yes. The monitoring of faults and compiling into patterns would present an opportunity to avoid major incidents. Often an incident is the combination of multiple smaller faults.

Data regarding breakdown faults needs to be provided in a neutral format to regulators. This would help with current systems too.

A body of independent regulators would be useful. The information access should be comprehensive, including sensors failure data rates and sensor misinterpretation rates. Weather.

Qu 18

Yes. I note discussion about automatic data acquisition (AI) and I am concerned that this makes errors hard to find and impossible to attribute. AI learning will also favour current biases (eg. Pedestrian and cyclists). We need to avoid any software being automatically developed as this makes processes opaque, reinforces bias and diminishes responsibilities. These will diminish safety and societal benefits.

Please note training is unrealistic, imo.

737 Max failed due to sensor failure. Sensor failure is a clear mode and would need to be monitored.

Qu 19

UK only is a folly. We are a small market and if we want the best companies to work with then we need to be in a global or at least regional regulation framework. It is the lesion which we are learning the hard way. Car manufacturing in UK is already damaged. Let's not pretend we are a rule maker, when we a bit player.

Cybersecurity is massively important. Nissan Leaf had a simple password in the early days. There was little functionality in the app. Autonomous driving such as calling car should not be available at any time as all systems are breakable. As in aircraft there should be a switch to stop AV mode in the car and it should always be possible to take command. PLease see 737 Max experience, where the machine caused the multiple fatalities.

This chapter also discussed training and as in flying the users need to be instructed in the systems. This needs to be a regulated activity too. Boeing did not want to have to pay for the additional training due to the MCAS system, and pretended the changes were minor. All changes will need to be communicated to the regulator and decisions on retraining will be needed if necessary.

The architecture of the software should allow for updates without impacting full system. Eg. Map updates.

Qu 20

I recommend a single body, as the regulation needs to be ongoing with rapid responses at times. Monitoring, assessment and improvement notices should be ongoing activity. The aerospace industry puts out regular advisories and enforcement notices.

The problem of capture is real. The 737 case illustrates clearly and the commercial pressures to compete can be insidious.

A whistleblower system should provide additional safeguards against deliberate hiding of uncomfortable facts.

If the separation from regulator and business is secure then there is no need for 2 agencies.

I would suggest that there should be full disclosure of all interests by regulation board members and these posts should be held for a maximum tenure to avoid capture. (10 years would seem reasonable with 2 terms).

Qu21

They need an appointment board. There should be a completely separate appointment board, which should be equally limited in term and appoint. The appointment board should be made up of representatives of wider society (disabled and cycling groups should both have representatives on this board).

Perhaps this board would have powers of oversight and the ability to report and if necessary, suspend or remove members.

Qu22

22. Financial penalties will be a deterrent and an accelerant for change and should be applied for the less egregious crimes. It may be noted that a car driver can often have his license withdrawn for multiple speeding offences. I can see no reason why an Autonomous vehicle should not suffer the same fate. Cyclists are often put in significant danger by car drivers, and it is noteworthy that fatalities for pedestrians and cyclists are much greater than car drivers. Choices about which transport mode are often made based on safety. Safety is given as the main reason for not cycling in multiple surveys.

With the UK declaring a climate emergency, it is imperative that new regulation does not degrade and should aim to improve emissions. The CCC has identified demand management as a major contributor to reductions, with modal shift to cycling and walking identified. The improvement of access to roads for other users must be part of any new regulation. Thus, the safety grade needs to reflect this and the system of fines and restrictions to operate need to be more severe than legacy systems. This is the case in aircraft where the bar is raised for any new type. It may be also noted that an automatic system may behave in unpredictable ways that are not currently illegal but may make reduce safety for other users. (eg. High acceleration, hard braking, high average speed, steering that is sudden and unexpected, stopping in middle of the road, etc).

Should also investigate when system crashes or vehicle becomes stationary.

Qu23

The problem is the complexity of proving guilt in these cases where a jury of peers is unlikely to be able to comprehend the systems or apportion blame. Motor accidents cause around 1700 deaths in the UK, and the death rate in other countries is much higher. The importance of regulation here is high and to remove criminal liability is to remove an important deterrent to bad or poor behaviour. These systems are however highly complex, and the regulations need to clearly apportion responsibility such that people can understand who and what they are responsible for. It is a high burden, but these systems are high risk.

In short NO. Criminal negligence is of paramount importance to not degrade safety as these complex systems will at any rate make apportioning of blame near impossible. It is a necessary part of the regulation that the systems are transparent, and responsibilities clearly held. A whistle blower system must be part of regulation to allow for a chance to stop bad actors early.

Qu. 24. There should be a system of monetary fines for small infringements which may be time based to encourage early correction.

No. this is not sufficient. Regulator should have powers to remove license from ADSE.

Q25

Recommendations are not sufficient. Fines for clear breaches of safety systems are necessary.

Repeated breaches should be sanctioned with removal of license to operate. Please note that the vulnerable are mainly outside the vehicle and they need to have representation to mitigate against bad actors.

Systemic risk needs to be avoided.

-26. This is not criminal responsibility. As such it is a weakening of an already weak law, where the burden of proof is already biased against the dead who have little evidence to offer up. Gross negligence needs to remain. Otherwise 737max happens.

737Max lessons show a weak under resourced regulator has little ability to understand and regulate complex safety systems which include millions of lines of software. PS. Where is the regulator?

737 Max lesson is that whistle-blower protection is required to highlight unsafe working in business that prioritises profit over safety.

29. Someone could be in direct sight and then a bus/hgv obscures their vehicle. Not really tenable in real life. Also terrorist potential?

30. No

I would recommend against.

31. Yes

32. Yes

33 No

34 yes

35 yes

36 Yes. Please be sure that sensors are cleaned. Eyes of the Automated system.

Remote operation

37. Yes.

38 yes. Except 2(b) Mirror Aircraft manufacturer and airline. Both need licenses.

39. Yes

40 Yes

41. No. Too early to say if this is a good idea.

42. yes

44. Yes

45 yes

46. Yes, vitally important

Information presentation. I believe that ISO 14971 relates to safety system designs. FMEA offers a good framework for identifying and quantifying risks. This needs to be mandated in bill, IMO.

47 yes

49 No.

The safety of AVs should not be predicated on additional infrastructure, which may hinder other uses or at least take resources away from human based systems.

50. No, see comment above. Machines do not have rights. The car industry with road infrastructure is already vastly over provided for in space and resources, and caused multiple unforeseen consequences on society; air pollution and obesity being the most obvious. We need to rebalance the system away from the car. A ban on AV specific infrastructure would at least avoid further intrusion on human society.

52. Suspect that this will reinforce current biases. NB. Insurance companies ask for non-disclosure after making payment for injuries. This system does not allow for data to be collected and amalgamated for better system design. Eg. An AV has tendency to stop for no reason and park in the middle of the road. Other cars hit it, but they are found liable. Information is not shared.

This is an important aspect of AV safety feedback and good data needs to be shared by insurance companies.

53. Clearly. It would seem sensible for ADSE to be last person of responsibility.

There seem to be no sanctions for poor operation. Further some additional qualifications may be needed for such remote driving.

55. Yes

56 yes

57. yes

58. yes